Documentation
GCenter V2.5.3.103

Version: 4

Translated from original manual version 4

Creation date: December 2024

Update date: June 2025

@Copyright: Gatewatcher - December 2024
Disclosure or reproduction of this document, and use or disclosure of the contents hereof,
are prohibited except with prior written consent. Any breach shall giveright to damages.
All rights reserved, particularly in the case of patent application or other registrations.

Table of contents

Table of contents 3

1 Description 9
1.1 Introduction . . . 9
1.2 Overview of the TAP . . . 9
1.3 Presentation of the GCap . . . 9
1.4 Presentation of the GCenter . . . 10
1.4.1 Different server models . . . 10
1.4.2 List of the GCenter inputs / outputs . . . 10
1.5 Presentation of Reflex . . . 13
1.6 Interconnection between devices . . . 13
1.6.1 Viewing communication flows . . . 13
1.6.2 Example of architectures . . . 17

2 Operation 20
2.1 Detection Engines . . . 20
2.1.1 Introduction of engines . . . 20
2.1.2 Malcore engine . . . 21
2.1.3 Shellcode detect engine . . . 30
2.1.4 Malicious Powershell detect engine . . . 35
2.1.5 Sigflow engine . . . 42
2.1.6 DGA detect engine . . . 64
2.1.7 Malcore retroanalyzer engine . . . 70
2.1.8 Active CTI engine . . . 71
2.1.9 Retro hunt engine . . . 77
2.1.10 Ransomware detect engine . . . 84
2.1.11 Beacon detect engine . . . 89
2.1.12 Yara engine . . . 95
2.1.13 Detection by GScan . . . 101
2.2 Management of the GCenter software . . . 102
2.2.1 Dedicated modules for managing updates: Threat DB update and Software update . . . 102
2.2.2 Upgrade presentation . . . 103
2.2.3 Update presentation . . . 104
2.2.4 Hotfix presentation . . . 105
2.2.5 Release note . . . 106
2.2.6 Overview of the backup and restoration . . . 106
2.3 Data use . . . 107
2.3.1 Detection data . . . 108
2.3.2 Data related to detection results . . . 109
2.3.3 Management and system status data . . . 109
2.3.4 Data retention . . . 110
2.3.5 Deleting data . . . 111
2.4 GApps management . . . 111
2.5 Interconnection with external systems . . . 111
2.5.1 Introduction . . . 111
2.5.2 Connection to a MIPS server . . . 112
2.5.3 Connection to Syslog servers . . . 112
2.5.4 Connection to a netdata server . . . 113
2.5.5 Access for a monitoring server . . . 113
2.6 API . . . 113
2.6.1 Introduction . . . 113
2.6.2 Use via the swagger GUI . . . 114
2.6.3 Use via CURL . . . 114
2.6.4 Authentication and access to the API . . . 115
2.6.5 Endpoints list . . . 115

3 Characteristics 116
3.1 Mechanical characteristics of the Center . . . 116
3.2 Electrical characteristics of the GCenter . . . 116
3.3 Functional characteristics of tGCenter . . . 116

4 Accounts **117**
4.1 List of accounts . . . 117
4.2 Setup account from the configuration menu . . . 117
4.2.1 Account from the configuration menu . . . 117
4.2.2 Related principles . . . 117
4.2.3 Functions reserved to the setup account . . . 118
4.3 Web interface accounts and their management . . . 118
4.3.1 Web Interface Accounts . . . 118
4.3.2 Functions allowed with the group or role `operator` . . . 119
4.3.3 Functions authorized with the group or role `administrator` . . . 119
4.3.4 Functions allowed in the admin account . . . 119
4.3.5 Summary tables of the menus per level . . . 119
4.3.6 Related principles . . . 121
4.3.7 Creating local users . . . 121
4.3.8 LDAP integration / Active Directory . . . 122
4.3.9 Audit trail . . . 122

5 Overview of the GCenter graphic interfaces **124**
5.1 Overview of the configuration menu . . . 124
5.2 Overview of the WEB UI . . . 125
5.2.1 Navigation bar . . . 126
5.2.2 Title bar . . . 127
5.2.3 Central screen . . . 127
5.3 Overview of the Kibana GUI . . . 127
5.3.1 Overview of the Kibana GUI . . . 127
5.3.2 Configuration of the Kibana GUI . . . 127
5.3.3 Main tabs . . . 128
5.3.4 Native dashboards of the `Alerts` tab . . . 128
5.3.5 Native dashboards of the `Network Metadata` tab . . . 130
5.3.6 Native dashboards of the `Administration` tab . . . 131
5.3.7 Data exploitation . . . 131
5.4 The legacy WebUI . . . 131
5.4.1 Overview of the legacy WebUI . . . 131
5.4.2 Description of the legacy WebUI . . . 132
5.5 Overview of the Netdata User Interface (Gstats) . . . 133
5.6 Screens of the WebUI navigation bar . . . 134
5.6.1 WebUI `Home` screen . . . 134
5.6.2 WebUI `Top risk` screen . . . 138
5.6.3 WebUI `Top Relations` screen . . . 140
5.6.4 WebUI `Overview` screen . . . 141
5.6.5 WebUI `Relations` screen . . . 146
5.6.6 WebUI `Alerts` screen . . . 147
5.6.7 WebUI `Hunting` screen . . . 156
5.6.8 WebUI `Users` screen . . . 156
5.6.9 WebUI `Assets` screen . . . 159
5.6.10 WebUI `GScan` screen . . . 161
5.6.11 Management of the current account . . . 163
5.7 Presentation of the WebUI menu bar screens . . . 166
5.7.1 Overview of the menu bar . . . 166
5.7.2 `Detection Strategy` menu . . . 166
5.7.3 `Health` menu . . . 245
5.7.4 `Administration` menu . . . 255
5.7.5 `Help` menu . . . 301
5.8 Graphical API . . . 311
5.8.1 Overview of the API interface . . . 311
5.8.2 Endpoints list . . . 317

6 Use case of the configuration menu: setup account **327**
6.1 Direct connection to the GCenter configuration menu with keyboard and monitor . . . 327
6.1.1 Introduction . . . 327
6.1.2 Preliminary operations . . . 327
6.1.3 Procedure to connect the monitor and keyboard . . . 327
6.1.4 Procedure to find out or changing the iDRAC network settings via the BIOS . . . 327
6.2 Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server) . . . 328
6.2.1 Introduction . . . 328
6.2.2 Preliminary operations . . . 328
6.2.3 Procedure . . . 328
6.3 Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode . . . 329
6.3.1 Introduction . . . 329
6.3.2 Preliminary operations . . . 330
6.3.3 Procedure on the remote PC running Linux . . . 330
6.3.4 Procedure on the remote PC running Windows . . . 330
6.4 Direct connection to the GCenter configuration menu via SSH . . . 330
6.4.1 Introduction . . . 330
6.4.2 Preliminary operations . . . 330

6.4.3 Procedure on the remote PC running Linux . . . 330
6.4.4 Procedure on the remote PC running Windows . . . 330
6.5 `About` command . . . 331
6.5.1 Introduction . . . 331
6.5.2 Prerequisites . . . 331
6.5.3 Preliminary operations . . . 331
6.5.4 Procedure . . . 332
6.6 `Tech Support` command . . . 332
6.6.1 Introduction . . . 332
6.6.2 Prerequisites . . . 332
6.6.3 Preliminary operations . . . 332
6.6.4 Procedure . . . 333
6.7 `Keyboard` command . . . 333
6.7.1 Introduction . . . 333
6.7.2 Prerequisites . . . 333
6.7.3 Preliminary operations . . . 333
6.7.4 Procedure . . . 333
6.8 `Authentication` command . . . 333
6.8.1 Introduction . . . 333
6.8.2 Prerequisites . . . 334
6.8.3 Preliminary operations . . . 334
6.8.4 Procedure to change the setup account password . . . 334
6.9 `DateTime` command . . . 335
6.9.1 Introduction . . . 335
6.10 `Network` command . . . 337
6.10.1 Introduction . . . 337
6.10.2 Prerequisites . . . 337
6.10.3 Preliminary operations . . . 337
6.10.4 Procedure to access the network interface configuration menu . . . 337
6.10.5 Procédure to configure the hostname . . . 338
6.10.6 Procedure to configure an interface . . . 338
6.10.7 Procedure to configure the DNS . . . 338
6.10.8 Procedure to configure the NTP . . . 339
6.11 `Arp Manager` command . . . 339
6.11.1 Introduction . . . 339
6.11.2 Prerequisites . . . 339
6.11.3 Preliminary operations . . . 339
6.11.4 Procedure to access to the `Arp Manager` submenu . . . 339
6.11.5 Procedure A: Adding an ARP entry . . . 340
6.11.6 Procedure B: Delete an ARP entry . . . 340
6.11.7 Procedure C: Clearing the ARP cache . . . 341
6.12 `Diagnose` command . . . 341
6.12.1 Introduction . . . 341
6.12.2 Prerequisites . . . 341
6.12.3 Preliminary operations . . . 341
6.12.4 Procedure . . . 342
6.13 `GCenter Services Management` command . . . 342
6.13.1 Introduction . . . 342
6.13.2 Prerequisites . . . 343
6.13.3 Preliminary operations . . . 343
6.13.4 Procedure to access to `GCenter Services Management` sub-menu . . . 343
6.13.5 Procedure A: Restarting an application . . . 344
6.13.6 Procedure B: Reset a service . . . 344
6.13.7 Procedure C: Restarting a service . . . 344
6.14 `Elasticsearch storage mode` command . . . 345
6.14.1 Introduction . . . 345
6.14.2 Prerequisites . . . 345
6.14.3 Preliminary operations . . . 345
6.14.4 Procedure . . . 345
6.15 `LPM Mode` command . . . 346
6.15.1 Introduction . . . 346
6.15.2 Prerequisites . . . 347
6.15.3 Preliminary operations . . . 347
6.15.4 Procedure . . . 347
6.16 `Restart` command . . . 347
6.16.1 Introduction . . . 347
6.16.2 Prerequisites . . . 347
6.16.3 Preliminary operations . . . 347
6.16.4 Procedure . . . 347
6.17 `Shutdown` command . . . 348
6.17.1 Introduction . . . 348
6.17.2 Prerequisites . . . 348
6.17.3 Preliminary operations . . . 348
6.17.4 Procedure . . . 348
6.18 `Reset` command . . . 348

6.18.1 Introduction . . . 348
6.18.2 Prerequisites . . . 348
6.18.3 Preliminary operations . . . 348
6.18.4 Procedure . . . 349
6.19 `Exit` command . . . 349
6.19.1 Introduction . . . 349
6.19.2 Prerequisites . . . 349
6.19.3 Preliminary operations . . . 349
6.19.4 Procedure . . . 349
6.20 Switching to a double interface configuration . . . 349
6.20.1 Introduction . . . 349
6.20.2 Prerequisites . . . 350
6.20.3 Preliminary operations . . . 350
6.20.4 Procedure for displaying the current configuration . . . 350
6.20.5 Procedure for switching from single to double interface configuration . . . 351
6.21 Switching to a single-interface configuration . . . 351
6.21.1 Introduction . . . 351
6.21.2 Prerequisites . . . 351
6.21.3 Preliminary operations . . . 351
6.21.4 Procedure for displaying the current configuration . . . 351
6.21.5 Procedure for switching from double to single interface configuration . . . 352

7 Use cases at the operator or analyst level 353
7.1 Connection to the GCenter web interface via a web browser . . . 353
7.1.1 Introduction . . . 353
7.1.2 Prerequisites . . . 353
7.1.3 Preliminary operations . . . 353
7.1.4 Procedure . . . 353
7.2 Managing current user . . . 354
7.2.1 Changing the checking account password . . . 354
7.2.2 Changing some of the current user's information . . . 356
7.3 Configuring the Sigflow engine . . . 358
7.3.1 Managing the Sigflow engine rule sources . . . 358
7.3.2 Managing a Sigflow engine ruleset . . . 366
7.3.3 Updating rules sources . . . 378
7.3.4 Modifying Sigflow engine rules . . . 379
7.3.5 Creation of automatic alarm limits . . . 385
7.4 Configuring GCaps using the `GCaps Profiles` . . . 389
7.4.1 Customizing the setting of the GCap profile . . . 389
7.4.2 Configuring the detection rulesets via the GCap profile . . . 391
7.4.3 Configuring the Base variables parameters via the GCap profile . . . 397
7.4.4 Configuring the network variables parameters via the GCap profile . . . 402
7.4.5 Configuring the flow timeouts via the GCap profile . . . 407
7.4.6 Configuring the file reconstruction rules via the GCap profile . . . 408
7.4.7 Configuring filters on targeted parts of the analyzed traffic via the GCap profile . . . 412
7.5 Analyzing the engine alerts . . . 415
7.5.1 Analyzing the Malcore alerts . . . 415
7.5.2 Analyzing the Shellcode detect alerts . . . 423
7.5.3 Analyzing the Malicious Powershell detect alerts . . . 427
7.5.4 Analyzing the Sigflow alerts . . . 434
7.5.5 Analyzing the DGA detect alerts . . . 444
7.5.6 Analyzing the Malcore retroanalyzer alerts . . . 450
7.5.7 Analyzing the Active CTI alerts . . . 451
7.5.8 Analyzing the Retrohunt alerts . . . 454
7.5.9 Analyzing the Ransomware detect alerts . . . 457
7.5.10 Analyzing the Beacon detect alerts . . . 460
7.5.11 Analyzing the Yara alerts . . . 464
7.6 Using of NDR dashboards . . . 470
7.6.1 Introduction . . . 470
7.6.2 Links associated . . . 470
7.6.3 Prerequisites . . . 470
7.6.4 Preliminary operations . . . 470
7.6.5 Procedure to retrieve information related to an alert . . . 471
7.6.6 Procedure to process the equipment . . . 473
7.6.7 Procedure to process the users . . . 475
7.6.8 Procedure to manage association rules . . . 476
7.6.9 Procedure to analyze the relationship between equipment and users . . . 478
7.7 Using of the Kibana dashboards . . . 480
7.7.1 Introduction . . . 480
7.7.2 Links associated . . . 480
7.7.3 Prerequisites . . . 480
7.7.4 Preliminary operations . . . 480
7.7.5 Procedure introducing the Kibana investigation method . . . 480
7.8 Detecting with GScan . . . 482
7.8.1 Introduction . . . 482

7.8.2 Links associated . . . 482
7.8.3 Prerequisites . . . 482
7.8.4 Preliminary operations . . . 483
7.8.5 Procedure . . . 483
7.8.6 Ex post facto search procedure . . . 487
7.8.7 Procedure to view the history . . . 487
7.9 Configuring Metadata Rate Limiters . . . 488
7.9.1 Introduction . . . 488
7.9.2 Links associated . . . 488
7.9.3 Prerequisites . . . 488
7.9.4 Preliminary operations . . . 488
7.9.5 Procedure to view metadata . . . 488
7.9.6 Procedure to setup the limiter then activate . . . 490
7.10 Logging out of the GCenter web interface . . . 490
7.10.1 Introduction . . . 490
7.10.2 Prerequisites . . . 490
7.10.3 Preliminary operations . . . 490
7.10.4 Procedure . . . 491

8 Use cases of the administrator level 492
8.1 Connecting to the GCenter web interface via a web browser . . . 492
8.1.1 Introduction . . . 492
8.1.2 Prerequisites . . . 492
8.1.3 Preliminary operations . . . 492
8.1.4 Procedure . . . 492
8.2 Configuring the NDR . . . 493
8.2.1 Introduction . . . 493
8.2.2 Links associated . . . 493
8.2.3 Prerequisites . . . 493
8.2.4 Preliminary operations . . . 493
8.2.5 Procedure to access the `Data Exports` window for an administrator account . . . 494
8.2.6 Procedure to enable the `Assets and users tracking` and `Relationship tracking` functions . . . 494
8.2.7 Procedure to disable the `Assets and users tracking` and `Relationship tracking` functions . . . 494
8.2.8 Procedure to configure the Elasticsearch retention . . . 495
8.3 Administrating a GCap . . . 495
8.3.1 Pairing a GCap with the GCenter . . . 495
8.3.2 Pairing again a GCap . . . 498
8.4 Managing the GCenter backup and restoration . . . 501
8.4.1 Setting the backup . . . 501
8.4.2 Operating the backup . . . 503
8.4.3 Operating the restoration . . . 504
8.5 Managing of the GCenter software . . . 508
8.5.1 Configuring automatic update of signatures and/or anti-viral engines . . . 508
8.5.2 Installing an update manually . . . 512
8.5.3 Installing a hotfix . . . 514
8.5.4 Installing of an upgrade . . . 516
8.6 Administrating the GCenter . . . 519
8.6.1 Configuring the export data to a SIEM via the syslog protocol . . . 519
8.6.2 Configuring the export data to ETL Logstash via the syslog protocol . . . 520
8.6.3 Creating a POC Logstash . . . 524
8.6.4 Configuring the connection to the MISP . . . 525
8.6.5 Deleting data (log files) . . . 526
8.6.6 Generating and loading files for diagnosis . . . 528
8.6.7 Using an endpoint API . . . 530
8.6.8 Managing the license . . . 534
8.6.9 Configuring the GCenter . . . 538
8.7 Managing user accounts . . . 540
8.7.1 Creating local user . . . 540
8.7.2 Changing some of a local user's information . . . 542
8.7.3 Resetting a local user's password . . . 543
8.7.4 Deleting a local user . . . 545
8.7.5 Displaying of the connection status between the GCenter and the LDAP server . . . 546
8.7.6 Enabling the connection between the GCenter and the LDAP server . . . 547
8.7.7 Configuring the connection between the GCenter and the LDAP server . . . 548
8.7.8 Configuring the users and groups defined on LDAP / ActiveDirectory . . . 551
8.7.9 Viewing the authentication history . . . 553
8.7.10 Configuring the authentication history . . . 554
8.7.11 Managing an API access token . . . 556
8.7.12 Managing the password policy . . . 558
8.8 Configuring the detection engines . . . 561
8.8.1 Setting up the Malcore engine . . . 561
8.8.2 Managing the Ignore list of the Malcore engine . . . 563
8.8.3 Setting up the Malcore retroanalyzer engine . . . 566
8.8.4 Setting up the Yara engine . . . 568
8.8.5 Setting up the DGA detect engine . . . 571

8.8.6 Managing the Ignore list of the DGA detect engine . . . 574
8.8.7 Setting up the Malicious Powershell detect engine . . . 576
8.8.8 Setting up the Shellcode detect engine . . . 579
8.8.9 Setting up the Active CTI engine . . . 582
8.8.10 Setting up the retro hunt engine . . . 584
8.8.11 Setting up the Ransomware detect engine . . . 586
8.8.12 Managing the Ignore list of the Ransomware detect . . . 589
8.8.13 Setting up the beacon detect engine . . . 591
8.8.14 Managing the Ignore list of the Beacon detect . . . 594
8.9 Managing current user . . . 596
8.9.1 Changing the checking account password . . . 596
8.9.2 Changing some of the current user's information . . . 598
8.10 Monitoring the netdata . . . 600
8.10.1 Configuring the Netdata polling interface . . . 600
8.10.2 Configuring the Netdata export interface . . . 602
8.10.3 Setting up a Netdata server . . . 603
8.10.4 Using a Netdata server . . . 606
8.11 Logging out of the GCenter web interface . . . 608
8.11.1 Introduction . . . 608
8.11.2 Prerequisites . . . 608
8.11.3 Preliminary operations . . . 609
8.11.4 Procedure . . . 609

9 Appendices **610**
9.1 Military Programming Law (MPL) . . . 610
9.1.1 Regulatory reminders . . . 610
9.1.2 Goal Reminders . . . 610
9.1.3 Reminders of requirements . . . 610
9.1.4 MPL applied to the GCenter . . . 611
9.1.5 Groups . . . 612
9.2 Engine log data structure . . . 614
9.2.1 Counters of the header part of logs . . . 614
9.2.2 Counters of the source part of logs . . . 614
9.3 Comparison of the counters between V02 and V103 . . . 634
9.3.1 Beacon detect engine . . . 634
9.3.2 Malcore engine . . . 634
9.3.3 DGA engine . . . 636
9.3.4 Malicious powershell engine . . . 636
9.3.5 Shellcode engine . . . 637
9.3.6 Ransomware detect engine . . . 638
9.3.7 Sigflow alert . . . 638
9.3.8 Sigflow dcerpc . . . 639
9.3.9 Sigflow DGA . . . 640
9.3.10 Sigflow dhcp . . . 641
9.3.11 Sigflow dnp3 . . . 641
9.3.12 Sigflow dns . . . 642
9.3.13 Sigflow file . . . 643
9.3.14 Sigflow ftp . . . 644
9.3.15 Sigflow ftp data . . . 645
9.3.16 Sigflow http . . . 645
9.3.17 Sigflow http2 . . . 646
9.3.18 Sigflow ikev2 . . . 647
9.3.19 Sigflow krb5 . . . 648
9.3.20 Sigflow mqtt . . . 649
9.3.21 Sigflow netflow . . . 649
9.3.22 Sigflow nfs . . . 650
9.3.23 Sigflow rdp . . . 651
9.3.24 Sigflow rfb . . . 652
9.3.25 Sigfmow sip . . . 652
9.3.26 Sigflow SMB . . . 653
9.3.27 Sigflow SMTP . . . 654
9.3.28 Sigflow snmp . . . 655
9.3.29 Sigflow ssh . . . 655
9.3.30 Sigflow tftp . . . 656
9.3.31 Sigflow tls . . . 657
9.3.32 Yara engine . . . 657
9.4 Malcore engine results . . . 657

10 Glossary **659**

Index **661**

Index **661**

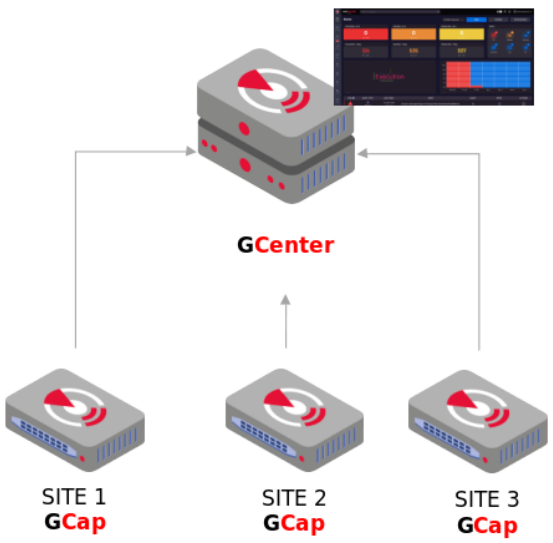
Chapter 1

Description

1.1 Introduction

The AIONIQ solution is Gatewatcher's Intrusion Detection System (IDS).
It includes:

- one or more TAPS
- one or more GCaps
- a GCenter
- the Reflex



1.2 Overview of the TAP

A Test Access Point (TAP) is a passive device enabling the monitoring of a computer network by duplicating certain flows that transit on the network and redirecting them to a detection probe (GCap), for example.
It is possible to connect several TAPs to a GCap, as the latter has several capture interfaces.

1.3 Presentation of the GCap

The GCap is an IDS type detection probe deployed at each site.
It enables:

- Capturing and analyzing network traffic from TAPs
- Reconstructing the files present in the analyzed flow (according to type and size parameters)
- Carrying out an initial analysis
- Generating alerts and / or metadata type events
- Transmitting files / codes / events to the GCenter

For more information, please refer to the GCAP documentation.

1.4 Presentation of the GCenter

The GCenter is the second component of the system working in conjunction with the GCap detection probe
Its main functions include:

- Management of the GCap probe including managing the analysis rules, signatures, health status supervision, and so on.
- In-depth analysis of the files retrieved by the probe
- Administering the system
- Displaying the results of the various analyzes in different dashboards
- Long-term data storage
- Exporting data to third-party solutions such as the Security Information and Events Management (SIEM) system

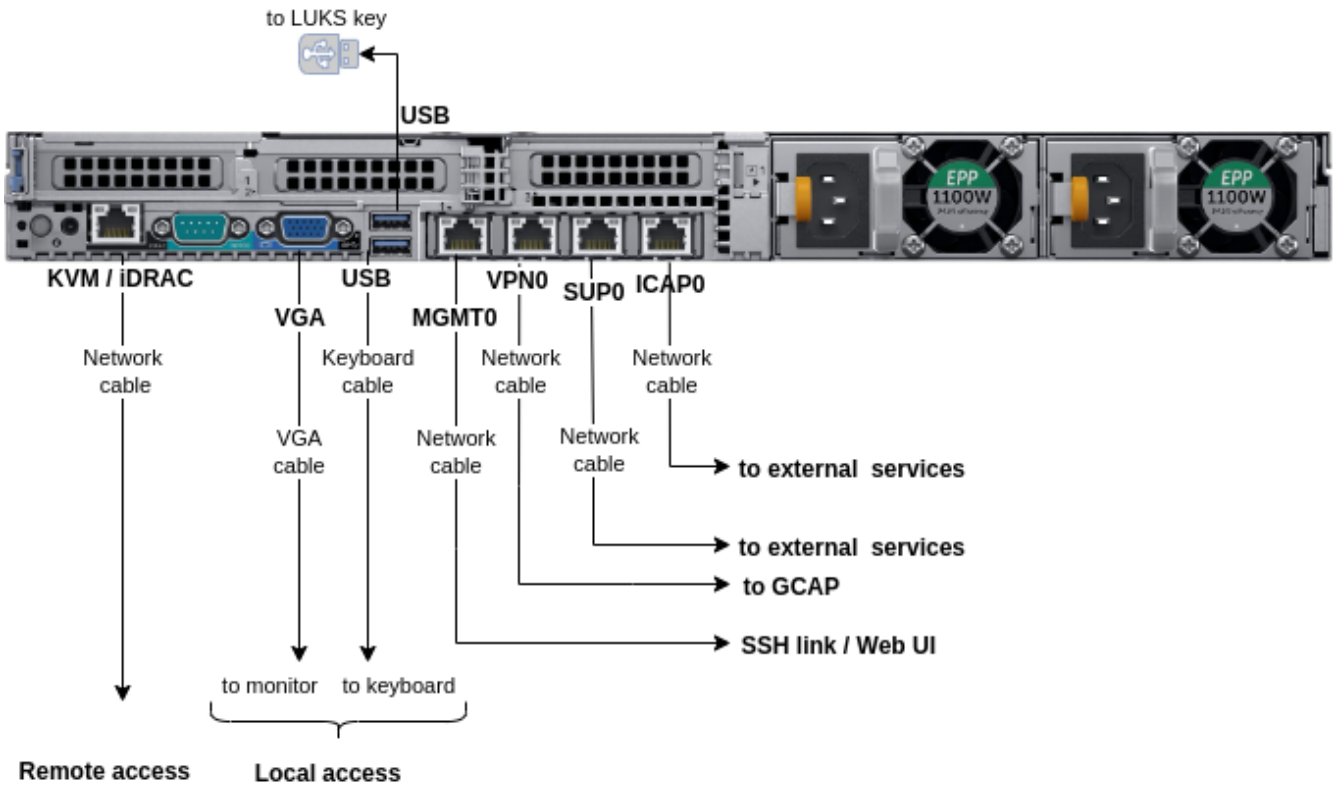
---

1.4.1 Different server models

For more information, please refer to *Mechanical characteristics of the Center*.

1.4.2 List of the GCenter inputs / outputs

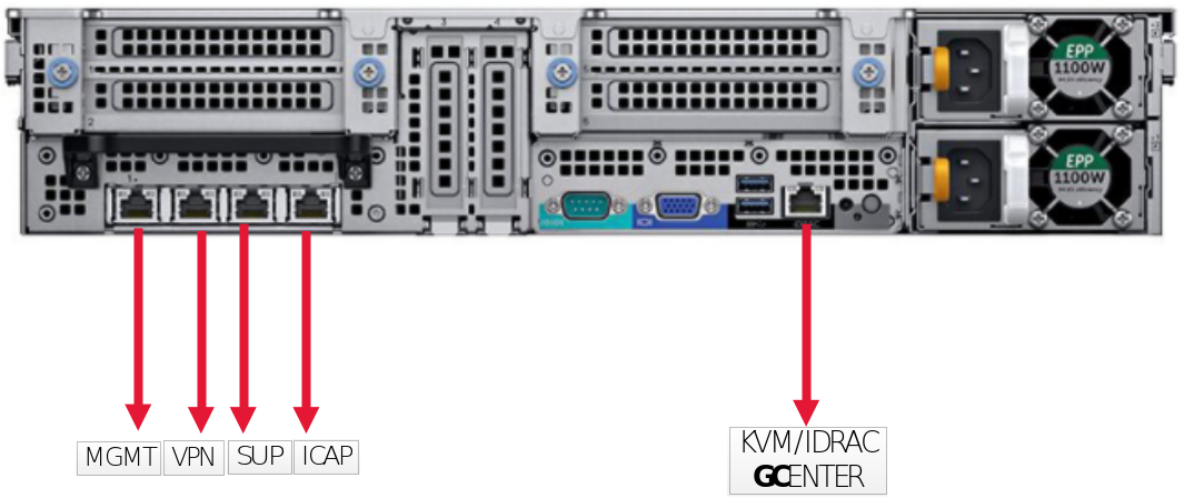
Example of a GCenter server 7100/8100/9100:



The **GCenter** comprises:

Inputs/outputs	Usage
USB and VGA connector	Directly access a keyboard and a monitor This connection mode is deprecated in favor of KVM/IDRAC/XCC and should only be used as a last resort
USB connector	Accommodates the USB key enabling disk decryption (standard Linux Unified Key Setup)
RJ-45 connector `KVM/IDRAC`	Remote access to the server's management and configuration interface
RJ-45 connector `MGMT0`	In the double interface configuration: used for the **Management** and **tunnel** roles In the single interface configuration: used for the **Management** role only
RJ-45 connector `VPN0`	In the double interface configuration: used for the Dedicated VPN interface for the **tunnel** role In the single interface configuration: not used
RJ-45 connector `ICAP0`	Interaction with external services
RJ-45 connector `SUP0`	Interaction with external services
Two power supplies	Redundant server power supplies

Example of a GCenter server 9900/10500:



Note:

Although the names of the interfaces may suggest that they are specifically dedicated, it is possible to use these interfaces for other purposes via the "output interfaces" options.

Viewing these communication links is provided in the section *Interconnection between devices*.

1.4.2.1 Use of USB and VGA connectors

Connecting a keyboard and monitor enables direct access to the GCenter console interface.

Important:

This mode is deprecated. It should only be used during initial installation and for advanced diagnosis.

1.4.2.2 Access to the server's management and configuration interface

Access to this management interface is via HTTPS:

- On a Dell server, this connector is called **iDRAC**. It is noted on the **KVM/IDRAC** diagram
- On a Lenovo server, this connector is called **TSM**. This connector can be identified by a wrench symbol on the bottom of it

---

1.4.2.3 `MGMT0` and `VPN0` network interfaces

The network interfaces `MGMT0` and `VPN0` are connected to:

- The `gcp0` tunnel network interface
- The `gcp1` management network interface

These interfaces enable the following 2 functions:

- Function 1: remote administration through the SSH protocol with access:
  - To the graphical setup/configuration menu
- Function 2: secure communication between the GCenter and the probe through an IPSEC tunnel in order to:
  - Escalate information such as files, alerts, metadata, and so on, derived from analyzing the monitored flows

- Report information on the health of the probe to the GCenter
- Control the probe - analysis rules, signatures, etc

There are 2 configuration possibilities:

- The **single interface configuration**
- The **double interface configuration**

In **single interface configuration**:

- The `MGMT0` interface is used and connected to the `gcp0` tunnel network interface of the GCap
  This interface ensures functions 1 and 2.
- The `VPN0` interface is not used

In **double interface configuration**:

- The `MGMT0` interface is used and connected to the `gcp0` tunnel network interface of the GCap
  This interface ensures function 1.
- The `VPN0` interface is used and connected to the `gcp1` management network interface of the GCap
  This interface ensures function 2.

  The purpose of the double interface configuration is to ensure that the management flow and the interconnection flow between the GCap and the GCenter are separated from each other.

Important:

This configuration of flow separation by interface is mandatory when using the **LPM mode** on the GCenter.

1.4.2.4 Network interfaces `ICAP0` and `SUP0`

These two interfaces enable, if needed, communicating with services external to the solution such as:

- An update server
- A supervision server
- An LDAP server
- A log server or an SIEM
- A storage server for backing up the solution
- etc

1.4.2.5 Electrical connection

The server has two electrical power supplies, each of which has the necessary power to operate the equipment.
It is strongly recommended that each power supply should be connected to a separate power supply.

1.4.2.6 USB connector and LUKS key

During installation, the contents of the disks (excluding /boot) are encrypted using the LUKS standard.
During this process, a unique encryption key is created and placed on the USB stick connected to the equipment.
Upon start-up, the USB key must be plugged into the equipment to allow the disks to be decrypted
It is strongly recommended to make a copy of this key because, in the event of failure, the data on the disks will no longer be accessible.
Once the system is up and running, the USB stick should be removed and placed in a secure place (e.g. in a safe).

1.5 Presentation of Reflex

Reflex is the solution for automation of responses to cybersecurity events offered by Gatewatcher.
It interacts with all the security equipment of the information systems before executing automated processes to process these events.

These automated processes are called playbooks in Reflex.
A playbook is a collection of pre-defined and organized sequences of actions or processes to be used to implement and/or optimize security incident response operations.

Security solutions that Reflex connects to can be, for example, Security Information and Event Management (SIEM), network security tools, data from Threat Intelligence solutions, etc.
For each third-party application on the market to which Reflex must connect, a package is assigned.

For example, the Gatewatcher-NDR package allows:

- To connect Reflex to the GCenter application of the AionIQ Gatewatcher solution
- To retrieve event data, to enrich it or collect alerts, and to respond to them

---

1.6 Interconnection between devices

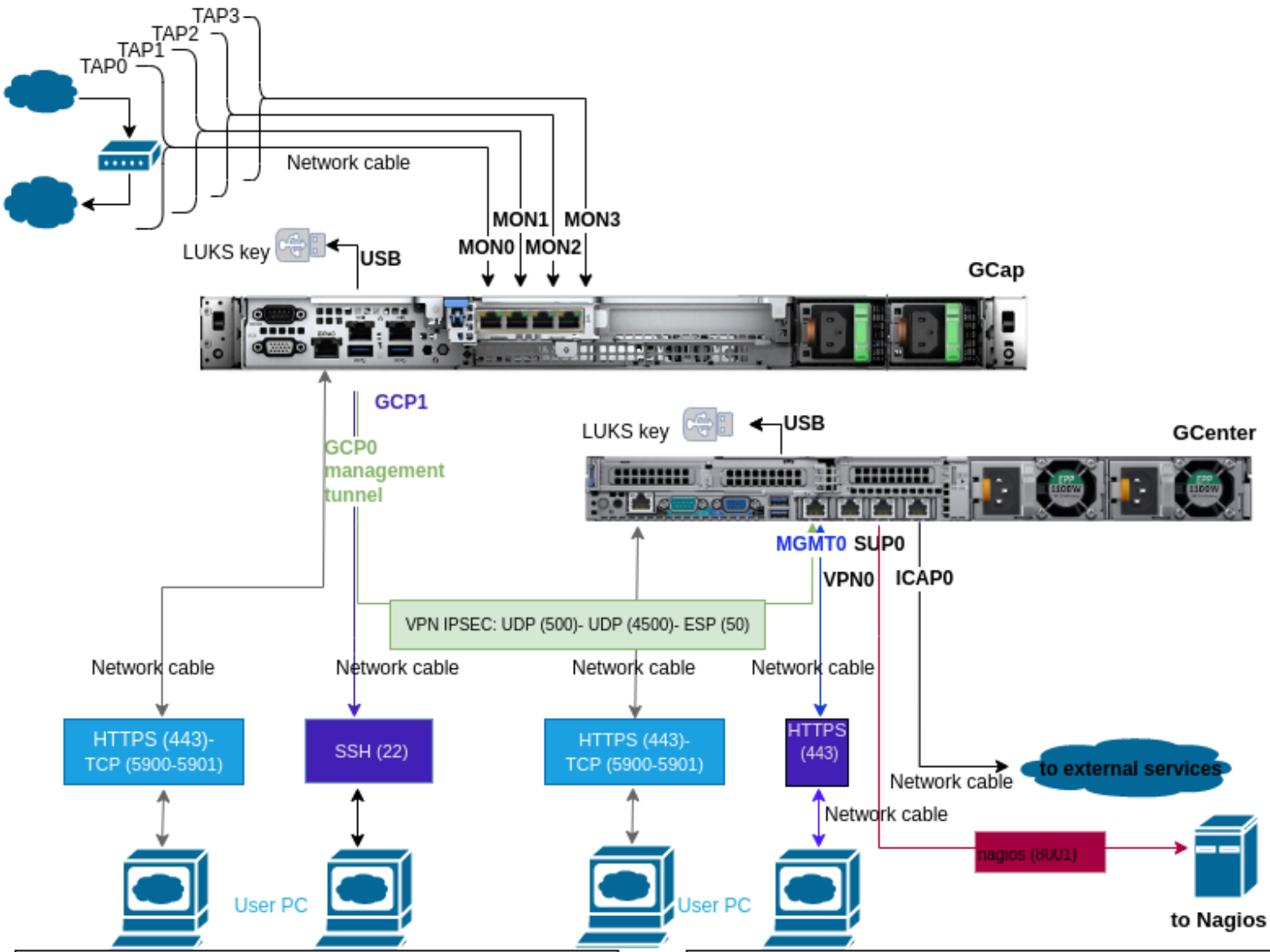
1.6.1 Viewing communication flows

Below, diagrams are displayed representing the various inputs/outputs of the GCap and the GCenter and the corresponding communication flows.
For the **GCap** or for the **GCenter**, there are two possible configurations for communicating:

- The **double interface configuration** is the mandatory mode in the event of a sensitive environment
  In this configuration:
  - One network port is used for secure communication between the probe and the GCenter via IPSEC tunnel
  - Another network port is used for the remote administration via the SSH protocol
- The **single interface configuration**, only one network port is used:
  - For secure communication between the probe and the GCenter via IPSEC tunnel
  - For the remote administration via the SSH protocol

The four cases of configuration are shown below:

1.6.1.1 Configuration: the GCap in single interface configuration and the GCenter in single interface configuration



Keys for the GCap in single interface configuration:

IDRAC: remote access port

- **GCP0**: port used for secure communication between the probe and GCenter via IPSEC tunnel and for the remote administration via SSH protocol

The role of this port is called **management tunnel**

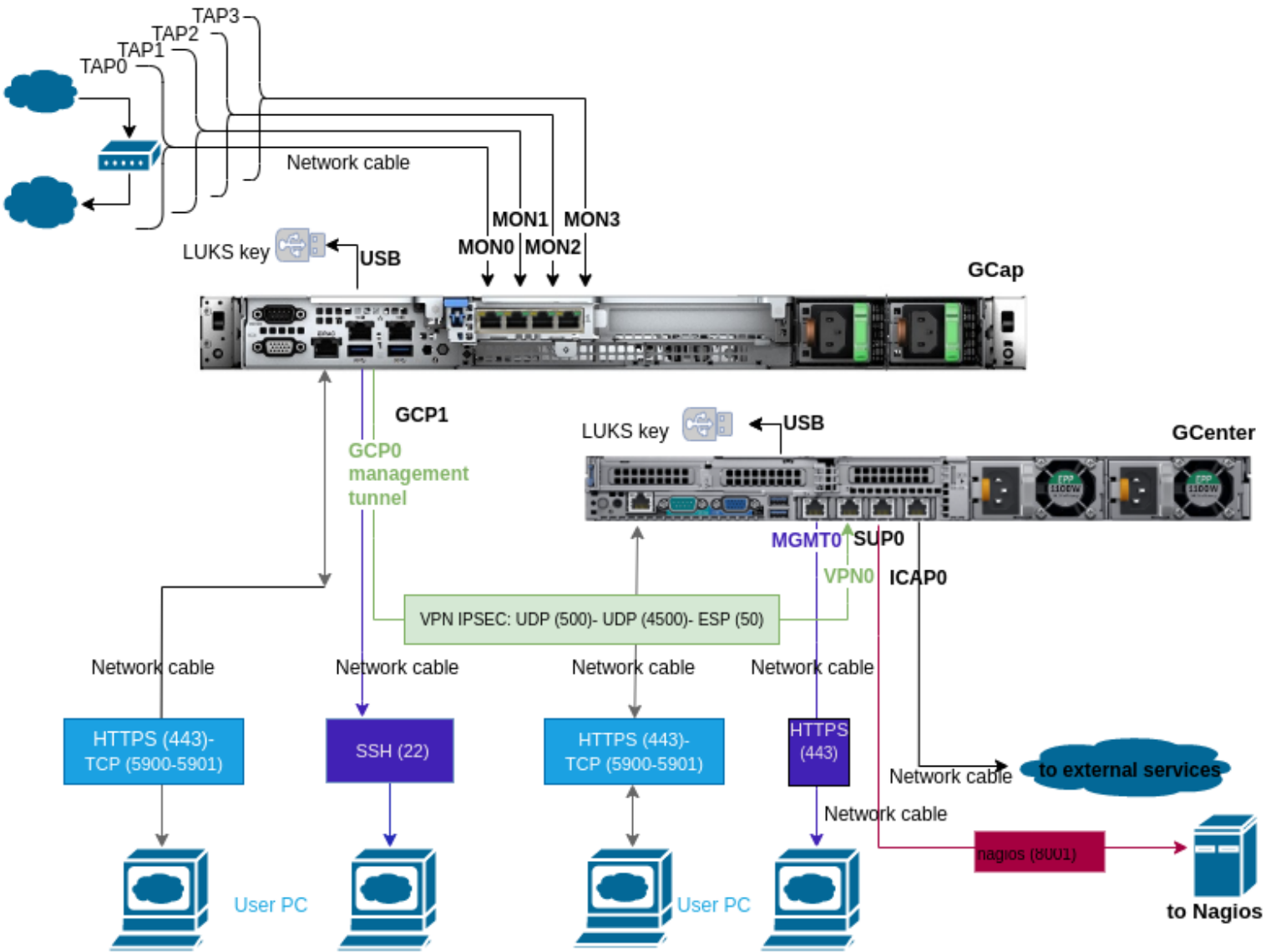
- **GCP1**: port not used
- **MON0 à MON3**: capture ports of the network coming from the TAP

The role of these ports is called **Capture**

Keys for the GCenter in single interface configuration:

- **IDRAC**: remote access port
- **VPN0**: port not used
- **MGNT0**: port used for secure communication between the probe and GCenter via IPSEC tunnel and for the remote administration via SSH protocol
- **SUP0**: port to external services type Nagios
- **ICAP0**: port to external services such as LDAP, SIEM, update

1.6.1.2 Configuration: the GCap in single interface configuration and the GCenter in double interface configuration



Keys for the GCap in single interface configuration:

IDRAC: remote access port

- **GCP0**: port used for secure communication between the probe and GCenter via IPSEC tunnel and for the remote administration via the SSH protocol

The role of this port is called **management tunnel**

- **GCP1**: port not used
- **MON0 à MON3**: capture ports of the network coming from the TAP

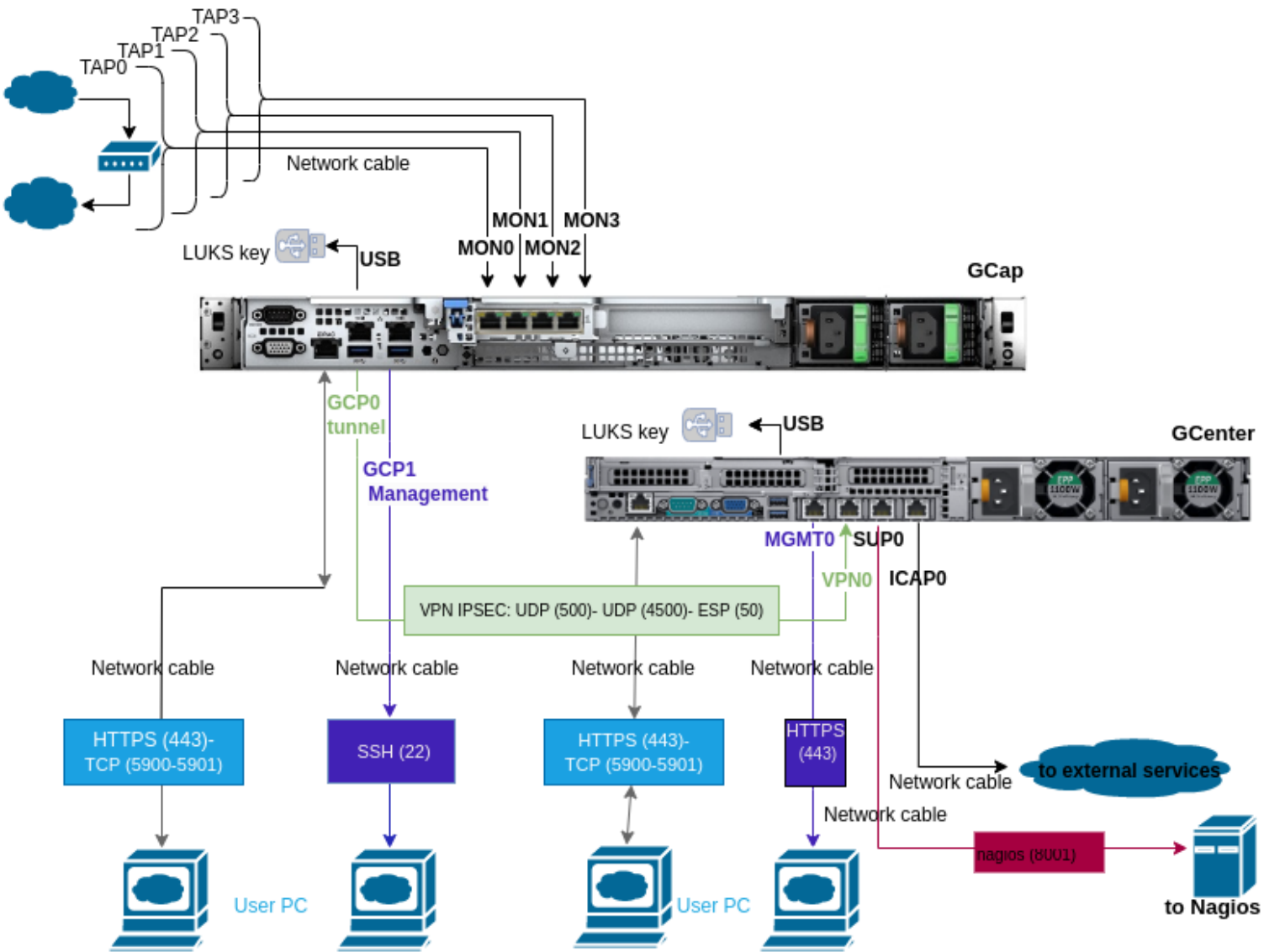
The role of these ports is called **Capture**

Keys for the GCenter in double interface configuration:

- **IDRAC**: remote access port
- **VPN0**: port used for communication secure between the probe and the GCenter via IPSEC tunnel
- **MGNT0**: port used in administration remote via HTTPS protocol
- **SUP0**: port to external services type Nagios
- **ICAP**: port to external services such as LDAP, SIEM, update

@Copyright: December 2024, Gatewatcher

1.6.1.3 Configuration: the GCap in double interface configuration and the GCenter in double interface configuration



Keys for the GCap in double interface configuration:

- **IDRAC**: remote access port
- **GCP0**: port used for communication secure between the probe and GCenter via IPSEC tunnel

The role of this port is called **tunnel**

- **GCP1**: port used for administration remote via SSH protocol

The role of this port is called **Management**

- **MON0 à MON3**: capture ports of the network coming from the TAP

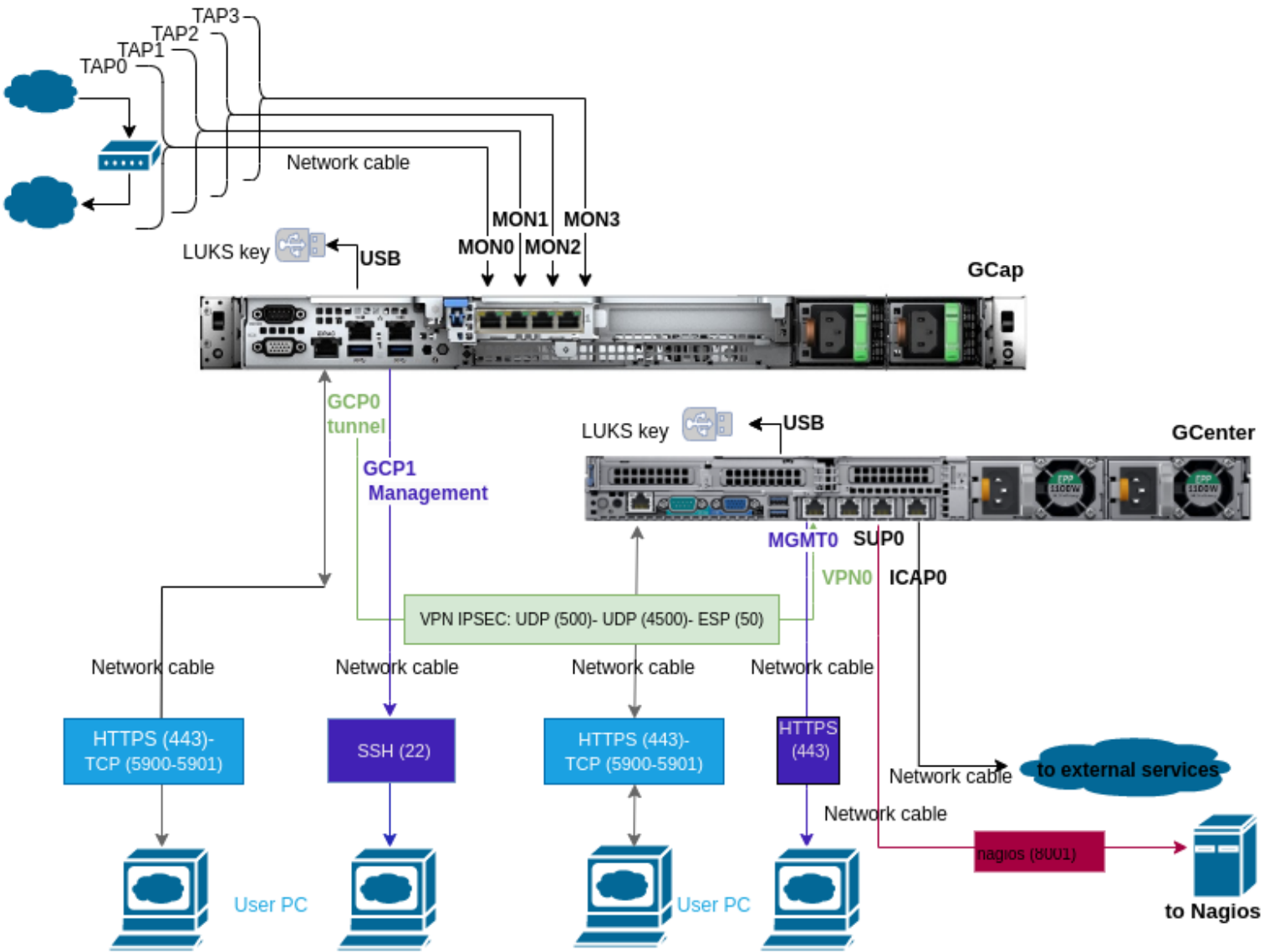
The role of these ports is called **Capture**

Keys for the GCenter in double interface configuration:

- **IDRAC**: remote access port
- **VPN0**: port used for communication secure between the probe and the GCenter via an IPSEC tunnel.
- **MGNT0**: port used in administration remote via HTTPS protocol
- **SUP0**: port to external services type Nagios
- **ICAP**: port to external services such as LDAP, SIEM, update

@Copyright: December 2024, Gatewatcher

1.6.1.4 Configuration: the GCap in double interface configuration and the GCenter in single interface configuration



Keys for the GCap in double interface configuration:

- **IDRAC**: remote access port
- **GCP0**: port used for communication secure between the probe and GCenter via IPSEC tunnel

The role of this port is called **tunnel**

- **GCP1**: port used for administration remote via the SSH protocol

The role of this port is called **Management**

- **MON0 à MON3**: capture ports of the network coming from the TAP

The role of these ports is called **Capture**

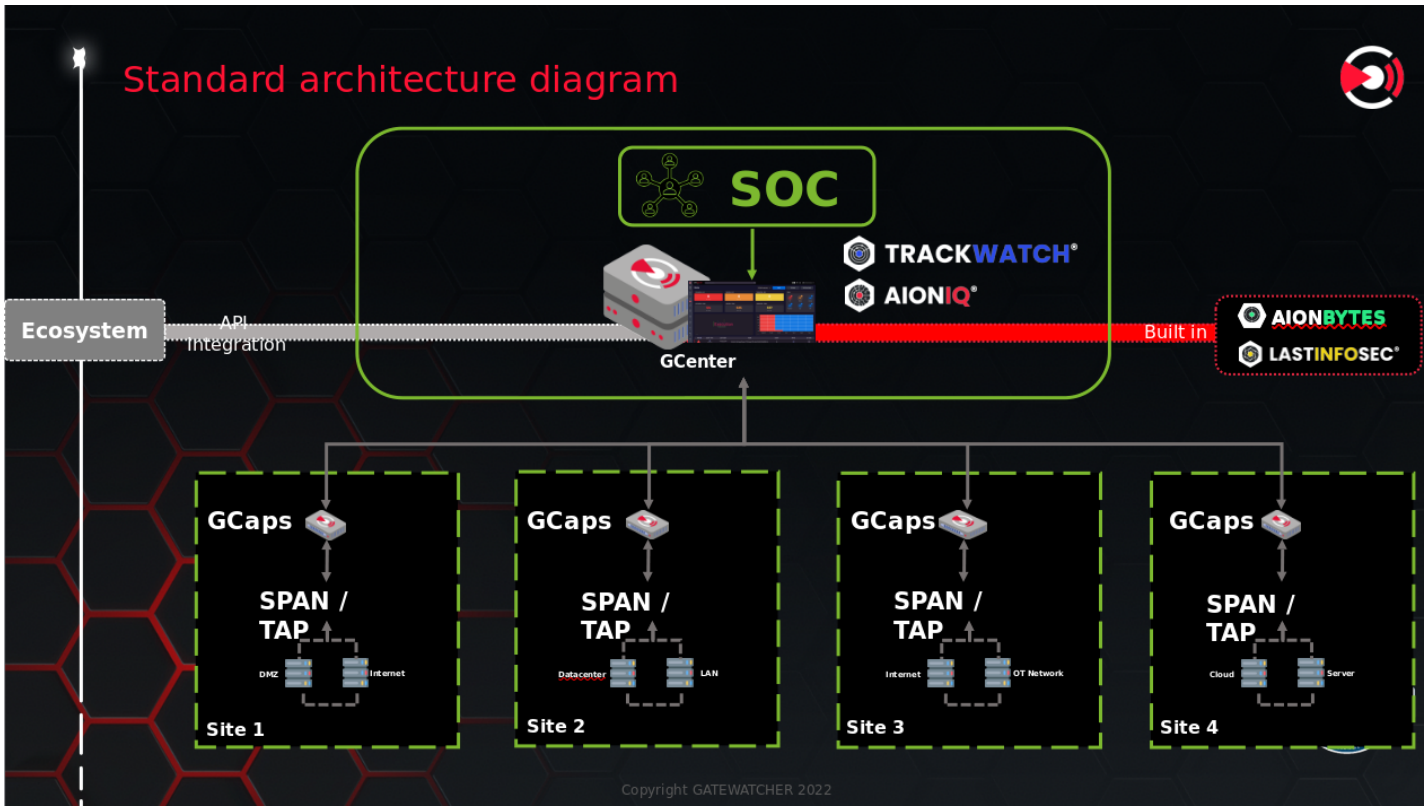
Keys for the GCenter in single interface configuration:

- **IDRAC**: remote access port
- **VPN0**: port not used
- **MGNT0**: port used for secure communication between the probe and GCenter via IPSEC tunnel and for the remote administration via the SSH protocol
- **SUP0**: port to external services type Nagios
- **ICAP**: port to external services such as LDAP, SIEM, update

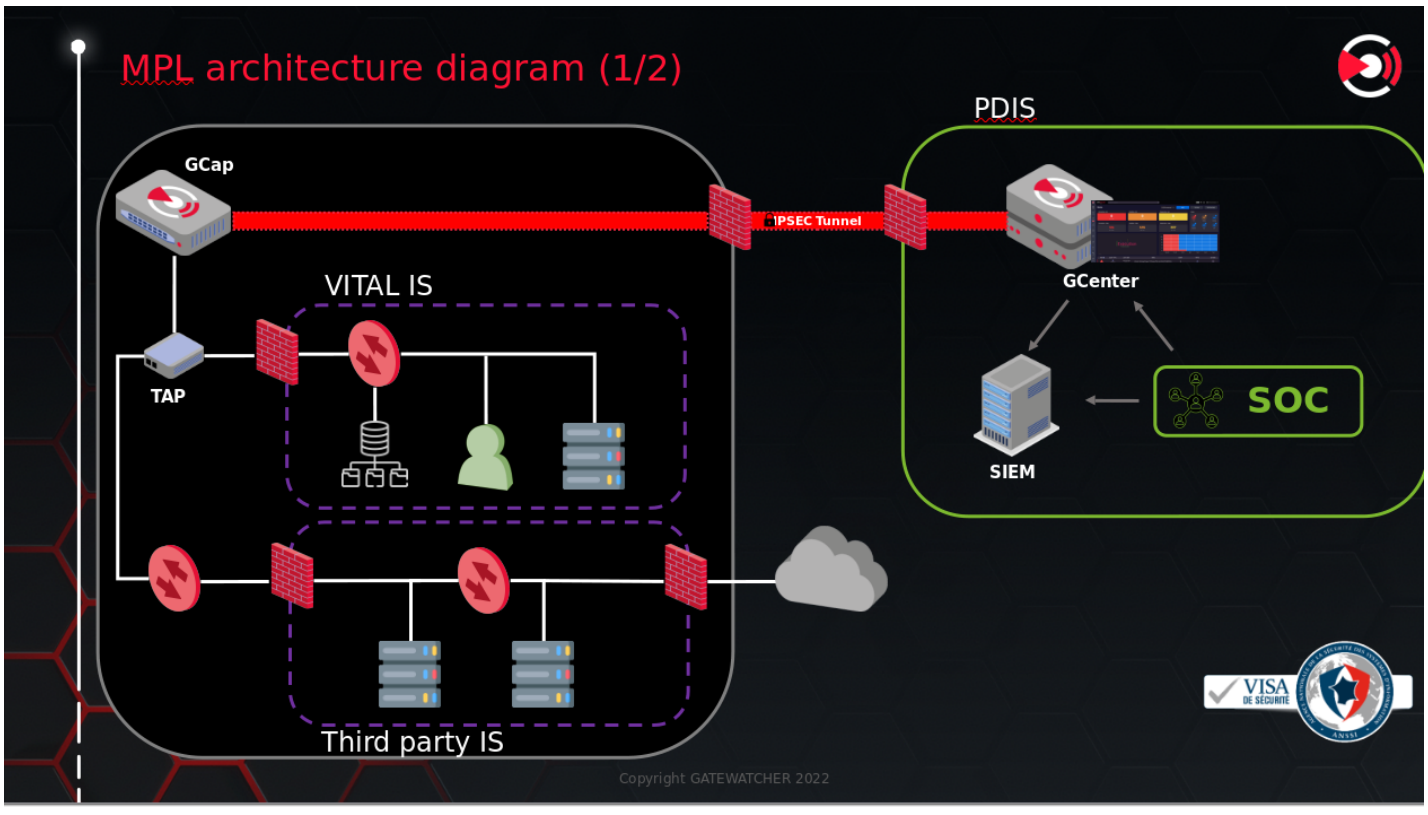
1.6.2 Example of architectures

Here are three examples of implementing the solution in an information system:

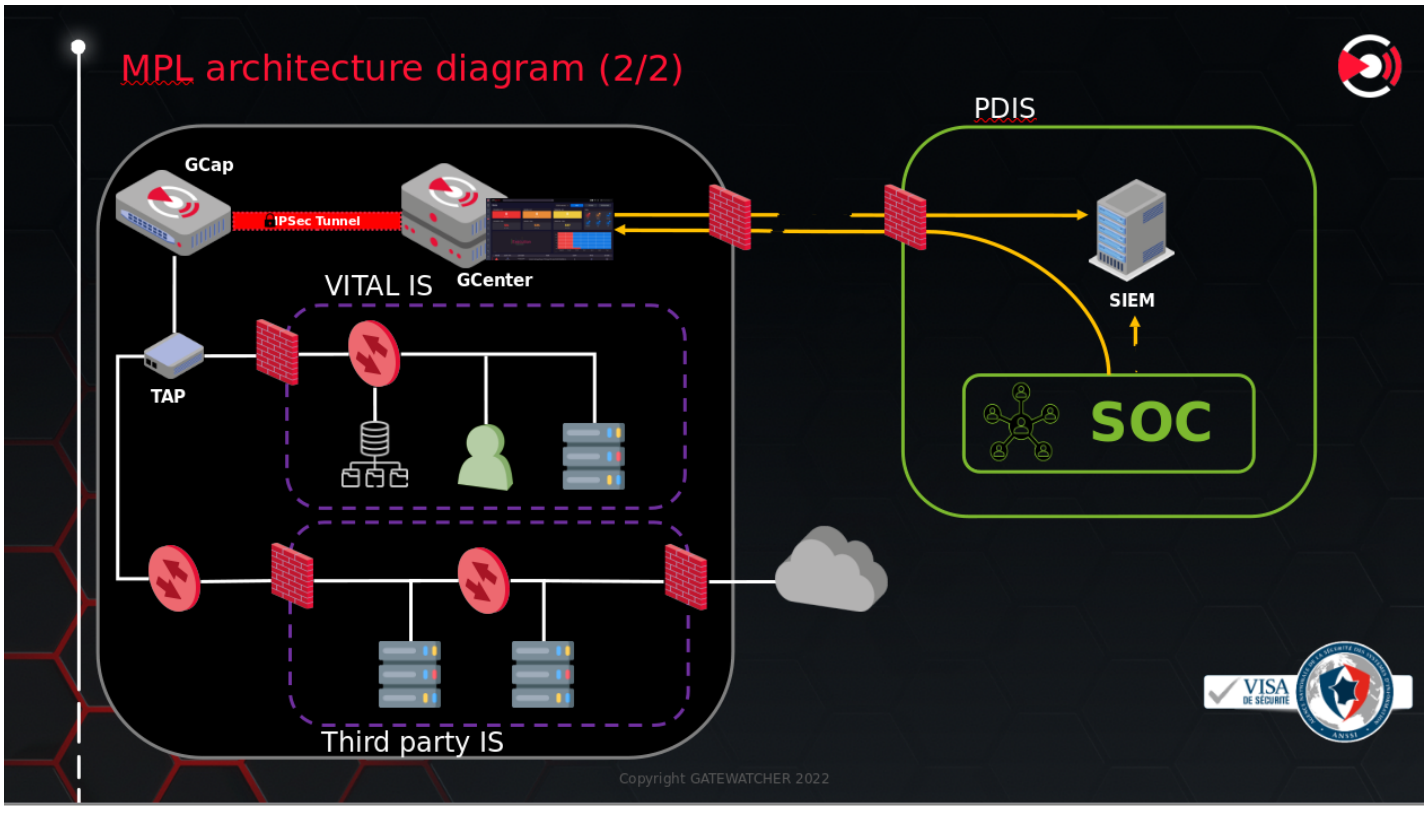
1.6.2.1 Detection architecture diagram



1.6.2.2 MPL 1 (PDIS 1 architecture diagram)



1.6.2.3 MPL 2 (PDIS 2 architecture diagram)



Chapter 2

Operation

2.1 Detection Engines

2.1.1 Introduction of engines

The GCenter uses several different engines for the following detections:

Detection type	Engine	Time of detection	See
Anti-viral analysis of files	Malcore	immediate on the network fux	*Malcore engine*
Anti-viral analysis of files	Malcore retroanalyzer	Delayed time after updating the Malcore engine database	*Malcore engine*
Powershell	Malicious Powershell detect	immediate on the network fux	*Malicious Powershell detect engine*
Shellcode	Shellcode detect	immediate on the network fux	*Shellcode detect engine*
search in network fux for attack characteristics defined in rules	Sigflow	immediate on the network fux	*Sigflow engine*
Malicious domain names	DGA detect	immediate on the network fux	*DGA detect engine*
Search in the fux network for Attack compromise indices defined in rules	Active CTI	immediate on the network fux	*Active CTI engine*
search in the fux network for Attack compromise indices defined in rules	Retrohunt	Delayed time after Retrohunt database update	*Retro hunt engine*
Search the ransomware executions	Ransomware detect	immediate on the network fux	*Ransomware detect engine*
Search the communications to a malicious server during a Command and Control (C&C) attack	Beacon detect	immediate on the network fux	*Beacon detect engine*
Detect the malwares using rules	Yara	immediate on the network fux	*Yara engine*

2.1.1.1 Detection by GScan

Files may be submitted manually to GScan.
The following options are available:

- Malware: submits files to the Malcore engine
- Powershell: scans files containing Powershell scripts and detects potential threats that can be used as a gateway to install malware on Windows.

  For malicious powershells, detection is based on a supervised machine learning model, and the fact that these scripts generally use offuscation techniques or similar (base64, concatenation, type conversion, etc).
- Shellcode: scans files to detect Shellcodes (a **binary** code designed to be injected and executed in a program by exploiting a vulnerability).

2.1.2 Malcore engine

2.1.2.1 Introduction

2.1.2.1.1 For what types of threats is this engine designed?

The Malcore engine performs anti-viral analysis of files by different engines to detect a wide range of malware.

2.1.2.1.2 How does this particular engine detect threats?

The Malcore engine uses several scanning methods to detect threats.
It combines:

- Static analysis, which examines the contents of files without executing them
- With heuristic analysis, which evaluates the potential behaviours of files to identify suspicious activities

---

2.1.2.1.3 How does Malcore engine work in the GCenter?

The engine:

- Analyzes the events sent by the GCap (for further details see *Malcore engine input data*)
- Analyzes these events (for further details see *How does this particular engine detect threats?*)
- Generates alerts (for further details see *Events generated*)

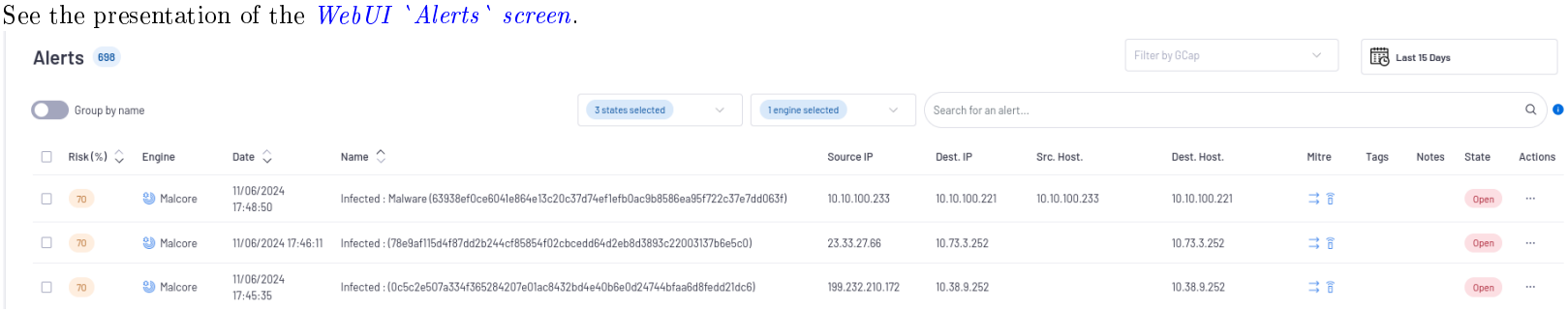
2.1.2.1.3.1 Malcore engine input data

The network flow is duplicated on the network by a TAP and the files are rebuilt by the GCap.
The file reconstruction is configured by the file reconstruction rules used by the GCap detection engine (refer to *Configuring the file reconstruction rules via the GCap profile*).
In the GCenter, when the file is submitted to Malcore, it is analyzed by Malcore itself, composed of a set of antivirus engines.
If one of these engines detects the file as malicious, an alert is generated in the dashboards.
Malcore integrates up to 16 separate antivirus engines, each using its own methods and signature bases to identify threats.
The antivirus engines are displayed under the name "engine-id.X.id" where X is the number of the engine concerned.
This approach provides extensive detection coverage, improving detection reliability and efficiency.
For example, if a user receives an email with an attachment containing a suspicious file, the Malcore engine takes action as soon as the file passes through the network.
This file undergoes analysis by the various available antivirus engines, each examining its content for malicious elements.

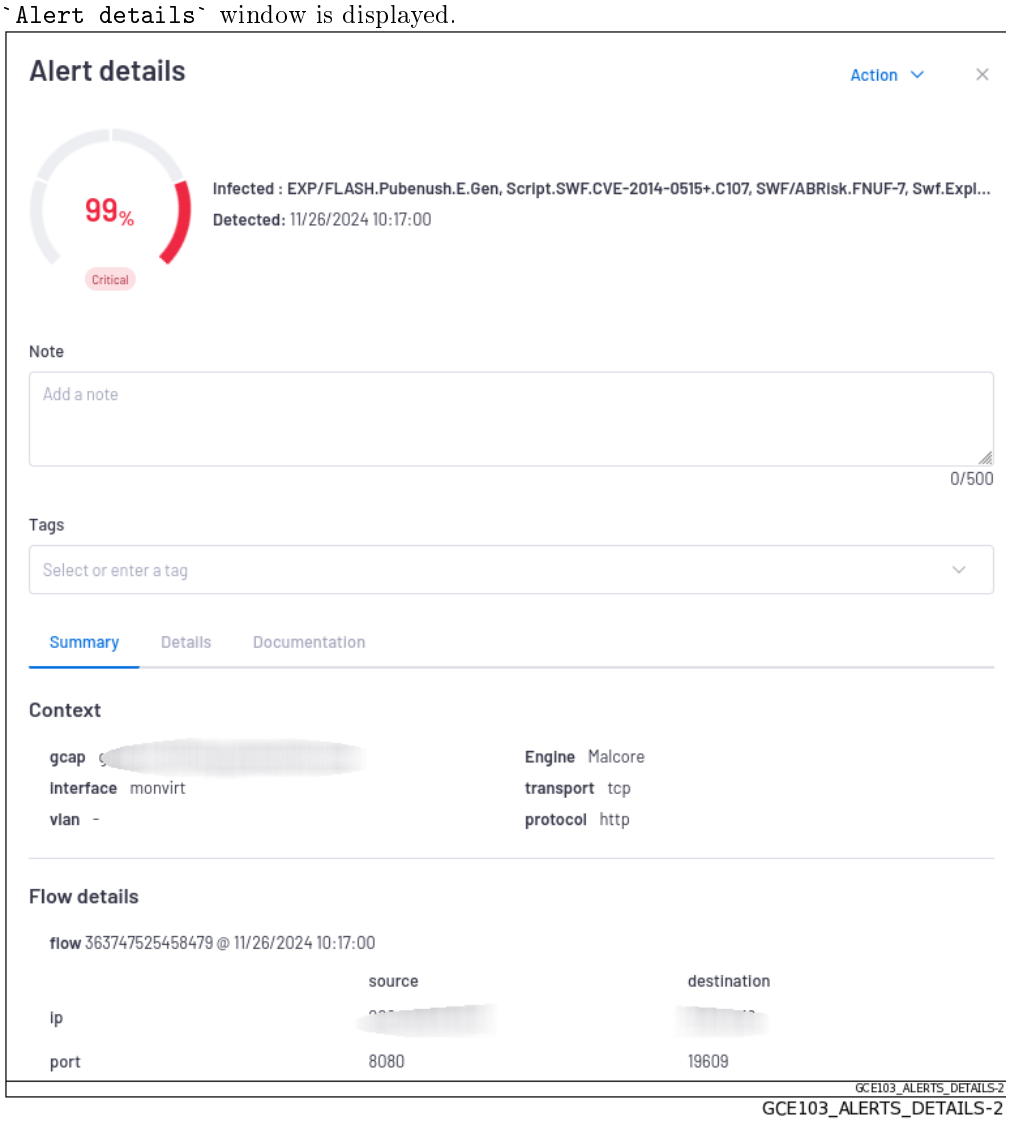
2.1.2.2 Events generated

Events generated by the Malcore engine are **alerts**.
Events generated by the Yara engine are included with the Malcore **alerts**.
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen:
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
- To view the alerts, select the `Malcore` engine filter.
  See the presentation of the *WebUI `Alerts` screen*.



- Click on the selected alert.
  The `Alert details` window is displayed.



  The following counters are displayed and give information on the alert category:

  - `total found:`
  - `threat:`
- If the `total found:` is 0/16 and the `threat:` is Yara Rule Matched then the alert category is **yara**
  Example of a Yara alert:

```
Malcore summary
state: Yara Rule Matched
total found: 0/16
file description: Adobe Portable Document Format
threat: Yara Rule Matched
```

  In this case, see the procedure *Analyzing the Yara alerts*.

- If the `total found:` is different to 0/16 then the alert category is **malcore**

Example of a Malcore alert:

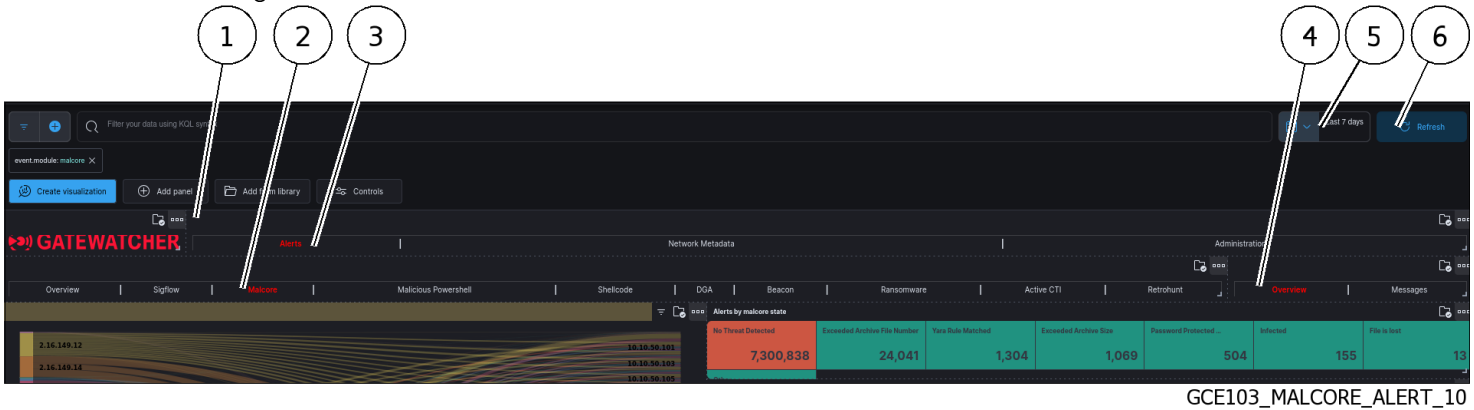
```
Malcore summary
state: Infected
total found: 1/16
file description
threat
Infected: pdf/malicious_confidence_100
```

The detailed information of this alert is displayed in *Example of a Malcore alert in the WebUI*.
The displayed counters are given in the *Engine log data structure* appendix.

In this case, the `total found` counter is different to 0/10, i.e at least one Malcore engine result is not CLEAN

- If the `Group by name` mode is activated, the name of the aggregated alerts and their number are displayed.
  Click on a grouping of alerts to display the list.
- When the `Group by name` mode is disabled, different Source and Destination information is displayed for each alert.
  `Tags` and `Notes` are also visible and editable.
  The various Quick Access `Actions` are available for each alert.

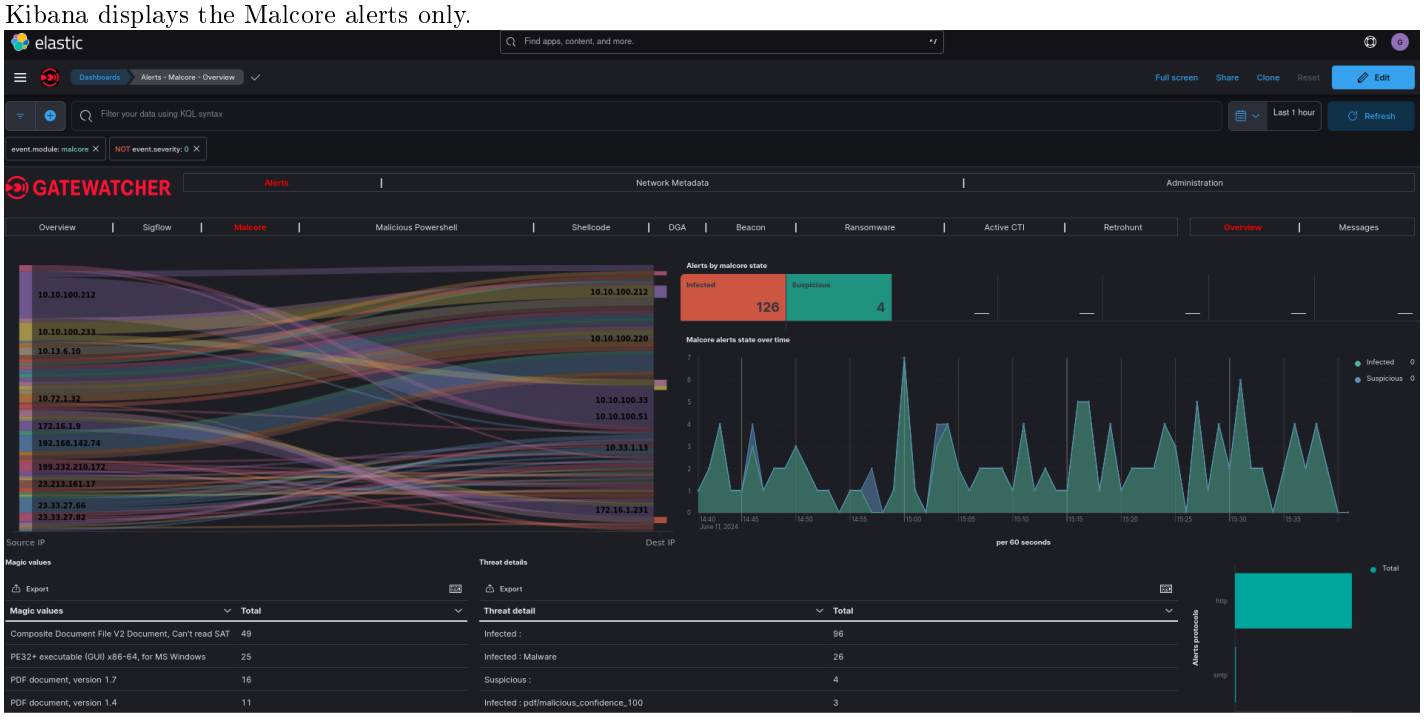
- In the **Kibana UI** interface
  - To view only the Malcore alerts without the Yara alerts:
    See the presentation of the *WebUI `Alerts` screen*.
    - Click on the `Hunting` icon of the `WebUI`.



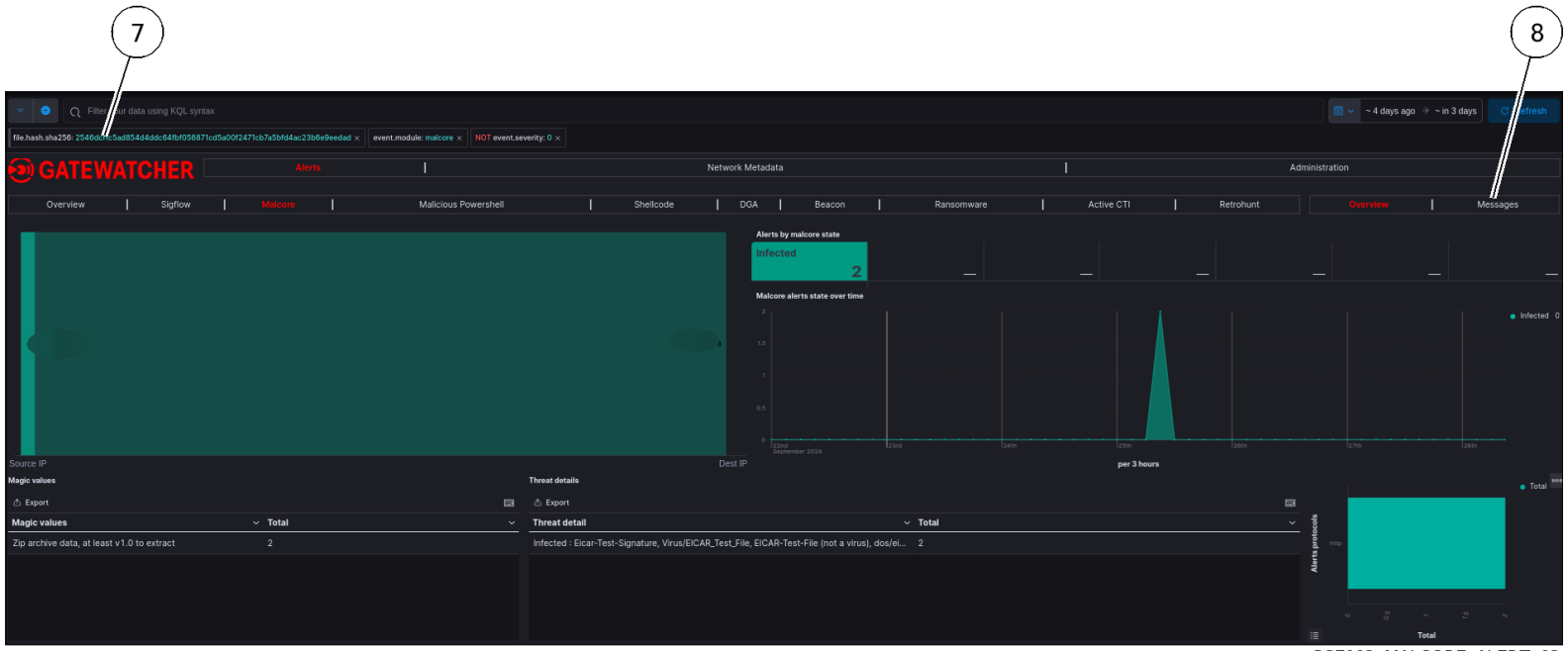
GCE103_MALCORE_ALERT_10

The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

- Click on the `Malcore` tab (2) of the `Alerts` category (3).
- Select the `Overview` tab (4).
- Select the time range (5) to display data.
- To filter the Malcore alerts without the Yara alerts on Kibana, enter the following command `event.module : "malcore" and NOT malcore.state : "Yara Rule Matched"` in the search field (1).
- Validate wih the `Refresh` button (6).
  Kibana displays the Malcore alerts only.

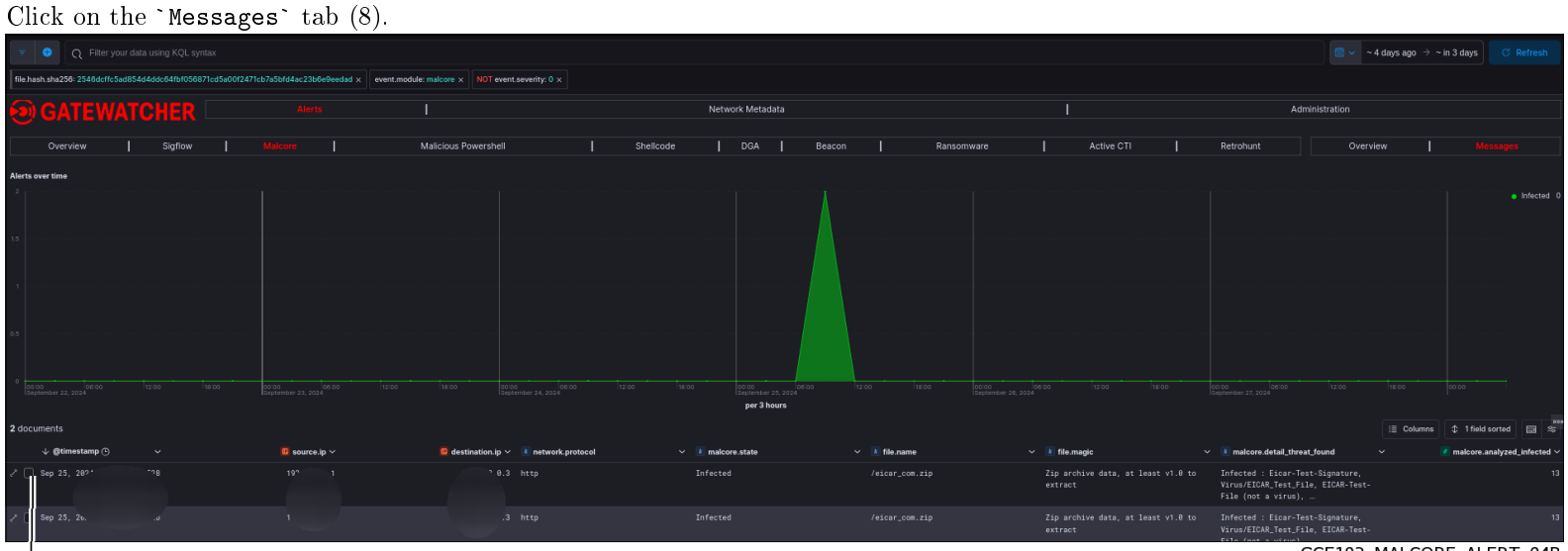


- To consult information about a specific alert:
- On the main interface **WebUI**, after clicking on an alert, click on the `Open malcore file transaction` command of the `Actions` menu.
  Kibana is opened on the `Malcore` tab of the `Alerts ` section: in the `Overview` tab, the database is filtered on the `file.hash.sha256` parameter (7).
  The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).



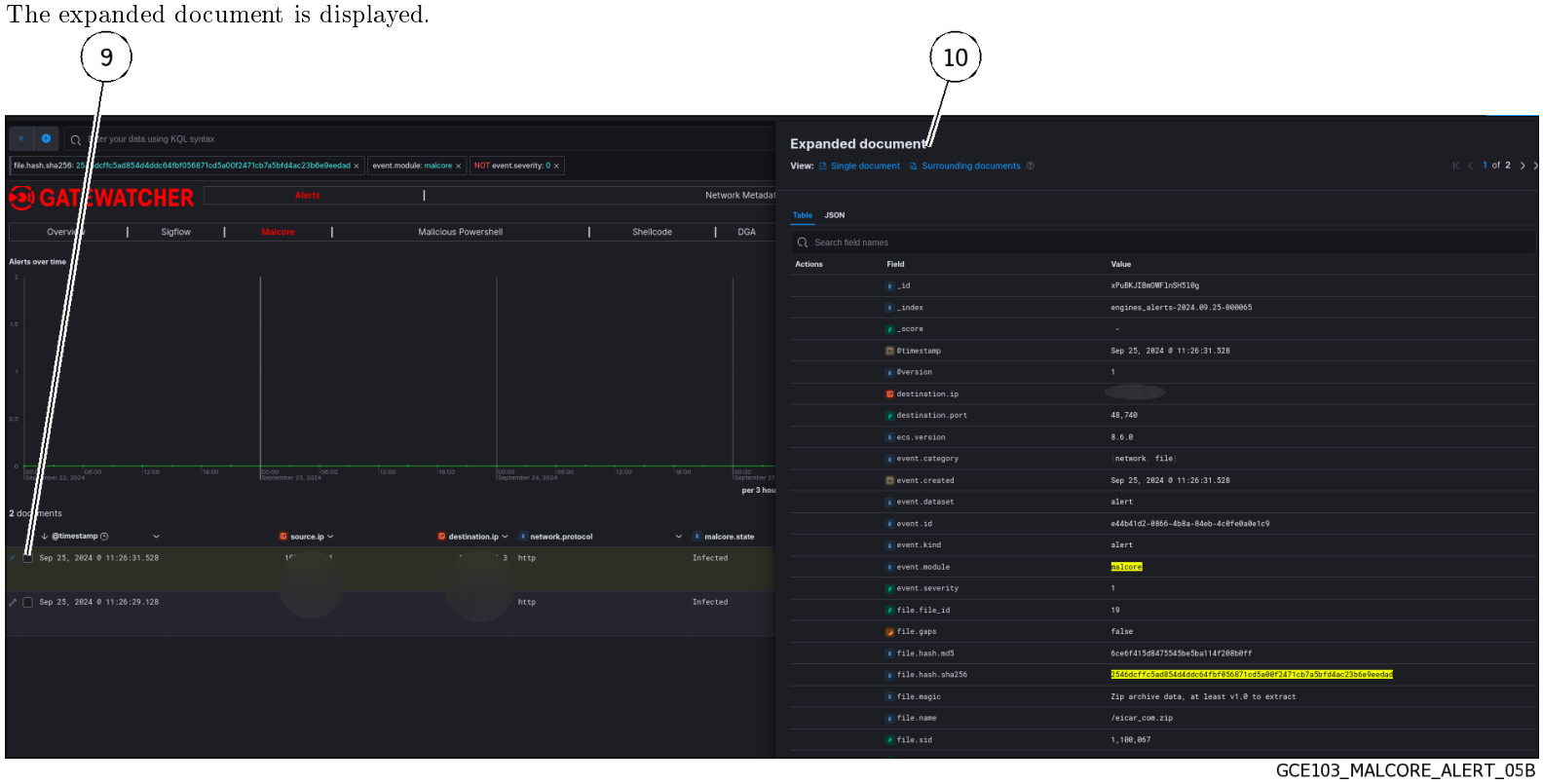
GCE103_MALCORE_ALERT_03

- Click on the `Messages` tab (8).



GCE103_MALCORE_ALERT_04B

- Click on the toggle icon on the left of the Alert (9).
  The expanded document is displayed.



GCE103_MALCORE_ALERT_05B

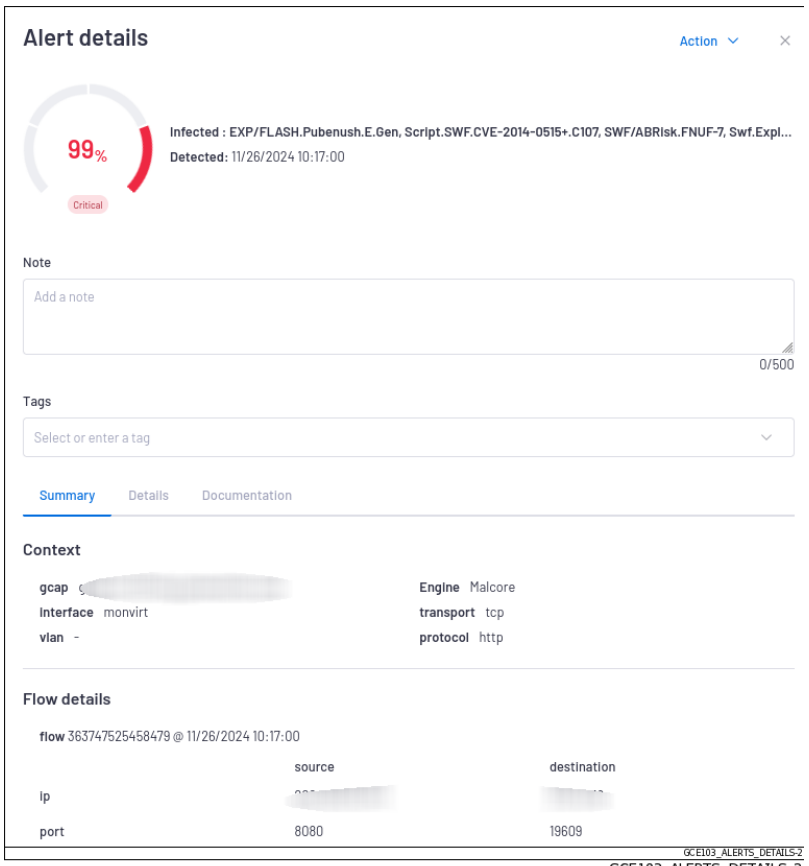
The detailed information of this alert can be viewed in table or json format (see the *Malcore log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

Note:

The **Kibana UI** can also be accessed without any filters via the `Hunting` icon on the left side menu bar in the WebUI.

An example is given in *The source part of Malcore logs*.

2.1.2.2.1 Example of a Malcore alert in the WebUI



The presentation of the `Alert details` window is given in the *`Alert details` window*.
The counters are given in the *Engine log data structure* appendix.

2.1.2.2.2 Malcore log data structure

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields"

This information is displayed in the `Expanded document` window of Kibana.

2.1.2.2.2.1 The header part of Malcore logs

The header section contains:

```
"_index": "engines_alerts-2024.11.26-000022",
"_type": "_doc",
"_id": "q5zQZ5MBe7GX5B2fx7DG",
"_version": 1,
"_score": 0,
```

The detailed information is given in the table (*Counters of the header part of logs*).

2.1.2.2.2.2 The source part of Malcore logs

The source part is defined by "_source" in the logs.

Note:

The data displayed on the WebUI (`alerts details` window) is a part of the data displayed on the `Extended document` screen on the Kibana interface.
All data can be exported to a SIEM via syslog (an example of an exported alert is shown).
The detailed information is given in the table (*Counters of the header part of logs*).

The example given here is a Kibana example.


```
"http": {
  "response": {
    "status": 200,
    "bytes": 77068,
    "mime_type": "application/x-shockwave-flash"
  },
  "http_port": 8080,
  "hostname": "tsevid-synonymi.justdanceatsea.com",
  "version": "HTTP/1.1",
  "http_refer": "http://tsevid-synonymi.justdanceatsea.com:8080/ndf4xx22ci.php",
  "request": {
    "method": "GET"
  }
},
"source": {
  "ip": "x.y.z.A",
  "port": 8080,
  "mac": "xx0"
},
"observer": {
  "gcap": {
    "ingress": {
      "interface": {
        "name": "monvirt"
      }
    },
    "hostname": "gcap",
    "version": "2.5.4"
  },
  "product": "gcenter",
  "hostname": "gcenter.domain",
  "version": "2.5.x.",
  "log_format_version": "1.0.0",
  "uuid": "fc1e66e3-a397-5eb4-9277-754be778f317",
  "vendor": "gatewatcher"
},
"file": {
  "gaps": false,
  "tx_id": 1,
  "name": "/6SuCHKKkf8Sf1aFXJPqD0R6r3oEDCrbwHFm23EU-Af2zwWdHgpn6mEGu5XlxFust",
  "magic": "Macromedia Flash data (compressed), version 14",
  "file_id": 646,
  "hash": {
    "sha256": "350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4",
    "md5": "67ca9a31f220bc7b68f203c07ad668b9"
  },
  "size": 77068,
  "state": "CLOSED",
  "stored": true,
  "sid": [
    1100020
  ]
},
"network": {
  "protocol": "http",
  "timestamp": "2024-11-26T09:17:00.775521+0000",
  "transport": "tcp",
  "flow_id": 363747525458479
},
```


(continues on next page)

(continued from previous page)


```
  "ecs": {
    "version": "8.6.0"
  },
  "metadata": {
    "flowbits": [
      "min.gethttp"
    ]
  },
  "user_agent": {
    "original": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.
↪30729; .NET CLR 3.0.30729)"
  },
  "destination": {
    "ip": "x.y.z.A",
    "port": 19609,
    "mac": "90:e2:ba:a6:a4:91"
  },
  "url": {
    "domain": "tsevid-synonymi.justdanceatsea.com",
    "path": "/6SuCHKKkf8Sf1aFXJPqD0R6r3oEDCrbwHFm23EU-Af2zwWdHgpn6mEGu5XlxFust"
  },
  "malcore": {
    "detail_threat_found": "Infected : EXP/FLASH.Pubenush.E.Gen, Script.SWF.CVE-2014-0515+.C107, SWF/ABRisk.FNUF-7, Swf.
↪Exploit.Angler-11, SWF/Exploit.ExKit.J trojan, Exploit.SWF, Exp.SWF.Angler.D",
    "engine_id": {
      "0": {
        "scan_result": "CLEAN",
        "threat_details": "",
        "id": "a32935b"
      },
      "1": {
        "scan_result": "INFECTED",
        "threat_details": "EXP/FLASH.Pubenush.E.Gen",
        "id": "acf9bba"
      },
      "2": {
        "scan_result": "CLEAN",
        "threat_details": "",
        "id": "af7872b"
      },
      "3": {
        "scan_result": "INFECTED",
        "threat_details": "Script.SWF.CVE-2014-0515+.C107",
        "id": "b557a5r"
      },
      "4": {
        "scan_result": "UNSUPPORTED_FILE_TYPE",
        "threat_details": "",
        "id": "c10195e"
      },
      "5": {
        "scan_result": "INFECTED",
        "threat_details": "SWF/ABRisk.FNUF-7",
        "id": "c18ab9n"
      },
      "6": {
        "scan_result": "INFECTED",
        "threat_details": "Swf.Exploit.Angler-11",
        "id": "c4839cv"
      },
      "7": {
        "scan_result": "INFECTED",
        "threat_details": "SWF/Exploit.ExKit.J trojan",
        "id": "e83bf1t"
      },
      "8": {
        "scan_result": "INFECTED",
        "threat_details": "Exploit.SWF",
        "id": "ib54e9s"
      },
      "9": {
        "scan_result": "CLEAN",
        "threat_details": "",
```


(continues on next page)

(continued from previous page)


```
      "id": "kfb8487"
    },
    "10": {
      "scan_result": "CLEAN",
      "threat_details": "",
      "id": "mb2b5fe"
    },
    "11": {
      "scan_result": "INFECTED",
      "threat_details": "Exp.SWF.Angler.D",
      "id": "qb9308l"
    },
    "12": {
      "scan_result": "CLEAN",
      "threat_details": "",
      "id": "sde882s"
    },
    "13": {
      "scan_result": "CLEAN",
      "threat_details": "",
      "id": "t3114fn"
    },
    "14": {
      "scan_result": "UNSUPPORTED_FILE_TYPE",
      "threat_details": "",
      "id": "we9a17t"
    }
  },
  "code": 1,
  "state": "Infected",
  "analyzed_other": 2,
  "file_type": "application/x-shockwave-flash",
  "analyzed_clean": 6,
  "engines_last_update_date": "2024-07-22T17:15:00Z",
  "reporting_token": "",
  "analyzed_suspicious": 0,
  "file_type_description": "Macromedia Flash Player",
  "analyzed_error": 0,
  "total_found": "7/15",
  "analyzed_infected": 7,
  "analyzers_up": 15,
  "magic_details": "Macromedia Flash data (compressed), version 14",
  "detail_scan_time": 1642,
  "detail_wait_time": 477,
  "processing_time": 2120
 },
 "@timestamp": "2024-11-26T09:17:00.775Z",
 "event": {
  "created": "2024-11-26T09:17:00.775521+0000",
  "dataset": "alert",
  "module": "malcore",
  "kind": "alert",
  "category": [
   "network",
   "file"
  ],
  "severity": 1,
  "id": "28e92cac-b1de-4b20-ab71-5eeb325f64ed"
 },
 "@version": "1"
},
```

2.1.2.2.2.3 List of counters of the alert

Note:

The alert counters are visible:
- In the `Alert details` screen of the WebUI
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.2.3 Management of the engine

2.1.2.3.1 Viewing the engine status

The current engine status is displayed in *`Health checks` screen*.
The visible information is:

- The status and status of each engine included in Malcore
- The latest update of each of them

2.1.2.3.2 Engine update

There are updates for the Malcore engine.
These updates can be done manually or scheduled via threat-DB update.
See *Dedicated modules for managing updates: Threat DB update and Software update* and in particular *Update presentation*.

2.1.2.3.3 Malcore configuration and management of the ignored list feature

The management interface is used:

- To modify the engine parameters:
  - See the screen description, refer to *`Malcore` screen*
  - See the *Setting up the Malcore engine* procedure.
- To manage the `Ignore list` feature.
  This feature is composed of:
  - The exception list of files that Malcore must consider healthy.
    These files are declared healthy without analysis and defined using:
    - Their SHA256 fingerprint (whatever the name)
    - The file name
  - The list of engins defined as too sensitive.
    When running malcore with multiple engines (see license details), some engines can be more sensitive than others.
    This feature will prevent alerts raised by **only one** engine considered as too sensitive.
    It will not affect alerts where more than one engine has detected something.
    It is only available when more than one engine is available.
  - See the screen description, refer to *`Malcore` screen*
  - See the *Managing the Ignore list of the Malcore engine* procedure.

2.1.2.4 Alert Analysis

The alerts are displayed on a specific screen: this screen is described in the *WebUI `Alerts` screen*.
The general procedure for analyzing alerts is described in the *Using of NDR dashboards*.
The specific procedure for analyzing malcore alerts is described in the *Analyzing the Malcore alerts*.

2.1.3 Shellcode detect engine

2.1.3.1 Introduction

2.1.3.1.1 For what types of threats is this engine designed?

The Shellcode Detect engine allows the detection and analysis of shellcodes.

A Shellcode is a **binary code** designed to be injected and executed into a program by exploiting a vulnerability.
Similar to a miniature malware, its goal is usually to take control of the infected system, but any type of action can be performed.
Shellcodes often have many constraints related to the exploited vulnerability (limited size, forbidden bytes, ...).
Thus, an attacker will generally use it to "*get a foot in the door*", before moving on to more advanced techniques.
A Shellcode can be used to open a backdoor on the machine, to let the attacker act live, or download directly in memory a malware and run it.

A Shellcode can also be obfuscated, "encoded", to avoid being detected by patterns, but while remaining executable as is.
It must be able to self-decode, we then speak of polymorphism.
There are many encoding algorithms for shellcodes on the internet, more or less complex.
Due to its nature, shellcode is difficult to detect:

- Not a file
- It is directly executed in memory in a healthy program
- Its small size reduces pattern possibilities for detection
- May be obfuscated to avoid pattern detection

A shellcode can also be used in a malware in order to blur the tracks during an antivirus scan.

2.1.3.1.2 How does this particular engine detect threats?

Shellcode detection is done in several steps:

1. The first step is to analyze the samples for shellcode encodings.
   Indeed, these algorithms are specific to shellcodes, they cannot be found in another context.
   This process allows accurate and indisputable identification of shellcodes.
2. If one or more encodings are identified, the shellcode is extracted and sent to the analysis step.
3. If no encoding has been identified, the sample goes through a thorough indicator search.
   This process will perform an intelligent, emulation-based search to try to identify a typical shellcode behaviour.
4. The last step is to analyze the identified shellcode in order to validate the detection, and extract as much information as possible.
   This process will perform full shellcode emulation and record all system functions called.

2.1.3.1.3 How does Shellcode Detect engine work in the GCenter?

The engine:

- Retrieves events sent by the GCap (for further details see *Shellcode Detect engine input data*)
- Analyzes these events (for further details see *How does this particular engine detect threats?*)
- Generates alerts (for further details see *Events generated*)

2.1.3.1.3.1 Shellcode Detect engine input data

Any packet passing through the network will undergo a search for smart patterns to identify those that may contain a shellcode.
These packages are then extracted and sent to the GCenter for further analysis by the Shellcode Detect engine.
Once the analysis is completed, if a shellcode has been identified, an alert is raised with all the information collected.

Note:

Currently, only shellcodes for Linux and Windows machines, under Intel x86 and x64 architecture, are detected.

Encoding identification will only be possible for a defined set of algorithms, but this will not prevent the detection of shellcodes whose encoding could not be identified.
Detection of shellcodes embedded in malware is possible and will follow the same scanning path, but will not work if they are "hidden" (encryption, compression, ...) since it would require a dynamic analysis of the malware itself.

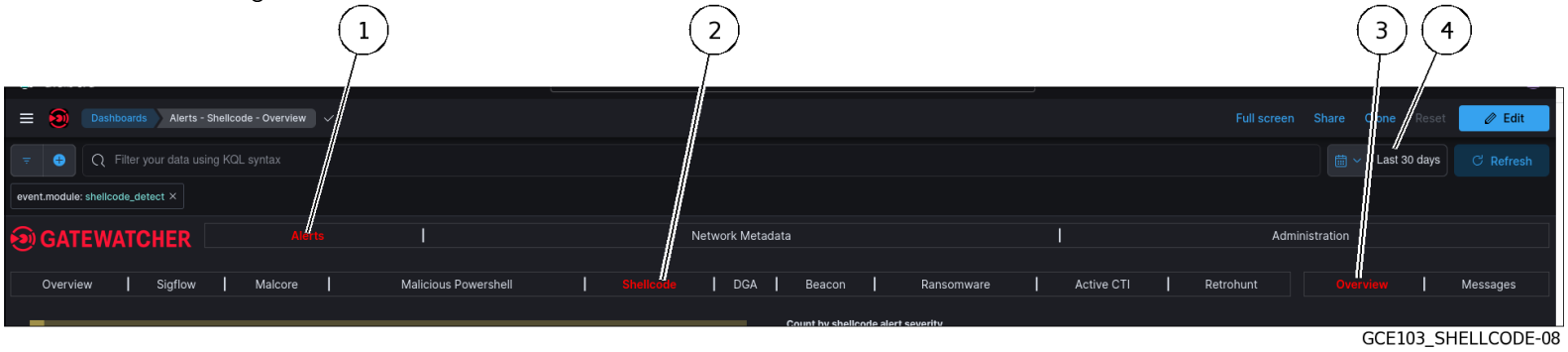
In order for the engine to be operational, a first update of the "Threat DB" will have to take place.

2.1.3.2 Events generated

Events generated by the Shellcode detect engine are **alerts** only.
These are displayed:

- In the main interface named **WebUI** on the GCenter in the `Alerts` screen
  The main interface named **WebUI** is described in the *Overview of the WEB UI*.
  - To display only these alerts, select the `Shellcode` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.

  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed in *Example of a Shellcode alert in the WebUI*.
    The displayed counters are given in the *Engine log data structure* appendix.
- In the interface named **Kibana UI**
  - Click on the `Hunting` icon of the `WebUI`.



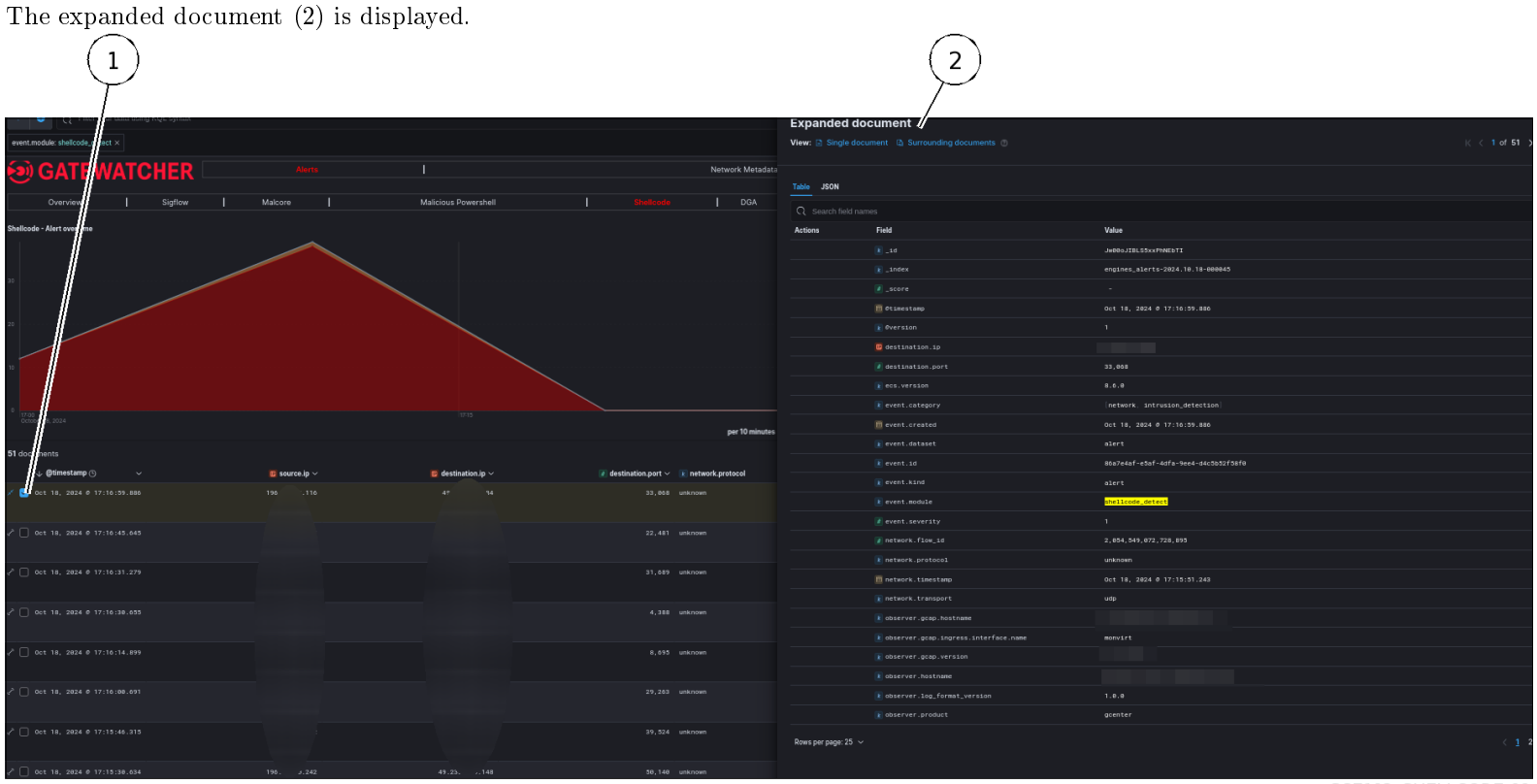
GCE103_SHELLCODE-08

The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

- Click on the `Shellcode` tab (2) of the `Alerts` category (1).
- Select the `Overview` tab (3).
- Select the time range (4) to display data.
  It is then possible to filter on certain values for, for example:
  - Do not display healthy machines (filter false positives)
  - Show only alerts from a particular IP

- Do not display alerts from a specific GCap

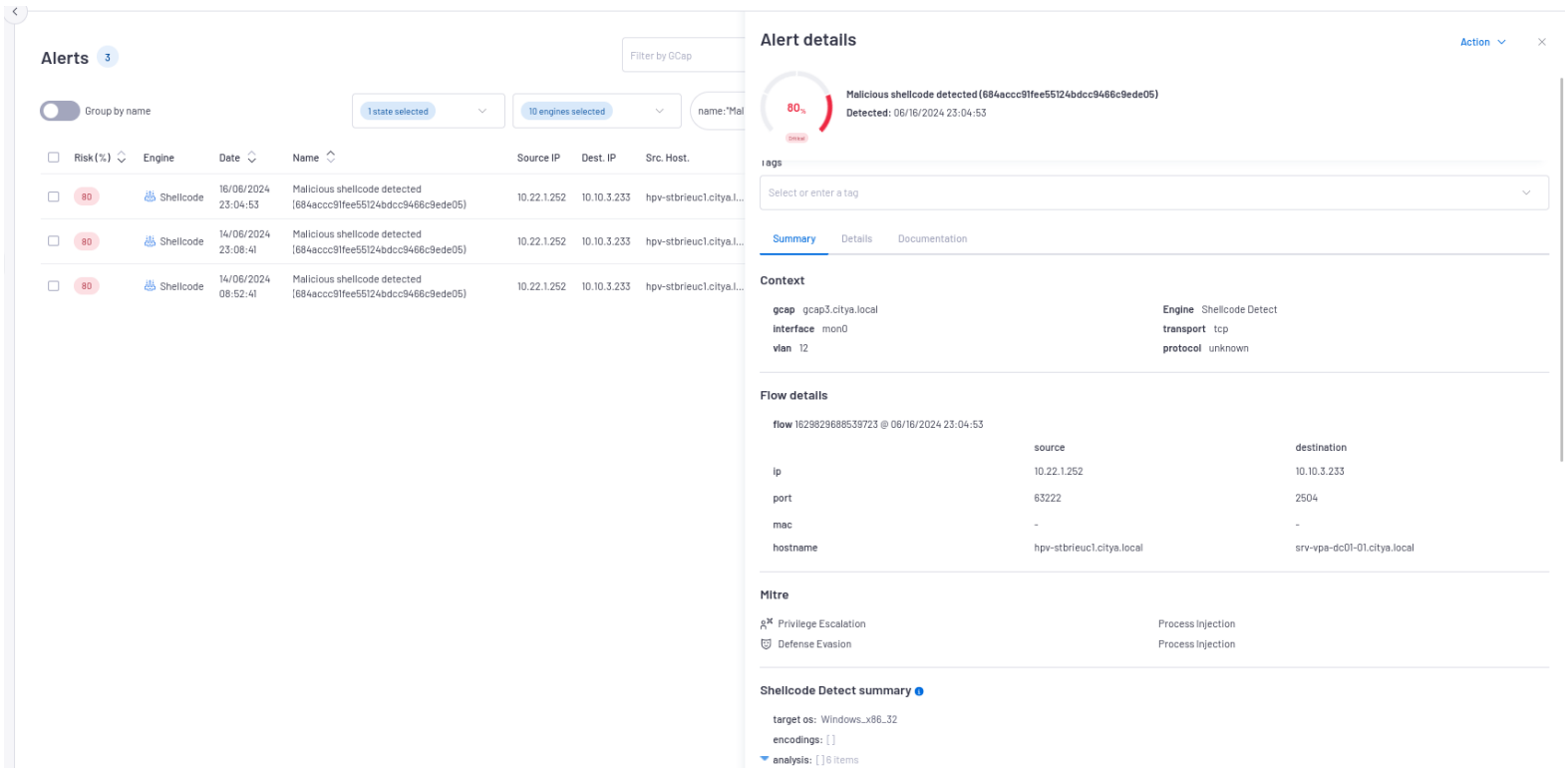
- To consult information about a specific alert:
  - Click on the toggle icon (1) on the left of the Alert.
    The expanded document (2) is displayed.



GCE103_SHELLCODE-09

The detailed information of this alert can be viewed in table or json format (see the *Shellcode log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

2.1.3.2.1 Example of a Shellcode alert in the WebUI



The presentation of the `Alert details` window is given in the *`Alert details` window*.
The counters are given in the *Engine log data structure* appendix.

2.1.3.2.2 Shellcode log data structure

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields"

This information is displayed In the `Expanded document` screen of Kibana.

2.1.3.2.2.1 The header part of the Shellcode logs

The header section contains:

```
"_index": "engines_alerts-2024.12.04-000030",
"_id": "BqIIkpMBe7GX5B2fdvZJ",
"_version": 1,
"_score": 0,
```

The detailed information is given in the table (*Counters of the header part of logs*).

2.1.3.2.2.2 The source part of the Shellcode logs

The source part defined by "_source" contains:

Note:

The data displayed on the WebUI (alerts details window) is a part of the data displayed on the `Extended document` screen on the Kibana interface.
All data can be exported to a SIEM via syslog (an example of an exported alert is shown).
The detailed information is given in the table (*Counters of the header part of logs*).

The example given here is a Kibana example.

```
"event": {
  "created": "2024-12-04T14:17:28.138941+0000",
  "dataset": "alert",
  "severity": 1,
  "module": "shellcode_detect",
  "kind": "alert",
  "category": [
    "network",
    "intrusion_detection"
  ],
  "id": "f22d2438-d436-4391-9e7d-3fe1321ebed0"
},
"@version": "1",
"destination": {
  "port": 9999,
  "ip": "X.Y.Z.A"
},
"source": {
  "port": 33390,
  "ip": "W.S.Q.E"
},
"observer": {
  "log_format_version": "1.0.0",
  "hostname": "gcenter.domain.local",
  "vendor": "gatewatcher",
  "gcap": {
    "ingress": {
      "interface": {
        "name": "monvirt"
      }
    },
    "hostname": "gcap.gatewatcher.com",
    "version": "2.5.4.0"
  },
```

(continues on next page)

(continued from previous page)


```
  "product": "gcenter",
  "uuid": "fc1e66e3-a397-5eb4-9277-754be778f317",
  "version": "2.5.3.103"
},
"ecs": {
  "version": "8.6.0"
},
"shellcode": {
  "sample_id": "12-04-2024T14:17:25_92517a8550cf4130b23466244880c1c7_gcap-int-129-dag.gatewatcher.com",
  "analysis": [
    {
      "args": "{'pathname': '//etc/passwd', 'flags': 'O_WRONLY|O_APPEND', 'mode': 'None'}",
      "_id": 0,
      "call": "sys_open",
      "ret": "4"
    },
    {
      "args": "{'fd': '//etc/passwd (4)', 'buf': 'bob::0:0::/://bin/sh', 'count': 20}",
      "_id": 1,
      "call": "sys_write",
      "ret": "20"
    },
    {
      "args": "{'fd': '//etc/passwd (4)'}",
      "_id": 2,
      "call": "sys_close",
      "ret": "0"
    },
    {
      "args": "{'status': 4}",
      "_id": 3,
      "call": "sys_exit",
      "ret": "0"
    },
    {
      "info": "Stop : End of shellcode (Exit)",
      "_id": -1
    }
  ],
  "sub_type": "Linux_x86_32",
  "encodings": [
    {
      "name": "Shikata_ga_nai",
      "count": 1
    }
  ],
  "id": "8ae5f9d35f3878cac3064fe93e4c311d"
},
"@timestamp": "2024-12-04T14:17:28.138Z",
"network": {
  "protocol": "unknown",
  "transport": "tcp",
  "timestamp": "2024-12-04T14:16:12.828909+0000",
  "flow_id": 1134126449059384
```


2.1.3.2.2.3 List of counters of the alert

Note:

The alert counters are visible:

- In the `Alert details` screen of the WebUI
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.3.3 Management of the engine

2.1.3.3.1 Viewing the engine status

The current engine status is displayed in the *`Health checks` screen*.

2.1.3.3.2 Engine update

The engine is updated with each new version of the GCenter.

2.1.3.3.3 Engine configuration

The configuration interface enables to activate the engine:

- See the description of the *`Shellcode detect` screen (Shellcode command)*
- See the *Setting up the Shellcode detect engine* procedure.

2.1.3.4 Alert Analysis

The alerts are displayed on a specific screen: this screen is described in the *WebUI `Alerts` screen*.
The general procedure for analyzing alerts is described in *Using of NDR dashboards*.
The specific procedure for analyzing Shellcode detect alerts is described in the *Analyzing the Shellcode detect alerts*.

2.1.4 Malicious Powershell detect engine

2.1.4.1 Introduction

2.1.4.1.1 For what types of threats is this engine designed?

The Malicious Powershell Detect engine allows the detection and analysis of malicious powershell scripts.
PowerShell is a programming language for Windows for system administrators.
Because of this, its capabilities to control a Windows machine are very numerous making it a very popular tool in the operation of a compromised machine.
Thus, an attacker will generally use it to maintain access to the machine or extract information from it, before pivoting to another machine.
A powershell script can therefore be used to maintain a backdoor on the machine, in order to let the attacker act later, or download directly in memory a malware and run it.
A powershell script can be obfuscated to avoid being detected by signatures and complicate its analysis.
There are many obfuscation techniques for powershell scripts, all using language-inherent methods.
Due to its nature, a malicious powershell script is difficult to detect because:

- This is a very common tool in Windows PC or server farms
- It does not necessarily pass through a file
- Often obfuscated to avoid signature detection
- Legitimate uses of PowerShell may be considered malicious behavior

---

2.1.4.1.2 How does this particular engine detect threats?

The detection of malicious powershell scripts is carried out in several steps:

1. The first step is to analyze the form, looking for obfuscation of the powershell script.
   Malicious scripts are usually obfuscated and legitimate scripts are not supposed to be, this step helps to avoid false positives.
2. The second step is to scan the content of the powershell script for potentially malicious commands.
   This step undoes the most common obfuscation techniques to characterize the threat.

2.1.4.1.3 How does Malicious Powershell Detect engine work in the GCenter?

The engine:

- Analyzes the events sent by the GCap (for further details see *Malicious Powershell Detect engine input data*)
- Analyzes these events (for further details see *How does this particular engine detect threats?*)
- Generates alerts (for further details see *Events generated*)

2.1.4.1.3.1 Malicious Powershell Detect engine input data

The network flow is duplicated on the network by a TAP and the files are rebuilt by the GCap.
The file reconstruction is configured by the file reconstruction rules used by the GCap detection engine (refer to the procedure *Configuring the file reconstruction rules via the GCap profile*).
Any packet passing through the network will undergo a search for smart patterns to identify those likely to contain a malicious powershell script.
These packages are then extracted and sent to the GCenter for further analysis by the Malicious Powershell engine.
Files with extension *.ps1* will also be extracted for analysis.

Once the scan is complete, if a malicious powershell script has been identified, an alert is raised with all the information collected.

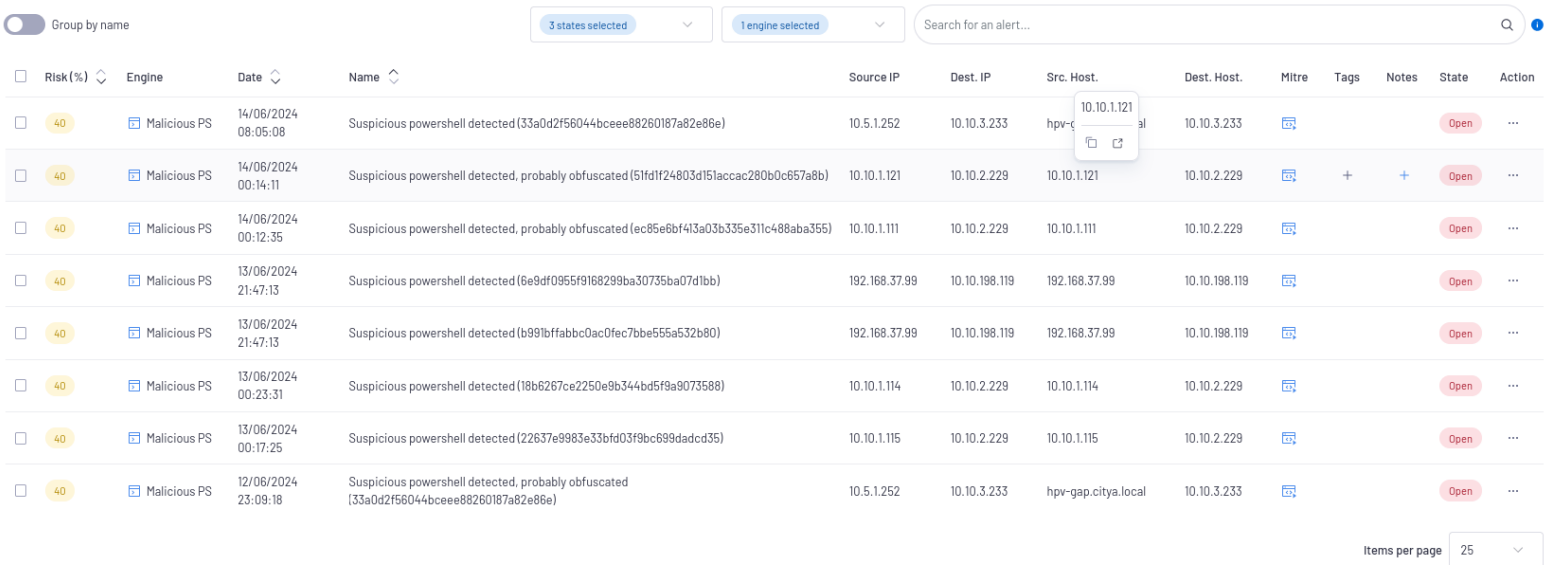
Currently, the management of obfuscations in the second step will only be possible for a defined set of techniques, but this will not prevent the detection of malicious powershell scripts whose obfuscation technique could not be identified.

In order for the engine to be operational, a first update of the "Threat-DB" will have to take place.

2.1.4.2 Events generated

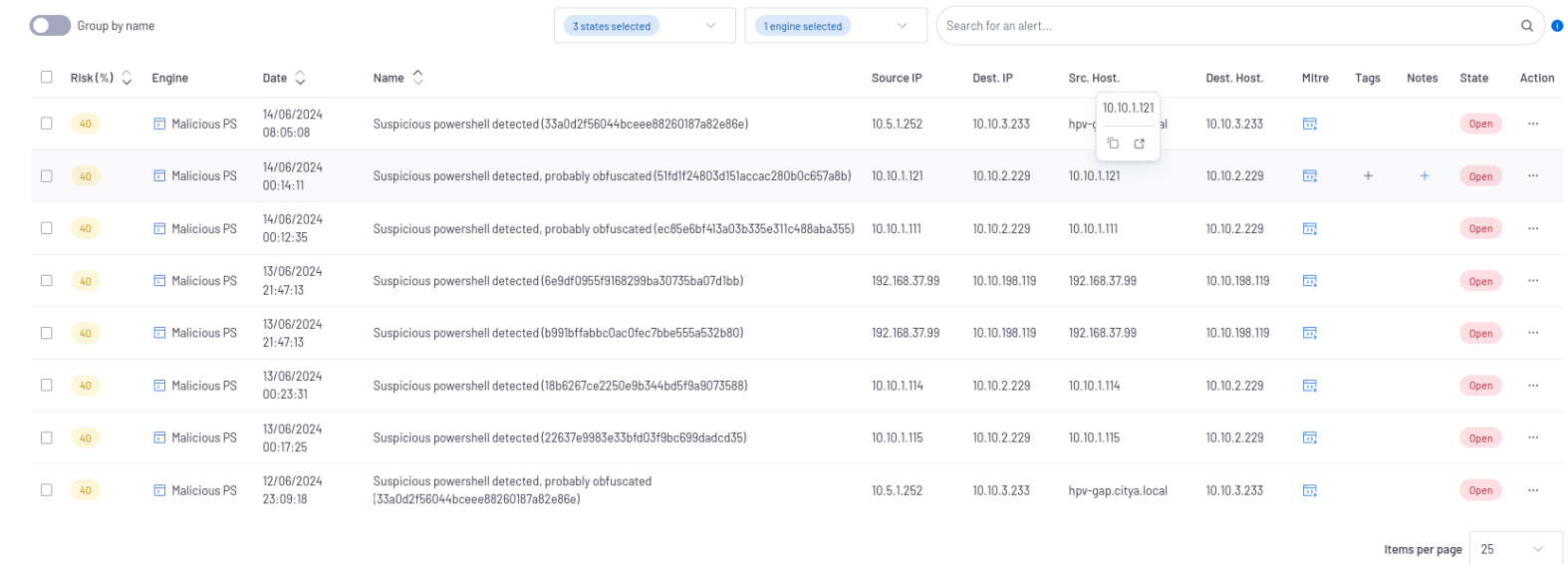
Events generated by the Malicious Powershell Detect engine are **alerts**.
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen:
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
  - To display only these alerts, select the `Malicious Powershell` engine filter then validate.
    See the presentation of the *WebUI `Alerts` screen*.

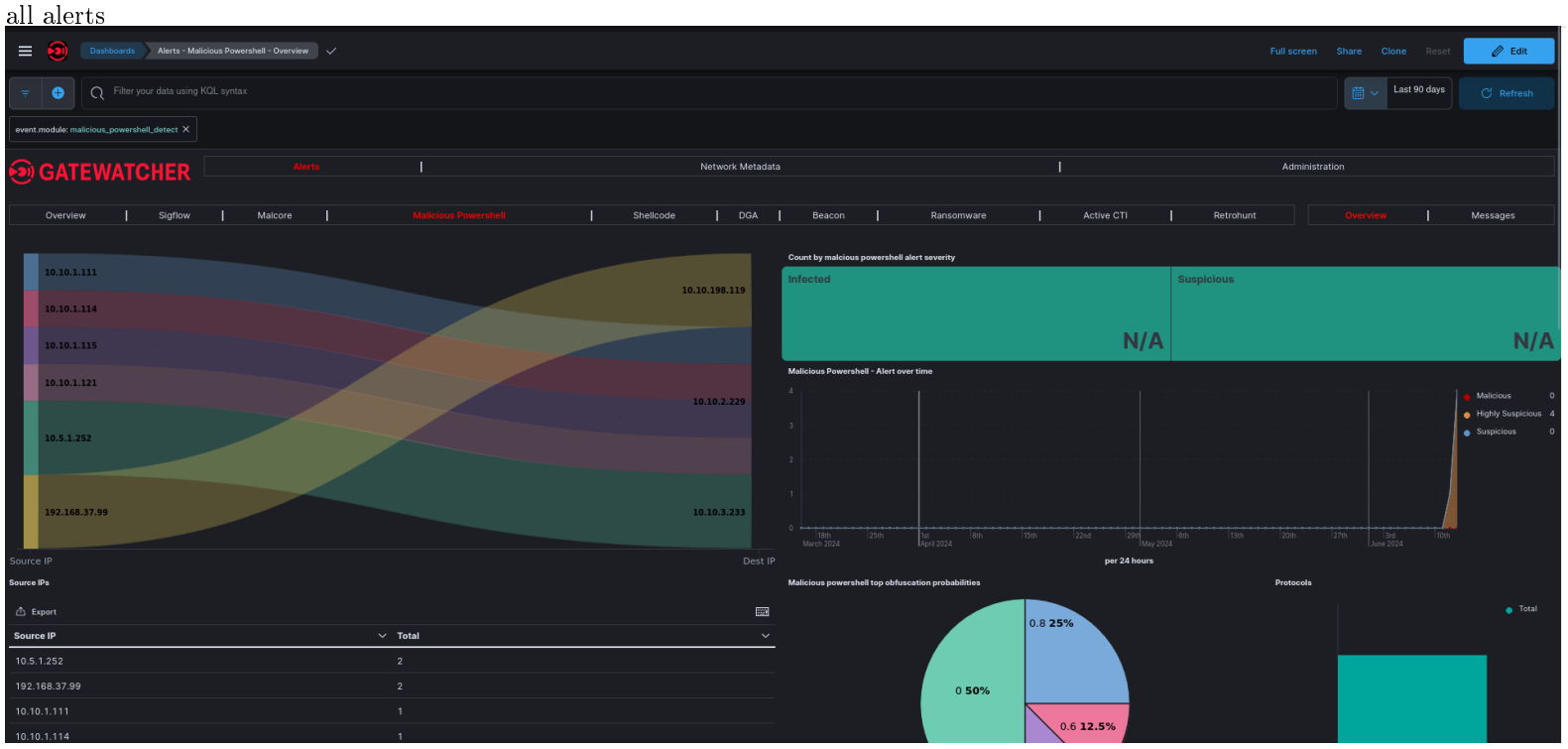


  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed in *Example of a Malicious Powershell detect alert in the WebUI*
    The displayed counters are given in the *Engine log data structure* appendix.
  - If the `Group by name` mode is activated, the name of the aggregated alerts and their number are displayed.
    Click on a grouping of alerts to display the list.
  - When the `Group by name` mode is disabled, different Source and Destination information is displayed for each alert.
    `Tags` and `Notes` are also visible and editable.
    The various Quick Access `Actions` are available for each alert.
- In the interface named **Kibana UI**:
  - In the `Alerts` screen of the **WebUI**, select the `Malicious Powershell` engine filter then validate.

See the presentation of the *WebUI `Alerts` screen*.



- After selecting the alert, click on the `Open powershell engine analytics` command of the `Actions` menu.
  Kibana is opened on the `Malicious Powershell` category of the `Alerts ` section: in the `Overview` tab, the database displays all alerts

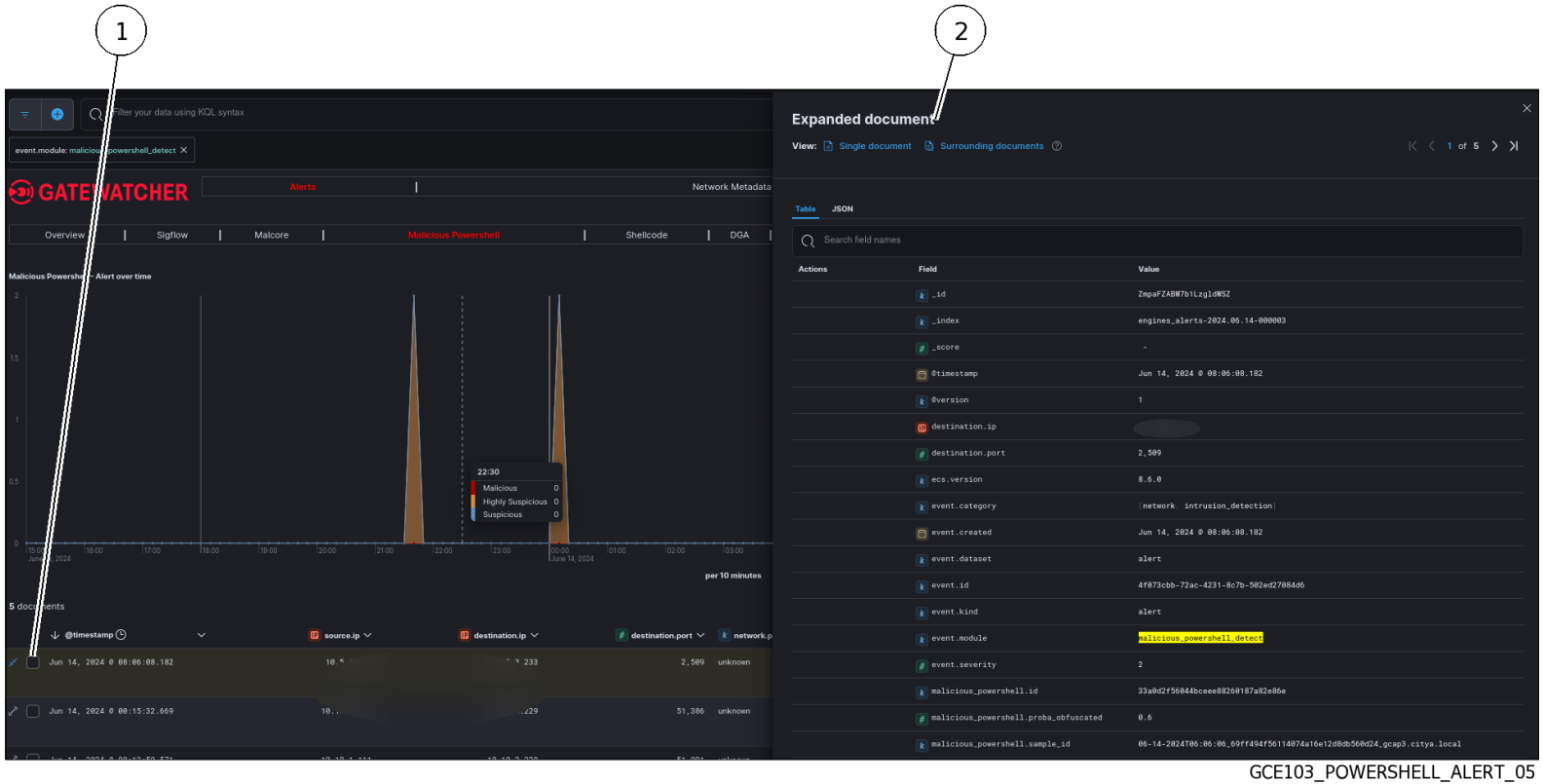


The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

- Click on the `Messages` tab (1).

GCE103_POWERSHELL_ALERT_04

- To consult information about a specific alert:
  - Click on the toggle icon (1) on the left of the Alert.
    The expanded document (2) is displayed.



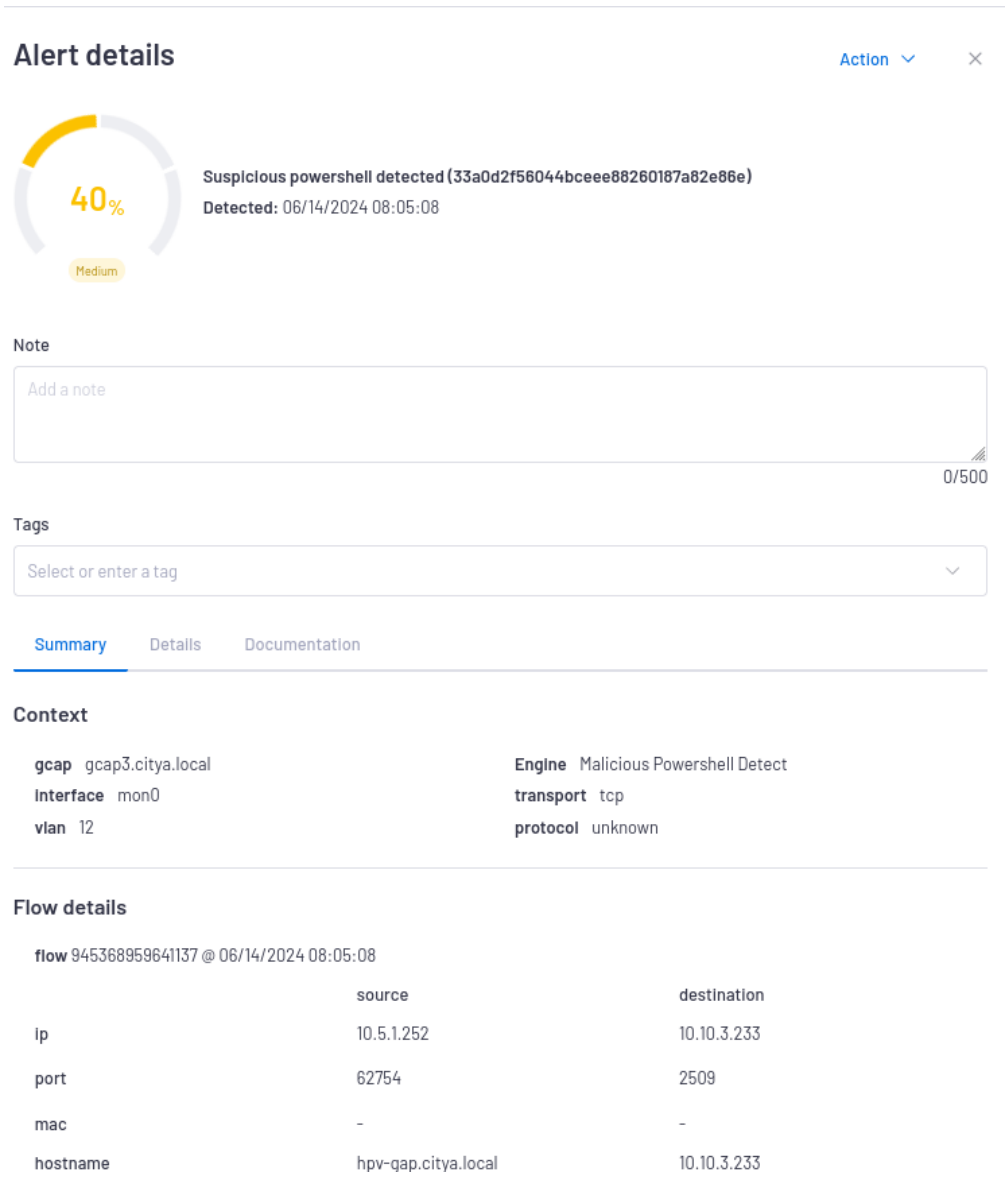
GCE103_POWERSHELL_ALERT_05

The detailed information of this alert can be viewed in table or json format (see the *Malicious Powershell log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

Note:

The **Kibana UI** can also be accessed without any filters via the `Hunting` icon on the left side menu bar in the WebUI.

2.1.4.2.1 Example of a Malicious Powershell detect alert in the WebUI



The presentation of the `Alert details` window is given in the *`Alert details` window*.
The counters are given in the *Example of an alert exported*.

2.1.4.2.2 Malicious Powershell log data structure

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields"

This information is displayed in the `Expanded document` screen of Kibana.

2.1.4.2.2.1 The header part of Malicious Powershell logs

The header section contains:

```
"_index": "engines_alerts-2024.12.04-000030",
"_id": "0KIEkpMBe7GX5B2fI_RU",
"_version": 1,
"_score": 0,
```

The detailed information is given in the table (*Counters of the header part of logs*).

2.1.4.2.2.2 The source part of Malicious Powershell logs

The source part is defined by "_source" in the logs.

Note:

The data displayed on the WebUI (alerts details window) is a part of the data displayed on the `Extended document` screen on the Kibana interface.
All data can be exported to a SIEM via syslog (an example of an exported alert is shown).
The detailed information is given in the table (*Counters of the header part of logs*).

The example given here is a Kibana example.


```
"malicious_powershell": {
  "sample_id": "12-04-2024T14:12:40_03afe38854c8443db03807bcc51cf935_gcap.gatewatcher.com",
  "score_details": {
    "InvokeRestMethod": 0,
    "StreamWriter": 0,
    "CharInt": 6,
    "AddContent": 0,
    "InvokeExpression": 100,
    "StrCat": 4,
    "StreamReader": 0,
    "SystemIOFile": 0,
    "InvokeWebRequest": 0,
    "StrJoin": 6,
    "WebClientInvokation": 20,
    "StrReplace": 0,
    "SetContent": 0,
    "GetContent": 0,
    "FmtStr": 8,
    "StartBitsTransfer": 0,
    "Base64": 188
  },
  "proba_obfuscated": 0.6,
  "score": 332,
  "id": "b5c38e2159f80a5a3076a353360cb5f1"
},
"event": {
  "created": "2024-12-04T14:12:44.750657+0000",
  "dataset": "alert",
  "module": "malicious_powershell_detect",
  "severity": 1,
  "kind": "alert",
  "category": [
    "network",
    "intrusion_detection"
  ],
  "id": "081d78f9-81f2-4408-84bf-2c8d6a8e5939"
},
"@version": "1",
"source": {
  "port": 33698,
  "ip": "x.y.z.A",
},
"ecs": {
  "version": "8.6.0"
},
"observer": {
  "log_format_version": "1.0.0",
  "hostname": "gcenter.domain",
  "vendor": "gatewatcher",
  "gcap": {
    "ingress": {
      "interface": {
        "name": "monvirt"
      }
    },
    "hostname": "gcap",
    "version": "2.5.x."
  },
  "product": "gcenter",
```


(continues on next page)

(continued from previous page)


```
  "uuid": "fc1e66e3-a397-5eb4-9277-754be778f317",
  "version": "2.5.x"
},
"destination": {
  "port": 9999,
  "ip": "x.A.V.X"
},
"@timestamp": "2024-12-04T14:12:44.750Z",
"network": {
  "protocol": "unknown",
  "transport": "tcp",
  "timestamp": "2024-12-04T14:11:36.408774+0000",
  "flow_id": 2227663757209674
```

2.1.4.2.2.3 List of counters of the alert

Note:

The alert counters are visible:
- In the `Alert details` screen of the WebUI
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.4.3 Management of the engine

2.1.4.3.1 Viewing the engine status

The engine status is displayed in the *`Health checks` screen*.

2.1.4.3.2 Engine update

The engine is updated with each new version of the GCenter.

2.1.4.3.3 Engine configuration

The configuration interface enables the engine activation:

- See the screen description, see the *`Malicious Powershell detect` screen (Malicious Powershell command)*
- See the *Setting up the Malicious Powershell detect engine* procedure.

2.1.4.4 Alert Analysis

The alerts are displayed on a specific screen described in the *WebUI `Alerts` screen*.
The general procedure for analyzing alerts is described in *Using of NDR dashboards*.
The specific procedure for analyzing Powershell alerts is described in the *Analyzing the Malicious Powershell detect alerts*.

2.1.5 Sigflow engine

2.1.5.1 Introduction

2.1.5.1.1 For what types of threats is this engine designed?

The Sigflow engine analyzes the whole network traffic and generate metadata and files and can, according to the **rules**, generate alerts.
Embedded detections are the following:

- Detections of uncommon behaviour or unrecommended actions perform on the corporate network
- Detections of suspicious/malicious actions perform on the corporate network such as malicious download, beaconing or file extraction
- Detections based on automatic generated rules based on indices of compromissions (IOCs) originated from CTI

2.1.5.1.2 How does this particular engine detect threats?

The Sigflow engine uses rules for threat detection.
These rules should describe the characteristics of the attacks and also be optimized to reduce false positives.
The GCenter allows to compile several sources and therefore several sets of rules.

2.1.5.1.3 How does Sigflow engine work in the GCenter?

Sigflow must be configured and this configuration is done by the GCap profile.
The`Ignored profile contains:

- Advanced configuration of the GCap parameters (including choice of protocols to monitor...)
- A structured list of rules

Note:

If the protocol monitored by rules is not selected then Sigflow will report these rules as incorrect and ignore them.

The GCap profile is created and updated on the GCenter.
Then this file is sent to the GCap.
The GCap retrieves packets from the TAP and reconstructs the files and creates the corresponding metadata.
Then, based on the defined rules, Sigflow applies the rules.
If a match is found between the rule and network traffic, it creates an alert indicating the reason for the detection.

2.1.5.1.3.1 For more information

Rules are organized: see *Organizing the rules*.
The rules manager manages the rules and sources: see *Sigflow engine signature sources*.
The set of rules to be applied to the GCap is defined in a ruleset: see *Rulesets*.
Sigflow is configured by the GCAP profile: see *GCAP Profiles*.

2.1.5.2 Detailed operation of the rules

2.1.5.2.1 Organizing the rules

The rules sent to the Sigflow engine are organized as follows:

- A list of sources providing signature set files grouped in categories
- A list of signatures capable of adapting to the needs of the environment to be monitored
- A list of Ruleset enabling signatures to be linked to a GCap

Note:

Managing the sources, categories, rules and rulesets is done in the rules manager built into the GCenter.

The following paragraphs describe the steps required to provide these rules in Ruleset form to the Sigflow module of the GCap through the GCenter:

- Management of available rule sources: see *Sigflow engine signature sources* paragraph
  Sources are used to report repositories where signatures are made available.
  Once downloaded and unzipped, the rules must be added to the **GCenter** interface.
  These sources update automatically in the case of public source/HTTP if the **GCenter** is connected to the internet, otherwise, a manual update can be made at this interface in order to have the latest signatures of available.
- The creation of rulesets from the sources: see the *Rulesets* paragraph
  Once the rules have been added, it is possible to directly assign this source to different rulesets
- The generation of rulesets: refer to *Generating rulesets*
- Applying rulesets to the GCap: refer to *Detection Rulesets*
- Advanced configuration of the GCap parameters: refer to *GCAP Profiles*

2.1.5.2.2 Sigflow engine signature sources

The sources include *Suricata* type detection signatures.
There are native sources: CTI like community CTI...

It is also possible to add public sources to the rules manager.
Each source issues a file of rule sets, grouped into categories.
It is possible to manage categories and rules.
The rules manager enables to:

- Define and manage the sources of signatures for the detection engine
- Manage the rule set files made available by the sources
- Manage the categories and rules of these files
- View the rules contained in the available sources

The signatures are updated using the `` `Threat-DB update` `` fonction.
The user (operator) can directly assign one or more sources to a Ruleset.

The source management manager is described in the *`Rulesets` screen*.
For implementation, see *Managing the Sigflow engine rule sources*.

2.1.5.2.3 Rulesets

Ruleset is the security and detection policy to be applied to the GCap.
As noted above, a ruleset is therefore composed of sources that include the various detection signatures.
The creation of the ruleset is mandatory for the **GCap** probe to be able to analyze the network traffic and raise alerts.
Modifications can be made to signatures or categories in order to adapt a rule to the specificities of the information system or to a particular need.
The source management manager is described in the *`Rulesets` screen*.

For implementation, see *Managing a Sigflow engine ruleset*.

2.1.5.2.3.1 Optimization of rulesets

Optimization of a ruleset consists of adapting it to the type of traffic analyzed (the different collection points).
The ruleset can be edited at any time by adding, modifying or deleting rules, categories or sources.
A modified ruleset must be applied to the GCap in order for the changes to take effect.

For implementation, see *Managing a Sigflow engine ruleset*.

2.1.5.2.3.2 Changing signatures

Signatures and categories can be enabled, disabled, or modified for a given Ruleset.
It is possible to:

- Activate signatures and categories
- Deactivate signatures and categories
- Modify the functioning of a signature in order to adapt it to the supervised information system by setting up a threshold or suppression of alert for a specific network.

To modify a signature in the following way:

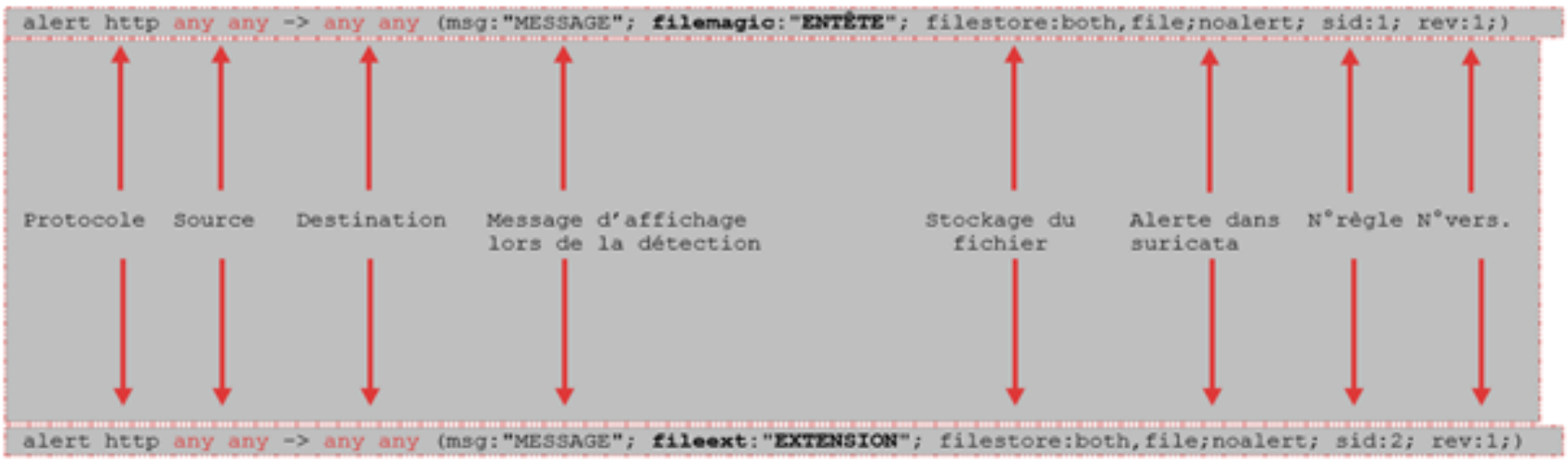
- Create a Suppress Rule on a rule: removes the raising of an alert according to a source or destination IP
- Create a Threshold Rule: limit the number of alerts to be displayed based on a source or destination IP

Note:

It is not possible to directly interact with the rule content from the rule manager.
For its implementation, see the *Modifying Sigflow engine rules* procedure.

2.1.5.2.3.3 Definition of signatures

Signatures in the sources can include references to blogs, CVEs, websites, and the like that can be accessed from the rules manager.
To better understand how a signature works, here is an example of a signature:



A signature is always made up of:

- An action
- A protocol
- Network parameters such as IP and source and destination port
- A message

Example of a signature:

```
  alert | drop tcp $HOME_NET -> EXTERNAL_NET any (msg;"icmp
detected";sid:1;rev:1;)
```

The following protocols may be subject to a rule:

TCP	UDP	ICMP
IP (représente « tout »)	HTTP	FTP
TLS (inclut SSL)	SMB	DNS

This signature is composed of:

- The first part "action": corresponds to the action to be performed in case of detection.
  For example: "alert, pass, drop..."
- The 2nd part "the header": it is this part that allows to define the meaning of the alert as well as the networks and protocols.
  For example: "tcp any -> any "
  This part is composed of:
- "Protocol" part: indicates the monitored protocol.
  For example: "tcp, udp, icmp"
- "Source and destination" section: specifies the source of traffic and the destination of traffic respectively.
  It is possible to assign IP addresses (IPv4 and IPv6 are supported) and IP ranges with operations if needed.
  It is also possible to use variables such as $HOME_NET and $EXTERNAL_NET that are managed in the *`Net variables` section of the `Config Gcaps profiles` menu* and *Net variables*
  These variables are used to increase the accuracy of the alerts provided by the signatures.
  The following syntax can be used to specify the addresses:

! 1.1.1.1	Toutes les IP sauf 1.1.1.1
![1.1.1.1, 1.1.1.2]	Toutes les IP sauf 1.1.1.1 et 1.1.1.2
$HOME_NET	Paramètre du HOME_NET en yaml
[$EXTERNAL_NET, !$HOME_NET]	EXTERNAL_NET et pas HOME_NET
[10.0.0.0/24, !10.0.0.1]	Le réseau 10.0.0.0/24 sauf pour 10.0.0.1

- The part "Ports (source and destination)" indicates the ports : the first is the source port, the second is the destination port (see the direction of the directional arrow).
  Traffic between and out of ports. Different protocols have different port numbers.
  For example, the default port for HTTP is 80 while 443 is usually the port for HTTPS.
  Note however that the port does not dictate which protocol is used in the communication. Rather, it determines which application receives the data.
  The list below gives examples of port specifications.

[80,81,82]	Ports 80, 81 et 82
[80: 82]	Plage de 80 à 82
[1024 :]	De 1024 jusqu'au plus haut numéro de port
!80	Tous les ports sauf 80
[80: 100,99]	Plage de 80 à 100 sauf 99 exclus

- the "Direction" part: indicates the direction of the flow.

->	De la source vers la destination (source -> destination)
<>	Les 2 directions (source <> destination)

- The last part corresponds to the options applied to the rule.
  These are surrounded by parentheses and separated by semicolons.
  Some options have parameters (such as msg), which are specified by the option keyword, followed by a colon, followed by the parameters.
  Others have no parameters, they are simply the keyword (like nocase).

For its implementation, see the procedure *Modifying Sigflow engine rules*.

2.1.5.2.3.4 Removing or limiting the number of alerts

The number of alerts sent can be limited automatically or manually:

- see *Manual creation of the deletion or limitation of the number of alerts*
- see *Automatic creation of limits on the number of alerts*

Deletion is used when alerts need to be deleted, that is, do not generate alerts for that particular signature.
This can only be done manually: see *Manual creation of the deletion or limitation of the number of alerts*.

2.1.5.2.3.5 Manual creation of the deletion or limitation of the number of alerts

The number of alerts for a particular signature can be controlled by deletion or limitation.
The limitation is usually used when the number of alerts must be kept to a minimum.
For example, if the need is to see only a maximum of one alert per minute for this signature.
Deletion is used when alerts need to be deleted, that is, do not generate alerts for that particular signature.
A rule can therefore contain the keyword *threshold* with the following syntax:

Syntaxe :

```
threshold: type <threshold|limit|both>, track <by_src|by_dst|by_rule|by_both>, count <N>, seconds <T>
```

The various fields are:

- `type` field: defines the limitation type. There are three possibilities:
- `limit`: limit alerts to no more than "N" times
- `threshold`: minimum threshold for a rule before it generates an alert
- `both`: limitation and threshold are applied
- `track` field: defines the scope. There are several possibilities:
- `by_src`: the limitation is applied to alerts with the same source IP address
- `by_dst`: the limitation is applied to alerts with the same destination IP address
- `by_rule`: the limitation is applied to all alerts triggered by the rule
- `by_both`: the limitation is applied to alerts with the same IP pair source address + destination
- `count` field: defines the quantity (limit or threshold) according to the type
- `seconds` field: defines the reference period

Example :

```
`threshold:  type threshold, track by_src, count 10, seconds 60;
```

This rule only generates an alert after 10 raised alerts with the same source IP address within a period of one minute.

The graphical interface for manually creating this limit or threshold rule is described in *`Rulesets` screen*.

The implementation of a limitation or deletion of alerts is done by modifying rules.
To do this, refer to *Modifying Sigflow engine rules*.

2.1.5.2.3.6 Automatic creation of limits on the number of alerts

Principle:

- The number of alerts for one or more GCaps can be controlled by limitation
- The GCenter counts alerts during an observation period and compares them to a programmable trigger point
- The GCenter determines the rules that generated this threshold exceeding and based on the selected criterion (filter type), GCenter automatically creates alarm limits
- These limits grouped by the GCap are communicated to the Sigflow engine present in each GCap to implement these limitations

There are several types of filtration:

- `by_src`: the limitation is applied to alerts with the same source IP address
- `by_dst`: the limitation is applied to alerts with the same destination IP address
- `by_rule`: the limitation is applied to all alerts triggered by the rule
- `by_both`: the limitation is applied to alerts with the same IP pair source address + destination

For more information, refer to the description given in *`Auto-threshold` screen*.
For implementation, refer to *Creation of automatic alarm limits*.

2.1.5.2.3.7 Generating rulesets

Once the ruleset is created and its configuration saved, the ruleset is generated and applied on the GCap.
For implementation, see the *Modifying Sigflow engine rules*.

2.1.5.2.4 GCAP Profiles

From this configuration interface, users will be able to apply specific policy rules. They can customize the settings from the following categories:

- *Detection Rulesets*
- *Base variables*
- *Net variables*
- *Flow timeouts*
- *Files rules management*
- *Packet filtering*

In order for the GCap to raise alerts, the user must first apply a ruleset to the GCap.
The GCap profile manager and its configurations are described in the *`GCaps profiles` screen*.
For implementation, see *Configuring GCaps using the `GCaps Profiles`*.

2.1.5.2.4.1 Detection Rulesets

The `Detection Rulesets` section enables the management of the network interfaces and defines the ruleset(s) used to inspect the captured traffic.

Note:

It is necessary to define rules in a ruleset before applying it to GCaps.
Failure to do so will result in no rules being applied to the GCap.
Only the ruleset previously saved in the Sigflow rules manager can be selected from this menu.

The `Detection Rulesets` section enables three configuration options:

- The *Single-tenant*
- The *Multi-tenant by interface*
- The *Multi-tenant by VLAN*

Note:

These configuration options are exclusive.
This means that it will not be possible to apply a single tenant and multi-tenant configuration at the same time.

2.1.5.2.4.2 Single-tenant

In Single-tenant mode, all traffic seen by the GCap is analyzed by the same ruleset.
The detection ruleset manager is described in the *`Detection Rulesets` section of the `GCaps profiles` screen*.
For implementation, see the procedure *Configuring the detection rulesets via the GCap profile*.

2.1.5.2.4.3 Multi-tenant by interface

In multi-tenant mode by interface, the user can apply a different ruleset depending on the capture interface.
Each tenant is a set of interfaces: for example, one can create the tenant 1 = {mon0} and the tenant 2 = {mon1, mon2}.
An interface can only be owned by one tenant.
If an interface is not assigned to any tenant, it will be in the "default tenant".
The default tenant scans all traffic that is not already scanned by a specific tenant.

The detection ruleset manager is described in the *`Detection Rulesets` section of the `GCaps profiles` screen*.
For implementation, see *Configuring the detection rulesets via the GCap profile*.

2.1.5.2.4.4 Multi-tenant by VLAN

The Multi-tenant by VLAN mode enables:

- The assigning one ruleset per VLAN
- The assigning a ruleset for the default VLAN for those VLANs not created via the interface

The **Multi-tenant by VLAN** enables a configuration to be applied for each VLAN previously created in the interface and to have distinct monitoring on different networks.
Thus, it is possible to apply a ruleset independently for each VLAN.
A VLAN named "default" is created as standard in the interface. It enables a ruleset to be applied for all VLANs not explicitly specified in the interface.

The detection ruleset manager is described in the *`Detection Rulesets` section of the `GCaps profiles` screen*.
For implementation, see *Configuring the detection rulesets via the GCap profile*.

2.1.5.2.4.5 Base variables

The **Base variables** section enables the probe's capture parameters to be adjusted using the advanced Sigflow functions that can be configured from **GCenter**.
Changes to this configuration have an impact on the alerts sent from the GCap probe to the GCenter.
Enabling certain options will enable the sending of alerts, anomalies, metadata, file information, and protocol-specific records.
Alerts are records of events triggered by the matching of a rule with network traffic.
An alert will be created with associated metadata, such as the application layer record (HTTP, DNS, etc).
The graphical interface of this base variable manager is described in *`Base variables` Section of the `GCaps profiles` screen*.

The basic variables section is composed of:

- *Stream analysis and file extraction*
- *HTTP Proxy*
- *Payload*
- *Community ID*
- *Alerting and logging*

2.1.5.2.4.6 Stream analysis and file extraction

The stream analysis and file extraction area enables you to control how the Sigflow engine handles maximum stream and file extraction sizes.
The graphical interface and the details of the parameters are described in the *`Stream analysis and file extraction` zone*.

2.1.5.2.4.7 HTTP Proxy

The HTTP Proxy area enables enhanced metadata and alerts for streams mandated with the X-Forwarded-For (XFF) http header.
The graphical interface and the details of the parameters are described in the *`HTTP Proxy` Zone*.

Note:

XFF is a standard header enabling to identify the original IP address of a client connecting to a web server through an HTTP proxy or load balancer.

2.1.5.2.4.8 Payload

The **Payload** section enables enabling or disabling various fields present (Http body, Payload printable, Http body printable...) in the events.
The graphical interface and the details of the parameters are described in the *`Payload` zone*.

2.1.5.2.4.9 Community ID

The **Community ID** section enables or disables this feature in events.
This enables identifying the network streams being analyzed.

Note:

This field is present in solutions other than Gatewatcher. It can therefore enable correlating the different tools of the same information system.

The graphical interface and the details of the parameters are described in the *`Community ID` zone*.

2.1.5.2.4.10 Alerting and logging

This section enables configuring the **alerting** and **logging** of the protocols used by the GCap.

Note:

If the GCap is one version ahead of the GCenter, it is possible that some protocols are not yet implemented in the latter.

This is discussed in more detail in the GCAP-documentation in the section *Sigflow detection engine > Rebuilding files*.

Terminology for alerting and logging:

- **alerting** consists in activating the Sigflow signature detection for a given protocol. Indeed, if Sigflow is activated for a protocol then the stream that is identified by a signature will raise an alert on the GCenter side.
- **logging** consists in enabling the generation of metadata for a given protocol. Indeed, if the latter is enabled for a protocol then each observed session will generate metadata for that protocol on the GCenter side.

Managing the configuration of the protocols is done:

- By using default profiles such as Essential, Balanced, Deep, Paranoid and Performance.
- By modifying the content of the profile uploaded to the GCap

The choice of the default profile and the loading on the GCap is done in the graphical interface detailed in the *`GCaps Pairing` screen*.
Changing the configuration of the profile loaded into the GCap is done in the graphical interface detailed in the *`Alerting and logging` zone*.
The default configuration of protocols varies depending on the GCap profile used: the list is shown in the *Default settings for existing profiles available*.
The list of protocols that can be configured with the alerting option and with the logging option is provided in the *Default settings for existing profiles available* paragraph.
For implementation, see the *Configuring the Base variables parameters via the GCap profile*.

2.1.5.2.4.11 Net variables

The **Net variables** area of the GUI enables defining the network variables used in the Sigflow rules.
The list of variables and their default values are given in the *`Net variables` section of the `Config Gcaps profiles` menu*.
This graphical interface is described in the *`Net variables` section of the `Config Gcaps profiles` menu*.
For implementation, see the procedure *Configuring the network variables parameters via the GCap profile*.

2.1.5.2.4.12 Flow timeouts

The **Flow timeouts** section enables configuring the time in seconds that Sigflow keeps a flow in memory depending on its status.
The list of variables and their default values are given in the *`Flow timeouts` section of the `GCaps profiles` screen*.
This graphical interface is described in the *`Flow timeouts` section of the `GCaps profiles` screen*.

2.1.5.2.4.13 Files rules management

The **Files rules management** section enables choosing the file types that the probe will retrieve for a given protocol.
File extraction works in parallel with the Sigflow signatures defined for these same protocols.
Files are reconstructed and then saved to disk with metadata that includes information such as:

- Time stamp
- Source/destination IP address
- Protocol
- Source/destination port
- Size
- Md5sum, etc

Managing the configuration of the file extraction rules is done:

- By using default profiles such as Essential, Balanced, Deep, Paranoid and Performance: in order from most to least complete
- By modifying the content of the profile uploaded to the GCap

The choice of the default profile and the loading on the GCap are done in the graphical interface detailed in the *`GCaps Pairing` screen*.
Changing the configuration of the profile loaded into the GCap is done in the graphical interface detailed in the *`File rules` section of the `GCaps profiles` screen*.
The list of protocols as well as the list of file types are given in the *`GCaps profiles` screen*.

For implementation, see the *Configuring the file reconstruction rules via the GCap profile*.

2.1.5.2.4.14 Packet filtering

The `Packet filters` section enables specific traffic to be ignored directly at the GCap network card level.
This feature enables the GCap to avoid overloading the GCap with "unnecessary" traffic such as encrypted streams, backup streams, etc., or traffic that may cause the cpus to overload such as Elephant Flow, Miles Flow, etc.
The selection of traffic to be ignored is based on vlan, network prefix, protocol, and network ports.

This graphical interface is described in the *`Packet filters` section of the `Gcaps profiles` screen*.
For implementation, see the *Configuring filters on targeted parts of the analyzed traffic via the GCap profile*.

2.1.5.3 Events generated

The events generated by Sigflow are:

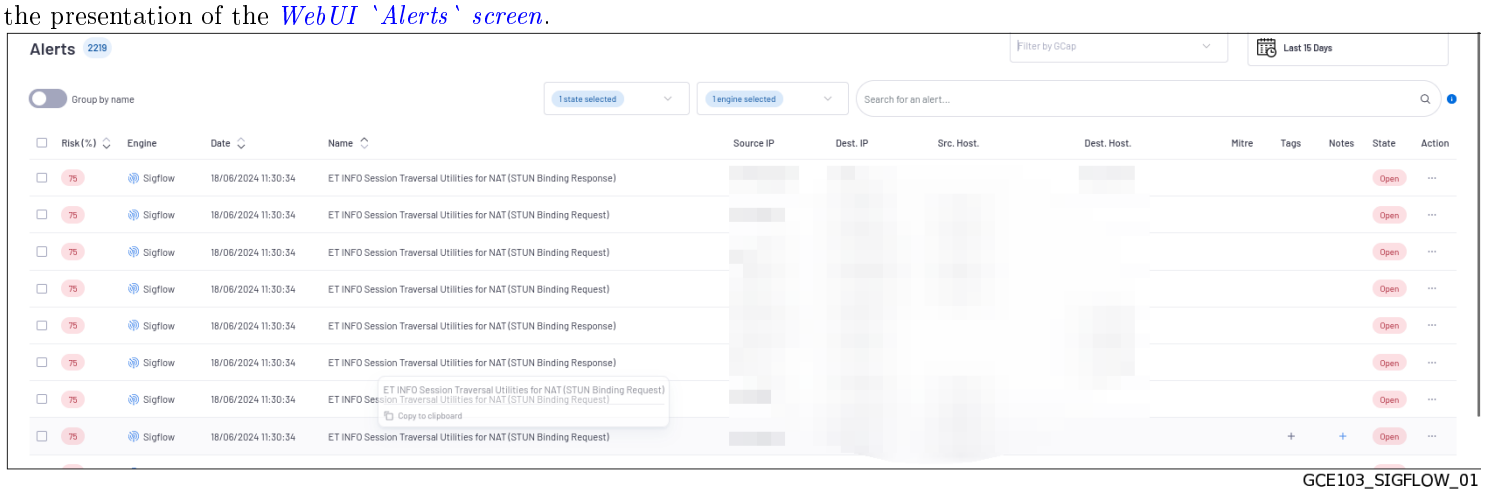
- *Events of type "alert"* when the engine has found a match with the signature defined in the alert rules.
  Events are displayed in the main GCenter interface as well as in Kibana.
- *Events of type "fileinfo"* when the Sigflow engine has reconstructed the network flow files`.
  These fileinfo events are only visible in the Kibana interface.
- *Events of type "meta-data"* when the Sigflow engine has recognized the network flow.
  These metadata events are only visible in the Kibana interface.

These events (or logs) are structured in the same way and this structure is presented in the *Data structure of the Events of type "alert"* paragraph.

2.1.5.3.1 Events of type "alert"

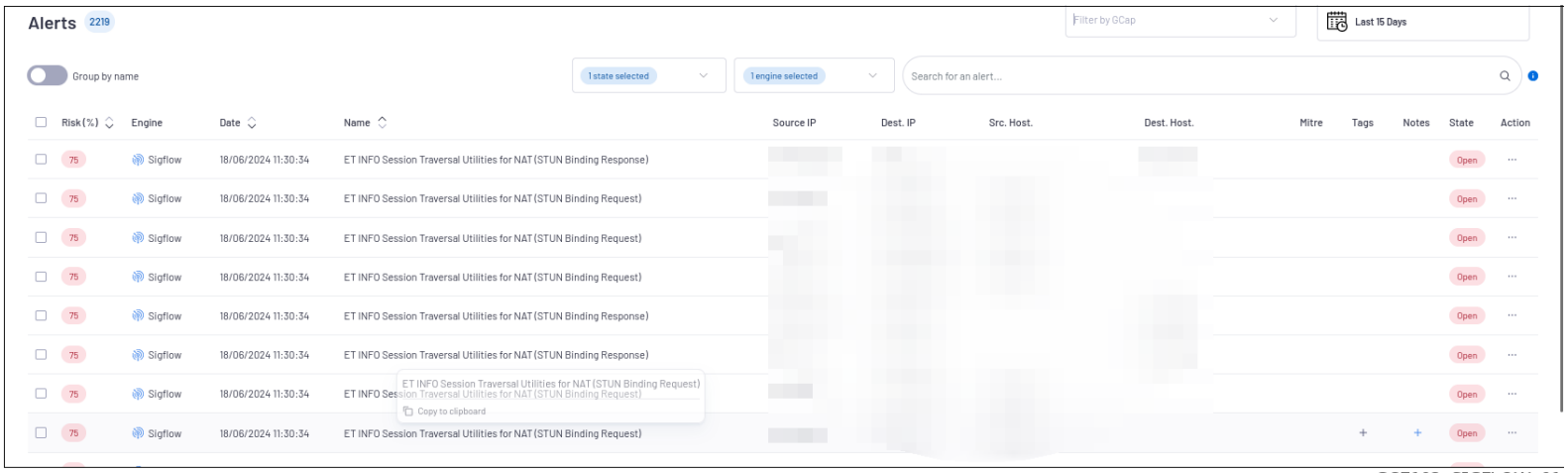
Events of type "alert" are generated when the engine has found a match with the signature defined in the alert rules.
These are displayed:

- In the main interface named **WebUI** on the GCenter in the `Alerts` screen
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
  It is possible to view the found signature and its definition.
  - To view the alerts, select the `Sigflow` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.



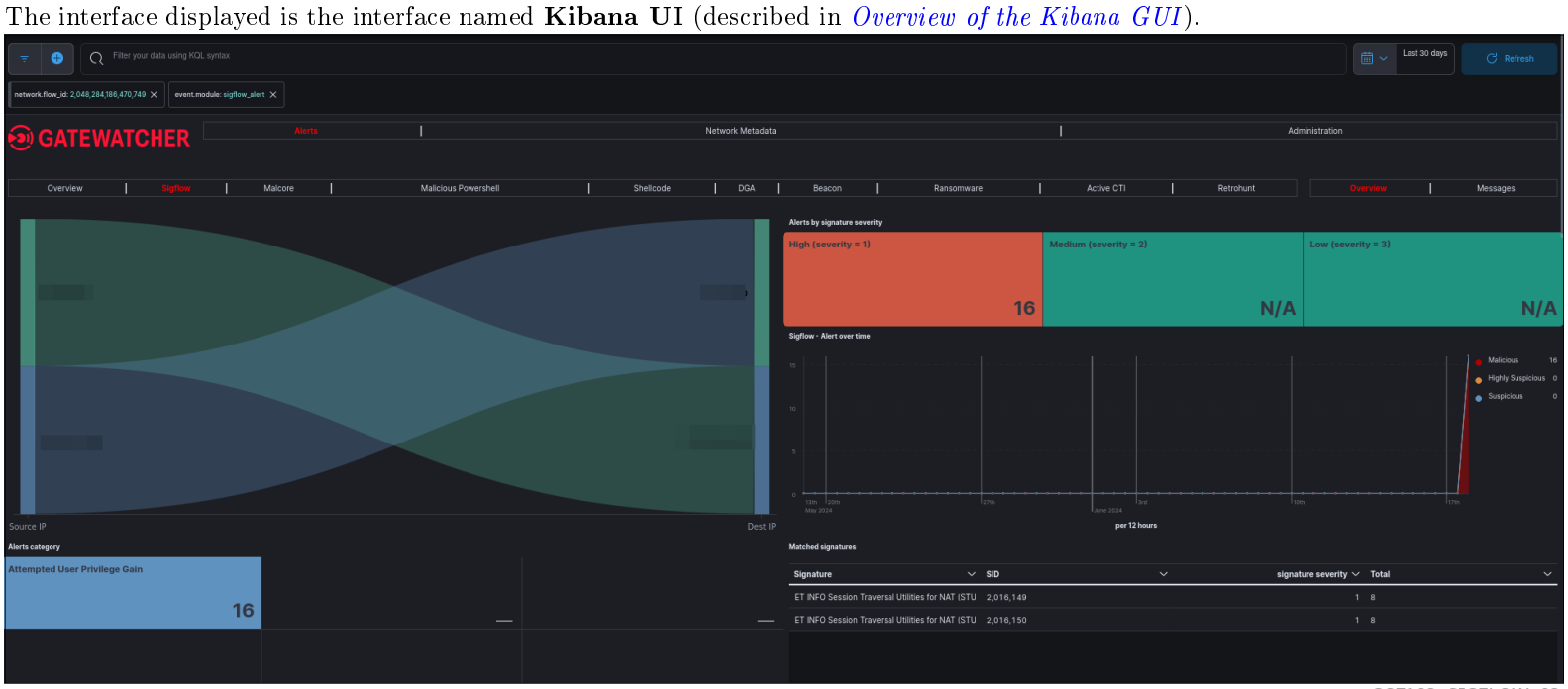
GCE103_SIGFLOW_01

  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed: see *Example of a Sigflow alert in the WebUI*.
    The displayed counters are given in the *Engine log data structure* appendix.
- In the interface named **Kibana UI**
  - In the main interface **WebUI**, to view the alerts, select the `Sigflow` engine filter.
    The screen displays only the list of Sigflow alerts.



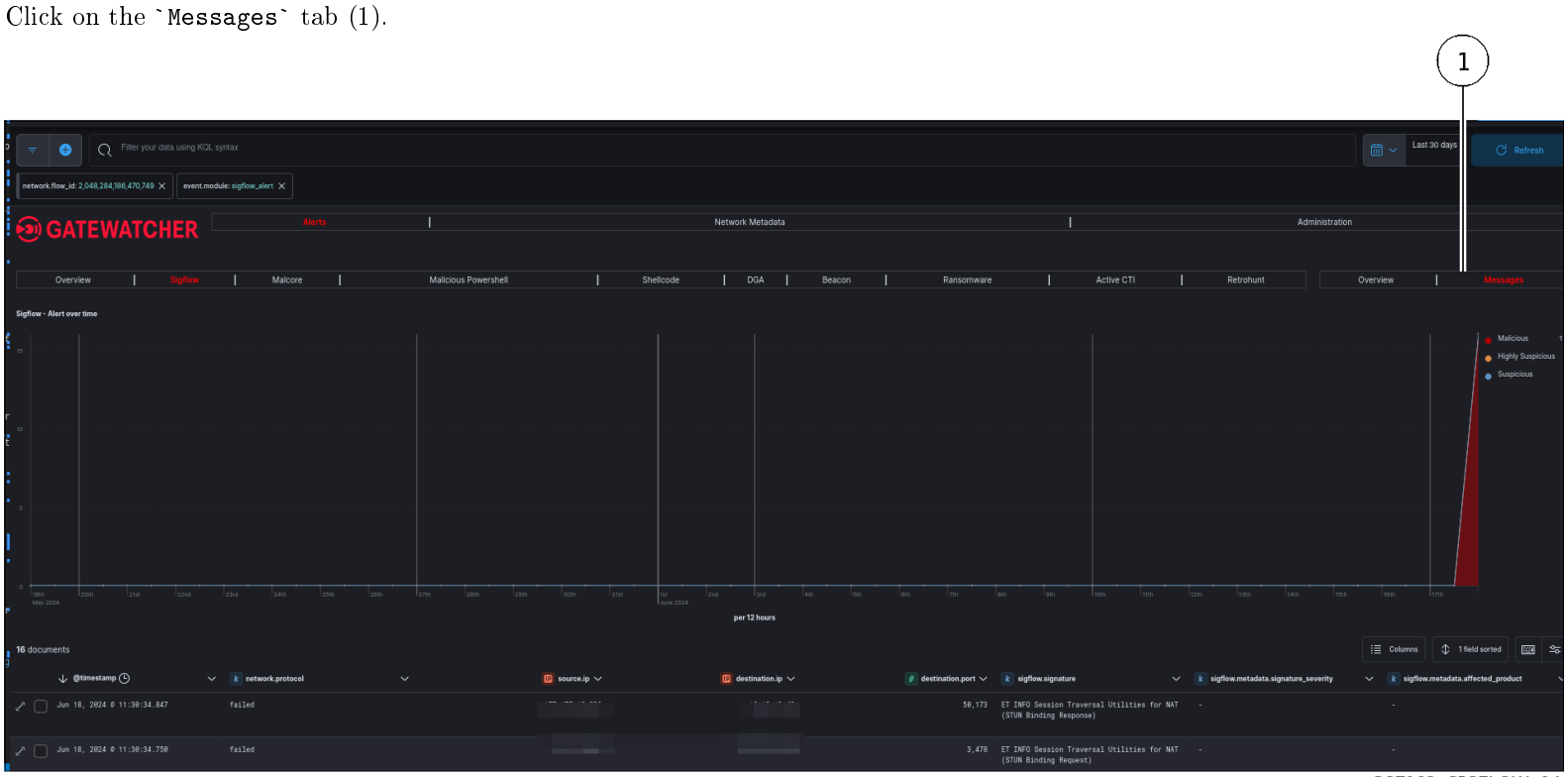
GCE103_SIGFLOW_01

- After selecting the alert, click on the `Open flow details` command of the `Actions` menu.
  See the presentation of the *WebUI `Alerts` screen*.
  Kibana is opened on the `Sigflow` category of the `Alerts ` section.
  The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).



GCE103_SIGFLOW_03

- Click on the `Messages` tab (1).



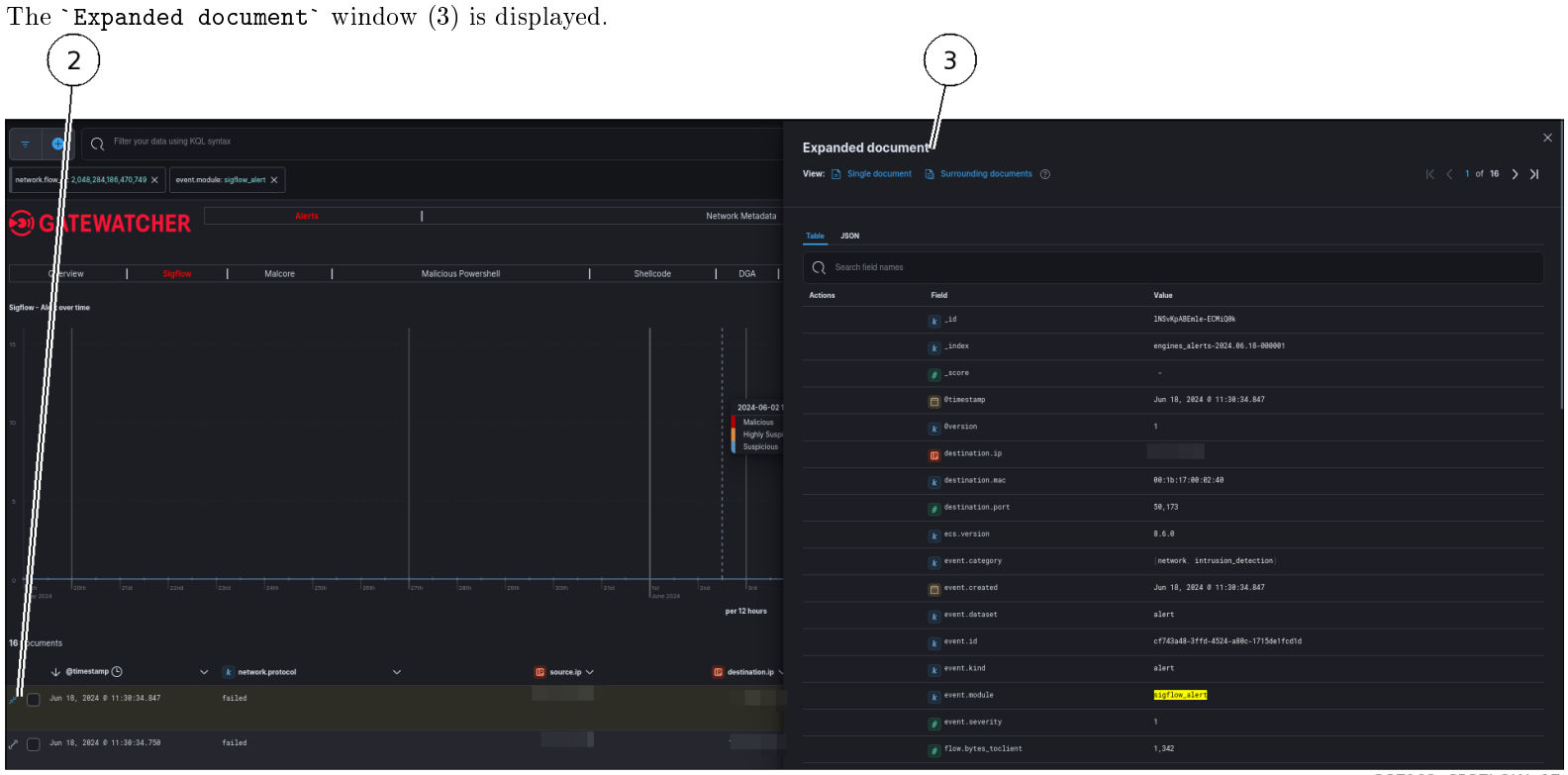
GCE103_SIGFLOW_04

The Kibana database is filtered with the filters:

- network.flow_id: unique ID of the flow selected
- event.module: sigflow_alert

This page displays all alerts detected by Sigflow in this network flow (whatever the IP addresses or the direction).

- Click on the toggle icon on the left of the alert (2).
  The `Expanded document` window (3) is displayed.

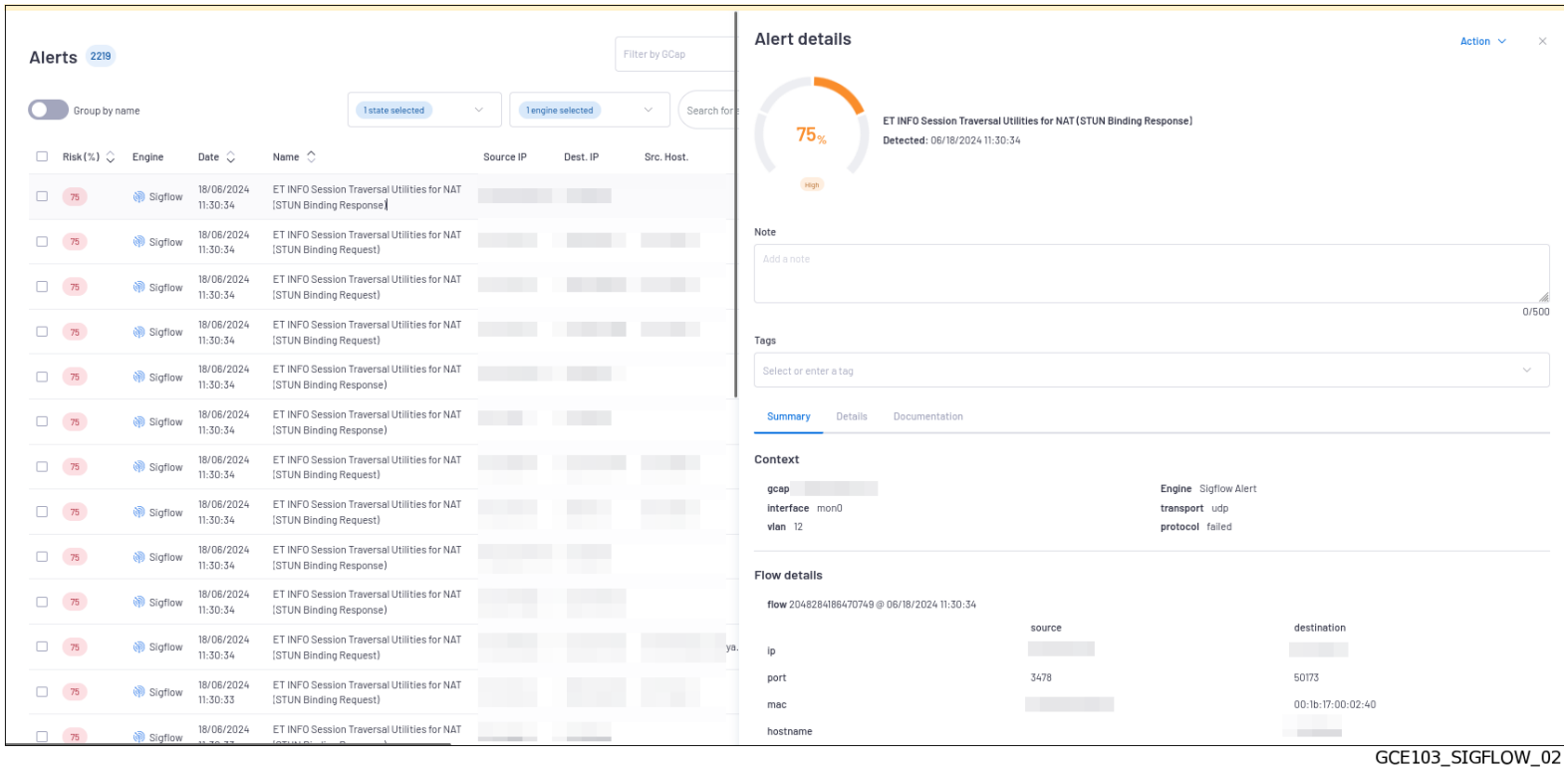


The detailed information of this alert can be viewed in table or json format (see the *Events of type "alert"*).
The displayed counters are given in the *Engine log data structure* appendix.

Note:

The **Kibana UI** can also be accessed without any filters via the `Hunting` icon on the left side menu bar in the WebUI.

2.1.5.3.1.1 Example of a Sigflow alert in the WebUI



The presentation of the `Alert details` window is given in the *`Alert details` window*.
The counters are given in the *Example of an alert exported*.

2.1.5.3.1.2 List of protocols in the Events of type "alert"

The list of protocols that can generate alerts is indicated by the parameter *Default settings for existing profiles available* (app_proto field)`.
If a protocol changes along the way (for example if SMTP is upgraded to TLS via STARTTLS) or if the protocols used are not the same in both directions of the flow, the following fields may appear:

- app_proto_tc (to client)
- app_proto_ts (to server)
- app_proto_orig

Note:

The protocol actually recognized by Sigflow is defined in the GCap profile in the `Alerting and logging` tab in the `Alerting` column.

2.1.5.3.1.3 Data structure of the Events of type "alert"

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields"

This information is displayed in the `Expanded document` screen of Kibana.

2.1.5.3.1.4 The header part of the Events of type "alert"

The header section contains:

```
"_index": "engines_alerts-2024.11.26-000022",
"_id": "yZzDZ5MBe7GX5B2fDKfY",
"_version": 1,
"_score": 0,
```

The detailed information is given in the table (*Counters of the header part of logs*).

2.1.5.3.1.5 The source part of the Events of type "alert"

The source part defined by "_source" contains:

Note:

The data displayed on the WebUI (alerts details window) is a part of the data displayed on the `Extended document` screen on the Kibana interface.
All data can be exported to a SIEM via syslog (an example of an exported alert is shown).
The detailed information is given in the table (*Counters of the header part of logs*).

The example given here is a Kibana example.

```
"http": {
  "response": {
    "status": 200,
    "bytes": 1197,
    "mime_type": "application/octet-stream"
  },
  "http_response_body": "TVqQAAMAAAAA//8AALgAAAOAADwELAQYAAAAAAAAAA",
  "http_response_body_printable": "MZ.....!..L.!This program cannot be run in DOS mode.\r\r\n$..............",
  "hostname": "",
  "version": "HTTP/1.1",
  "request": {
    "method": "GET"
  }
},
"source": {
```

(continues on next page)

(continued from previous page)


```
  "ip": "",
  "port": 41710,
  "mac": ""
},
"flow": {
  "pkts_toserver": 4,
  "bytes_toserver": 338,
  "pkts_toclient": 12,
  "bytes_toclient": 15280,
  "start": "2024-11-26T09:16:56.277148+0000"
},
"observer": {
  "gcap": {
    "ingress": {
      "interface": {
        "name": "monvirt"
      }
    },
    "hostname": "gcap.gatewatcher.com",
    "version": "2.5.x"
  },
  "product": "gcenter",
  "hostname": "gcenter.domain.local",
  "version": "2.5.3.103",
  "log_format_version": "1.0.0",
  "uuid": "fc1e66e3-a397-5eb4-9277-754be778f317",
  "vendor": "gatewatcher"
},
"network": {
  "tx_id": 0,
  "protocol": "http",
  "timestamp": "2024-11-26T09:16:56.278736+0000",
  "transport": "tcp",
  "flow_id": 95140270586524
},
"ecs": {
  "version": "8.6.0"
},
"metadata": {
  "flowbits": [
    "min.gethttp",
    "exe.no.referer"
  ]
},
"destination": {
  "ip": "x.y.z.a",
  "port": 16122,
  "mac": "10:e2:ba:a6:a4:70"
},
"sigflow": {
  "action": "allowed",
  "payload_printable": "GET /emd.exe HTTP/1.1\r\nHost: opred.net\r\nConnection: Keep-Alive\r\n\r\n",
  "stream": 1,
  "packet": "kOK6pqSQkOK6pqSRmgk2FpoJNha",
  "packet_info": {
    "linktype": 1
  },
  "signature_id": 2019714,
  "metadata": {
    "updated_at": [
      "2024_04_22"
    ],
    "performance_impact": [
      "Significant"
    ],
    "created_at": [
      "2014_11_15"
    ]
  },
  "gid": 1,
  "signature": "ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile",
  "payload": "ROVUIC9lbWQuZXhlIEhUVFAvMS4mUNCgOK",
  "category": "Potentially Bad Traffic",
```


(continues on next page)

(continued from previous page)


```
    "rev": 11
  },
  "url": {
    "domain": "opred.net",
    "path": "/emd.exe"
  },
  "@timestamp": "2024-11-26T09:16:56.278Z",
  "event": {
    "created": "2024-11-26T09:16:56.278736+0000",
    "dataset": "alert",
    "module": "sigflow_alert",
    "kind": "alert",
    "category": [
      "network",
      "intrusion_detection"
    ],
    "severity": 2,
    "id": "ce95f31d-6bb1-45f9-9f06-1661f5431329"
  },
  "@version": "1"
}
```


2.1.5.3.1.6 List of counters of the Events of type "alert"

Note:

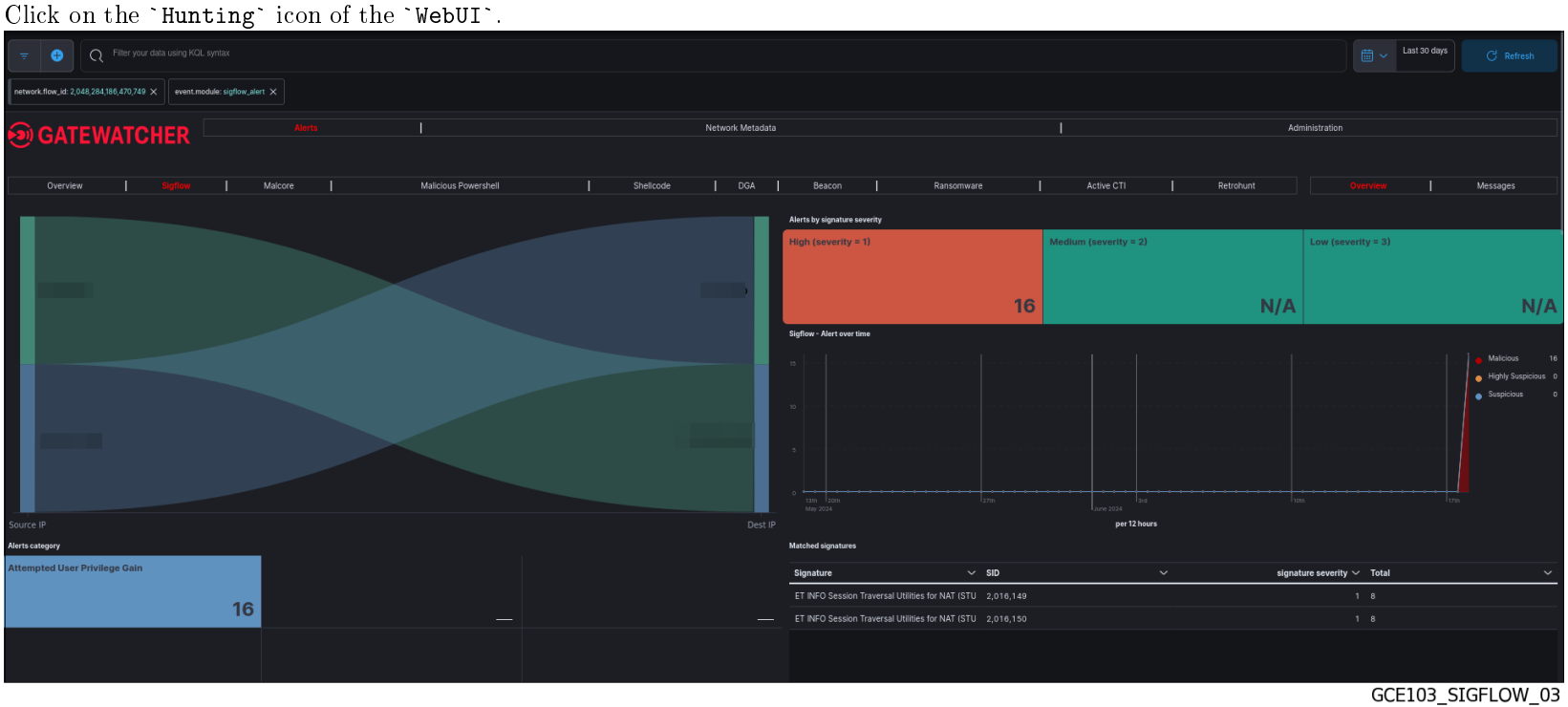
The alert counters are visible:
- In the `Alert details` screen of the WebUI
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.5.3.2 Events of type "fileinfo"

Events of type "fileinfo" are generated when the Sigflow engine has reconstructed the network flow **files**.
These fileinfo events are visible in the Kibana interface.

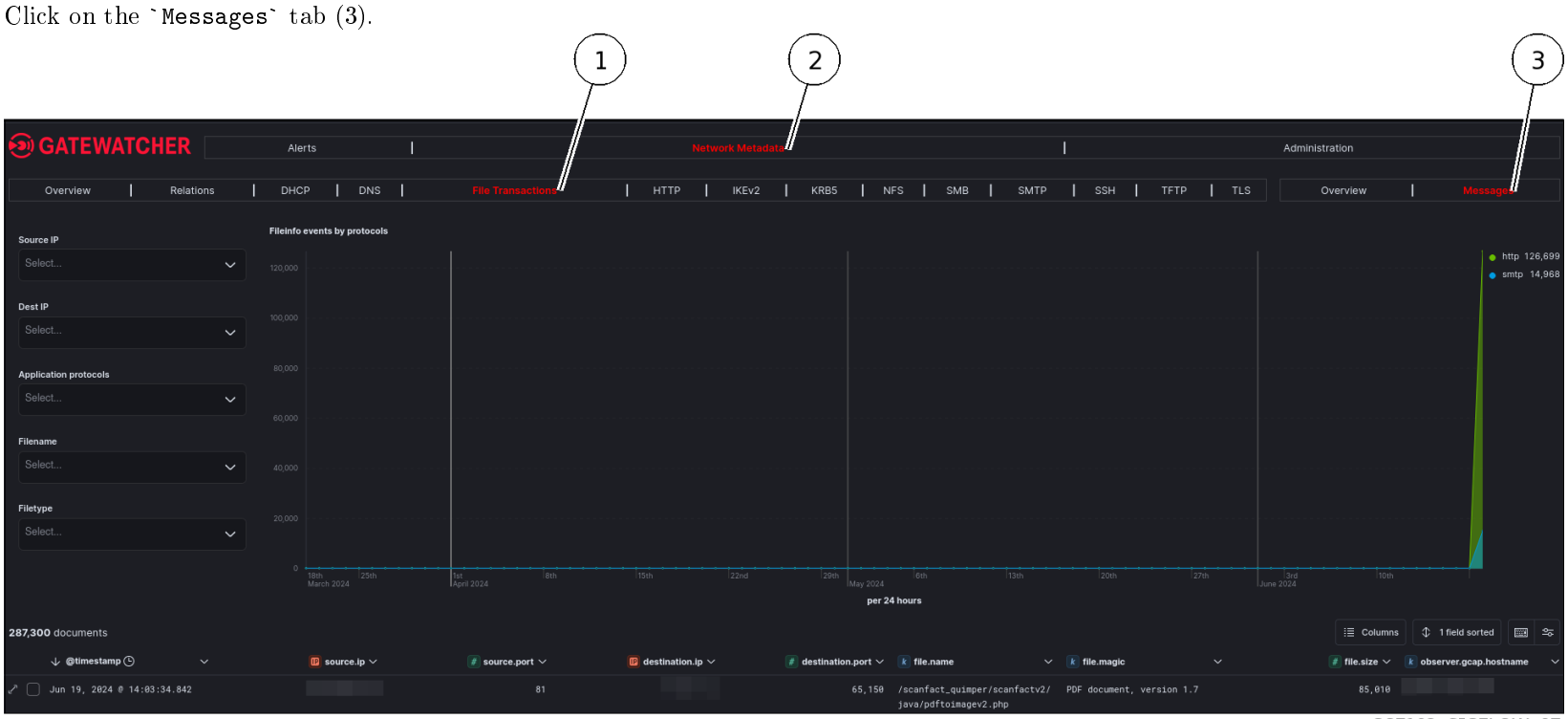
- Click on the `Hunting` icon of the `WebUI`.



GCE103_SIGFLOW_03

The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

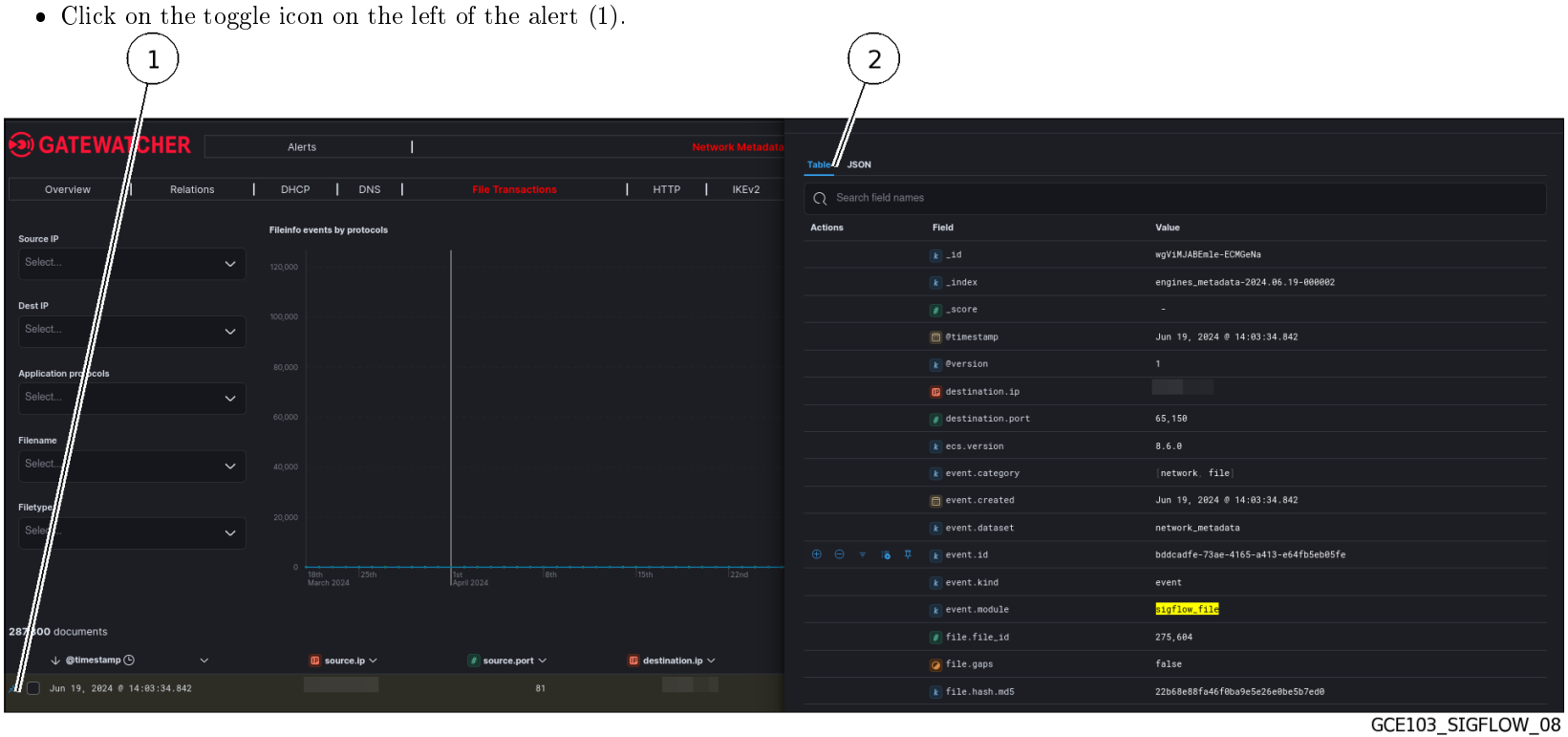
- Click on the `Network Metadata` section (2) then the `File Transactions` category (1).
- Click on the `Messages` tab (3).



GCE103_SIGFLOW_07

This page displays all events of fileinfo type corresponding to the reconstructed files in this network flow.

- Click on the toggle icon on the left of the alert (1).



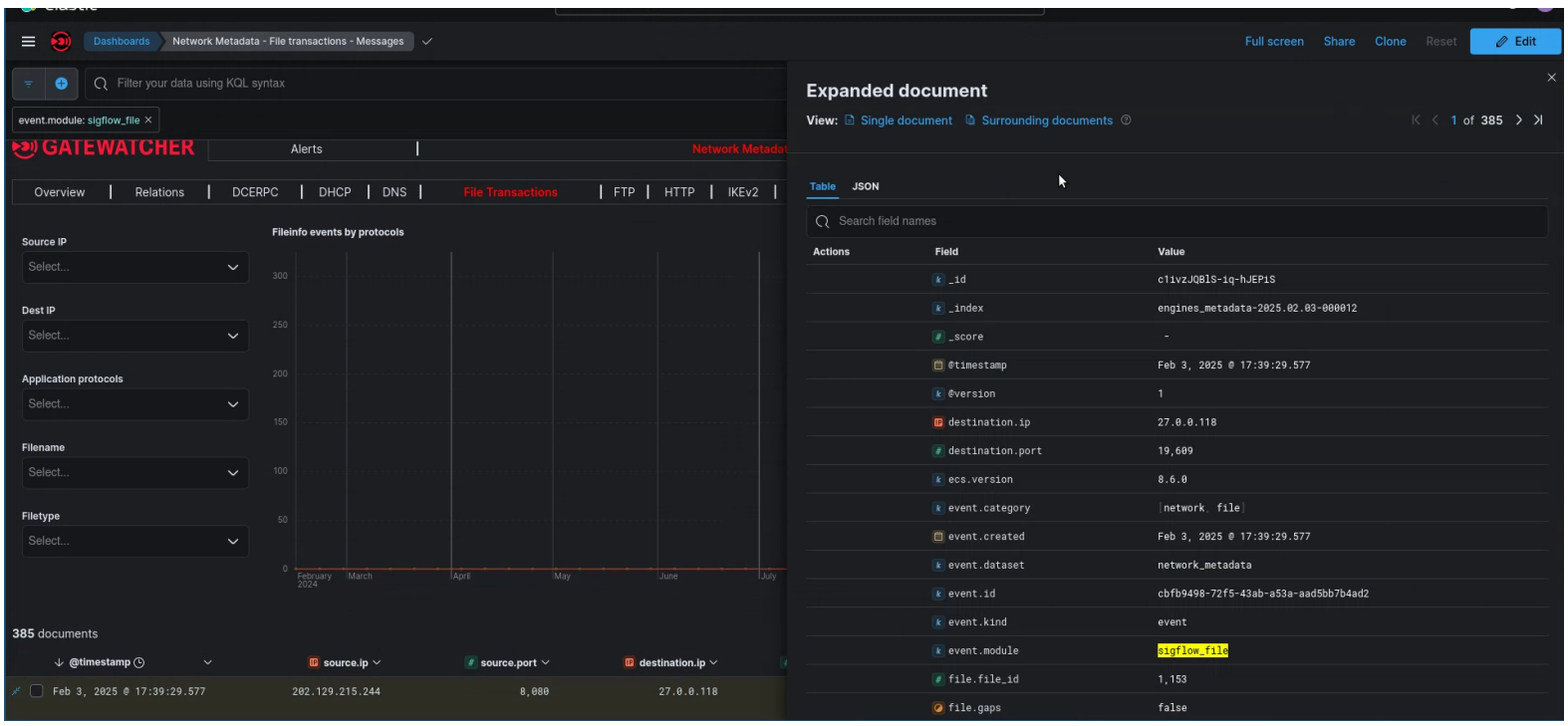
GCE103_SIGFLOW_08

The detailed information (2) of this event can be viewed in table or json format.

Note:

The **Kibana UI** can also be accessed without any filters via the `Hunting` icon on the left side menu bar in the WebUI.

2.1.5.3.2.1 Example of the events of type "fileinfo"



The counters are given in the *Example of an alert exported*.

2.1.5.3.2.2 Data structure of the events of type "fileinfo"

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields"

This information is displayed in the `Expanded document` screen of Kibana.

2.1.5.3.2.3 The header part of the events of type "fileinfo"

The header section contains:

```
"_index": "engines_metadata-2025.02.03-000012",
"_id": "c1ivzJQBlS-iq-hJEPiS",
"_version": 1,
"_score": 0,
```

The detailed information is given in the table (*Counters of the header part of logs*).

2.1.5.3.2.4 The source part of the events of type "fileinfo"

The source part defined by "_source" contains:

Note:

All data can be exported to a SIEM via syslog (an example of an event of type "fileinfo" is shown).
The detailed information is given in the table (*Counters of the header part of logs*).

The example given here is a Kibana example.

```
"user_agent": {
  "original": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.
↪30729; .NET CLR 3.0.30729)"
},
"destination": {
  "port": 19609,
  "ip": "x.y.z.a"
},
"source": {
  "port": 8080,
  "ip": "a.b.c.d"
},
"event": {
  "dataset": "network_metadata",
  "module": "sigflow_file",
  "category": [
    "network",
    "file"
  ],
  "created": "2025-02-03T16:39:29.577001+0000",
  "id": "cbfb9498-72f5-43ab-a53a-aad5bb7b4ad2",
  "kind": "event"
},
"@version": "1",
"file": {
  "tx_id": 1,
  "magic": "Macromedia Flash data (compressed), version 14",
  "name": "/6SuCHKKkf8Sf1aFXJPqD0R6r3oEDCrbwHFm23EU-Af2zwWdHgpn6mEGu5XlxFust",
  "sid": [
    1100020
  ],
  "state": "CLOSED",
  "file_id": 1153,
  "hash": {
    "sha256": "350836364013549b6a76aab79d57d109df6acc143759e24a952d3ff5d6a76ec4",
    "md5": "67ca9a31f220bc7b68f203c07ad668b9"
  },
  "size": 77068,
  "gaps": false,
  "stored": true
},
"http": {
  "http_refer": "http://tsevid-synonymi.justdanceatsea.com:8080/ndf4xx22ci.php",
  "response": {
    "mime_type": "application/x-shockwave-flash",
    "status": 200,
    "bytes": 77068
  },
  "hostname": "tsevid-synonymi.justdanceatsea.com",
  "http_port": 8080,
  "version": "HTTP/1.1",
  "request": {
    "method": "GET"
  }
},
"url": {
  "domain": "tsevid-synonymi.justdanceatsea.com",
  "path": "/6SuCHKKkf8Sf1aFXJPqD0R6r3oEDCrbwHFm23EU-Af2zwWdHgpn6mEGu5XlxFust"
},
"observer": {
  "product": "gcenter",
  "uuid": "78f4fed1-c9ad-52b9-b509-6b87767f501f",
  "hostname": "gcenter.domain.local",
  "gcap": {
    "ingress": {
      "interface": {
        "name": "monvirt"
      }
    },
    "hostname": "gcap.gatewatcher.fr",
    "version": "2.5.x"
  },
  "version": "2.5.x",
  "vendor": "gatewatcher",
```


(continues on next page)

(continued from previous page)


```
  "log_format_version": "1.0.0"
},
"@timestamp": "2025-02-03T16:39:29.577Z",
"ecs": {
  "version": "8.6.0"
},
"network": {
  "protocol": "http",
  "transport": "tcp",
  "timestamp": "2025-02-03T16:39:29.577001+0000",
  "flow_id": 1156097574154966
}
```


2.1.5.3.2.5 List of counters of the events of type "fileinfo"

Note:

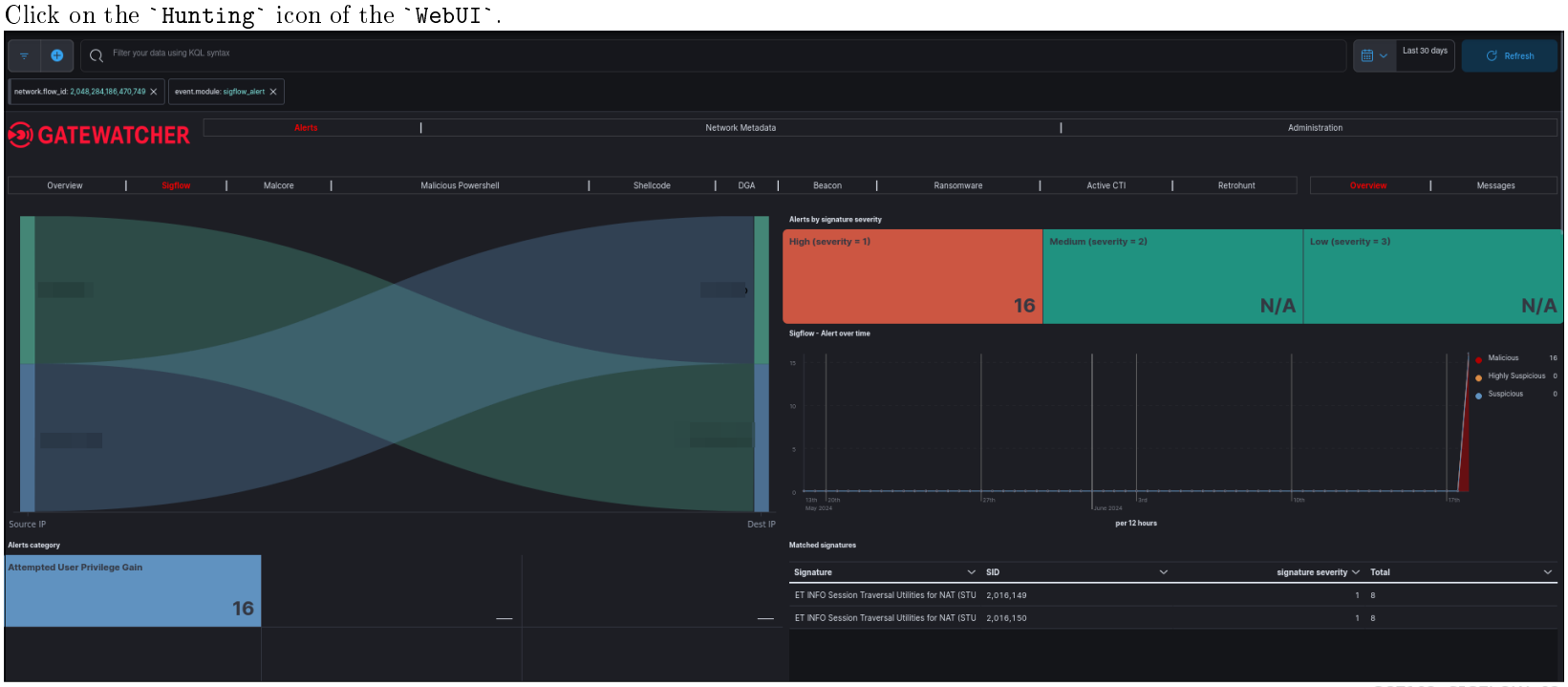
The alert counters are visible:
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.5.3.3 Events of type "meta-data"

Events of type "metadata" are generated when the Sigflow engine has recognized the network flow **protocols**.
These metadata events are visible in the Kibana interface.

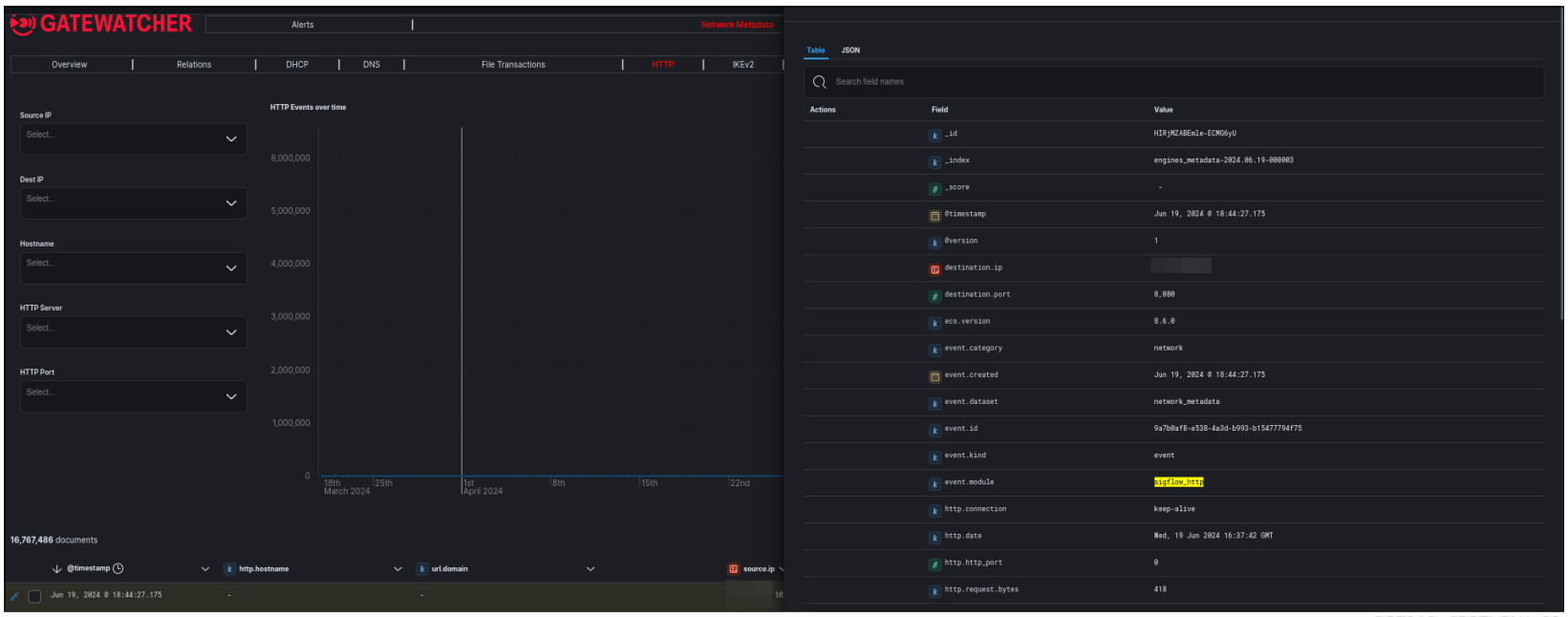
- Click on the `Hunting` icon of the `WebUI`.



GCE103_SIGFLOW_03

The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

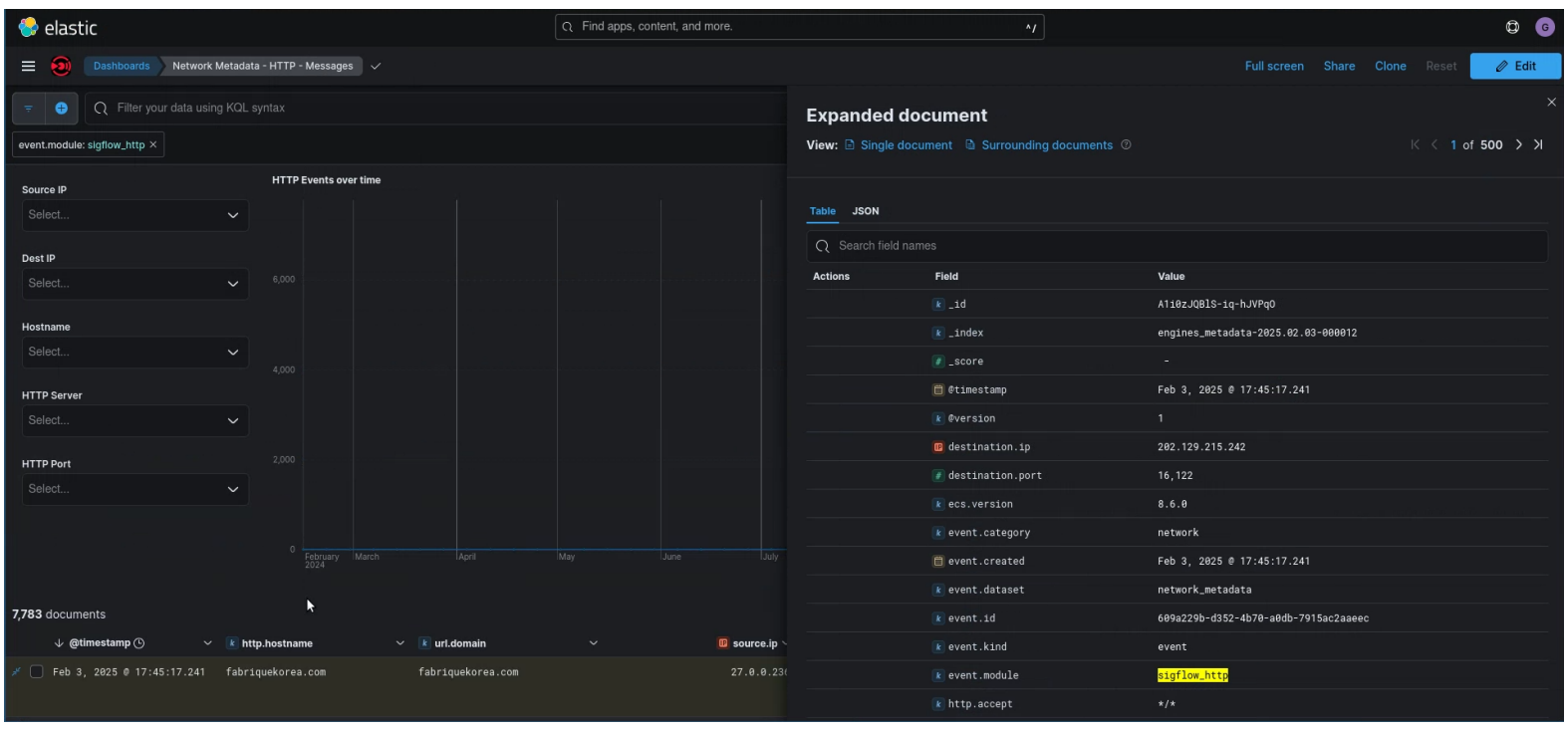
- Click on the `Network Metadata` section then the protocol category (HTTP for example).
- Click on the `Messages` tab.
  This page displays all events of metadata type (metadata) corresponding to the detected protocol in this network flow.
- Select the arrow to the left of the event.



GCE103_SIGFLOW_09

The detailed information of this event can be viewed in table or json format.

2.1.5.3.3.1 Example of the events of type "meta-data"



The counters are given in the *Example of an alert exported*.

2.1.5.3.3.2 Data structure of the events of type "meta-data"

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields"

This information is displayed in the `Expanded document` screen of Kibana.

2.1.5.3.3.3 The header part of the events of type "meta-data"

The header section contains:

```
"_index": "engines_metadata-2025.02.03-000012",
"_id": "A1i0zJQBlS-iq-hJVPqO",
"_version": 1,
"_score": 0,
```

The detailed information is given in the table (*Counters of the header part of logs*).

2.1.5.3.3.4 The source part of the events of type "meta-data"

The source part defined by "_source" contains:

Note:

All data can be exported to a SIEM via syslog (an example of an event of type "meta-data" is shown).
The detailed information is given in the table (*Counters of the header part of logs*).

The example given here is a Kibana example.

```
 "user_agent": {
  "original": "\"Mozilla/5.2 (Windows NT 6.2; rv:50.2) Gecko/20200103 Firefox/50.2\""
},
"destination": {
  "port": 16122,
  "ip": "x.y.z.a"
},
"source": {
  "port": 62219,
  "ip": "a.b.c.d"
},
"event": {
  "dataset": "network_metadata",
  "module": "sigflow_http",
  "category": [
    "network"
  ],
  "created": "2025-02-03T16:45:17.241433+0000",
  "id": "609a229b-d352-4b70-a0db-7915ac2aaeec",
  "kind": "event"
},
"@version": "1",
"ether": {},
"http": {
  "connection": "Keep-Alive",
  "response": {
    "mime_type": "text/plain",
    "status": 200,
    "bytes": 186503
  },
  "server": "Microsoft-IIS/5.0",
  "date": "Thu, 01 Jun 2017 20:55:46 GMT",
  "version": "HTTP/1.1",
  "request": {
    "mime_type": "text/plain",
    "bytes": 251904,
    "method": "GET"
  },
  "last_modified": "Thu, 01 Jun 2017 20:25:44 GMT",
  "hostname": "fabrique.com",
  "accept": "*/*",
  "accept_encoding": "gzip, deflate",
  "accept_language": "en-US"
},
"url": {
  "domain": "fabrique.com",
  "path": "/7rvmnb"
},
```

(continues on next page)

(continued from previous page)


```
"observer": {
  "product": "gcenter",
  "uuid": "78f4fed1-c9ad-52b9-b509-6b87767f501f",
  "hostname": "gcenter.domain.local",
  "gcap": {
    "ingress": {
      "interface": {
        "name": "monvirt"
      }
    },
    "hostname": "gcap.gatewatcher.fr",
    "version": "2.5.x"
  },
  "version": "2.5.x",
  "vendor": "gatewatcher",
  "log_format_version": "1.0.0"
},
"@timestamp": "2025-02-03T16:45:17.241Z",
"ecs": {
  "version": "8.6.0"
},
"network": {
  "tx_id": 0,
  "protocol": "http",
  "transport": "tcp",
  "community_id": "1:cxHEBTJgZCFfWpryH1AkluiYEGk=",
  "timestamp": "2025-02-03T16:45:17.241433+0000",
  "flow_id": 575568319996003
}
```


2.1.5.3.3.5 List of counters of the events of type "meta-data"

Note:

The alert counters are visible:
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.5.4 Management of the engine

2.1.5.4.1 View the status of Sigflow

The current engine status is displayed in the *`Health checks` screen*.

2.1.5.4.2 Engine update

There are updates (Updates) for the Sigflow engine.
These updates can be done manually or scheduled via Threat-DB update module.
See *Dedicated modules for managing updates: Threat DB update and Software update* and in particular the part *Update presentation*.

2.1.5.4.3 Rules update

The rule sources are defined in the GCaps profiles via the rulesets.
These sources have to be manually or automatically updated according to the configuration.
For further information, refer to *Organizing the rules*.
To manage the rules, see the *Managing the Sigflow engine rule sources*.
To update the rules, see the *Updating rules sources*.

2.1.5.4.4 Sigflow configuration

The engine is configured by profiles.
For more information, see the *GCAP Profiles* paragraph.
For implementation, see the *Configuring GCaps using the `GCaps Profiles`*.

2.1.5.5 Alert Analysis

The alerts are displayed on a specific screen described in the *WebUI `Alerts` screen*.
The general procedure for analyzing alerts is described in the *Using of NDR dashboards*.
The specific procedure for analyzing Sigflow alerts is described in the file *Analyzing the Sigflow alerts*.

2.1.6 DGA detect engine

2.1.6.1 Introduction

2.1.6.1.1 For what types of threats is this engine designed?

The **GCenter** embeds an engine capable of detecting the technique of Domain Generating Algorithm, often used by advanced threat actors in their malware.
DGA detect engine:

- Works on DNS (plaintext protocol) and will work even if the malware later uses ciphered protocol like HTTPS.
- Can detect DGA that have never be seen before. For instance, it could have detected solarwind even if it was trained before solarwind existed.

The presence of DGA-generated domain names on a network is a strong indicator of being compromised.
Indeed, malware can use HTTP requests to automatically generated domain names to contact their command and control servers. They are also called CnC, C&C, or C2.

2.1.6.1.2 How does this particular engine detect threats?

Domain names generated by DGAs have different properties than legitimate domain names.
Conventional detection approaches such as blacklists are not relevant in the case of constantly renewed domains.
Simple entropy calculations generate a large amount of false positives.

The detection of suspicious domain is based on a pre-trained, supervised *Machine Learning* model.
The detection of behavior "DGA" is based on domain analysis AND behavioral analysis
DGA detect combines multiple hybrid approaches to get the best of each techniques:

- A supervised machine learning algorithm to detect likely-DGA domains. The model is based on multiple models, one using deep learning (LSTM) and one using domain-specific features.
- A behavior analysis based on aggregation over time

2.1.6.1.3 How does this DGA detect engine work in the GCenter?

- On the GCAP, DNS answers are logged and sent to the GCenter.
- A machine learning algorithm detects the domains that look like being produced by a DGA
- A behavior analysis is performed to detect hosts that are associated with an unusual amount of NXDOMAIN DNS answers (=host that produce a lot of queries for domain that don't exist)
- The results from the behavior analysis and from each individual domain are combined to produce an aggregated alert.

What are real-life examples of DGA ?

- Conficker:
  - One of the earliest and most well-known examples of a DGA is from the Conficker worm, which infected millions of computers worldwide.
  - Conficker's DGA generated 250 domains daily, making it difficult for defenders to block the domains fast enough.
- Zeus Gameover: The Zeus Gameover malware also used a DGA to generate domain names, helping it evade detection and take control of infected machines for financial theft.

How DGA works?

Algorithmic Domain Generation: the malware uses a predefined algorithm to generate a list of domain names. The algorithm may take various inputs, such as the current date and time, a seed value, or other dynamic parameters, to produce a unique set of domain names each time it runs.
Attempt to Connect: the malware will attempt to connect to the generated domains in sequence or at random until it successfully communicates with an active C2 server. The C2 server will also know the same algorithm and parameters, so it will register one or more of the generated domains in advance.
Resilience to Blocking: since a DGA can create thousands or even millions of potential domain names, it becomes challenging for cybersecurity teams to block all possible domains in advance. Even if some domains are detected and blacklisted, the DGA can quickly switch to new domains, maintaining the malware's ability to communicate with its operators.

Why an attacker would use DGA?

Evading Detection: Traditional security systems that rely on blocking specific domains or IP addresses find it difficult to keep up with the rapid generation and use of new domains.
Resilience and Redundancy: If one domain is shut down or blocked, the malware can simply use another domain generated by the algorithm.
Flexibility: Allows cybercriminals to move their C2 infrastructure quickly and easily, which makes it harder for law enforcement or security teams to disrupt their operations.

What are the different types of DGA?

Time-based DGAs: These use the current date or time as a seed to generate domains.
For example: a1b2c3d4.com, e5f6g7h8.net, ijklmnop.org, qrs8tuv9.biz, wxyz1234.inf.

Wordlist-based DGAs: These use a predefined list of words to create domain names, combining them in different ways.
For example: blueelephantapple.com, silverfoxbanana.net, quickmonkeytree.org, redcherrybunny.biz, happykoalaplanet.info

Hash-based DGAs: These use cryptographic functions like hashing to generate domains, making the domains appear more random.
For example: 4d2ffg71f65d.com, a9c4d3b6f12e.net, 7f8a9bcd0342.org, 0f9b8a7cd45e.biz, d5c6b7a8e9f0.info

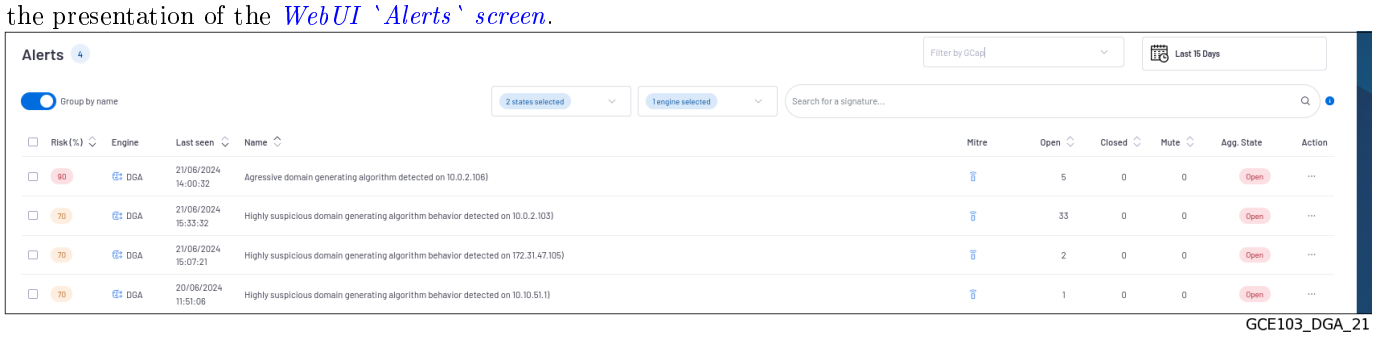
Machine Learning-based DGAs: Newer types of DGAs may use machine learning models to create domains that are hard to distinguish from legitimate domains.
For example: secureloginservice.com, mailverifytool.net, updateauthenticator.org, dataexchangeserver.biz, clientaccessmanager.info

A list of exceptions can be set up to force the engine to declare domain names as healthy (Ignore list).
It removes alerts related to recurring false positives.

2.1.6.2 Events generated

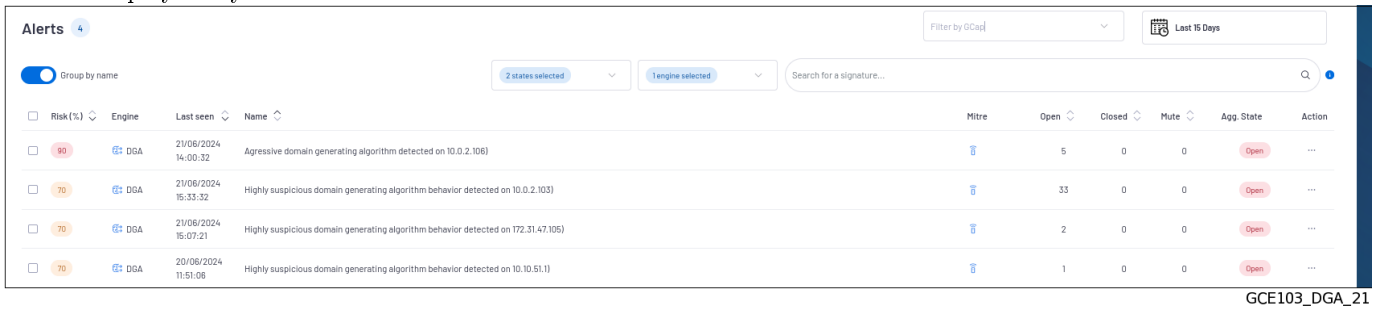
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen.
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
  - To view the alerts, select the `DGA` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.



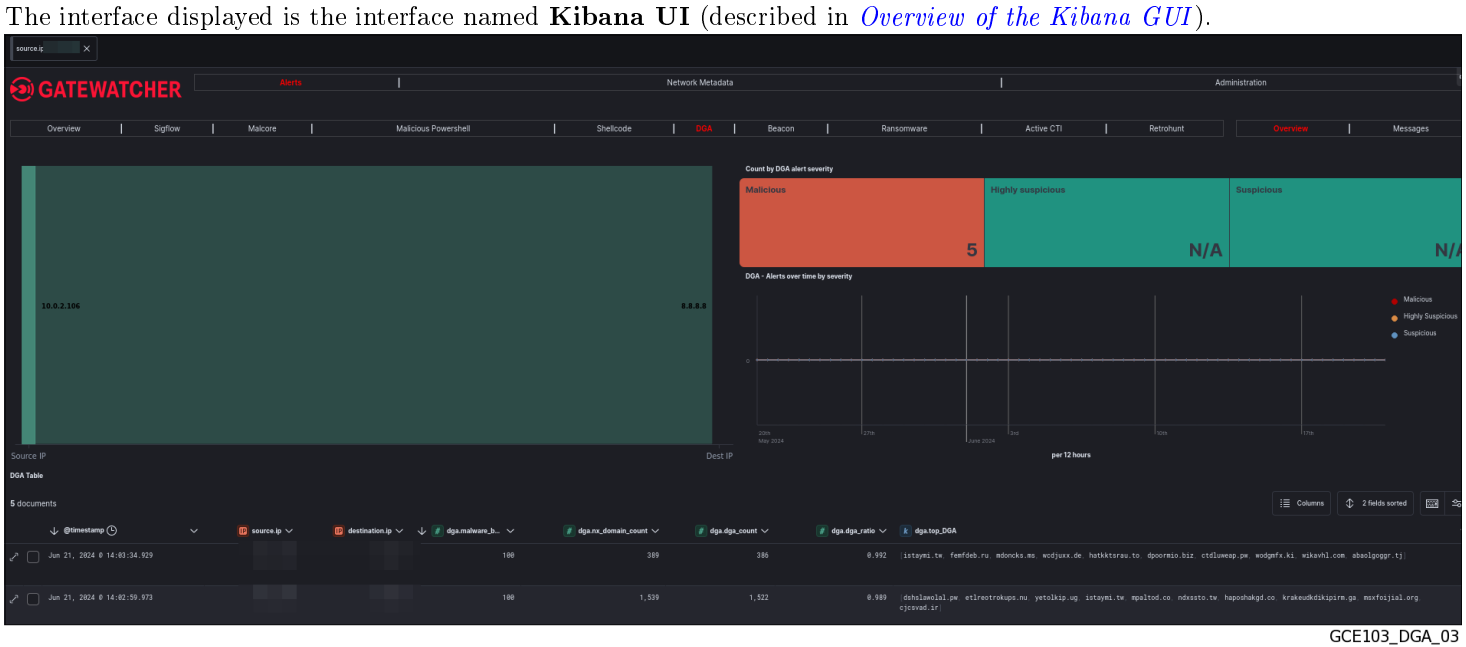
GCE103_DGA_21

  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed in *Example of a DGA detect alert in the WebUI*.
- In the interface named **Kibana UI**
  - To view the alerts, select the `DGA` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.
    The screen displays only the list of DGA alerts.



GCE103_DGA_21

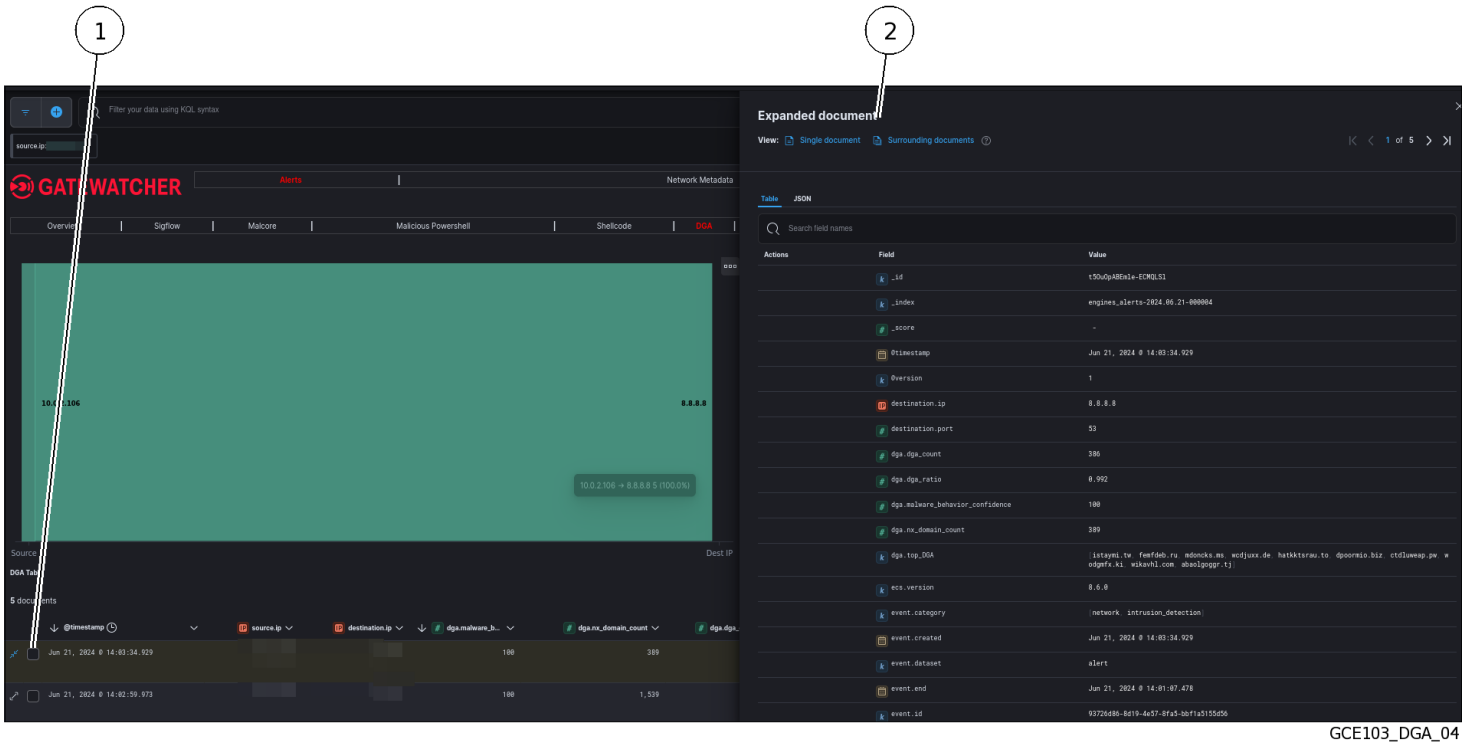
  - After selecting the alert, click on the `Open DGA activity` command of the `Actions` menu.
    Kibana interface is opened in the `Overview` tab, the `DGA` category of the `Alerts ` section.
    The database is filtered on the `source.ip:` parameter which sends the DGA request.
    The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).



GCE103_DGA_03

This page displays all alerts from this IP address detected by DGA.

- Click on the toggle icon (1) on the left of the alert.
  The `Expanded document` window (2) is displayed.



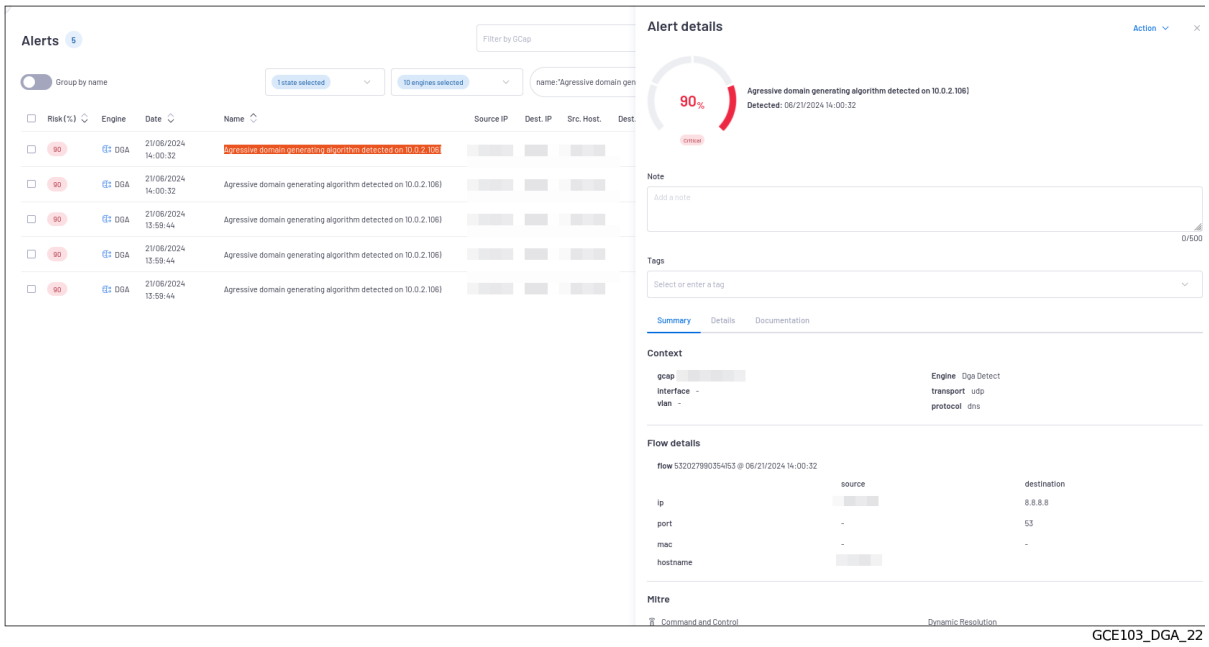
GCE103_DGA_04

The detailed information of this alert can be viewed in table or json format (see the *DGA detect log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

Note:

If a GCap oversees several networks or if several GCaps supervise several networks, it is possible that a domain name that appears several times will generate only one alert.

2.1.6.2.1 Example of a DGA detect alert in the WebUI



GCE103_DGA_22

The presentation of the `Alert details` window is given in the *`Alert details` window*.
The displayed counters are given in the *Engine log data structure* appendix.

2.1.6.2.2 DGA detect log data structure

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields"

This information is displayed in the `Expanded document` screen of Kibana.

2.1.6.2.2.1 The header part of the DGA detect logs

The header section contains:


```
"_index": "engines_alerts-2024.12.17-000043",
"_id": "-a9H1JMBe7GX5B2fgaSz",
"_version": 1,
"_score": 0,
```


The detailed information is given in the table (*Counters of the header part of logs*).

2.1.6.2.2.2 The source part of the DGA detect logs

The source part is defined by "_source" in the logs.

Note:

The data displayed on the WebUI (alerts details window) is a part of the data displayed on the `Extended document` screen on the Kibana interface.
All data can be exported to a SIEM via syslog (an example of an exported alert is shown).
The detailed information is given in the table (*Counters of the header part of logs*).

The example given here is a Kibana example.


```
"event": {
  "created": "2024-12-17T11:01:15.955324+00:00",
  "dataset": "alert",
  "end": "2024-12-17T11:00:05.717000+00:00",
  "module": "dga_detect",
  "severity": 1,
  "kind": "alert",
  "category": [
    "network",
    "intrusion_detection"
  ],
  "start": "2024-12-17T10:59:59.513000+00:00",
  "id": "113dfa89-3b96-4e93-af67-e11df6446ff0"
},
"dga": {
  "malware_behavior_confidence": 50,
  "nx_domain_count": 29,
  "dga_ratio": 1,
  "top_DGA": [
    "tjzjyiheo.com",
    "nvtcvimt.com",
    "vmfyaxnse.com",
    "htjykhvta.com",
    "csmanuivsrlx.com",
    "sbxsgfddr.com",
    "oyttwuyshcgxxaenbit.com",
    "seklusaprnkwhvybzc.com",
    "xxcnirvbqivbucfsbliu.com",
    "jgjvgfetpammdrxwn.com"
  ],
  "dga_count": 29
},
"source": {
  "ip": "192.168.56.104"
```


(continues on next page)

(continued from previous page)


```
  },
  "ecs": {
    "version": "8.6.0"
  },
  "destination": {
    "port": 53,
    "ip": "78.46.218.253"
  },
  "observer": {
    "log_format_version": "1.0.0",
    "hostname": "gcenter.domain.local",
    "vendor": "gatewatcher",
    "gcap": {
      "hostname": "gcap-int-129-dag.gatewatcher.com",
      "version": "2.5.4.0-rc5"
    },
    "product": "gcenter",
    "uuid": "fc1e66e3-a397-5eb4-9277-754be778f317",
    "version": "2.5.3.103"
  },
  "@version": "1",
  "@timestamp": "2024-12-17T11:01:15.955Z",
  "network": {
    "protocol": "dns",
    "transport": "udp",
    "timestamp": "2024-12-17T11:00:05.434623+00:00",
    "flow_id": 2110172624313946
  }
},
```


The DGA detect engine enriches the information already provided by the **Sigflow** module.
Thus, for a domain not detected as a generated domain, the field `dga_probability` will be added.
A value close to 0 indicates a low probability that the domain has been generated.
Conversely, a value close to *1* indicates that there is a good chance that this domain is the result of a random generation.

2.1.6.2.2.3 List of counters of the alert

Note:

The alert counters are visible:
- In the `Alert details` screen of the WebUI
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.6.3 Management of the engine

2.1.6.3.1 Viewing the engine status

The current engine status is displayed in the *`Health checks` screen*.

2.1.6.3.2 Engine update

The engine is updated with each new version of the GCenter.

2.1.6.3.3 Configure the DGA detect engine and manage the list of ignored files

The management interface enables:

- To activate the engine and change its settings
  Configuration implementation is given in *Setting up the DGA detect engine* procedure.
- To manage the `Ignore list` : defines the list to explicitly filter healthy domains or IPs
  For more information on the procedure, see *Managing the Ignore list of the DGA detect engine*.

The management interface is described in *`DGA detect` screen (DGA command)*.

2.1.6.4 Alert Analysis

The alerts are displayed on a specific screen described in the *WebUI `Alerts` screen*.
The general procedure for analyzing alerts is described in *Using of NDR dashboards*.
The specific procedure for analyzing DGA alerts is described in the file *Analyzing the DGA detect alerts*.

2.1.7 Malcore retroanalyzer engine

2.1.7.1 Introduction

2.1.7.1.1 For what types of threats is this engine designed?

Regarding files for which a verdict cannot be determined during a first scan by the Malcore engine, the Malcore retroanalyzer engine makes it possible to resubmit them periodically to antivirus engines.
Thus, the Malcore retroanalyzer engine quickly identifies malware as soon as a signature is available in the case of an analysis of a sample previously flagged as suspicious.

2.1.7.1.2 How does this particular engine detect threats?

The Malcore retroanalyzer engine uses the same detection methods as the *Malcore engine*.
However, this engine focuses on analyzes previously declared as "suspicious" status.
Please refer to the *Malcore engine* documentation for more information about the detection process.

2.1.7.1.3 How does Malcore retroanalyzer work in the GCenter?

When a file, rebuilt by a GCap (according to the *Configuring the file reconstruction rules via the GCap profile*) is submitted to Malcore, this sample is analyzed by a set of antivirus engines composing Malcore.
If one of these engines detects the file as malicious, an alert is generated in the dashboards.

However, in the case of a new strain or a new variant, anti-viral signature may not be available at the time of the analysis, but the expected behaviour of the sample is specific enough to be suspicious about it.
In this case, this sample will be flag as such and a periodic analysis will be scheduled periodically in order to clearly determine if this sample is malicious or not.
This loop will last until either a state has been set for the sample (CLEAN or INFECTED) or the sample has reached the data expiration time.

2.1.7.2 Events generated

Events generated by the Malcore retroanalyzer engine are **alerts** only.
Alerts are displayed in the `Alerts` screen and are displayed as detected by the Malcore engine.

The events generated by the Malcore retroanalyzer and the Malcore engines are the same: see *Events generated*.

2.1.7.2.1 List of counters of the alert

Note:

The alert counters are visible:
- In the `Alert details` screen of the WebUI
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.7.3 Management of the engine

2.1.7.3.1 Viewing the engine status

The Malcore retroanalyzer engine and the Malcore engine use the same anti-viral engines: see the *`Health checks` screen*.

2.1.7.3.2 Engine update

The Malcore retroanalyzer engine and the Malcore engine use the same update system: see the *Engine update* paragraph.

2.1.7.3.3 Configuration of Malcore retroanalyzer engine

The management interface enables to activate the engine: this activation is done in the *`Malcore retroanalyzer` screen*.

2.1.7.4 Alert Analysis

The alerts are displayed on a specific screen described in the *WebUI `Alerts` screen*.
The general procedure for analyzing alerts is described in the *Using of NDR dashboards*.
The specific procedure for analyzing Malcore retroanalyzer alerts is described in the *Analyzing the Malcore retroanalyzer alerts*.

2.1.8 Active CTI engine

2.1.8.1 CTI module overview

The CTI module uses Indicators Of Compromise (IOC) to generate alerts.
The CTI module is composed of:

- A database of Indicators Of Compromise named Gatewatcher CTI
- The Active CTI engine: it generates Sigflow rules on the basis of the database of Indicators Of Compromise in order to raise alerts
- The Retro hunt engine: it searches the Indicators Of Compromise (defined in the database) in metadata (corresponding of the network flow captured by Sigflow)

Note:

An additional license is required to activate this module. It is therefore not automatically activated in the solution.

2.1.8.2 Introduction

2.1.8.2.1 For what types of threats is this engine designed?

The active CTI engine is designed to detect:

- Malicious URLs
- Malicious domain names

2.1.8.2.2 How does this particular engine detect threats?

The Active CTI engine generates specific Sigflow rules based on the compromise indices of the Gatewatcher CTI platform.
These rules configure the Sigflow engine to raise alerts if it finds malicious URLs/ domain names in the network feed it monitors.

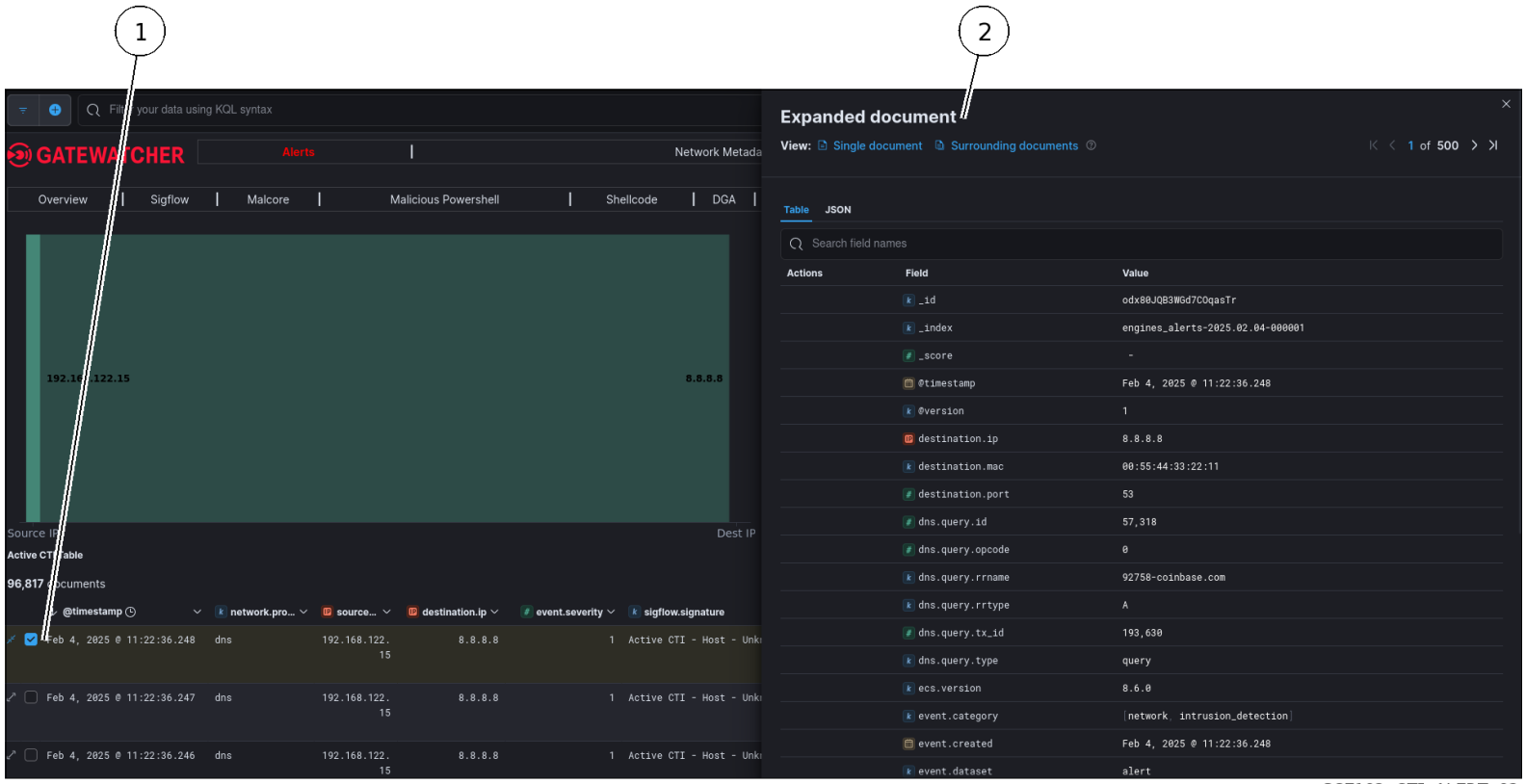
2.1.8.2.3 How does Active CTI work in the GCenter?

The GCenter regularly receives evidence of compromise from the Gatewatcher CTI platform.
Based on this information, the Active CTI engine produces new Sigflow rules daily.
These rules are grouped in a new source named 'Active_CTI' and can therefore be included in a ruleset with other rule sources.
This ruleset is then integrated into the GCap Profile sent to the Sigflow engine to configure it.
These rules allow it to raise alerts when these rules correspond to the flow.
When an alert is raised, it is displayed in the various dashboards: NDR and Kibana.

2.1.8.3 Events generated

Events generated by the engine are **alerts** of the Sigflow type.
They will therefore be available in the ACTIVE CTI dashboards.
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
  - To view the alerts, select the `Active CTI` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.
  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed in *Example of an Active CTI alert in Kibana*.
    The displayed counters are given in the *Engine log data structure* appendix.
- In the interface named **Kibana UI**:
  - In the main interface **WebUI**, click on the `Hunting` icon.
    The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).
  - Click on the `Active CTI` category of the `Alerts` section then the `Overview` or `Messages` tab.
- To consult information about a specific alert:
  - Click on the toggle icon (1) on the left of the Alert.
    The expanded document (2) is displayed.



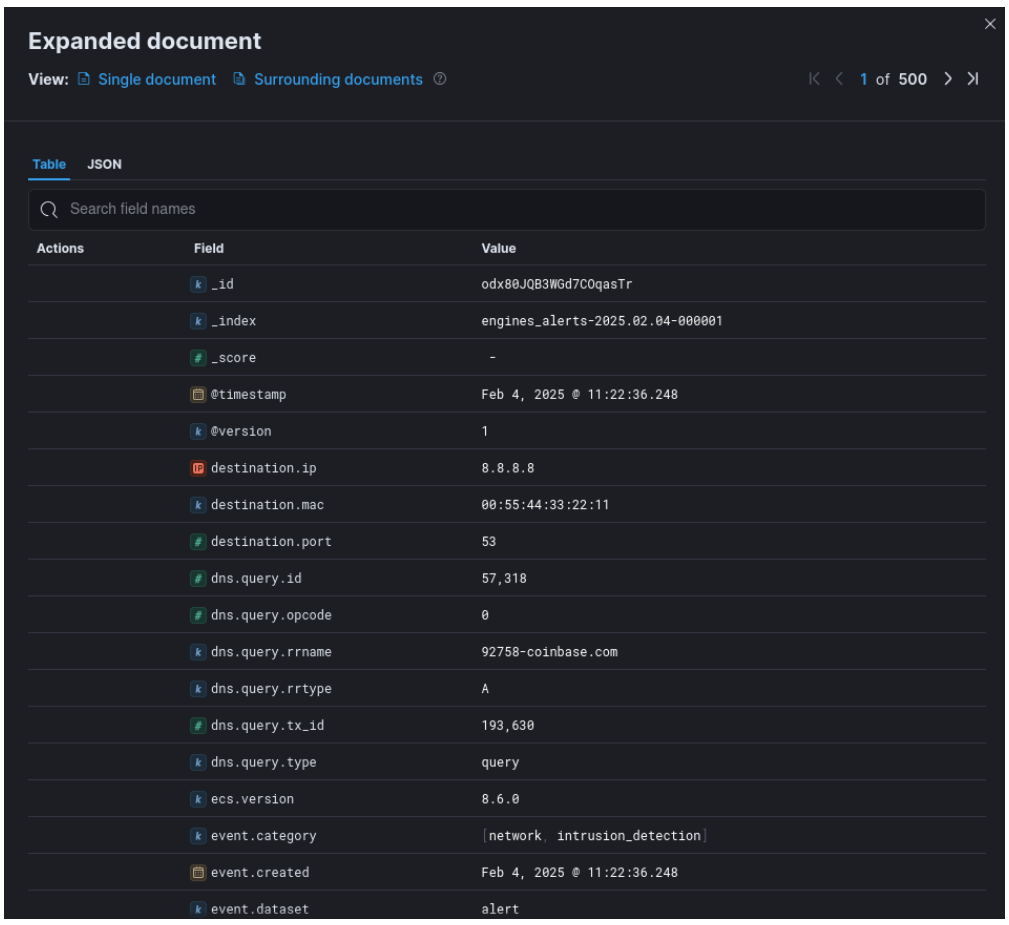
GCE103_CTI_ALERT_02

The detailed information of this alert can be viewed in table or json format (see the *Active CTI logs data structure*).
The displayed counters are given in the *Engine log data structure* appendix.
Active CTI alerts are alerts that can be filtered by searching for the term *event.module: active_ cti* in the Kibana search bar.

Note:

The **Kibana UI** can also be accessed without any filters via the `Hunting` icon on the left side menu bar in the WebUI.

2.1.8.3.1 Example of an Active CTI alert in Kibana



The presentation of the `Alert details` window is given in the *`Alert details` window*.
The counters are given in the *Engine log data structure* appendix.

2.1.8.3.2 Active CTI logs data structure

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields

This information is displayed in the `Expanded document` screen of Kibana.

2.1.8.3.2.1 The header part of Active CTI logs

The header section contains:

```
"_index": "engines_alerts-2025.02.04-000001",
"_id": "odx80JQB3WGd7COqasTr",
"_version": 1,
"_score": 0,
```

The detailed information is given in the table (*Counters of the header part of logs*).

2.1.8.3.2.2 The source part of Active CTI logs

The source part is defined by "_source" in the logs.

Note:

The data displayed on the WebUI (alerts details window) is a part of the data displayed on the `Extended document` screen on the Kibana interface.
All data can be exported to a SIEM via syslog (an example of an exported alert is shown).
The detailed information is given in the table (*Counters of the header part of logs*).

The example given here is a Kibana example.

```
"@version": "1",
"source": {
  "ip": "x.y.z.a",
  "port": 53,
  "mac": "00:11:22:33:44:55"
},
"network": {
  "protocol": "dns",
  "tx_id": 193630,
  "flow_id": 2201432362562192,
  "transport": "udp",
  "timestamp": "2025-02-04T10:22:36.248783+0000"
},
"destination": {
  "ip": "8.8.8.8",
  "port": 53,
  "mac": "00:55:44:33:22:11"
},
"@timestamp": "2025-02-04T10:22:36.248Z",
"event": {
  "dataset": "alert",
  "created": "2025-02-04T10:22:36.248783+0000",
  "kind": "alert",
  "severity": 1,
  "module": "active_cti",
  "category": [
    "network",
    "intrusion_detection"
  ],
  "id": "d79bff72-01b6-4639-979c-efcb5e6faf23"
```

(continues on next page)

(continued from previous page)


```
},
"sigflow": {
  "payload": "3+YBAAABAAAAAAAADjkyNzU4LWNvaW5iYXNlA2NvbQAAAQAB",
  "signature_id": 1300000773,
  "metadata": {
    "risk": [
      "highly suspicious"
    ],
    "signature_severity": [
      "2"
    ],
    "ioc": [
      "fffc7e75-cb75-4210-a244-669cba3cae06"
    ],
    "updated_at:": [
      "2025_02_04"
    ],
    "created_at:": [
      "2025_02_04"
    ]
  },
  "gid": 1,
  "action": "allowed",
  "rev": 0,
  "stream": 0,
  "payload_printable": ".............92758-coinbase.com.....",
  "signature": "Active CTI - Host - Unknown/Unknown - Unknown family - Unknown threat actor - fffc7e75-cb75-4210-a244-
↪669cba3cae06",
  "category": "Active CTI"
},
"flow": {
  "bytes_toclient": 10843280,
  "pkts_toclient": 96815,
  "bytes_toserver": 7551648,
  "pkts_toserver": 96816,
  "start": "2025-02-04T10:20:39.242320+0000"
},
"ecs": {
  "version": "8.6.0"
},
"dns": {
  "query": [
    {
      "rrname": "92758-coinbase.com",
      "rrtype": "A",
      "tx_id": 193630,
      "opcode": 0,
      "type": "query",
      "id": 57318
    }
  ]
},
"observer": {
  "product": "gcenter",
  "vendor": "gatewatcher",
  "gcap": {
    "hostname": "gcap.gatewatcher.fr",
    "ingress": {
      "interface": {
        "name": "monvirt"
      }
    },
    "version": "2.5.x"
  },
  "hostname": "gcenter.gatewatcher.fr",
  "uuid": "72cbafc7-96d2-203a730252a8",
  "version": "2.5.x",
  "log_format_version": "1.0.0"
```

2.1.8.3.2.3 List of counters of the alert

Note:

The alert counters are visible:
- In the `Alert details` screen of the WebUI
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.8.4 Management of the engine

2.1.8.4.1 Viewing the engine status

The current engine status is displayed in the *`Health checks` screen*.

2.1.8.4.2 CTI update

2.1.8.4.2.1 The database of indicators of compromise

If a malicious file was not detected as such by Malcore during its analysis, because it was too recent for the Malcore antivirus database for example, then if one of the indices matches the hash of the file in question in the metadata, an alert will be raised.

Note:

The correlation of indices and metadata will depend on the data retention time configured on the GCenter.

Match analysis between indices and metadata is triggered when updating the index database.
It is therefore only possible to trigger the match analysis manually by updating the database of indicators of compromise manually.
This database of indicators of compromise is included in the CTI.gwp file.
There are three different ways to update this database:

- Manual update with cti.gwp package
- *Online* update: the download is performed periodically based on the package posted by Gatewatcher
- *Local* update: the download is performed periodically based on the package in the local repository.

The update frequency depends on the threat db update parameters.
See the section *Dedicated modules for managing updates: Threat DB update and Software update* and in particular *Update presentation*.

Note:

In order to optimize the implementation of the update of the database in *Local* mode, it is necessary that the local repository retrieves the package cti.gwp every hour.
Otherwise the update as well as the match search will only be performed according to the recovery frequency of the package on the local deposit.

2.1.8.4.2.2 The Active CTI engine update

The engine is updated with each new version of the GCenter.

2.1.8.4.3 Active CTI engine configuration

The configuration interface is used:

- To active the Active CTI engine
- To modify the engine parameters

The management interface is described in the *`Active CTI` screen*.
The procedure is described in the *Setting up the Active CTI engine*.

2.1.8.5 Alert Analysis

The alerts are displayed on a specific screen described in the *WebUI `Alerts` screen*.
The general procedure for analyzing alerts is described in *Using of NDR dashboards*.
The specific procedure for analyzing Active CTI alerts is described in the *Analyzing the Active CTI alerts*.

2.1.9 Retro hunt engine

2.1.9.1 CTI module overview

The CTI module uses Indicators Of Compromise (IOC) to generate alerts.
The CTI module is composed of:

- A database of Indicators Of Compromise named Gatewatcher CTI
- The Active CTI engine: it generates Sigflow rules on the basis of the database of Indicators Of Compromise in order to raise alerts
- The Retro hunt engine: it searches the Indicators Of Compromise (defined in the database) in metadata (corresponding of the network flow captured by Sigflow)

Note:

An additional license is required to activate this module. It is therefore not automatically activated in the solution.

2.1.9.2 Introduction

2.1.9.2.1 For what types of threats is this engine designed?

The Retro hunt engine searches the Indicators Of Compromise in metadata to generate alerts.
It can be the hash of a file, a file name, a URL or a domain.

2.1.9.2.2 How does this particular engine detect threats?

Upon receipt of IOCs from the Gatewatcher CTI site, the Retro hunt engine searches for these IOCs in the Elastic database metadata.
The Retro hunt engine raises alerts if it finds concordance between IOC and metadata.

2.1.9.2.3 How does Retro hunt work in the GCenter?

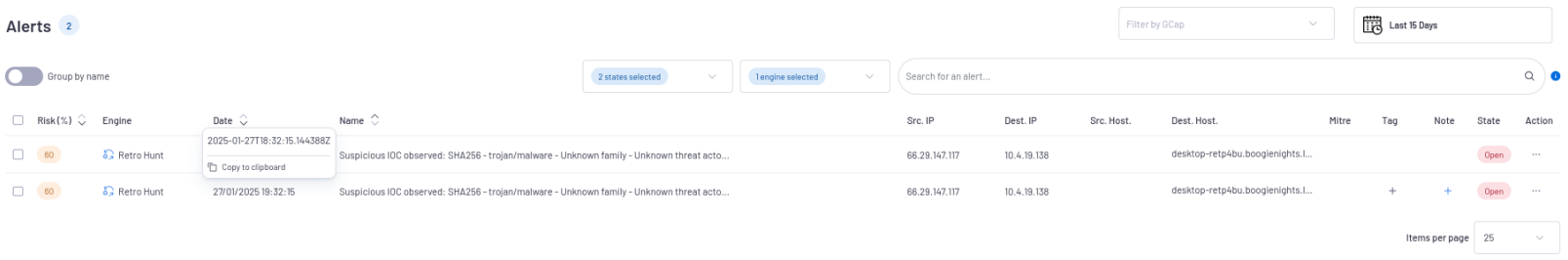
The GCenter regularly receives Indicators Of Compromise from the Gatewatcher CTI platform.
In parallel, the Sigflow engine analyzes the network flow.
Sigflow reconstructs the files and stores them for further analysis by other engines.
Sigflow generates the metadata of the reconstituted files and is kept in Elastic/Kibana during the metadata retention period.
The Retro hunt engine searches for concordances between Indicators Of Compromise and the metadata present.
If this is the case, an alert is raised in the various NDR and Kibana alert display dashboards.
The idea is that if a malicious file was not detected as such by Malcore during its analysis (too recent for the Malcore anti-viral database for example), then if one of the clues corresponds to the hash of the file in question in the metadata, an alert will be raised.
It can be:

- Hash of a file
- Name of a file
- An IP
- A domain
- A URL

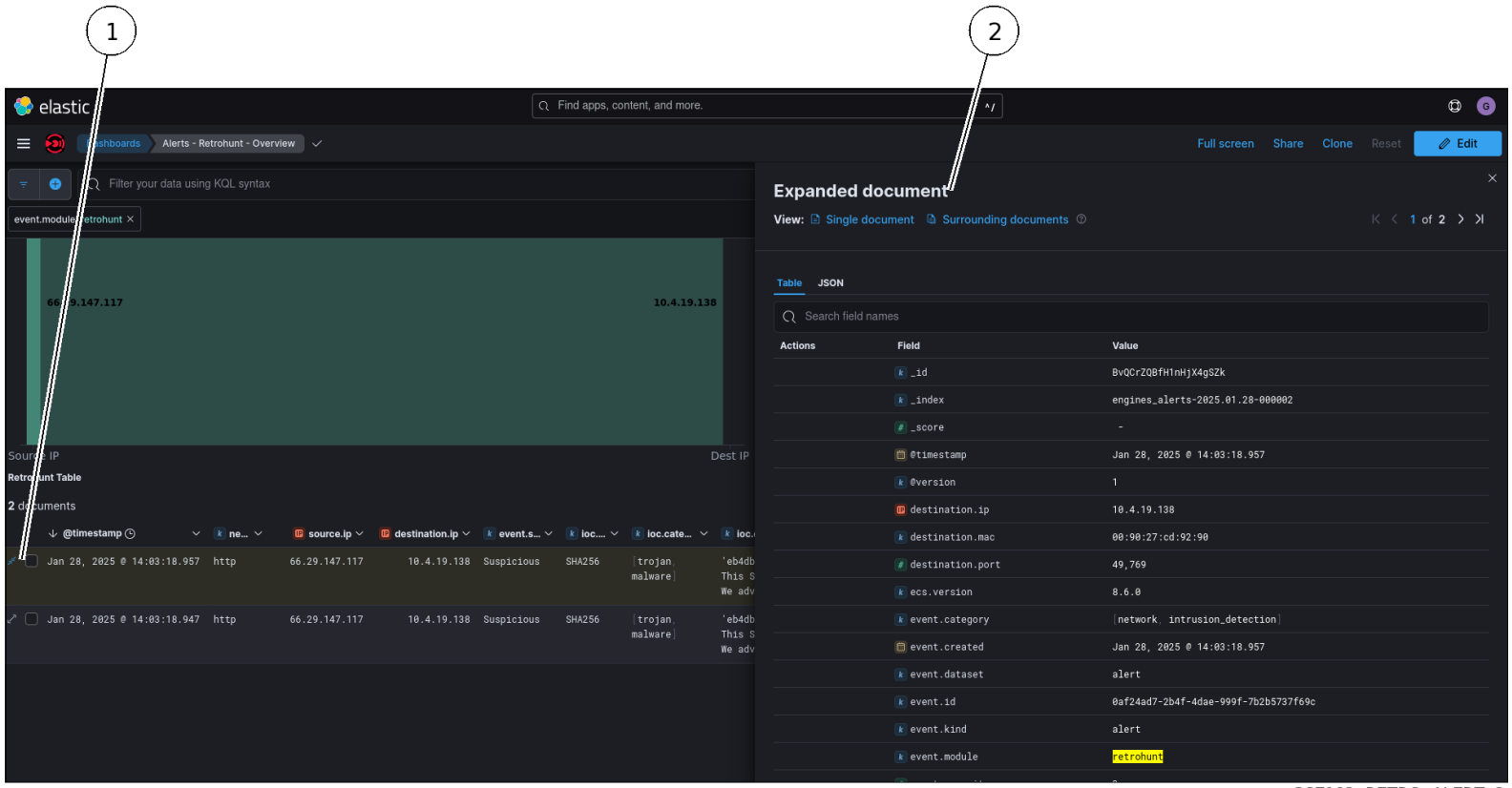
2.1.9.3 Events generated

Events generated by the Retrohunt engine are **alerts**.
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen:
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
- To view only these alerts, select the `Retrohunt` engine filter.
  See the presentation of the *WebUI `Alerts` screen*.



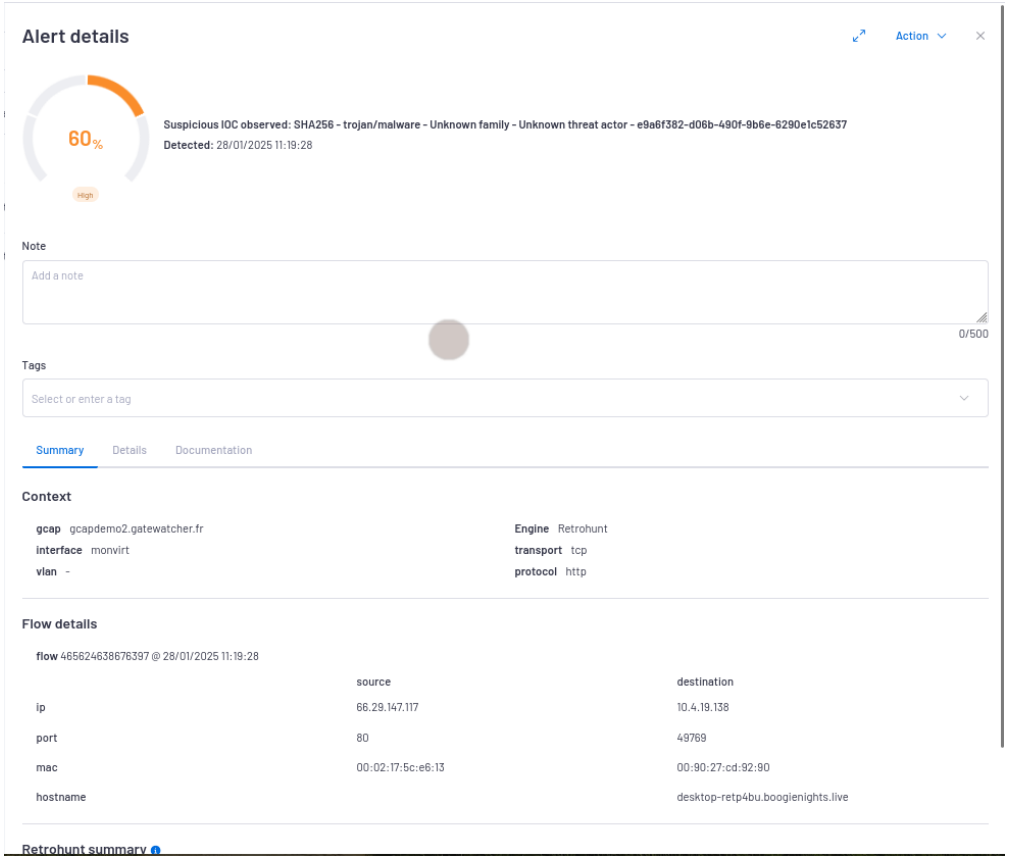
- Click on the selected alert.
  The `Alert details` window is displayed
  The detailed information of this alert is displayed in *Example of a Retro hunt alert in the WebUI*.
- In the interface named **Kibana UI**:
  - Click on the `Hunting` icon on the left side menu bar in the WebUI.
    The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).
  - Select the `Retro hunt` category of the `Alerts` section in Kibana then the `Overview` or the `Messages` tab.
  - Click on the `Messages` tab.
- To consult information about a specific alert:
  - Click on the toggle icon (1) on the left of the Alert.
    The expanded document (2) is displayed.



GCE103_RETRO_ALERT_2

The detailed information of this alert can be viewed in table or json format (see the *Retro hunt logs data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

2.1.9.3.1 Example of a Retro hunt alert in the WebUI



The presentation of the `Alert details` window is given in the *`Alert details` window*.
The counters are given in the *Retro hunt logs data structure*.

2.1.9.3.2 Retro hunt logs data structure

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields"

This information is displayed in the `Expanded document` screen of Kibana.

2.1.9.3.2.1 The header part of Retro hunt logs

The header section contains:

```
"_index": "engines_alerts",
"_id": "-",
"_version": 1,
"_score": 0,
```

The detailed information is given in the table (*Counters of the header part of logs*).

2.1.9.3.2.2 The source part of Retro hunt logs

The source part is defined by "_source" in the logs.

Note:

The data displayed on the WebUI (alerts details window) is a part of the data displayed on the `Extended document` screen on the Kibana interface.
All data can be exported to a SIEM via syslog (an example of an exported alert is shown).
The detailed information is given in the table (*Counters of the header part of logs*).

The example given here is a Kibana example.

The source part defined by "_source" contains:

```
"event": {
     "kind": "alert",
     "module": "retrohunt",
     "dataset": "alert",
     "created": "2025-01-28T13:03:18.957749+00:00",
     "category": [
       "network",
       "intrusion_detection"
     ],
     "severity_human": "Suspicious",
     "id": "0af24ad7-2b4f-4dae-999f-7b2b5737f69c",
     "severity": 3
   },
   "network": {
     "transport": "tcp",
     "protocol": "http",
     "timestamp": "2025-01-28T10:19:28.070435+00:00",
     "flow_id": 465624638676397
   },
   "source": {
       "port": 80,
       "ip": "x.y.z.A",
       "mac": "02:04:c8:5c:e6:13"
   },
   "matched_event": {
     "content": {
       "event": {
         "kind": "event",
         "module": "sigflow_file",
         "dataset": "network_metadata",
         "created": "2025-01-28T10:19:28.070435+0000",
         "category": [
```

(continues on next page)

(continued from previous page)


```
        "network",
        "file"
      ],
      "id": "e997dbcb-5432-4f53-af03-447a6ea7debc"
    },
    "network": {
      "transport": "tcp",
      "protocol": "http",
      "timestamp": "2025-01-28T10:19:28.070435+0000",
      "flow_id": 465624638676397
    },
    "source": {
      "port": 80,
      "ip": "x.y.z.A",
      "mac": "02:04:c8:5c:e6:13"
    },
    "user_agent": {
      "original": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0␣
↪Safari/537.36 Edg/112.0.1722.48"
    },
    "file": {
      "magic": "Zip archive data, at least v2.0 to extract",
      "file_id": 43,
      "sid": [
        1100083
      ],
      "name": "643d0491bcea1.zip",
      "tx_id": 0,
      "state": "CLOSED",
      "stored": true,
      "gaps": false,
      "hash": {
        "md5": "b054104df97949cbeb3da2290da0cf40",
        "sha256": "eb4db357dc6f2dd8facf132ecaf6916e7219bf0e29990601b1f4babefa4d02f9"
      },
      "size": 5665
    },
    "observer": {
      "log_format_version": "1.0.0",
      "hostname": "gcenter.gatewatcher.fr",
      "version": "2.5.3.103",
      "gcap": {
        "hostname": "gcap.gatewatcher.fr",
        "version": "2.5.4.0-rc9",
        "ingress": {
          "interface": {
            "name": "monvirt"
          }
        }
      },
      "uuid": "27863930-fab5-5abe-ba40-1fbd5481e9a4",
      "product": "gcenter",
      "vendor": "gatewatcher"
    },
    "metadata": {
      "flowbits": [
        "et.http.PK"
      ]
    },
    "destination": {
      "port": 49769,
      "ip": "x.y.z.a",
      "mac": "00:90:27:cd:92:90"
    },
    "ecs": {
      "version": "8.6.0"
    },
    "url": {
      "domain": "cotecsecuritygroup.com",
      "path": "/wicd/643d0491bcea1.zip"
    },
    "http": {
      "response": {
```


(continues on next page)

(continued from previous page)


```
          "status": 200,
          "bytes": 5673,
          "mime_type": "application/zip"
        },
        "hostname": "cotecsecuritygroup.com",
        "version": "HTTP/1.1",
        "request": {
          "method": "GET"
        }
      }
    },
    "id": "e997dbcb-5432-4f53-af03-447a6ea7debc"
  },
  "ioc": {
    "case_id": "aa8d51ed-0883-4b12-8b43-4b285306b0a6",
    "type": "SHA256",
    "threat_actor": [],
    "updated_date": "2025-01-28T08:04:31+00:00",
    "categories": [
      "trojan",
      "malware"
    ],
    "signature": "SHA256 - trojan/malware - Unknown family - Unknown threat actor - e9a6f382-d06b-490f-9b6e-6290e1c52637
↪",
    "creation_date": "2025-01-28T08:02:50+00:00",
    "targeted_platforms": [],
    "external_links": [
      {
        "url": "https://info.gatewatcher.com/fr/speed-meeting-lastinfosec",
        "source_name": "IOCAnalysisCollector"
      }
    ],
    "vulnerabilities": [],
    "relations": [
      "0e3cc27b-7999-48ce-8484-dc12b325a355",
      "5556c4ab-3e5e-4d56-8410-60b29cecbeb6"
    ],
    "targeted_organizations": [],
    "families": [],
    "tags": [
      "trojan.generickd.66527077",
      "troj/drodzp-cf",
      "trojan.generickd.66527077 (b)",
      "trojan/generickd!vemnohoo"
    ],
    "targeted_sectors": [
      "Services - Autres"
    ],
    "description": "'eb4db357dc6f2dd8facf132ecaf6916e7219bf0e29990601b1f4babefa4d02f9' is a Suspicious SHA256.\nThis␣
↪SHA256 is linked to a trojan attack.\nWe advised to use this IoC in detection mode.",
    "ttp": [],
    "usage_mode": "detection",
    "tlp": "green",
    "campaigns": [],
    "targeted_countries": [],
    "meta_data": {
      "descriptions": [],
      "usageMode": "detection",
      "cwe": []
    },
    "value": "eb4db357dc6f2dd8facf132ecaf6916e7219bf0e29990601b1f4babefa4d02f9",
    "kill_chain_phases": [],
    "id": "e9a6f382-d06b-490f-9b6e-6290e1c52637",
    "package_date": "2025-01-28T08:50:04.124404+00:00"
  },
  "observer": {
    "log_format_version": "1.0.0",
    "hostname": "gcenter.gatewatcher.fr",
    "version": "2.5.3.103",
    "gcap": {
      "hostname": "gcap.gatewatcher.fr",
      "version": "2.5.4.0-rc9",
      "ingress": {
```


(continues on next page)

(continued from previous page)


```
        "interface": {
          "name": "monvirt"
        }
      }
    },
    "uuid": "27863930-fab5-5abe-ba40-1fbd5481e9a4",
    "product": "gcenter",
    "vendor": "gatewatcher"
  },
  "destination": {
    "port": 49769,
    "ip": "x.y.z.a",
    "mac": "00:90:27:cd:92:90"
  },
  "@timestamp": "2025-01-28T13:03:18.957Z",
  "ecs": {
    "version": "8.6.0"
  },
  "@version": "1"
```


2.1.9.3.2.3 List of counters of the alert

Note:

The alert counters are visible:
- In the `Alert details` screen of the WebUI
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.9.4 Management of the engine

2.1.9.4.1 Viewing the engine status

The current engine status is displayed in the *`Health checks` screen*.

2.1.9.4.2 CTI update

2.1.9.4.2.1 The basis of compromise indices

See *The database of indicators of compromise*

2.1.9.4.2.2 Engine update

The engine is updated with each new version of the GCenter.

2.1.9.4.3 Engine configuration

The configuration interface enables to active the Retro hunt engine.
The management interface is described in the *`Retro hunt` screen*.
The procedure is described in the *Setting up the retro hunt engine*.

2.1.9.5 Alert Analysis

The alerts are displayed on a specific screen described in the *WebUI `Alerts` screen*.
The general procedure for analyzing alerts is described in the *Using of NDR dashboards*.
The specific procedure for analyzing Retro hunt alerts is described in the *Analyzing the Retrohunt alerts*.

2.1.10 Ransomware detect engine

2.1.10.1 Introduction

2.1.10.1.1 For what types of threats is this engine designed?

The **GCenter** includes an engine capable of detecting *ransomware* executions.
A ransomware is a malware that blocks access to the computer or files by encrypting them and demands ransom payments from the victim to regain access.
Most *ransomware* will not only encrypt files locally on an infected computer but will also try to encrypt all files accessible from network shares.
For this, the *ransomware* uses the SMB protocol (including its most widespread version in business: SMBv2).
In order to be as generic as possible, and to be able to detect new *ransomware*, the model uses only the commands for reading and writing files.

2.1.10.1.2 How does this particular engine detect threats?

The *ransomware* detect engine functions as a semi-supervised anomaly detector (*novelty detection*).
It is therefore necessary to be trained with legitimate data corresponding to the customer's specific traffic (over a certain period of time which depends on the amount of SMB traffic on its network).
The training uses a neural network algorithm called autoencoder.
Once the model is trained and tested on a number of examples of *ransomware* whose network traffic could be captured, an optimal anomaly score threshold is determined.
The model is then ready to be used to make predictions: for each sample tested (each sample corresponds to one end (20 seconds) of a SMB session, containing at least one READ or WRITE event), an anomaly score is determined.
If this score is higher than the threshold defined above, then a unit alert for this sample is recorded.

2.1.10.1.3 How does Ransomware detect work in the GCenter?

The engine:

- Retrieves events sent by the GCap (for further details, see the *Detections / Predictions*)
- Analyzes these events (for further details, see the *How does this particular engine detect threats?*)
- Generates alerts (for further details, see the *Events generated*)

2.1.10.1.3.1 Training and re-training

The first training is triggered **automatically** by the GCenter, as soon as the number of examples (*samples*) needed (of the order of 200000) is reached.
A periodic process check regularly that if a re-training is necessary because the client traffic can be modified enough (for example via a change in network configuration) so that the learning done previously has become obsolete.
If re-training is required, a notification is issued to the user to inform him.
The effective triggering of the re-drive is then triggered **manually**.

Note:

During re-training, the engine continues to detect with previous learning.

2.1.10.1.3.2 Detections / Predictions

The trained model can then be used by the engine to make predictions of *ransomware*.
Detection is done in two steps:

- The first step uses the *machine learning* model to make unit predictions on *samples*
- The second step takes into account the contextual information of the SMB session in order to determine if it corresponds to a *ransomware*
  Indeed, legitimate traffic is likely to occasionally (at least for a part of SMB sessions) have abnormal behaviour, and therefore raise unit alerts at the end of the first step. It is therefore necessary to have a second step to determine whether it is a *ransomware*.

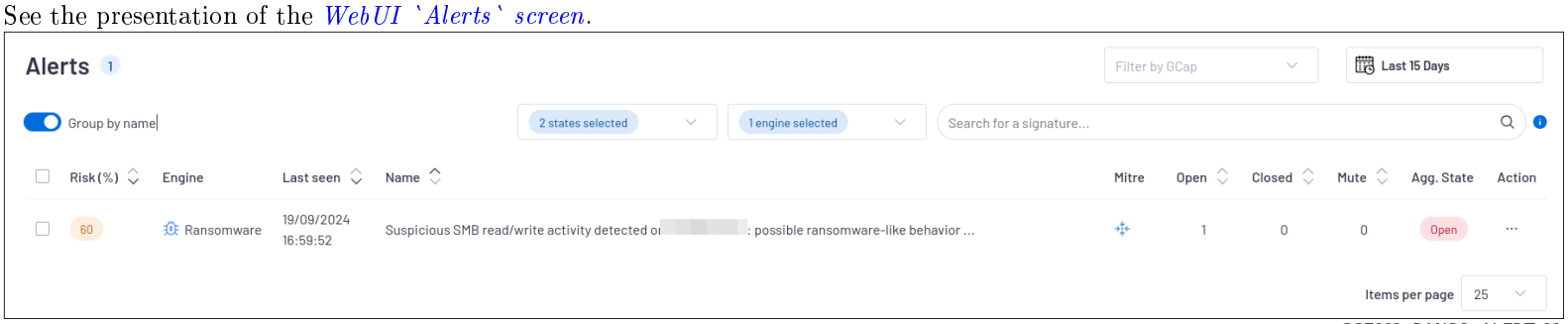
Periodically, the following process is executed:

- Step 1:
  - The engine tracks each SMB session and cut them in small 20-seconds time windows, that we will call "sample"
  - On each sample, features are built on READ and WRITE commands: for instance, READ/WRITE ratio or READ/WRITE sequences : many other features are employed
  - Based on these features, a prediction is made on each sample and produce an abnormality score
  - When multiple samples of the same SMB session are suspicious, and depending on the sensitivity level, an alert is produced
- Step 2: for each SMB session with at least an abnormality score above the defined threshold, the following actions are performed:
  - Analysis of ransomware behaviour shows that the number/share of abnormal samples in their SMB session is much larger than in legitimate traffic.
    Similarly, the observed anomaly scores are also generally much higher.
  - All this information is taken into account to raise or not a **global alert** on the corresponding SMB session.
  - Multiple sensitivity levels (5 levels. 5 corresponding to the highest sensitivity) corresponding to as many severity levels are associated with alerts.
  - In practice, the engine will potentially sequentially raise alerts for increasingly low sensitivities (and therefore significant severity) as the SMB session is analyzed.

2.1.10.2 Events generated

Events generated by the Ransomware engine are **alerts**.
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
  - To view the alerts, select the `Ransomware` filter and view the list of alerts
    See the presentation of the *WebUI `Alerts` screen*.



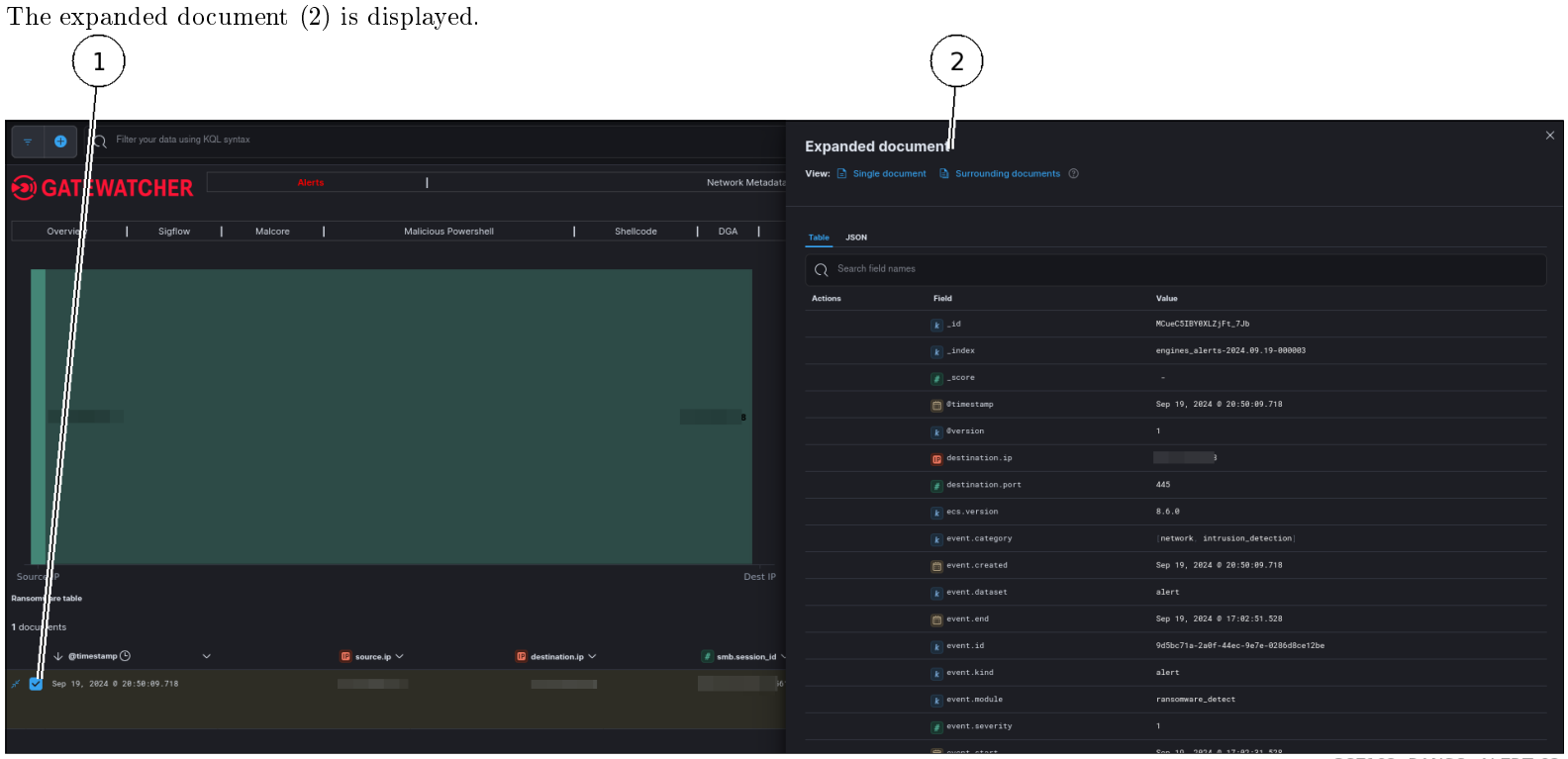
GCE103_RANSO_ALERT-01

  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed in *Example of Ransomware detect alert in the WebUI*.

- In the interface named **Kibana UI**
  - In the main interface **WebUI**, to view the alerts, select the `Ransomware` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.
  - After selecting the alert, click on the `Open host SMB activity` command of the `Actions` menu.
    Kibana is opened on the `Ransomware` category of the `Alerts ` section.
    The interface displayed is the interface named **Kibana UI** (described in the *Overview of the Kibana GUI*).

    In the `Overview` tab, the database is filtered on the `source.ip:` parameter.

  - Click on the toggle icon (1) on the left of the Alert.
    The expanded document (2) is displayed.



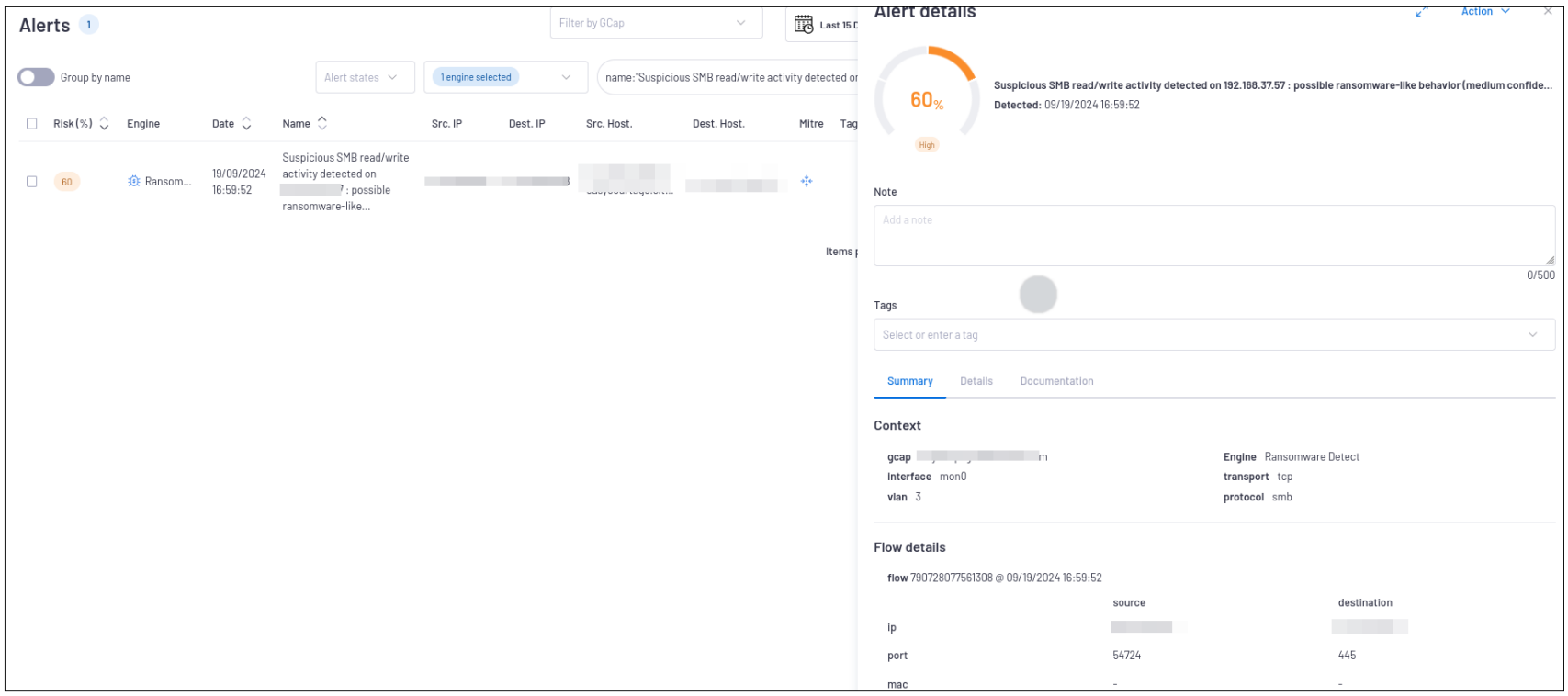
GCE103_RANSO_ALERT-03

The detailed information of this alert can be viewed in table or json format (see the *Ransomware detect log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

Note:

The **Kibana** user interface is also accessible without a filter via the `Hunting` icon in the left menu bar.

2.1.10.2.1 Example of Ransomware detect alert in the WebUI



GCE103_RANSO_ALERT-02

The presentation of the `Alert details` window is given in the *`Alert details` window*.
The counters are given in the *Engine log data structure* appendix.

2.1.10.2.2 Ransomware detect log data structure

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields"

This information is displayed In the `Expanded document` screen of Kibana.

2.1.10.2.2.1 The header part of the Ransomware detect logs

The header section contains:

```
"_index": "engines_alerts-2024.12.17-000002",
"_id": "maMz2pMBPJntoSnXt_aZ",
"_version": 1,
"_score": 0,
```

The detailed information is given in the table (*Counters of the header part of logs*).

2.1.10.2.2.2 The source part of the logs

The source part defined by "_source" contains:

Note:

The data displayed on the WebUI (alerts details window) is a part of the data displayed on the `Extended document` screen on the Kibana interface.
All data can be exported to a SIEM via syslog (an example of an exported alert is shown).
The detailed information is given in the table (*Counters of the header part of logs*).

The example given here is a Kibana example.

```
"source": {
     "ip": "x.x.x.x",
     "port": 50066
   },
   "network": {
     "protocol": "smb",
     "transport": "tcp",
     "timestamp": "2024-12-18T14:34:54.069000+00:00",
     "community_id": "UNDEFINED",
     "flow_id": 2133648979435527
   },
   "@version": "1",
   "observer": {
     "log_format_version": "1.0.0",
     "hostname": "gcenter.gatewatcher.fr",
     "product": "gcenter",
     "uuid": "34b30bd0-ff0f-5fb2-a746-6500d47b45dd",
     "gcap": {
       "hostname": "gcap.gatewatcher.fr",
       "ingress": {
         "interface": {
           "name": "monvirt"
         }
       },
       "version": "2.5.4.0-rc9"
     },
     "version": "2.5.3.103",
```

(continues on next page)

(continued from previous page)


```
    "vendor": "gatewatcher"
  },
  "event": {
    "kind": "alert",
    "created": "2024-12-18T14:37:08.775755+00:00",
    "end": "2024-12-18T14:35:20.642000",
    "dataset": "alert",
    "module": "ransomware_detect",
    "start": "2024-12-18T14:35:00.642000",
    "category": [
      "network",
      "intrusion_detection"
    ],
    "severity": 1,
    "id": "ce827e02-7eb6-4842-8863-b787f52d1104"
  },
  "destination": {
    "ip": "y.y.y.y",
    "port": 445
  },
  "ecs": {
    "version": "8.6.0"
  },
  "@timestamp": "2024-12-18T14:37:08.775Z",
  "smb": {
    "session_id": 593737889611873
  },
  "ransomware": {
    "alert_threshold": 930,
    "session_score": 35,
    "malicious_behavior_confidence": 80
```


2.1.10.2.2.3 List of counters of the alert

Note:

The alert counters are visible:
- In the `Alert details` screen of the WebUI
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.10.3 Management of the engine

2.1.10.3.1 Viewing the engine status

The engine status is displayed in the *`Health checks` screen*.
The engine can be activated if the installed license allows it; see the *`License` screen*.

2.1.10.3.2 Engine update

The engine is updated with each new version of the GCenter.

2.1.10.3.3 Ransomware detect configuration and management of the ignored list feature

The management interface is used:

- To activate the engine or modify its parameters:
  - See the screen description, see *`Ransomware detect` screen (Ransomware command)*.
  - See the *Setting up the Ransomware detect engine* procedure.
- To manage the `Ignore list`, list to explicitly filter healthy destinations (defined by IP):
  - See the screen description, see *`Ransomware detect` screen (Ransomware command)*.
  - See the *Managing the Ignore list of the Beacon detect* procedure.

Note:

Even with metadata limiter enabled, ransomware detect will perform normally.

2.1.10.4 Alert Analysis

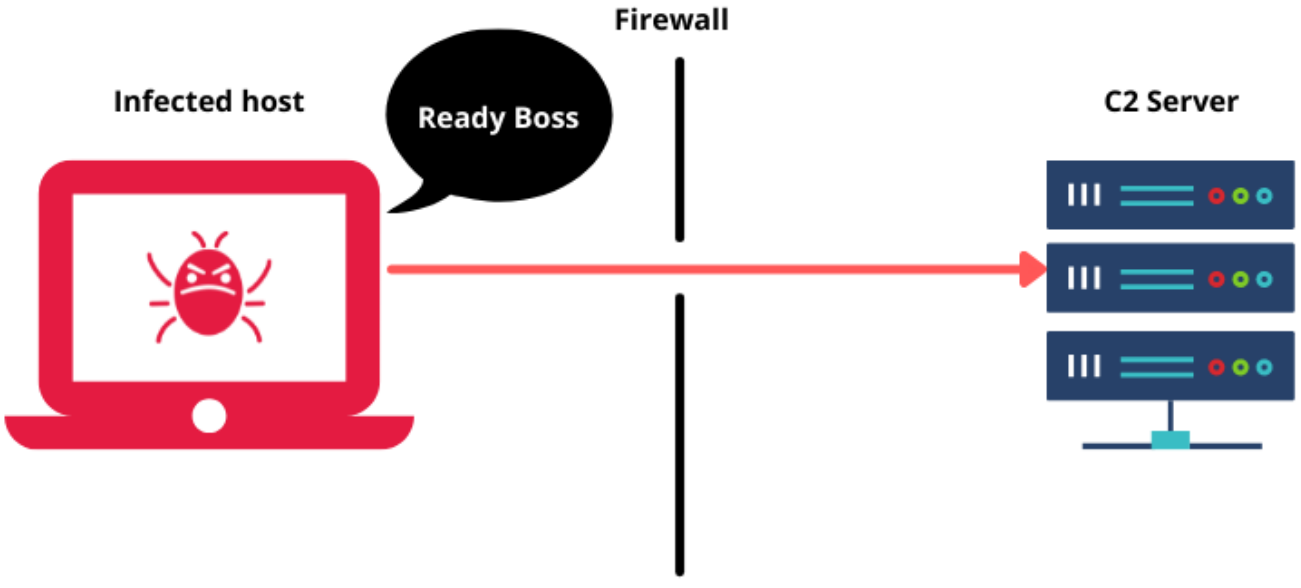
The alerts are displayed on a specific screen described in the *WebUI `Alerts` screen*.
The general procedure for analyzing alerts is described in *Using of NDR dashboards*.
The specific procedure for analyzing Ransomware detect alerts is described in the *Analyzing the Ransomware detect alerts*.

2.1.11 Beacon detect engine

2.1.11.1 Introduction

2.1.11.1.1 For what types of threats is this engine designed?

The Beacon detect engine allows the detection of the communications to a malicious server during a *Command and Control* (C&C) attack.
These communications are established from a **beacon**: malware implanted on the compromised host that makes connections to the C&C server at regular intervals.
The *beacons* are also called *implant* or *agent*.
After running on the compromised host, the beacon will be able to transmit information to the C&C server and receive commands to execute.
Cobalt Strike and Brute Ratel are among the C&C frameworks frequently used for such attacks.
This threat is particularly subtle because it resembles a standard internet stream and is therefore not necessarily blocked by a firewall.



2.1.11.1.2 How does this particular engine detect threats?

The engine detects C&C threats through different HTTP and HTTPS metadata scans:

- Identification of statistical distributions indicating periodicity in metadata
- The presence of anomalies characterizing the execution of commands
- Heuristics to specifically identify certain C&C software

Depending on the configuration used, detection algorithms can withstand the following escape methods:

- Data encryption or over-encryption
- Random time between each communication
- Random data size
- Usurpation of known domain names

Some C&C are specifically identified:

- Cobalt Strike
- BruteRatel
- Caldera
- Powershell Empire
- Sliver

The configuration is done with several options which prevent the analysis of healthy communications.
These options filter in particular:

- Frequently accessed domains within the infrastructure
- Commonly known domains
- Generic special domains used in the internal endpoints (example: .local)

Disabling these options increases detection sensitivity and may require adding domains to the ignore destinations list.

2.1.11.1.3 How does the Beacon detect engine work in the GCenter?

The engine:

- Retrieves events sent by the GCap (for further details see *Beacon detect engine input data*)
- Analyzes these events (for further details see *How does this particular engine detect threats?*)
- Generates alerts (for further details see *Events generated*)

2.1.11.1.3.1 Beacon detect engine input data

HTTP or HTTPS sessions (or events) reconstructed by the GCap are regularly sent to the Beacon detect engine, which then performs statistical analyzes.
Depending on the configuration used, DNS queries reconstructed by the GCap can also be exploited.
For basic engine operation:

- HTTP logging and TLS logging must be enabled in the `Base variables` section of the `Detection strategy/Sigflow engine/Gcaps profiles` menu
  For further details of these functions and their activations, see *`Base variables` Section of the `GCaps profiles` screen*.
- The Metadata rate limiter must be disabled for HTTP and TLS protocols in the `Detection strategy/Sigflow engine/Metadata rate limiter` menu
  For further details of its function and the protocols activations, see *`Metadata rate limiter` screen*.

Important:

Activate the HTTP or TLS protocol disables the detection of the Beacon detect engine for these protocols.

For optimal engine operation:

- DNS logging must be enabled in the `Base variables` section of the `Detection strategy/Sigflow engine/Gcaps profiles` menu
  For further details of these functions and their activations, see the *`Base variables` Section of the `GCaps profiles` screen*.

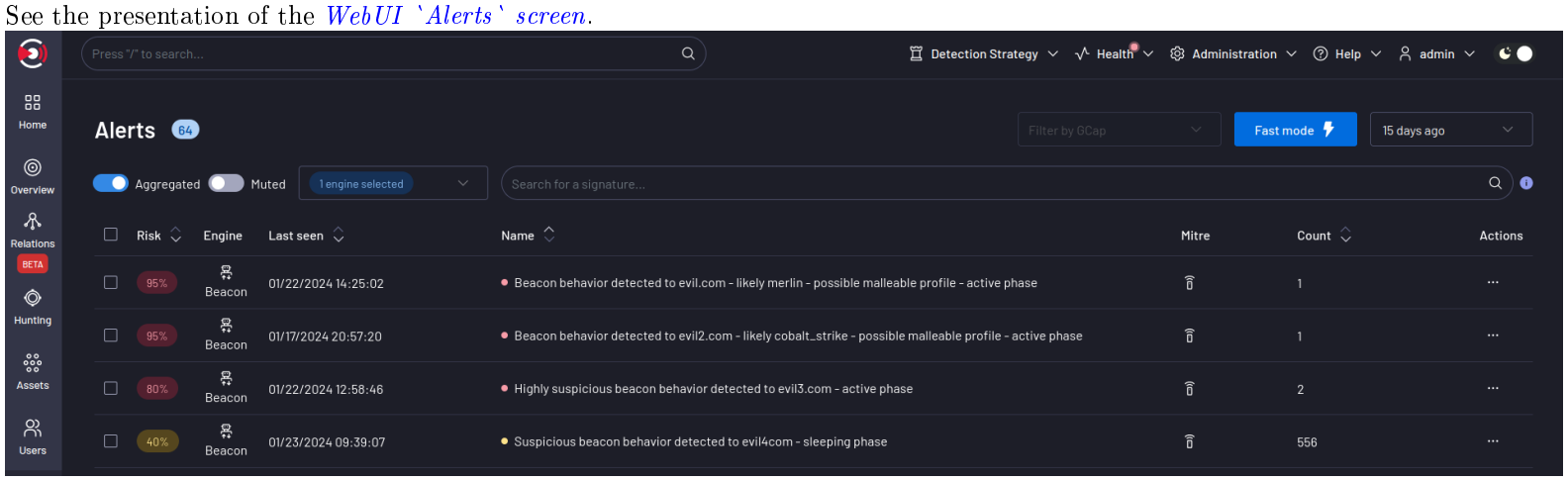
Note:

- To modify the options of the engine: see the *Setting up the beacon detect engine*

2.1.11.2 Events generated

Events generated by the Beacon detect engine are **alerts** only.
These are displayed:

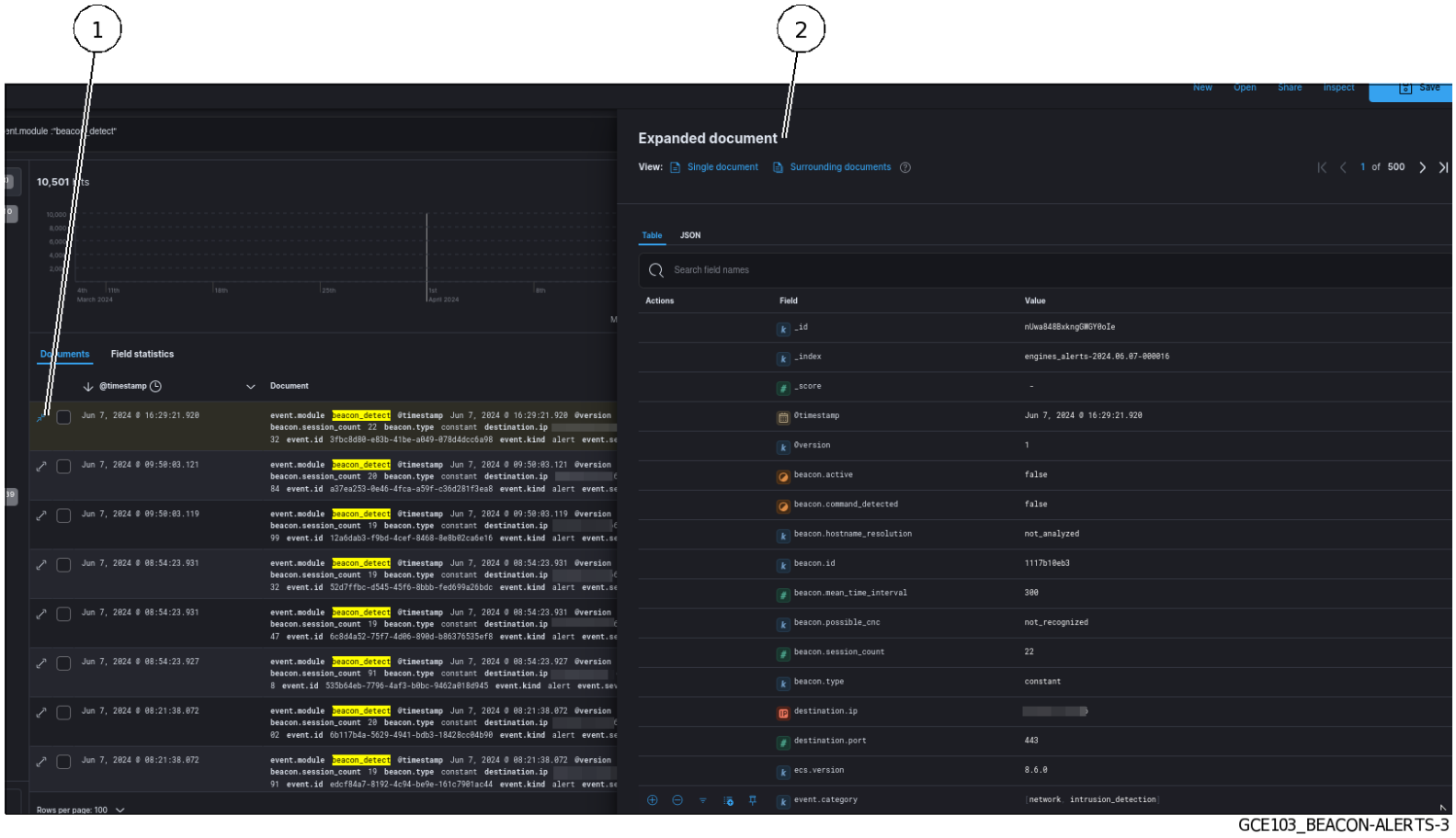
- In the main interface named **WebUI** of the GCenter in the `Alerts` screen.
  The main interface named **WebUI** is described in the *Overview of the WEB UI*.
  - To display the beacon alerts, select the `Beacon` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.



  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed in *Example of a Beacon detect alert in Kibana*.
- In the interface named **Kibana UI**:
  - Click on the `Hunting` icon of the `WebUI`.
    The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).
  - Click on the icon and then on `Discover`
  - Select the `engines_alerts*` choice in the Data View
  - In the search field, enter `event.module :"beacon_detect"` filter to display only the alerts of the Beacon detect engine

GCE103_BEACON-ALERTS-1

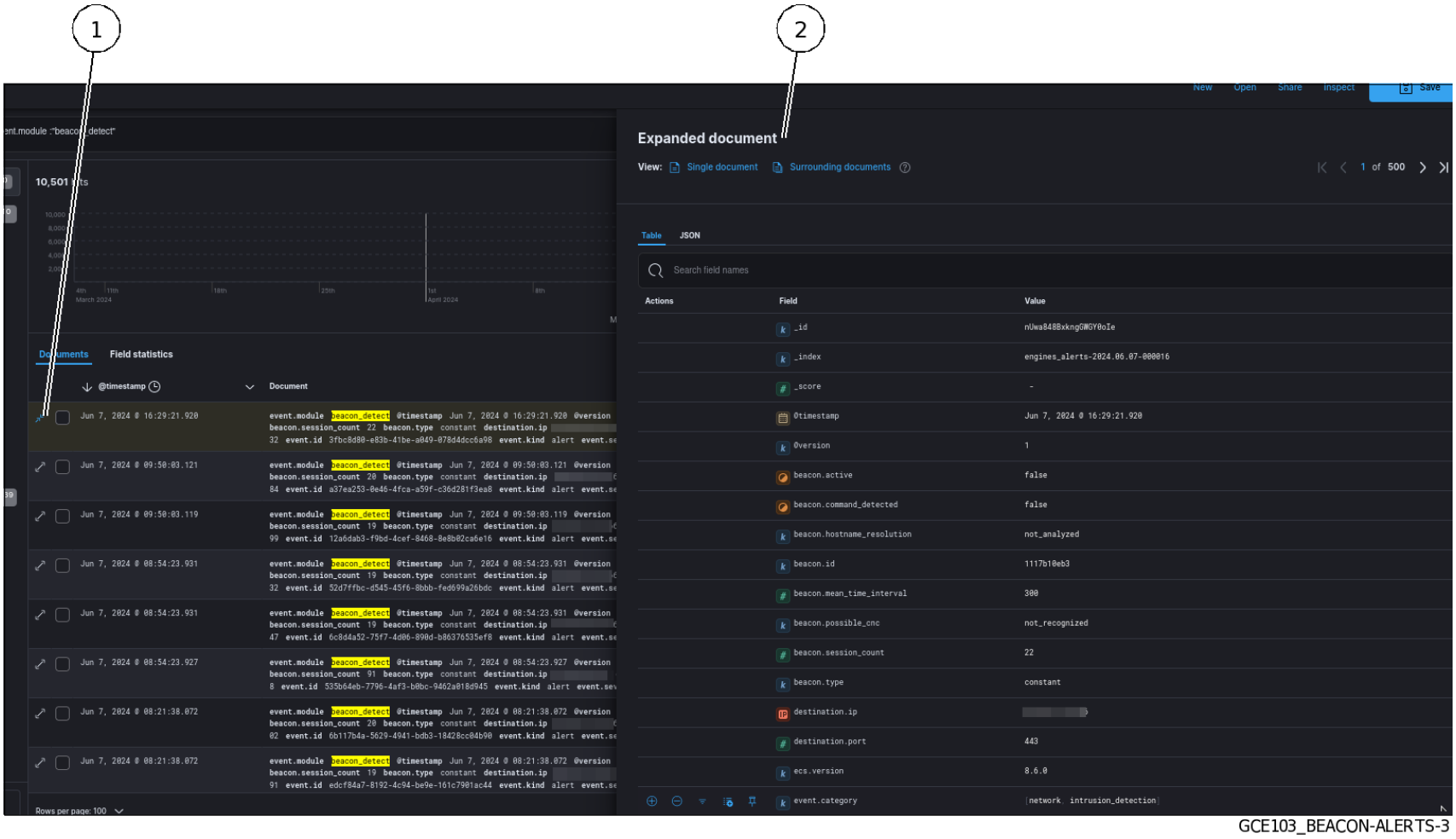
  - Click on the toggle icon (1) on the left of the Alert.
    The expanded document (2) is displayed.



GCE103_BEACON-ALERTS-3

The detailed information of this alert can be viewed in table or json format (see the *Beacon detect log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

2.1.11.2.1 Example of a Beacon detect alert in Kibana



GCE103_BEACON-ALERTS-3

The presentation of the `Alert details` window is given in the *`Alert details` window*.
The counters are detailed in the *Beacon detect log data structure*.

2.1.11.2.2 Beacon detect log data structure

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields"

This information is displayed in the `Expanded document` screen of Kibana.

2.1.11.2.2.1 The header part of the Beacon detect logs

The header section contains:

```
"_index": "engines_alerts-,
"_id": "-a9H1JMBe7Sz",
"_version": 1,
"_score": 0,
```

The detailed information is given in the table (*Counters of the header part of logs*).

2.1.11.2.2.2 The source part of the Beacon detect logs

The source part is defined by "_source" in the logs.

Note:

The data displayed on the WebUI (alerts details window) is a part of the data displayed on the `Extended document` screen on the Kibana interface.
All data can be exported to a SIEM via syslog (an example of an exported alert is shown).
The detailed information is given in the table (*Counters of the header part of logs*).

The example given here is a Kibana example.

```
"tls": {
  "client": {
    "server_name": "cisco-update.com"
  }
},
"@version": "1",
"event": {
  "created": "2024-09-09T13:02:34.254441+00:00",
  "end": "2024-09-09T11:52:25.666000+00:00",
  "severity": 3,
  "module": "beacon_detect",
  "start": "2024-09-09T11:47:44.012000+00:00",
  "category": [
    "network",
    "intrusion_detection"
  ],
  "kind": "alert",
  "id": "5e7bb104-6493-43b2-be4d-f7c28ce79e85",
  "dataset": "alert"
},
"source": {
  "ip": "10.0.0.60",
  "mac": "60:57:18:e9:4f:5d"
},
"beacon": {
  "mean_time_interval": 1,
  "active": true,
  "possible_cnc": "not_recognized",
  "session_count": 260,
  "type": "constant",
  "id": "c4c886b4ad",
  "hostname_resolution": "not_analyzed"
},
"destination": {
```

(continues on next page)

(continued from previous page)


```
  "ip": "157.230.93.100",
  "port": 443
},
"observer": {
  "product": "gcenter",
  "uuid": "78f4fed1-c9ad-52b9-b509-6b87767f501f",
  "log_format_version": "1.0.0",
  "hostname": "gcenter-clelyo-01.gatewatcher.com",
  "gcap": {
    "hostname": "gcap-clement-l.gatewatcher.fr",
    "version": "2.5.4.0-rc1"
  },
  "version": "2.5.3.103",
  "vendor": "gatewatcher"
},
"ecs": {
  "version": "8.6.0"
},
"@timestamp": "2024-09-09T13:02:59.354490664Z",
"url": {
  "domain": "cisco-update.com"
},
"network": {
  "protocol": "tls",
  "timestamp": "2024-09-09T11:47:44.012000+00:00",
  "transport": "tcp"
}
```


2.1.11.2.2.3 List of counters of the Malcore alert

Note:

The alert counters are visible:
- In the `Alert details` screen of the WebUI
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.11.3 Management of the engine

2.1.11.3.1 Viewing the engine status

The engine status is displayed in the *'Health checks' screen* if the engine has been activated: to check see *'Beacon detect' screen (Beacon command)*.
The engine can be activated if the installed license allows it; see the *'License' screen*.

2.1.11.3.2 Engine update

There are updates for the engine.
These updates can be done manually or scheduled via the Threat DB update command.
See *Dedicated modules for managing updates: Threat DB update and Software update* and in particular the part *Update presentation*.

2.1.11.3.3 Beacon detect configuration engine and management of the ignored destination list

The management interface is used:

- To filter the events (engine inputs) either to activate protocols or to filter events:
  - see the screen description, see *`Metadata rate limiter` screen*
  - see the procedure, see *Configuring Metadata Rate Limiters*
- To activate the engine or modify its parameters (sensitivity or Alerts rate limiter):
  - see the screen description, see *`Beacon detect` screen (Beacon command)*
  - see the procedure, see *Setting up the beacon detect engine*
- To manage the `` `Ignore list` `` used to explicitly filter healthy destinations (defined by domain name or IP):
  - see the screen description, see *`Beacon detect` screen (Beacon command)*
  - see the procedure, see *Setting up the beacon detect engine*

2.1.11.4 Alert Analysis

The alerts are displayed on a specific screen described in the *WebUI `Alerts` screen*.
The general procedure for analysing alerts is described in *Using of NDR dashboards*.
The specific procedure for analysing Beacon detect alerts is described in the *Analyzing the Beacon detect alerts*.

2.1.12 Yara engine

2.1.12.1 Introduction

2.1.12.1.1 For what types of threats is this engine designed?

The Yara engine allows detection of malware using rules.

2.1.12.1.2 How does this particular engine detect threats?

When a file, rebuilt by the GCap is submitted to Yara engine, it is analyzed and compared with each of Yara rules.
Yara rules define a number of variables that contain patterns found in a malware sample.
When the Yara engine finds a match between the network stream analyzed and the definition of a rule then an alert is raised and classified as malware in the same way as for the Malcore engine.

2.1.12.1.3 How does the Yara engine work in the GCenter?

The engine:

- Retrieves events sent by the GCap (for further details see *Yara engine input data*)
- Analyzes these events (for further details see *How does this particular engine detect threats?*)
- Generates alerts (for further details see *Events generated*)

2.1.12.1.3.1 Yara engine input data

The network flow is duplicated on the network by a TAP and the files are rebuilt by the GCap.
The file reconstruction is configured by the file reconstruction rules used by the GCap detection engine (refer to *Configuring the file reconstruction rules via the GCap profile*).

Yara needs Yara rules to run.
These rules are defined in a specific ruleset.
This ruleset has to be downloaded via the *`YARA` screen*.

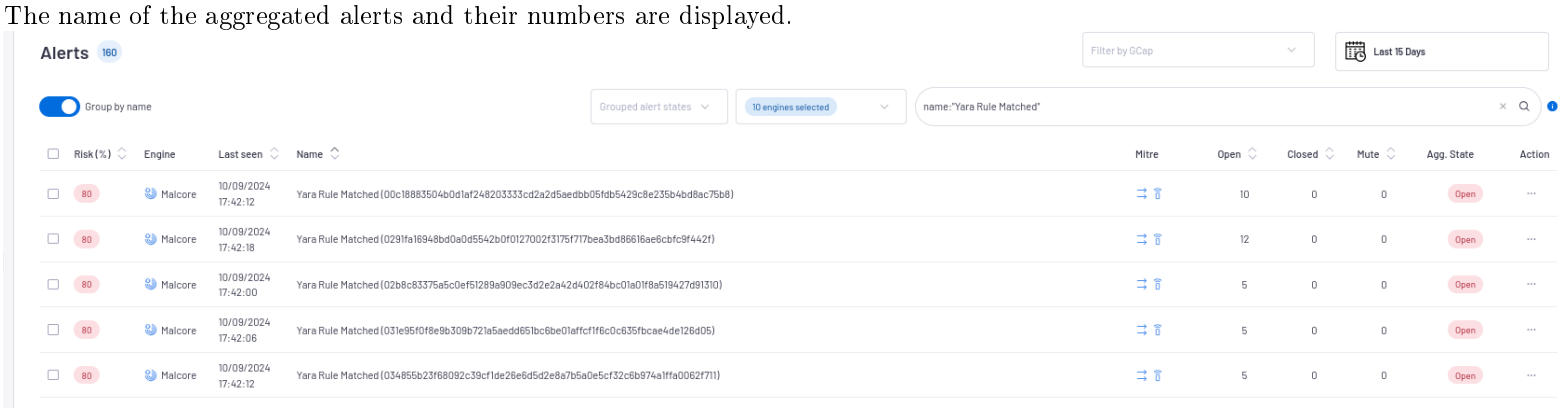
Note:

For further information about the Yara rules, see information on https://yara.readthedocs.io/en/stable/writingrules.html
To validate the rules, it is possible to use the validator (https://yaravalidator.manalyzer.org/).
To download an Yara ruleset example, `yara_ruleset_example.yara`.

2.1.12.2 Events generated

Events generated by the engine are **alerts** only.
Events generated by the Yara engine are included with the Malcore **alerts**.
These are displayed:

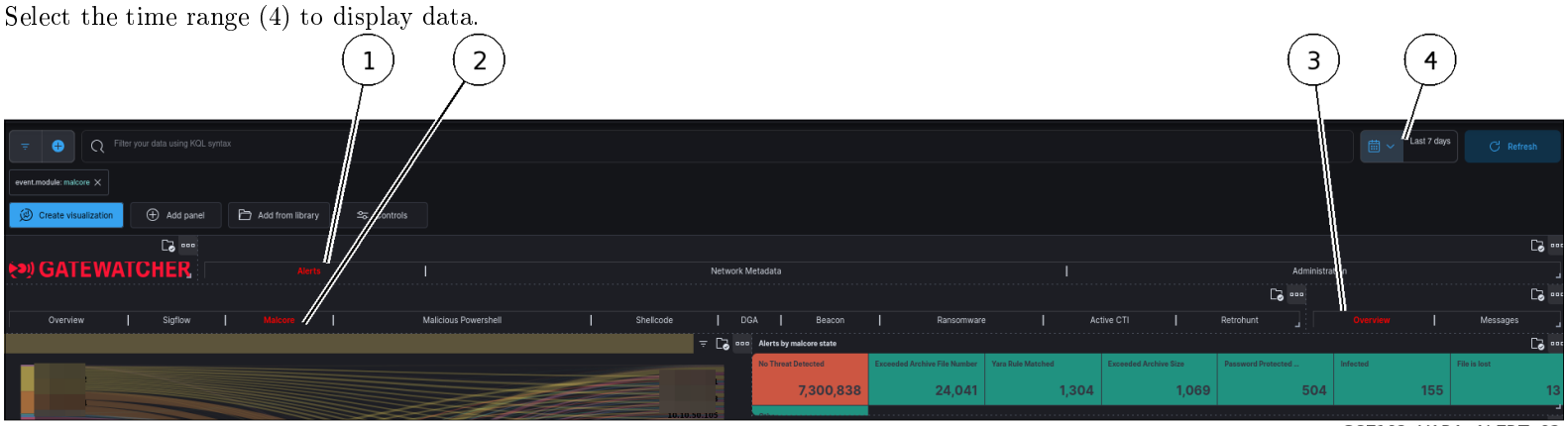
- In the main interface named **WebUI** of the GCenter in the `` `Alerts` `` screen:
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
  - To filter the Yara alerts, type `` `name:"Yara Rule Matched"` `` in the search field then validate.
  - Use the `` `Group by name` `` selector to view the number of different alerts.
    The name of the aggregated alerts and their numbers are displayed.



  - Click on a grouping of alerts to display the list, if needed.
  - Disable the `` `Group by name` `` selector.
    Different Source and Destination information is displayed for each alert.
    `` `Tags` `` and `` `Notes` `` are also visible and editable.
    The various Quick Access `` `Actions` `` are available for each alert.
  - Click on an alert.

    The detailed information of this alert is displayed in *Example of an Yara alert in the WebUI*.

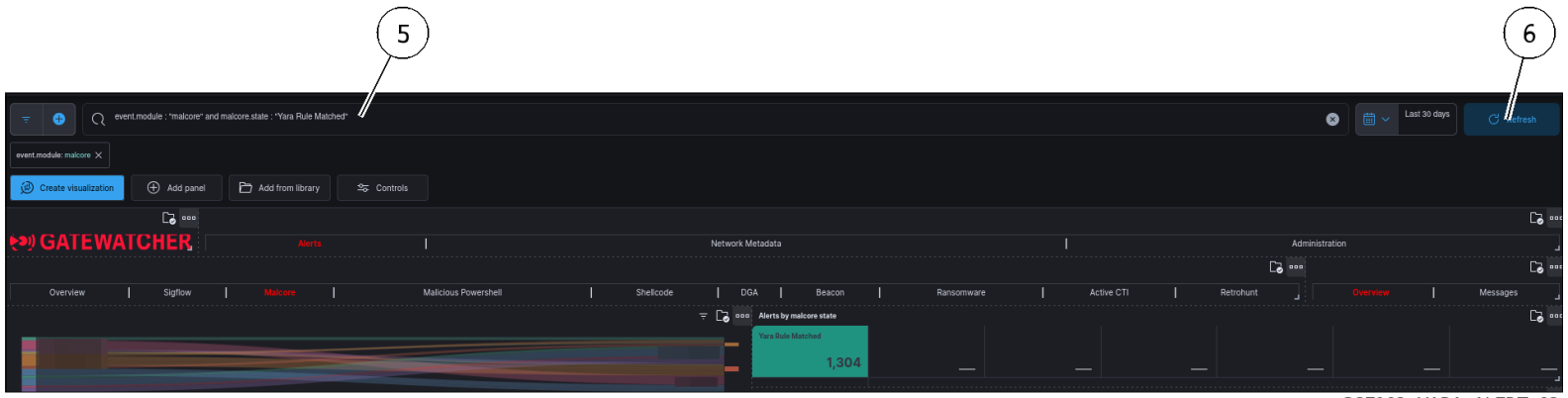
- In the **Kibana UI** interface
  - To view all Yara alerts:
  - In the main interface **WebUI**, click on the `` `Hunting` `` icon.
    The main interface named **WebUI** is described in *Overview of the WEB UI*.
  - Click on the `` `Malcore` `` tab (2) of the `` `Alerts` `` category (1).
  - Select the `` `Overview` `` tab (3).
  - Select the time range (4) to display data.



GCE103_YARA_ALERT_02

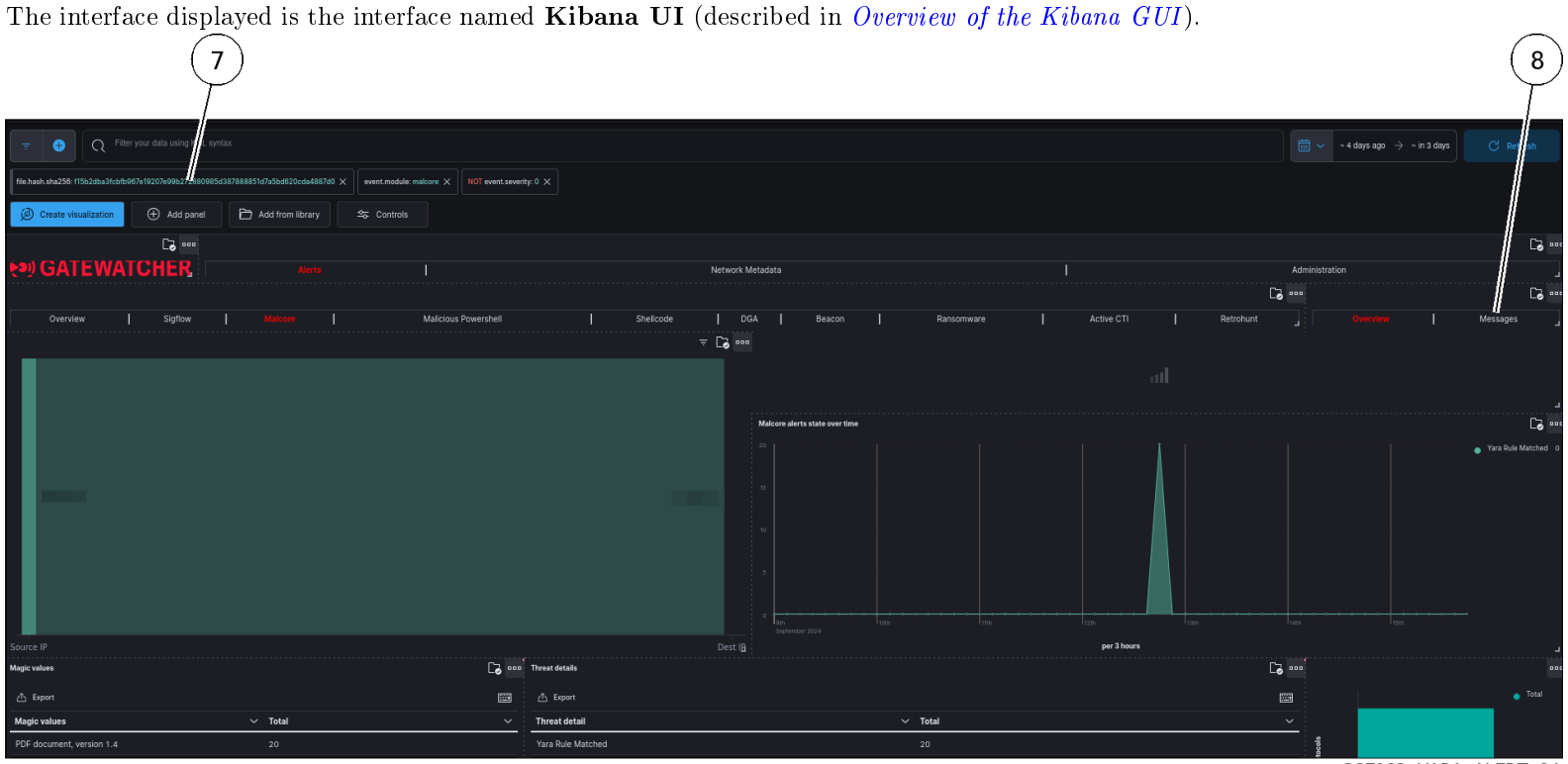
  See the presentation of the *WebUI `Alerts` screen*.

  - To filter the Yara alerts on Kibana, enter the following command `` `event.module : "malcore" and malcore.state : "Yara Rule Matched"` `` (5) in the search field.
  - Validate wih the `` `Refresh` `` button (6).



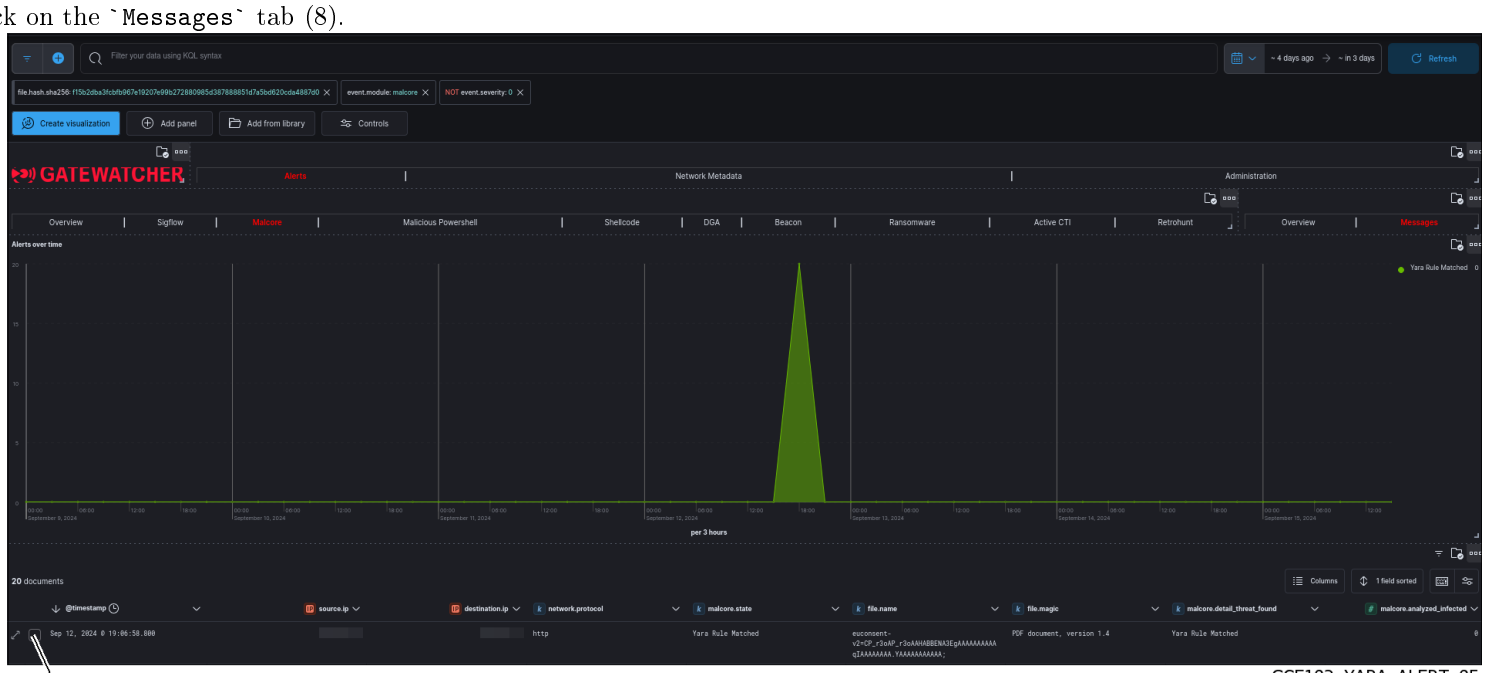
GCE103_YARA_ALERT_03

- To consult information about a specific alert:
- After selecting the alert, click on the `Open malcore file transaction` command of the `Actions` menu.
  Kibana is opened on the `Malcore` tab of the `Alerts ` section: in the `Overview` tab, the database is filtered on the `file.hash.sha256` parameter (7).
  The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).



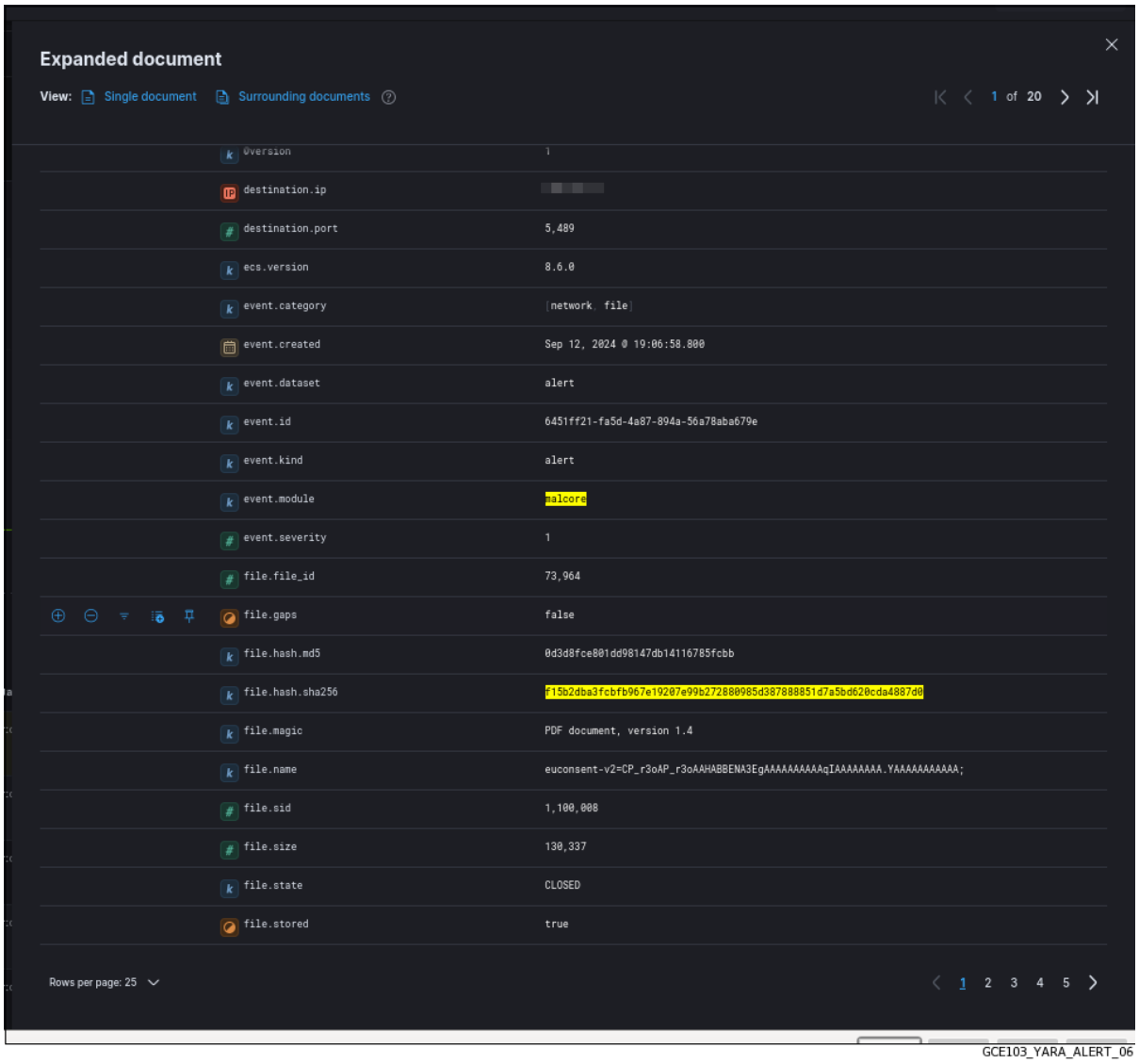
GCE103_YARA_ALERT_04

- Click on the `Messages` tab (8).



GCE103_YARA_ALERT_05

- Click on the toggle icon (9) on the left of the Alert
  The expanded document is displayed.

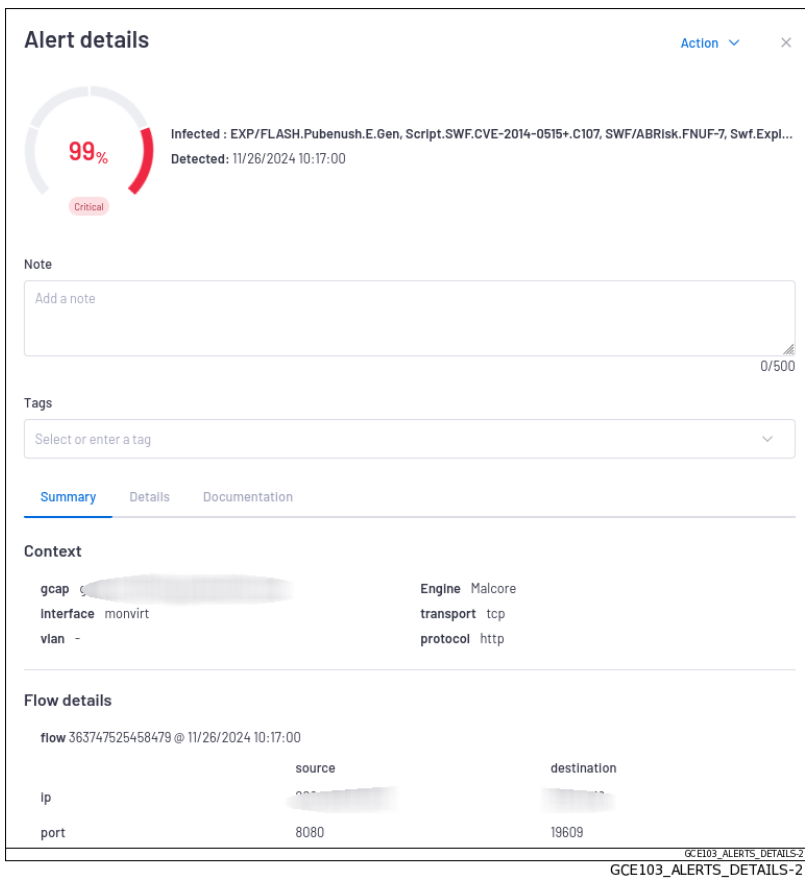


GCE103_YARA_ALERT_06

The detailed information of this alert can be viewed in table or json format (see the *Yara log data structure*).

An example is given in *The source part of Yara logs*.

2.1.12.2.1 Example of an Yara alert in the WebUI



GCE103_ALERTS_DETAILS-2

The presentation of the `Alert details` window is given in the *`Alert details` window*.

The counters are given in the *Engine log data structure* appendix.

2.1.12.2.2 Yara log data structure

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields"

This information is displayed in the `Expanded document` screen of Kibana.

2.1.12.2.2.1 The header part of Yara logs

The header section contains:

```
"_index": "engines_alerts-2025.02.04-000001",
"_id": "odx80JQB3WGd7COqasTr",
"_version": 1,
"_score": 0,
```

The detailed information is given in the table (*Counters of the header part of logs*).

2.1.12.2.2.2 The source part of Yara logs

The source part is defined by "_source" in the logs.

Note:

The data displayed on the WebUI (alerts details window) is a part of the data displayed on the `Extended document` screen on the Kibana interface.
All data can be exported to a SIEM via syslog (an example of an exported alert is shown).
The detailed information is given in the table (*Counters of the header part of logs*).

The example given here is a Kibana example.

```
"@version": "1",
"source": {
  "ip": "192.168.122.15",
  "port": 53,
  "mac": "00:11:22:33:44:55"
},
"network": {
  "protocol": "dns",
  "tx_id": 193630,
  "flow_id": 2201432362562192,
  "transport": "udp",
  "timestamp": "2025-02-04T10:22:36.248783+0000"
},
"destination": {
  "ip": "8.8.8.8",
  "port": 53,
  "mac": "00:55:44:33:22:11"
},
"@timestamp": "2025-02-04T10:22:36.248Z",
"event": {
  "dataset": "alert",
  "created": "2025-02-04T10:22:36.248783+0000",
  "kind": "alert",
  "severity": 1,
  "module": "active_cti",
  "category": [
    "network",
    "intrusion_detection"
```

(continues on next page)

(continued from previous page)


```
  ],
  "id": "d79bff72-01b6-4639-979c-efcb5e6faf23"
},
"sigflow": {
  "payload": "3+YBAAABAAAAAAAADjkyNzU4LWNvaW5iYXNlA2NvbQAAAQAB",
  "signature_id": 1300000773,
  "metadata": {
    "risk": [
      "highly suspicious"
    ],
    "signature_severity": [
      "2"
    ],
    "ioc": [
      "fffc7e75-cb75-4210-a244-669cba3cae06"
    ],
    "updated_at:": [
      "2025_02_04"
    ],
    "created_at:": [
      "2025_02_04"
    ]
  },
  "gid": 1,
  "action": "allowed",
  "rev": 0,
  "stream": 0,
  "payload_printable": ".............92758-coinbase.com.....",
  "signature": "Active CTI - Host - Unknown/Unknown - Unknown family - Unknown threat actor - fffc7e75-cb75-4210-a244-
↪669cba3cae06",
  "category": "Active CTI"
},
"flow": {
  "bytes_toclient": 10843280,
  "pkts_toclient": 96815,
  "bytes_toserver": 7551648,
  "pkts_toserver": 96816,
  "start": "2025-02-04T10:20:39.242320+0000"
},
"ecs": {
  "version": "8.6.0"
},
"dns": {
  "query": [
    {
      "rrname": "92758-coinbase.com",
      "rrtype": "A",
      "tx_id": 193630,
      "opcode": 0,
      "type": "query",
      "id": 57318
    }
  ]
},
"observer": {
  "product": "gcenter",
  "vendor": "gatewatcher",
  "gcap": {
    "hostname": "gcap1000-s-2.mgmt.qa.gatewatcher.fr",
    "ingress": {
      "interface": {
        "name": "monvirt"
      }
    },
    "version": "2.5.4.0-rc9"
  },
  "hostname": "gcent9100r2.mgmt.qa.gatewatcher.fr",
  "uuid": "72cbafc7-7306-5382-96d2-203a730252a8",
  "version": "2.5.3.103",
  "log_format_version": "1.0.0"
}
```

2.1.12.2.2.3 List of counters of the alert

Note:

The alert counters are visible:
- In the `Alert details` screen of the WebUI
- In the `Expanded document` screen of Kibana
- In the export to the SIEM

The detailed information is given in the table (*Counters of the source part of logs*).

2.1.12.3 Management of the engine

2.1.12.3.1 Viewing the engine status

The engine status is displayed in *`Health checks` screen*.

2.1.12.3.2 Engine update

The engine is updated with each new version of the GCenter.

2.1.12.3.3 Engine configuration

The management interface is used:

- To active the engine
- To load a Yara ruleset

For more information on the procedure: see the *Setting up the Yara engine*.
The management interface is described in *`YARA` screen*.

2.1.12.4 Alert Analysis

The alerts are displayed on a specific screen described in the *WebUI `Alerts` screen*.
The general procedure for analyzing alerts is described in *Using of NDR dashboards*.
The specific procedure for analyzing Yara alerts is described in the *Analyzing the Yara alerts*.

2.1.13 Detection by GScan

GScan allows you to manually submit files for analysis.
The following options are possible:

- Malware: submit files to the Malcore engine
- Powershell: scans files containing Powershell scripts and detects potential threats that can serve as a gateway to install malware on Windows.
  With regard to malicious powershells, detection is based on a supervised machine learning model, and on the fact that these scripts generally use obfuscation techniques or that are similar to them (base64, concatenation, type conversion, etc.).
- Shellcode: submits files for analysis by the shellcode detect engine

Before starting an analysis, it is necessary to check the type of analysis to be performed, see above.
To start parsing a file, simply drag the file into the `DRAG and DROP or CLICK TO SELECT YOUR FILES` area or click on this area to send the suspicious file.
The result of the analysis is then displayed in a thumbnail with the status of the file for each type of analysis chosen.

The `SCAN HISTORY` page displays the history of the analysis performed.

Note:

Attention the maximum file size should not exceed 30MB by default.
There is no limitation on the number of file scans.

Concerning the compressed files analyzed by Malcore:

- The number of files contained in an archive is:
- limited
- editable (50 is the default)
- The number of times the file is compressed is:
- limited (max recursion level)
- editable (5 is the default)
- If files are password protected, the password must be declared in the global settings.

These settings are only accessible to members of the administrator group.

See procedure for *Setting up the Malcore engine*.

- Modify if necessary the maximum size of files sent to Gscan (MB)
- Modify if necessary the maximum recursion level for archives sent to Gscan
- Modify if necessary the maximum number of archive files sent to Gscan

The GUI is described in *WebUI `GScan` screen*.
For implementation, see the *Detecting with GScan*.

2.2 Management of the GCenter software

2.2.1 Dedicated modules for managing updates: Threat DB update and Software update

Updates are managed via the following modules:

- **Software update** for the installation of **Upgrades**. These are the **GCenter or GCaps upgrades** (operations to be done manually)
- **Software update** for the installation of **Hotfix**. These are the **patches that modify the equipment without having to perform a complete upgrade**
- **Threat DB update** for the installation of **Updates**. These are **updates of detection signatures and/or anti-viral engines**
  The installation process can be manual or scheduled.
- **Threat DB update** for the configuration of **Updates** planning
  The management of updates is indicated in *Release note*.
  The various existing updates are:

Update type	To do what?	How	See for more information	See procedure
Upgrade	Upgrade version	Manually	*Upgrade presentation*	*Installing of an upgrade*
Update	Update detection signatures and/or anti-viral motors	Manually	*Update presentation*	*Installing an update manually*
		Automatically		*Configuring automatic update of signatures and/or anti-viral engines*
Hotfix	Patch application	Manually	*Hotfix presentation*	*Installing a hotfix*

Note:

Sigflow engine updates and version upgrades for a GCap are managed from the GCenter.

2.2.2 Upgrade presentation

The upgrade is a version upgrade and significantly changes the GCenter and the GCap.

Note:

It is necessary for the administrator to read the Release Note before performing a version upgrade.

When applying a version upgrade to GCenter, it will be necessary to restart the GCenter manually at the end of the operation.
For a GCap version upgrade, simply load the version upgrade package into the GCenter. The rest of the actions will be on the GCap side (See GCap documentation).
An upgrade increments the version number such as 2.3.5.101 to 2.3.5.102.

Note:

Upgrades are done manually by the administrator; no automation is possible in the Updates menu.

Note:

There are also upgrade packages that include hotfixes directly.
This allows you not to have to apply all hotfixes after installing an appliance.

The GUI is described in the *`Software update` screen*.
For implementation, see the *Installing of an upgrade* procedure.

2.2.2.1 Minor update case

For example, when moving from v2.3.5.101 to 2.3.5.101-hf1, there are two ways to perform the system update:

- Applying only the HF1 patch
- Applying an upgrade

These two solutions are equivalent.

2.2.2.2 In the case of a major update

For example, for the transition from v2.3.5.101 to 2.3.5.102, only the upgrade is applicable.
For implementation, see the *Installing of an upgrade* procedure.

2.2.2.3 Upgrade path

The general rule for update paths is that it is necessary to be on the last patch before performing a version upgrade.
Otherwise, this will be notified in the Release Note of the relevant version.

2.2.3 Update presentation

Threat-DB updates apply to GCenter and the GCap.
There are several types of update packages:

- beacon.gwp package: this package contains beacon update
- cti.gwp package: this package contains update of the database of Indicators Of Compromise
- dga.gwp package: this package contains update to the DGA detect engine
- sigflow.gwp package: this package contains the sigflow engine update and the rules base updates
- malcore directory: this directory contains the updates of Malcore engines and their antivirus databases
- full package (full.gwp): this package is the sum of the previous packages

Note:

The malcore directory contains:
- One package for each antivirus engine named after the hash of the engine to which it relates, same hash as what is presented in malcore healthcheck
- A package of utilities named "common_utilities.gwp"

These packages can be installed as follows:

- *Manual Update*
- *Automatic update*

2.2.3.1 Manual Update

The manual update is suitable for isolated environments.
The administrator must first manually download the update packages to an administration workstation and then upload them to the GCenter via the web interface.

Note:

The cti.gwp package is updated hourly on update.gatewatcher.com
The other packages are updated daily.

Note:

If network has no limited bandwidth, the easiest way is to load the full.gwp file to update everything in a single operation

In this case, the GUI to be used is described in *`Threat DB update` screen*.
For manual installation, see the *Installing an update manually* procedure.

2.2.3.2 Automatic update

They can be carried out in different ways according to the needs of the information system:

- *Online update*: packages are downloaded directly from GATEWATCHER websites
- *Local update*: packages are downloaded from a local repository

This schedule has be configured.
In this case, the GUI to be used is described in *`Threat DB update` screen*.
For planning implementation, see the *Configuring automatic update of signatures and/or anti-viral engines* procedure.

2.2.3.2.1 Online update

The **Online** update automates updates and reduces administration tasks.
The **Online** update is done automatically from https://update.gatewatcher.com/ and https://gupdate.gatewatcher.com.

Note:

In the case of scheduled **Online** mode, the schedule only applies to the **Sigflow** engine.
Engine updates **Malcore** are performed every 24 hours.

2.2.3.2.2 Local update

In order to meet specific security constraints, the GCenter can load its updates from a local repository previously configured to receive packets.
The steps for setting up a local repository are as follows:

- Prerequisites: a listening web server on port 80
- Create the following tree structure: "2.5.3.10X/GCenter" according to the GCenter version (2.5.3.103).
  In the following configuration example, this tree should be created at the root of the server.
- Retrieve gwp files for the 2.5.3.103 (beacon.gwp, cti.gwp, dga.gwp, all packages of the malcore folder, sigflow.gwp) on https://update.gatewatcher.com/update/
- In "2.5.3.10X/GCenter", put the previously recovered gwp files
- In "2.5.3.10X/GCenter", put the files . sha256 corresponding to the files above

Note:

The cti.gwp package is updated hourly on update.gatewatcher.com
The other packages are updated every day.
It is possible to download the full.gwp file in automatic mode by using the option '''use one .gwp file instead of split''' in Threat DB update configuration.

Note:

In case of limited bandwidth, the exact required package list coherent with the license is available in threat-DB update configuration, with the `show requirements` button.

Note:

Before a version upgrade, it is strongly recommended to update the local repository tree by adding a folder with the name of the new version.
If this is not the case, the equipment will no longer be able to update and this will cause errors during automatic updates.

2.2.4 Hotfix presentation

The hotfix enables to apply one or more patches without having to perform a complete upgrade of the equipment.
Therefore, restart is not necessary.
Applying a hotfix should be done in the order (for example v102 -> v102-hf1 -> v102-hf2 -> ...).

Note:

In most cases, hotfixes will not require a restart of the web service.

The GUI is described in the *`Software update` screen*.
For implementation, see the *Installing a hotfix* procedure.

2.2.5 Release note

The Release Note contains the list of changes made by the given version, the list of known issues but also important notes related to the upgrade process.
Release Notes are referenced in the following table.

Version	Release Note
2.5.3.102	https://releases.gatewatcher.com/en/gcenter/2.5.3/102/
2.5.3.103	https://releases.gatewatcher.com/en/gcenter/2.5.3/103/

2.2.6 Overview of the backup and restoration

The **Backup/Restore** component of the GCenter enables to:

- Backup the entire configuration (format : .gwc)
- Restore the configuration

Attention:

There is no specificity in terms of choosing what to backup or restore. The entire backup will be restored.

The saved elements are:

- For the Sigflow engine:
- The sources
- The rulesets
- Ruleset changes (suppress, threshold, etc.)
- For the GCaps:
  - All GCaps and what allows their pairing: after the restore, if the GCaps are UP and correctly configured, the tunnels must be established
  - The entire configuration of each GCap:
  - Detection rulesets
  - Variable base
  - Net variables
  - Flow timeouts
  - File rule management
  - Packet filters
- Operator group parameters of NDR:
- Asset detection network range
- Static IP-Asset mapping
- Ignored IP for users association
- Ignored MAC for assets association
- Administrator group parameters of NDR (feature activation and retention time):
- The backup server configuration
- The data export configurations
- Engines configuration (activation/Ignore list)
- Configuration of third party modules
- User list, LDAP settings, API keys and password policy
- All parameters of the "configuration" menu, except for the license (see specific point for licenses below)
- CTI parameters and LIS license
- The parameters of update configuration

Note:

The size of the backup file is larger than in earlier GCenter versions due to the presence of the NDR data.

You can select how many backups should be kept on the GCenter.
The default value is 3 and the maximum is 10.

The backup can be scheduled on a regular basis:

- On a daily basis with a choice of time
- Once a week with a choice of time and day of the week
- Once a month with a choice of time and day of the month

The various types of backup available are as follows:

- `Local`: for a direct backup on the GCenter
- `SCP`: enables eternalizing the backup to a remote SSH server
- `FTP` enables eternalizing the backup to a remote FTP server

When backing up in SCP or FTP mode, the configuration is exported to the remote server. However, a copy is also kept in the list of local backups.
It is important to note that when restoring a backup, the GCenter will automatically restart at the end of the operation.
In the event the restoration must be done on a new machine, certain requirements must be met:

- The GCenter network configuration must be the same (same FQDN, same number of enabled network interfaces)
- The version of the GCenter that restores must be the same as the version that saved it.

Important:

If the previous GCenter was installed in v102 and 2 hotfixes were applied manually, this order must be respected when reinstalling the new GCenter.
The restore function works only for GCenter that are in the exact same version (including minor version).

Note:

In the case of a reinstallation or reset of the **GCenter**, it will be necessary to enter a license in order to access the **Restore** menu

The graphical interface that manages the backup restore configuration is described in *`Configuration` screen*.
The graphical interface for using backup restore is described in *`Backup operations` screen*.
To configure the backup, see *Setting the backup*.
To perform a backup, see *Operating the backup*.
To carry out a restore, see *Operating the restoration*.

2.3 Data use

The GCenter generates several data: events, statistics, health logs, authentication logs.
The GCenter generates events based on the GCap data (captured traffic), the GScan data and the GCenter engines.
The data (events) created by the GCap and the GCenter is of various types:

- *Detection data*
- *Data related to detection results*
- *Management and system status data*

This data can, if necessary, be managed by the administrator.
This management involves:

- Managing and modifying if necessary the *Data retention*
- *Deleting data*

2.3.1 Detection data

In addition to dashboards present from the GCenter web interface, it is possible to use external equipment using the Syslog protocol (such as a SIEM), in order to exploit the data reported by the solution.

2.3.1.1 Data export via the Syslog protocol

The GCenter offers administrators the option of configuring up to two data exports to different destinations.
Data can be exported to a SIEM for example.
Once an export is activated, all selected data will be sent to the configured destination.
It is of course possible for the administrator to choose which data they wish to export.

Note:

When referring to exported data, only "alert" and "metadata" type data are concerned.
No GCenter or`Ignored system log file is concerned by this export.

The GUI is described in the *`Data export` screen*.

2.3.1.2 ECS format for the data export

The GCenter uses the ECS format for the data export.
The Elastic Common Schema (ECS) is an open source specification, developed with support from the Elastic user community.
ECS defines a common set of fields to be used when storing event data in Elasticsearch, such as logs and metrics.
ECS specifies field names and Elasticsearch data types for each field, and provides descriptions and example usage.
ECS also groups fields into ECS levels, which are used to signal how much a field is expected to be present.

2.3.1.2.1 Example of an alert exported

For information : this example shown an alert of infected type


```
<0>Sep 11 09:31:00 gcenter-xxxo-01.gatewatcher.com gatewatcher[-]: {"observer":{"vendor":"gatewatcher","uuid":"78f4fed1-
↪c9ad-52b9-b509-6b87767f501f","gcap":{"ingress":{"interface":{"name":"monvirt"}},"hostname":"gcap-xxx.gatewatcher.fr",
↪"version":"2.5.x.x-yy"},"version":"2.5.3.103","log_format_version":"1.0.0","hostname":"gcenter-xxx.gatewatcher.com",
↪"product":"gcenter"},"source":{"port":80,"ip":"xx.xx.xx.xx"},"file":{"magic":"Macromedia Flash data (compressed),␣
↪version 13","sid":[1100020],"hash":{"sha256":"6d3a6e2c771ab1a3721235ed3b3c4a2c3013290564272bcb6f79278b"},"name":"/",
↪"file_id":219,"tx_id":2,"state":"CLOSED","gaps":false,"size":55351,"stored":true},"@timestamp":"2024-09-11T09:31:00.
↪111583612Z","malcore":{"file_type":"application/x-shockwave-flash","analyzers_up":16,"analyzed_clean":9,"engines_last_
↪update_date":"2024-09-03T17:15:00Z","state":"Infected","total_found":"3/16","detail_scan_time":373,"reporting_token":"
↪","analyzed_infected":3,"detail_threat_found":"Infected : EXP/Flash.EB.502, SWF/Exploit, Exploit.Flash","analyzed_
↪suspicious":0,"analyzed_error":0,"processing_time":1576,"engine_id":{"5":{"scan_result":"CLEAN","threat_details":"","id
↪":"c18ab9n"},"8":{"scan_result":"INFECTED","threat_details":"Exploit.Flash","id":"ib54e9s"},"4":{"scan_result":
↪"UNSUPPORTED_FILE_TYPE","threat_details":"","id":"c10195e"},"14":{"scan_result":"CLEAN","threat_details":"","id":
↪"t3114fn"},"13":{"scan_result":"CLEAN","threat_details":"","id":"sde882s"},"9":{"scan_result":"CLEAN","threat_details":
↪"","id":"kfb8487"},"12":{"scan_result":"CLEAN","threat_details":"","id":"qb93081"},"10":{"scan_result":"CLEAN","threat_
↪details":"","id":"mb2b5fe"},"0":{"scan_result":"CLEAN","threat_details":"","id":"a32935b"},"15":{"scan_result":
↪"UNSUPPORTED_FILE_TYPE","threat_details":"","id":"we9a17t"},"6":{"scan_result":"CLEAN","threat_details":"","id":
↪"c81e55c"},"7":{"scan_result":"NOT_SCANNED","threat_details":"","id":"e83bf1t"},"3":{"scan_result":"CLEAN","threat_
↪details":"","id":"b557a5r"},"1":{"scan_result":"INFECTED","threat_details":"EXP/Flash.EB.502","id":"acf9bba"},"11":{
↪"scan_result":"NOT_SCANNED","threat_details":"Unavailable (permanently_failed)","id":"n00000e"},"2":{"scan_result":
↪"INFECTED","threat_details":"SWF/Exploit","id":"af7872b"}},"detail_wait_time":660,"file_type_description":"Macromedia␣
↪Flash Player","code":1,"magic_details":"Macromedia Flash data (compressed), version 13","analyzed_other":4},"@version":
↪"1","network":{"protocol":"http","timestamp":"2024-09-11T09:15:23.329615+0000","transport":"tcp","flow_id
↪":1779492455056060},"destination":{"port":47858,"ip":"x.x.x.x"},"url":{"domain":"exnchantingweddingsants.co.uk","path":
↪"/?q=&g=BDvv&y=enL16_6s_&s=t5qV-&e=_b_J--DqR&w=C2pZhaRyfn3uVT_v5Sfgs"},"user_agent":{"original":"Mozilla/5.0 (Windows␣
↪NT 6.1; Trident/7.0; rv:11.0) like Gecko"},"ecs":{"version":"8.6.0"},"http":{"request":{"method":"GET"},"hostname":
↪"nchantingweddingsandevents.co.uk","version":"HTTP/1.1","http_refer":"http://echantingweddingsandevents.co.uk/topic/
↪03251-esplanade-interoperability-fuchsias-renegotiate-percent-youngster-trounced/","response":{"status":200,"mime_type
↪":"application/x-shockwave-flash","bytes":55351}},"event":{"id":"7c4e2a77-3481-4201-8247-889fe0718ed8","kind":"alert",
↪"module":"malcore","severity":1,"category":["network","file"],"created":"2024-09-11T09:15:23.329615+0000","dataset":
↪"alert"}}
```


The counters are detailed in the *Engine log data structure*.

2.3.2 Data related to detection results

The data providing the results of the detection, i.e. the information related to the threats, is processed in the GCenter and displayed in the form of dashboards:

- Dashboards **synthetic**
  These are managed by the WEB User Interface.
  For more information, see the *Overview of the WEB UI*.
  Alerts displayed in dashboards are sorted using a threat score.
  This score is calculated from the analysis score returned by the different active engines at the time of detection.
  Threat level is defined as:
  - **Critical risk** (score from 75% to 100%)
  - **High risk** (score from 50% to 74%)
  - **Medium risk** (score from 25% to 49%)
  - **low risk** (no score displayed)

  Note:
  These threat levels are detailed in *WebUI `Home` screen*.

- Dashboards **complete**
  These are managed by the Kibana interface.
  For more information, see the *Overview of the Kibana GUI*.

2.3.3 Management and system status data

This data enables the following functions:

- *Viewing the system status*
- *Export system state data to remote servers*
- *System management and configuration*

2.3.3.1 Viewing the system status

- `Health checks` screen of the WebUI
  System status data is managed through the WebUI.
  For more information, see the *`Health checks` screen*.
- **Gstats** GUI
  System state data is also managed by Netdata services.
  Specifically, each`Ignored has a Netdata service that sends its information to the Netdata server located in the GCenter.
  Similarly, GCenter has a Netdata service that sends its information to the internal Netdata server at GCenter.
  The GCenter internal Netdata server allows the display of this data via the Gstats graphical interface.
  For more information, see the *Overview of the Netdata User Interface (Gstats)*.

2.3.3.2 Export system state data to remote servers

2.3.3.2.1 Export data to a Netdata server

In addition to the Netdata interface used for Gstats, the GCenter has another Netdata export interface whose purpose is to export data to an external server.
It must be configured: for more information, see the presentation of the *`Retention policy` screen*.
For implementation, see the *Configuring the Netdata export interface*.

2.3.3.2.2 Data retrieval by a Nagios server

For more information, see the presentation in the *`Retention policy` screen*.

2.3.3.3 System management and configuration

System management, in particular configuration, is carried out via:

- The configuration menu
  For more information, see the *Overview of the configuration menu*.
- Configuration options managed by the web interface
  For more information, see the *Overview of the `Administration` menu*.

In the event of an obstructing problem, it is necessary to access the solution logs in order to resolve the problem.
This information is used for diagnosis in collaboration with GATEWATCHER support.
The diagnostic function enables:

- Generating log files and uploading them for analysis by GATEWATCHER support.
  The export file log is protected by a password only known by the GATEWATCHER administrator team.
  Messages from all logs will be accessible as well as all system calls from the system.
- Generating the "Tech support" file and uploading it for analysis by an administrator.
  The "Tech support" file provides information on the health of the GCenter server although it does not contain any captured data.
  This file is not encrypted and is usable by the administrator.

Note:

In some sensitive environments, it may not be possible to extract the full set of non-anonymized logs as is possible with the `Log files` archive.
`Tech support` enables the administrator to provide non-sensitive, anonymized diagnostic information to support.

The graphical interface of the diagnostic function is described in *`Diagnostics` screen*.

Note:

It is also possible from the *setup* menu to generate a "Tech Support".
For more information, see the *`Diagnostics` screen*.

In these two situations, it is generally necessary for the administrator to contact GATEWATCHER support.
These files will enable the support team to identify potential malfunctions and to solve them.

2.3.4 Data retention

Data is stored on the GCenter for a limited time (called retention time) and for a maximum size.

Tip:

Increasing this time will increase the size of the stored data. This entails higher latencies and reduced performance and stability.

Note:

Configuration is performed in two steps:
- The first on the GCenter in this field,
- The second step on the GCap detection probe in the configuration parameters.

These parameters are adjustable.
The graphical interface is described in the *`Retention policy` screen*.

2.3.5 Deleting data

After a full or incremental save by the backup functionality, the old logs are automatically deleted, depending on the data retention time, thus freeing up disk space.
It is possible to delete information manually, by selecting all or part of the type and dates of the information to be removed.
This deletion period is selected by the administrator, however, it cannot exceed the total retention period of the data already pre-configured in the solution.
The same applies to the ICAP and Syslog services.

Important:

Data not yet processed will also be deleted.

The graphical interface is described in the *`Data Management` screen*.
For implementation, see the *Deleting data (log files)* procedure.

2.4 GApps management

GApps represent the different services running on the GCenter.
These services are listed in the *`GCenter Services Management` command*.
It may be necessary in some instances to restart or reset them.

Warning:

Resetting a service is equivalent to returning it to its factory-set configuration. It may be necessary to reapply certain configurations or updates.

2.5 Interconnection with external systems

2.5.1 Introduction

The GCenter can connect with external equipment such as:

- A Malware Information Sharing Platform server (MISP)
  The MISP server allows to retrieve the Compromise Indices in the form of detection rules usable by Sigflow
  For more information, see the presentation of *Connection to a MIPS server*
- SYSLOG servers via the syslog protocol
  These servers (SIEM, SPLUNK, LOGSTASH) import the detection data from the GCenter for centralization of this information
  For more information, see the overview of *Connection to Syslog servers*
- A Netdata server via the Netdata export interface.
  The Netdata interface exports system state data to an external Netdata server
  For more information, see the presentation of *Connection to a netdata server*
- A Nagios monitoring server via the Netdata polling interface.
  The `Netdata polling` part enables access to data for a Nagios type monitoring server: it reads the information on the input interface.
  For more information, see the presentation of *Access for a monitoring server*.

2.5.2 Connection to a MIPS server

The connection to a MIPS server (Malware Information Sharing Platform) makes it possible to retrieve the Indices of Compromises in the form of detection rules.
After connecting to a MISP, it becomes a possible source of rules for the Sigflow detection engine.
The connection status and configuration of the MISP connection is described in *`MISP settings` screen*.

Note:

Connection to MIPS server is experimental

The integration was tested with MISP version 2.4.159.
In case of problems, contact GATEWATCHER support.

For connection configuration implementation, refer to *Configuring the connection to the MISP*.
To implement the new rule source, see the *`Sources` screen*.

2.5.3 Connection to Syslog servers

2.5.3.1 Introduction

The Syslog protocol enables the export of detection-related data from the GCenter to remote Syslog servers.
Example of remote servers:

- A SIEM
- A Splunk SIEM
- ETL Logstash

The number of Syslog servers is limited to two.
The data to be exported can be:

- Alerts or
- Alerts and metadata

This data can be filtered in the *`Data export` screen*

Note:

No GCenter or GCap system data is affected by this export.

Finally the data can be encrypted: this encryption is defined in the *`Data export` screen*.
For details on data management, see the *Data use*.

2.5.3.2 SIEM

To connect the GCenter to a SIEM, it must be defined as a Syslog server in the *`Data export` screen*.
For implementation, see the *Configuring the export data to a SIEM via the syslog protocol*.

2.5.3.3 SIEM Splunk

To connect the GCenter to a Splunk SIEM, the SIEM must be defined as a Syslog server in the *`Data export` screen*.

2.5.3.4 Logstash

To connect the GCenter to the Logstash ETL, it must be defined as a Syslog server in the *`Data export` screen*.
A pipeline developed by Gatewatcher makes it possible to retrieve the JSON content of the exported logs so that it can then be manipulated with the Logstash filters.
For implementation, see the *Configuring the export data to ETL Logstash via the syslog protocol*.

Note:

It is possible to quickly create a POC (Proof Of Concept).
For implementation, see the *Creating a POC Logstash*.

2.5.4 Connection to a netdata server

The Netdata export interface enables the export of system-related data from the GCenter to a remote Netdata server.

For details on data management, see the *Data use*.
The description of the configuration is given in the *`Netdata Export Configuration` screen*.
For implementation, see the *Configuring the Netdata export interface*.

2.5.5 Access for a monitoring server

The `Netdata polling` feature allows access to data for a Nagios type monitoring server: it reads the information on the input interface.

For details on data management, see the *Data use*.
The configuration description is given in the *`Netdata polling` screen*.
For implementation, see the *Configuring the Netdata polling interface*.

2.6 API

2.6.1 Introduction

The API (Application Programming Interface) is the set of endpoints (also called resources or end of URL).
Each of these endpoints allows you to perform an action on the GCenter and return information without having to go through the graphical interface.
This facilitates the sharing and integration of GCenter features and data into existing architectures.

Each of these endpoints has a simple syntax.

These endpoints are predetermined: the list of these endpoints is limited and is displayed by theme (analyzers ...).

The execution of these endpoints can be done:

- Via SWAGGER (*Use via the swagger GUI*)
  This allows the use of endpoints and to understand its configuration and to test its execution and analyze its results
- Via CURL (*Use via CURL*)
  This allows to execute a Curl request directly and not to go through the GUI

2.6.2 Use via the swagger GUI

Each endpoint of the API:

- Performs a specific operation. Its name and description are indicated in the graphical interface (or in the *Endpoints list*)
- Performs one of four possible methods: GET, DELETE, POST, PUT
- Needs authentication rights that are the same as for the GUI (Operators or Administrators)
- May need operating parameters (input and/or output): for example, in the case of a filter, the value of this filter must be indicated

All this information is visible in the swagger GUI and is therefore the documentation of all API endpoints.
The swagger GUI description is given in *Overview of the API interface*.
For implementation of the swagger interface, see the *Using an endpoint API* procedure.

This interface enables to:

- Have a list of existing endpoints (listed by theme)
- Have details of possible parameters for running an endpoint
- Have information on the expected result (data model and an example with default values)
- Execute queries
- Retrieve the Curl command equivalent to the request via the API

Note:

A known bug affects the /api/alerts endpoint (see GCenter release note).
It is recommended to use the elasticsearch API to query data on the/api/data/es/search endpoint.

2.6.3 Use via CURL

It is possible to execute an endpoint by a CURL command.
This command is accessible via the swagger GUI after selecting the endpoint, entering any parameters and then starting the execution of the endpoint.
The curl command is displayed in the `Responses` area.

For a user called **username** and with **operators** rights.

Recovery of the API token:

```
curl -X POST "https://<hostname>/api/auth/login" -H "accept: application/json" -H "Content-Type: application/
↪json" -d "{ \"username\": \"username\", \"password\": \"password\"}" -k
```

where hostname is GCenter.

Answer:

```
{"token":"urxn5hlezbk3vnlgq1t45rifhg0vi951","expiration_date":"2021-04-13T16:26:45.743826"}
```

Sending a request:

```
curl -X POST "https://<hostname>/api/<endpoint> -H "accept: application/json" -H "Content-Type: application/json
↪" -H "API-KEY: x0zc5py1e2lrppe6ws0kgc8le0oxm9hg" -d "{\"test\": \"test\"}" -k
```

Example of a query that will query elasticsearch on its suricata* indexes and retrieve 100 logs over the last 24 hours:

```
curl -X POST "https://<hostname>/api/<endpoint> -H "accept: application/json" -H "Content-Type: application/json
↪" -H "API-KEY: x0zc5py1e2lrppe6ws0kgc8le0oxm9hg" -d "{ \"size\" : 100, \"query\" : { \"bool\": { \"must\": [],
↪ \"filter\": [ { \"match_all\": {} }, { \"range\": { \"@timestamp\": { \"gte\": \"now-24h\", \"lte\": \"now\
↪" } } } ], \"should\": [], \"must_not\": [] } } }" -k
```

2.6.4 Authentication and access to the API

Access to the swagger graphical interface is via the GCenter web GUI and then press the `API` button.
Authentication allows access to the API (For more information, see the *Title bar* paragraph).
Using curl request requires authentication to be done in the request.
This authentication is done using the name/password pairs or tokens defined in the *`API keys` screen*.

2.6.5 Endpoints list

See the *Endpoints list*.

Chapter 3

Characteristics

3.1 Mechanical characteristics of the Center

REFERENCE	DIMENSIONS (H x W x D)	RACKAGE	WEIGHT (KG)
GCENT8100r2	42.8 x 482 x 808.5 mm	1 U	21.9
GCENT9100r2	42.8 x 482 x 808.5 mm	1 U	21.9
GCENT900r2	86.8 x 434 x 836 mm	2 U	36.6
GCENT10500r2	86.8 x 434 x 836 mm	2 U	36.6

3.2 Electrical characteristics of the GCenter

REFERENCE	LOCAL STORAGE (SSD)	BACKUP STORAGE	EXTENSION STORAGE	POWER SUPPLY ELECTRICAL
GCENT8100r2	2x 960GB RAID1	2x 2 TB RAID1	N/A	2 x 750W
GCENT9100r2	4x 480GB RAID5	2x 2 TB RAID1	Contact GATEWATCHER	2 x 750W
GCENT9900r2	10 x 480GB RAID5	4 x 2 TB RAID5		2 x 1100W
GCENT10500r2	12 x 480GB RAID5	4 x 2 TB RAID5		2 x 1100W

3.3 Functional characteristics of tGCenter

REFERENCE	GCENT8100r2	GCENT9100r2	GCENT9900r2	GCENT10500r2
Events per second	2000	4000	6000	8000
Number of stored events	1 million	10 million	80 million	300 million
Number of files scanned per second	10	20	30	50
MPL qualified	OK			
SIEM infrastructure	OK			
GBox connector	OK			
FULL EDITION (FE) license	OK			
CRITICAL INFRASTRUCTURE (CIE) license	OK			
AD/LDAP authentication	OK			
SUPERVISION	OK			
IDRAC EXPRESS license	OK			
IDRAC BUSINESS license	OPTIONAL			

Chapter 4

Accounts

4.1 List of accounts

There are two user interfaces:

- The configuration menu (GUI)
- The web interface

For each of the two interfaces, user accounts exist.
Remote or local access to the administration interface is protected by a login password.

4.2 Setup account from the configuration menu

4.2.1 Account from the configuration menu

The user profile to access the configuration menu is **setup**.
The default password is: **default**.

4.2.2 Related principles

4.2.2.1 Authentication mode

A user's authentication is achieved by means of a login/password pair.

4.2.2.2 Password management

It is possible to change the password of the **setup** account from the GUI.
See the *`Authentication` command*

4.2.2.3 Password management policy

The passwords entered must comply with the password management policy.
The default policy is as follows:

Criteria	Default value
Number of different characters to make a password to be considered different	2
Minimum password length	12
At least one lower case letter	Yes
At least one upper case letter	Yes
At least one digit (0 to 9)	Yes
At least one symbol (i.e. neither a number nor a letter)	Yes

4.2.2.4 Anti-bruteforce system

An anti-bruteforce system is included on the GCenter.
The latter's policy will be as follows:

- Blocking for 15 minutes after 3 failed authentication attempts in a row
- 10 second delay between each failed authentication attempt

4.2.3 Functions reserved to the setup account

From the **setup** account, it is possible to access the entire configuration menu (GUI).
The configuration menu is described in the *Overview of the configuration menu*.
The permitted functions are described in the *Use case of the configuration menu: setup account*.

4.3 Web interface accounts and their management

The **GCenter** enables access to:

- Managing users and related groups
- History of the changes on the platform (see this in the history part)
- Linking with an LDAP server

4.3.1 Web Interface Accounts

4.3.1.1 List of groups

In the GCenter web interface, two different account types are defined by group membership:

- operator
- administrator

From the user account configuration menu, it is possible to create user accounts and belong to one or more groups and thus inherit the rights of each group.

Note:

The proposed groups fully comply with the Military Programming Act.

Note:

It is necessary to change the password from the first login and keep it in a safe place, for example, with the encryption keys of the appliances.

4.3.1.2 Generic account

Generic account has been defined with rights levels listed in the table below:

Generic Account Name	intended for a...	Group member
admin	access to all the functionalities of the analyst and administrator	operator and administrator

4.3.2 Functions allowed with the group or role `operator`

The **Operator** account accesses to the `Detection strategy` and `health` menus

4.3.3 Functions authorized with the group or role `administrator`

The **administrator** account accesses to the `administration` and `health` menus

---

4.3.4 Functions allowed in the admin account

From the **admin** account, it is possible to access all the features present in the navigation bars and menus of the WebUI.

4.3.5 Summary tables of the menus per level

4.3.5.1 Main menu

Menu	Description	operator	administrator
GATEWATCHER logo Home	page `Home` : general view of the GCenter	access	displays page Healthchecks
Overview	`Global overview` page	access	displays page Healthchecks
Relations	`Relations` page showing the relationships between the elements on the network	access	displays page Healthchecks
Hunting	KIBANA user interface	access	access without data
Assets	`Assets` page showing the characteristics of the elements present on the network	access	displays page Healthchecks
Users	`Users` page showing the characteristics of the users on the network	access	displays page Healthchecks
Alerts	`Alerts` page showing the characteristics of the alerts displayed	access	displays page Healthchecks
Gscan	`GScan` page to run a scan on a specific file	access	displays page Healthchecks

4.3.5.2 Menu bar

4.3.5.2.1 The `Detection strategy` menu

The `Detection strategy` menu consists of the following:

Command	Description	Operator Group	Administrator Group
`Sigflow engine`: `Gcaps profiles` command	Configuration of the sigflow engine by creating a Gcap profile	Access	No access
`Sigflow engine`: `Metadata rate limiter` command	Metadata rate limiters	Access	No access
`Malware`: `Malcore` command	Engine configuration	Access	No access
`Malware`: `Malcore Retroanalyzer` command	Engine configuration	Access	No access
`Malware`: `YARA` command	Engine configuration	Access	No access
`Exploit`: `Malicious Powershell` command	Engine configuration	Access	No access
`Exploit`: `Shellcode` command	Engine configuration	Access	No access
`Sigflow rules manager`: `Sources` command	Sigflow rules manager, source management	Access	No access
`Sigflow rules manager`: `Rulesets` command	Sigflow rules manager, ruleset management	Access	No access
`Sigflow rules manager`: `Auto-threshold` command	Sigflow rules manager, management of thresholds	Access	No access
`Threat intel': ```Active CTI` command	Engine configuration	Access	No access
`Threat intel`: `Retro Hunt` command	Engine configuration	Access	No access
`Behaviour analysis`: `Ransomware` command	Engine configuration	Access	No access
`Assets and users detection`: `Configuration` command	Configuration of association rules	Access	No access
`C&C`: `DGA` command	Engine configuration	Access	No access
`C&C`: `Beacon` command	Engine configuration	Access	No access

4.3.5.2.2 `Health` menu

The `Health` menu consists of the following:

Command	Description	Operator Group	Administrator Group
`Monitoring`: `Healthchecks` command	Visualization of the status of each type of detection	Access	Access
`Monitoring`: `Advanced metrics` command	Visualization of the status of the various physical and software components of the solution	No access	Access

---

4.3.5.2.2.1 `Administration` menu

The `Administration` menu consists of the following:

Command	Description	Operator Group	Administrator Group
`Updates`: `Threat-DB update` command	Configuration of signature updates and/or anti-viral engines (update)	No access	Access
`Updates`: `Software update` command	Configuration of upgrades (or upgrade) and patches (or hotfix)	No access	Access
`Authentication`: `History` command	Configuration and visualization of event history	No access	Access
`Authentication`: `Users management` command	Manage local user accounts in the GCenter	No access	Access
`Authentication`: `LDAP binding` command	Configuring the association between a GCenter and an LDAP server	No access	Access
`Authentication`: `API keys` command	API access token management	No access	Access
`Authentication`: `Password policy` command	Password policy management	No access	Access
`Third party`: `Reflex` command	Configuring the connection to the Reflex site	No access	Access
`Third party`: `MISP` command	Configuring the connection to the MISP site	No access	Access
`Gcap setup`: `Gcap Pairing` command	Configuring the GCap connection	No access	Access
`System`: `Licensing` command	Display information on current license, validity and available features.	No access	Access
`System`: `Network settings` command	Configuration of the GCenter network settings	No access	Access
`System`: `Global settings` command	GCenter configuration	No access	Access
`Maintenance`: `System logs` command	Display of data present in the GCenter ElasticSearch indexes	No access	Access
`Maintenance`: `Diagnostics` command	Generation of files for diagnosis	No access	Access
`Backup and restore`: `Configuration` command	Backup configuration	No access	Access
`Backup and restore`: `Operation` command	Running backup or restore	No access	Access
`Data`: `Retention policy` command	Elasticsearch Data Retention Configuration	No access	Access
`Data`: `Data management` command	Management of the GCenter data	No access	Access
`Data`: `Data export` command	Configuration of event export using syslog protocol	No access	Access
`Monitoring`: `Metrics export` command	Configure system data export to remote Netdata server	No access	Access
`Monitoring`: `Metrics polling` command	Configuring data access for a Nagios type monitoring server	No access	Access

---

4.3.5.2.3 `Help` menu

The `Help` menu consists of the following:

Command	Description	Operator Group	Administrator Group
`Documentation`: `API reference` command	Overview of the API	Access	Access
`Documentation`: `Online documentation` command	Access to online documentation	Access	Access
`External Resources`: `Gatewatcher Customer Portal` command	Access to the GATEWATCHER CUSTOMER PORTAL website	Access	Access
`External Resources`: `Gatewatcher support` command	Accessing https://support.gatewatcher.com/	Access	Access
`External Resources`: `Gatewatcher update repository` command	Accessing https://update.gatewatcher.com/update	Access	Access
`External Resources`: `Gatewatcher lab` command	Accessing https://www.gatewatcher.com/en/the-lab/	Access	Access

---

4.3.6 Related principles

4.3.6.1 Authentication mode

A user's authentication is achieved by means of a login/password pair.

4.3.6.2 Password management

The checking account manages its own password and potentially other accounts as well.
Details are provided in the table below:

User	can change the password		
	operator	administrator	admin
admin	X	X	X

4.3.6.3 Password management policy

The passwords entered must comply with the password management policy.
The policy is divided into the categories:

- General settings
- Specific password settings

These general parameters are:

- Period of validity
- Recording of previous password hashes

These specific parameters are the criteria that passwords must contain, such as lower case, upper case, and so on.
The details of these parameters and the graphical interface enabling the management of this policy are described in the *`Password policy` screen*.
For implementation, see the *Managing the password policy* procedure.

4.3.7 Creating local users

In addition to generic accounts, it is possible to create user accounts each having different rights.

Note:

The proposed groups fully comply with the Military Programming Law.

When creating a new user account, it is possible to assign different roles to the user.
The role(s) the user is assigned will enable them to access more or less menus in the web interface.
Indeed, depending on the actions carried out, it will be necessary to assign a specific role.
The administrator fills in the following fields concerning the user they wish to create:

- Username
- Password
- Email address
- First Name
- Last Name

It is also necessary to activate the account for it to be usable and to assign it the available roles: operator and/or administrator
These fields will be used later to trace the user in the connection history or in the event of changes concerning this same account.
The graphical interface enabling the creation of users is done in the *`Users management` screen*.
For implementation, see:

- the *Creating local user*

- the *Changing some of a local user's information*
- the *Resetting a local user's password*
- the *Deleting a local user*

4.3.8 LDAP integration / Active Directory

Authentication of the GCenter's user accounts can be managed by the GCenter as well as by a Lightweight Directory Access Protocol (LDAP) server.
Configuring the connection between the GCenter and the LDAP server is also done by the GCenter.
The main functions include:

- Displaying the connection status
- Enabling the connection to a remote authentication server
- Managing connection information to a remote authentication server
- Mapping of users and groups between the GCenter and the remote authentication server
- Advanced configuration of the connection to a remote authentication server

The graphical interface enabling the creation of users is done in the *`LDAP binding` screen*.
For implementation, see:

- The *Displaying of the connection status between the GCenter and the LDAP server*
- The *Enabling the connection between the GCenter and the LDAP server*
- The *Configuring the connection between the GCenter and the LDAP server*
- The *Configuring the users and groups defined on LDAP / ActiveDirectory*

4.3.9 Audit trail

The system records the various actions carried out in the web interface over time, in order to ensure traceability.
This traceability is carried out for:

- Users' connection or disconnection
- Creating and deleting accounts
- Changing the permissions of an account

4.3.9.1 Authentication history function

The history of all authentications on the GCenter is available.
To view the graphical interface presentation, see the *`History` screen*.
For the implementation, refer to *Viewing the authentication history*.

4.3.9.2 Historical function of all creations or deletions

The history of all creations or deletions of the GCenter users is available.
To view the graphical interface presentation, see the *`History` screen*.

4.3.9.3 History function for all changes in user rights

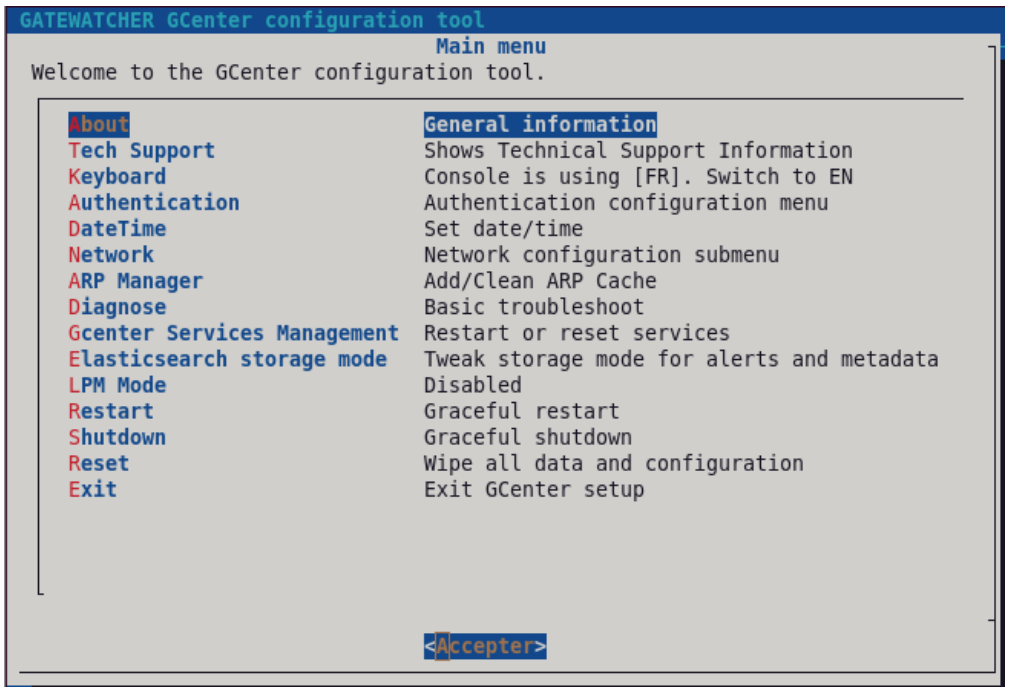
The history of all user permissions on the GCenter is available.
To view the graphical interface presentation, see the *`History` screen*.

Chapter 5

Overview of the GCenter graphic interfaces

5.1 Overview of the configuration menu

The configuration menu is displayed.



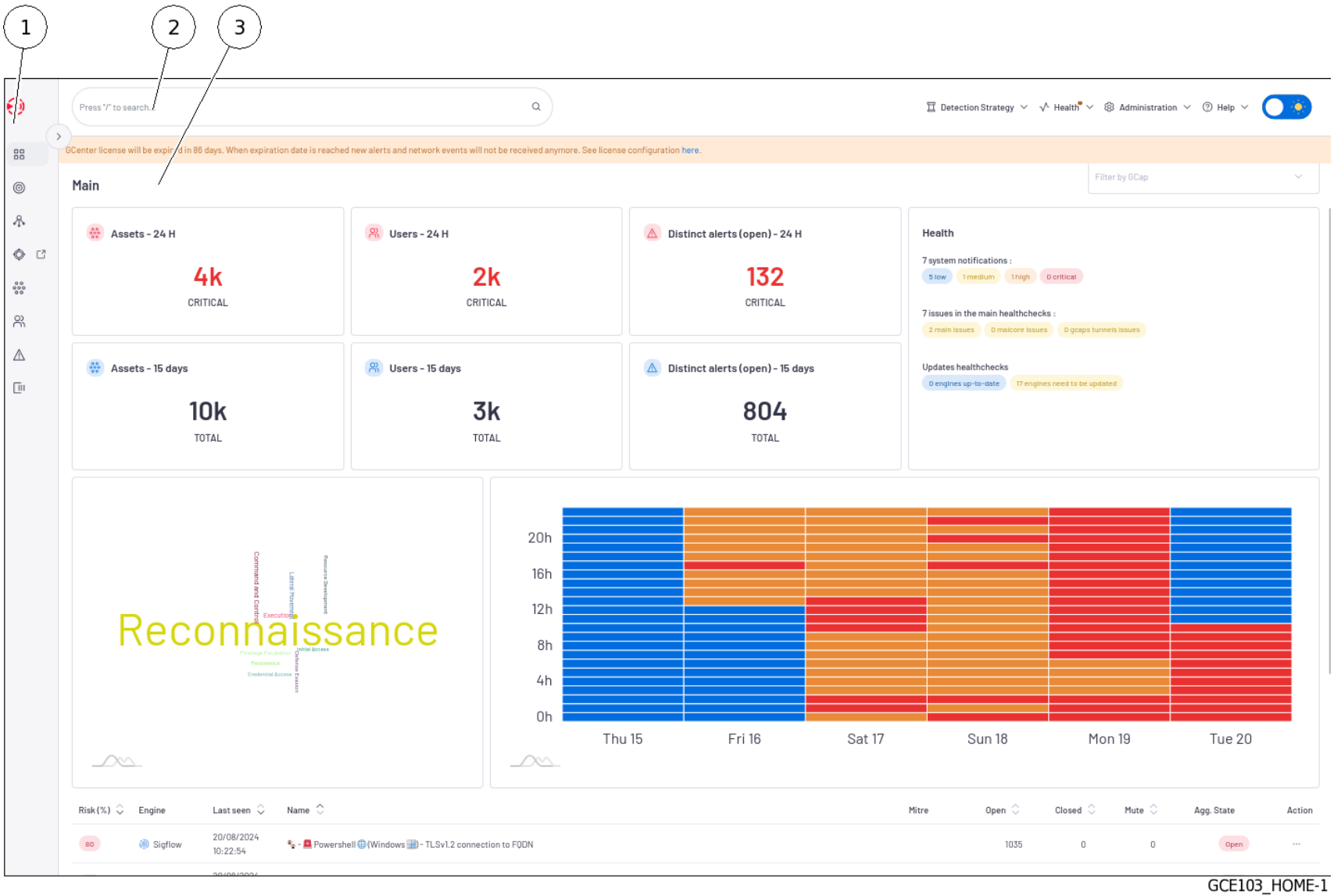
Each of these commands enables an action to be taken.
These commands are detailed in the table below, including links to the corresponding procedures.

Choice	Shortcut key	Explanation	See procedure
About	A	General information about the GCenter	*`About` command*.
Tech Support	T	Enables generating a diagnostic file	*`Tech Support` command*.
Keyboard	K	Enables modifying the keyboard	*`Keyboard` command*.
Authentication	P	Enables changing the password of the `setup` account	*`Authentication` command*.
DateTime	D	Enables changing the date and time of the GCenter.	*`DateTime` command*.
Network	N	Enables configuring the network section of the GCenter	*`Network` command*.
ARP Manager	A	Enables manually creating entries in the GCenter ARP table	*`Arp Manager` command*.
Diagnose	D	Enables diagnosing the network configuration of the GCenter	*`Diagnose` command*.
GCenter Services Management	G	Enables restarting or resetting certain GCenter services	*`GCenter Services Management` command*.
Elasticsearch storage mode	E	Enables modifying the storage mode for the alerts and the metadata.	*`Elasticsearch storage mode` command*.
LPM Mode	L	Enables switching the solution to LPM mode	*`LPM Mode` command*.
Restart	R	Enables restarting the GCenter	*`Restart` command*.
Shutdown	S	Enables switching off the GCenter	*`Shutdown` command*.
Reset	R	Enables restoring the GCenter to its "factory default" settings	*`Reset` command*.
Exit	E	Enables exiting the configuration menu	*`Exit` command*.

5.2 Overview of the WEB UI

Important:

This section describes the graphical elements available to members of the operator group.



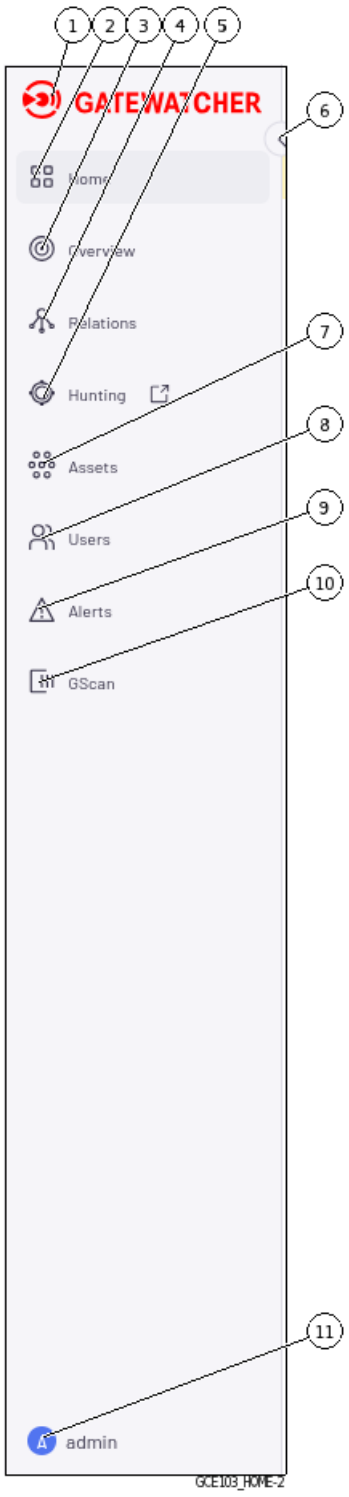
GCE103_HOME-1

The screen consists of following parts:

Item	Name	Description
1	*Navigation bar*	Displays the icons used to access the main functions
2	*Title bar*	Gives direct access to certain functions (search, visual theme...)
3	*Central screen*	Displays the screen selected by clicking on the icon in the navigation bar Each screen is named like the shareholder icon: example `Home` screen

5.2.1 Navigation bar

The navigation bar consists of buttons used to access the various functions.



Item	Button name	Display
1	GATEWATCHER logo	*WebUI `Home` screen*: opens the main dashboard
2	`Home`	*WebUI `Home` screen*: opens the main dashboard
3	`Overview`	*WebUI `Overview` screen*: opens the dashboard detailing the most significant risks for each item
4	`Relations`	*WebUI `Relations` screen*: opens the page showing the network mapping. This shows the relationships between the elements in the network
5	`Hunting`	*WebUI `Hunting` screen*: enables access to Kibana dashboards
6	icon `<`	Fold or unfold the menu
7	`Assets`	*WebUI `Assets` screen*: opens the page showing the characteristics of the active elements on the network
8	`Users`	*WebUI `Users` screen*: opens the page showing the characteristics of the users on the network
9	`Alerts`	*WebUI `Alerts` screen*: opens the page showing the characteristics of the displayed alerts
10	`Gscan`	*WebUI `GScan` screen*: opens the page to run a scan on a specific file
11	account name	*Management of the current account*: opens the menu to manage the account

5.2.2 Title bar

The title bar is located and consists of the following items:

Item	Name	Description
1	Search field	After entering the search text and validating, the system displays the results
2	Menu bar	See the *Overview of the menu bar*
3	Theme change button	Enables switching between the two light and dark themes

---

5.2.3 Central screen

The central screen displays the information selected by a button on the navigation bar.
By default, the `Main` screen is displayed.

5.3 Overview of the Kibana GUI

5.3.1 Overview of the Kibana GUI

The Kibana web interface displays the data present in the ElasticSearch indexes of the GCenter.
This data comes from different analysis engines.
Before GCenter indexing, this data can:

- Come from analyzes on the GCap side (alerts and metadata reported by the Sigflow detection engine)
- Come from analyzes on the GCenter side (alerts by the other detection engines)

Important:

This section describes the graphic elements accessible to members of the operator group.

5.3.2 Configuration of the Kibana GUI

The Kibana interface is fully editable by the user.
It is possible to create visualizations and dashboards.
Natively, the interface has pre-recorded dashboards to visualize the data of the different engines of the solution.
These dashboards are also editable by the user.
Different viewing rights apply to this interface:

- Users who are members of the group **operator** can view the data present in the detection event dashboards
- Users who are members of the group **administrator** can view the data present in the system dashboards (System logs)

Note:

Kibana interface access is available:
- For members of the operator group, by clicking on the `Hunting` button on the navigation bar
- For members of the administrator group, by clicking on the command `System logs` from the menu `Administration - Maintenance`

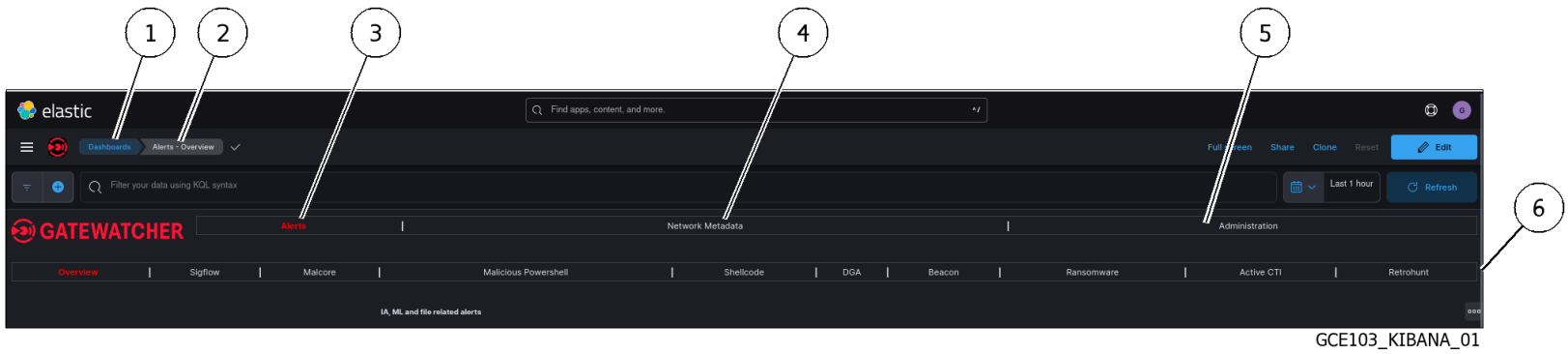
The `Dashboards` button (1) enables to display and to select the existing dashboards.
The `Alerts - Overview` (2) is the default dashboard for members of the operator group.

5.3.3 Main tabs

There are main tabs:

- `Alerts` tab (3) : displays the Alert dashboards created by the detection engines (see *Native dashboards of the `Alerts` tab*)
  The native dashboards (6) of the `Alerts` tab (3) are displayed below.
- `Network Metadata` tab (4) : displays the network dashboards (see *Native dashboards of the `Network Metadata` tab*)
- `Administration` (5): displays the Administration dashboards (see *Native dashboards of the `Administration` tab*)

5.3.4 Native dashboards of the `Alerts` tab



GCE103_KIBANA_01

The `Alerts` information of the different engines is grouped in the Kibana interface as tabs (6):

Tab	Displays all alerts generated by the
`Overview	GCenter
`Sigflow`	Sigflow engine
`Malcore`	Malcore engine
`Malicious Powershell`	Malicious Powershell detect engine
`Shellcode`	Shellcode detect engine
`DGA`	DGA detect engine
`Beacon`	Beacon detect engine
`Ransomware`	Ransomware detect engine
`Active CTI`	Active CTI engine
`Retro hunt`	Retro hunt engine

Note:

For most dashboards, the following pages are available:
- `Overview`
- `Messages`

Each of these tabs corresponds to a specific type of data, here is the detail:

- a graph showing the number of alerts per engine over time
- a counter displaying the number of alerts per engine, the number of metadata and the number of files scanned
- a top 10 source IP addresses by type of alert
- a top 10 destination IP addresses by type of alert
- a graph showing the proportion of the different severity of Sigflow alerts
- a graph showing the number of unique signatures that escalated alerts over time

- a list of Malcore alerts identified by the solution (in the form of a message)
- a top 10 alerts
- a top in the distribution of DGA domain names
- Top 10 Machine Learning Alerts

The main view `Overview` shows different graphs and statistics for the selected time slot.

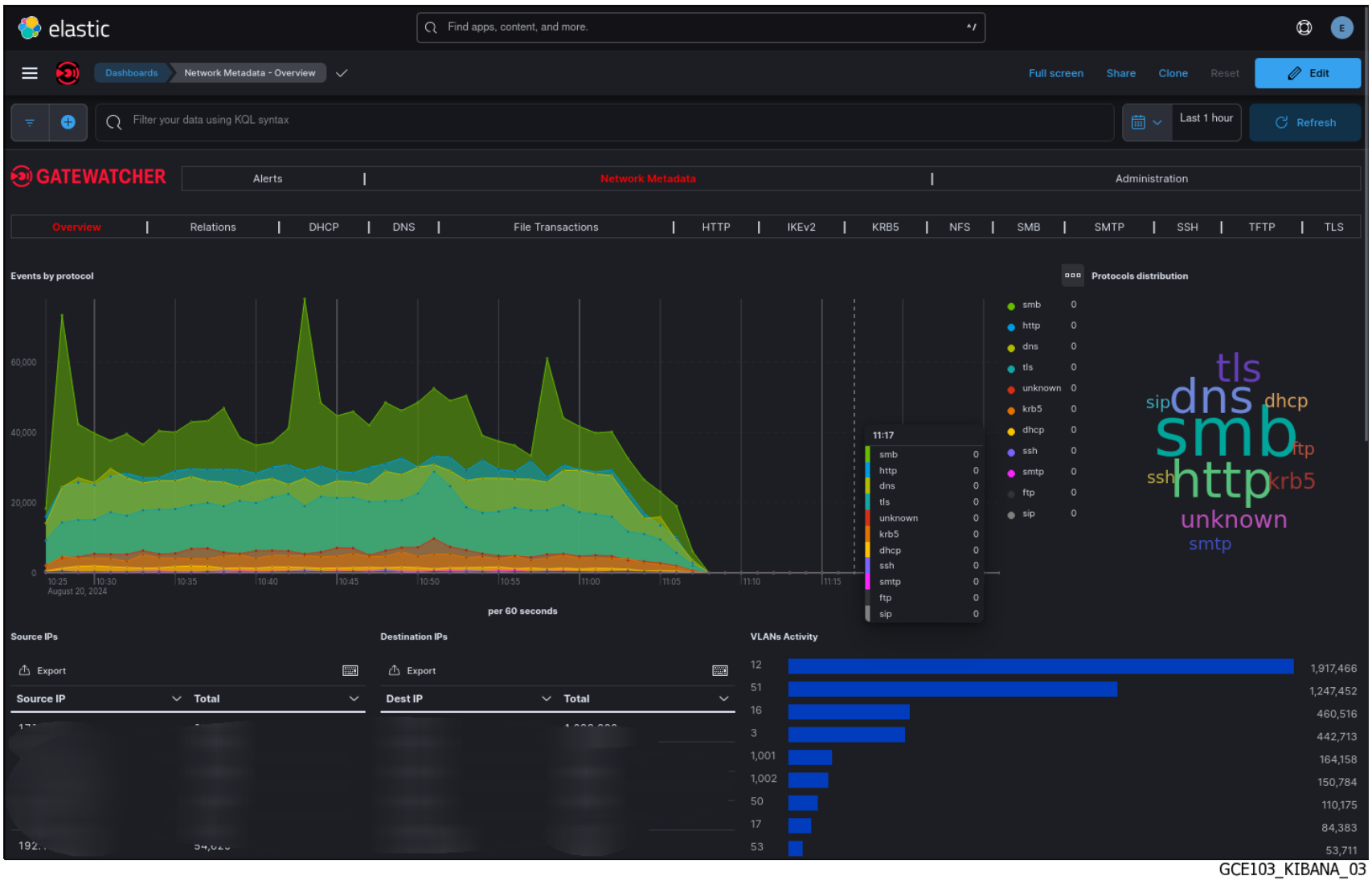
It also contains an explanatory paragraph on Malicious Powershell alerts.
Click on `Messages` to display the list of alerts.

The secondary view `Messages` shows a histogram and the list of alerts.
The histogram shows the distribution of alerts over the selected time range.
It can notably reveal a certain periodicity of alerts, or a particularly active time of day.
The list of alerts can be modified by deleting or adding certain columns.

Click on the «double arrow» icon at the beginning of the line to display all the alert fields.
It is then possible to filter on certain values for, for example:

- Do not display healthy machines (filter false positives)
- Show only alerts from a particular IP
- Do not display alerts from a specific GCap

5.3.5 Native dashboards of the `Network Metadata` tab



GCE103_KIBANA_03

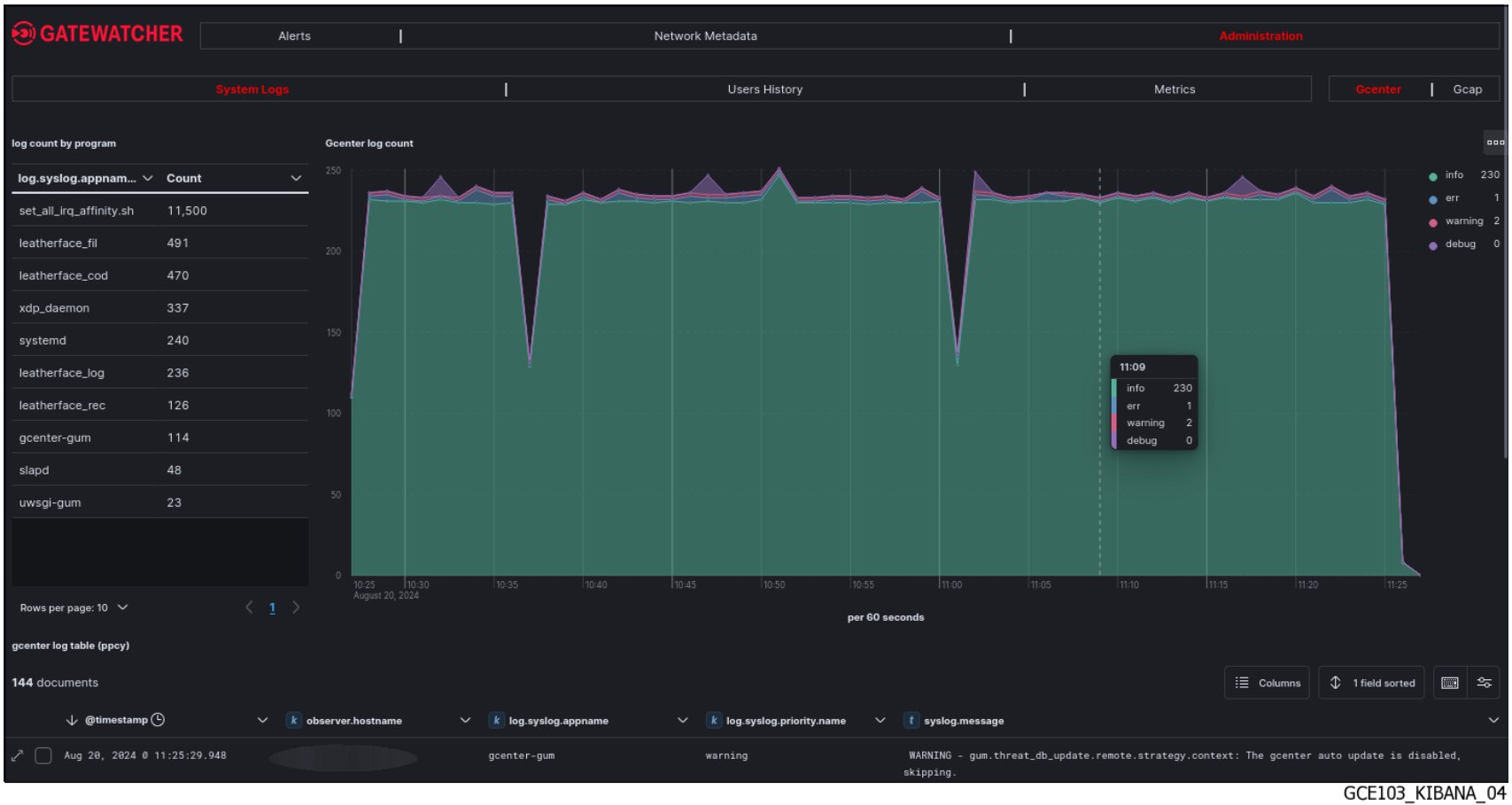
`Network Metadata` displays, in sub-tabs, the metadata for the different protocols analyzed by the GCap:

- Overview synthesizes all metadata
- Relations synthesizes all metadata into visualizations in chart form
- DHCP, DHCP metadata details
- DNS, DNS metadata details
- File Transaction, details of the metadata related to the file reconstructed by the probe
- HTTP, HTTP metadata details
- IKEv2, IKEv2 metadata details
- KRB5, KRB5 metadata details
- NFS, NFS protocol metadata details
- SMB, SMB metadata details
- SMTP, SMTP metadata details
- SSH, SSH metadata details
- TFTP, TFTP metadata details
- TLS, TLS metadata details

Attention:

Some protocols do not have a native dashboard despite the fact that they can generate metadata.
These metadata are still indexed and usable in Kibana.

5.3.6 Native dashboards of the `Administration` tab



GCE103_KIBANA_04

The native dashboards are grouped in the Kibana interface as tabs.
The `Administration` tab displays, in sub-tabs, the information grouped by theme:

- `System Logs` displays the syslog system events
- `Users History` displays the Users history events
- `Metrics` displays the Administration metrics

5.3.7 Data exploitation

In each dashboard, it is possible to perform a filtering to display only the desired data.
To do this, several options are possible:

- Filter by changing the time interval (top right of page)
- Filter by searching using the `Search` bar (top left)
- Filter by creating a filter on a specific field of the desired events (button `+ Add filter` below the search bar)

5.4 The legacy WebUI

5.4.1 Overview of the legacy WebUI

This interface is the traditional interface of the solution, also referred to as the legacy WebUI.
It consists of all the configuration menus.
When connecting to the GCenter, the interface displayed is the main WebUI and not the traditional interface.
To access it:

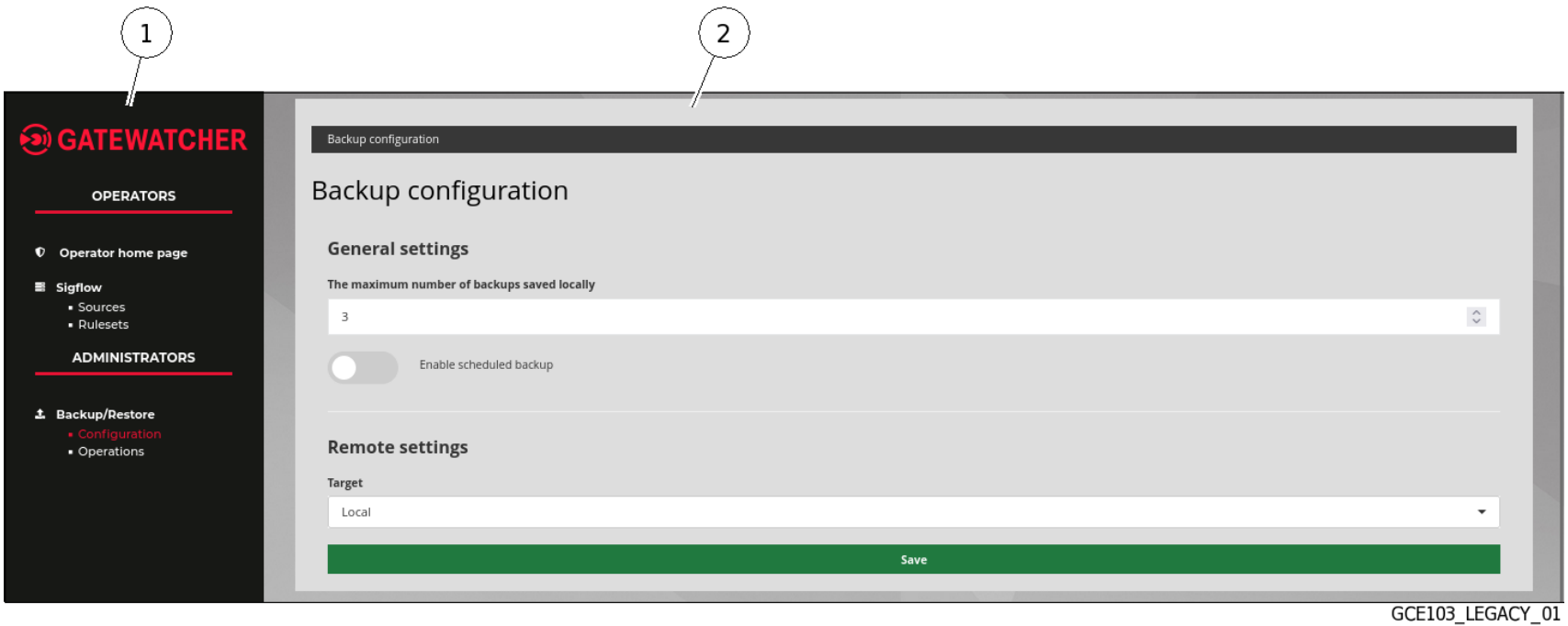
- Click on the `Administration` button in the navigation bar at the bottom left of the page and select the `Backup and restore` menu
- Click on the `Detection strategy` button in the navigation bar at the bottom left of the page and select the `Sigflow rules manager` menu

In this interface, most of the menus are not accessible to a user member of the operator group.
The only menus accessible to members of the operator group are the following:

- Sigflow > Sources
- Sigflow > Rulesets

All other menus are only accessible to members of the administrator group.

5.4.2 Description of the legacy WebUI



GCE103_LEGACY_01

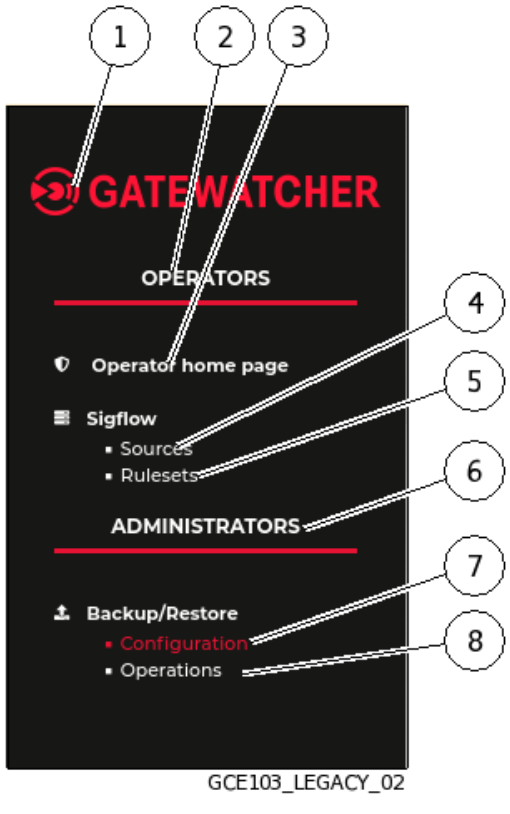
The screen consists of following parts:

Item	Name	Display
1	*Navigation bar of the legacy WebUI*	Displays the menus and commands for accessing the main functions
2	Central screen	Displays the screen selected by pressing a command on the navigation bar

---

5.4.2.1 Navigation bar of the legacy WebUI

The navigation bar consists of buttons used to access the various functions.
This section provides access to the security policy management functions of the Sigflow engine



GCE103_LEGACY_02

Item	Name	Display
1	GATEWATCHER logo	*WebUI `Home` screen* : the use of the button enables returning to the main interface if rights are enabled
2	`OPERATORS`	For members of the administrator group: these commands are visible but not authorized. For members of the operator group: these commands are activated. This section includes the following items: - The `Operator home page` command (3): this enables returning to the main interface (*WebUI `Home` screen*) - The `Sigflow` menu includes the following commands: - The `Source` command (4) manages the sources (*`Sources` screen*) - The `Rulesets` command (5) manages the rulesets (*`Rulesets` screen*)
6	`ADMINISTRATORS`	For members of the operator group: these commands are visible but not allowed. For members of the administrator group: this section enables access to all administration menus. This section includes the `Backup/Restore` menu includes the following commands: - The `Configuration` command (7) configures the backup (*`Configuration` screen*) - The `Operations` command (8) operates the backup (*`Backup operations` screen*)

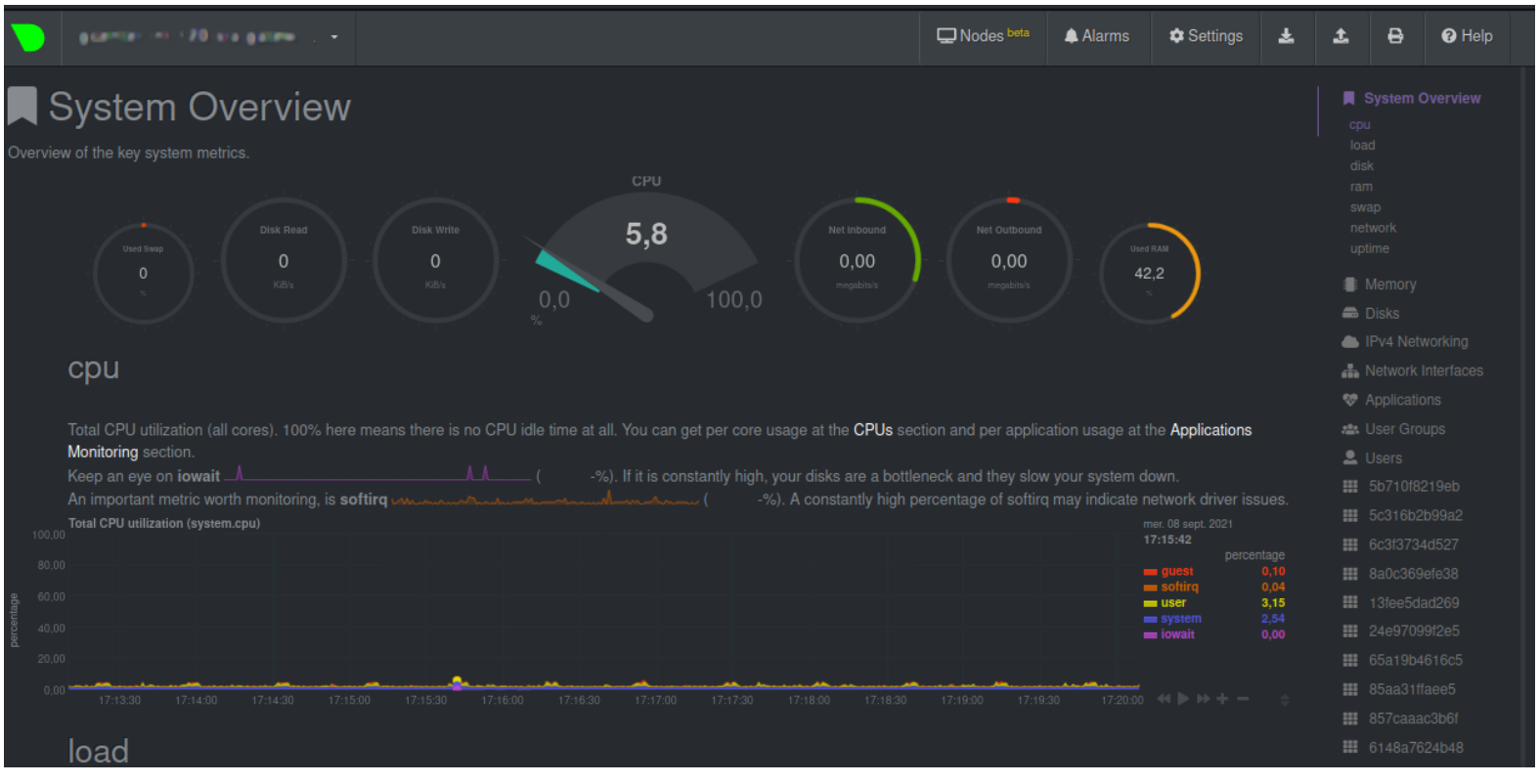
5.5 Overview of the Netdata User Interface (Gstats)

The GCenter retrieves the GCap metrics.

The GCap and the GCenter metrics are transmitted via Netdata to the Netdata server present on the GCenter.

The GCenter Gstats interface uses this data and allows to visualize it for an analysis of the state and consumption of the various physical and software components.

Access to this Gstats interface is available with the `Advanced metrics` command of the `health` menu.



This Gstats interface provides administrators with a large number of metrics on different devices.

It is possible via the menu at the top of the page to select the equipment to be administered such as **GCenter** but also the paired GCaps.

Note:

Alternatively, this data will also be available from Kibana in tabs (or dashboards) accessible from the `Kibana` Dashboards menu.

See the *`Advanced metrics` screen of the Netdata User Interface (Gstats)*.

Note:

Only administrators have access to this interface.

5.6 Screens of the WebUI navigation bar

5.6.1 WebUI `Home` screen

5.6.1.1 Introduction

The `Home` screen is the main screen which shows the detection results

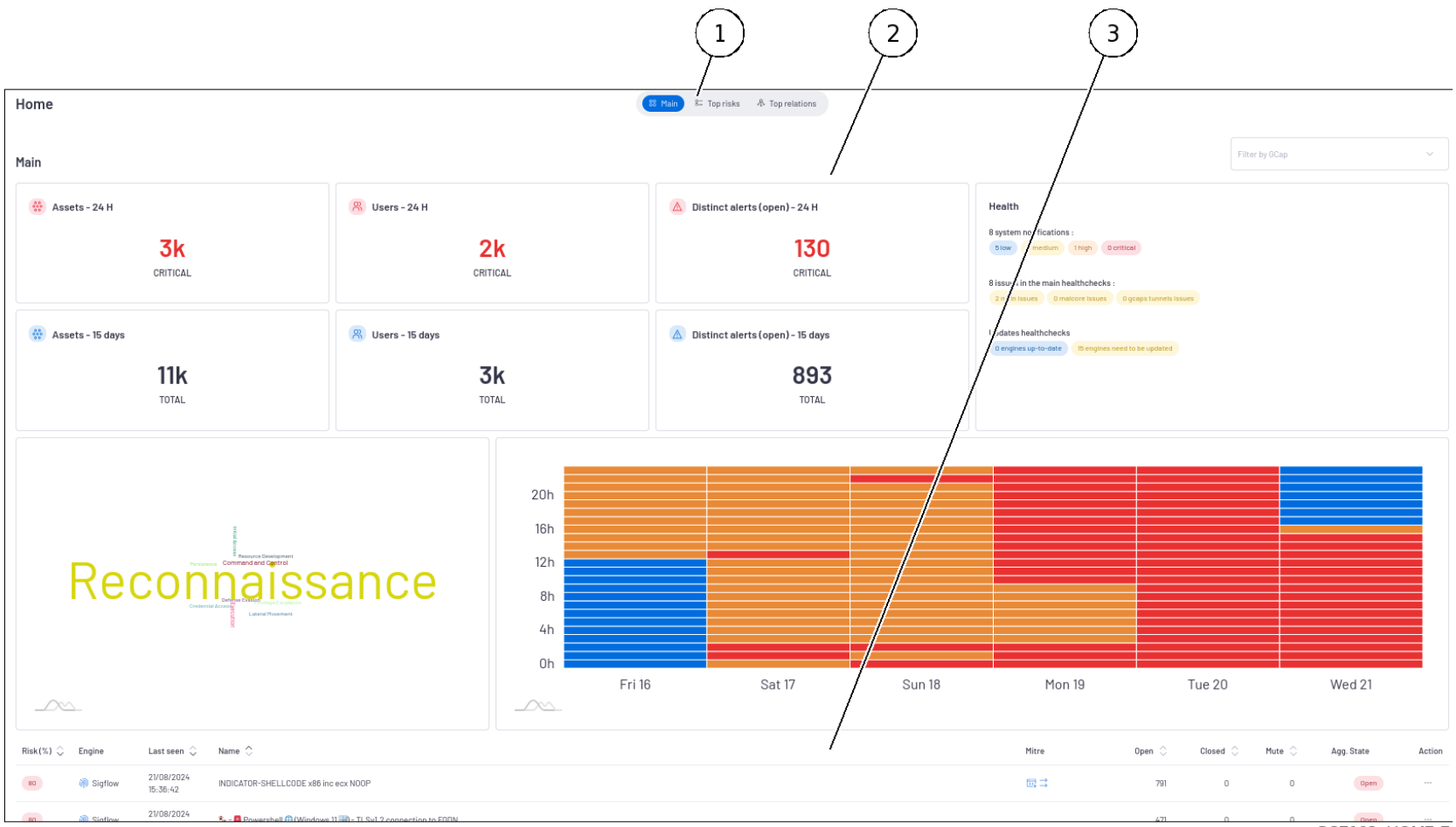
---

5.6.1.2 Links associated

None

5.6.1.3 Screen description

After pressing one of the `Home` or `GATEWATCHER` buttons on the navigation bar, the `Home` screen is displayed.
It includes the following items:



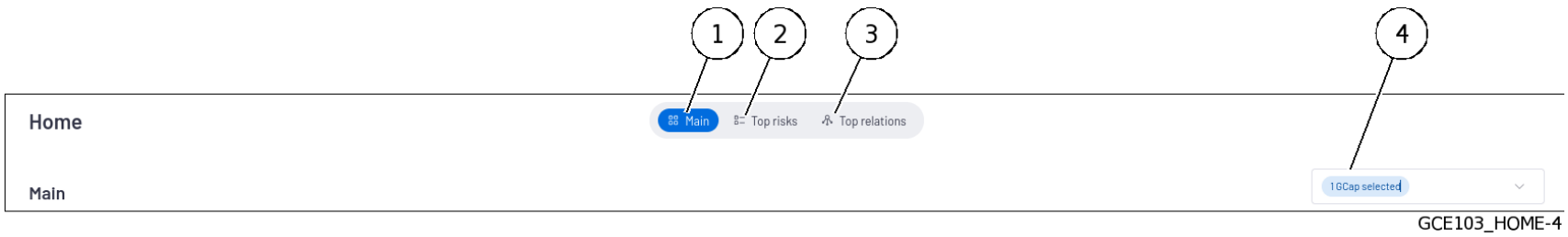
GCE103_HOME-7

Item	Description
1	*`Home` screen dashboard selector*
2	*`Main` screen display area*
3	*`Home` screen message area*

5.6.1.3.1 `Home` screen dashboard selector

The screen displays a set of:

- A button to select the GCap whose information is displayed
- Three buttons to set the theme of the items displayed



GCE103_HOME-4

Item	Name	Description	See
1	`Main`	Selection of the default display	*`Main` screen display area*
2	`Top risks`	Selection of the main risk screen	*WebUI `Top risk` screen*
3	`Top relations`	Selection of the main relationships screen	*WebUI `Top Relations` screen*
4	Display of selected GCaps	Selection of GCaps	

5.6.1.3.2 `Main` screen display area

After pressing one of the `Home` or `GATEWATCHER` buttons, the display area looks like this:

GCE103_HOME-5

The display shows the information of the selected GCap(s).
The screen provides a summary of the detection status:

- The area indicating the number of potential risks by type and date (item 1 to 6)
  These elements forming this zone are listed below:
  - `Assets` zones (1) and (2)
    The assets are the active equipment on the network
    The zone indicates the number of alerts and the threat level
    - The `Assets-24 H` zone (1) gives the number of risks **critical** appeared in the last 24 hours

- The `Assets-15 days` zone (2) gives the total number of alerts appeared in the last 14 days

> **Note:**
> If you press this counter then the system displays the detailed list of alerts (`Assets` screen).

- `Users` zones (3) and (4)
  The users are the different users present on the network.
  The zone indicates the number of alerts and the threat level
  - The `Users-24 H` zone (3) gives the number of risks **critical** appeared in the last 24 hours
  - The `Users-15 days` zone (4) gives the total number of alerts appeared in the last 14 days

> **Note:**
> If you press this counter then the system displays the detailed list of alerts (`Users` screen).

- `Distinct alerts (open)` zones (5) and (6)
  The zone indicates the number of alerts and the threat level: the alerts counted are the separate alerts (grouped by name and whose status is open)
  - The `Distinct alerts (open)-24 H` zone (5) gives the number of risks **critical** in the last 24 hours
  - The `Distinct alerts (open)-15 days` zone (6) gives the total number of alerts appeared in the last 14 days

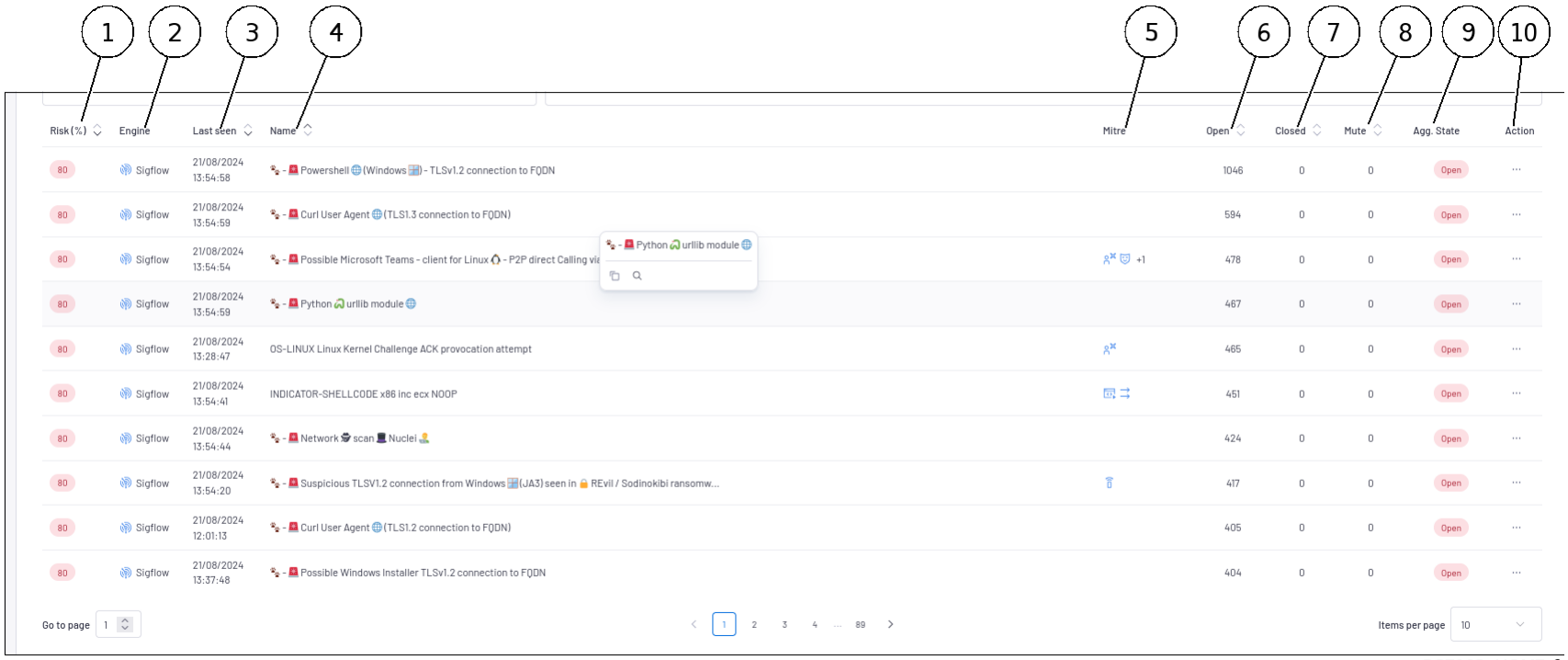
> **Note:**
> If you press this counter then the system displays the detailed list of alerts (`Alerts` screen).

- The area indicating the date of detection (8): this calendar indicates when potential threats have been detected.
  If pressed, then the system displays the `Alerts` date filtering page (see *WebUI `Alerts` screen*).
- The MITRE association area (9).
  If pressed, then the system displays the `Alerts` MITRE filtering page (see *WebUI `Alerts` screen*).

5.6.1.3.3 Threat level

- Threat level classified as **Critical risk**:
- Definition of a **critical risk**: very suspicious activity was detected. Dangerous activity was detected. There is a high probability that your organization is facing a serious threat and counter-meseares should be taken immediately.
  For example, a user downloaded malware or an active network element contacted a known command and control domain.
- Definition of the color used for this type of alarms in the WebUI: red
- Risk level of this category: 75 to 100%
- Threat level classified as **High risk**:
- Definition of a **high risk**: a very suspicious activity has been detected. This type of event should be investigated promptly as it could be a sign of significant compromise.
  It is possible that this event is a false positive or related to a bad representation in the network.
- Definition of the color used for this type of alarms in the WebUI: orange
- Risk level in this category: 50-74%
- Threat level classified as **Medium risk**:
- Definition of a **medium risk**: an activity that could be related to a threat has been detected.
  The risk has been established at low values because the potential threat does not appear critical or because the probability of false is high.
- Definition of the color used for this type of alarms in the WebUI: yellow
- Risk level in this category: 25-49%
- Threat level as **low risk** have no counter displayed:
- Definition of a **low risk**: unusual activity has been detected. This could mean that you have unusual network policies or uses.
  These types of events should be mentioned last because they are not a direct sign of significant compromises.
- Definition of the color used for this type of alarms in the WebUI: blue
- Risk level for this category: 0-24%

5.6.1.3.4 `Home` screen message area



GCE103_HOME-6

The list of messages displays the 10 aggregate threats with the highest level of risk.
This area gives the following information:

Benchmark	Name	Description
1	`Risk	If you press the icon then the Alerts window displays the selected alerts and shows all alerts with the same filter (Name)
2	`Engine`	displays the engine which has detected this threat
3	`Last seen`	Date and time of last appearance
4	`Name`	Name of alert
5	`MITRE`	Type of threat icon: see *MITRE Icons* paragraph
6	`Open`	Number of alarm occurrences with the opened state
7	`Closed`	Number of alarm occurrences with the closed state
8	`Mute`	Number of alarm occurrences with the muted state
9	`Agg state`	Group by name state: `Open`` means that this state is disabled
10	`Action`	Displays `actions` sub menu This submenu is detailed in the Alerts screen

Pressing a threat opens the `Alerts` window that displays threats with the same infection as the selected infection.

5.6.1.3.5 MITRE Icons

In the MITRE column, the following icons can be displayed:

Icon	Name	Description of threat type	see more information
	Execution	Opponent is trying to execute malicious code.	https://attack.mitre.org/versions/v10/tactics/TA0002/
	Persistence	Opponent trying to maintain hold	https://attack.mitre.org/versions/v10/tactics/TA0003/
	Privilege Escalation	Opponent trying to get higher level permissions	https://attack.mitre.org/versions/v10/tactics/TA0004/
	Defense Evasion	The opponent tries to avoid being detected.	https://attack.mitre.org/versions/v10/tactics/TA0005/
	Lateral Movement	The opponent tries to move around your environment.	https://attack.mitre.org/versions/v10/techniques/T1210/

5.6.2 WebUI `Top risk` screen

5.6.2.1 Introduction

The `Top risk` screen displays the threats with the highest level of risk.

5.6.2.2 Links associated

None

5.6.2.3 Screen description

After pressing one of the `Main` buttons and then the `Top risks` button, the following screen is displayed.

GCE103_TOP-RISK_1

This screen includes the following:

Item	Zone	To display
1	*`RISK TIMELINE` zone*	Alarm timing and risk levels
2	*`ASSETS` zone*	List of found active equipment
3	*`ASSETS RISK` zone*	Representation of the number of alerts filtered by active equipment
4	*`STATS` zone*	Statistics on detected threats
5	`Filter by GCap` and Calendar fields	Selection of the GCap and range time to filter information
6	*`USERS RISK` zone*	Representation of the number of alerts filtered by active users

---

5.6.2.3.1 `RISK TIMELINE` zone

The `RISK TIMELINE` zone indicates the alarm sequence and their risk levels:

- Horizontal axis: date and time of threat occurrence
- Vertical axis: risk level
- Each threat is placed on the graph, its size indicating the number of alerts.

  Hovering over the threat displays the following:

- Hostname
- IP
- Risk
- Alert count
- Date
- MITRE threat type

5.6.2.3.2 `ASSETS` zone

The `ASSETS` zone displays the list of active equipment found in the detected threats.
By clicking on each equipment, the `Assets` window is displayed on that equipment.

5.6.2.3.3 `ASSETS RISK` zone

The `ASSETS RISK` zone displays the number of alerts of active equipment in the form of a bubble.
The size of the bubble depends on the number of alerts on this equipment.
By clicking on an equipment, the `Assets` detailed window is displayed on that equipment.

5.6.2.3.4 `STATS` zone

The `STATS` zone displays the following counters:

- `Hostnames`
- `@mac`
- `Users`
- `OS`
- MITRE counters:
  - `Execution`
  - `Persistence`
  - `Privilege Escalation`
  - `Defense Evasion`
  - `Lateral Movement`

  If a counter is pressed, the system displays a detailed list of each of these risks (`Alerts` screen).

5.6.2.3.5 `USERS RISK` zone

The `USERS RISK` zone displays the number of active user alerts as bubbles.

5.6.3 WebUI `Top Relations` screen

5.6.3.1 Introduction

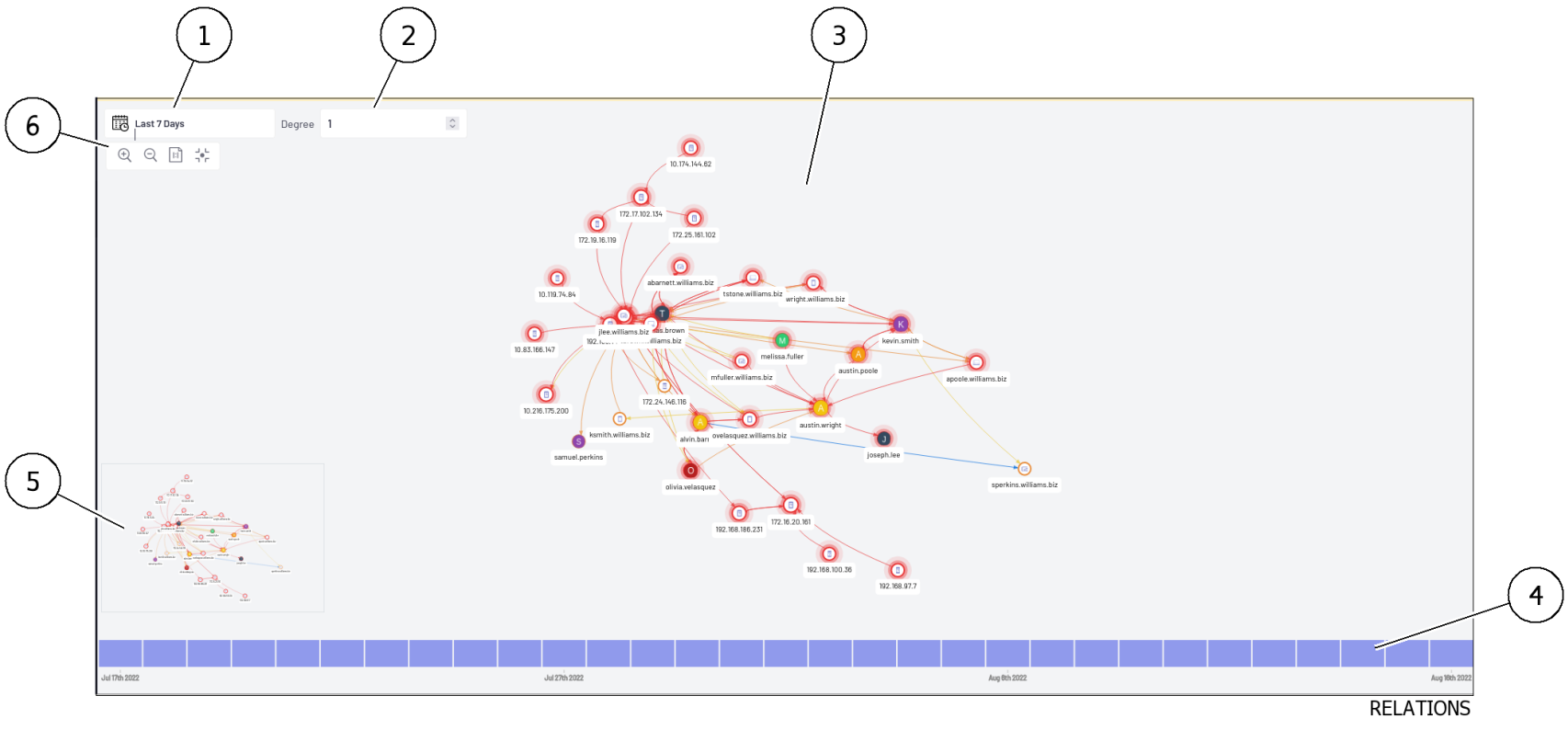
This screen shows the equipment on the network and the relationships between them.

5.6.3.2 Links associated

This screen is detailed in the *WebUI `Relations` screen*.

5.6.3.3 Screen description

After pressing one of the `Main` buttons and then the `Top Relations` button, the following screen is displayed.



5.6.4 WebUI `Overview` screen

5.6.4.1 Introduction

The `Overview` screen displays the found threats sorted by:

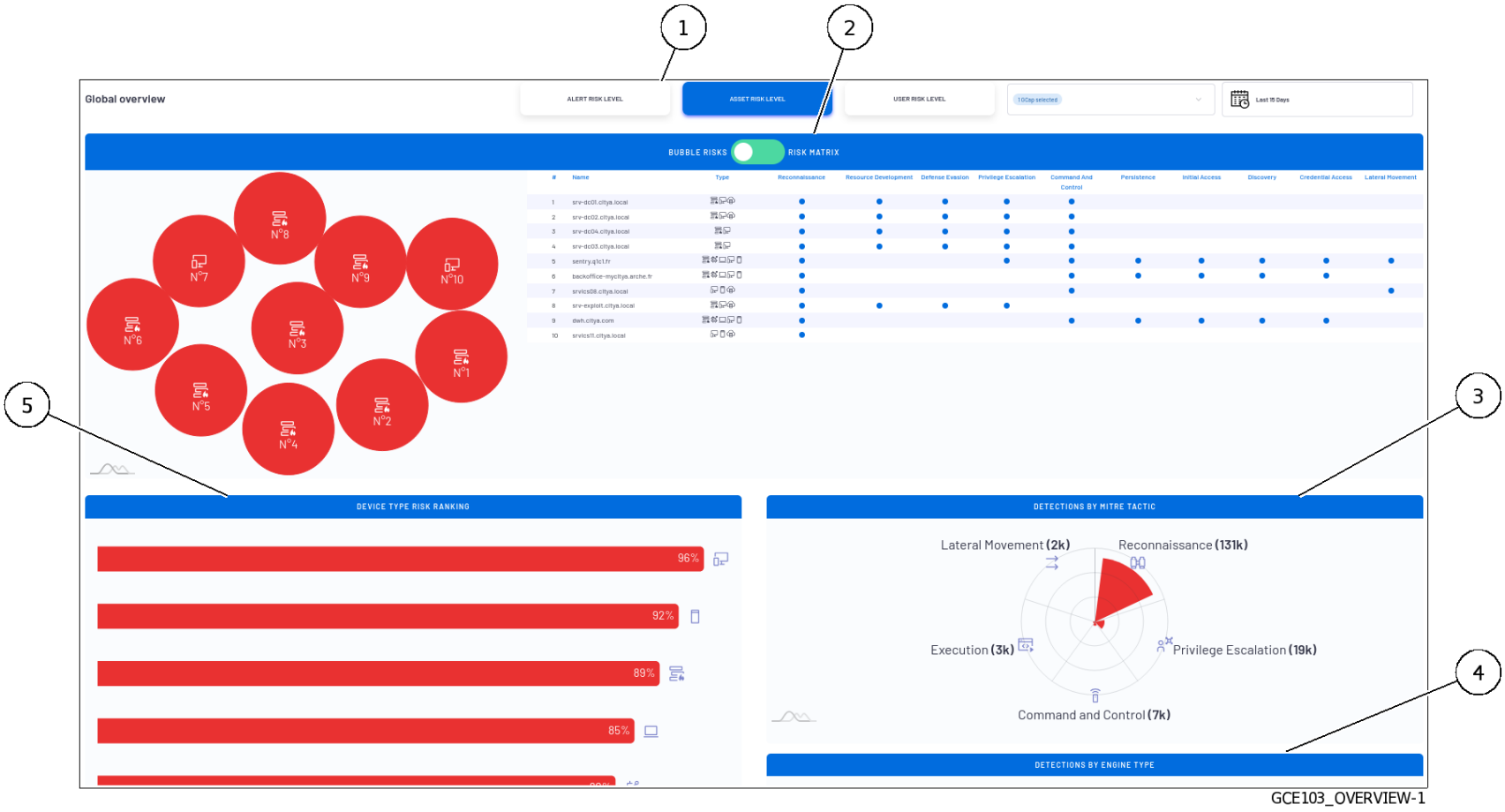
- Alert Risk Level
- Risk level of assets
- User Risk Level

5.6.4.2 Links associated

None

5.6.4.3 Screen description

After pressing the `Overview` buttons on the navigation bar, the `Overview` screen is displayed.
It includes the following items:



GCE103_OVERVIEW-1

Item	Description
1	*`Overview` screen : dashboard selector*
2	*`Overview` screen: alerts list display area*
3	*`Overview` screen: `DETECTIONS BY ENGINE TYPE` area*
4	*`Overview` screen: `DETECTIONS BY MITRE TACTIC` area*
5	*`Overview` screen: `ALERTS TYPE RISK RANKING` area*

5.6.4.3.1 `Overview` screen : dashboard selector

OVERVIEW_REP1

The screen displays a set of:

- One button (4) to select the GCap(s) whose information is displayed
- One button (5) for the period for which the information is displayed
- Three buttons (1 to 3) to define the theme of the dashboards displayed on this page

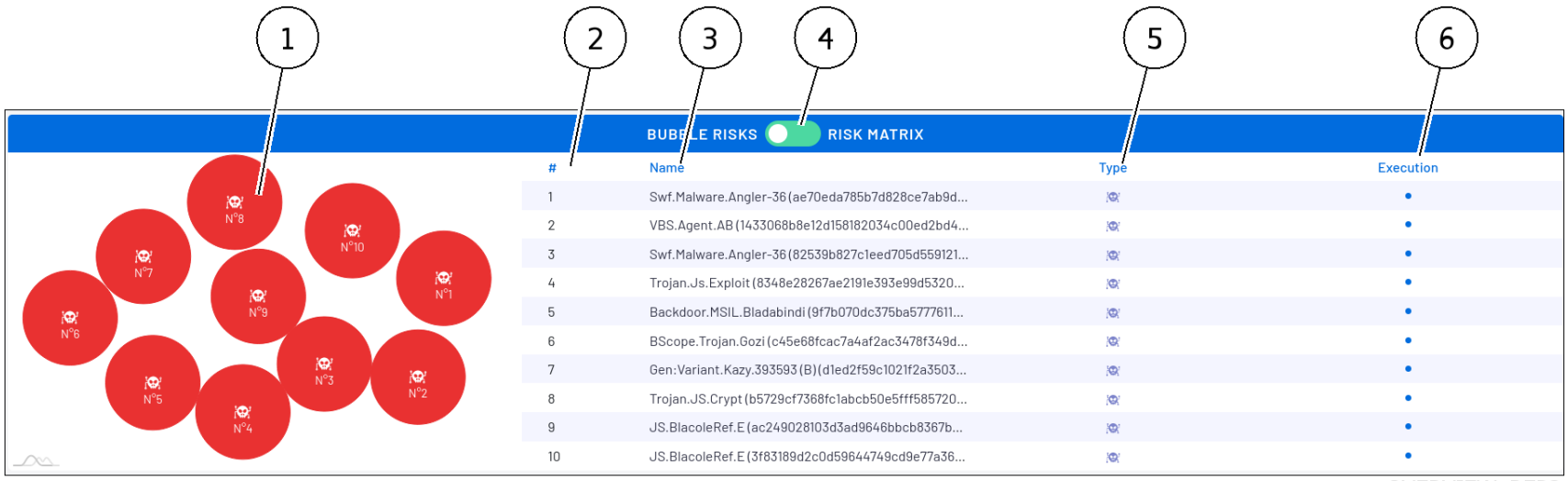
Item	Name	Description
1	`ALERT RISK LEVEL`	Alert Risk Level. Defines `ALERTS` theme for dashboards
2	`ASSET RISK LEVEL`	Risk level of assets. Defines the `ASSET` theme for dashboards
3	`USER RISK LEVEL`	User Risk Level . Defines the `USER` theme for dashboards
4	Gcap selector	Selection of the GCap
5	Time period selector	Selection of the display period

5.6.4.3.2 `Overview` screen: alerts list display area

The display of the alerts is possible in 2 ways selectable by the button (4):

- Display `BUBBLE RISKS`
- Display `RISK MATRIX`

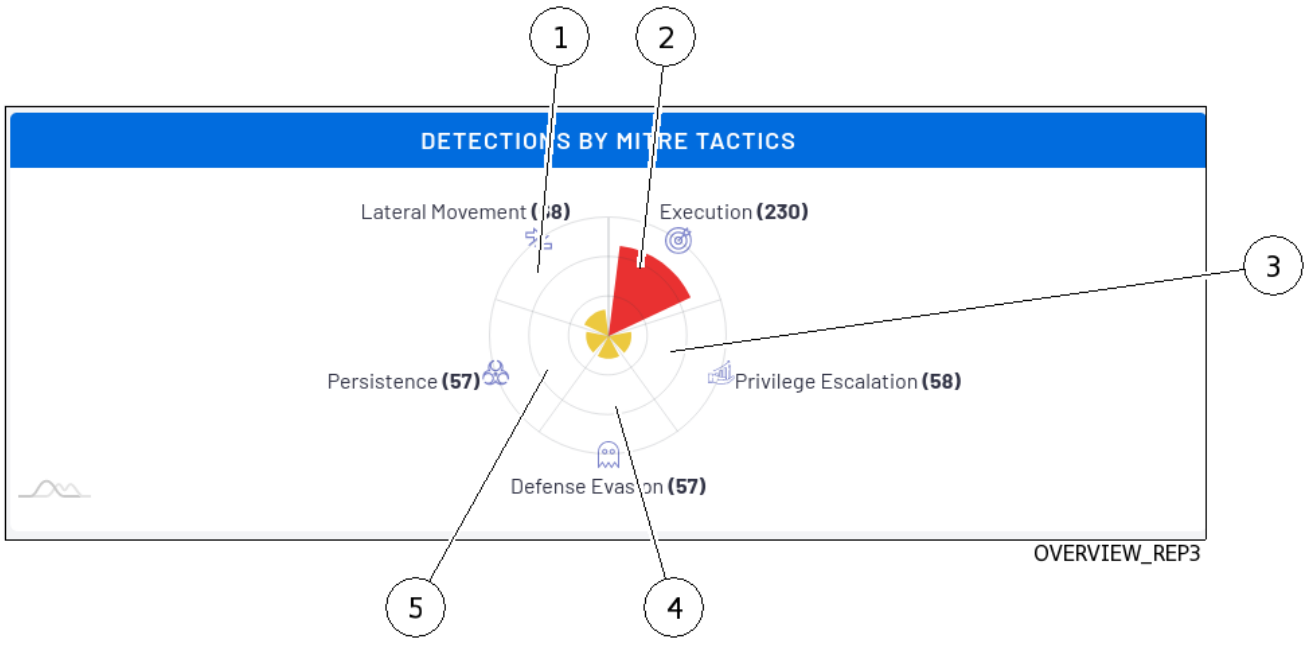
For the ALERTS theme, the `BUBBLE RISKS` display consists of:



OVERVIEW_REP2

Item	Description
1	Bubble zone. Each element (here an alert) is displayed as a bubble. Each item is numbered and corresponds to the list displayed next to it. By hovering over an element, a window gives additional information. - Number, not Alert - Risk: percentage level of risk - Alert counter - type of MITRE alerts
2	Alert number
3	Name of detected threat By hovering over an element, a window gives the same additional information. By clicking on the name, the system displays the `Alerts` screen for the selected threat for more information.
4	Display change button (bubbles/matrix)
5	`Type` field: type of risk (malware...)
6 and following	Each column indicates the category MITRE (`Execution`, `Persistence`, `Privilege Escalation`, `Defense Evasion`, `Lateral Movement`). Each point defines the threat category.

5.6.4.3.3 `Overview` screen: `DETECTIONS BY MITRE TACTIC` area



The system displays the distribution of risks between the following categories in a circular fashion:

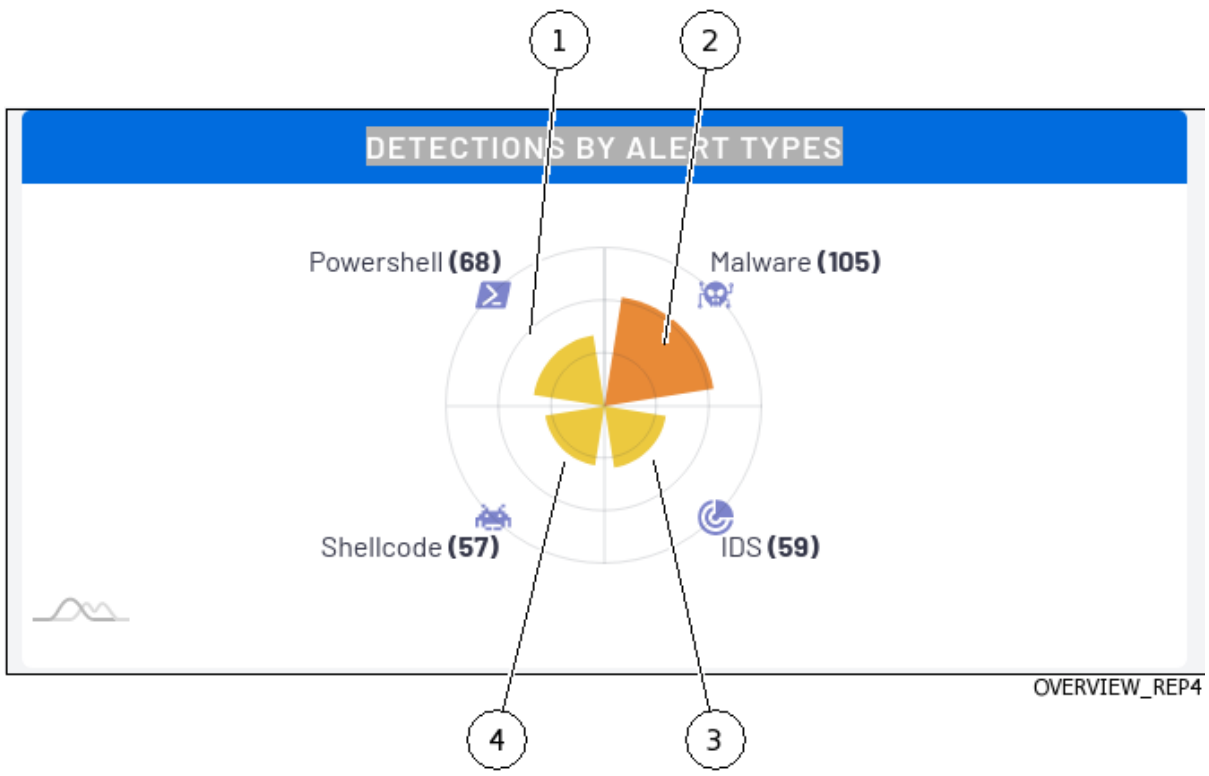
Benchmark	Name	Description
1	`Lateral Movement`	Number of lateral movements
2	`Execution`	Number of threats executed
3	`Privilege Escalation`	Number of privilege escalation
4	`Defense Evasion`	Number of defensive escapes
5	`Persistence`	Number of persistent threats

Note:

Depending on the threat, only the categories present are displayed.

Icon	Name	Description of threat type	see more information
	Execution	Opponent is trying to execute malicious code.	https://attack.mitre.org/versions/v10/tactics/TA0002/
	Persistence	Opponent trying to maintain hold	https://attack.mitre.org/versions/v10/tactics/TA0003/
	Privilege Escalation	Opponent trying to get higher level permissions	https://attack.mitre.org/versions/v10/tactics/TA0004/
	Defense Evasion	The opponent tries to avoid being detected.	https://attack.mitre.org/versions/v10/tactics/TA0005/
	Lateral Movement	The opponent tries to move around your environment.	https://attack.mitre.org/versions/v10/techniques/T1210/

5.6.4.3.4 `Overview` screen: `DETECTIONS BY ENGINE TYPE` area



The system displays a circular risk breakdown between the following categories:

Benchmark	Name	Description
1	`Powershell`	Number of powershells detected
2	`Malware`	Number of shellcodes detected
3	`IDS`	Number of malware detected
4	`shellcode`	Number of IDS detected

5.6.4.3.5 `Overview` screen: `ALERTS TYPE RISK RANKING` area

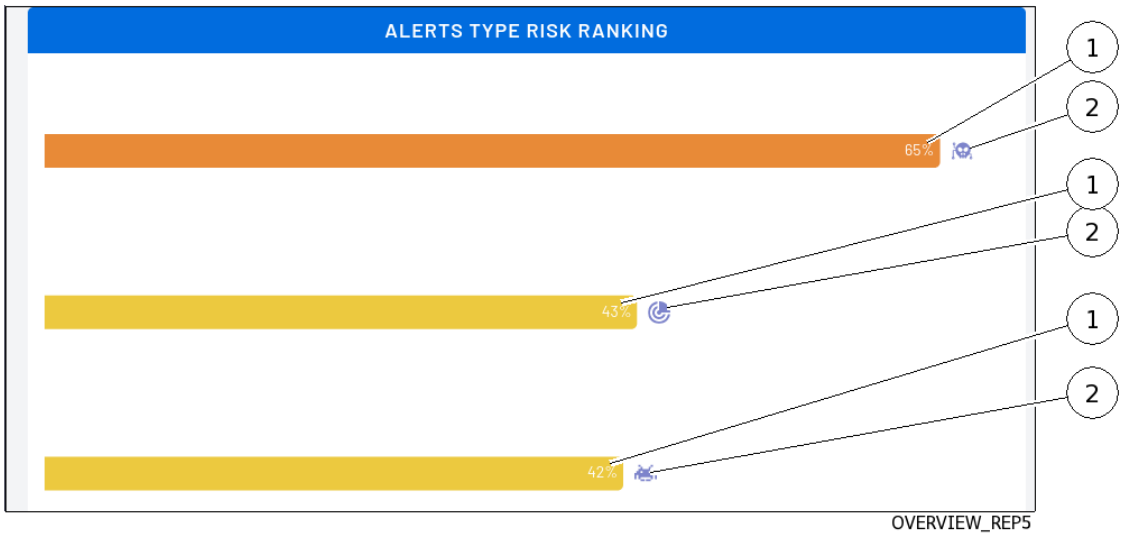
The system displays the risks:

- Grouped by type of alert
- Sorted by decreasing risk level

Each bar of the graph indicates the percentage of the risk and the type of alert.
Passing the cursor, the system displays:

- The type of alert
- The percentage of risk
- The number of alerts

By clicking on the bar, the system displays the information defined in the `Alerts` screen for the selected risk type.
In the example below, the window displays the following information:



Item	Name	Description
1	Percentage for this type of alert	Indicates the probability that this likely risk is real
2	Alert type	Alert type `Malcore`, `Sigflow`, `Malicious PS` ...

5.6.5 WebUI `Relations` screen

5.6.5.1 Introduction

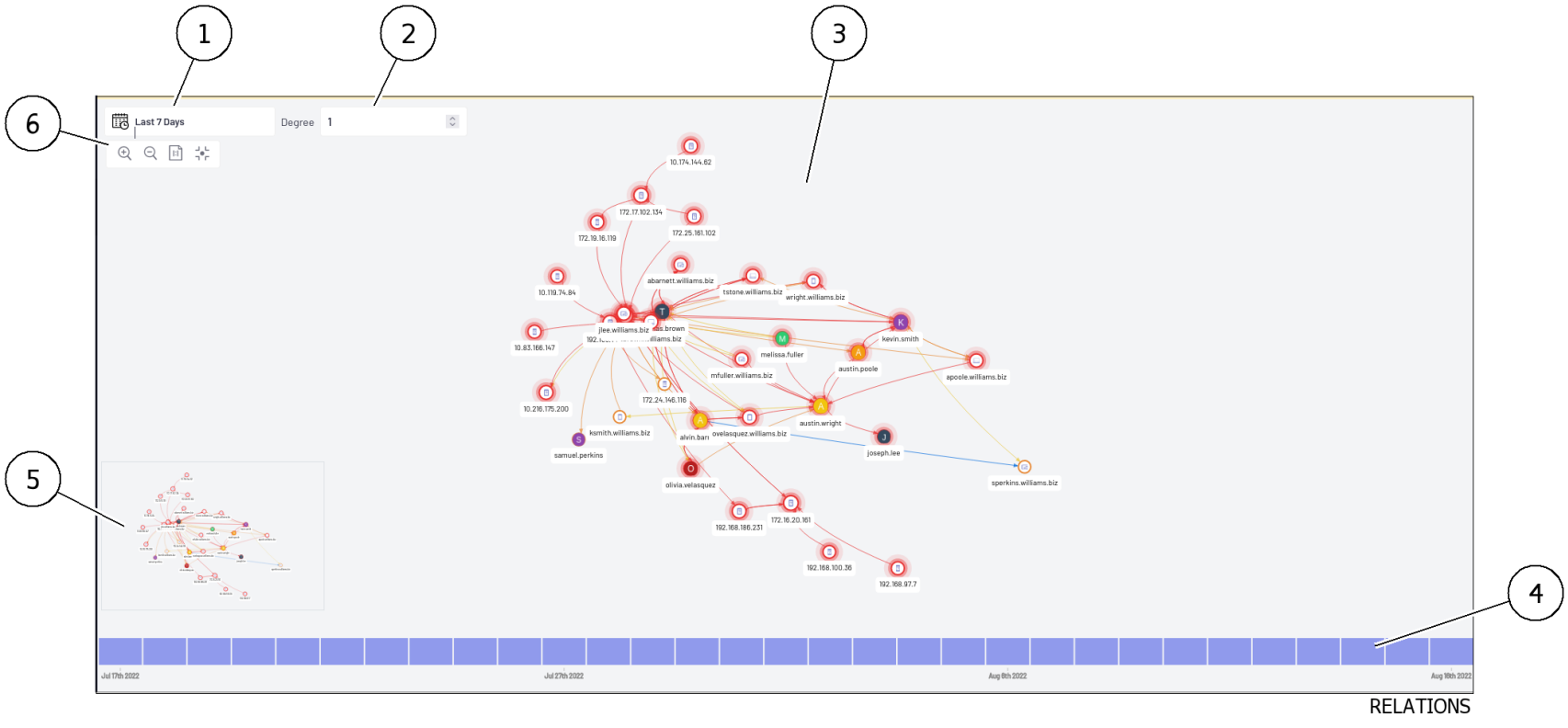
This screen shows the equipment on the network and the relationships between them.

5.6.5.2 Links associated

None

5.6.5.3 Screen description

After pressing the `Relations` button on the navigation bar, the following screen is displayed.



Item	Description
1	Time period selector
2	`Degree` field
3	Area for viewing active elements and their relationships
4	Timeline: enables selecting the display period
5	Total view area
6	Zoom tool area

Note:

If the message `This feature is disabled; check your configuration or your license` is displayed:
- Check the NDR configuration, see the *Configuring the NDR*
- Check the license, see the *`License` screen*

5.6.6 WebUI `Alerts` screen

5.6.6.1 Introduction

The alert management interface presents a list of the various alerts on the network classified by risk score and type.
The alert type is indicated alert by alert but it is possible to filter these alerts by type.
By clicking on an alert, the screen is updated and displays the information related to this alert (detection engine, no threat and network flow information with IPs, hostname...).
By clicking on this alert again, the `Alert details` window is displayed to view the detailed information.

Tip:

Alerts are detected by engines that:
- Operate
- Are up to date
- Have been activated

The visualization of the current engine status is given in *`Health checks` screen*.
For the Malcore engine, check the ignore list that intervene on the alarm detection display.
For other engines, they have to be enabled in their specific configuration screen.

5.6.6.2 Links associated

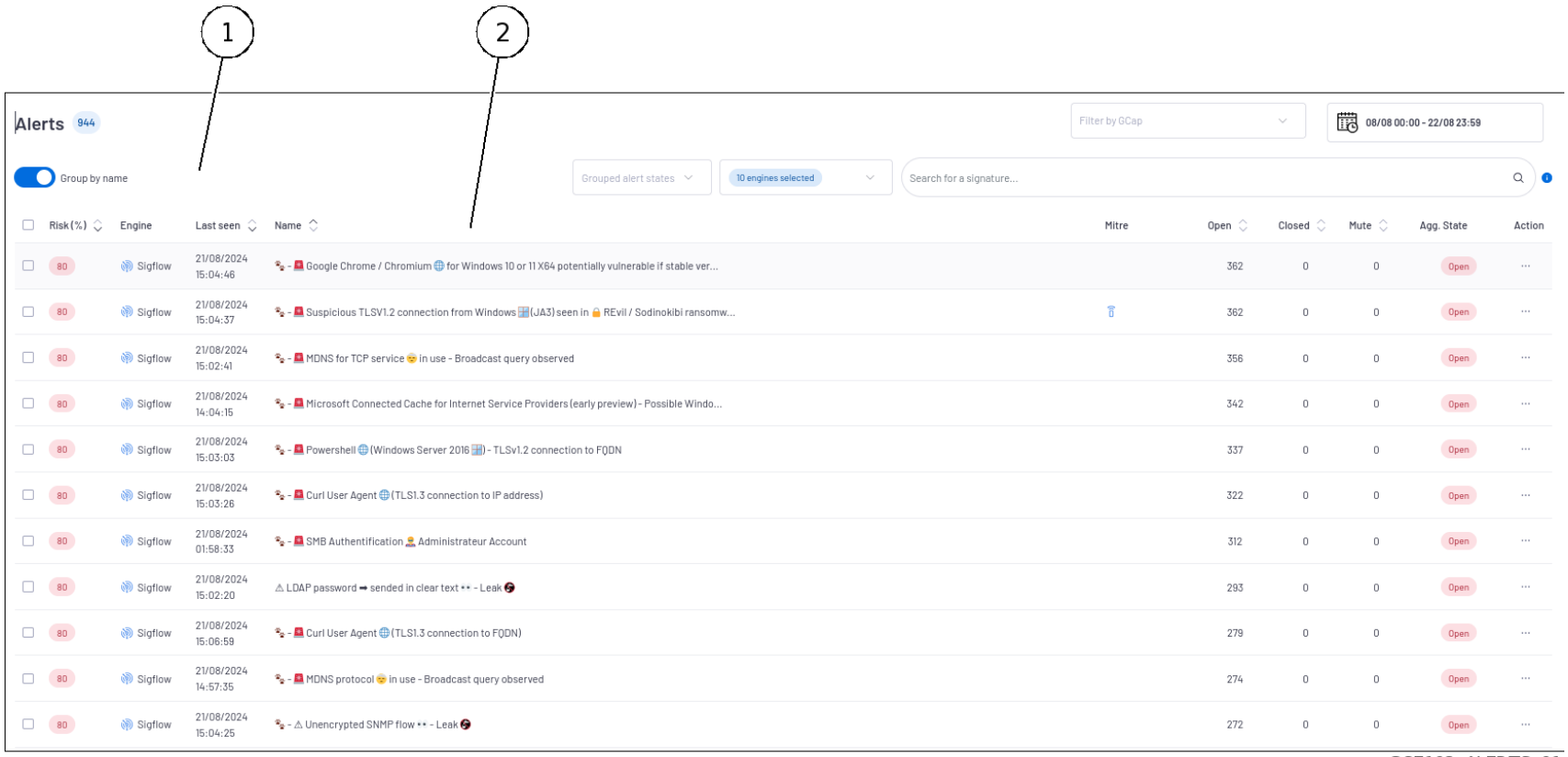
Engines operation is detailed in the *Detection Engines* paragraph.
The general treatment of alerts is indicated in the *Using of NDR dashboards* procedure.

The specific processing of alerts detected by...	is indicated in the ...
The Malcore engine	*Analyzing the Malcore alerts*
The Powershell detect engine	*Analyzing the Malicious Powershell detect alerts*
The Shellcode detect engine	*Analyzing the Shellcode detect alerts*
The Sigflow engine	*Analyzing the Sigflow alerts*
The DGA engine	*Analyzing the DGA detect alerts*
The Retroanalyzer engine	*Analyzing the Malcore retroanalyzer alerts*
The CTI engine	*Analyzing the Active CTI alerts*
The Retro hunt engine	*Analyzing the Retrohunt alerts*
The Ransomware detect engine	*Analyzing the Ransomware detect alerts*
The Beacon detect engine	*Analyzing the Beacon detect alerts*
The Yara engine	*Analyzing the Yara alerts*

The counters displayed in the Alert details windows are given in the *Engine log data structure* appendix.

5.6.6.3 Screen description

After pressing the `Alerts` button on the navigation bar, the following screen appears.

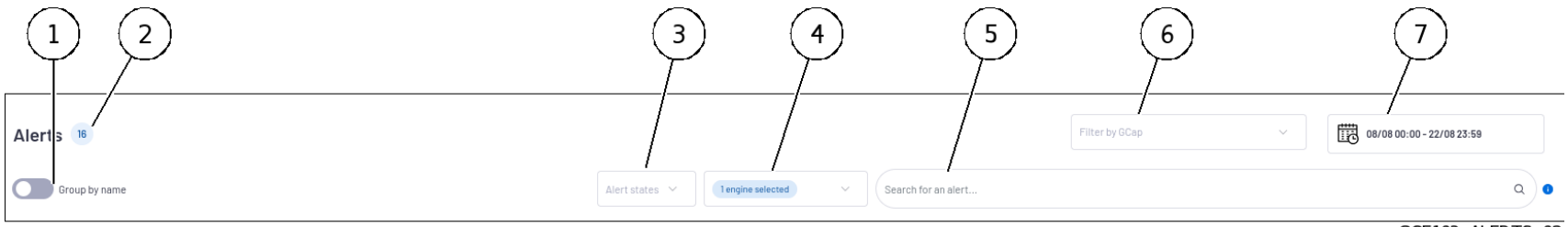


GCE103_ALERTS_01

Item	Description
1	Dashboard selector
2	Display area for the list of filtered alerts

5.6.6.3.1 `Alerts` screen dashboard selector

The selector includes the following items:



GCE103_ALERTS_02

Item	Name	Description
1	`Group by name`	Aggregates the alerts by name. In this mode the information fields are different.
2	Number of alerts	Display of the number of found alerts corresponding to the selector (1), (3), (4), (5)
3	Selected status type	The possible states are Mixed / Muted / Opened / Closed
4	Number of engines selected	The different choices: unselect all, select all ...
5	Search field	Enables to select the type : Name, Description, Type, Username, Mitre... Then enter the text to be searched
6	GCap Selector	Selection of the GCap to filter the alert source
7	Time period selector button	Selection of the display period

5.6.6.3.2 `Alerts` window (`Group by name` on position disabled)

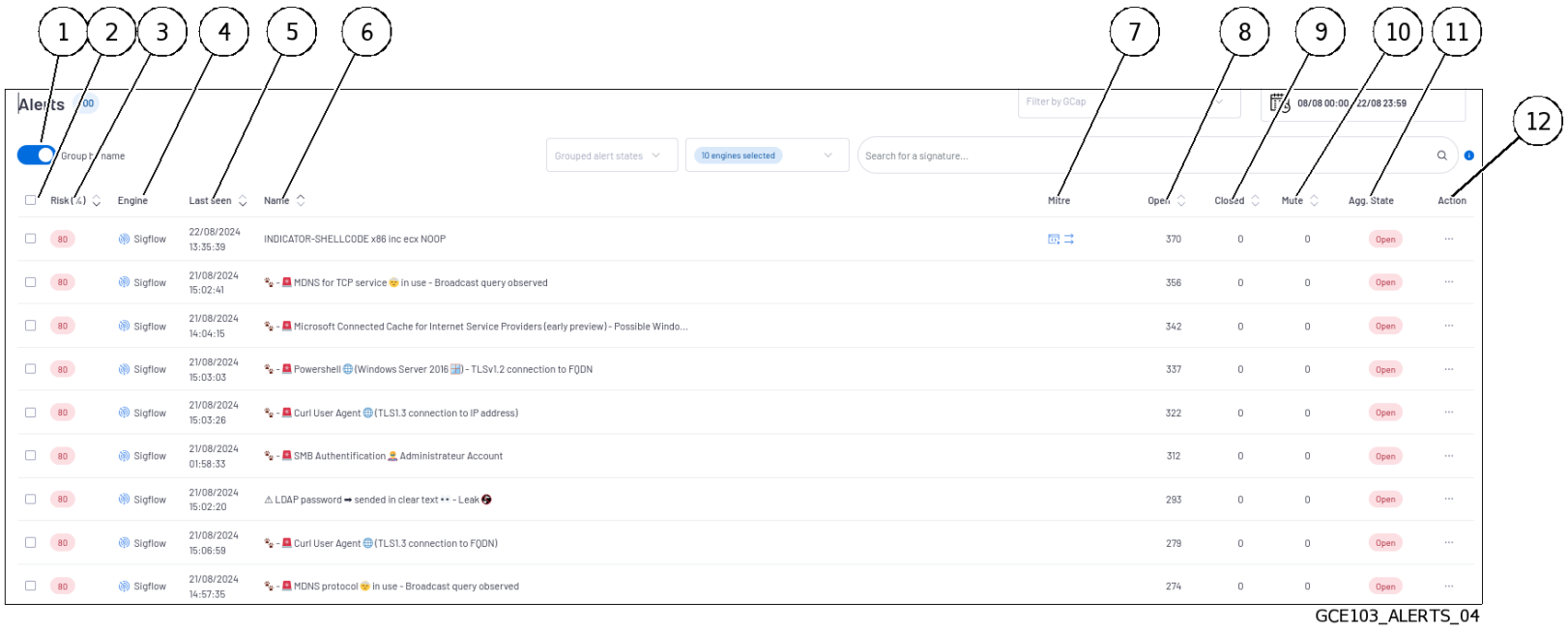
When the `Group by name` selector is on disabled position, the `Alerts` window consists of:

GCE103_ALERTS_03

Item	Name	Description
1	Line selection	Select one, several lines or all lines to execute an action
2	`Risk`	The threat level is indicated by a color and a score calculated from the analysis score returned by the various active engines at the time of detection. - **Critical risk** (score from 75% to 100%) - **High risk** (score from 50% to 74%) - **Medium risk** (score from 25% to 49%) - **low risk** (no score displayed) By clicking on the score of an alert, the `Alerts` window is refreshed to filter only that threat (listed in the `Name` field). So there can be multiple recordings. In addition, the `Alert details` window is displayed on the right side of the screen.
3	`Engine`	Engine which has detected the alert
4	`Date`	Date and time of the recording
5	`Name`	Name of the detected threat
6	`Src IP`	Network stream source IP address
7	`Dest IP`	Network stream destination IP address
8	`Src Host`	Source hostname
9	`Dest Host`	Destination hostname
10	`Mitre`	Viewing the MITRE category
11	`Tag`	Tags field if indicated (Confirmed incident, Critical, Doing, Done)
12	`Note`	Notes field if indicated
13	`State`	The possible states are Mixed / Muted / Opened / Closed
14	`Action`	Menu of possible actions. Depends on the threat type Refer to the *The sub menu `Actions`* paragraph

5.6.6.3.3 `Alerts` window (`Group by name` on position enabled)

When the `Group by name` selector (1) is on the enabled position, the `Alerts` window consists of:



GCE103_ALERTS_04

Item	Name	Description
2	Line selection	Allows to select one, several lines or all lines to execute an action
3	`Risk`	The threat level is indicated by a color and a score calculated from the analysis score returned by the various active engines at the time of detection. - **Critical risk** (score from 75% to 100%) - **High risk** (score from 50% to 74%) - **Medium risk** (score from 25% to 49%) - **low risk** (no score displayed) By clicking on the score of an alert, the `Alerts` window is refreshed to filter only that threat (listed in the `Name` field). So there can be multiple recordings. In addition, the `Alert details` window is displayed on the right side of the screen.
4	`Engine`	Engine which has detected the alert
5	`Date`	Date and time of the recording
6	`Name`	Name of the detected threat
7	`Mitre`	Viewing the MITRE category
8	`Open`	Number of opened alerts
9	`Closed`	Number of closed alerts
10	`Mute`	Number of muted alerts
11	`Agg state`	State of the alert group
12	`Action`	Menu of possible actions. Depends on the threat type. Refer to the *The sub menu `Actions`* paragraph

---

5.6.6.3.4 The sub menu `Actions`

This menu displays an command list.
The commands depend on the type of threat and are detailed in the following tables:

Note:

These commands are not fully activated in the `Group by nam` state.

5.6.6.3.4.1 List of common commands to all engines

Command	Action
`Add a tag`	A tag enables to have a tag about the threat and to give a status
`Edit or remove note`	A note enables to have a comment about the threat
`Close this alert` `Open this alert`	If the alert is opened, this command closes this alert and the state becomes `Closed` If the alert is closed, this command opens this alert and the state becomes `Opened`
`Close all similar alerts` `Open all similar alerts`	If the alert is opened, this command closes this alert and all similar alerts: the state becomes `Closed` If the alert is closed, this command opens this alert and all similar alerts: the state becomes `Opened`
`Mute all similar alerts, past and future`	If the alert is opened (or closed), this command mutes this alert: the state becomes `Mute` From this moment, all old alerts are muted. all alerts **with the same name** will be mute
`Unmute and re-open all alerts with the same name`	The old alerts are unmuted and become `Closed`. the state of the new one is `Opened`

5.6.6.3.4.2 Commands for a Beacon

Command	Action
`Open beacon network activity`	Kibana is opened on the `Beacon` category of the `Alerts` section: in the `Overview` tab, the database is filtered on this specific alert (address and destination IP)
`Open beacon network activity towards host`	Kibana is opened on the `Beacon` category of the `Alerts` section: in the `Overview` tab, the database is filtered on the destination IP defined on this specific alert.
`Open beacon engine analytics`	Kibana is opened on the `Beacon` category of the `Alerts` section: in the `Overview` tab, the database displays all beacon alerts.
`Beacon detect configuration`	Opens the `Settings` tab of the `Beacon detect` configuration screen: refer to *`Beacon detect` screen (Beacon command)*
`Beacon detect ignore list`	Opens the `Ignore list` tab of the `Beacon detect` configuration screen: refer to *`Beacon detect` screen (Beacon command)*

5.6.6.3.4.3 Commands for a DGA

Command	Action
`Open DGA activity`	Kibana is opened on the `DGA` category of the `Alerts ` section: in the `Overview` tab, the database is filtered on the `source.ip:` parameter which sends the DGA request
`Open DGA engine analytics`	Kibana is opened on the `DGA` category of the `Alerts ` section: in the `Overview` tab, the database displays all DGA alerts
`DGA detect configuration`	Opens the `Settings` tab of the `DGA detect` configuration screen: refer to *`DGA detect` screen (DGA command)*
`Open DGA detect ignore list`	Opens the `Ignore list` tab of the `DGA detect` configuration screen: refer to *`DGA detect` screen (DGA command)*

5.6.6.3.4.4 Commands for a malware detected by Malcore

Command	Action
`Open malcore engine analytics`	Kibana interface is opened on the `Malcore` category of the `Alerts ` section: in the `Overview` tab, the database displays all Malcore alerts
`Open malcore file transaction`	Kibana is opened on the `Malcore` tab of the `Alerts` section: in the `Overview` tab, the database is filtered on the `file.hash.sha256` parameter and the `event.module : malcore` filter.
`Download Malware`	Download the compressed file (name is UD.zip) to the user's PC.
`Malcore configuration`	Opens the Malcore configuration screen: refer to *`Malcore` screen*

5.6.6.3.4.5 Commands for a malware detected by Malcore retroanalyzer

Command	Action
`Open retroanalyzer file transaction`	Kibana is opened on the `Malcore` tab of the `Alerts` section: in the `Overview` tab, the database is filtered on the `file.hash.sha256` parameter and the `event.module : malcore_retroanalyzer` filter.
`Download Malware`	Download the compressed file (name is UD.zip) to the user's PC.
`Malcore retroanalyzer configuration`	Opens the Malcore retroanalyzer configuration screen: refer to *`Malcore retroanalyzer` screen*

5.6.6.3.4.6 Commands for a powershell

Command	Action
`Show hexdump`	Displays the file
`Download powershell`	Download the compressed file (name is UD.zip) to the user's PC
`Open powershell engine analytics`	Kibana is opened on the `Malicious Powershell` category of the `Alerts ` section: in the `Overview` tab, the database displays all alerts
`Malicious PS configuration`	Opens the Malicious Powershell configuration screen: refer to *`Malicious Powershell detect` screen (Malicious Powershell command)*
`Open sigflow engine analytics`	Kibana interface is opened on the `Malicious Powershell` category of the `Alerts ` section: in the `Overview` tab, the database displays all Malicious Powershell alerts

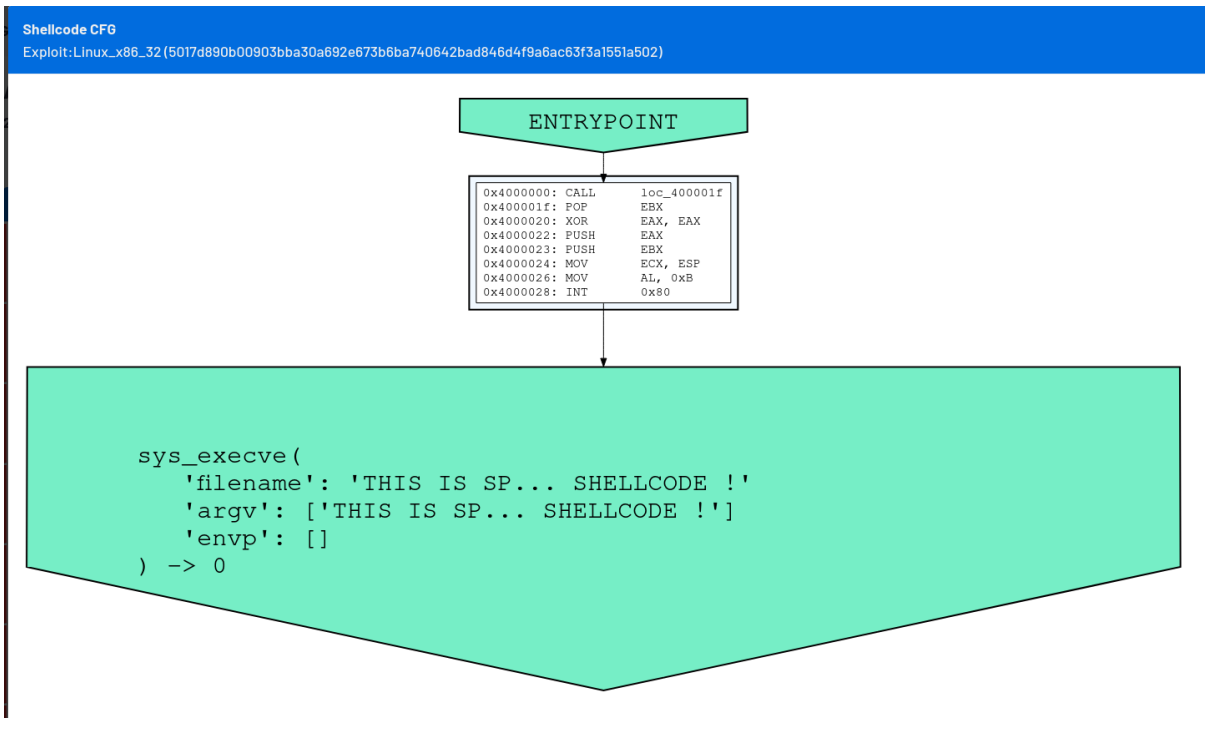
5.6.6.3.4.7 Commands for a ransomware

Command	Action
`Open host SMB activity`	Kibana is opened on the `Ransomware` category of the `Alerts` section In the `Overview` tab, the database is filtered on the `source.ip:` parameter
`Open ransomware detect analytics`	Kibana interface is opened in the `Overview` tab, the `Ransomware` category of the `Alerts` section The database displays all Ransomware alerts
`Open SMB session activity`	Opens the `Investigation` tab of the `Ransomware detect` configuration screen : refer to *`Ransomware detect` screen (Ransomware command)*
`Ransomware detect configuration`	Opens the Ransomware configuration screen: refer to *`Ransomware detect` screen (Ransomware command)*
`Ransomware detect ignore list`	Opens the `Ignore list` tab of the `Ransomware detect` configuration screen: refer to *`Ransomware detect` screen (Ransomware command)*

5.6.6.3.4.8 Commands for a shellcode alert

Command	Action
`Open flow details`	Displays flow details. Kibana is opened on the `Shellcode` tab of the `Alerts` section: in the `Messages` tab, the database is filtered on the `network.flow_id` parameter
`Show hexdump`	Displays the file
`Show shellcode CFG`	Generate the control flow graph (CFG) to obtain a graphical and simplified version of the Shellcode instructions detected: an example is given below
`Download shellcode`	Download the compressed file (name is UD.zip) to the user's PC.
`Shellcode detect configuration`	Opens the Shellcode detect configuration screen: refer to *`Shellcode detect` screen (Shellcode command)*
`Open Shellcode detect analytics`	Kibana interface is opened on the `Shellcode` category of the `Alerts ` section: in the `Overview` tab, the database displays all Shellcode alerts

Below is an example of a CFG generation of a simple shellcode detected by the Shellcode detect engine:



Below is an example of file content:

Hexdump
Exploit:Linux_x86_32 (5017d890b00903bba30a692e673b6ba740642bad846d4f9a6ac63f3a1551a502)

```
00000000:   e8 ff ff ff ff c3 5b 80 c3 02 53 59 49 49 49 49   ......[...SYIIII
00000010:   49 49 49 49 49 49 49 49 49 43 43 43 37 51 5a 6a   IIIIIIIIICCC7QZj
00000020:   41 58 50 30 41 30 41 6b 41 41 51 32 41 42 32 42   AXP0A0AkAAQ2AB2B
00000030:   42 30 42 42 41 42 58 50 38 41 42 75 4a 49 4a 48   B0BBABXP8ABuJIJH
00000040:   44 5a 75 50 37 70 53 30 71 44 73 78 61 59 62 73   DZuP7pS0qDsxaYbs
00000050:   45 70 32 69 32 73 37 50 52 73 62 70 36 4e 76 4e   Ep2i2s7PRsbp6NvN
00000060:   66 4e 57 50 42 73 30 48 67 35 70 4c 42 6c 51 53   fNWPBs0Hg5pLBlQS
00000070:   50 4f 70 44 31 55 35 70 65 71 73 30 43 6b 45 61   POpD1U5peqs0CkEa
00000080:   69 50 66 30 56 33 4e 69 58 61 68 30 36 6b 7a 6d   iPf0V3NiXah06kzm
00000090:   6f 70 41 41                                       opAA
```

5.6.6.3.4.9 Commands for a sigflow alert

Command	Action
`` `Open flow details` ``	Displays flow details. Kibana is opened on the `` `Sigflow` `` tab of the `` `Alerts` `` section: The database is filtered on the `` `flow id` `` parameter to view the alerts generated when the Sigflow engine has reconstructed the network flow **files**.
`` `Open sigflow alert summary` ``	Displays summary of this alert Kibana is opened on the `` `Sigflow` `` tab of the `` `Alerts` `` section: In the `` `Overview` `` tab, the database is filtered on the `` `alert.signature_id` `` **and** on the parameter on the IP address of the source (`` `src_ip` ``) and the destination (`` `dest_ip` ``).
`` `Open signature definition` ``	Displays the rule that detected the alert in the legacy WebUI.
`` `Open sigflow alert history` ``	Kibana interface is opened on the `` `Sigflow` `` tab of the `` `Alerts` `` section: in the `` `Overview` `` tab, the database is filtered on the `` `alert.signature` `` parameter``` **or** on the `` `alert.signature_id` `` parameter.
`` `Open sigflow engine analytics` ``	Kibana is opened on the `` `Sigflow` `` tab of the `` `Alerts` `` section: In the `` `Overview` `` tab, the database displays all sigflow alerts

5.6.6.3.5 `Alert details` window

By clicking directly on an alert, the following window is displayed:

GCE103_MALCORE_ALERT_08

The window consists of:

- Upper part:
  This section includes:
  - The level of risk
  - The name of the detected threat (1)
  - The detection date and time
  - The Possible `Actions` (5): these are the same actions as the commands detailed in *The sub menu `Actions`* paragraph
  - The `Note` (8)
  - The `Tags` (7)
- The `Summary` tab (2) gives the summary of the alert information
- The `Details` tab (3) gives the detailed information of the alert information:
  - The file (ID, UUID, SHA256...)
  - The detected threat (type, type alert, name, description...)
  - Source GCap (GAP, Host)
  - Etc
- The `Documentation` tab (4) displays the procedure to follow for alert analyzing

5.6.7 WebUI `Hunting` screen

5.6.7.1 Introduction

The Kibana web interface displays the data present in the ElasticSearch indexes of the GCenter.
After pressing the `Hunting` button on the navigation bar, Kibana UI is opened on the `Overview` tab of the `Alerts` section:

5.6.7.2 Links associated

This interface is described in the paragraph *Overview of the Kibana GUI*.

5.6.8 WebUI `Users` screen

5.6.8.1 Introduction

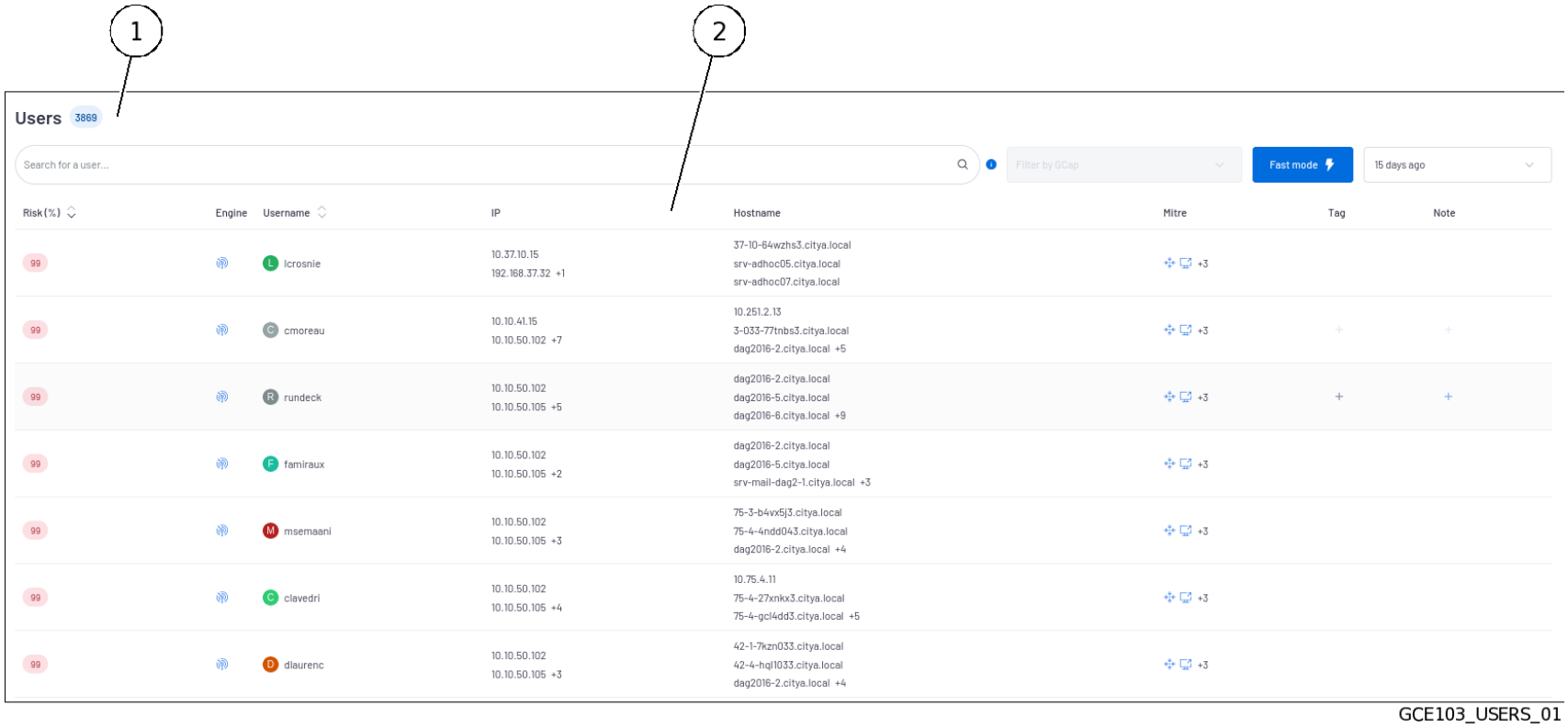
The user management interface presents a list of the different users present on the network classified by risk score.
The user with the highest risk score is the one with the highest criticality alerts.

5.6.8.2 Links associated

None

5.6.8.3 Screen description

After pressing the `Users` button on the navigation bar, the following screen is displayed.



GCE103_USERS_01

Item	Description
1	Dashboard selector
2	User list display area

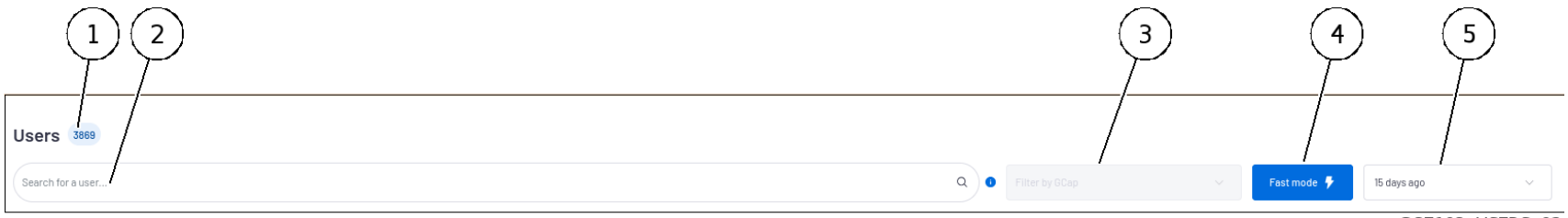
Note:

If the message `This feature is disabled; check your configuration or your license` is displayed:

- Check the NDR configuration, see *Configuring the NDR*
- Check the license, see *`License` screen*

5.6.8.3.1 `Users` screen dashboard selector

The selector includes the following items:



GCE103_USERS_02

Item	Name	Description
1	Number of results	Display of the number of records found
2	Search field	Enables entering a text to be searched in the page
3	GCap selector	Selection of the GCap
4	`Fast mode` button	Select the GCap and and the period `15 days ago` Quick mode uses cached data to present results faster. When the quick mode is enabled (default), only two time ranges are available: `15 days ago` and `yesterday`. When the fast mode is enabled, it is not possible to filter by GCap.
5	Time period selector	Selection of the display period if the Fast mode is enabled

5.6.8.4 User list display area

The display consists of:

GCE103_USERS_03

Item	Description
1	Type of risks. The risk level is indicated by the color. The type of risk is indicated by the corresponding icons. Above 2, an indicator shows the number of risk. By clicking on this indicator, a window gives additional information such as the name of the user and the list of risk types.
2	`Engine` Engine which has detected the alert
3	`Username` By clicking on this field, a window provides additional information about this user:
4	`IP`: IP address of the infected device. By clicking on this field, a window opens providing additional information about this IP address.
5	`Hostname` Unique name of the infected computer
6	`MITRE` Viewing the MITRE category
7	`Tag` Tags field if indicated (Confirmed incident, Critical, Doing, Done)
8	`Notes` Notes field if indicated

5.6.9 WebUI `Assets` screen

5.6.9.1 Introduction

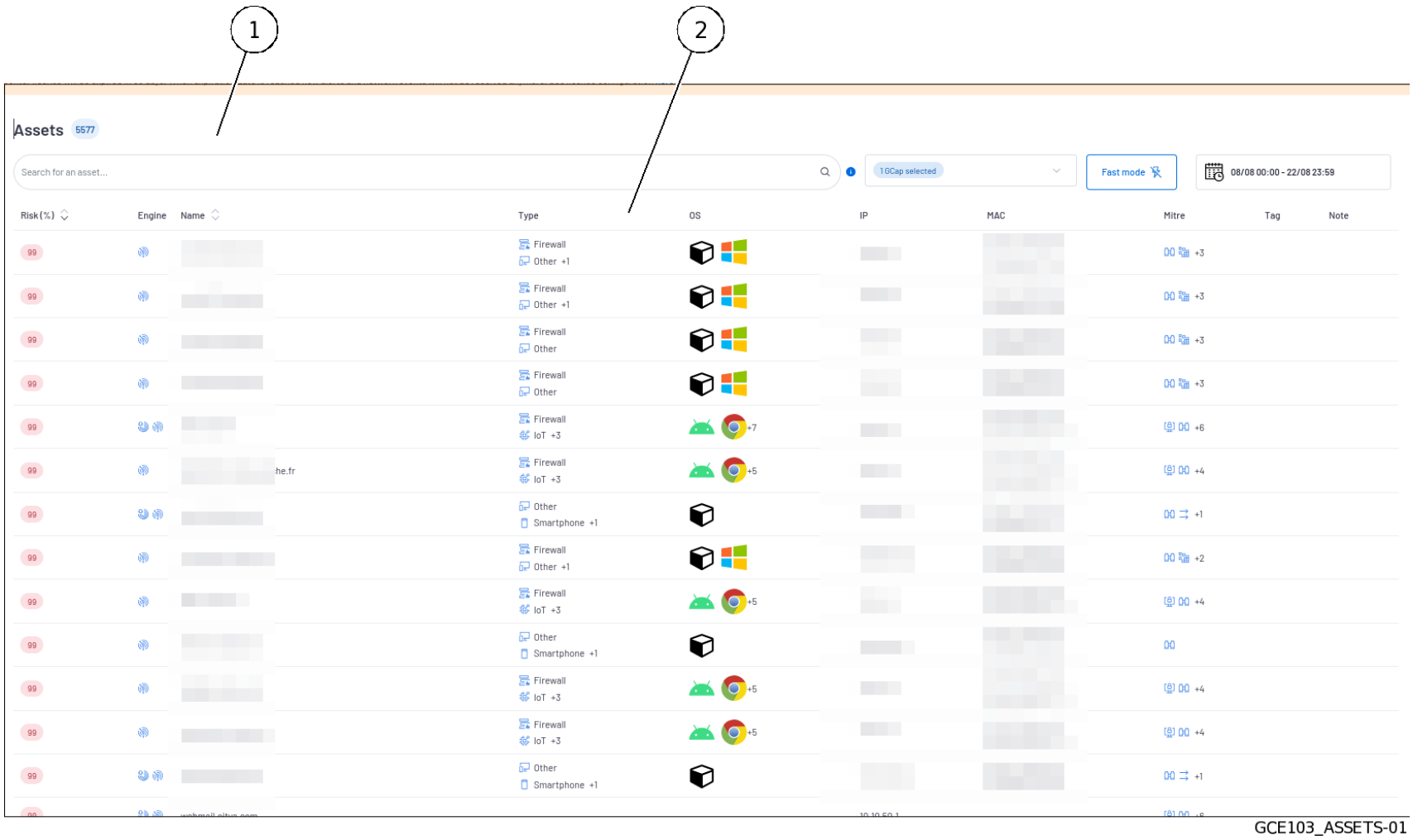
The active equipment management interface presents a list of the various equipment present on the network classified by risk score.
The equipment with the highest risk score is the one with the most high criticality alerts.

5.6.9.2 Links associated

None

5.6.9.3 Screen description

After pressing the `Assets` button on the navigation bar, the following screen is displayed.



GCE103_ASSETS-01

Item	Description
1	Dashboard selector
2	Active equipment list display area

Note:

If the message `This feature is disabled; check your configuration or your license` is displayed:

- Check the NDR configuration, see the *Configuring the NDR*
- Check license, see the *`License` screen*

5.6.9.3.1 `Assets` screen dashboard selector

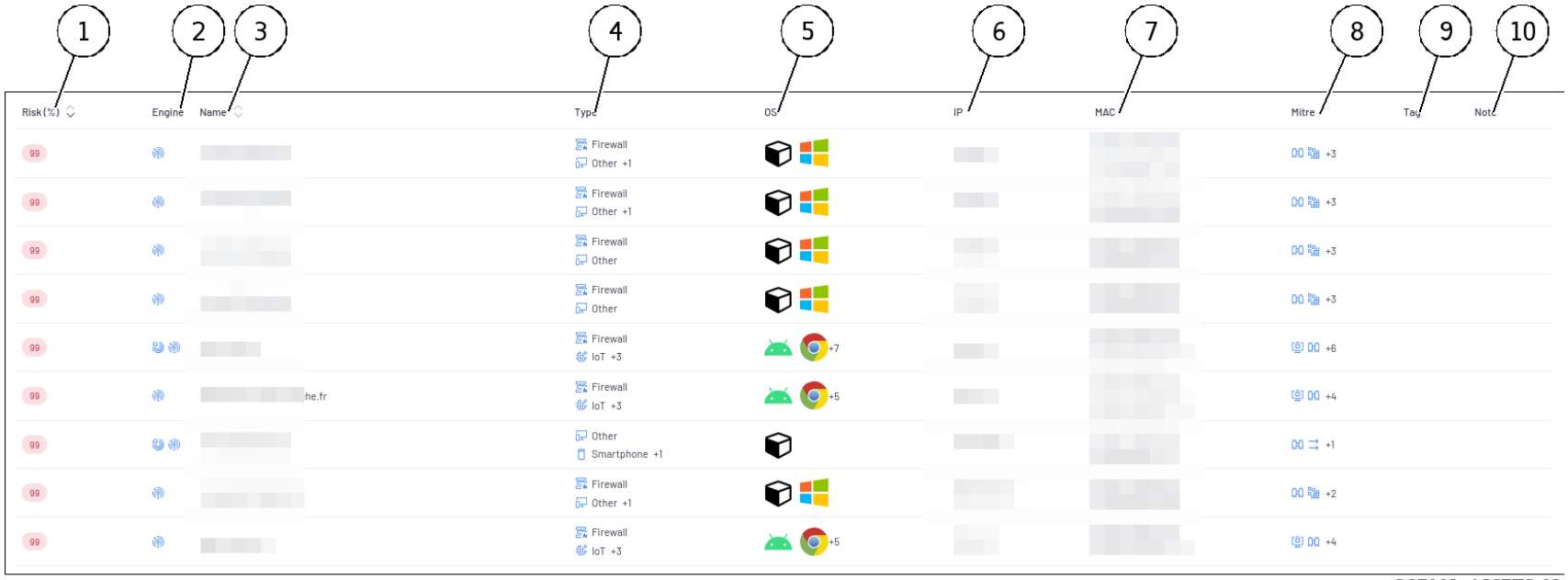
The selector includes the following items:

GCE103_ASSETS-02

Item	Name	Description
1	Number of results	Display of the number of records found
2	Search field	Enables entering a text to be searched in the page
3	GCap selector	Selection of the GCap
4	`Fast mode` field	Select the GCap and and the period `15 days ago`. The fast mode uses cached data to present faster results. When fast mode is enabled (default), only two timerange are available : 15 days ago and yesterday. When fast mode is enabled, it is not possible to filter by GCap.
5	Time period selector	Selection of the display period if the Fast mode is enabled

5.6.9.3.2 Active equipment list display area

The display consists of:



GCE103_ASSETS-03

Item	Description
1	Type of risks. The risk level is indicated by the color. The type of risk is indicated by the corresponding icons. Above 2, an indicator shows the number of risk. By clicking on this indicator, a window gives additional information.
2	`Engine` Engine which has detected the alert
3	`Name` Name of the active equipment either the IP address or the hostname
4	Type of the active device (laptop, smartphone...)
5	`OS` Operating system either MAC OS, IOS, Windows, Android or ...)
6	IP address IP address of the infected device.
7	`MAC address` MAC address
8	`MITRE` Viewing the MITRE category
9	`Tag` Tags field if indicated (Confirmed incident, Critical, Doing, Done)
10	`Notes` Notes field if indicated

5.6.10 WebUI `GScan` screen

5.6.10.1 Introduction

GScan allows you to manually submit files for analysis.
The following options are possible:

- Malware: submit files to the Malcore engine
- Powershell: scans files containing Powershell scripts and detects potential threats that can serve as a gateway to install malware on Windows.

  With regard to malicious powershells, detection is based on a supervised machine learning model, and on the fact that these scripts generally use obfuscation techniques or that are similar to them (base64, concatenation, type conversion, etc.).
- Shellcode: submits files for analysis by the shellcode detect engine

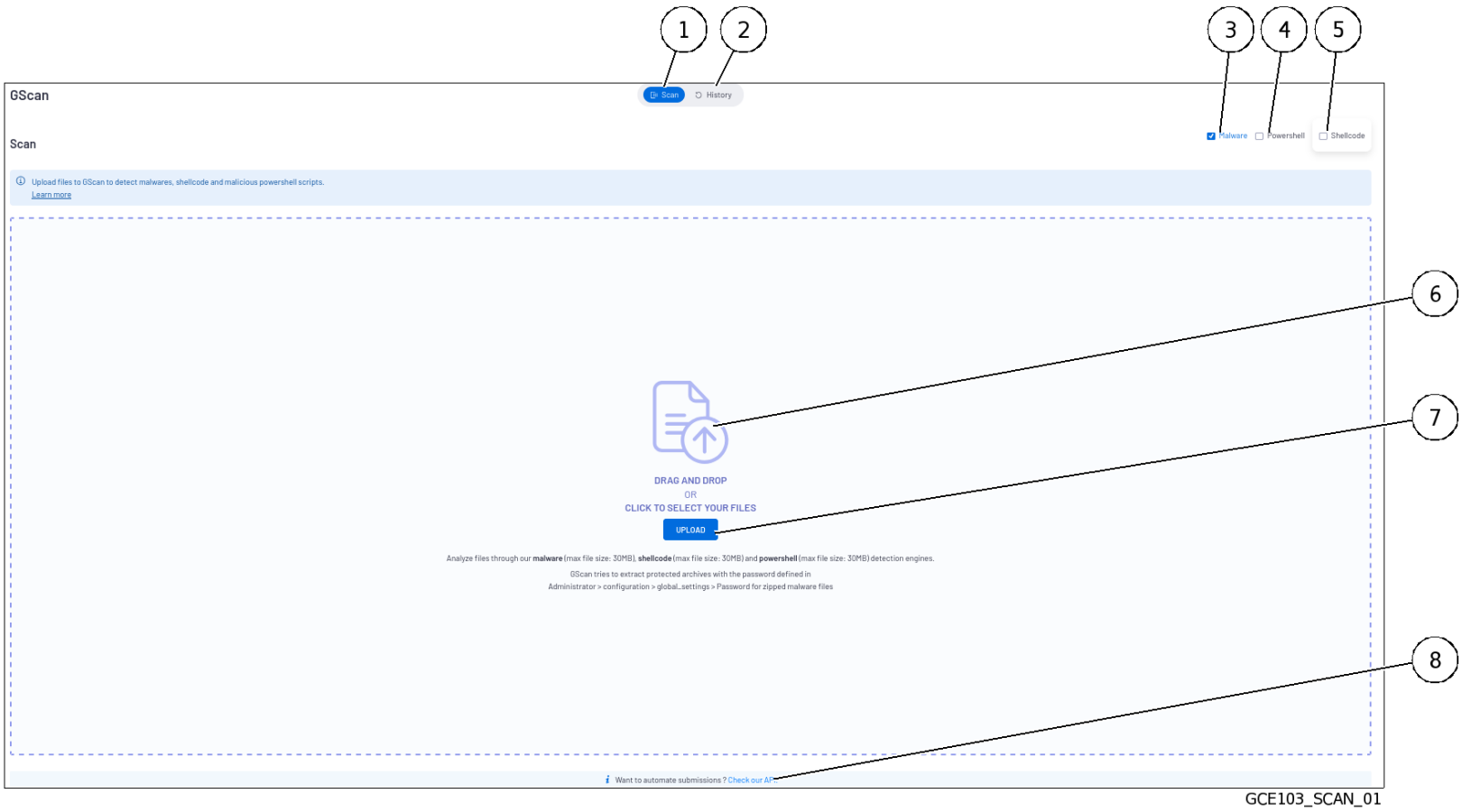
---

5.6.10.2 Links associated

See the Gscan presentation in *Detection by GScan*.
To configure the engine, see the *Setting up the Malcore engine*.
For implementation, see the *Detecting with GScan*.

5.6.10.3 Screen description

After pressing the `Gscan` button on the navigation bar, the following screen is displayed.

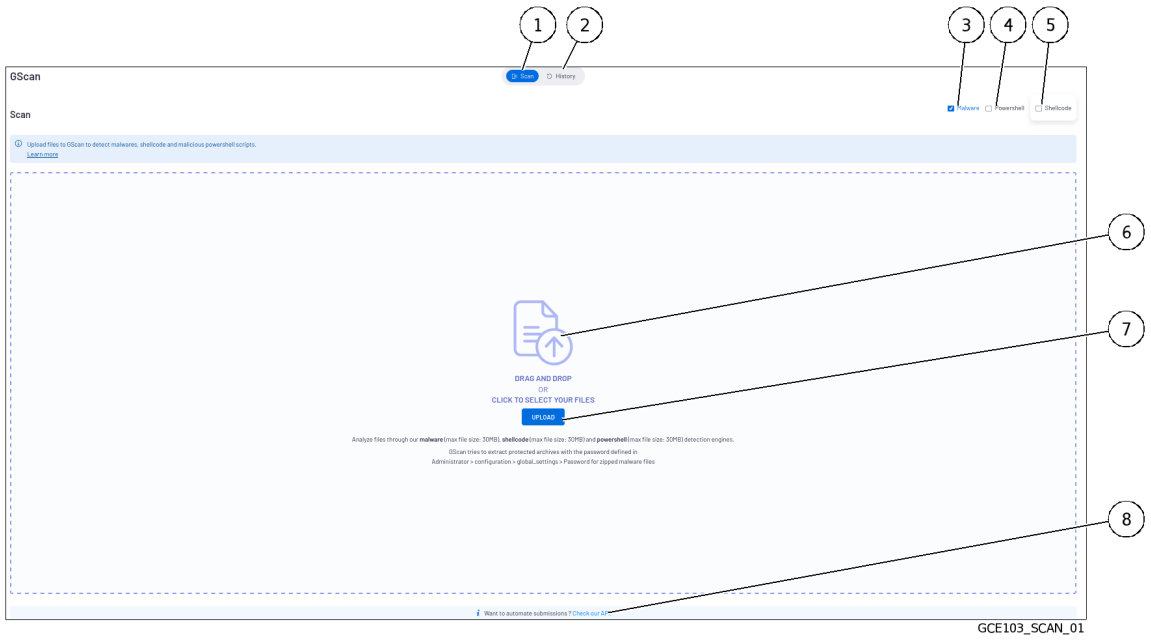


GCE103_SCAN_01

The `GScan` screen contains the following areas:

Area	Function
`Scan` (1)	detection area to select the file to be scanned
`History` (2)	List of recent scans

5.6.10.3.1 `Scan` screen

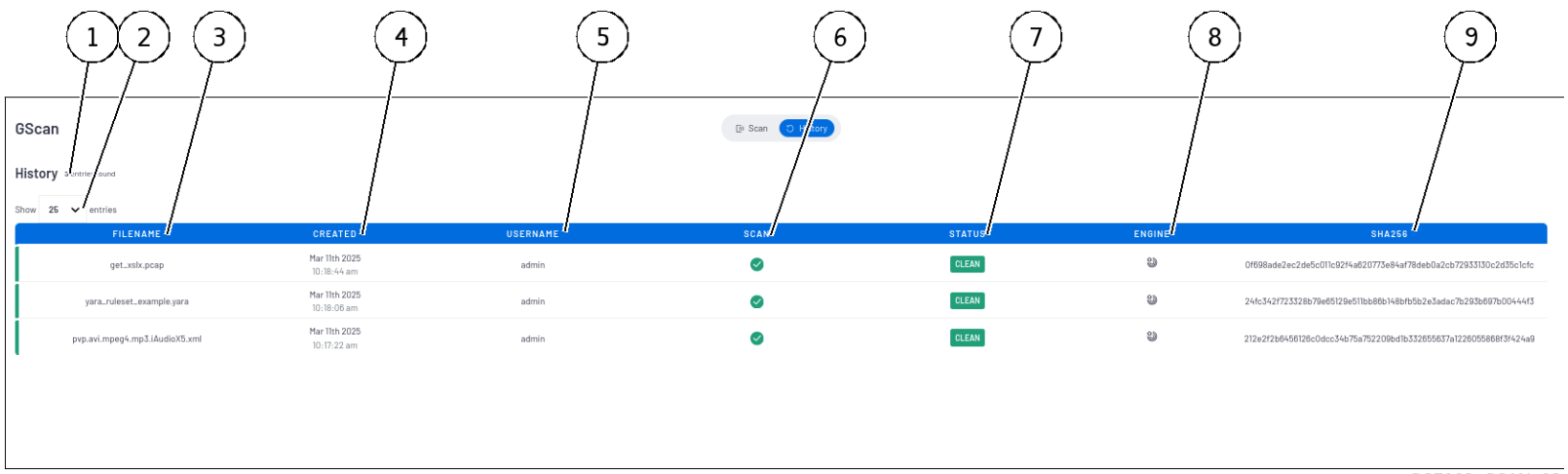


GCE103_SCAN_01

Item	Name	Description
3	`Malware`	Activation detection engine
4	`Powershell`	Activation detection engine
5	`Shellcode`	Activation detection engine
6	`DRAG AND DROP`	Zone to deposit a file to be analyzed / zone of reports of the analyzed files
7	`UPLOAD`	Button to open a window to load a file(s) to be analyzed
8	`Want to automate submissions ? Check our API.`	link to access to the API

The analysis made by GScan depends on several configurable limits (such as the maximum size of files extracted by a GCap): the procedure to modify these values is given in *Setting up the Malcore engine*.

5.6.10.3.2 `History` screen of the `GScan` screen



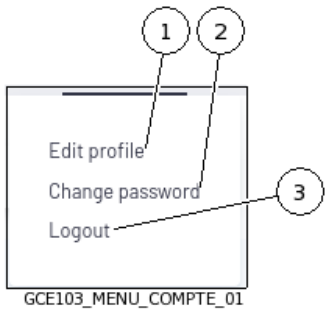
GCE103_SCAN_02

Item	Name	Description
1	`History`	Count of saved scans
2	`Show 25 entries`	Number of scans per page
3	`FILENAME`	Name of scanned file
4	`CREATED`	Creation date
5	`USERNAME`	The name of the user who has launched the scan
6	`SCAN`	Icon to indicate the correct analyse files
7	`STATUS`	Analyse status
8	`Engine`	Indicates the motor used during the analyse. Click on the icon displays the report
9	`SHA 256`	Indicates the sha256 of the scanned file

5.6.11 Management of the current account

5.6.11.1 Overview of the account management menu

This menu consists of the following:



GCE103_MENU_COMPTE_01

Item	Command	Description
1	`Edit profile`	See *`Profile / Edit profile` screen*
1	`Change password`	See *`Profile / Edit Password` screen*
3	`Logout`	Disconnects checking account. Returns to login screen

5.6.11.2 `Profile / Edit profile` screen

5.6.11.2.1 Introduction

The `Edit profile` screen is used:

- To display the account information (creation date, date of the last connection)
- To display or modify the email address of the owner of this account
- To display or modify the name and first name of the owner of this account

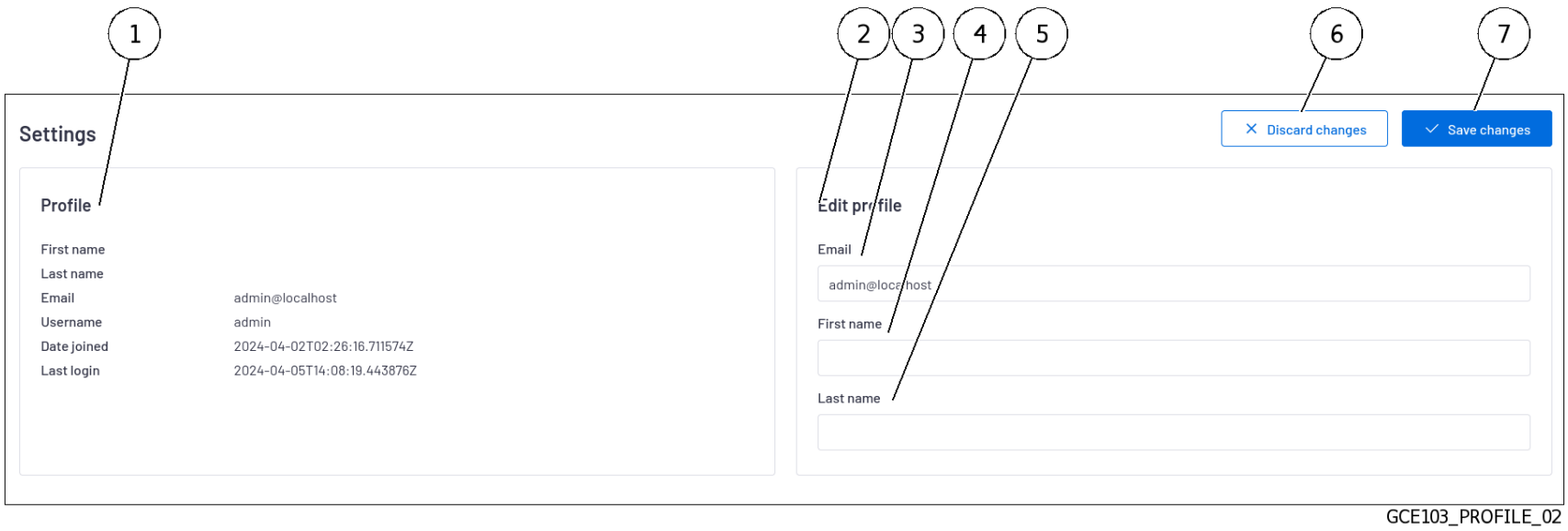
---

5.6.11.2.2 Links associated

For further details about the accounts, see *Web interface accounts and their management*
For implementation for an operator account, see *Changing some of the current user's information*.
For implementation for an administrator account, see *Changing some of the current user's information*.

5.6.11.2.3 Screen description

After pressing the `Edit profile` command of the checking account menu, the following screen is displayed.



GCE103_PROFILE_02

Item	Name	Function
1	`Profile`	Area to display the account parameters - First name - Last name - Email : for example admin@localhost - Username: for example admin - Date joined: for example 2024-04-02T02:26:16.711574Z - Last login: for example 2024-04-05T14:08:19.443876Z
2	`Edit profile`	Area to modify account parameters
3	`Email` field	Field to enter the email address of the owner of this account
4	`First name` field	Field to enter the first name of the owner of this account
5	`Last name` field	Field to enter the name of the owner of this account
6	`Discard changes` button	Cancels current changes
7	`Save changes` button	Saves changes

5.6.11.3 `Profile / Edit Password` screen

5.6.11.3.1 Introduction

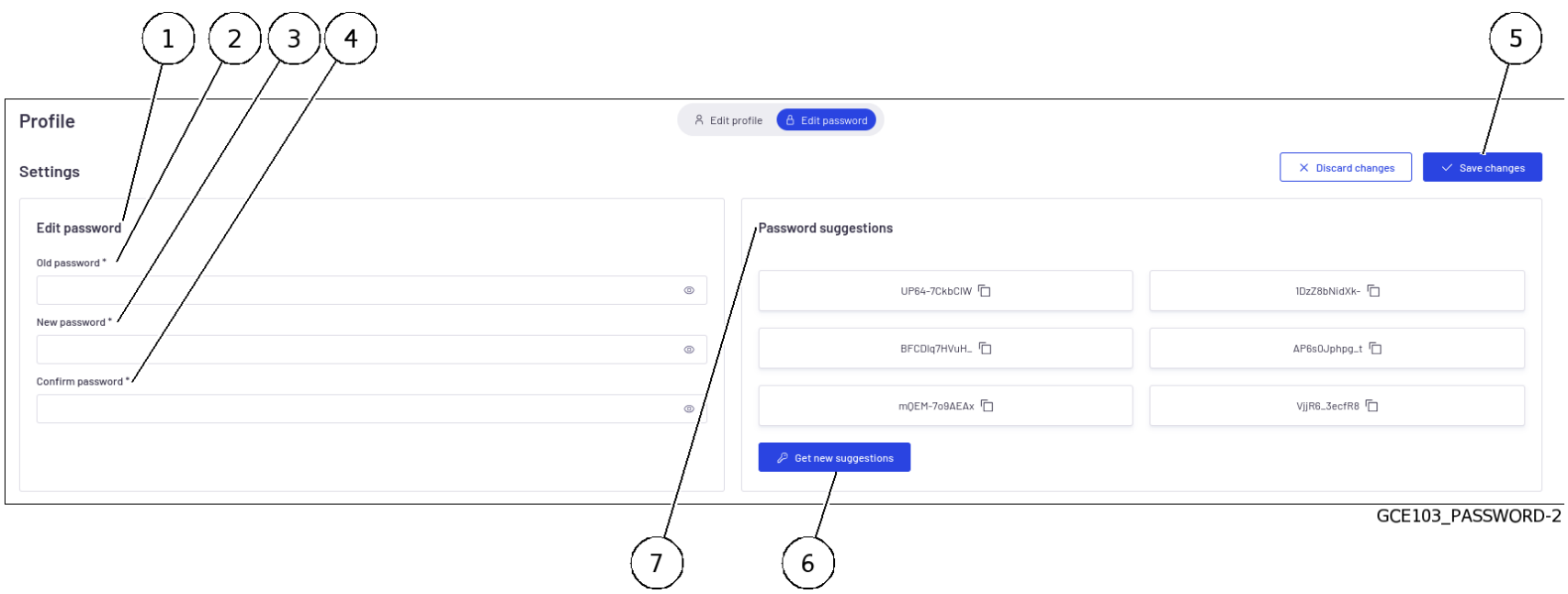
The `Profile / Edit Password` screen enables to modify the account password.

5.6.11.3.2 Links associated

For further details about the accounts, see the *Web interface accounts and their management*.
For implementation for an operator account, see the *Changing the checking account password*.
For implementation for an administrator account, see the *Changing the checking account password*.

5.6.11.3.3 Screen description

After pressing the `Edit password` command of the checking account menu, the following screen is displayed.

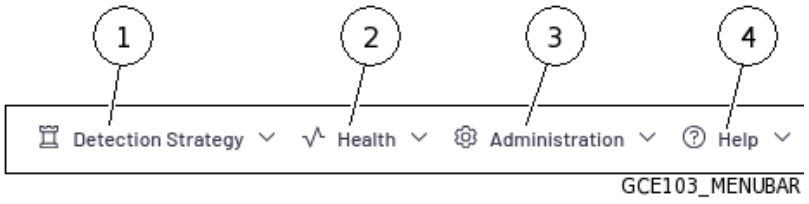


Item	Name	Function
1	`Edit Password` Zone	Zone to modify the current password
2	`Old password` Field	Field to enter the old password
3	`New password` Field	Field to enter the new password
4	`New password confirmation` Field	Field to enter again the new password
5	`Save changes` button	Saves changes
6	`Get new suggestions` button	Create 6 new passwords (7) generated by the system and in line with the password policy
7	`Password suggestions`	Zone to get password suggestions according to the password policy

5.7 Presentation of the WebUI menu bar screens

5.7.1 Overview of the menu bar

The menu bar is located in the title bar and consists of the following:

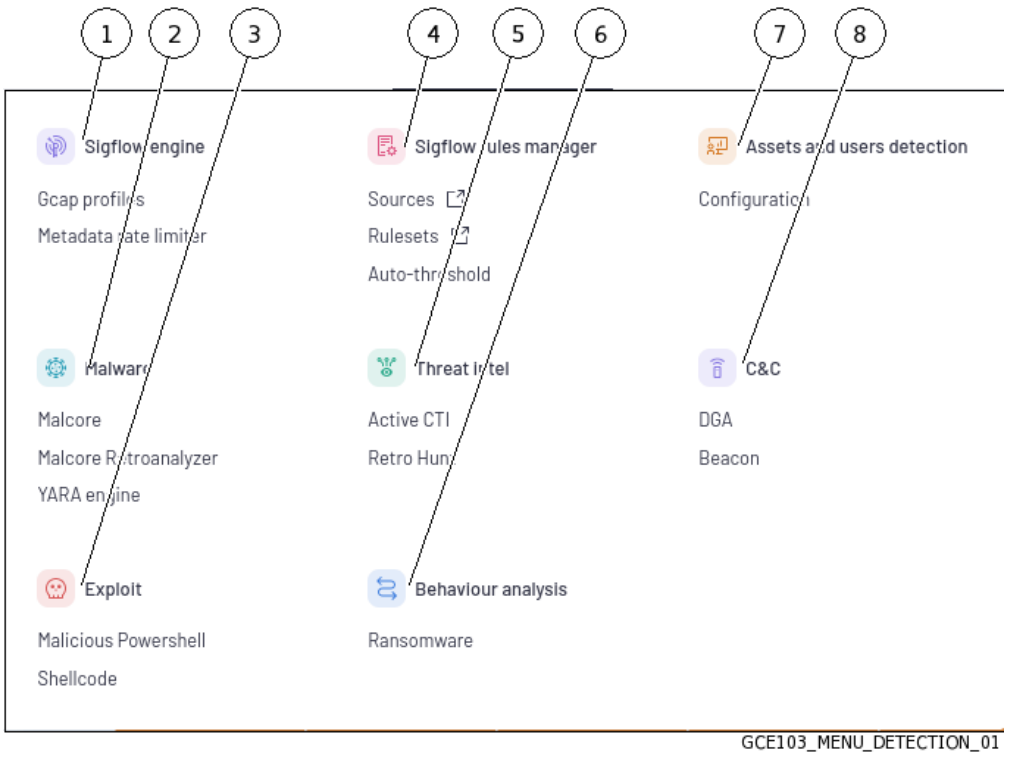


Item	Name	Description
1	`Detection strategy`	See the *Overview of the `Detection strategy` menu*
2	`Health`	See the *Overview of the `Health` menu*
3	`Administration`	See the *Overview of the `Administration` menu*
4	`Help`	See the *Overview of the `Help` menu*

5.7.2 `Detection Strategy` menu

5.7.2.1 Overview of the `Detection strategy` menu

The `Detection strategy` menu consists of the following:



Item	Heading	Command	Description
1	`Sigflow engine`	`GCap profiles` `Metadata rate limiter`	Configuration of sigflow engine by creating Gcaps profile: see *`GCaps profiles` screen* Metadata rate limiters: see *`Metadata rate limiter` screen*

2	`Malware`	`Malcore`
		`Malcore Retroanalyzer`
		`YARA engine`
			See *`Malcore` screen*
			See *`Malcore retroanalyzer` screen*
			See *`YARA` screen*

3	`Exploit`	`Malicious Powershell` `Shellcode`	See *`Malicious Powershell detect` screen (Malicious Powershell command)* See *`Shellcode detect` screen (Shellcode command)*

4	`Sigflow rules manager`	`Sources`
		`Rulesets`
		`Auto-threshold`
			Sigflow rules manager, source management: see *`Sources` screen*
			Sigflow rules manager, ruleset management: see *`Rulesets` screen*
			Sigflow rules manager, threshold management: see *`Auto-threshold` screen*

5	`Threat intel`	`Active CTI` `Retro Hunt`	See *`Active CTI` screen* See *`Retro hunt` screen*
6	`Behaviour analysis`	`Ransomware`	See *`Ransomware detect` screen (Ransomware command)*
7	`Assets and users detection`	`Configuration`	See *`Association rules` screen (Configuration command)*
8	`C&C`	`DGA` `Beacon`	See *`DGA detect` screen (DGA command)* See *`Beacon detect` screen (Beacon command)*

5.7.2.2 `GCaps profiles` screen

5.7.2.2.1 Introduction

This screen is used to configure the predefined profil selected during the pairing of each GCap to this GCenter.
This configuration consists of :

- Modification of parameters grouped in different categories then
- Apply this new GCAp profile to the GCap

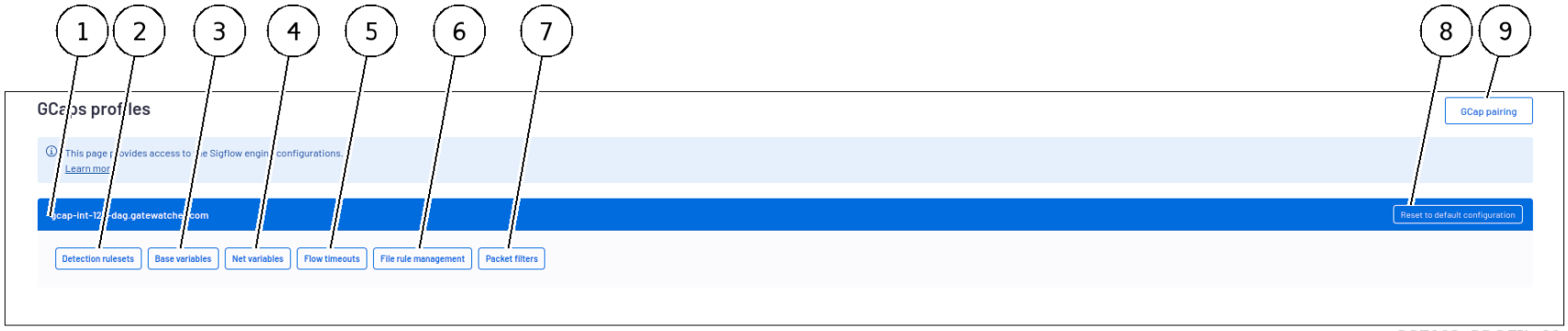
This screen is only accessible to members of the *operator* group.

5.7.2.2.2 Links associated

The Sigflow rulesets profiles are presented in the paragraph *Detection Rulesets*.
The GCap profiles are presented in *Sigflow engine*.
To manage the rules, see the *Configuring the Sigflow engine* menu.
To manage the GCaps profiles, see the *Configuring GCaps using the `GCaps Profiles`* menu.

5.7.2.2.3 Screen description

After pressing the `GCaps profiles` command of the `Detection strategy - Sigflow engine` menu, the following screen is displayed.



GCE103_PROFIL-01

For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Item	Function	See the description and the procedure
1	FQDN	GCap name paired with the GCenter
2	`Detection Rulesets` button Manages the rulesets of the paired GCaps	*`Detection Rulesets` section of the `GCaps profiles` screen* *Configuring the detection rulesets via the GCap profile*
3	`Base variables` button Manages configuration of advanced GCAP settings	*`Base variables` Section of the `GCaps profiles` screen* *Configuring the Base variables parameters via the GCap profile*
4	`Net variables` button Manages network variables used in Sigflow rules	*`Net variables` section of the `Config Gcaps profiles` menu* *Configuring the network variables parameters via the GCap profile*
5	`Flow timeouts` button Configures how long Sigflow keeps a stream in memory based on its state	*`Flow timeouts` section of the `GCaps profiles` screen* *Configuring the flow timeouts via the GCap profile*
6	`File rule management` button Configures the file types that the GCap will extract for a given protocol	*`File rules` section of the `GCaps profiles` screen* *Configuring the file reconstruction rules via the GCap profile*
7	`Packet filters` button Adjusts GCap capture settings with advanced Sigflow features	*`Packet filters` section of the `Gcaps profiles` screen* *Configuring filters on targeted parts of the analyzed traffic via the GCap profile*
8	`Reset to default configuration` button Resets the configuration and loads the selected profile in the `GCaps pairing and status` screen	
9	`GCap pairing` button Displays the screen to manage the pairing of a GCap	*`GCaps Pairing` screen*

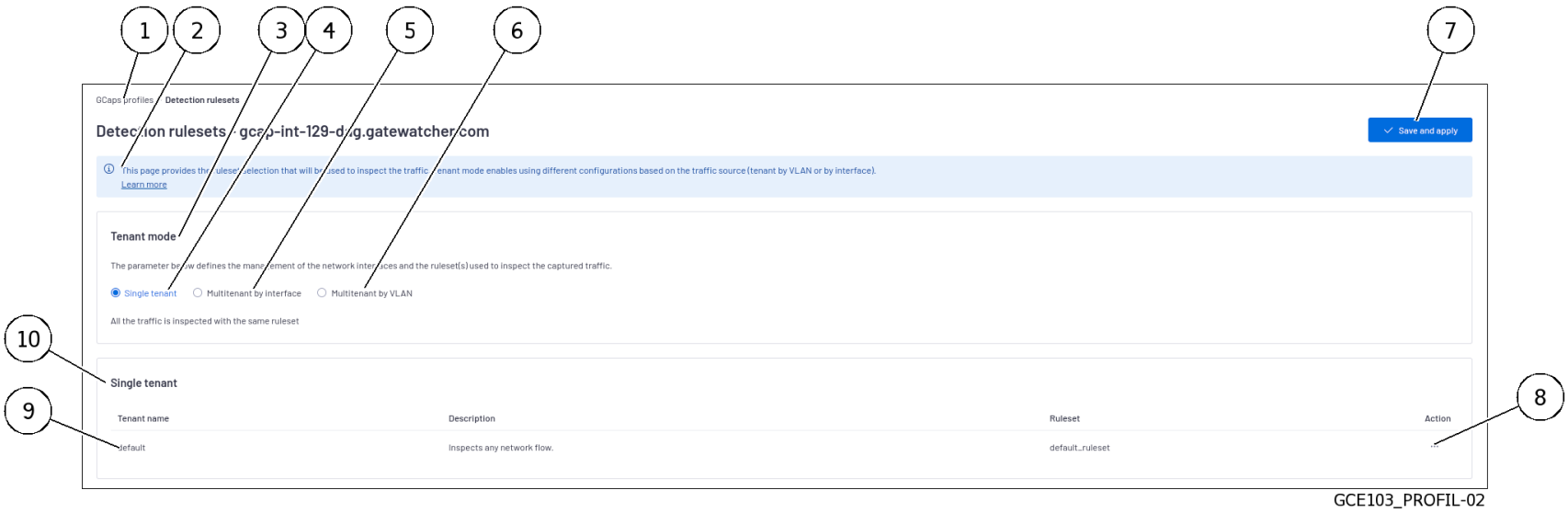
Note:

The buttons listed above give access to the parts listed below, each managing a subset of the configuration.
Each change is automatically saved.
The use of an `APPLY` button triggers the transmission of the global configuration to the selected GCap.

5.7.2.2.4 `Detection Rulesets` section of the `GCaps profiles` screen

The `Detection Rulesets` screen enables to define the current Tenant mode.
It enables using different configurations based on the traffic source:

- The `single tenant`: only one ruleset is used to analyze the traffic
- The `multi-tenant by interface`: the traffic is inspected with different rulesets, depending on the network interface it is captured on
- The `multi-tenant by VLAN`: the traffic is inspected with different rulesets, depending on its VLAN

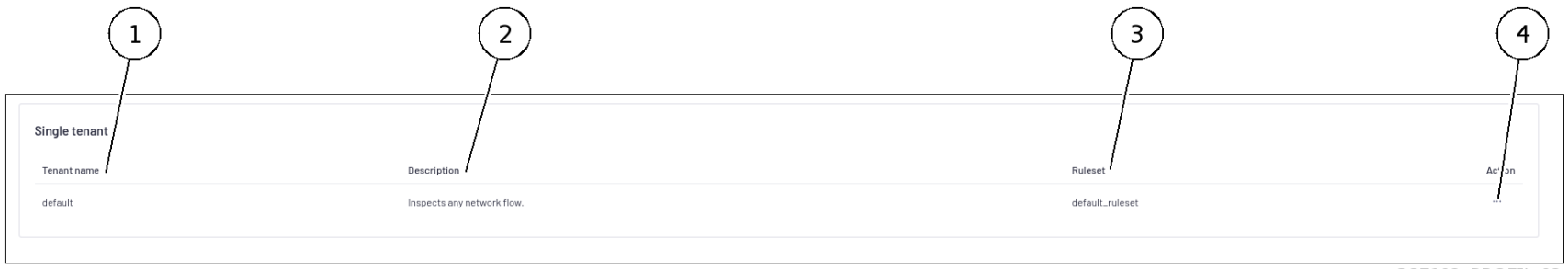


GCE103_PROFIL-02

Item	Name	Function
1	`Gcaps profiles`	Link to return to the `GCaps profiles` screen
2		Message box to inform that the selected ruleset has been updated
3	`Tenant mode` zone	Provides the ruleset selection that will be used to inspect the traffic whatever interface is present
4	`Single tenant` choice	Defines the ruleset used to inspect all the traffic If this choice is selected, the `Single tenant` part is displayed: see below the description of the **Single tenant part**
5	`Multitenant by interface` choice	Defines the rulesets used for each of the interfaces If this choice is selected, the `Single tenant` part is displayed: see below the description of the **Multitenant by interface part**
6	`Multitenant by VLAN` choice	Defines the rulesets used for each VLAN
7	`Save and apply` button	Saves the parameters of the current option (Single tenant...) then saves parameters and makes rulesets available to GCaps
10		Part of the screen which display the parameters of the configuration selected In this example, the `Single tenant` choice is selected.
9		This part displays the parameters of choice selected (4 to 6)
8	`Action` field	Displays the list of possible actions

5.7.2.2.4.1 `Single tenant` part

The `Single tenant` part displays the parameters of this configuration, i.e displays the current ruleset used by the GCap.
It is possible to modify this ruleset.

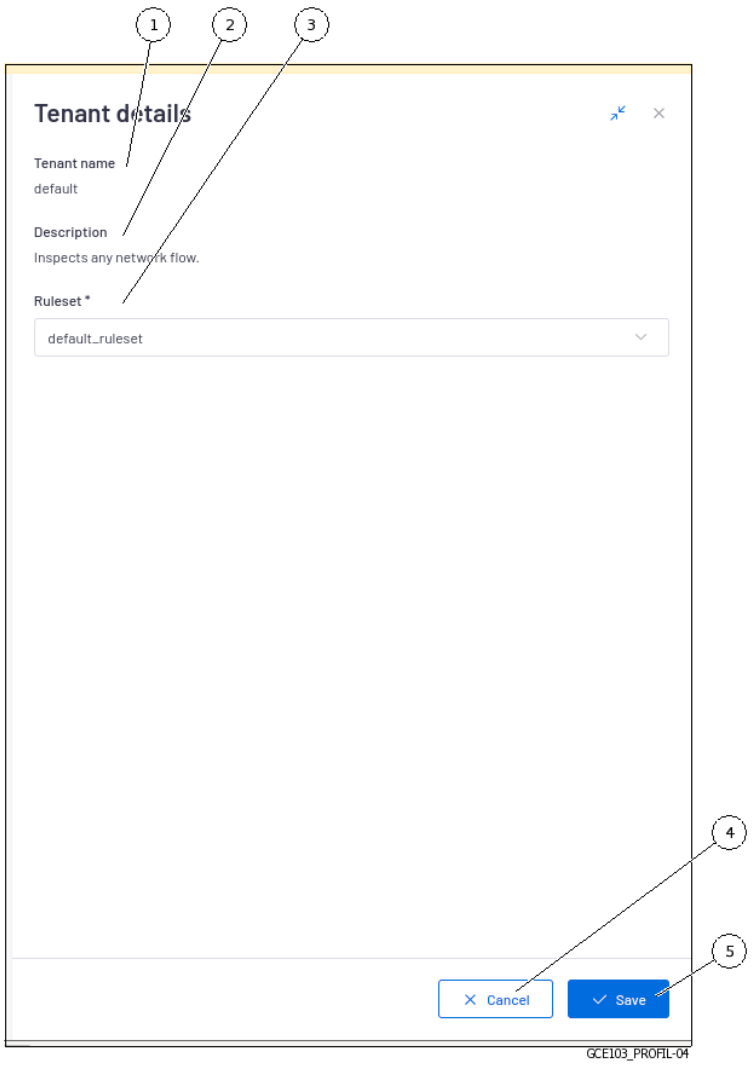


GCE103_PROFIL-03

Item	Name	Function
1	`Tenant name` field	Displays the tenant name Default value is `default`
2	`Description` field	Displays the tenant description Default value is `Inspects any network flow`
3	`Ruleset` field	Displays the current ruleset used for this tenant Default value is `default_ruleset`
4	`Action` field	Displays the `Edit tenant` command and opens the `Tenant details` window described below

5.7.2.2.4.2 `Tenant details` window

The `Tenant details` window enables to modify the ruleset to be used.

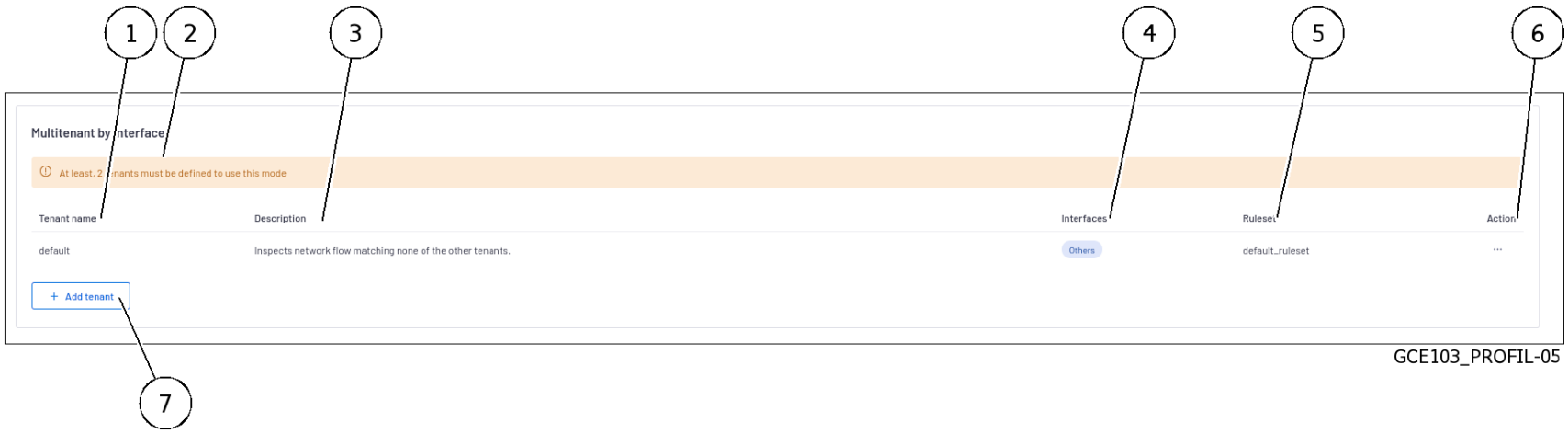


Item	Name	Function
1	`Tenant name` field	Displays the tenant name Default value is `default`
2	`Description` field	Displays the tenant description Default value is `Inspects any network flow`
3	`Ruleset` field	Selects the ruleset to be used. Default value is `default_ruleset`
4	`Cancel` button	Cancel the current modifications
5	`Save` button	Saves the current modifications

5.7.2.2.4.3 `Multitenant by interface` part

The `Multitenant by interface` part displays the GCap existing interfaces and the ruleset used fo each interface.
Is is possible:

- To modify the ruleset used for an existing interface
- To create a new interface then select the ruleset to be applied



GCE103_PROFIL-05

Item	Name	Function
1	`Tenant name` field	Displays the tenant name Default value is `default`
2	Information field	This message `At least, two tenants must be defined to use this mode`` indicates the requirement to have 2 interfaces (tenant) defined In this example only one tenant is defined
3	`Description` field	Displays the tenant description Default value is `Inspects network flow matching none of the other tenants.`
4	`Interfaces` field	Displays the used interface name Default value is `others`
5	`Ruleset` field	Displays the current ruleset used for this interface Default value is `default_ruleset`
6	`Action` field	Displays the `Edit tenant` command of the `Tenant details` window. The `Tenant details` window enables to modify: - The `Tenant name`, `Description` fields - The `Interfaces` and `Ruleset`
7	`Add tenant` button opens the window described below	Enables adding a new tenant

GCE103_PROFIL-09

In this example, there are three tenants:

- The tenant named `default` (1) allows:
- To analyze the traffic coming from interfaces not defined by other tenants (indicated by the name `Others`)
- To configure the Sigflow engine with rules defined in ruleset named with defaul_ruleset

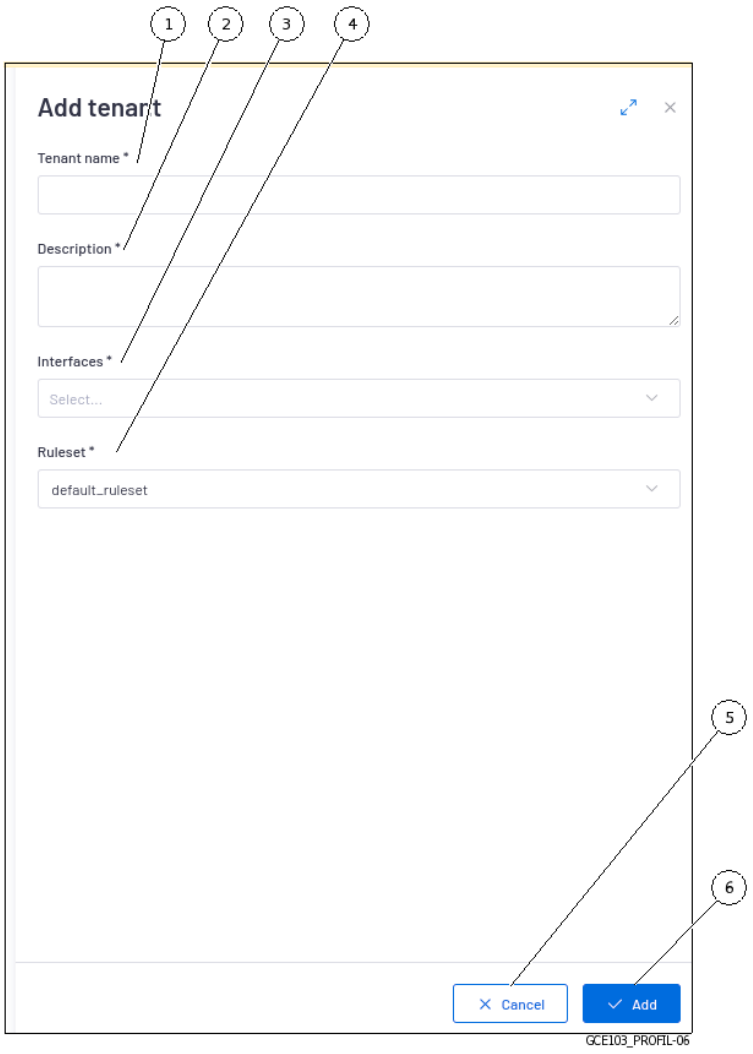
- The tenant named `monvirt` (2) allows:
- To analyze the traffic coming from the monvirt interface (indicated by the name `monvirt`)
- To configure the Sigflow engine with rules defined in ruleset named with ruleset-test3
- The tenant named `tenant mon0t` (3) allows:
- To analyze the traffic coming from the mon0 interface (indicated by the name `mon0`)
- To configure the Sigflow engine with rules defined in ruleset named with ruleset-test

---

5.7.2.2.4.4 `Add tenant` window

The `Add tenant` window enables:

- To add a new interface
- To select a ruleset for this new interface

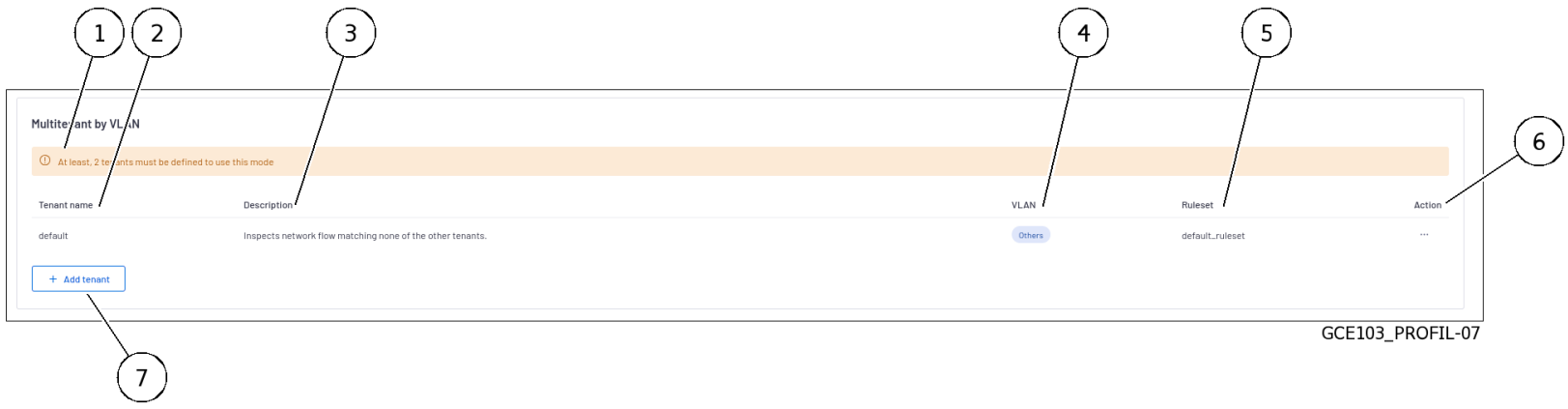


Item	Name	Function
1	Champ `Tenant name` field	Enables to enter the tenant name Default value is `default`
2	Champ `Description`	Displays the tenant description Default value is `Inspects network flow matching none of the other tenants.`
3	`Interfaces` field	Field to select interface to be used No default value
4	`Ruleset` field	Selects the ruleset to be used Default value is `default_ruleset`
5	`Cancel` button	Cancels the current modifications
6	`Save` button	Saves the current modifications

5.7.2.2.4.5 Multitenant by VLAN part

The `Multitenant by VLAN` part displays the existing VLAN and the ruleset used fo each VLAN.
Is is possible:

- To modify the ruleset used for an existing VLAN
- To create a new VLAN then select the ruleset to be applied

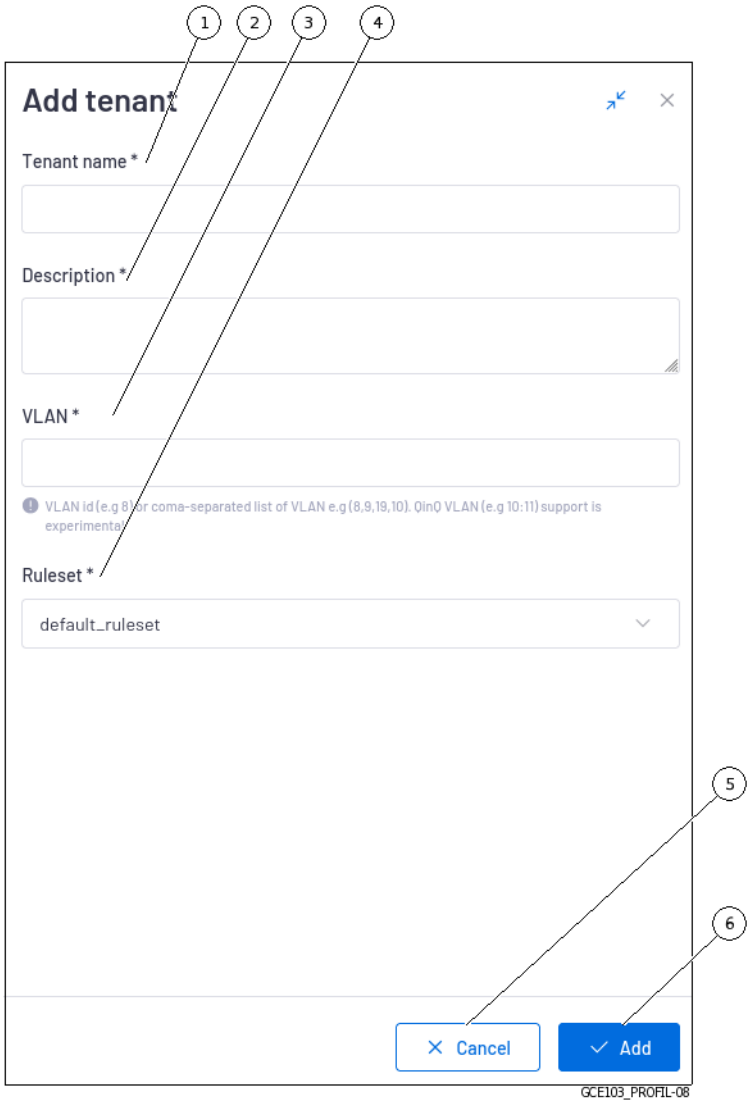


Item	Name	Function
1	Information field	This message `At least, 2 tenants must be defined to use this mode` indicates the requirement to have 2 interfaces (tenant) defined In this example only one tenant is defined
2	`Tenant name` field	Displays the tenant name Default value is `default`
3	`Description` field	Displays the tenant description Default value is `Inspects network flow matching none of the other tenants.`
4	`VLAN` field	Displays the used VLAN name Default value is `others`
5	`Ruleset` field	Displays the current ruleset used for this VLAN Default value is `default_ruleset`
6	`Action` field	Displays the `Edit tenant` command of the `Tenant details` window The `Tenant details` window enables to modify: - The `Tenant name`, `Description` fields - The `VLAN` and `Ruleset`
7	`Add tenant` button opens the window described below	Enables adding a new tenant i.e: - To enter the `Tenant name`, `Description` - To select `VLAN` and `Ruleset`

5.7.2.2.4.6 `Add tenant` window

The `Add tenant` window enables:

- To add a new VLAN
- To select a ruleset foo this new VLAN



Item	Name	Function
1	`Tenant name` field	Displays the tenant name Default value is `default`
2	`Description` field	Displays the tenant description Default value is `Inspects network flow matching none of the other tenants.`
3	`VLAN` field	Selects VLAN to be used No default value
4	`Ruleset` field	Selects the ruleset to be used. Default value is `default_ruleset`
5	`Cancel` button	Cancels the current modifications
6	`Save` button	Saves the current modifications

5.7.2.2.5 `Base variables` Section of the `GCaps profiles` screen

The `Base variables` section enables to adjust the probe capture parameters thanks to the advanced functions of Sigflow configurable from the GCenter.
Changes to this configuration will impact alert escalation from the GCap probe to the GCenter.

Enabling some options will allow alerts, anomalies, metadata, file information, and protocol-specific records to be issued.
Alerts are records of events caused by matching a rule with network traffic.
An alert will be generated with associated metadata, such as the application layer record (HTTP, DNS, etc.).

The `Base variables` screen is comped of the following areas:

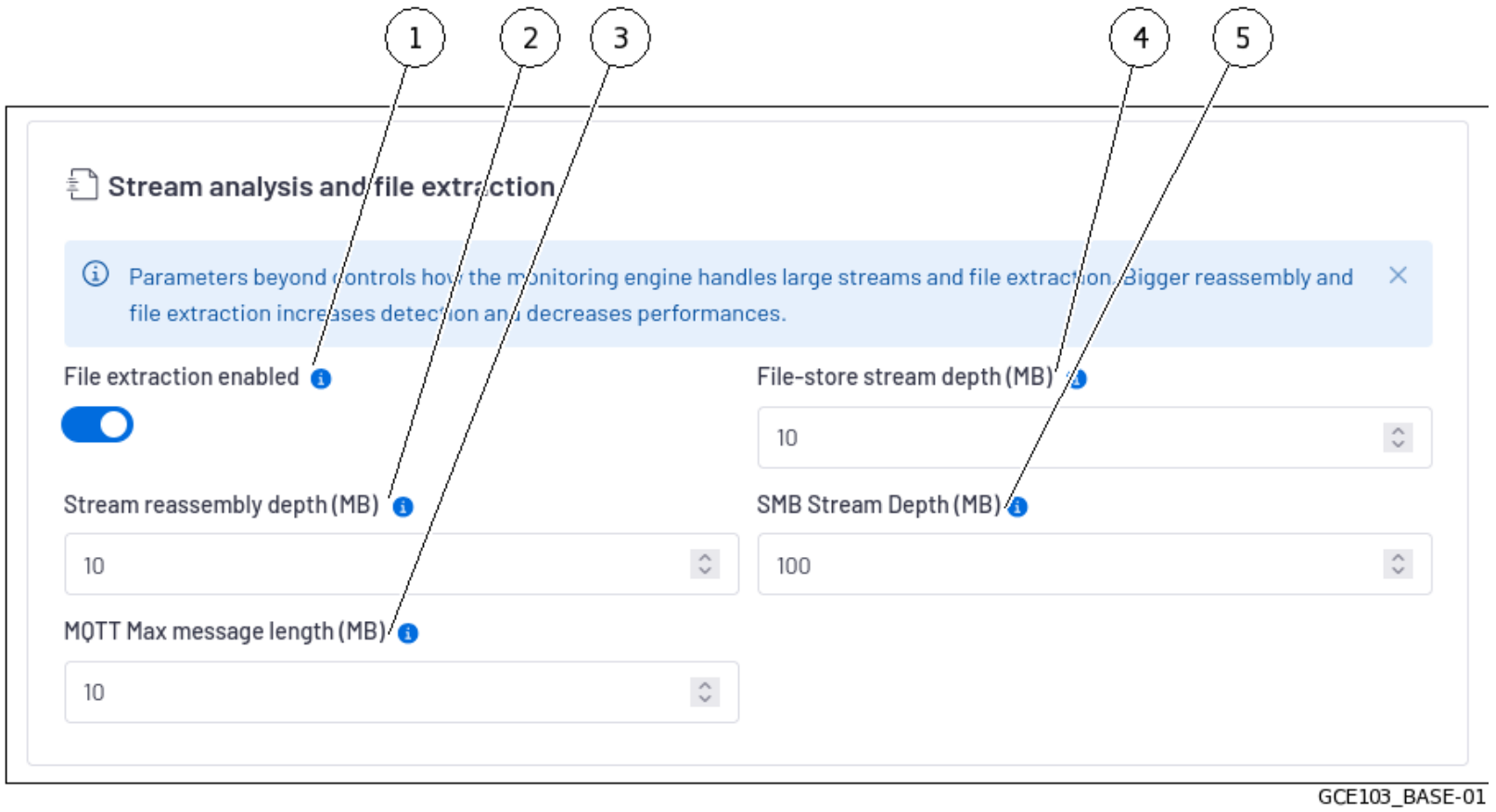
- *`Stream analysis and file extraction` zone*
- *`HTTP Proxy` Zone*
- *`Payload` zone*
- *`Community ID` zone*
- *`Alerting and logging` zone*

5.7.2.2.5.1 `Stream analysis and file extraction` zone

The Flow Analysis and File Extraction area enables to control how the Sigflow engine handles maximum flow and file extraction sizes.

5.7.2.2.5.2 Description of `Stream analysis and file extraction` area

This area allows you to activate the file extraction control and the configuration of the following elements:



GCE103_BASE-01

Item	Name	Function
1	`File extraction enabled`	Enables control of the size of stored files See *`File rules` section of the `GCaps profiles` screen* to specify which files are extracted.
2	`Stream reassembly depth (MB)`	Maximum size of network flow in megabytes. The default is a parameter that can be replaced by protocol parsers that perform file extraction. Inspection will be skipped if this value is reached for a particular flow rate. Setting this value to 0 allows storing any stream size.
3	`MQTT Max message length (MB`	Maximum size of an MQTT message to be parsed. Beyond this value, the message will not be parsed.
4	`File-store stream depth (MB)`	Maximum size of a file reconstructed and stored in megabytes. If this value is reached, the file may be truncated and may not be stored completely. This means that after this value, the HTTP session will no longer be tracked. A negative value disables the option and the value 0 allows storing any file size. If this option is not enabled, then the value of `Stream reassembly depth (Mb)` will be taken into account. This value must be greater than the value of `Stream reassembly depth (Mb)`
5	`SMB Stream Depth (MB)`	Maximum size ,in megabytes, of SMB network stream Beyond this value, no reconstruction will be performed. If this value is reached, the file may be truncated and may not be stored completely. This means that after this value, the SMB session will no longer be followed. Also, negative values disable the option. Setting this value to 0 allows storing any file size.

Tip:

A value too large for these parameters increases detection but decreases performance.

Caution:

Changing these parameters may cause solution malfunctions. This part is reserved for support and advanced users.

Only the variable `file_store_stream_depth_mb` can be modified, never exceeding 100 MB.

5.7.2.2.5.3 Default configuration of the `Base variables`

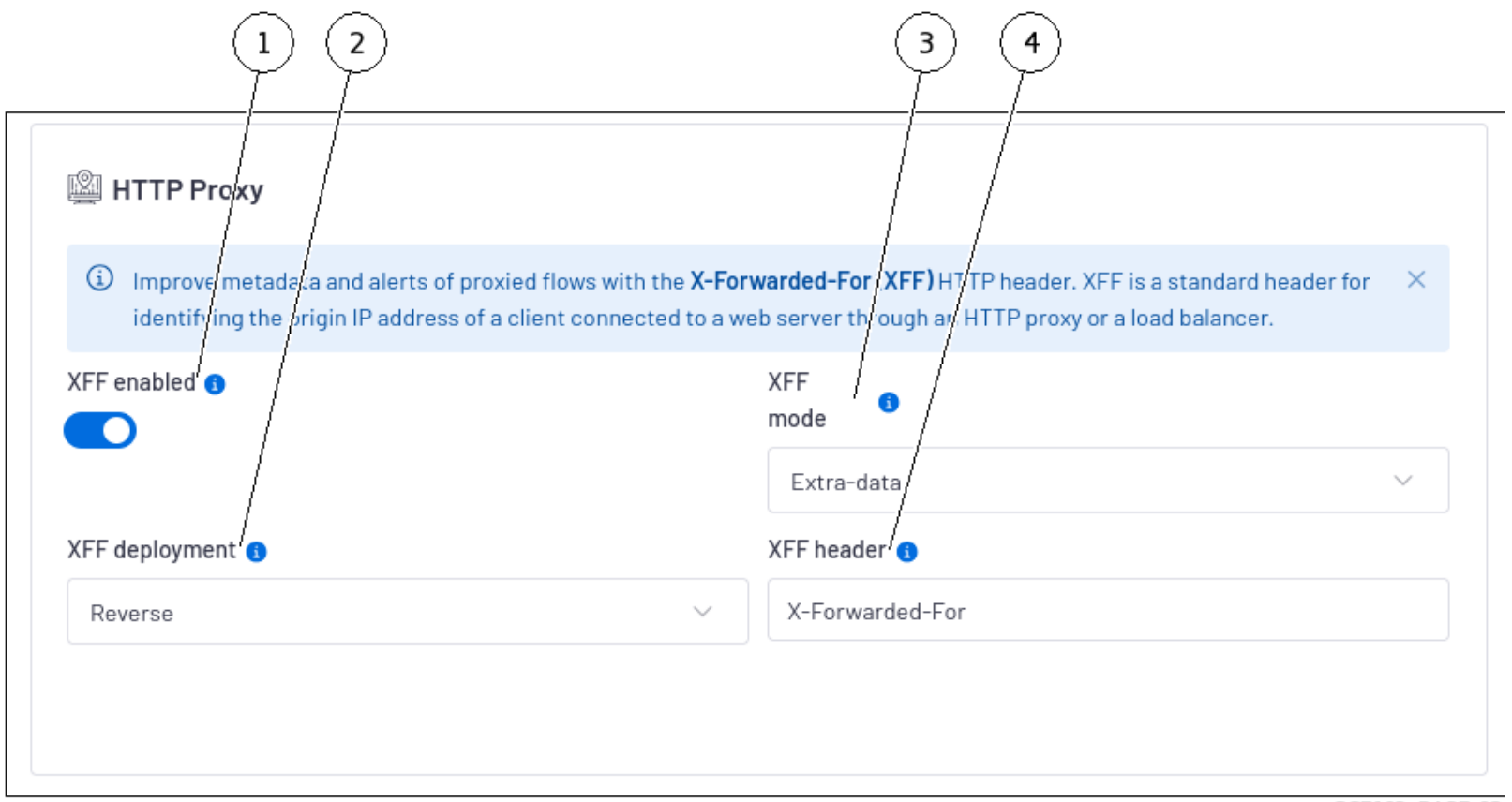
Variable	Essential profil	Balanced profil	Deep profil	Paranoid profil	Performance profil
File extraction enabled	Enabled	Enabled	Enabled	Enabled	Enabled
File-store stream depth (MB)	10	10	10	10	10
Stream reassembly depth (MB)	10	10	10	10	5
SMB Stream Depth (MB)	100	100	100	100	10
MQTT Max message length (MB)	10	10	10	10	10

5.7.2.2.5.4 `HTTP Proxy` Zone

The `HTTP Proxy` zone improves the metadata and alerts of the mandated streams with the X-Forwarded-For (XFF) http header.
XFF is a standard header for identifying the original IP address of a client connecting to a web server via an HTTP proxy or load balancer.

5.7.2.2.5.5 Description of the `HTTP Proxy` zone

This zone includes the following:



Item	Name	Function
1	`XFF enabled` selector	Enable HTTP header management *X-Forwarded-For* by adding a new field or by overwriting the source or destination ip address (depending on the direction of the flow) by the IP entered in this header. The behavior (adding field or overwriting) is managed by the directive `XFF mode`. This directive is useful in the case of processing flows behind a reverse proxy for example.
2	`XFF deployment`	XFF deployment type. Two deployment types are available (`reverse` or `forward``). In a *reverse* deployment, the IP address used is the last while in a *forward* deployment, the IP address used is the first.
3	`XFF mode`	Behavior expected when activating XFF. Two types of operating modes are available: `extra-data` or `overwrite`. Note that in `overwrite` mode, if the IP address reported in the HTTP header X-Forwarded-For is of a different version of the received packet, then it will switch to 'extra-data' mode
4	`XFF header`	Name of the HTTP header where the actual IP address is present. If there is more than one IP address present then the last IP address is taken into account.

5.7.2.2.5.6 Default configuration of the `HTTP Proxy` zone settings

Variable	Essential profil	Balanced profil	Deep profil	Paranoid profil	Performance profil
XFF enabled	enabled	enabled	enabled	enabled	enabled
XFF mode	Extra-data	Extra-data	Extra-data	Extra-data	Extra-data
XFF deployment	Reverse	Reverse	Reverse	Reverse	Reverse
XFF header	X-Forwarded-For	X-Forwarded-For	X-Forwarded-For	X-Forwarded-For	X-Forwarded-For

---

5.7.2.2.5.7 `Payload` zone

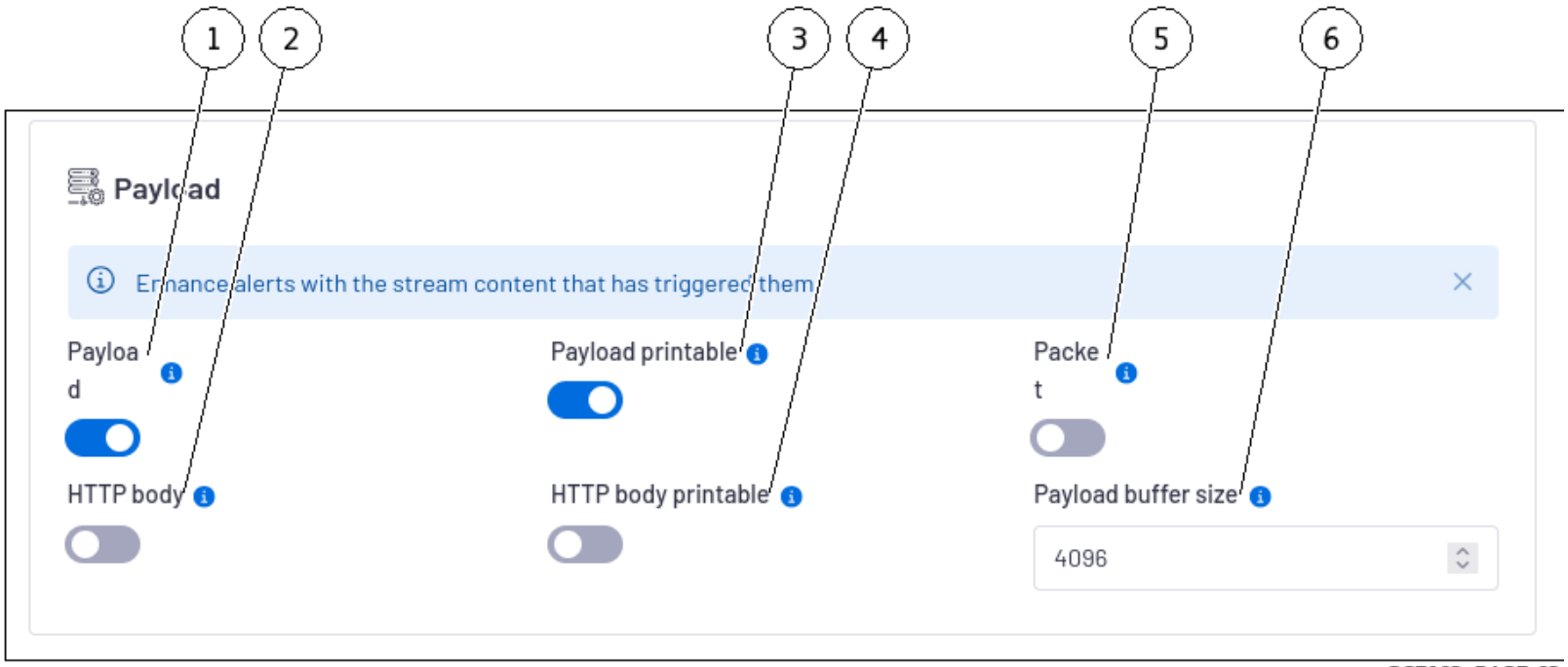
This zone enables to enrich alerts with the content of the feed that triggered them.

Note:

Enabling all of the following fields can generate events larger than 65kb, but exporting data cannot transmit events larger than that size. In case an event exceeds 65ko, it will be truncated and the remote server will not receive the entire event.

5.7.2.2.5.8 Description of `Payload` zone

This zone includes the following:



Item	Name	Function
1	`Payload` selector	Adds a field containing the payload encoded in base 64 of a stream triggering an alert
2	`HTTP body` selector	Adds a field containing the body of HTTP requests encode to base64. To work, this parameter requires metadata.
3	`Payload printable` selector	Adds a field containing the payload (*Payload*) in ASCII format (known as 'human')
4	`HTTP body printable` selector	Adds a field containing the body of HTTP requests in ASCII format. To work, this parameter requires metadata.
5	`Packet` selector	Dumps the captured packet encoded in base64
6	`Payload buffer size` selector	Maximum size of the payload buffer to be added to the alert

---

5.7.2.2.5.9 Default configuration of `Payload` zone settings

Variable	Essential profil	Balanced profil	Deep profil	Paranoid profil	Performance profil
Payload	Enabled	Enabled	Enabled	Enabled	Enabled
Payload printable	Enabled-data	Enabled-data	Enabled-data	Enabled-data	Enabled-data
Packet	Disabled	Disabled	Enabled	Enabled	Disabled
HTTP body	Disabled	Disabled	Enabled	Enabled	Disabled
HTTP body printable	Disabled	Disabled	Enabled	Enabled	Disabled
Payload buffer size	4096	4096	4096	4096	2048

5.7.2.2.5.10 `Community ID` zone

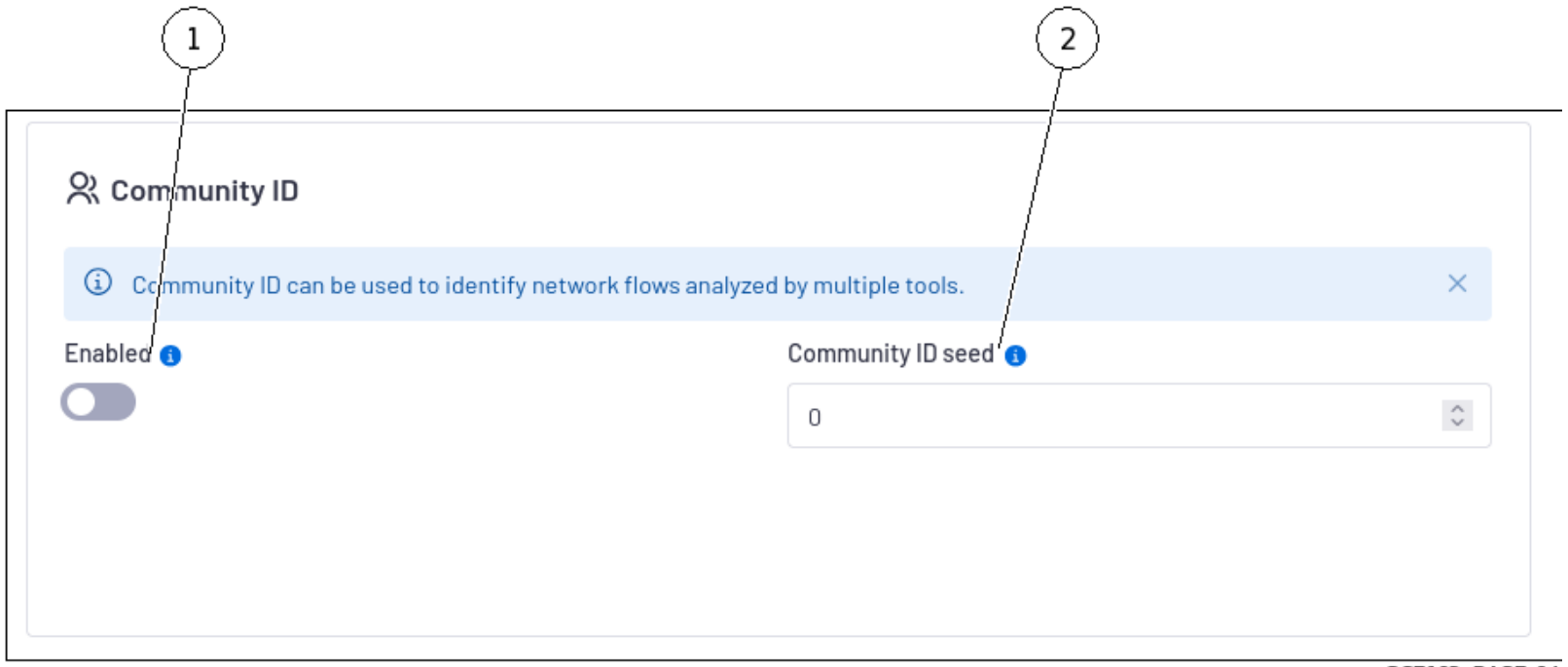
This zone enables:

- To activate the `Community ID` field in the events. The latter identifies the network flows analyzed
- To configure the "seed" to make it identical to other tools of the same information system

---

5.7.2.2.5.11 Description of the `Community ID` zone

The zone includes the following:



GCE103_BASE-04

Item	Name	Function
1	`Enabled` selector	Add the `Community ID` field in the events
2	`Community ID seed`	Configure the "seed" to make it identical to other tools

---

5.7.2.2.5.12 Default configuration of the `Community ID` zone settings

Variable	Essential profil	Balanced profil	Deep profil	Paranoid profil	Performance profil
On/Off	disabled	disabled	disabled	Enabled	disabled
Community ID seed	0	0	0	4096	0

5.7.2.2.5.13 `Alerting and logging` zone

This zone defines which protocol are inspected (alerting) and if the generation of metadata is enabled (logging).

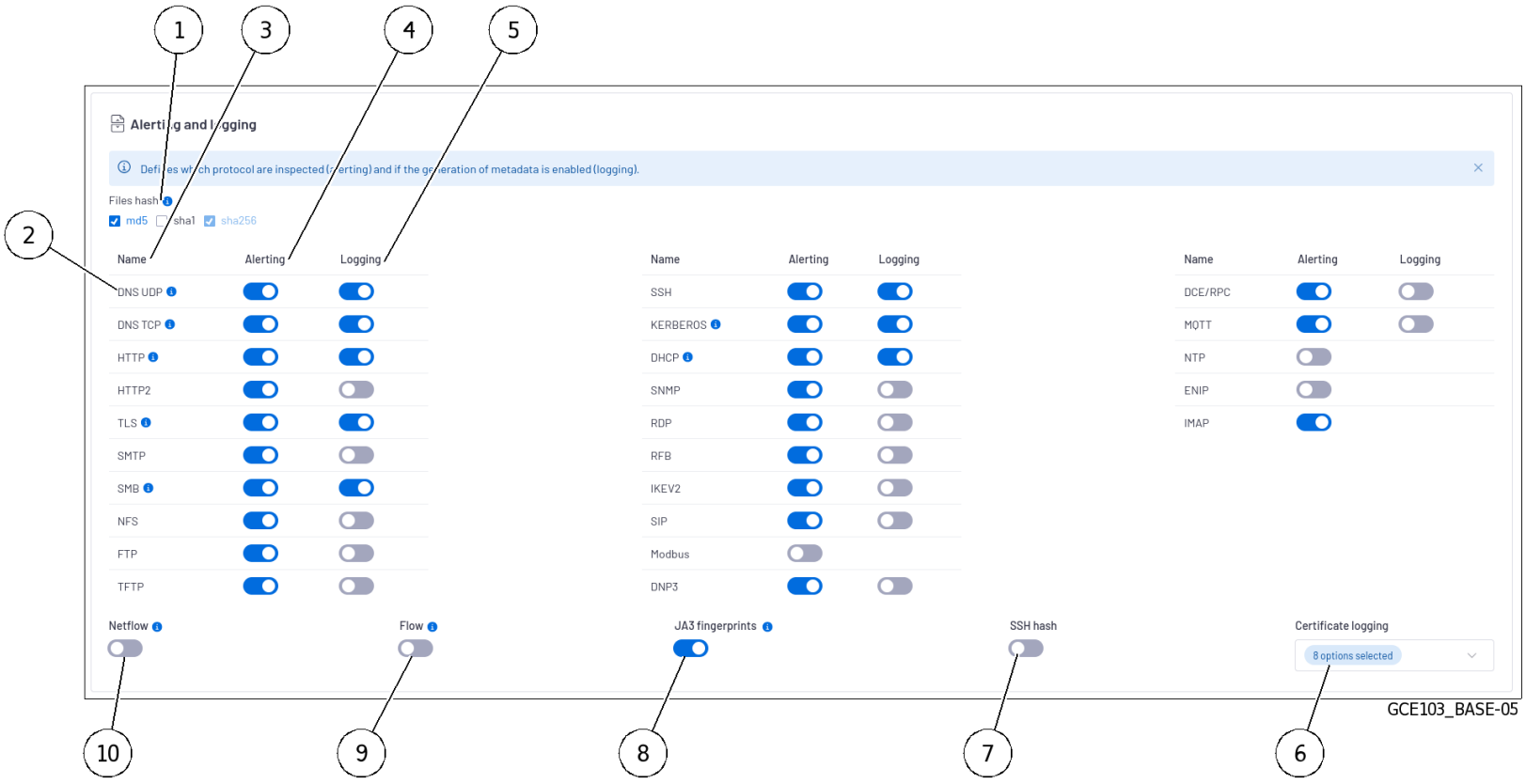
Note:

In the event that a GCap has a version ahead of the GCenter, it is possible that some protocols are not yet implemented in the GCenter.

This is discussed in more detail in the documentation GCap in the section *Moteur de détection > 3. Sélectionner les protocoles analysés*

5.7.2.2.5.14 Description of the `Alerting and logging` zone

This zone includes the following items:



Item	Function
1	Selector for choosing the hash function for reconstructed files (md5, sha1 and sha256) By default, md5 is selected. The sha256 hash will in all cases be added by the Malcore module
2	List of protocols. For each of these protocols, are listed: - The name (3) - The switch for enabling the `alerting` (4) - The switch for enabling the `logging` (5) The parameters displayed here are those of the profile previously loaded in the GCap. This was done by: - Using the `GCaps pairing` command in the *`GCaps Pairing` screen*. - Select a default profiles such as Essential, Balanced, Deep, Paranoid, and Performance: in order from most to least permissive
6	`Certificate logging`. Number of enabled Logging In this example, there are 8 enabled logging
7	`SSH hash`
8	`fingerprint JA3` If enabled, JA3 fingerprints are active for the inspection of TLS flow (if TLS alerting is enabled) and the inspection of TLS logging (if TLS logging is enabled)
9	`Flow` Generate one log for each flow observed, whether it is bidirectional or not. On average, flow generates half the amount of data would have generated Warning: may generate huge amount of data
10	`Netflow` Generate one log for each flow observed for each direction: two logs are generated for each half-flow in the case of bidirectional/connection-oriented protocols Warning: may generate huge amount of data

Note:

The user can enable either `netflow`, `flow` or neither, but he cannot enable both at the same time.

Note:

The `Netflow` and `fingerprint JA3` options are disabled by default (`Balanced` profile).

- If necessary, use the `Reset to default configuration` command to reload this default profile with the default values.

5.7.2.2.5.15 Default settings for existing profiles available

Protocol	Essential profil	Balanced profil	Deep profil	Paranoid profil	Performance profil
DNS_UDP	Enabled	Enabled	Enabled	Enabled	Enabled
DNS_TCP	Enabled	Enabled	Enabled	Enabled	Enabled
HTTP	Enabled	Enabled	Enabled	Enabled	Enabled
HTTP2	Enabled	Enabled	Enabled	Enabled	Enabled
TLS	Enabled	Enabled	Enabled	Enabled	Enabled
SMTP	Enabled	Enabled	Enabled	Enabled	Enabled
SMB	Enabled	Enabled	Enabled	Enabled	Enabled
NFS	Enabled	Enabled	Enabled	Enabled	Enabled
FTP	Enabled	Enabled	Enabled	Enabled	Enabled
TFTP	Enabled	Enabled	Enabled	Enabled	Enabled
SSH	Enabled	Enabled	Enabled	Enabled	Enabled
KERBEROS	Enabled	Enabled	Enabled	Enabled	Enabled
DHCP	Enabled	Enabled	Enabled	Enabled	Enabled
SNMP	Enabled	Enabled	Enabled	Enabled	Enabled
RDP	Enabled	Enabled	Enabled	Enabled	Enabled
RFB	Enabled	Enabled	Enabled	Enabled	Disabled
IKEV2	Enabled	Enabled	Enabled	Enabled	Disabled
SIP	Enabled	Enabled	Enabled	Enabled	Disabled
Modbus	Disabled	Enabled	Enabled	Enabled	Disabled
DNP3	Enabled	Enabled	Enabled	Enabled	Disabled
DCE/RPC	Enabled	Enabled	Enabled	Enabled	Disabled
MQTT	Enabled	Enabled	Enabled	Enabled	Enabled
NTP	Disabled	Enabled	Enabled	Enabled	Disabled
ENIP	Disabled	Enabled	Enabled	Enabled	Disabled
IMAP	Enabled	Enabled	Enabled	Enabled	Disabled

5.7.2.2.5.16 The default values of the parameters

Protocol	Essential profil	Balanced profil	Deep profil	Paranoid profil	Performance profil
Netflow	Disabled	Disabled	Disabled	Disabled	Disabled
Flow	Disabled	Disabled	Disabled	Disabled	Disabled
JA3 fingerprints	Enabled	Enabled	Enabled	Enabled	Disabled
SSH hash	Disabled	Disabled	Enabled	Enabled	Disabled

5.7.2.2.6 `Net variables` section of the `Config Gcaps profiles` menu

5.7.2.2.6.1 Information on the `Net variables` section

Network variables are used by Sigflow rules to assess which flow must be inspected and in which direction.
In the structure of a rule, just after 'alert' and the protocol keyword, it is possible to use variables that will enable defining groups of IP addresses.

In the following example:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL SCAN NULL"; flow:stateless; ack:0; flags:0; seq:0;␣
↪reference:arachnids,4; classtype:attempted-recon; sid:2100623; rev:7;)
```

For an alert to be raised under this rule, the source must therefore be included in the $EXTERNAL_NET variable and its destination in the $HOME_NET variable.
Both the traffic source and the traffic destination must be specified.
IP addresses (IPv4 and IPv6 are supported) or networks can be assigned. These parameters will be used instead of variables in the detection rules.

Variables adapt as needed and rules can change according to the specified values:

- `list`: enables the action of the rule to be defined in relation to the variable
- `default (equals to HOME_NET)`: enables defining the action of the rule in relation to the addresses given in the HOME_NET environment
- `exclude (opposite of HOME_NET)`: enables the rule to be used for all addresses that are not part of the HOME_NET environment

It is not necessary to define an address for each of the existing variables.
By default, if nothing is specified, this is equivalent to applying the rule to all traffic (the variable is equivalent to any).

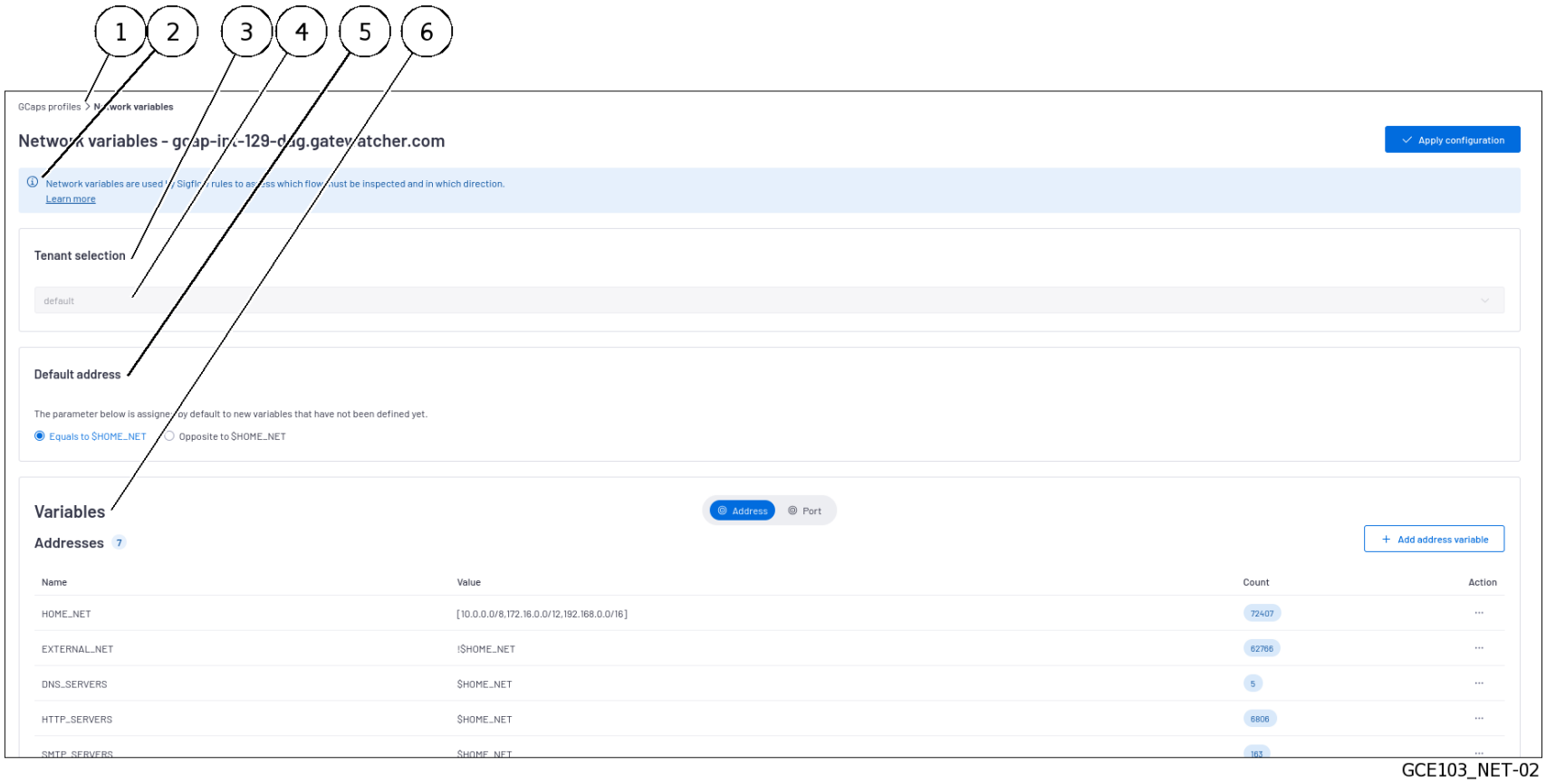
Note:

Good practice for the $EXTERNAL_NET variable is to choose the value "Opposite of HOME_NET", anything that is not $HOME_NET by definition.

The `Net variables` area enables defining the contents of these variables used in Sigflow rules.

5.7.2.2.6.2 Description of the `Net variables` zone

This zone includes the following items:

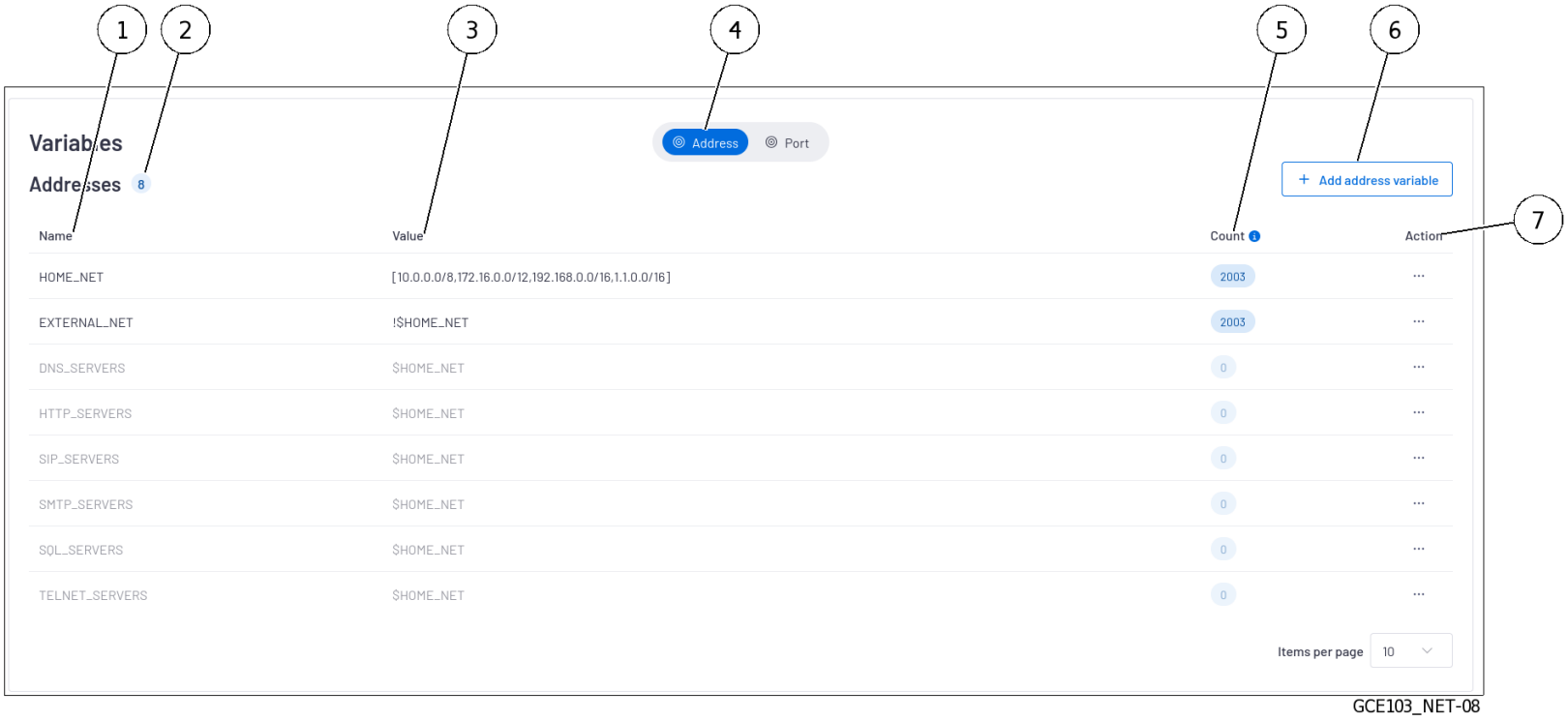


GCE103_NET-02

Item	Function
1	Link to return to the `GCaps profiles` screen
2	Message `Network variables are used by Sigflow rules to assess which flow must be inspected and in which direction.
3	`Tenant selection` zone Provides the tenant selection depends of the current tenant mode: - For `Single tenant` mode, the `Tenant selection` zone is not activated - For `Multitenant by interface` mode, the `Tenant selection` zone (4) allows to select the interface - For `Multitenant by VLAN mode` mode, the `Tenant selection` zone (4) allows to select the VLAN
5	`Default address` zone The parameter is assigned by default to new variables that have not been defined yet 2 choices: `Equals to $HOME_NET` or `Opposite to $HOME_NET`
6	`Variables` zone The zone contents two categories: - `Address`: to define the address variables - `Port`: to define the port variables

5.7.2.2.6.3 `Address` category in `Variables` mode

The `Address` category (4) of the `Variables` screen is composed of:



GCE103_NET-08

Item	Name	Field
2		The total number of addresses is indicated in this field
1	`Name`	: indicates the address name
3	`Value`	: indicates the current value of the current variable
5	`Count`	: number of time that variable is used in the ruleset of the selected tenant
7	`Action`	: displays the `Edit` command and opens the `Address variable details` window The `Address variable details` window enables to modify the `Name` field and the `Value` field
6	`Add address variable` button	opens the window described below Enables adding a new address parameter

Variable	Value
HOME_NET	10.0.0.0/8, 172.16.0.0/12 192.168.0.0/16
EXTERNAL_NET	HOME_NET
DNS_SERVERS	HOME_NET
HTTP_SERVERS	HOME_NET
SIP_SERVERS	HOME_NET
SMTP_SERVERS	HOME_NET
SQL_SERVERS	HOME_NET
TELNET_SERVERS	HOME_NET

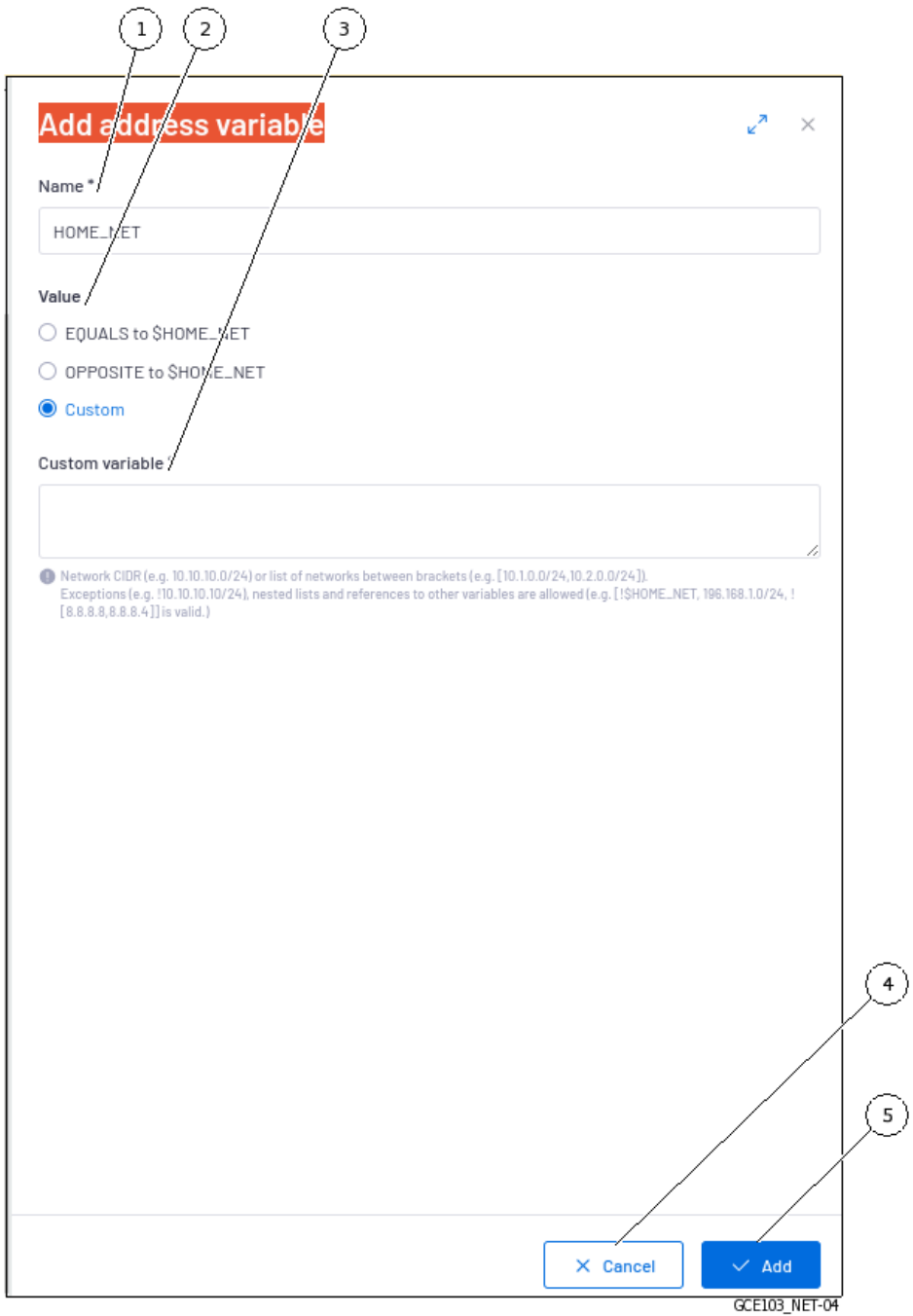
Note:

All predefined profils (Essential, Balanced, Deep, Paranoid, Performance) have the same values.

5.7.2.2.6.4 `Add address variable` window

The `Add address variable` window enables:

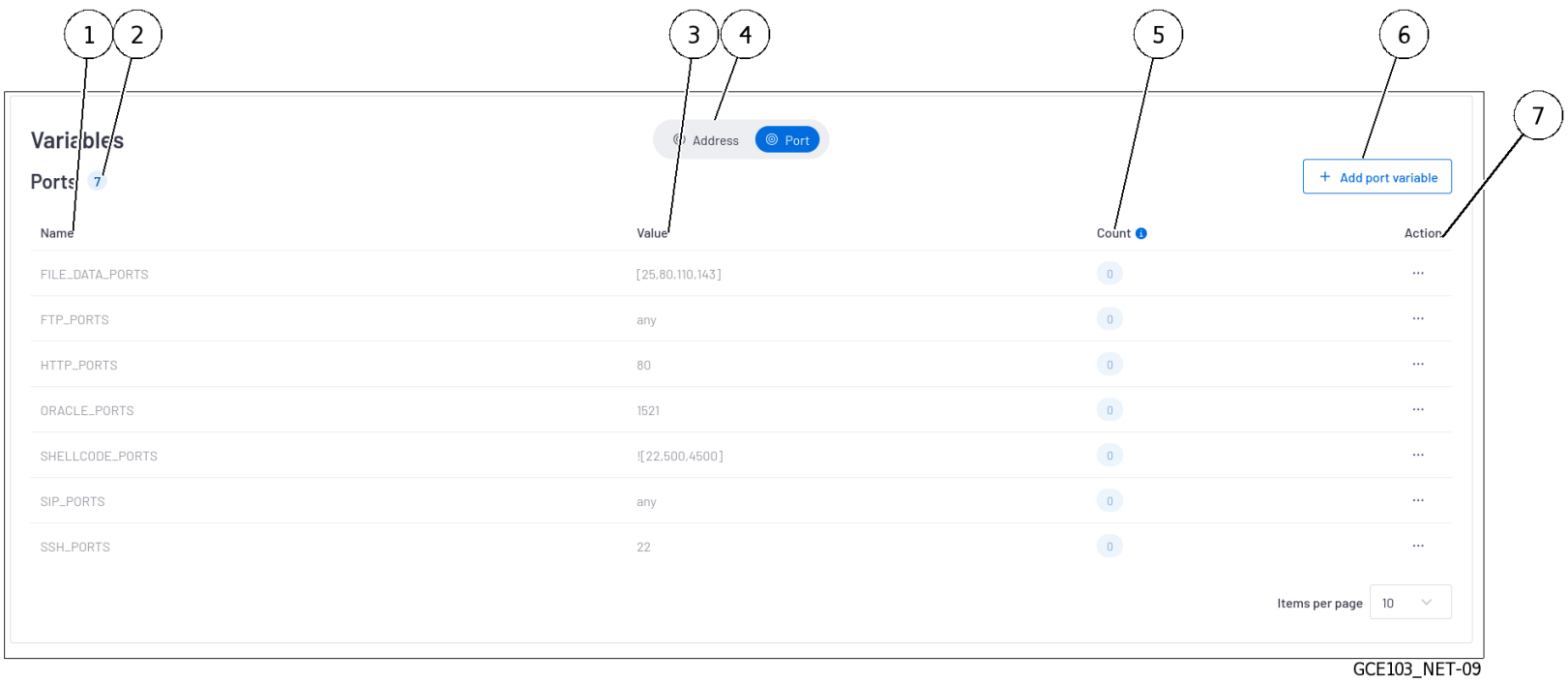
- To add a new variable
- To indicate the variable parameters



Item	Name	Function
1	`Name` field	Enables to enter the new address variable name
2	`Value` field	Displays the possible choices: `Equals to $HOME_NET` or `Opposite to $HOME_NET` or `Custom` Default value is `Inspects network flow matching none of the other tenants.`
3	`Custom variable`	Field to enter value if this choice is selected Network CIDR (e.g. 10.10.10.0/24) or list of networks between brackets (e.g. [10.1.0.0/24,10.2.0.0/24]). Exceptions (e.g. !10.10.10.10/24), nested lists and references to other variables are allowed (e.g. [!$HOME_NET, 196.168.1.0/24, ![8.8.8.8,8.8.8.4]] is valid.)
4	`Cancel` button	Cancels the current modifications
5	`Add` button	Adds the new variable

5.7.2.2.6.5 `Port` category in `Variables` mode

The `Port` category of the `Variables` screen is composed of:



GCE103_NET-09

Item	Name	Field
2		The total number of ports is indicated in this field
1	`Name`	Indicates the port name
3	`Value`	Indicates the current value of the current variable
5	`Count`	Indicates the variable count
7	`Action`	Displays the `Edit` command and opens the `Port variable details` window The `Address variable details` window enables to modify the `Name` field and the `Value` field
6	`Add port variable` button	Opens the window described below Enables adding a new port i.e

Variable	Value
FILE_DATA_PORTS	25,80,110,143
FTP_PORTS	any
HTTP_PORTS	80
ORACLE_PORTS	1521
SHELLCODE_PORTS	22,500,4500
SIP_PORTS	any
SSH_PORTS	22

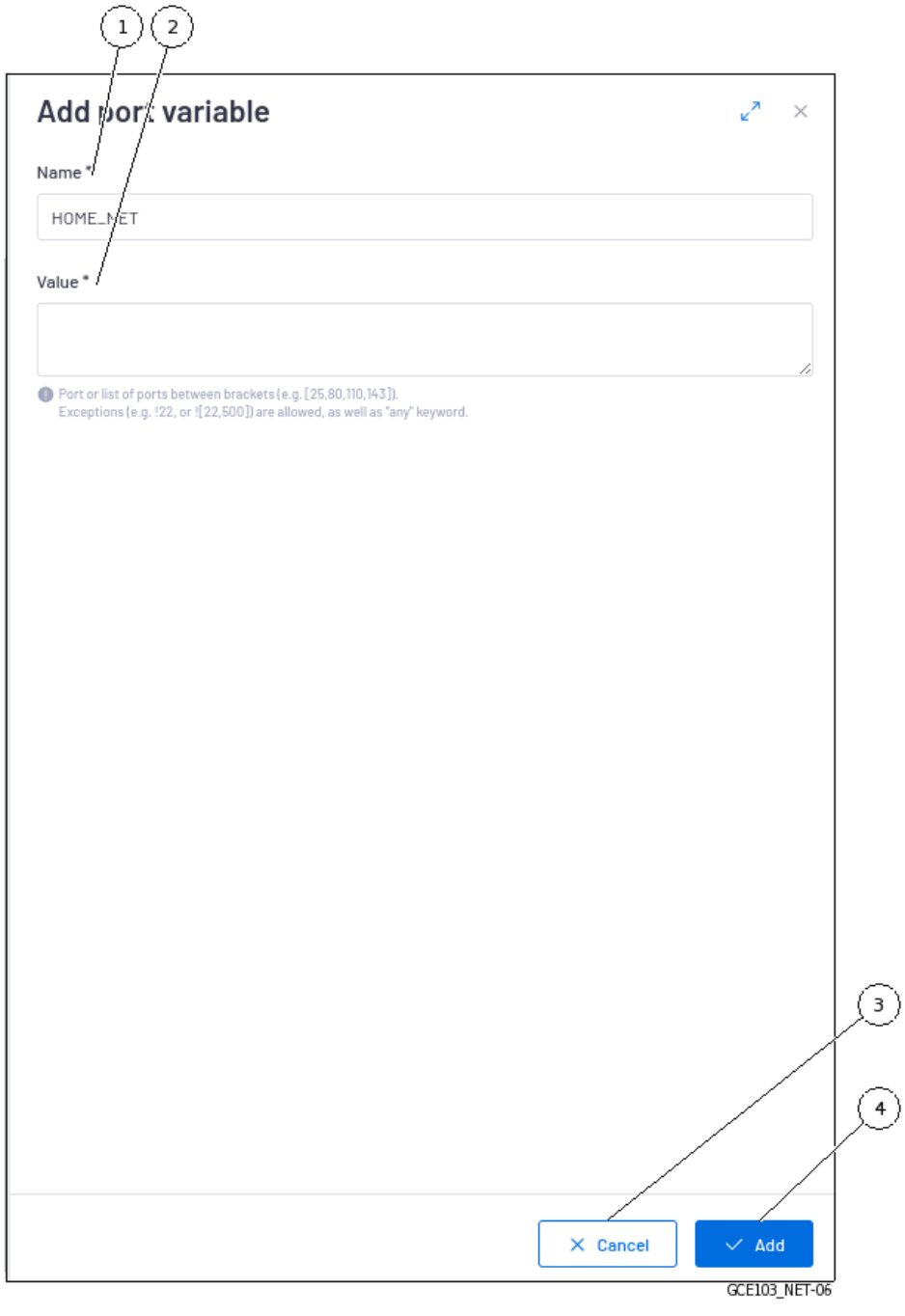
Note:

All predefined profils (Essential, Balanced, Deep, Paranoid, Performance) have the same values.

5.7.2.2.6.6 `Add port variable` window

The `Add address variable` window enables:

- To add a new variable
- To indicate the variable parameters



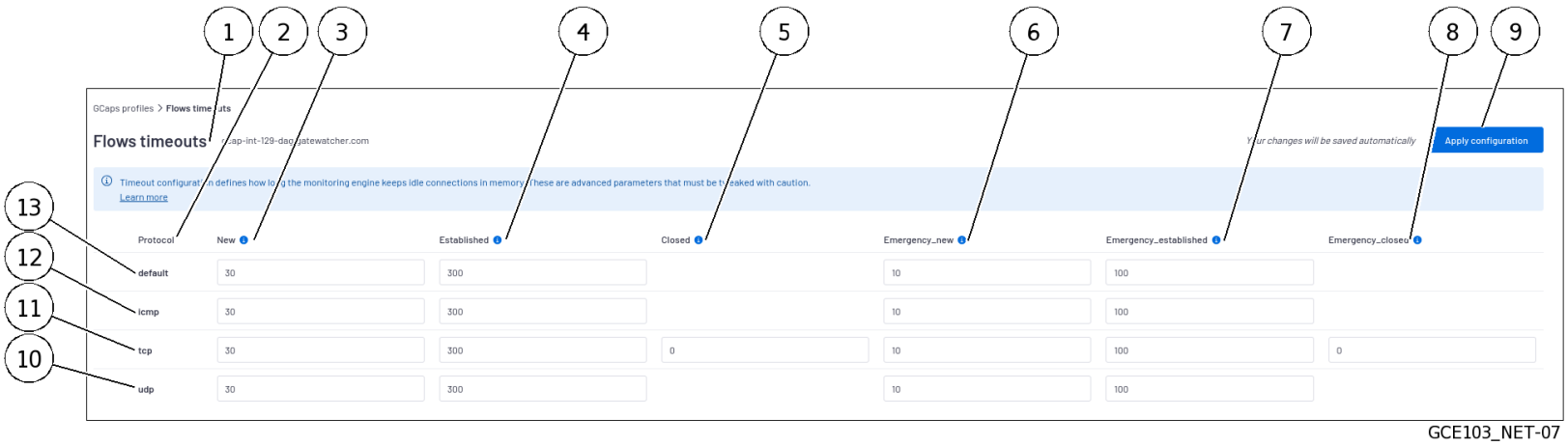
Item	Name	Function
1	`Name` field	Enables to enter the name of the new port variable
2	`Value` field	Port or list of ports between brackets (e.g. [25,80,110,143]). Exceptions (e.g. !22, or ![22,500]) are allowed, as well as "any" keyword.
3	`Cancel` button	Cancels the current modifications
4	`Add` button	Adds the new variable

5.7.2.2.7 `Flow timeouts` section of the `GCaps profiles` screen

The `Flow timeouts` section sets the timeouts of the different states (New, Established and closed) for the listed protocols.

5.7.2.2.7.1 Description of the `Flow timeouts` section

This section includes the following items:



GCE103_NET-07

Item	Function
1	GCap selected
2	List of protocols (10 to 12). For each of these protocols, the following are listed: • The `New` field (3) `New` signification: in connectionless protocol, `New` is the state during flows are in only one direction. In connection-oriented protocols, `New` is the state during the session is not established yet. This field is the time in seconds after the last activity of this flow in this status type. • The `Established` field (4): period during which the data transfer takes place. `Established` signification: In connectionless protocol, `Established` is the state during flows are bidirectional. In connection-oriented protocols, `Established` is the state during the session established. This field is the time in seconds after the last activity of this flow in this status type. • The `Closed` field (5): period during which the end of the connection is established. `Closed` signification: in connection-oriented protocols, `Closed` is the state during the session is closed (e.g. RESET or FIN handshake). This field is the time in seconds after the last activity of this flow in this status type. • The `Emergency_new` field (6) Same as New but when the engine is in emergency mode (i.e. when flow engine memcaps have been reached). • The `Emergency_established` field (7) Same as Established but when the engine is in emergency mode (i.e. when flow engine memcaps have been reached). • The `Emergency_closed` field (8) Same as Closed but when the engine is in emergency mode (i.e. when flow engine memcaps have been reached).
9	The `APPLY` button: saves and applies the configuration to the GCap

Caution:

Changing the settings in this section may cause the AIONIQ solution to malfunction.
This section is reserved for support staff and advanced users.

The UDP, TCP and ICMP protocols are configurable.
Each protocol, there are different statuses in which a flow can be found:

- Protocol TCP (11):
  - `New`
  - `Established`
  - `Closed`
- Protocols UDP (10) and ICMP (12):
  - `New`
  - `Established`

`Emergency_new`, `Emergency_established` and `Emergency_closed` are the emergency modes for the three states of TCP, UDP, and ICMP.

5.7.2.2.7.2 Default configuration of the `Flow timeouts` section

The default configuration used depending on the protocol (all values are in seconds):

Protocol	New	Established	Closed	Emergency new	Emergency established	Emergency closed
default	30	300	33	10	100	33
udp	30	300	33	10	100	33
tcp	30	300	0	10	100	0
icmp	30	300	33	10	100	33

Note:

All predefined profils (Essential, Balanced, Deep, Paranoid, Performance) have the same values.

5.7.2.2.8 `File rules` section of the `GCaps profiles` screen

5.7.2.2.8.1 Information on the `File rules` section

The `Files rules` section enables configuring the file types that the probe will retrieve for a given protocol.
The supported protocols are:

- FTP
- HTTP
- HTTP2
- NFS
- SMB
- SMTP

Files are reconstructed and then saved to disk with metadata that includes information such as:

- Time stamp
- Source/destination IP address
- Protocol
- Source/destination port
- Size
- md5sum, etc

File extraction works in parallel with the Sigflow signatures defined for these same protocols.
Each line in the `Files rules` section corresponds to an extraction rule for a file type.

Note:

Too many file extraction rules can have a significant impact on the performance of the GCap.

Note:

Changes to this section require the GCap configuration to be backed up and implemented via the `Apply` button.

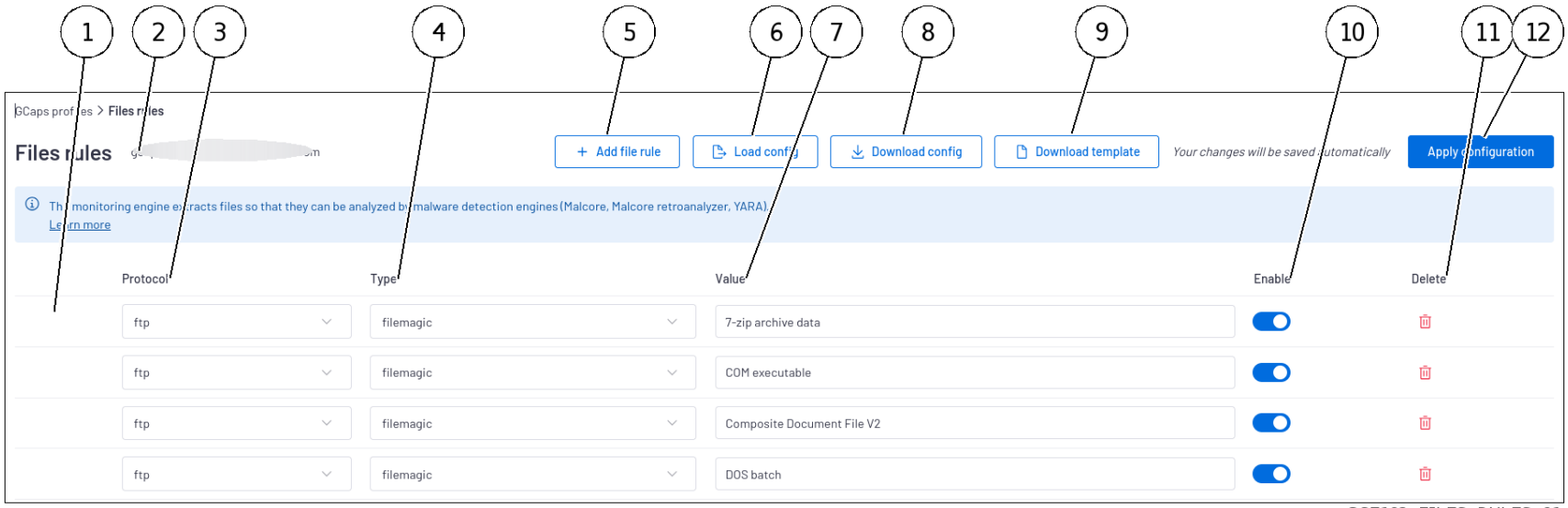
5.7.2.2.8.2 Description the `File rules management` section

This section allows:

- To show the existing the files rules for the selected GCap (2): the list displayed depends of the GCap profile used then modification made
- To add some new rules one by one or by completion of a furnished template
- To save the existing files rules

Note:

The rules displayed are those of the profile previously loaded into the GCap.
The rule list is given in paragraph *Rules applied depending on the GCap profile used*.



GCE103_FILES_RULES_01

Item	Function
1	Defining a file rule. It includes the following fields:
3	• The `Protocol` field enables selecting the protocol for which the file will be extracted from among FTP, HTTP, HTTP2, NFS, SMB, SMTP.

4	• The `Type` field enables defining the way Sigflow recognizes the file. The choices are available:
	  • The `extension` choice: this choice uses the extension to define the file type. Comparison between the extension of the rebuild file with the value entered in the `Value` field
	  • The `filemagic` choice: the filemagic function returns the file type without using the extension file then comparison between the filemagic file type with the value entered in the `Value` field

7	• The `Value` field: file type to rebuild according to the previously method
	• if the choice `extension` has been selected then this extension must be specified, e.g.:
	  • for a Javascript file, enter `js`
	  • for a Windows executable file, enter `exe`
	• if the choice `filemagic` has been selected then this information must be specified, e.g.:
	  • for a javascript file, enter `Javascript`
	  • for a windows executable file, enter `PE32 executable`

10	• The `ENABLE` selector activates this rule
11	• The `DELETE` choice deletes this line
12	The `Apply configuration` button saves the settings and sends the updated GCap profile to the selected GCap
5	The `Add file rule` button adds a new rule This button opens the window described below
6	The `Load config` button imports a pre-configured configuration file (csv type file).
8	The `Download config` button downloads the files rules configuration as a file named 1_files-rules-config.csv
9	The `Download template` button enables a configuration file template to be uploaded and populated: see *Configuration file template*

Note:

It is strongly recommended to use the filemagic type.
This is more accurate because it is based on the file's content and not on its extension.
A file is therefore reconstructed for what it really is.

The displayed rules are those of the profile previously loaded in the GCap.
This required:

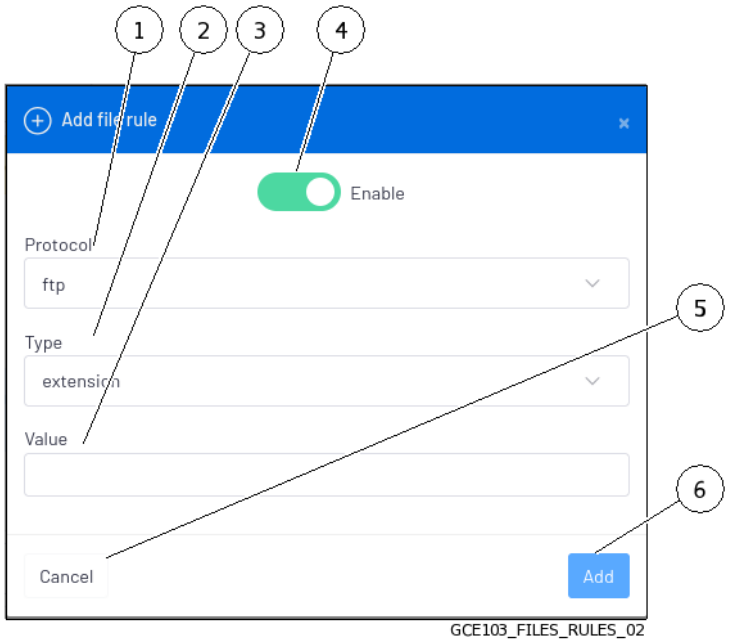
- Use the `GCaps pairing and status` command in the WebUI
- Select a default profiles such as Essential, Balanced, Deep, Paranoid, Performance

The default profile is loaded into the GCap when it is paired with the GCenter.
If necessary, it is possible to reload or change a profile on an already paired GCap with the `Reset to default configuration` command.

5.7.2.2.8.3 `Add file rule` window

The `Add file rule` window enables:

- To add a new rule
- To enter the rule parameters



Item	Name	Function
1	`Protocol` field	Selects the protocol for which the file will be extracted
2	`Type` field	Enables selecting the mode to detect the file type
3	`Value` field	Field to enter value of the file type
4	`Enable` selector	Enables or disables this rule
5	`Cancel` button	Cancels the current modifications
6	`Add` button	Adds the new rule

5.7.2.2.8.4 File named 1_files-rules-config.csv

Here is a sample file:

```
enabled,file_type,protocol,value
True,filemagic,ftp,7-zip archive data
True,filemagic,ftp,COM executable
True,filemagic,ftp,Composite Document File V2
True,filemagic,ftp,DOS batch
True,filemagic,ftp,ELF
True,filemagic,ftp,Java archive data
True,filemagic,ftp,Javascript
True,filemagic,ftp,MS Windows shortcut
True,filemagic,ftp,MS-DOS executable
True,filemagic,ftp,Mach-O
True,filemagic,ftp,Macromedia Flash
True,filemagic,ftp,Microsoft Cabinet archive data
True,filemagic,ftp,Microsoft Excel
True,filemagic,ftp,Microsoft OOXML
True,filemagic,ftp,Microsoft Office Document
True,filemagic,ftp,Microsoft PowerPoint
True,filemagic,ftp,Microsoft Word
True,filemagic,ftp,Node.js script text
True,filemagic,ftp,OS/2 REXX batch file
True,filemagic,ftp,OpenDocument
True,filemagic,ftp,PDF document
True,filemagic,ftp,PE32 executable
True,filemagic,ftp,PE32 executable (DLL)
True,filemagic,ftp,PE32+ executable
True,filemagic,ftp,POSIX tar archive
```

5.7.2.2.8.5 Configuration file template

The `Download template` button downloads a *1_files-rules-template.csv* file to the user's PC to be uploaded and populated.
After, it is possible to load this completed file with the `Load config` button.

```
enabled,file_type,id,protocol,value
true,filemagic,,ftp,Microsoft Excel
true,extension,,http,exe
true,filemagic,,http2,7-zip archive data
```

This template file contains column names and titles enabling the user to create a custom configuration file.

5.7.2.2.8.6 Rules applied depending on the GCap profile used

Protocol	Type	Values	Essential	Balanced	Deep	Paranoid	Performance
ftp	filemagic	7-zip archive data	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	COM executable	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Composite Document File V2	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	DOS batch	not created	created and enabled	created and enabled	created and enabled	not created

continues on next page

Table 1 – continued from previous page

Protocol	Type	Values	Essential	Balanced	Deep	Paranoid	Performance
ftp	filemagic	ELF	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Java archive data	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Javascript	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	MS Windows shortcut	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	MS-DOS executable	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Mach-O	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Macromedia Flash	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Microsoft Cabinet archive data	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Microsoft Excel	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Microsoft OOXML	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Microsoft Office Document	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Microsoft PowerPoint	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Microsoft Word	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Node.js script text	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	OS/2 REXX batch file	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	OpenDocument	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	PDF document	not created	created and enabled	created and enabled	created and enabled	not created

continues on next page

Table 1 – continued from previous page

Protocol	Type	Values	Essential	Balanced	Deep	Paranoid	Performance
ftp	filemagic	PE32 executable	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	PE32 executable (DLL)	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	PE32+ executable	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	POSIX tar archive	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	RAR archive data	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	Zip archive data	not created	created and enabled	created and enabled	created and enabled	not created
ftp	filemagic	gzip compressed data	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	7-zip archive data	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	COM executable	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	Composite Document File V2	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	DOS batch	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	ELF	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	Java archive data	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	Javascript	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	MS Windows shortcut	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	MS-DOS executable	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	Mach-O	not created	created and enabled	created and enabled	created and enabled	not created

continues on next page

Table 1 – continued from previous page

Protocol	Type	Values	Essential	Balanced	Deep	Paranoid	Performance
http	filemagic	Macromedia Flash	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	Microsoft Cabinet archive data	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	Microsoft Excel	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	Microsoft OOXML	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	Microsoft Office Document	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	Microsoft PowerPoint	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	Microsoft Word	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	Node.js script text	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	OS/2 REXX batch file	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	OpenDocument	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	PDF document	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	PE32 executable	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	PE32 executable (DLL)	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	PE32+ executable	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	POSIX tar archive	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	RAR archive data	not created	created and enabled	created and enabled	created and enabled	not created
http	filemagic	Zip archive data	not created	created and enabled	created and enabled	created and enabled	not created

continues on next page

Table 1 – continued from previous page

Protocol	Type	Values	Essential	Balanced	Deep	Paranoid	Performance
http	filemagic	gzip compressed data	not created	created and enabled	created and enabled	created and enabled	not created
nfs	filemagic	7-zip archive data	not created	not created	not created	created and enabled	not created
nfs	filemagic	COM executable	not created	not created	not created	created and enabled	not created
nfs	filemagic	Composite Document File V2	not created	not created	not created	created and enabled	not created
nfs	filemagic	DOS batch	not created	not created	not created	created and enabled	not created
nfs	filemagic	ELF	not created	not created	not created	created and enabled	not created
nfs	filemagic	Java archive data	not created	not created	not created	created and enabled	not created
nfs	filemagic	Javascript	not created	not created	not created	created and enabled	not created
nfs	filemagic	MS Windows shortcut	not created	not created	not created	created and enabled	not created
nfs	filemagic	MS-DOS executable	not created	not created	not created	created and enabled	not created
nfs	filemagic	Mach-O	not created	not created	not created	created and enabled	not created
nfs	filemagic	Macromedia Flash	not created	not created	not created	created and enabled d	not created
nfs	filemagic	Microsoft Cabinet archive data	not created	not created	not created	created and enabled	not created
nfs	filemagic	Microsoft Excel	not created	not created	not created	created and enabled	not created
nfs	filemagic	Microsoft OOXML	not created	not created	not created	created and enabled	not created
nfs	filemagic	Microsoft Office Document	not created	not created	not created	created and enabled	not created
nfs	filemagic	Microsoft PowerPoint	not created	not created	not created	created and enabled	not created

continues on next page

Table 1 – continued from previous page

Protocol	Type	Values	Essential	Balanced	Deep	Paranoid	Performance
nfs	filemagic	Microsoft Word	not created	not created	not created	created and enabled	not created
nfs	filemagic	Node.js script text	not created	not created	not created	created and enabled	not created
nfs	filemagic	OS/2 REXX batch file	not created	not created	not created	created and enabled	not created
nfs	filemagic	OpenDocument	not created	not created	not created	created and enabled	not created
nfs	filemagic	PDF document	not created	not created	not created	created and enabled	not created
nfs	filemagic	PE32 executable	not created	not created	not created	created and enabled	not created
nfs	filemagic	PE32 executable (DLL)	not created	not created	not created	created and enabled	not created
nfs	filemagic	PE32+ executable	not created	not created	not created	created and enabled	not created
nfs	filemagic	POSIX tar archive	not created	not created	not created	created and enabled	not created
nfs	filemagic	RAR archive data	not created	not created	not created	created and enabled	not created
nfs	filemagic	Zip archive data	not created	not created	not created	created and enabled	not created
nfs	filemagic	gzip compressed data	not created	not created	not created	created and enabled	not created
smb	filemagic	7-zip archive data	not created	not created	not created	created and enabled	not created
smb	filemagic	COM executable	not created	not created	not created	created and enabled	not created
smb	filemagic	Composite Document File V2	not created	not created	not created	created and enabled	not created
smb	filemagic	DOS batch	not created	not created	not created	created and enabled	not created
smb	filemagic	ELF	not created	not created	not created	created and enabled	not created

continues on next page

Table 1 – continued from previous page

Protocol	Type	Values	Essential	Balanced	Deep	Paranoid	Performance
smb	filemagic	Java archive data	not created	not created	not created	created and enabled	not created
smb	filemagic	Javascript	not created	not created	not created	created and enabled	not created
smb	filemagic	MS Windows shortcut	not created	not created	not created	created and enabled	not created
smb	filemagic	MS-DOS executable	not created	not created	not created	created and enabled	not created
smb	filemagic	Mach-O	not created	not created	not created	created and enabled	not created
smb	filemagic	Macromedia Flash	not created	not created	not created	created and enabled	not created
smb	filemagic	Microsoft Cabinet archive data	not created	not created	not created	created and enabled	not created
smb	filemagic	Microsoft Excel	not created	not created	not created	created and enabled	not created
smb	filemagic	Microsoft OOXML	not created	not created	not created	created and enabled	not created
smb	filemagic	Microsoft Office Document	not created	not created	not created	created and enabled	not created
smb	filemagic	Microsoft PowerPoint	not created	not created	not created	created and enabled	not created
smb	filemagic	Microsoft Word	not created	not created	not created	created and enabled	not created
smb	filemagic	Node.js script text	not created	not created	not created	created and enabled	not created
smb	filemagic	OS/2 REXX batch file	not created	not created	not created	created and enabled	not created
smb	filemagic	OpenDocument	not created	not created	not created	created and enabled	not created
smb	filemagic	PDF document	not created	not created	not created	created and enabled	not created
smb	filemagic	PE32 executable	not created	not created	not created	created and enabled	not created

continues on next page

Table 1 – continued from previous page

Protocol	Type	Values	Essential	Balanced	Deep	Paranoid	Performance
smb	filemagic	PE32 executable (DLL)	not created	not created	not created	created and enabled	not created
smb	filemagic	PE32+ executable	not created	not created	not created	created and enabled	not created
smb	filemagic	POSIX tar archive	not created	not created	not created	created and enabled	not created
smb	filemagic	RAR archive data	not created	not created	not created	created and enabled	not created
smb	filemagic	Zip archive data	not created	not created	not created	created and enabled	not created
smb	filemagic	gzip compressed data	not created	not created	not created	created and enabled	not created
smtp	filemagic	7-zip archive data	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	COM executable	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	Composite Document File V2	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	DOS batch	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	ELF	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	Java archive data	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	Javascript	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	MS Windows shortcut	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	MS-DOS executable	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	Mach-O	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	Macromedia Flash	not created	created and enabled	created and enabled	created and enabled	not created

continues on next page

Table 1 – continued from previous page

Protocol	Type	Values	Essential	Balanced	Deep	Paranoid	Performance
smtp	filemagic	Microsoft Cabinet archive data	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	Microsoft Excel	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	Microsoft OOXML	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	Microsoft Office Document	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	Microsoft PowerPoint	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	Microsoft Word	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	Node.js script text	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	*OS/2 REXX batch file*	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	OpenDocument	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	PDF document	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	PE32 executable	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	PE32 executable (DLL)	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	PE32+ executable	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	POSIX tar archive	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	RAR archive data	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	Zip archive data	not created	created and enabled	created and enabled	created and enabled	not created
smtp	filemagic	gzip compressed data	not created	created and enabled	created and enabled	created and enabled	not created

Note:

The filemagic that can be used in the `Value` field are those present in the Libmagic library.
A filemagic not present in this library will not be functional.

5.7.2.2.9 `Packet filters` section of the `Gcaps profiles` screen

5.7.2.2.9.1 Information on the `Packet filters` section

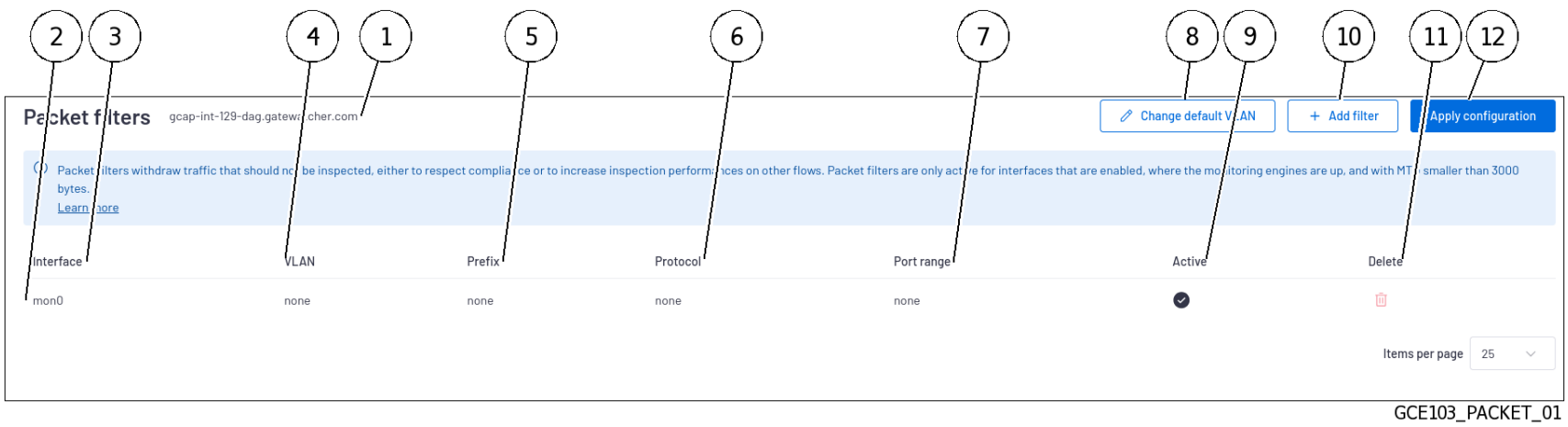
The `Packet filters` section enables specific traffic to be ignored directly at the GCap network card level.
This feature enables the GCap to avoid overloading the GCap with "unnecessary" traffic such as encrypted streams, backup streams, etc., or traffic that may cause the cpus to overload such as Elephant Flow, Miles Flow, etc.
The selection of traffic to be ignored is based on vlan, network prefix, protocol, and network ports.

Packet filtering is only active:

- For active interfaces monX on the GCap
- With an MTU of less than 3000 bytes
- With the monitoring engine enabled

5.7.2.2.9.2 Description the `Packet filters` section

This section includes the following items:



GCE103_PACKET_01

Item	Function
1	GCAP selected

2	Defining a packet filtering rule. it includes the following fields:
	• The `Interfaces` field (3) indicates the capture interface to which the filter applies: mon0, mon1, mon2, mon3 or monvirt
	• The `VLAN` field (4) indicates the VLAN number
	• The `Prefix` field (5) indicates the IP address filtering to be ignored
	• The `Protocol` field (6) indicates the ignored protocol:
	  • TCP
	  • UDP
	  • Tunnel protocols (AH, ESP, GRE, L2TP)
	  • All TCP
	  • All UDP
	  • All TCP and UDP
	  • All
	  • AH
	  • ESP
	  • GRE
	  • L2TP
	• The `Port range` choice (7) indicates the filter to ignore only the selected port or port range. Only available for the protocols:
	  • TCP
	  • UDP
	• The `Active` choice (9): selector to activate this rule
	• The `Delete` choice (11): delete this line

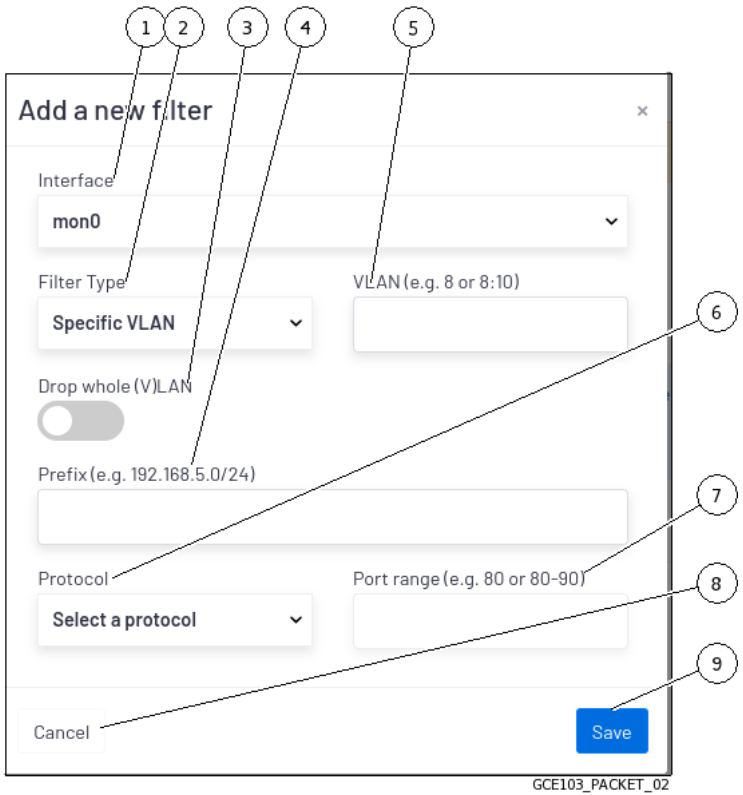
8	The `Change default VLAN` button enables modifying the default vlan for the various active interfaces on the GCap. By default, this vlan is 1 for each interface.
10	The `Add filter` button displays a window for creating a new filter
12	The `Apply configuration` button enables the settings to be saved and makes the filters available to GCaps

Note:

If an interface can use `Packet filtering` then a line is displayed in the filter list with the various fields empty.

5.7.2.2.9.3 `Add a new filter` window

The `Add a new filter` window enables to add a new filter.



Item	Name	Function
1	`Interface` field	Select the capture interface to which the filter applies
2	`Specific VLAN` field	Select between `Specific VLAN` and `Default VLAN & untagged traffic`
3	`Drop whole LAN` selector	Choose whether the filter applies to the whole vlan (enable) or a part of the vlan (disable)
4	`Prefix` field	Enter the network to apply the filter to. If the `Drop whole LAN` field is enabled, this box is not editable.
5	`VLAN` field	Field to enter the value of the desired vlan. If the "Filter Type" field is set to `default VLAN & untagged traffic` the box is not editable.
6	`Protocol` field	Field to enter the protocol to apply the filter to. If the `Drop whole LAN` field is enabled, this box is not editable.
7	`Port range` field	Field to enter the port or port range to apply the filter to. If the `Drop whole LAN` field is enabled, this box is not editable.
8	`Cancel` button	Cancels the current modifications
9	`Save` button	Saves the current modifications

5.7.2.3 `Metadata rate limiter` screen

5.7.2.3.1 Introduction

In addition to alerts, GCaps generate metadata events on analyzed network flows.
This information can be useful in surveys, but in a certain context, it can quickly exceed the indexing capabilities of the GCenter.
In order to reduce the amount of metadata while maintaining most information exchanges, it is possible to enable the limiters defined below.

Tip:

Use the hunting tool (hunting > Metadata) to understand what kind of metadata should be optimized first.

This screen enables:

- To enable metadata limiters
- To define on which protocols they are activated
- To define the metadata filtering rule

This screen is only accessible to members of the *operator* group.

Important:

Activate the HTTP or TLS protocol disables the detection of the Beacon detect engine for these protocols.

Note:

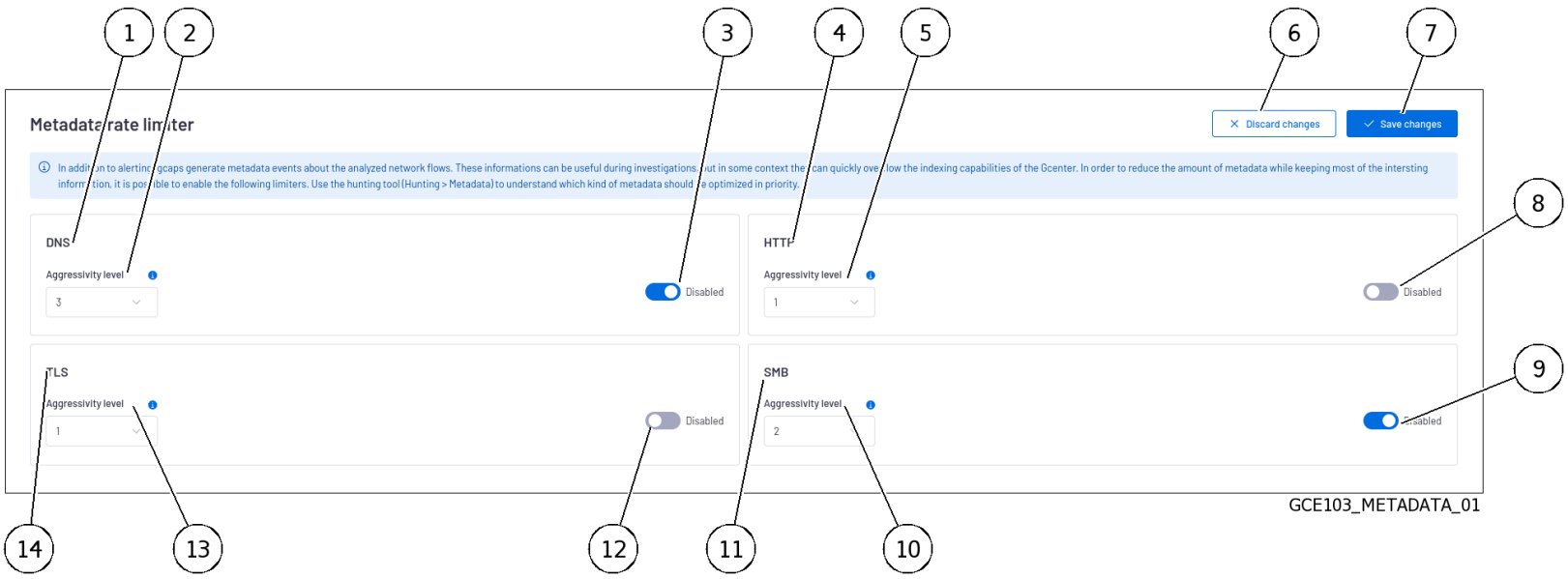
Filtering the events entering in the detection engines has two consequences:
- On the engine detection performances
- On the volume of event data

5.7.2.3.2 Links associated

For implementation of the Metadata rate limiter, see the *Configuring Metadata Rate Limiters*.

5.7.2.3.3 Screen description

After pressing the `Metadata rate limiter` command of the `Detection Strategy\Sigflow engine` menu, the following screen is displayed.



For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Item	Name	Function
1	`DNS`	Configures the limiter for the `DNS` protocol. This includes:
2	`Aggressivity level`	Filtration level. Includes the following choices: • Level 1: Removes metadata from DNS queries, but retains responses • Level 2: Removes metadata related to DNS queries. If a response is type A, AAAA or PTR with a response code NOERROR, keeps only one response per domain name and source IP, with a 1 minute mobile window • Level 3: Removes metadata related to DNS queries. For all responses with a NOERROR response code, keep only one response per domain name and source IP, with a 1-hour mobile window
3	`Enabled` selector	Enables/disables the metadata rate limiter for the `DNS` protocol
4	`HTTP`	Configures the limiter for the `HTTP` protocol. This includes:
5	`Aggressivity level`	Filtration level. Includes the following choices: • Level 1: for events with status code 200, only keeps a single request per source IP, method, destination port, destination IP and URL, with a 1-minute mobile window. • Level 2: for events with status code 200, keeps only one request per source IP, method, destination hostname, with a 1 hour mobile window. • Level 3: keeps only events with status code different from 200.
8	`Enabled` selector	Enables/disables the metadata rate limiter for the `HTTP` protocol
11	`SMB`	Configure the limiter for the `SMB` protocol. This includes:
10	`Aggressivity level`	Filtration level. Includes the following choices: • Level 1: for each SMB session and for different SMB commands from READ and WRITE, only keeps 100 records per command type on a 1-minute mobile window • Level 2: for each SMB session and for different SMB commands from READ and WRITE, keeps only 10 records per command type on a 1-hour mobile window
9	`Enabled`	Enables/disables the metadata rate limiter for the `SMB` protocol

continues on next page

Table 2 – continued from previous page

Item	Name	Function
14	`TLS`	Configures the limiter for the `TLS` protocol. This includes:
13	`Aggressivity level`	Filtration level. Includes the following choices: • Level 1: for connection-related events, only keeps a record by source IP, destination IP and TLS subject, with a 1-minute mobile window. For other events, only keeps a record by source IP and destination IP with a 1-minute mobile window. • Level 2: for connection-related events, only keeps a record by source IP, destination IP and TLS subject, with a 1-hour mobile window. For other events, only keeps a record by source IP and destination IP with a 1 hour mobile window.
12	`Enabled` selector	Enables/disables the metadata rate limiter for the `TLS` protocol
6	`Discard changes` button	Cancels current changes
9	`Save changes` button	Saves current changes. The following message is displayed after saving `Metadata rate limiting successfully applied !`

Note:

The default configuration is:

Item	Protocol	Title	Position or value
2	`DNS`	`Aggressivity level`	3
3	`DNS`	`Aggressivity level`	activate
8	`HTTP`	`Enabled` selector	deactivate
9	`SMB`	`Enabled` selector	activate
10	`SMB`	`Aggressivity level`	3
12	`TLS`	`Enabled` selector	deactivate

5.7.2.4 `Malcore` screen

5.7.2.4.1 Introduction

The `Malcore` screen enables to:

- Configure the Malcore engine
- Define the list of files not to be analyzed and therefore consider them to be healthy

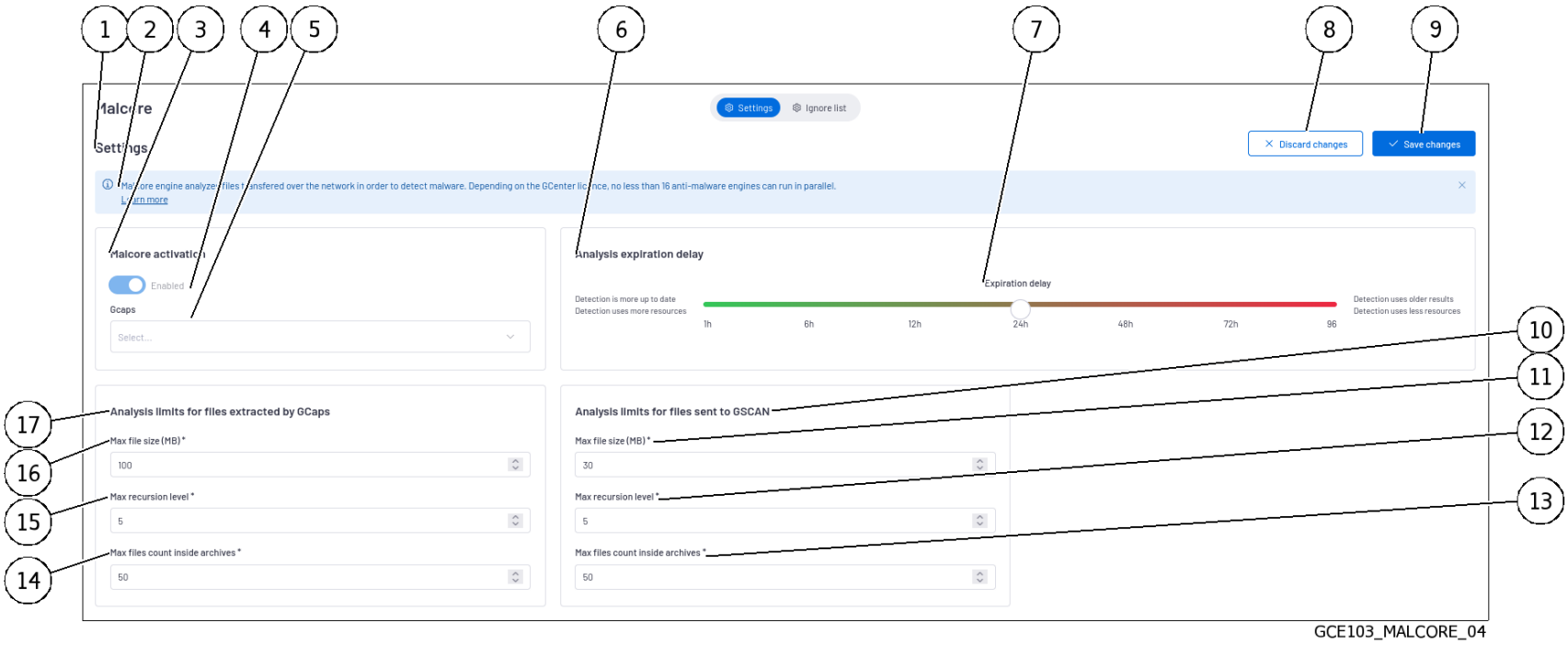
This screen is only accessible to members of the *operator* group.

5.7.2.4.2 Links associated

The engine is presented in the *Malcore engine* paragraph.
The visualization of the current engine status is given in the procedure *`Health checks` screen*.
For engine setting implementation, see *Setting up the Malcore engine*.
For the implementation of the file exception list, see *Managing the Ignore list of the Malcore engine*

5.7.2.4.3 Screen description

After pressing the `Malcore` command on the `Detection Strategy\Malware` menu, the following screen is displayed.



GCE103_MALCORE_04

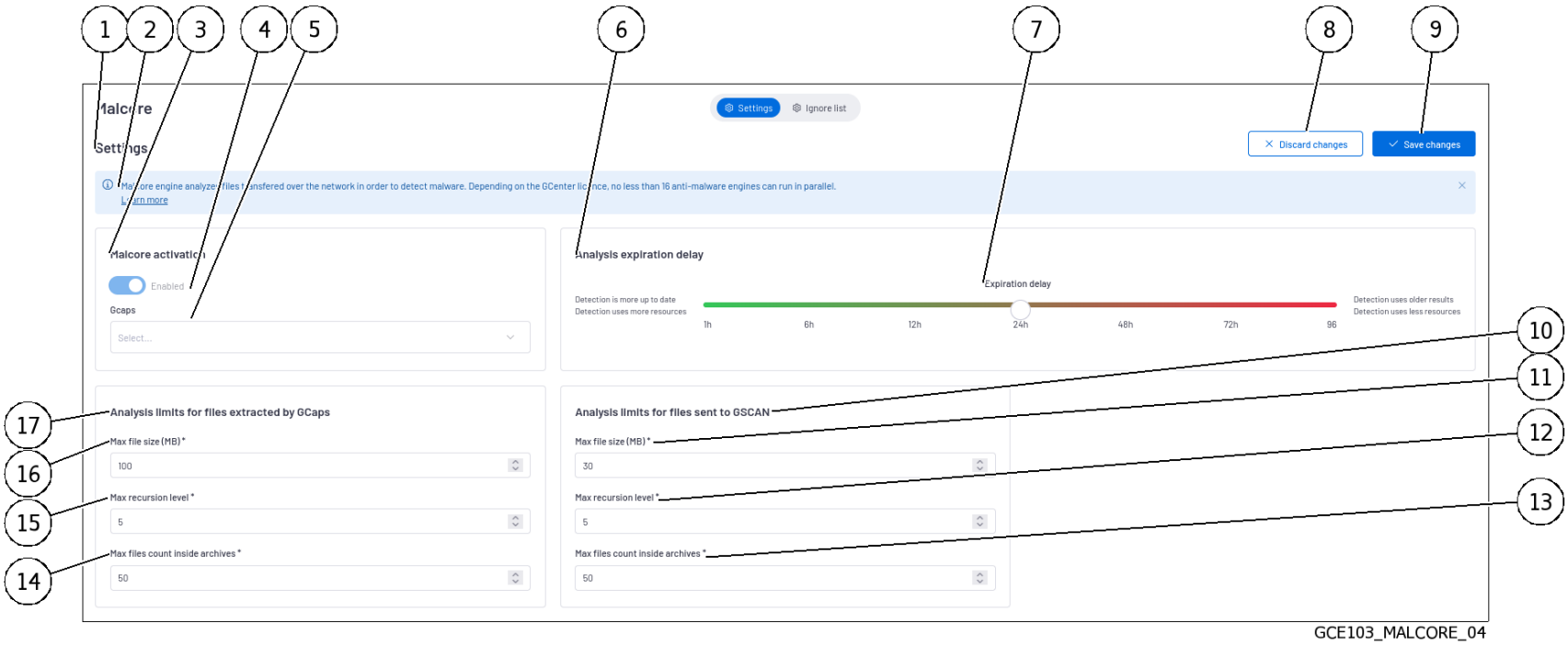
For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

The `Malcore` screen contains the following parts:

Area	Function
`Settings`	Engine settings
`Ignore list`	Defines the files that are considered healthy because they are present in the list of items ignored (are considered healthy)

5.7.2.4.3.1 `Settings` area of the `Malcore` screen

The `Settings` window (1) displays the engine settings.



GCE103_MALCORE_04

Item	Name	Function
1	`Settings`	Includes all engine settings
2	`Malcore engine analyzes files transferred over the network in order to detect malware. Depending on the GCenter license, no less than 16 anti-malware engines can run in parallel.`	Short information about this screen. The Learn more link opens the embedded documentation on the corresponding page
3	`Malcore activation`	Parameters area
4	`Enabled` selector	This selector is locked on engine activation
5	`Gcaps` selector	This selector is locked

continues on next page

Table 3 – continued from previous page

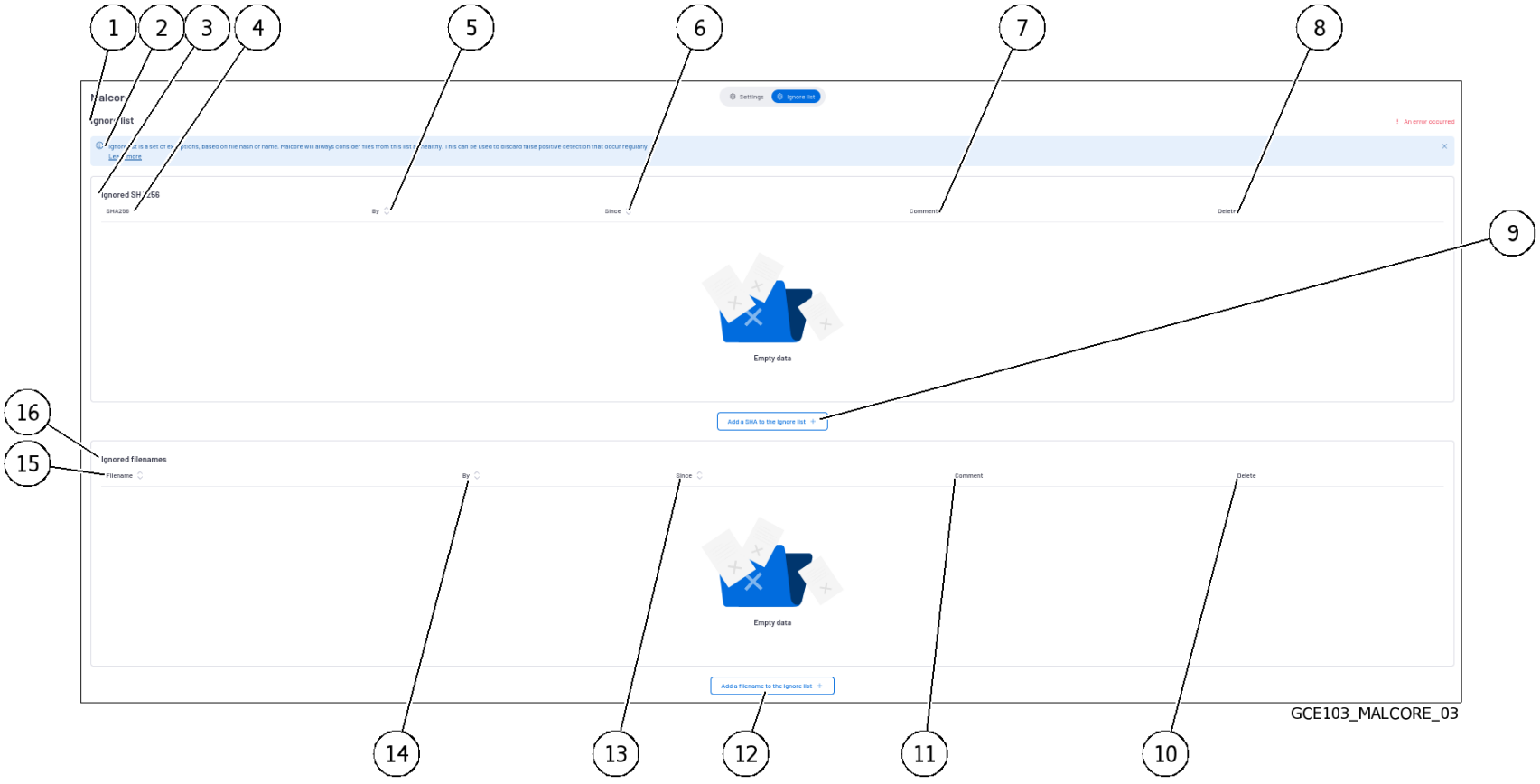
Item	Name	Function
6	`Analysis expiration delay`	Area containing the parameter `Expiration delay`. This defines the delay (in hours) after which a malware scan is considered outdated. If the antivirus engines have been updated and the same file reappears, it will be scanned again. If the antivirus engines have not been updated or the timeout is not complete, the Malcore scan will reuse its previous results.
7	`Expiration delay` button	Sets the delay value. Default value: 24h
8	`Discard changes` button	Cancels current changes
9	`Save changes` button	Saves current changes
10	`Analysis limits for files sent to GSCAN`	Analysis limits of files sent to Gscan
11	`Max file size (MB)`	Maximum size of files sent to Gscan (MB)
12	`Max recursion level`	Maximum recursion level for archives sent to Gscan
13	`Max files count inside archives`	Maximum number of files in archives sent to Gscan
17	`Analysis limits for files extracted by GCaps`	Analysis limits of files extracted by GCap
16	`Max file size (MB)`	Maximum size of files extracted by GCap (MB)
15	`Max recursion level`	Maximum recursion level for archives extracted by GCap
14	`Max files count inside archives`	Maximum number of files for archives extracted by GCap

5.7.2.4.3.2 `Ignore list` area of the `Malcore` screen

This `Ignore list` area displays the exception list of files that Malcore must consider healthy.
These files are declared healthy without analysis and defined using:

- Their SHA256 fingerprint (whatever the name)
- The file name

After clicking on the `Ignore list` button, the `Ignore list` (1) window is displayed.



Item	Name	Function
1	`Ignore list`	Their SHA256 fingerprint (whatever the name) The name of the file

continues on next page

Table 4 – continued from previous page

Item	Name	Function

2	`Ignore list is a set of exceptions, based on file hash or name.`
	`Malcore will always consider files from this list as healthy.`
	`This can be used to discard false positive detection that occur regularly.`
		Short information about this screen.
		The Learn more link opens the embedded documentation on the corresponding page.

3	`Ignored SHA256`	This area list the exception list of files defined by its SHA256. For each file, the following information is displayed:
4	`SHA256`	• File SHA256
5	`By`	• Indicates the account that created the record
6	`Since`	• Indicates the date and time the record was created
7	`Comment`	• Indicates the comment, if any, for further details.
8	`Delete`	• Displays the icon to delete
9	`Add a SHA to the ignore list` button	Adds a new record to the list
16	`Ignored filename`	This area list the exception list of files defined by its name. For each file, the following information is displayed:
15	`Filename`	• Name of the file
14	`By`	• Indicates the account that created the record
13	`Since`	• Indicates the date and time the record was created
11	`Comment`	• Indicates the comment, if any, for further details.
10	`Delete`	• Displays the icon to delete
12	`Add a filename to the ignore list` button	Adds a new record to the list

5.7.2.5 `Malcore retroanalyzer` screen

5.7.2.5.1 Introduction

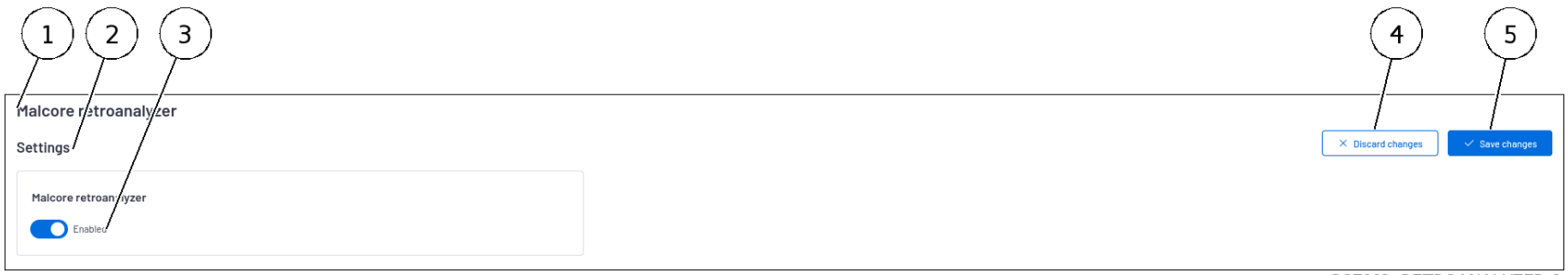
The `Malcore retroanalyzer` screen enables to activate the engine.
This screen is only accessible to members of the *operator* group.

5.7.2.5.2 Links associated

The engine is presented in *Malcore retroanalyzer engine* paragraph.
The visualization of the current engine status is given in *`Health checks` screen*.
For engine setting implementation, see *Setting up the Malcore retroanalyzer engine*

5.7.2.5.3 Screen description

After pressing the `Malcore retroanalyzer` command on the `Detection Strategy\Malware` menu, the `Malcore retroanalyzer` screen is displayed.



GCE103_RETROANALYZER-1

For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Item	Name	Function
1	`Malcore retroanalyzer`	Window to configure the engine
2	`Settings`	Zone to set the engine
3	`Enabled` selector	Activates or deactivates the engine
4	`Discard changes` button	Cancels current changes
5	`Save changes` button	Saves current changes

5.7.2.6 `YARA` screen

5.7.2.6.1 Introduction

The `Yara engine` screen enables to:

- Activate the engine
- Upload a ruleset

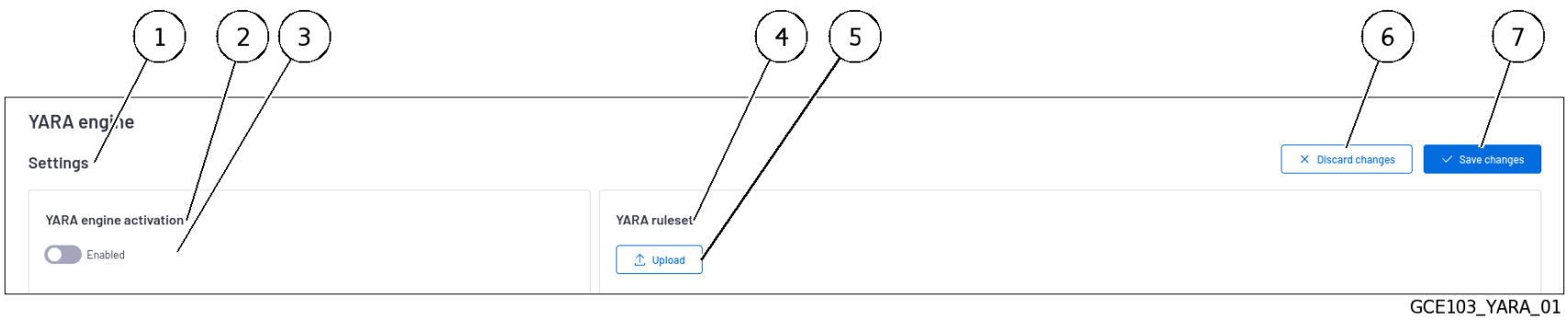
This screen is only accessible to members of the *operator* group.

5.7.2.6.2 Links associated

The engine is presented in *Yara engine* paragraph.
The visualization of the current engine status is given in *`Health checks` screen*.
For engine setting implementation, see *Setting up the Yara engine*.

5.7.2.6.3 Screen description

After pressing the `Yara engine` command on the `Detection Strategy\Malware` menu, the following screen is displayed.



GCE103_YARA_01

For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Item	Name	Function
1	`Settings`	Includes all engine settings
2	`Yara activation`	Parameter zone
3	`Enabled - Disabled` selector	Activates or deactivates the engine.
4	`Yara ruleset`	Yara ruleset
5	`Upload` button	Uploads a ruleset of the engine
6	`Discard changes` button	Cancels current changes
7	`Save changes` button	Saves current changes

5.7.2.7 `Malicious Powershell detect` screen (Malicious Powershell command)

5.7.2.7.1 Introduction

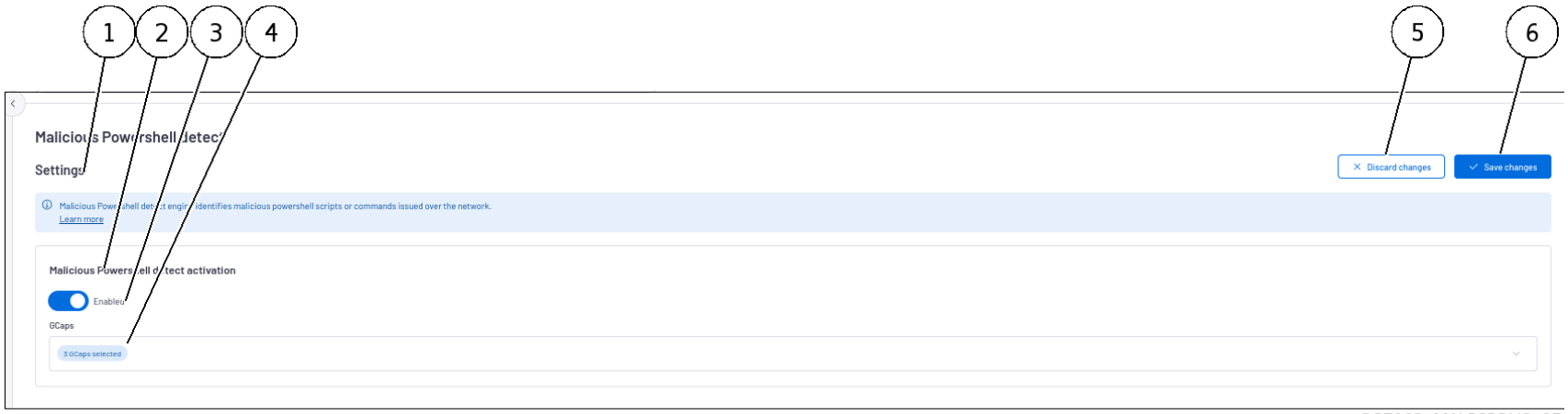
The `Malicious Powershell` screen is used to activate the Malicious Powershell engine on the various GCaps.
This screen is only accessible to members of the *operator* group.

5.7.2.7.2 Links associated

The engine is presented in *Malicious Powershell detect engine* paragraph.
The visualization of the current engine status is given in *`Health checks` screen*.
For engine setting implementation, see *Setting up the Malicious Powershell detect engine*.

5.7.2.7.3 Screen description

After pressing the `Malicious Powershell` command on the `Detection Strategy\Exploit` menu, the following screen is displayed.



GCE103_MALICIOUS_05

For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Item	Name	Function
1	`Settings`	Includes all engine settings
2	`Malicious powershell detect activation`	Engine Activation Zone
3	`Enabled` selector	Activates the engine of the selected GCaps
4	`Gcaps`	Selects the GCaps to enable or disable engine
5	`Discard changes` button	Cancels current changes
6	`Save changes` button	Saves current changes

5.7.2.8 `Shellcode detect` screen (Shellcode command)

5.7.2.8.1 Introduction

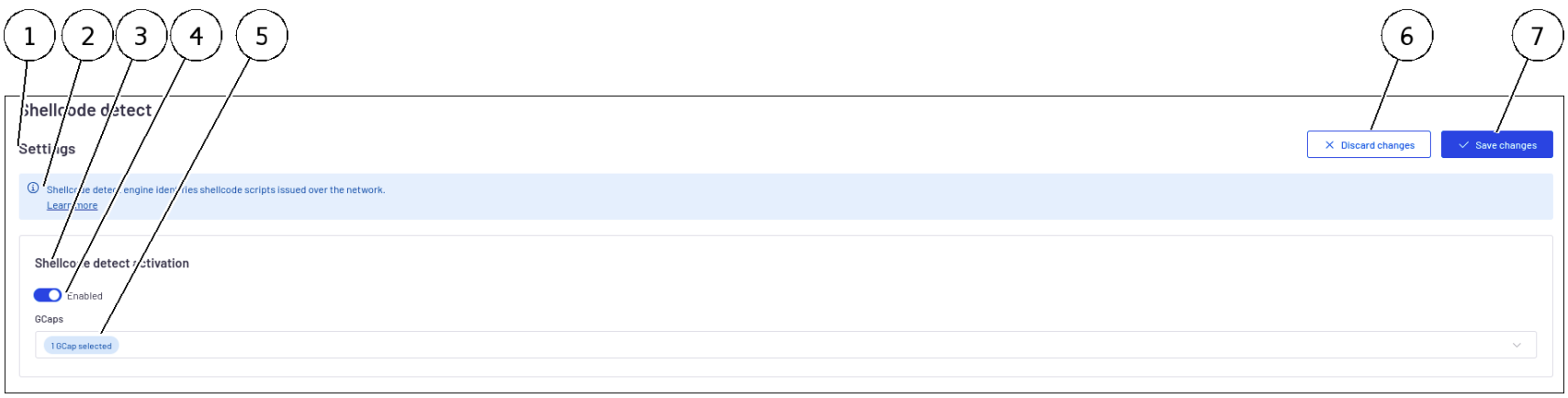
The `Shellcode detect` screen enables to activate the engine.
This screen is only accessible to members of the *operator* group.

5.7.2.8.2 Links associated

The engine is presented in *Shellcode detect engine* paragraph.
The visualization of the current engine status is given in *`Health checks` screen*.
For engine setting implementation, see the procedure *Setting up the Shellcode detect engine*.

5.7.2.8.3 Screen description

After pressing the `Shellcode` command on the `Detection Strategy\Exploit` menu, the following screen is displayed.



For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Item	Name	Function
1	`Settings`	Includes all engine settings
2	`Shellcode detect engine identifies shellcode scripts issued over the network.`	Short information about this screen. The Learn more link opens the embedded documentation on the corresponding page.
3	`Shellcode detect activation`	Engine Activation Zone
4	`Enabled` selector	Activates the engine of the selected GCaps
5	`Gcaps`	Selects the GCaps to enable or disable engine
6	`Discard changes` button	Cancels current changes
7	`Save changes` button	Saves current changes

5.7.2.9 `Sources` screen

5.7.2.9.1 Introduction

This screen enables to:

- Define signature sources for the detection engine
- Manage existing sources
- Manage the files of the set of rules made available by the sources
- Manage the categories and rules of these files

This screen is only accessible to members of the *operator* group.

5.7.2.9.2 Links associated

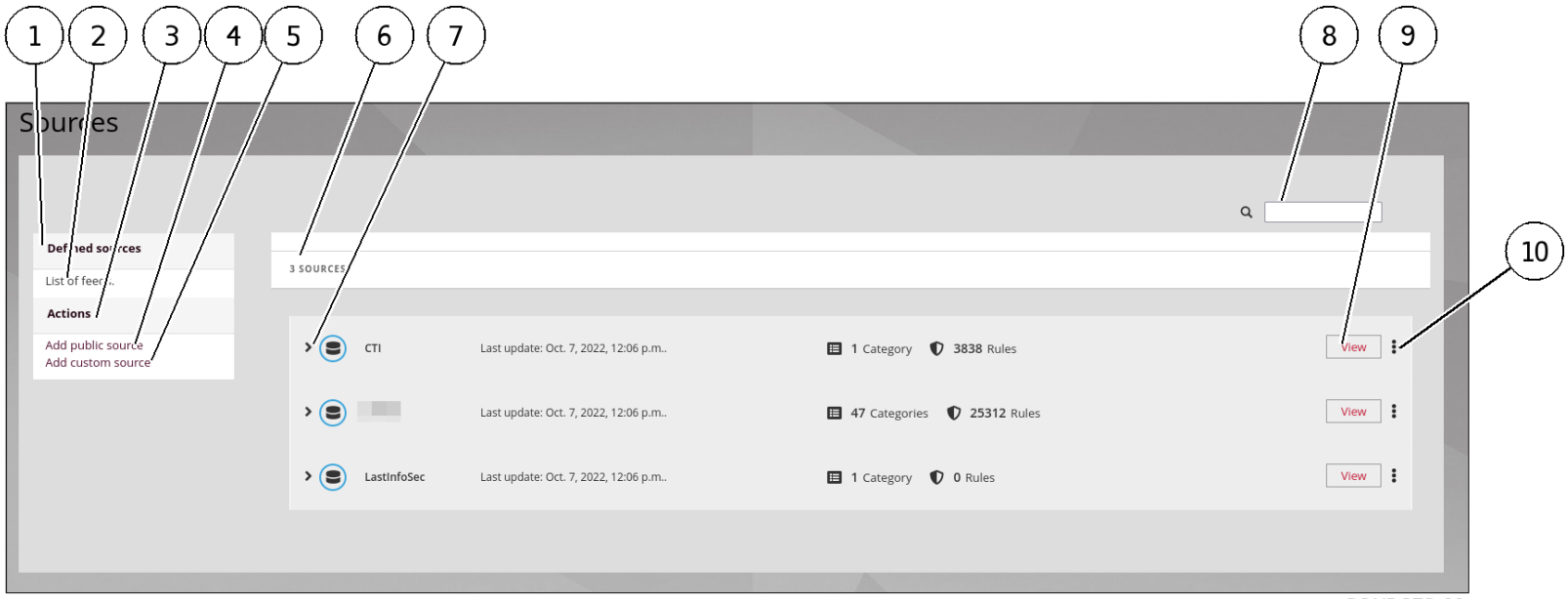
See the *Managing the Sigflow engine rule sources* procedure for:

- Source visualization and management
- Viewing and managing rule files

See the *Updating rules sources* procedure.

5.7.2.9.3 Screen description

After pressing the `Sources` command of the `Detection Strategy / Sigflow rules manager` submenu, the following screen is displayed.



SOURCES-01

For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Item	Name	Function
1	`Defined sources`	Indicates the list of existing sources
2	`List of feeds`	List of streams
3	`Action`	Area of possible actions. The possible actions listed below depend on the context:
4	`Add public source` button	• adds public sources
5	`Add custom source` button	• adds custom sources
6	`3 Sources`	Field indicates the number of sources defined
7	Description of a source	Defined source. This includes the following types of information: - The source name (CTI Gatewatcher CTI...) - The date and time of the last update - The number of categories and signatures You can add a MIPS source. To do so, refer to the *Configuring the connection to the MISP*
8	Search field	Enables a search
9	`View` button	Displays the `Sources: view` screen (see below)
10	Context menu	Displays the management sub-menu for this source for access to the `Edit source` and `Delete source` commands

Note:

There are two Gatewatcher CTI entries:

- An entry named `LastinfoSec(Experimental)`: this entry only exists if the GCenter was in version V101 and migrated to V102. This entry must be deleted. To do this, refer to *Procedure to delete a source*.
- An entry named `LastinfoSec`: this entry is created in V102 and is linked to the CTI function and presents only if the LastinfoSec license is enabled. This entry must be kept and used.

After pressing the `View` button (9), the `Sources: view` screen contains the following sections:

Item	Name	Function
1	Source field	Indicates the selected source (here CTI). it includes the following fields:
10	Source creation field	• The date and time the source was created
9	Update field	• The date and time of the last update
2	`Action`	Area of possible actions. The possible actions listed below depend on the context
8	`Changelog`	• Displays the history of the current source
7	`Update`	• Updates the current source
6	`Edit`	• Edits the current source
5	`Delete`	• Deletes the current source
3	`Catégories`	List of categories. This includes three types of information: - The category name - The category description - The creation date of the category
4	Search field	Enables searching for text in the categories including the description field of the rules

Note:

Each source is made up of categories.
Each of these categories can be edited.
Each category is composed of rules. Clicking on a category will display the list of rules.
Each of these rules can be edited.
The source rules `LastinfoSec` are neither editable nor disabling.

5.7.2.10 `Rulesets` screen

5.7.2.10.1 Introduction

This screen enables:

- Creating files called **rulesets**
- Managing the categories and rules of Ruleset files.
  Once a file is generated, its content can also be managed, i.e. modification of categories and rules
- Providing these files to the Sigflow detection engine of the GCap
- Exporting these files to the local download directory with the extension rules

Note:

A **ruleset** file is composed of one or more **source** files downloaded from different sources.
Each **source** file is composed of different categories.
Each category consists of rules (or signatures).

This screen is only accessible to members of the *operator* group.

5.7.2.10.2 Links associated

For more information on Sigflow and its rules, refer to *Sigflow engine*.
See the *Managing a Sigflow engine ruleset* procedure for:

- Creating a Ruleset file
- Managing its content, modifying categories and rules
- Sending a Ruleset file to the Sigflow detection engine in the GCap
- Exporting a file to the local download directory of the user PC with the rules extension

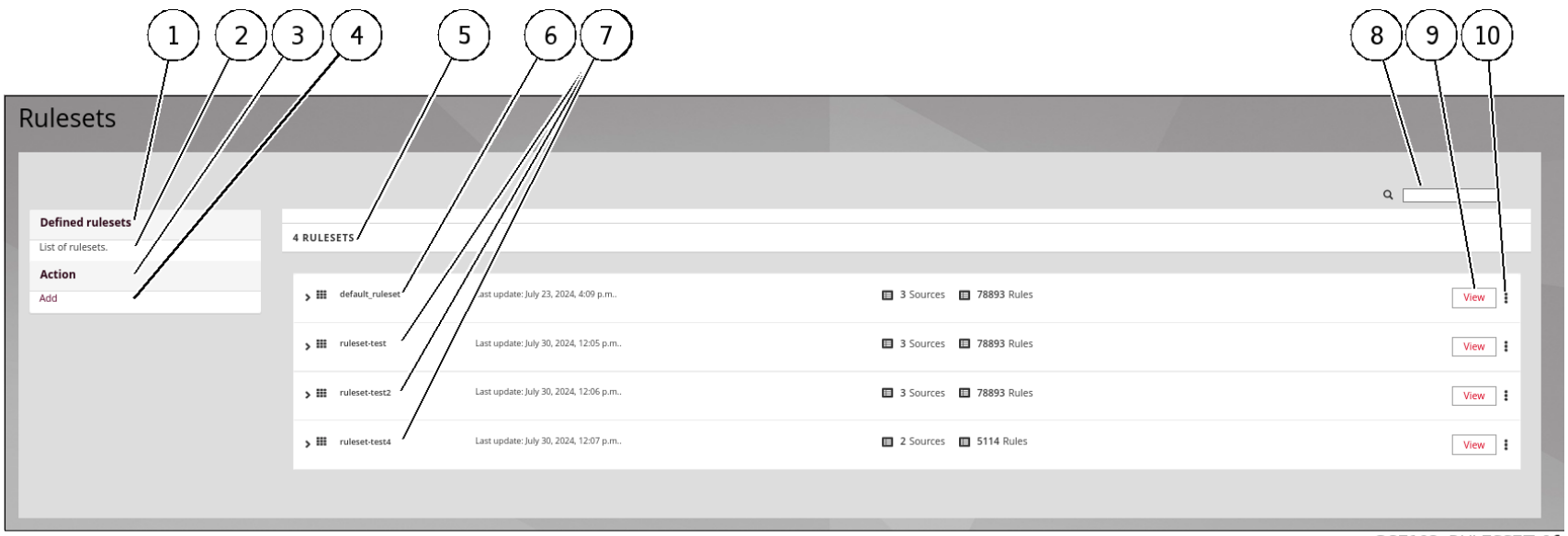
See the *Modifying Sigflow engine rules* procedure for:

- The implementation of a transformation rule (Transform rule)
- Deactivation of the rule of a transformation rule
- Activation of the rule of a transformation rule
- Threshold rule
- The deletion rule (Suppress rule)

See the *Modifying Sigflow engine rules* procedure.

5.7.2.10.3 Screen description

After pressing the `Rulesets` command from the sub-menu `Detection Strategy / Sigflow rules manager`, the following screen is displayed.

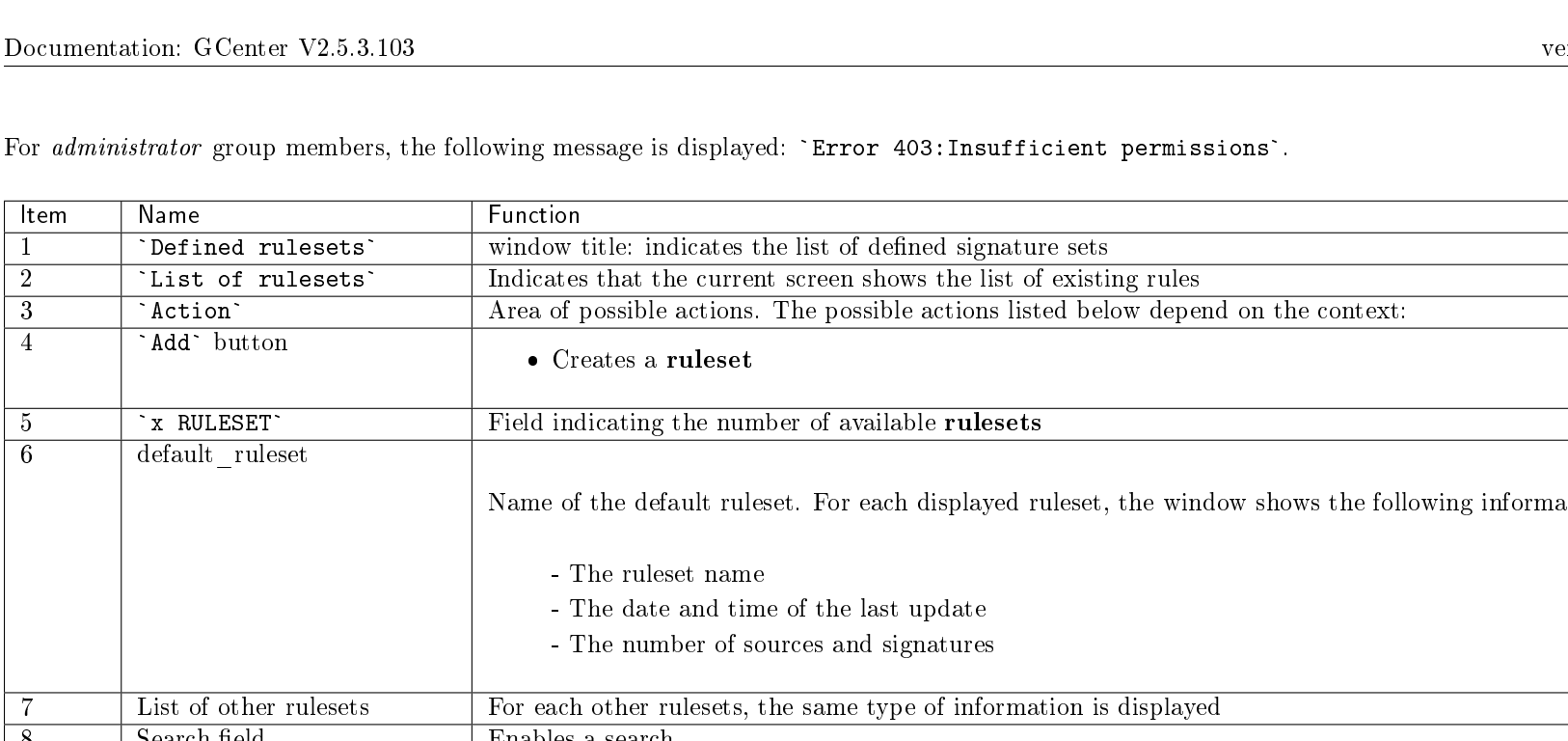


GCE103_RULESSET-06

For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Item	Name	Function
1	`Defined rulesets`	window title: indicates the list of defined signature sets
2	`List of rulesets`	Indicates that the current screen shows the list of existing rules
3	`Action`	Area of possible actions. The possible actions listed below depend on the context:
4	`Add` button	• Creates a **ruleset**
5	`x RULESET`	Field indicating the number of available **rulesets**
6	default_ruleset	Name of the default ruleset. For each displayed ruleset, the window shows the following information: - The ruleset name - The date and time of the last update - The number of sources and signatures
7	List of other rulesets	For each other rulesets, the same type of information is displayed
8	Search field	Enables a search
9	`View` button	Displays the `Rulesets: view` screen (see below)
10	Context menu	Displays the management sub-menu for this source: - `Update rule set` command: updates the ruleset i.e the update the rules defined in the existing sources of this ruleset - `Edit ruleset` command: opens the `Edit ruleset` window - `Copy ruleset` command: opens the `Copy ruleset` window - `Delete ruleset` command: opens the `Delete object` window

After pressing the `View` command button, the following screen is displayed:



Item	Name	Function
1	ruleset name field	Indicates the name of the file containing the selected ruleset. This includes the following fields
2	`Created`	• The date and time the ruleset was created
20	`Updated`	• The date and time of the last update
19	`All rules operational:`	• Status of operational rules (true or false)
18	`Rules count:`	• Rules counter
3	`Action`	Area of possible actions. The possible actions listed below depend on the context:
4	`Changelog` Button	• Displays the file history
5	`Update` button	• Updates the ruleset
17	`Edit` button	• Edits the ruleset
16	`Copy` button	• Copies the ruleset
15	`Delete` button	• Deletes the ruleset
6	`Display`	Area of possible actions. The possible actions listed below depend on the context:
14	`Show structure` button	• Displays the ruleset by source and then by category
13	`Show rules` button	• Displays the ruleset by rules, listed by SID
12	`Export rules files` button	• Exports the ruleset
7 8 10	`Source`	List of categories (9) for each source. This includes three types of information: - The name of the category - The description of the category - The creation date of the category
11	Search field	Enables a search
	`Save` button	Saves modification then generates the rules file from the current file

Note:

Each of these categories can be edited.
Clicking on a category will display the list of rules.
Each of these rules can be edited.

5.7.2.11 `Auto-threshold` screen

5.7.2.11.1 Introduction

See paragraph *Removing or limiting the number of alerts*
This screen automatically limits the number of alerts sent.

Note:

The user can manually create rules using the `threshold: type limit` function described in the screen **?**

The system counts alerts and compares them to a programmable trigger point.

For alerts exceeding this value, and depending on the selected criterion (filter type); it is possible to automatically create a programmable limit of alarms reported.

The `Auto-threshold` screen is used:

- To active automatic limit creation functionality
- To configure automatic creation from:
  - Of predefined profiles
  - Customization based on:
    - A rule creation trigger (based on a number of alarms counted over a defined time)
    - A criterion for sorting alarms to count only those desired (cursor `Aggressivity`) to trigger limit creation
    - The values of the limit created (number of alarms appearing within the defined period from which no more alarms will be raised)

Automatic limit creation updates are normally pushed to GCaps daily when rule updates occur.
As a reminder, filtering alarms can be done:

- *by_src*: the limitation is applied to alarms with the same source IP address
- *by_dst*: the limitation is applied to alarms with the same destination IP address
- *by_rule*: the limitation is applied to all alarms triggered by the rule
- *by_both*: the limitation is applied to alarms with the same IP pair source address + destination

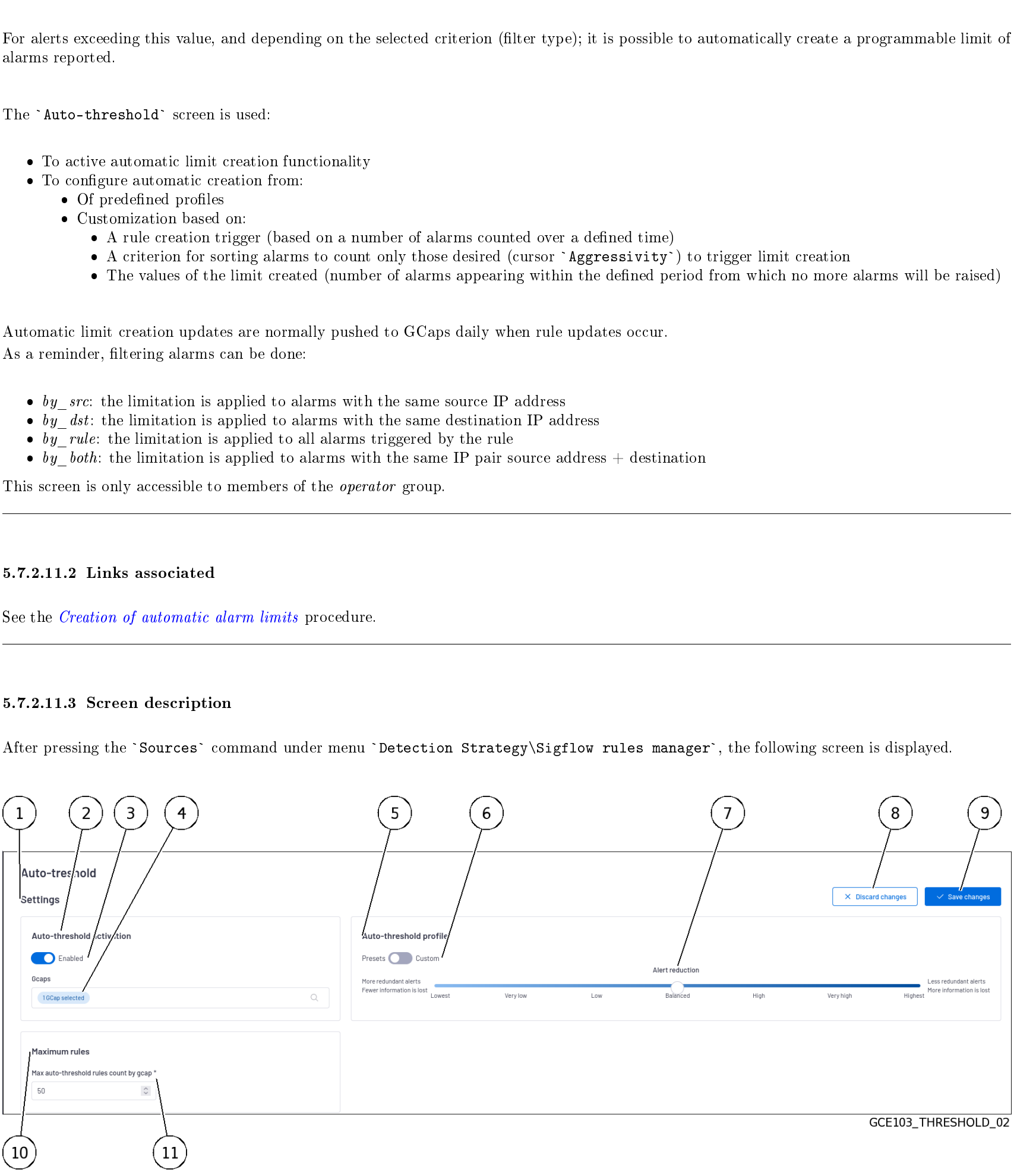
This screen is only accessible to members of the *operator* group.

5.7.2.11.2 Links associated

See the *Creation of automatic alarm limits* procedure.

5.7.2.11.3 Screen description

After pressing the `Sources` command under menu `Detection Strategy\Sigflow rules manager`, the following screen is displayed.



GCE103_THRESHOLD_02

For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

When configured with the `Auto-threshold profile` in the `Preset` position, the `Auto-threshold` screen contains the following parts:

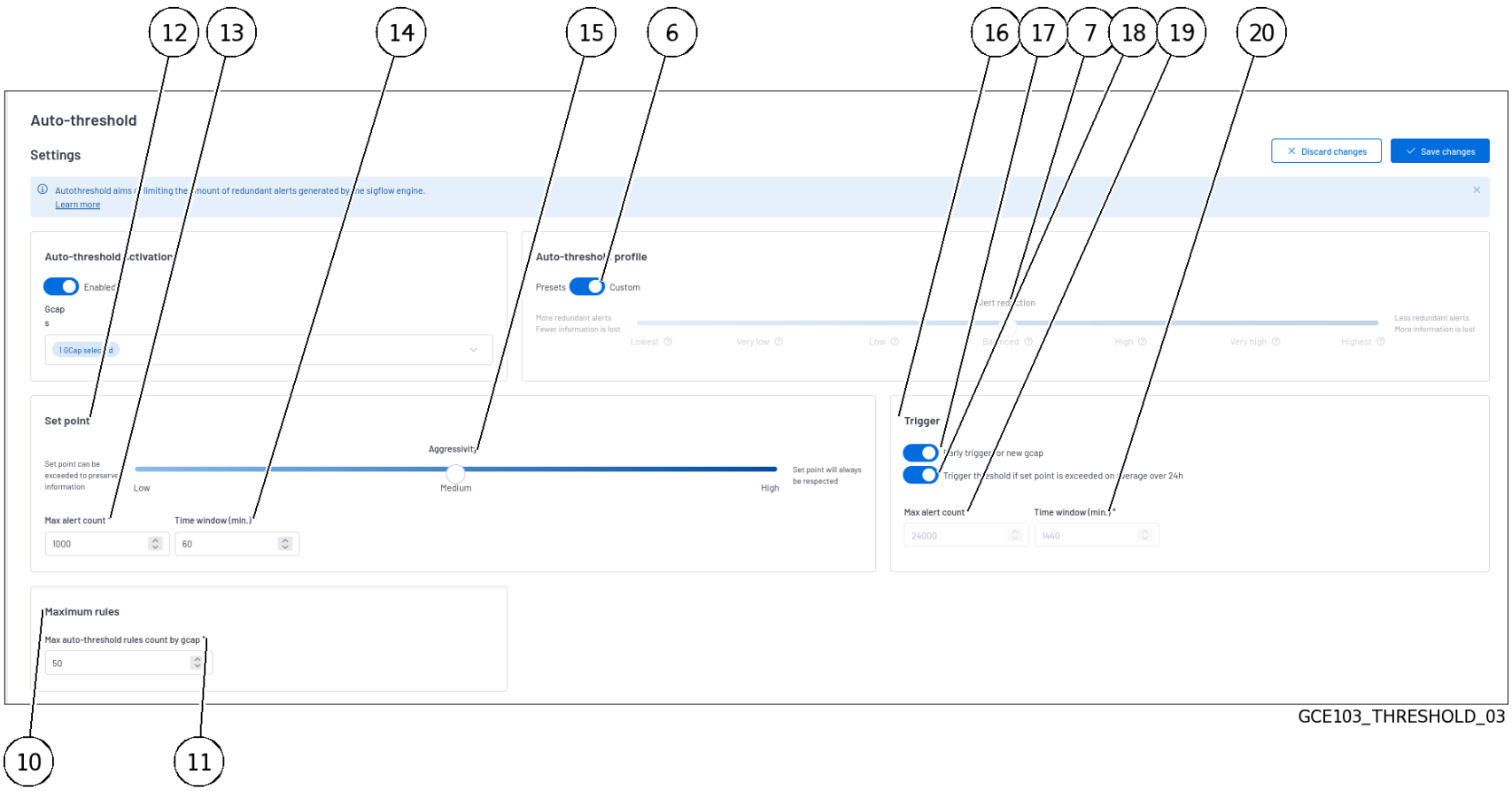
Item	Name	Function
1	`Settings`	Includes all setting parameters
2	`Auto-threshold activation`	Automatic threshold creation activation area
3	`Enabled` selector	Activates or deactivates the function
4	`Gcaps`	Selects the GCaps (name of the GCap or information that a GCap is selected). By default, all except GCap that use multi-tenant.
10	`Maximum rules`	Maximum number of threshold rules

continues on next page

Table 11 – continued from previous page

Item	Name	Function
11	`Max auto-threshold rules count by gcap`	Maximum number of limits per GCcap. The system can continuously create new limits and keep the ones that trigger the most.
5	`Auto-threshold profile`	Automatic threshold creation profiles configuration area
6	`Presets / Custom`	This selector has 2 positions: - `Presets`, the default mode: uses pre-existing and editable profiles using the cursor (7). See paragraph *Cursor part of pre-existing and editable profiles*. - `Custom`: configures threshold parameters. To do so, the "Set point" and "Trigger point" sections are displayed. See below
7	`Alert reduction` cursor	Uses predefined settings. See *Cursor part of pre-existing and editable profiles*.
8	`Discard changes` button	Cancels current changes
9	`Save changes` button	Saves current changes

When configured with the `Auto-threshold profile` in the `Custom` position, the `Auto-threshold` screen contains the following parts:



GCE103_THRESHOLD_03

Item	Name	Function
6	`Presets / Custom`	This selector has 2 positions: - Presets (setting): this function uses pre-existing and editable profiles using the cursor (see above) - Custom: this function configures threshold parameters. To do so, the "Set point" and "Trigger" sections are displayed.
7	`Alert reduction` cursor	This feature is disabled in this configuration
10	`Maximum rules`	Maximum number of threshold rules
11	`Max auto-threshold rules count by gcap`	Maximum number of limits per GCcap. The system can continuously create new limits and keep the ones that trigger the most.
12	`Set point`	Limit pivot value definition area
13	`Max alert count`	Pivot point setting: maximum number of alerts sent
14	`Time window (min)`	Pivot point setting: time window during the maximum number of alerts reported applies

continues on next page

Table 12 – continued from previous page

Item	Name	Function
15	`Aggressivity` cursor	Selects the alarm type criterion to limit 3 possible settings (Low, Medium, High): see details below The default level is: low
16	`Trigger`	Trigger configuration area
17	`Early trigger for new gcap`	Early trigger for new gcap
18	`Trigger threshold if set point is exceeded on average over 24h` selector	If the selector is activated, the GCenter counts alerts by rule and when a rule exceeds the pivot value set in the `Max alert count` parameter reduced to 24 hours measured over 24 hours. This option is enabled by default. For example: for a value of 1000 in the parameter `Max alert count` and a value of 60 in the parameter `Time window` then the system triggers the automatic creation from the appearance of 24000 alerts during the last 24 hours. If the selector is disabled, the system triggers from the value set in the `Max alert count` (20) parameter that appeared during the `Time window` (19) parameter value.
19	`Max alert count`	Pivot point setting: maximum number of alerts sent
20	`Time window (min)`	Pivot point setting: time window during the maximum number of alerts reported applies

5.7.2.11.4 Low Setting

- The limitation is applied to alarms *by_ both* having the same source and destination IP addresses
- Only alarms that have the same source IP addresses AND destination are counted to activate the threshold.
- Once triggered, then there is 24 hour observation period.
- After this period, the IP source AND destination pairs that exceeded the trigger threshold are defined.
- From the time the limit is triggered, for each of these pairs, the number of alarms raised is limited to the pivot value of the field `Max alert count` in the time `Time window (min)` then no alarm is raised.
- Each alert with the same IP source AND destination pair will be limited to the maximum number (`Max alert count` field) divided by the number of torque that exceeded the trigger threshold.
- For example if 3 pairs of IP have generated more alarms than the trigger value then each of the 3 pairs of IP will have a 1000/3 limit or 333 alarms/hour.
- But if a 4th pair of IP generates more alarms than the trigger value, then the system will exceed the pivot value in order to preserve the information (the 4 pairs of IP will have alarms reported).
- This choice being very limited, it is likely that there are many duplicates in the alerts sent. Activating the limit will just limit these duplicates and therefore there is little loss of information.

In conclusion **sorting is very selective, few alarms are filtered by the limitation but little loss of information**

5.7.2.11.5 Medium Setting

- The limitation is applied to alarms:
  - *by_ both*: meaning having the same IP source and destination addresses
  - *by_ src*: means having the same source IP address.
  - *by_ dst*: meaning having the same destination IP address
- Alarms reported with each of the 3 criteria are counted to activate the trigger threshold.
- Once triggered, then there is 24 hour observation period.
- After this period, only one of the three criteria is chosen according to the result.
- Whatever the criterion, the operation is the same as before.
- The choices (only same IP source/ IP destination) being wider, it is likely that there are few duplicates in the alerts sent. Activating the limit will therefore lead to loss of information.

Note:

same for "same IP destination" criterion

In conclusion **sorting is less selective, more alarms are filtered by the limitation then there is loss of information**

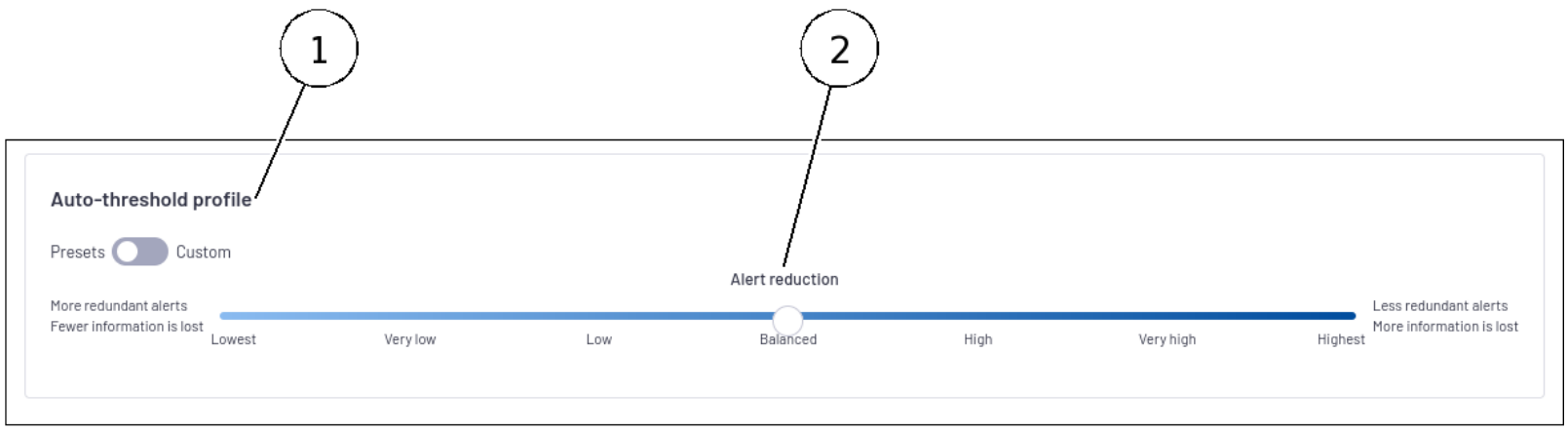
5.7.2.11.6 High Setting

- The limitation is applied to alarms:
  - *by_both* meaning having the same IP source and destination addresses
  - *by_src*: means having the same source IP address.
  - *by_dst*: meaning having the same destination IP address
  - *by_rule*: meaning having to all alarms triggered by the rule
- Alarms reported with each of the 3 criteria are counted to activate the trigger threshold.
- Once triggered, then there is 24 hour observation period.
- After this period:
- only one of the first three criteria is chosen, so the operation is the same as before
- if none of the first three criteria is selected then the limit is valid for all alerts in the rule
- Alerts will be taken in order of appearance until the pivot value.
- After the pivot value defined in the field `` `Max alert count` `` in the time `` `Time window (min)` ``, no alarm is raised.
- The pivot value is respected but this last choice (limit for the rule) will therefore lead to loss of information.

In conclusion **sorting is not selective, the limitation applies to the whole rule, so there is a lot of information loss**

5.7.2.11.7 Cursor part of pre-existing and editable profiles

The `` `Auto-threshold profile` `` (1) section displays the area below when the `` `Preset / Custom` `` selector is in the `` `Preset` `` position.
This function allows you to use pre-existing profiles using the `` `Alert reduction` `` slider.



GCE103_THRESHOLD_04

Item	Name	Function
1	`` `Auto-threshold profile` ``	Automatic threshold creation profiles configuration area
2	`` `Alert reduction` ``	Slider allows you to select different preset settings. The details of the predefined profiles are shown in the table below.

Profile	Trigger	Central value	Aggressiveness (selection criterion)
`` `Lowest` ``	96k alerts per 24 hours	4k alerts per hour	1
`` `Very low` ``	48k alerts per 24 hours	2k alerts per hour	1
`` `Low` ``	24k alerts per 24 hours	1k alerts per hour	1
`` `Balanced (default)` ``	24k alerts per 24 hours	1k alerts per hour	2
`` `High` ``	12k alerts per 24 hours	500 alerts per hour	2
`` `Very high` ``	12k alerts per 24 hours	500 alerts per hour	3
`` `Highest` ``	1200 alerts per 24 hours	50 alerts per hour	3

5.7.2.12 `Active CTI` screen

5.7.2.12.1 Introduction

The `Active CTI` screen enables to :

- Activate the engine
- Configure the retention time of compromise indices used for the detection done by the `Retro Hunt` engine

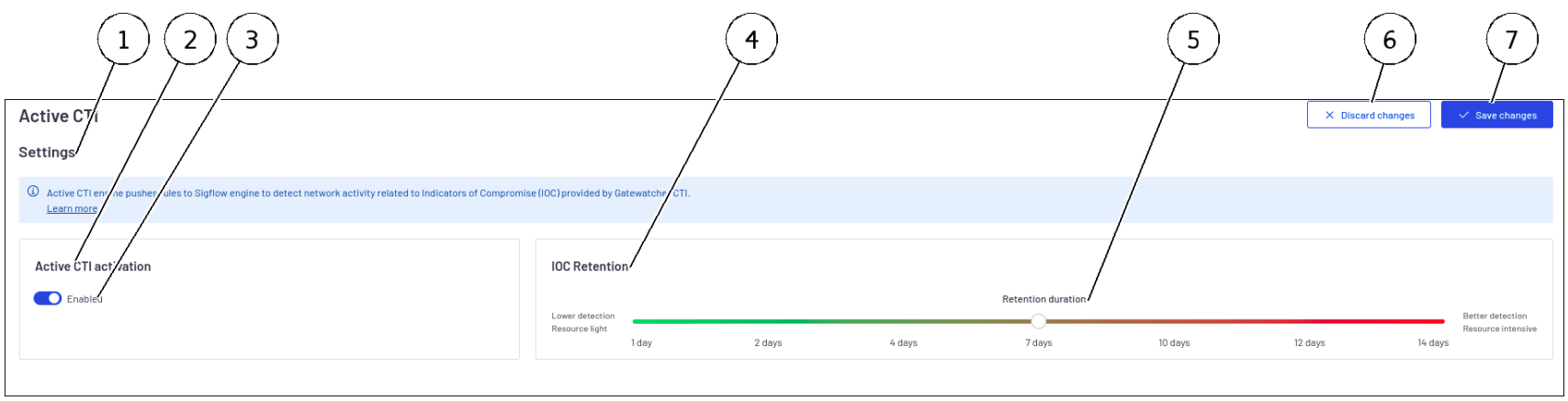
This screen is only accessible to members of the *operator* group.

5.7.2.12.2 Links associated

The engine is presented in *Active CTI engine* paragraph.
The visualization of the current engine status is given in the *`Health checks` screen*.
For engine setting implementation, see the procedure *Setting up the Active CTI engine*.

5.7.2.12.3 Screen description

After pressing the `Active CTI` command on the `Detection Strategy\Threat intel` menu, the `Active CTI` screen is displayed.



For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Item	Name	Function
1	`Settings`	Includes all engine settings
2	`Active CTI activation`	Engine Activation Zone
3	`Enabled` selector	Activates or deactivates the engine. Activating the engine activates the `IOC Retention` zone.
4	`IOC Retention`	Zone to adjust the retention time of the IOC.
5	`Retention duration` cursor	Adjusts the retention time. Default value: 7 days The IOC coming from the Gatewatcher CTI source will be deleted at the end of this retention time.
6	`Discard changes` button	Cancels current changes
7	`Save changes` button	Saves current changes

5.7.2.13 `Retro hunt` screen

5.7.2.13.1 Introduction

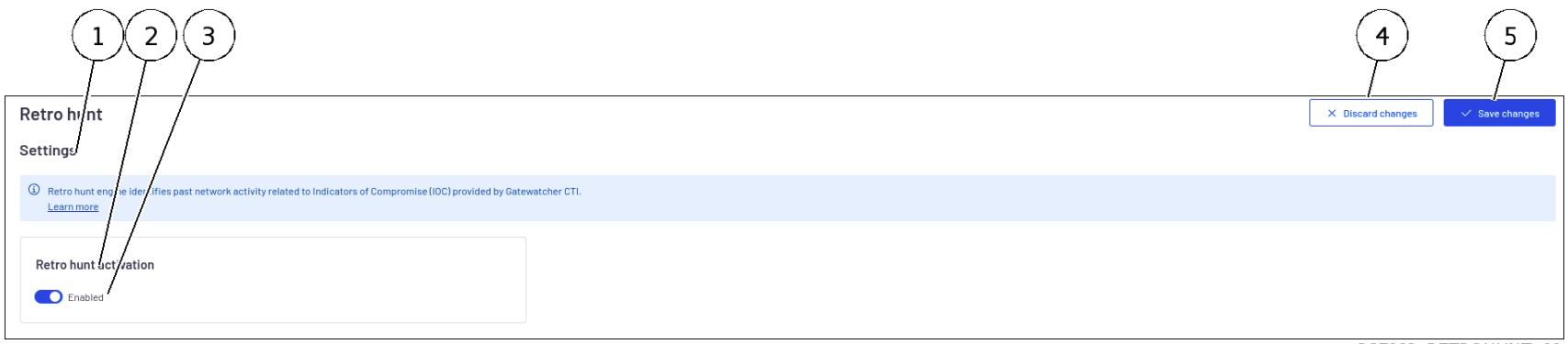
The `Retro Hunt` screen enables to activate the engine.
This screen is only accessible to members of the *operator* group.

5.7.2.13.2 Links associated

The engine is presented in the *Retro hunt engine* paragraph.
The visualization of the current engine status is given in *`Health checks` screen*.
For engine setting implementation, see *Setting up the retro hunt engine*.

5.7.2.13.3 Screen description

After pressing the `Retro Hunt` command on the `Detection Strategy\Threat intel` menu, the following screen is displayed.



For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Item	Name	Function
1	`Settings`	Includes all engine settings
2	`Retro Hunt activation`	Engine Activation Zone
3	`Enabled` selector	Activates the engine
4	`Discard changes` button	Cancels current changes
5	`Save changes` button	Saves current changes

5.7.2.14 `Ransomware detect` screen (Ransomware command)

5.7.2.14.1 Introduction

The `Ransomware detect` screen enables to:

- Activate the engine and show its state
- Set the engine sensitivity
- Investigate on the alerts and the detection threshold
- Define the list of IP addresses not to be analyzed and therefore consider them to be healthy

This screen is only accessible to members of the *operator* group.

5.7.2.14.2 Links associated

The engine is presented in the *Ransomware detect engine* paragraph.
The visualization of the current engine status is given in the *`Health checks` screen*.
For engine setting implementation, see the *Setting up the Ransomware detect engine*.
For the implementation of the ignored file list, see the *Managing the Ignore list of the Ransomware detect*.

5.7.2.14.3 Screen description

After pressing the `Ransomware` command on the `Detection Strategy\Threat intel` menu, the `Ransomware detect` screen is displayed.

GCE103_RANSO_01

For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

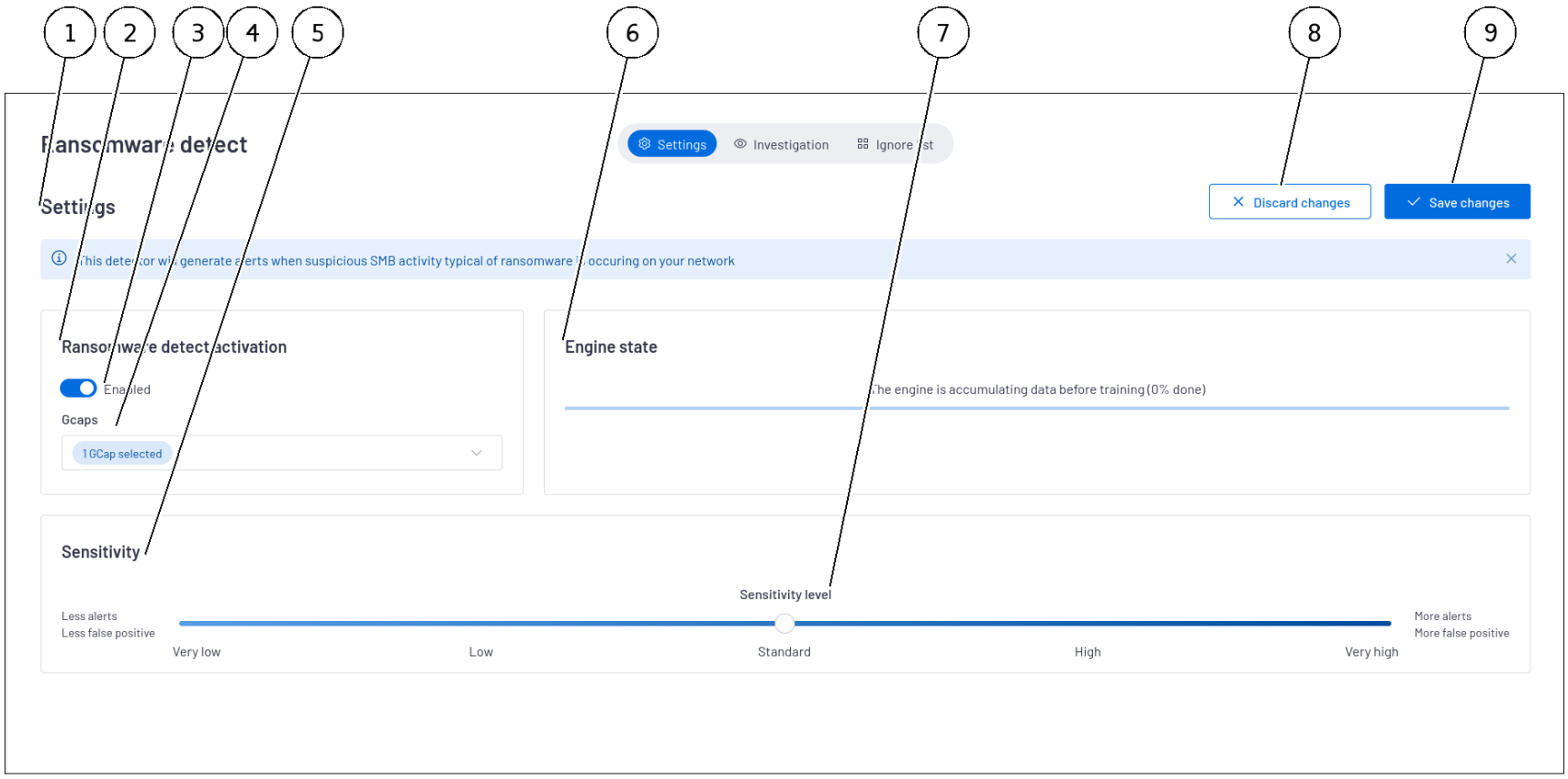
The `Ransomware detect` screen contains the following areas:

Area	Function
`Settings`	Engine settings
`Investigation`	Session activity
`Ignore list`	List of ignored IP addresses considered healthy.

5.7.2.14.4 `Settings` area of the `Ransomware detect` screen

The `Settings` area is used to:

- Activate the engine
- Show its state
- Set the engine sensitivity
- Define the list of files not to be analyzed and therefore consider them to be healthy



GCE103_RANSO_01

Item	Name	Function
1	`Settings`	Includes all engine settings
2	`Ransomware detect activation`	Engine Activation Zone
3	`Enabled` selector	Activates or deactivates the engine in the selected GCaps
4	`Gcaps`	This field displays the selected GCaps (default = all)
5	`Sensitivity`	Engine sensitivity adjustment area
7	`Sensitivity level` slider	Adjusts the sensitivity threshold to raise an alert
6	`Engine state`	Indicates the current state: training state or running In training state: - The following message is displayed : `The engine is accumulating data before training (x%)`. - The engine is trained with legitimate data corresponding to the specific traffic (for further information, see the *Analyzing the Ransomware detect alerts*) - If this is the first training, the engine does not trigger alerts. Otherwise alerts are triggered with the previous settings. In Running state: - The following message is displayed: `The engine is running` - The engine raises alerts according to the sensitivity
8	`Discard changes` button	Cancels current changes
9	`Save changes` button	Saves current changes

The user chooses a sensitivity level.

To display an alert on an SMB stream, the engine will analyze parts of that stream (sample).

Each sample is analyzed and scored.

When a sample's score exceeds the detection threshold, that sample is potentially attributed to ransomware.

When the number of samples that have exceeded the detection threshold is higher than the detection threshold set by the sensitivity setting then a Ransomware-type alarm is created.

It is therefore this number of samples that exceeded the detection threshold that is defined by the adjustment of the sensitivity.

Level	Definition
`Very low`	Sensitivity 1: the detection threshold is higher than the optimum value defined by the engine training. Generates fewer alerts, including fewer false positives
`Low`	Sensitivity 2
`Standard`	Sensitivity 3: default value. The detection threshold is at the optimal value defined by the engine training.-
`High`	Sensitivity 4
`Very high`	Sensitivity 5: the detection threshold is lower than the optimum value defined by the engine training. Generates more alerts, including more false positives

The engine will then issue all alerts whose sensitivity level is less than or equal to the configured sensitivity level:

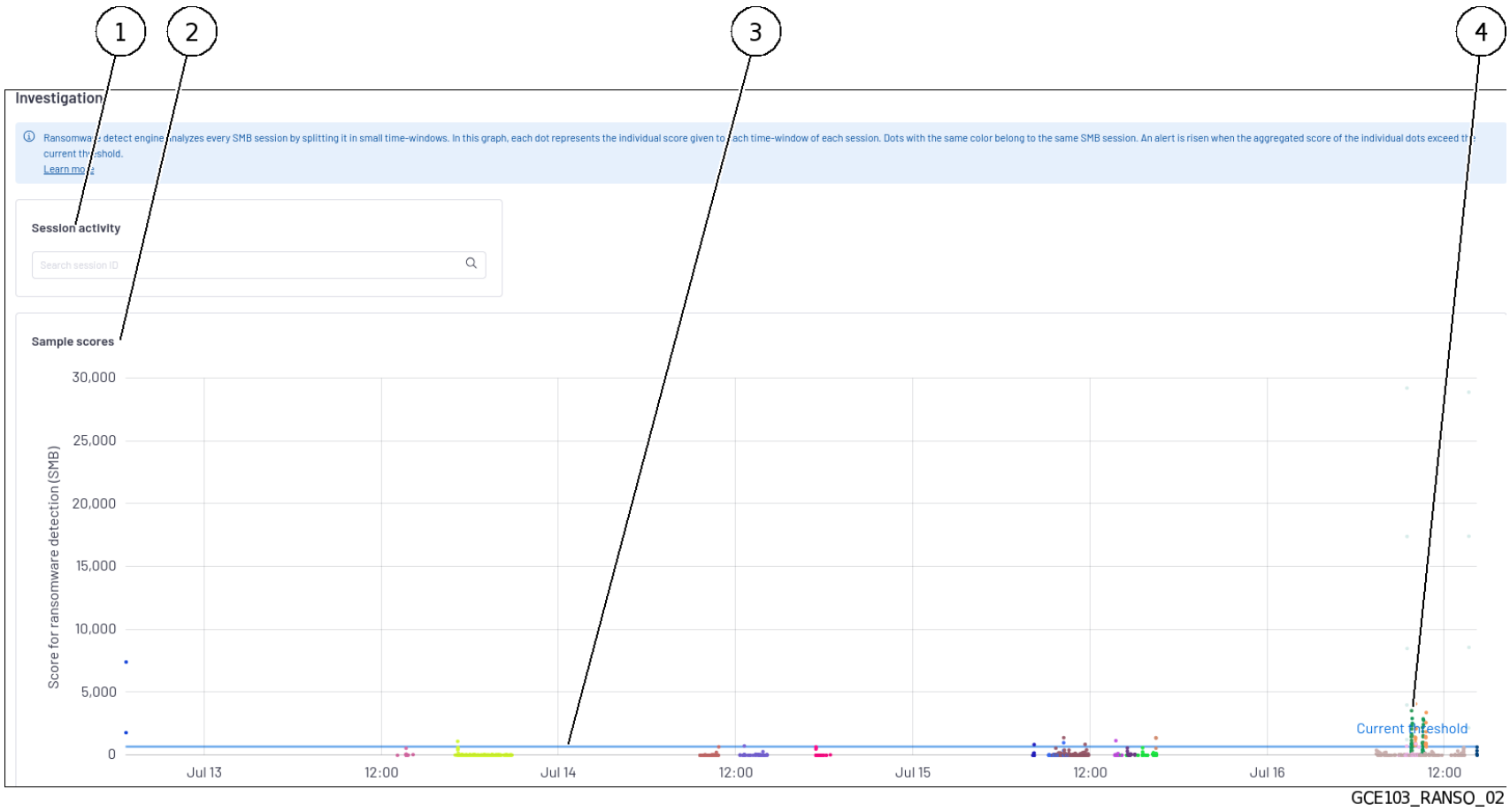
- For example, if the user sets the maximum sensitivity level (5), the engine will issue level 1,2,3,4 and 5 alerts
- If the user sets the sensitivity level to 3 (default), the engine will issue level 1, 2 and 3 alerts
- If the user sets the sensitivity level to 1 (the least sensitive), the engine will only issue level 1 alerts

Important:

In order to use the Ransomware detect engine correctly, GCaps must have:
- SMB logging enabled
- SMB stream-depth parameter set to 100MB minimum.
  The default value when pairing a GCap is only 10MB on some profiles, a notification is then issued.

5.7.2.14.5 `Investigation` area of the `Ransomware detect detect detect` screen

The `Investigation` area is used to investigate on the alerts and the detection threshold.



GCE103_RANSO_02

Item	Name	Function
1	`Session activity`	Allows to find a sample after entered the session_ID
2	Sample scores	dynamic scale for the score for the ransomware detection
3	`Current threshold`	Samples with a score above the current threshold are counted as alerts

continues on next page

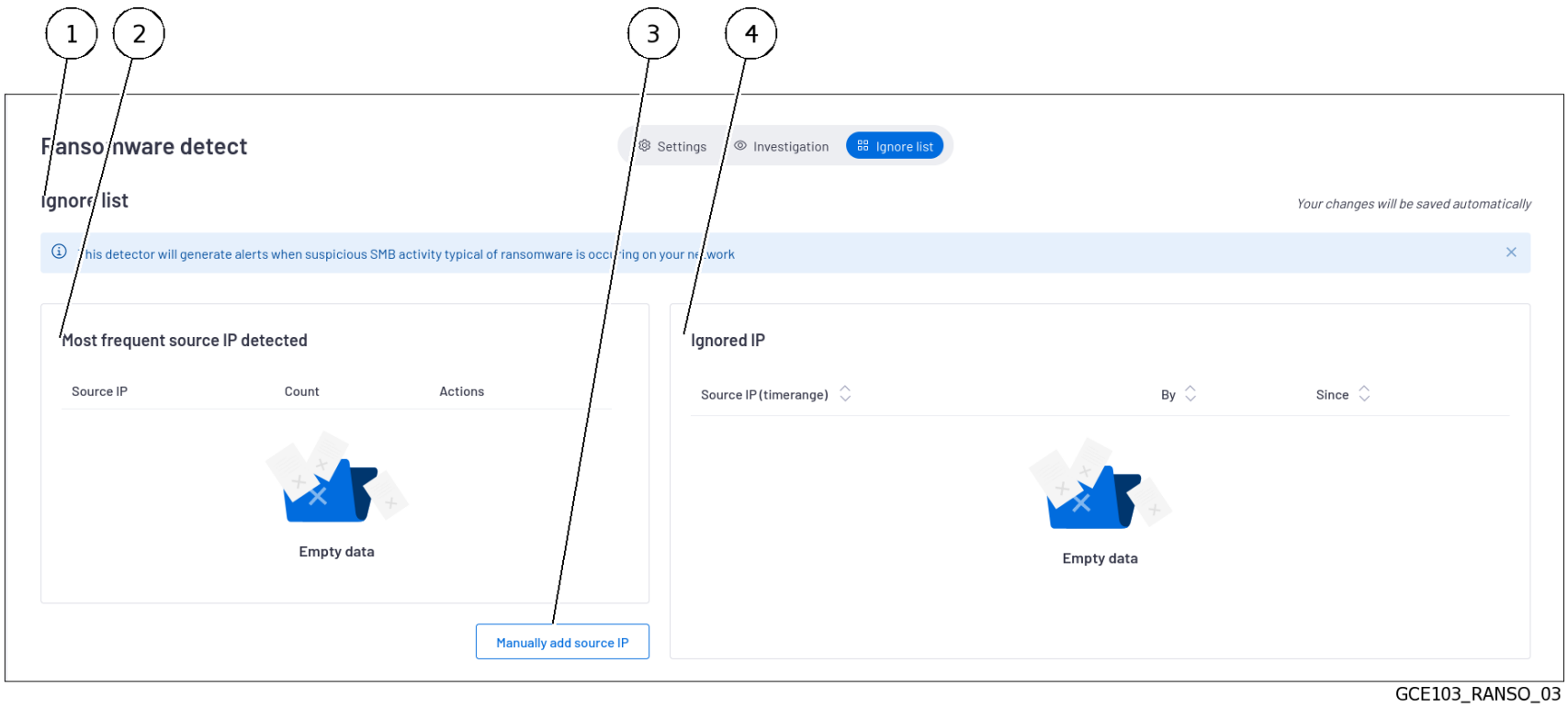
Table 19 – continued from previous page

Item	Name	Function
4	Examples of samples defined as alerts	These samples have values higher than the current threshold

Ransomware detect engine analyzes every SMB session by splitting it in small time-windows.
In this graph, each dot represents the individual score given to each time-window of each session.
Dots with the same color belong to the same SMB session.
An alert is risen when the aggregated score of the individual dots exceed the current threshold.

5.7.2.14.6 `Ignore list` area of the `Ransomware detect` screen

The `Ignore list` area is used to define the list of files not to be analyzed and therefore consider them to be healthy



GCE103_RANSO_03

Item	Name	Function
1	`Ignore list`	Window to create the IP addresses to ignore
2	`Most frequent source IP detected`	Field displaying the most frequent source IP addresses detected
3	`Manually add source IP` button	Adds a source IP address to ignore
4	`Ignored IP`	Field listing the IP addresses to ignore It is possible to specify a time range

---

5.7.2.15 `Association rules` screen (Configuration command)

5.7.2.15.1 Introduction

The `Asset detection network range` screen consists of the following sections.

Section	Description	See
Asset detection network range	Entering private network address ranges for detection d'equipment	*`Asset detection network range` section of the `Assets/Users Association rules` screen*
Static IP -Asset mapping	Mapping and IP address assignment of active equipment	*`Static IP- Asset mapping` section of the `Assets/Users Association rules` screen*
Ignored IP for users association	Definition of IP addresses to be ignored	*`Ignored IP for users association` section of the `Assets/Users Association rules` screen*

continues on next page

Table 21 – continued from previous page

Section	Description	See
Ignored MAC for assets association	List of MAC addresses not to be associated with active devices	*`Ignored MAC for assets association` section of the `Assets/Users Association rules` screen*
Forbidden users	List of prohibited users	*`Forbidden users` section on the `Assets/Users Association rules` screen*
Forbidden assets	List of active network equipment that is prohibited	*`Forbidden assets` section on the `Assets/Users Association rules` screen*

This screen is only accessible to members of the *operator* group.

5.7.2.15.2 Links associated

For implementation, see the *Procedure to manage association rules*.

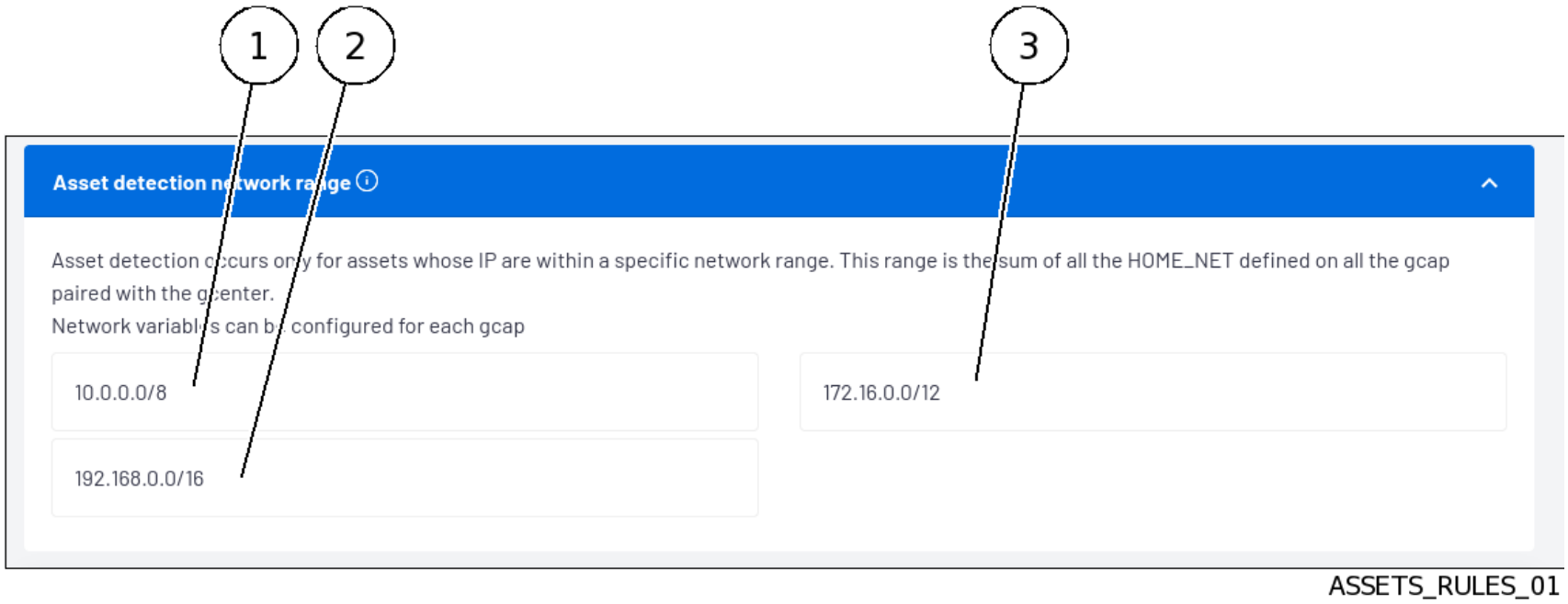
5.7.2.15.3 Screen description

After pressing the `Configuration` button on the menu `Assets and users detection`, the screen `Association rules` is displayed:

For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

5.7.2.15.4 `Asset detection network range` section of the `Assets/Users Association rules` screen

The `Asset detection network range` section enables to view/modify the private network address ranges for asset detection.



ASSETS_RULES_01

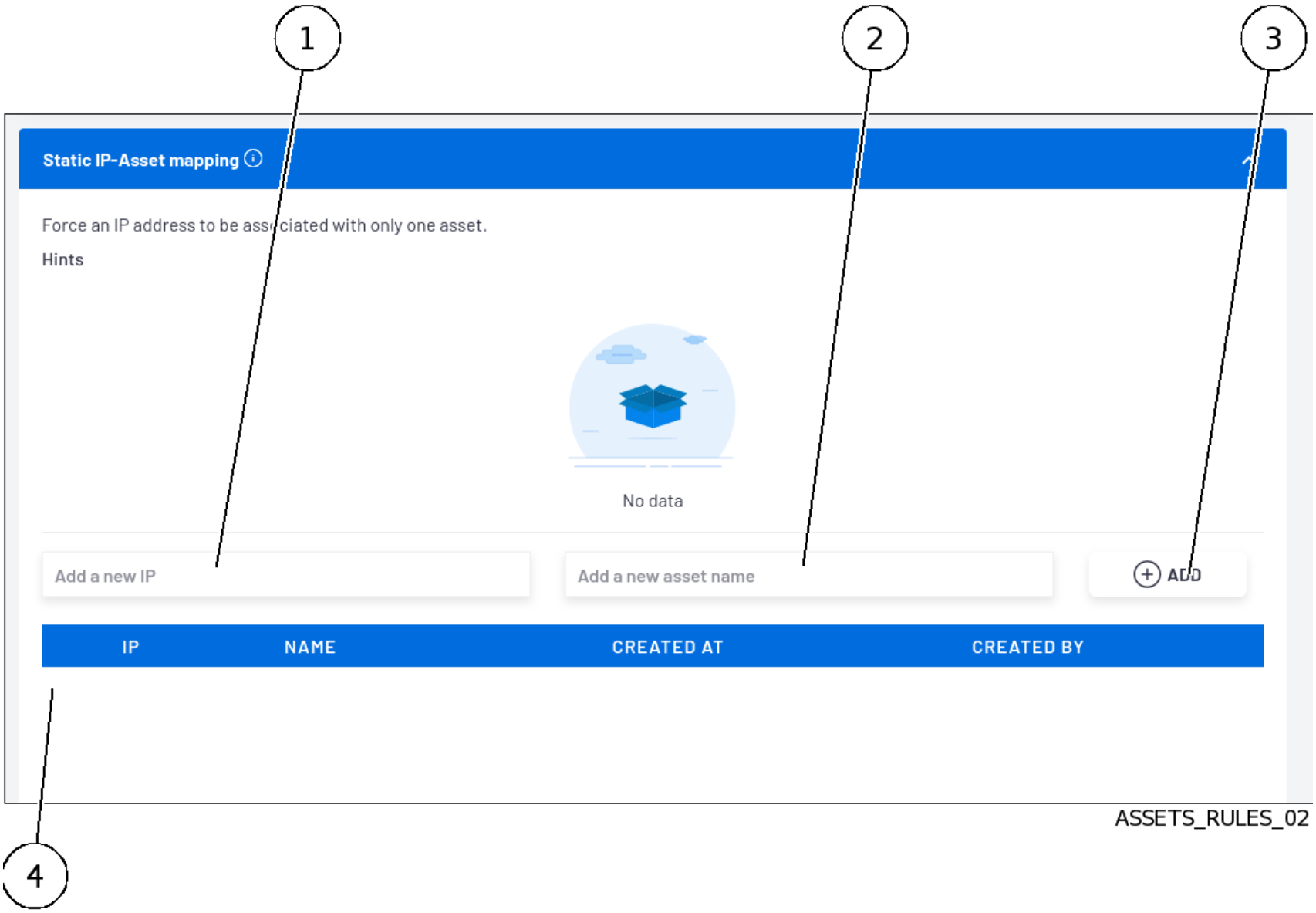
Active device detection only occurs for devices with an IP address within a specific network range.
This range is the amount of HOME_NET defined on all GCap paired with the GCenter.
Network variables can be configured for each GCap.
For GCaps where network variables have not been specified, HOME_NET is associated by default with the private networks defined by RFC1918.
This window displays the input fields in the address ranges reserved for private networks in IPv4:

Item	Private address view field	Detailed IP Range
1	prefix (10.0.0.0/8)	10.0.0.0 – 10.255.255.255
2	prefix (172.16.0.0/12)	172.16.0.0 – 172.31.255.255
3	prefix (192.168.0.0/16)	192.168.0.0 – 192.168.255.255

The link `Network variables can be configured for each gcap` modifies internal networks via the GCAP profile customization function.
This link takes you to the `GCaps profiles` window (see *`GCaps profiles` screen*).

5.7.2.15.5 `Static IP- Asset mapping` section of the `Assets/Users Association rules` screen

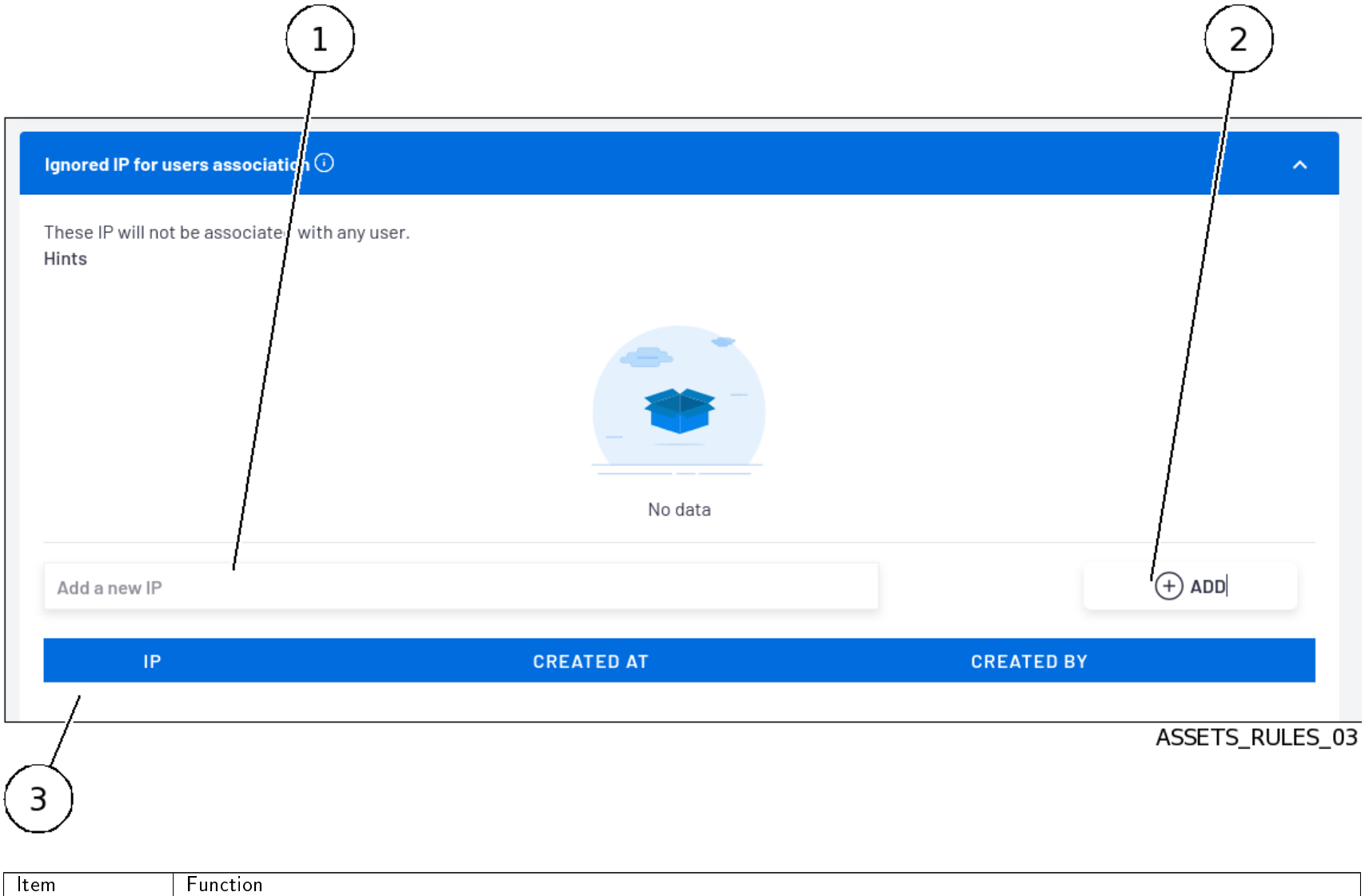
The `Static IP Asset mapping` section displays the list each association of a static IP with an active asset on the network.



Item	Function
1	Input field for the IP address to be associated with a new asset
2	Input field for a new asset
3	Button to add a new asset with the previous parameters
4	List of existing equipment. This includes the following types of information: - IP address - The name - The creation date - The creator's name

5.7.2.15.6 `Ignored IP for users association` section of the `Assets/Users Association rules` screen

The `Ignored IP for user association` section displays the list of IP addresses not to be associated with users.

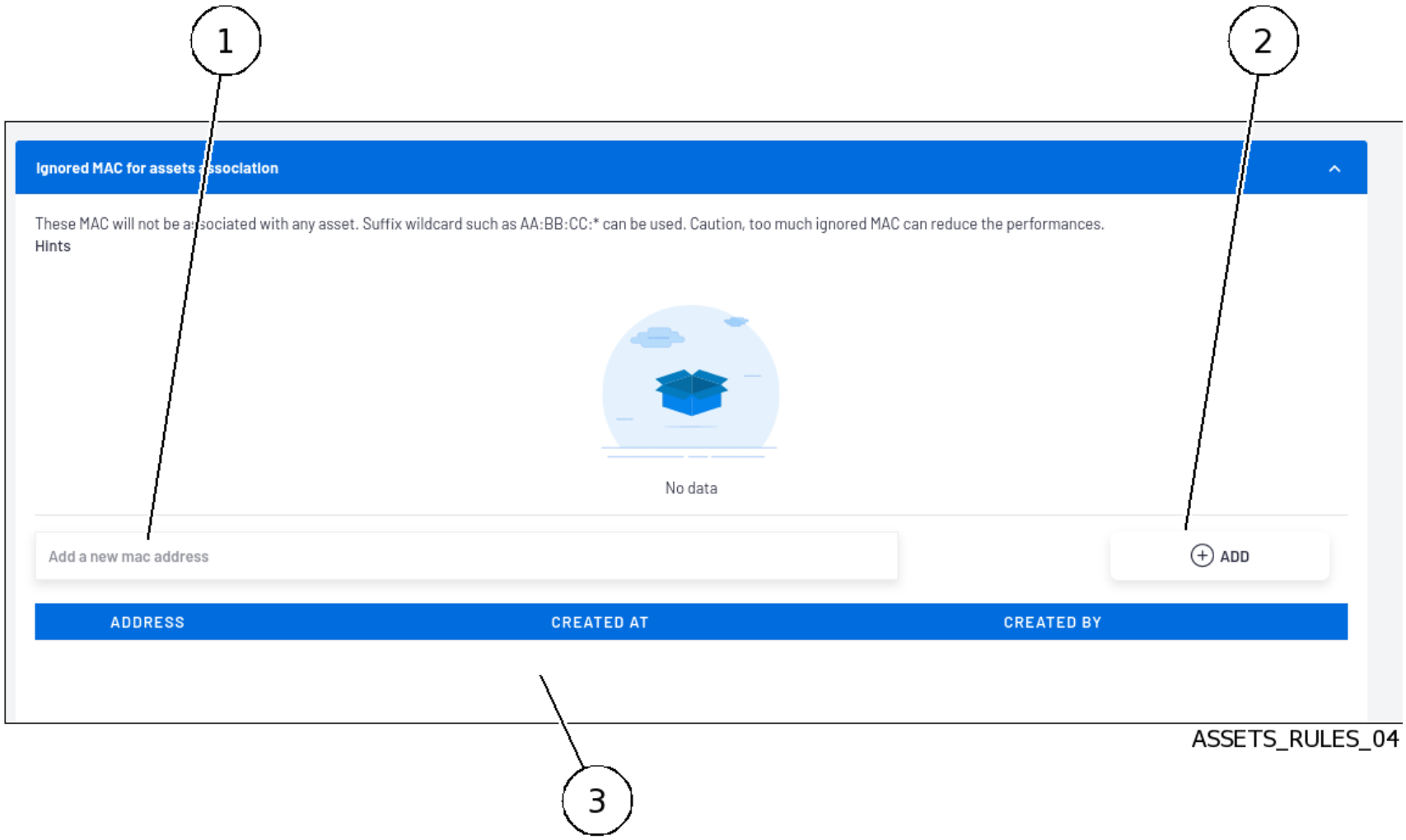


Item	Function
1	Input field for the IP address to be ignored
2	Button to add a new IP address
3	List of existing equipment. This includes the following types of information: - IP address - The creation date - The creator's name

---

5.7.2.15.7 `Ignored MAC for assets association` section of the `Assets/Users Association rules` screen

The `Ignored MAC for asset association` section displays the list of MAC addresses not to be associated with active assets.



ASSETS_RULES_04

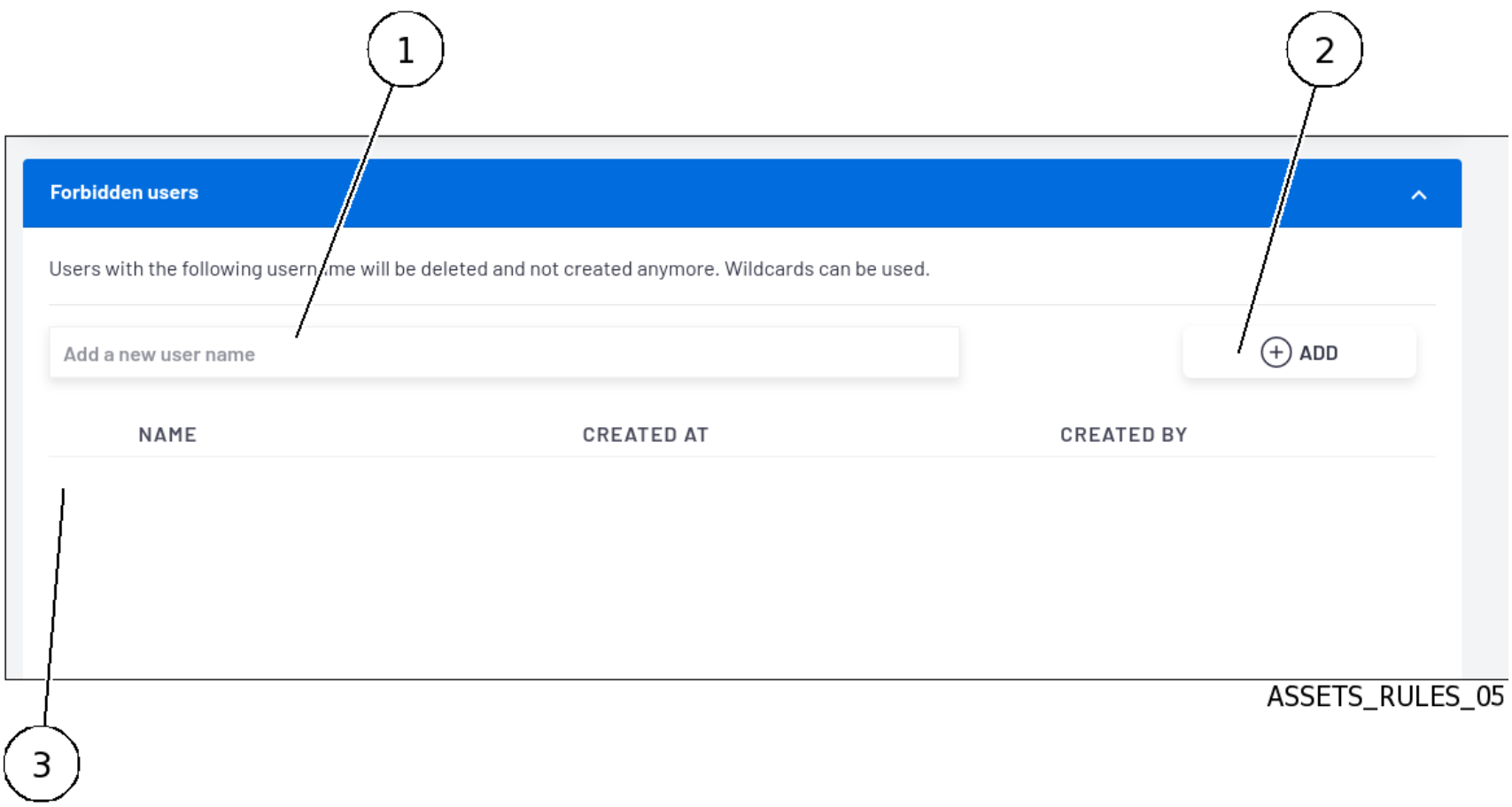
Item	Function
1	Input field for the MAC address to be ignored
2	Button to add a new MAC address
3	List of existing equipment. This includes the following types of information: - MAC address - The creation date - The creator's name

Note:

Ignore MAC addresses will not be associated with any active equipment.
Suffix wildcard characters such as AA:BB:CC:* can be used.
Caution: Setting too many ignore MAC addresses may reduce performance.

5.7.2.15.8 `Forbidden users` section on the `Assets/Users Association rules` screen

The "Forbidden users" section displays a list of users who are forbidden.
Users with the user name defined here will be deleted. They will no longer be displayed in the dashboards.
Wildcard characters can be used.

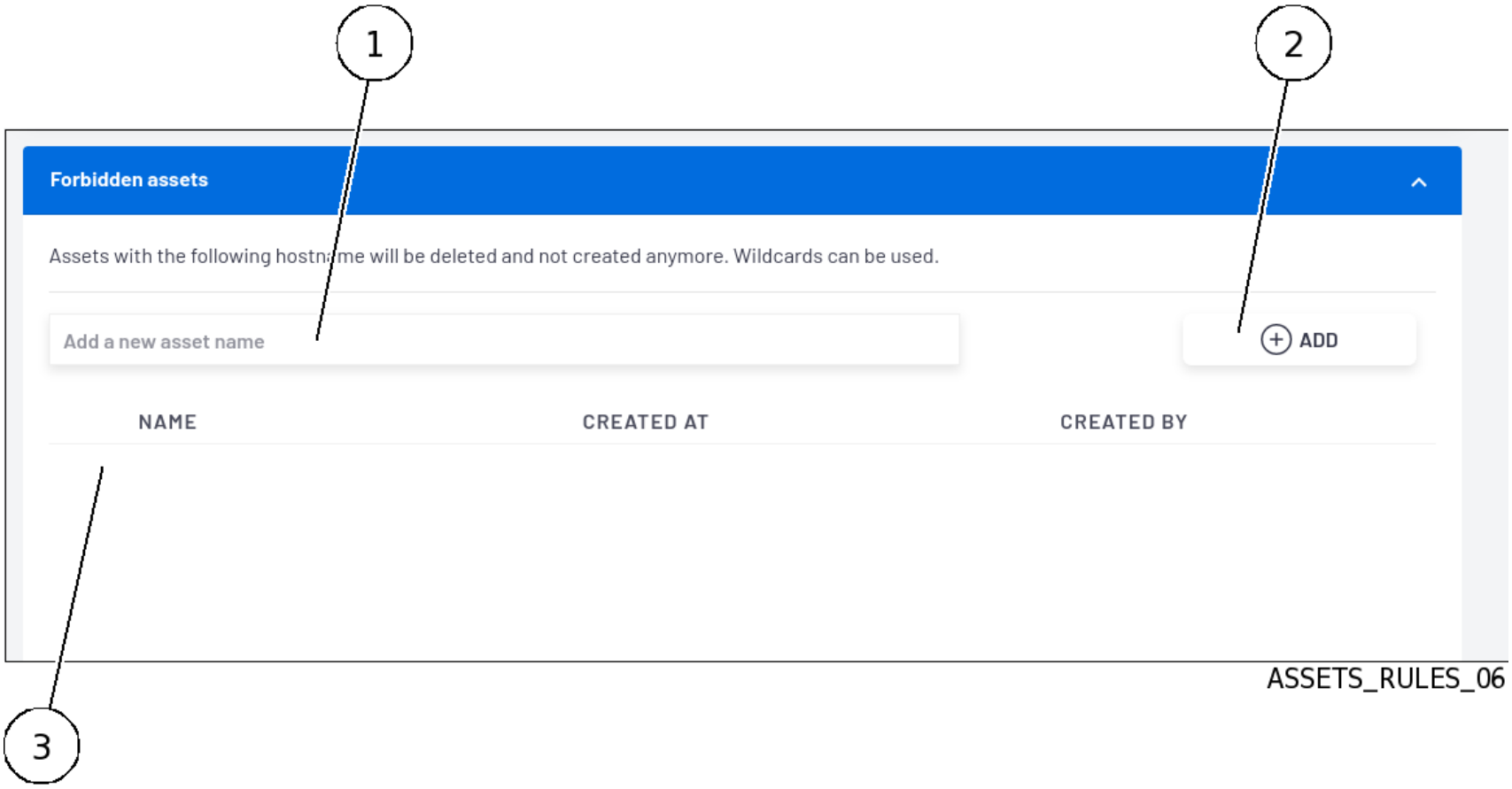


Item	Function
1	Input field for the user name to be prohibited
2	Button to add a new user name
3	List of existing names. This includes the following types of information: - The name - The creation date - The creator's name

---

5.7.2.15.9 `Forbidden assets` section on the `Assets/Users Association rules` screen

The `Forbidden assets` section displays a list of active network assets that are to be forbidden.
Active devices with the name declared in this list will be deleted. They will no longer be displayed in the dashboards.
Wildcard characters can be used.



ASSETS_RULES_06

Item	Function
1	Input field for the name of the equipment (hostname) to be prohibited
2	Button to add a new device name (hostname)
3	List of existing names. This includes the following types of information: - The name of the device (hostname) - The creation date - The creator's name

5.7.2.16 `DGA detect` screen (DGA command)

5.7.2.16.1 Introduction

The `DGA` screen enables to:

- Activate the engine
- Configure detection sensitivity
- Define the list of url not to be analyzed and therefore consider them to be healthy

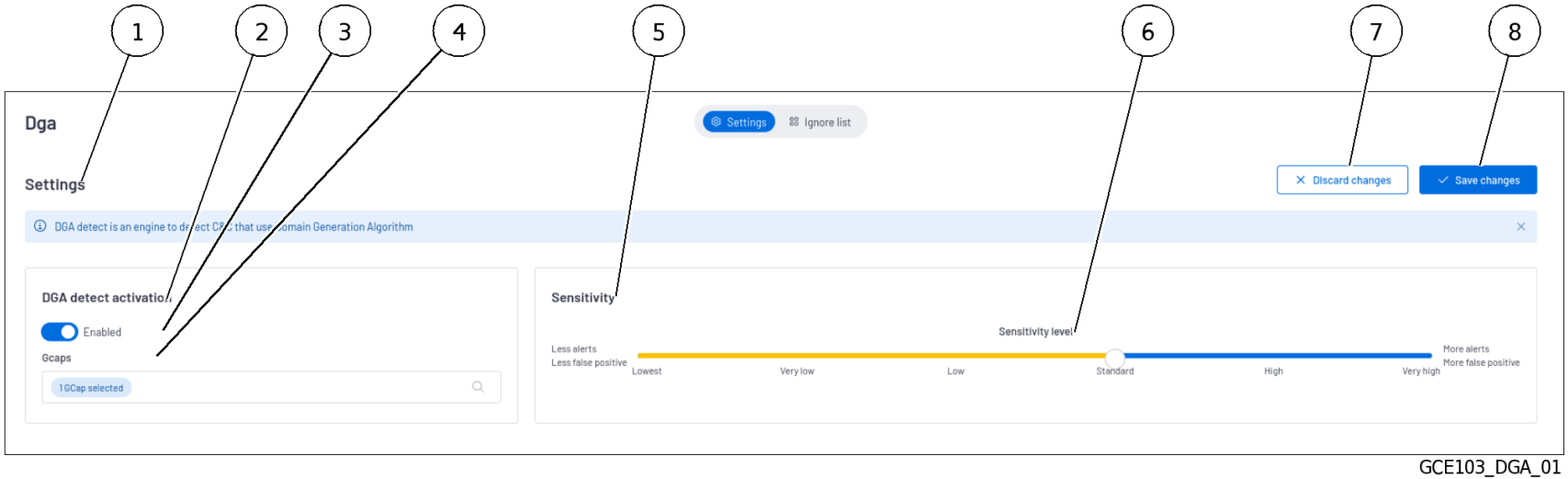
This screen is only accessible to members of the *operator* group.

5.7.2.16.2 Links associated

The engine is presented in the *DGA detect engine* paragraph.
The visualization of the current engine status is given in the *`Health checks` screen*.
For engine setting implementation, see the *Setting up the DGA detect engine*.
For implementation of the exception list, see the *Managing the Ignore list of the DGA detect engine*.

5.7.2.16.3 Screen description

After pressing the `DGA` command on the `Detection Strategy\C&C` menu, the `DGA detect` screen is displayed.



GCE103_DGA_01

For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Area	Function
`Settings`	Engine settings
`Ignore list`	List of ignored items are considered healthy

5.7.2.16.3.1 `Settings` area of the `DGA` screen

The `Settings` section (1) displays the engine settings.

GCE103_DGA_01

Item	Name	Function
1	`Settings`	Includes all engine settings
2	`DGA detect activation`	Engine activation area parameters
3	`Enabled` selector	Activates or deactivates the engine
4	`Gcaps`	This field displays the selected GCaps
5	`Sensitivity`	Engine sensitivity adjustment area
6	`Sensitivity level` slider	Sensitivity slider
7	`Discard changes` button	Cancels current changes
8	`Save changes` button	Saves current changes

Level	Definition
`Very low`	Sensitivity 1
`Low`	Sensitivity 2
`Standard`	Sensitivity 3 : default value
`High`	Sensitivity 4
`Very high`	Sensitivity 5

Note:

Sensitivity 3 is the optimum that is used:

- To have a near zero false positive rate (once the few specific domain names of the client are added to the ignore list)
- To have a very high detection rate

Note:

Sensitivity 5 is closest to the unit alerts of v102 of **GCenter**.

The DGA detect engine produces 5 levels of alerts.
The level of an alert is computed by tracking for each source ip, the count of domains classified by the engine as being generated by a DGA:

- If sensitivity is set to `Low`, only the critical alerts will be issued
- If sensitivity is set to `Very high`, every alerts will be issued: this results in a better detection at the price of more false positive

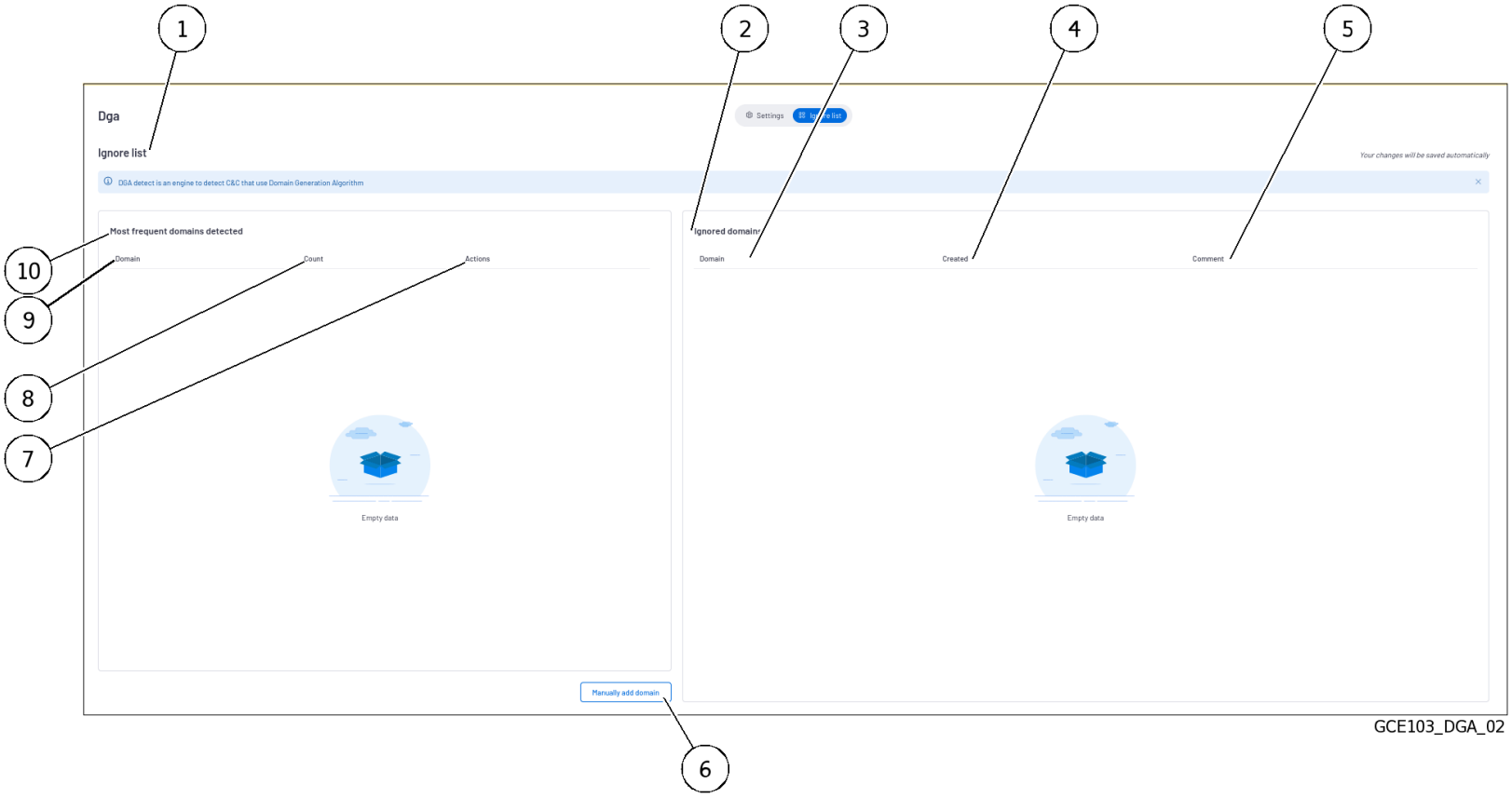
---

5.7.2.16.3.2 `Ignore list` area of the `DGA` screen

The `Ignore list` area enables to filter the domains and IP addresses considered healthy.
It can be completed manually:

- The first days of engine activation to correct some possible false positives
- Following the activation of an option to increase engine sensitivity
- After an investigation leading to the identification of a false positive

After clicking on the `Ignore list` button, the following window is displayed.



Item	Name	Function
1	`Ignore list`	The `Ignore list` area enables to filter the domains considered healthy. Ignore list is a set of exceptions, based on domain names. The engine discards alerts that match these exceptions.``` This can be used to discard false positive detections that occur regularly.
	Short information about this screen.	The Learn more link opens the embedded documentation on the corresponding page.

continues on next page

Table 30 – continued from previous page

Item	Name	Function
2	`Ignored domains`	This area list the exception list of domain defined by its URL For each domain, the following information is displayed:
3	`Domain`	Domain URL
4	`Created`	Indicates the date and time the record was created
5	`Comment`	Indicates the comment, if any, for further details
	`Delete` icon	Enables the domain deletion
6	`Manually add domain` button	Adds a new record to the list
10	• `Most frequent domains detected`	Field displaying the most frequent domains detected For each domain, the following information is displayed:
9	`Domain`	• Domain URL
8	`Count`	• Indicates the number of occurrences of the domain name
7	`Action`	• Possible actions for this domain

5.7.2.17 `Beacon detect` screen (Beacon command)

5.7.2.17.1 Introduction

The `Beacon detect` screen is used to:

- Activate the engine
- Configure detection sensitivity
- Define the list of url not to be analyzed and therefore consider them to be healthy

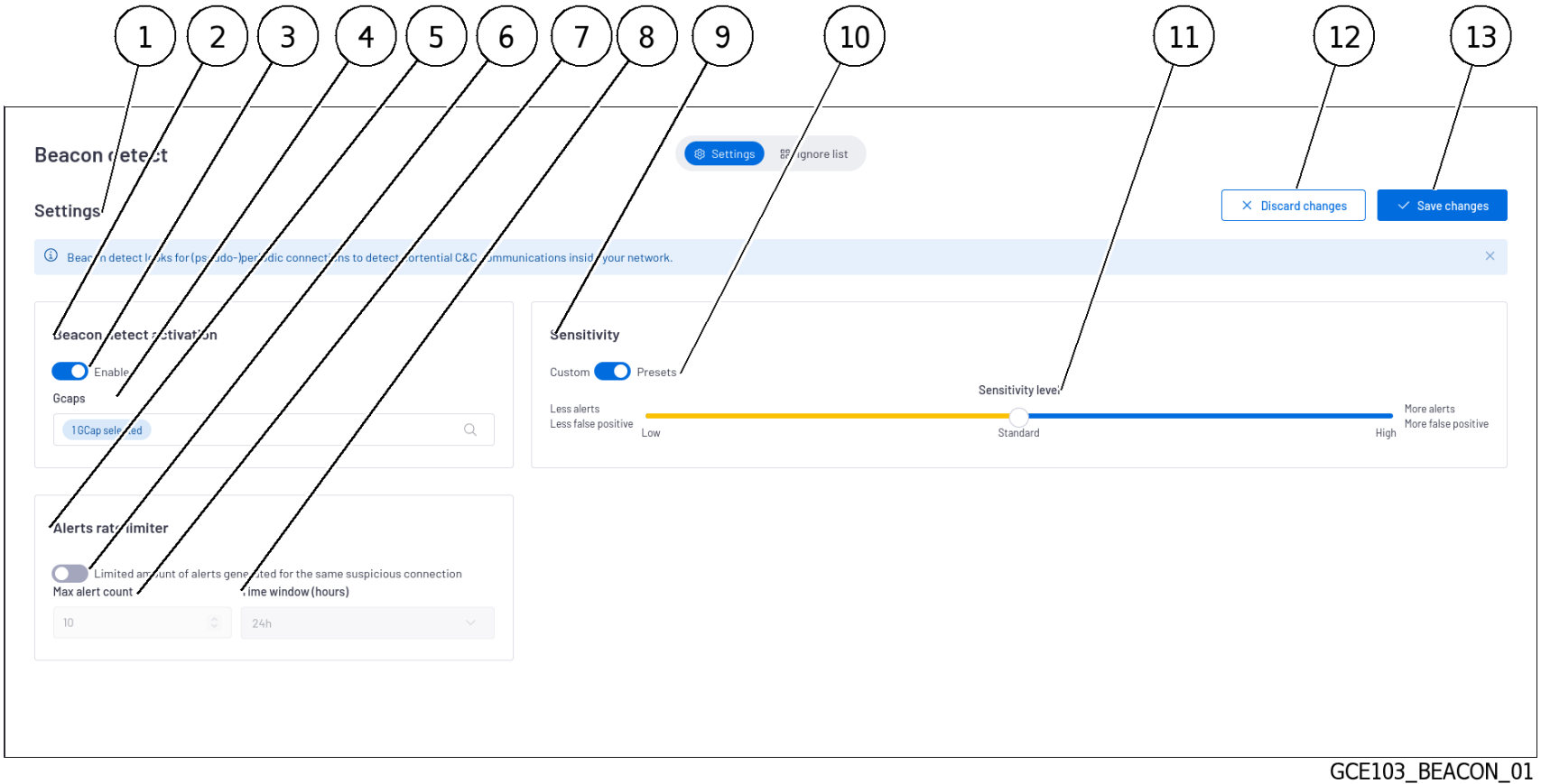
This screen is only accessible to members of the *operator* group.

5.7.2.17.2 Links associated

The engine is presented in the *Beacon detect engine* paragraph.
The visualization of the current engine status is given in the *`Health checks` screen*.
For engine setting implementation, see the *Setting up the beacon detect engine* procedure.
For implementation of the exception list, see the *Managing the Ignore list of the Beacon detect* procedure.

5.7.2.17.3 Screen description

After pressing the `Beacon` command on the `Detection Strategy\C&C` menu, the `Beacon detect` screen is displayed.



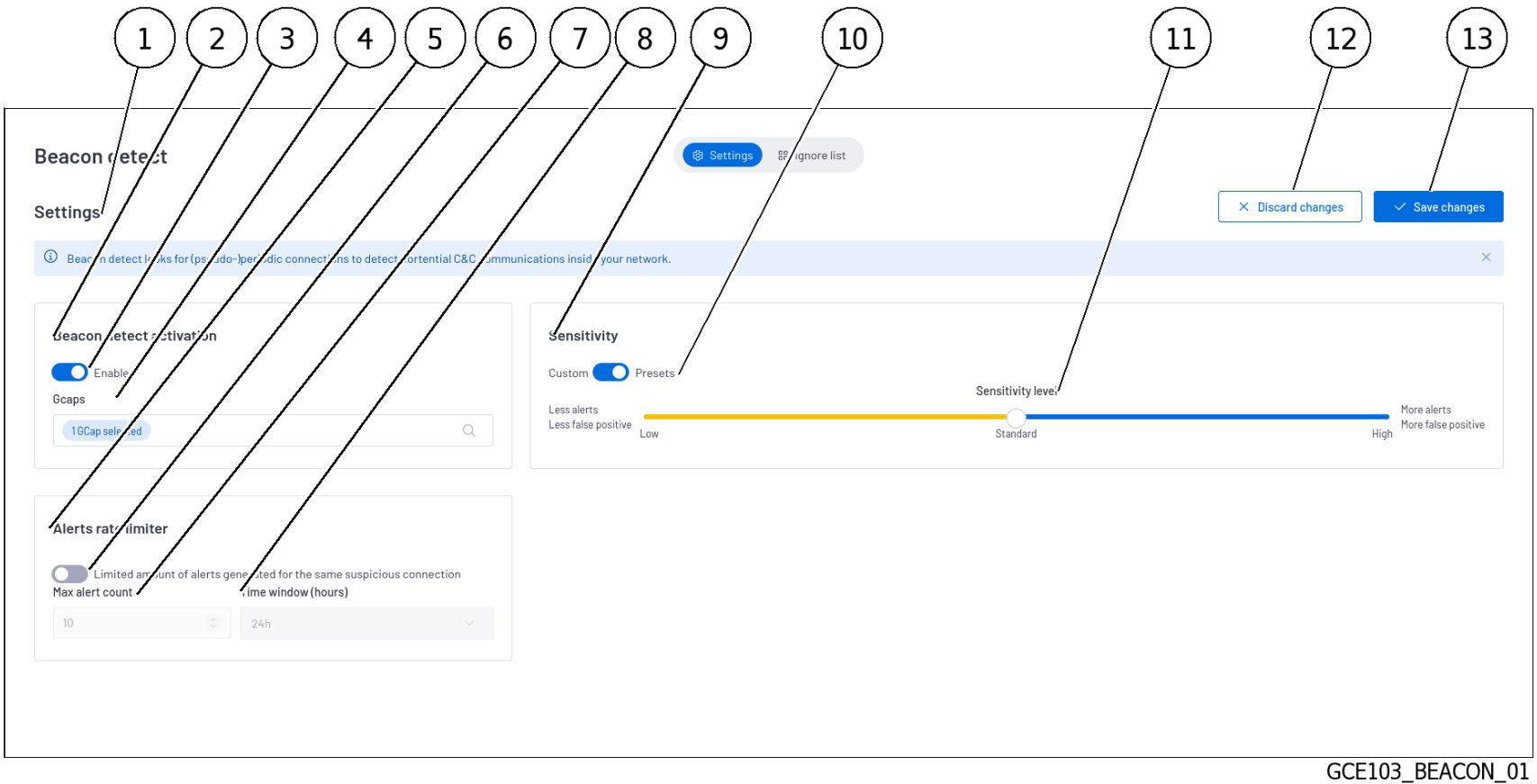
GCE103_BEACON_01

For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Area	Function
`Settings`	Engine settings
`Ignore list`	List of ignored url which are considered healthy

5.7.2.17.4 `Settings` area of the `Beacon detect` screen

The `Settings` area (1) displays the engine settings.



GCE103_BEACON_01

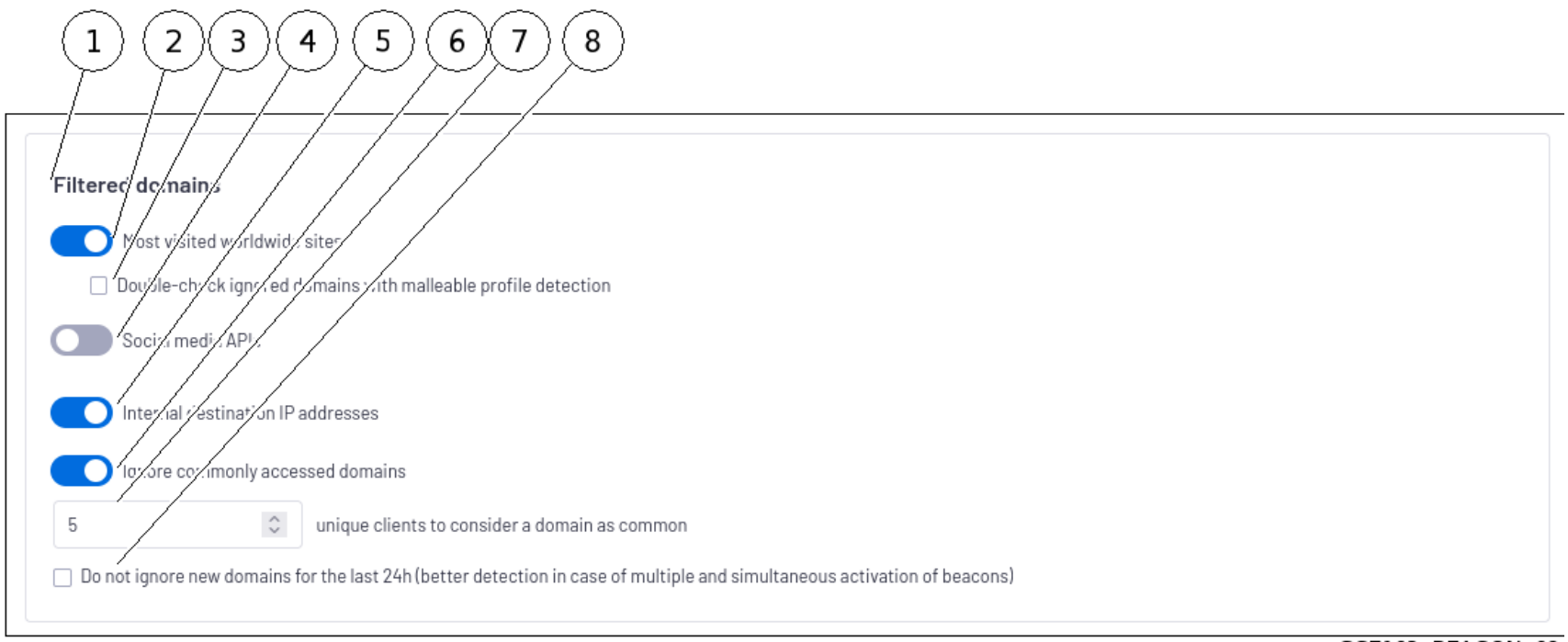
Item	Name	Function
1	`Settings`	Includes all engine settings
2	`Beacon detect activation`	Engine activation zone

continues on next page

Table 31 – continued from previous page

Item	Name	Function
3	• `Enabled` selector	• Activates or deactivates the engine
4	• `Gcaps` field	• Displays the selected GCaps
5	`Alerts rate limiter` zone	Limits the alerts generated for the same suspicious connection`
6	• `Limited amount of alerts generated for the same suspicious connection` selector	• Activates the function
7	• `Max alert count`	• Maximum number of alerts
8	• `Time window (hours)`	• Duration during which the counting is done
9	`Sensitivity`	Engine sensitivity adjustment zone
10	• `Custom-Presets`	• Sensitivity level setting slider The sensibility level is the combinaison of the activation of different parameters. This combinaison can be define manually (`Custom` choice) or use predefined settings (`Presets` choice) If cursor is in position `Presets`, setting the sensitivity level is done by the selector `Sensitivity level`. If the selector is in the `Custom` position, the sensitivity level is set by the `Filtered domains` area that appears. For more details see below.
11	• `Sensitivity level` slider	• Sets sensitivity by preset levels. Default: Standard
12	`Discard changes` button	Cancels current changes
13	`Save changes` button	Saves current changes

5.7.2.17.4.1 Filtered domains area



GCE103_BEACON_08

Item	Name	Function
1	`Filtered domains`	Configuration window to filter domains ie the listed domains are considered healthy

continues on next page

Table 32 – continued from previous page

Item	Name	Function
2	• `Most visited worldwide sites` selector	If used, the domains that correspond to Most visited sites in the world are filtered
3	• `Double-check ignored domains with malleable profile detection`	The `Double-check ignored domains with malleable profile detection` is displayed only when `Social media APIs` is displayed. This option only applies to http event-type whose hostname is not an IP address. This option is only used when a hostname associated with a http beaconing connection is present in one of the public ignore lists (known public domains and social network APIs). It is then necessary to verify that the hostname is present in a DNS log and that its IP address (found in the DNS log) corresponds to the dest_ip of the connection. The presence of the hostname in the ignore list but also in the DNS logs confirms that it is a legitimate beacon. The presence of the hostname in the ignore list but not in the DNS logs can indicate the presence of a potentially malicious beacon that has undergone a change in the Host field of the HTTP header. This scan should be performed if there are at least 24 hours of DNS events. These 24 hours are necessary because the default configuration of most DNS servers is a 24-hour cache. Thus, not finding a domain resolution in the last 24 hours does not necessarily mean that the domain has not been resolved (and is therefore a malleable profile), since it could be in the cache.
4	• `Social media APIs` selector	If used, the domains that correspond to social media APIs are filtered The `Double-check ignored domains with malleable profile detection` is displayed only when `Social media APIs` is displayed.
5	• `Internal destination IP addresses` selector	If used, only alerts with a public IP destination are displayed in the `destination.ip`.
6	• `Ignore commonly accessed domains` selector	If used, filters frequently accessed/popular domains within the company. The popularity of a domain is determined by the number of unique customers in the company who have accessed that domain. This number is defined in the parameter `unique clients to consider a domain as common`. By default, the time range [now; -3 days] determines the popularity of a domain. However, there is the following risk. Taking into account the last 24 hours, a C2 that has implants on several machines that can be activated simultaneously, making the C2 domain a popular domain. Hence the presence of the option `Do not ignore new domains for the last 24h (better detection in case of multiple and simultaneous activation of beacons)`
7	• `unique clients to consider a domain as common`	Defines the number of different clients that have accessed this domain.
8	• `Do not ignore new domains for the last 24h (better detection in case of multiple and simultaneous activation of beacons)`	This option allows to not ignore (i.e., allow the analysis of new domains) new domains from the last 24 hours. In conclusion, after analysis on the 24h, the new analyzed and therefore healthy domains can then be ignored because being part of `Ignore commonly accessed domains`

5.7.2.17.4.2 Presets choices and the associated parameters

Table 33: Definition of preset levels

Parameter	`Low`	`Standard`	`High`	`Very high`
`Most visited worldwide sites`	Active with malleable profile detection option is inactive	Active with malleable profile detection option is inactive	Active with malleable profile detection option is active	Active with malleable profile detection option is active
`Most visited worldwide sites`	Active with malleable profile detection option is inactive	Active with malleable profile detection option is inactive	Active with malleable profile detection option is active	Inactive
`Social media APIs`	Active but (option malleable profile detection option is inactive)	Inactive	Inactive	Inactive
`Internal destination IP addresses`	Active	Active	Active	Inactive
`Ignore commonly accessed domains`	Active with Max. 2 unique clients to consider as common. Domains from last 24h are also ignored	Active with Max. 5 unique clients to consider as common. Domains from last 24h are also ignored	Active with Max. 5 unique clients to consider as common. Domains from last 24h will not be ignored	Inactive

Note:

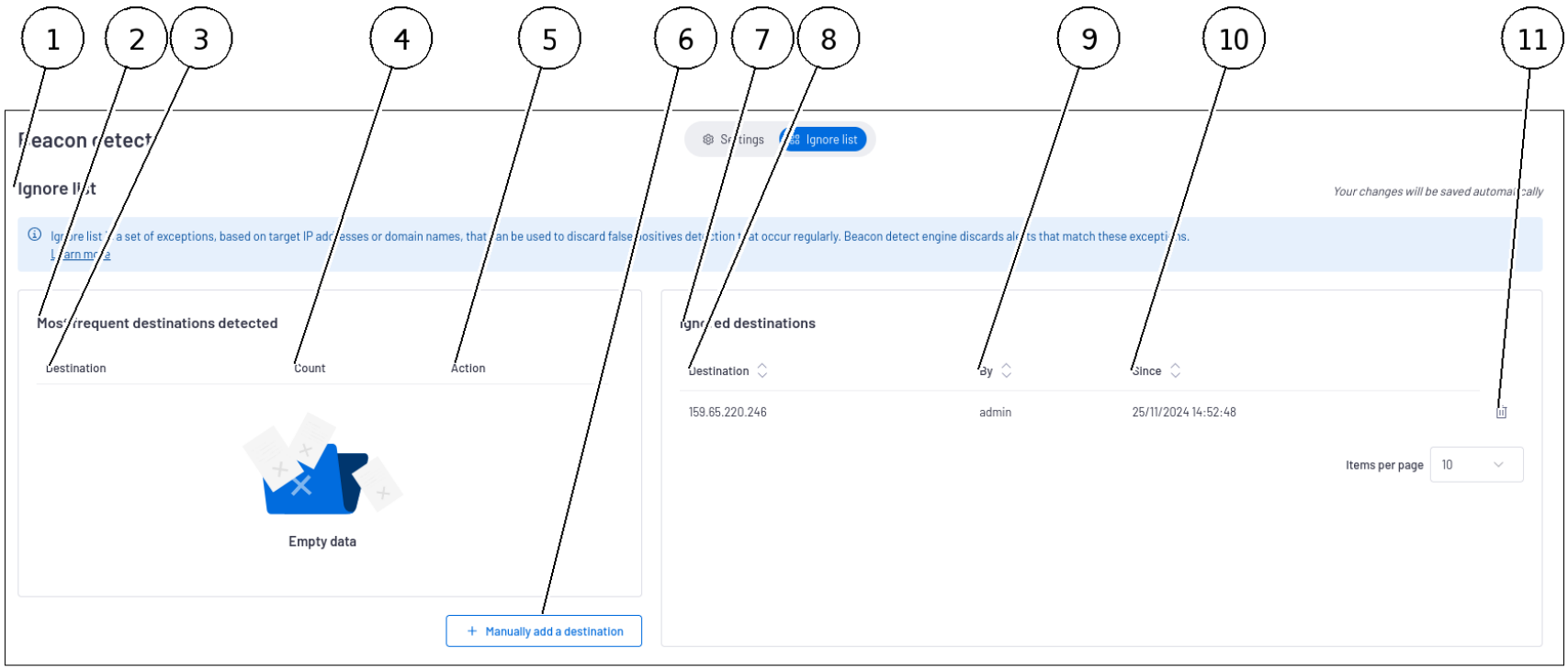
- The `Low` setting increases the number of domain names ignored so there will be fewer alerts and less false positives.
- At the moment, the `Very high` setting generates more alerts and therefore more false positives.

5.7.2.17.5 `Ignore list` area of the `Beacon detect` screen

The `Ignore list` area enables to filter the domains and IP addresses considered healthy.
It can be completed manually:

- The first days of engine activation to correct some possible false positives
- Following the activation of an option to increase engine sensitivity
- After an investigation leading to the identification of a false positive

After clicking on the `Ignore list` button, the following window is displayed.



GCE103_BEACON_02

Item	Name	Function
1	`Ignore list` area	The `Ignore list` area enables to filter the domains and IP addresses considered healthy.

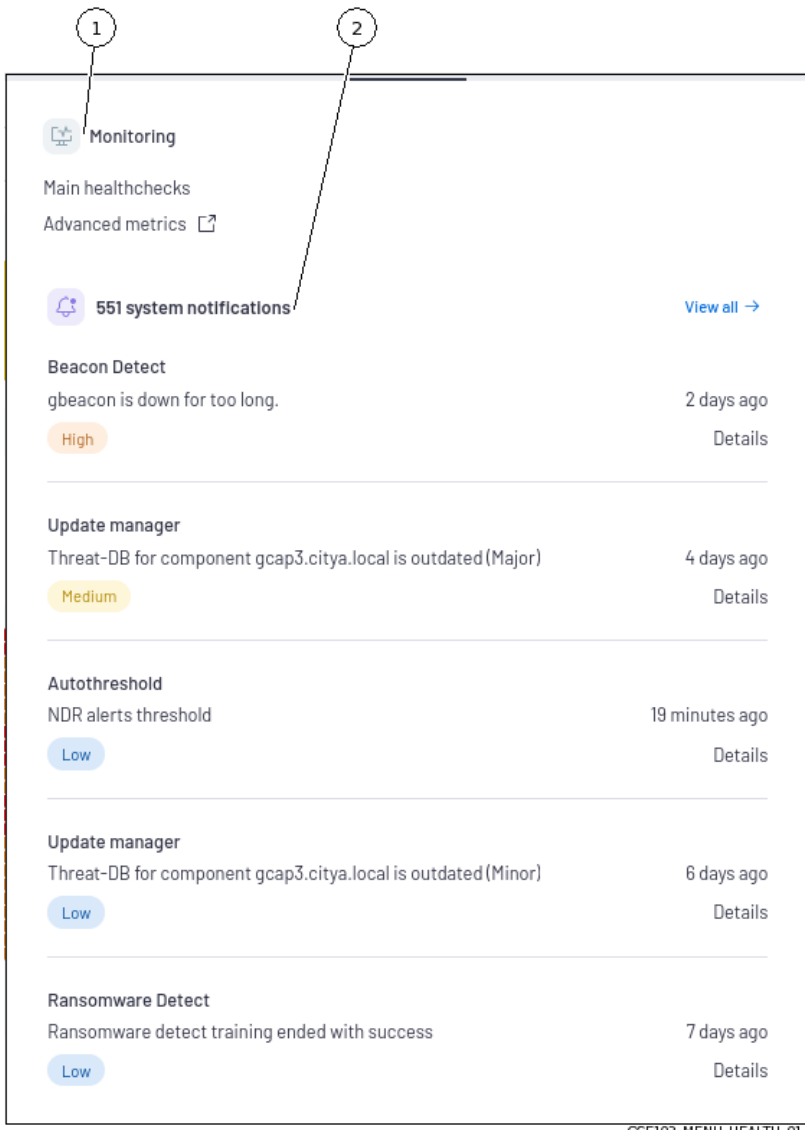
	• `Ignore list is a set of exceptions, based on target IP or domains.`
	`Beacon detect discards alerts that match these exceptions.`
	`This can be used to discard false positive detections that occur regularly, for instance because a legitimate software is implemented with a beacon-like mechanism where clients poll servers periodically..`
		Short information about this screen.
		The Learn more link opens the embedded documentation on the corresponding page.

2	`Most frequent domains detected` zone	Zone displaying the most frequent domains detected For each domain, the following information is displayed:
3	• `Destination`	• Domain URL or IP address
4	• `Count`	• Indicates the number of occurrences of the domain name
5	• `Actions`	• Possible actions for this destination
6	`Manually add a destination` button	Opens the window to add manually a new destination
7	`Ignored destinations` area	This area list the exception list of domain defined by its URL For each domain, the following information is displayed:
8	• `Destination`	• Domain URL or IP address
9	• `By`	• Indicates the account which has created the destination
10	• `Since`	• Indicates the date and time of destination creation
11	• `Delete` icon	• Deletes the domain deletion

5.7.3 `Health` menu

5.7.3.1 Overview of the `Health` menu

The `Health` menu consists of the following:



GCE103_MENU_HEALTH_01

Item	Menu	Command	Description
1	`Monitoring`	`Main healthchecks` `Advanced metrics`	See *`Health checks` screen* See *`Advanced metrics` screen of the Netdata User Interface (Gstats)*
2	System notifications	`View all` or `Details`	See *The `System notifications`*

5.7.3.2 `Health checks` screen

5.7.3.2.1 Introduction

The `Health checks` screen displays:

- The status of the main components
- The detailed status of component engines
- The detailed status of the Sigflow engine

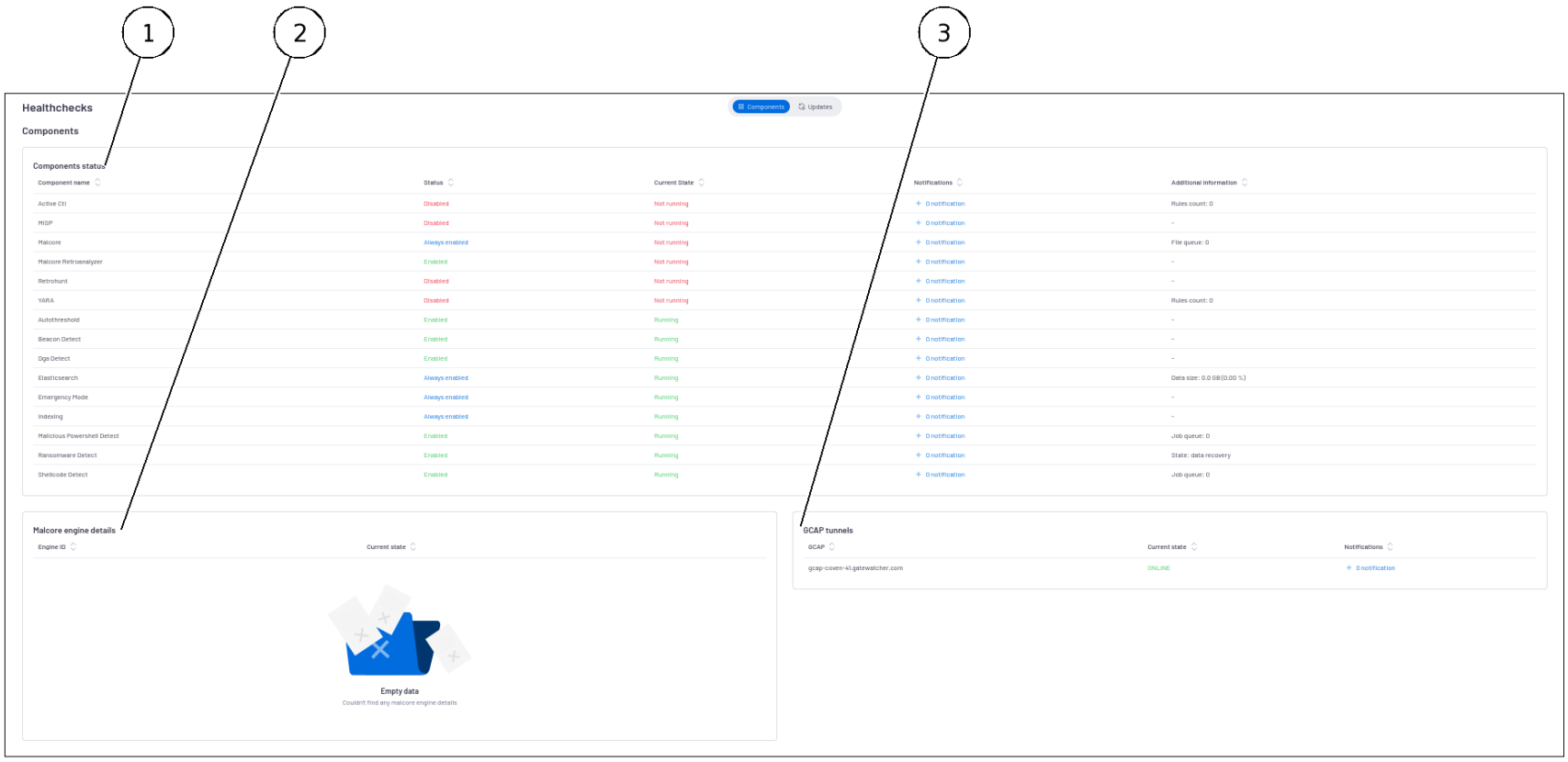
This screen is only accessible to members of the *operator* group.

5.7.3.2.2 Links associated

- To restart a engine, see the *`GCenter Services Management` command*
- To update, refer to *Installing an update manually* to download and install the latest sigflow.gwp file.

5.7.3.2.3 Screen description

After pressing the `Main healthchecks` command on the `Health-Monitoring` menu, the `Healthchecks` screen is displayed.



For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Section	Function
`Components`	Area displaying information about the main components
`Updates`	Area displaying information about the components updates

---

5.7.3.2.4 The `Components` area

The `Components` area consists of the following zones:

- zone (1) `Components status` indicating the main components status: see *The `Components status` zone*
- zone (2) `Malcore engine details` indicating the status of the GCenter Malcore engine: see *The `Malcore engine details` zone*
- zone (3) `GCAP tunnels` indicating the status of the GCap Sigflow engine: see *The `GCAP tunnels` zone*

5.7.3.2.4.1 The `Components status` zone

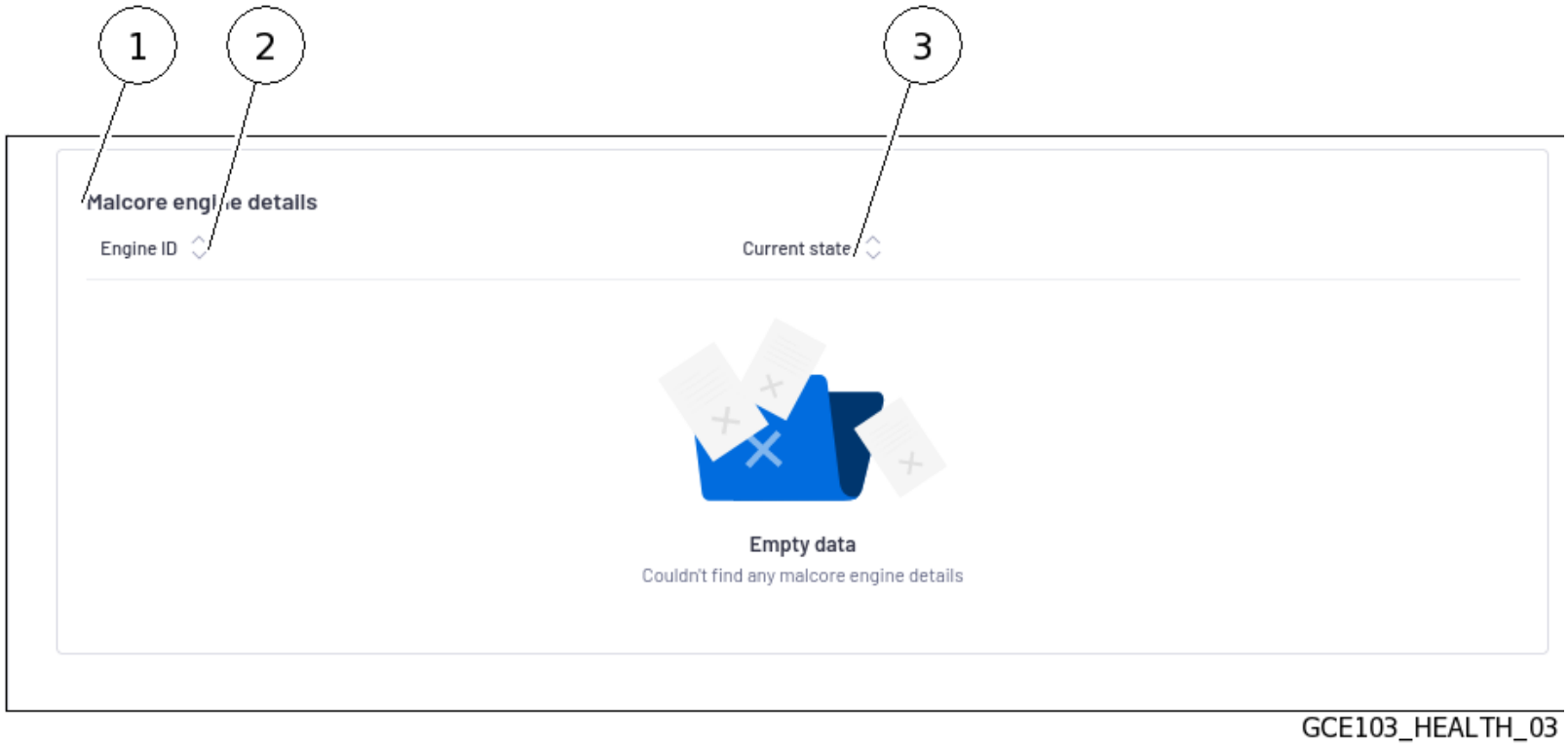
The `Components status` zone includes:

GCE103_HEALTH_02

Item	Name	Description
1	`Components status`	Window showing the state of the GCenter main components
3	`Status`	Indicates the component status - `Disabled`: component disabled in the configuration screen - `Enabled`: component enabled in the configuration screen - `Always enabled`: the Malcore engine is always enabled
4	`Current State`	`Running`: the engine is in `running` status if the Sigflow engine is installed and the API is up. `Not running`
5	`Notifications`	Indicates the notification number about this component Click on this link opens the `System notifications` window
6	`Additional information`	Displays specific information on this component

5.7.3.2.4.2 The `Malcore engine details` zone

The `Malcore engine details` zone includes:



GCE103_HEALTH_03

Item	Name	Description
1	`Malcore engine details`	Displays the current state of each internal engine
2	`Engine ID`	Displays the list of internal motors ID (Engine hash name)
3	`Current state`	Displays this information

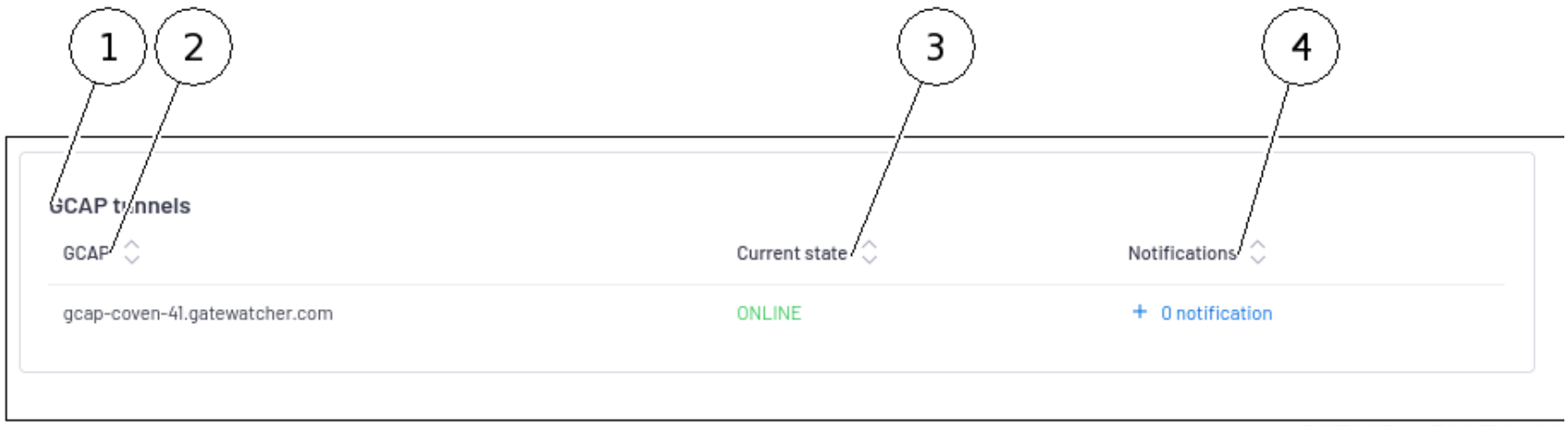
The `Malcore engine details` zone includes:

- An antivirus engine (for some licenses)
- Or 16 antivirus engines (for other licenses)

To restart the Malcore engine, use the `Restart a GApp` command from the configuration menu and select `gmalcore`.

5.7.3.2.4.3 The `GCAP tunnels` zone

The `GCAP tunnels` zone includes:



GCE103_HEALTH_04

Item	Name	Description
1	`GCAP tunnels`	Displays the state of the connexion with each GCap
2	• `GCAP`	• Displays the name of each GCAP connected to the GCenter
3	• `Current state`	• Displays the connection state (ONLINE or OFFLINE)
4	• `Notifications`	• Indicates the notification number about this component Click on this link opens the `System notifications` window

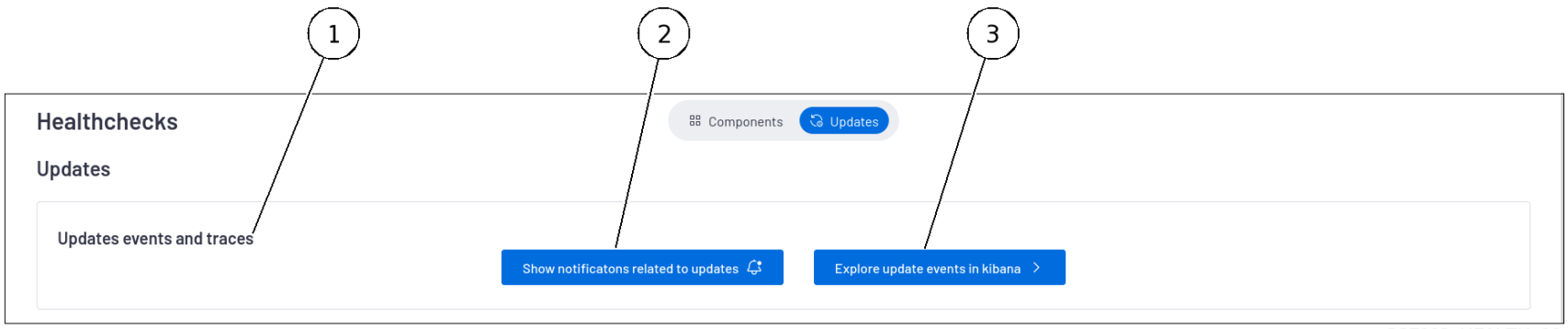
5.7.3.2.5 The `Updates` area

The `Updates` window consists of the following zones:

- `Updates events and traces` zone indicating the two buttons that redirect to what they say they are redirecting to: see *The `Updates events and traces` zone*
- `GCAP updates` zone indicating the GCap name, last update, next synchronisation, recommanded update interval, update lag
  The update lag is computed based on the last update date and the recommanded update time interval
  For instance, if last update was 26h ago, and recommanded update ime is 24h, then update lag is 2h: see *The `GCAP updates` zone*
  - `IOC` zone indicating the CTI last update: see *The `IOC` zone*
- `Sigflow sources` zone indicating the status of the GCap Sigflow engine: see *The `Sigflow sources` zone*
- `Malcore engine` zone indicating the status of the Malcore engine: see *The `Malcore engine` zone*
- `Other engines` zone indicating the status of the other engines: see *The `GCAP tunnels` zone*

5.7.3.2.5.1 The `Updates events and traces` zone

The `Updates events and traces` zone includes:

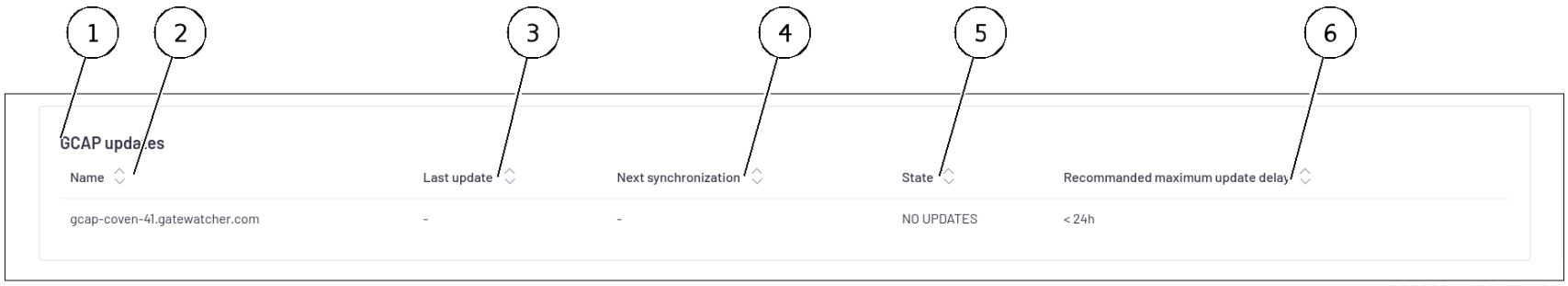


GCE103_HEALTH_10

Item	Name	Description
1	`Updates events and traces` zone	Main section dedicated to the display of activities and logs related to updates..
2	`Show notifications related to updates` button	Opens the `Notifications` window by selecting the Update manager component
3	`Explore update events in Kibana` button	Opens Kibana and displays the update events

5.7.3.2.5.2 The `GCAP updates` zone

The `GCAP updates` zone includes:

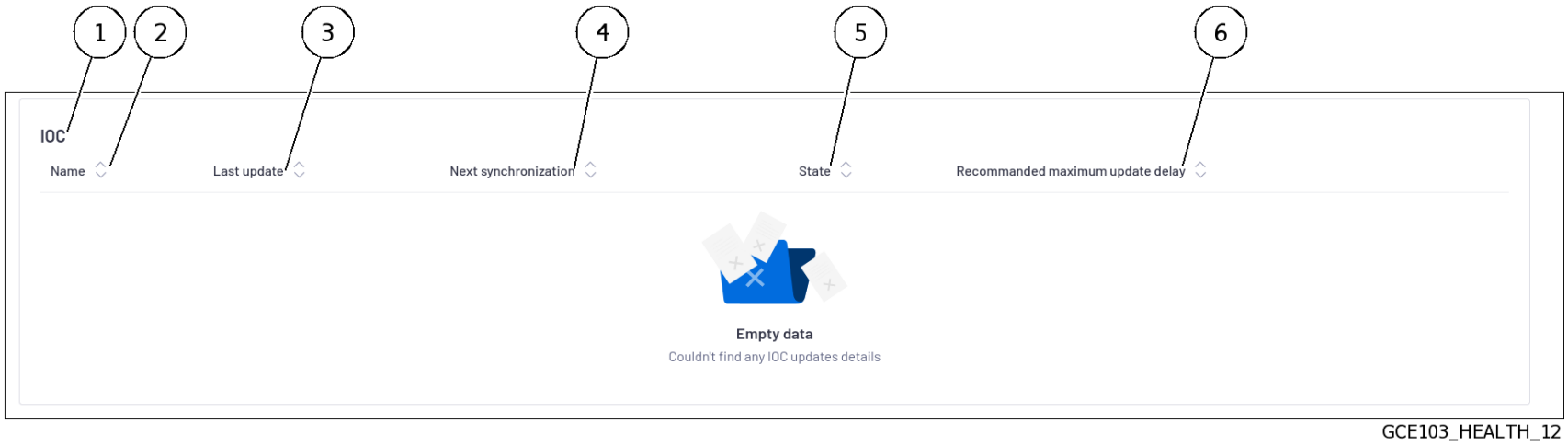


GCE103_HEALTH_11

Item	Name	Description
1	`GCAP updates` zone	Displays the information about the GCap updates
2	• `Name`	• Displays the name of each GCAP connected to the GCenter
3	• `Last update`	• Last update date
4	• `Next synchronisation`	• Next synchronisation date
5	• `State`	• State of the engine update
6	• `Recommanded maximum update delay`	• Recommanded maximum update delay

5.7.3.2.5.3 The `IOC` zone

The `IOC` zone includes:

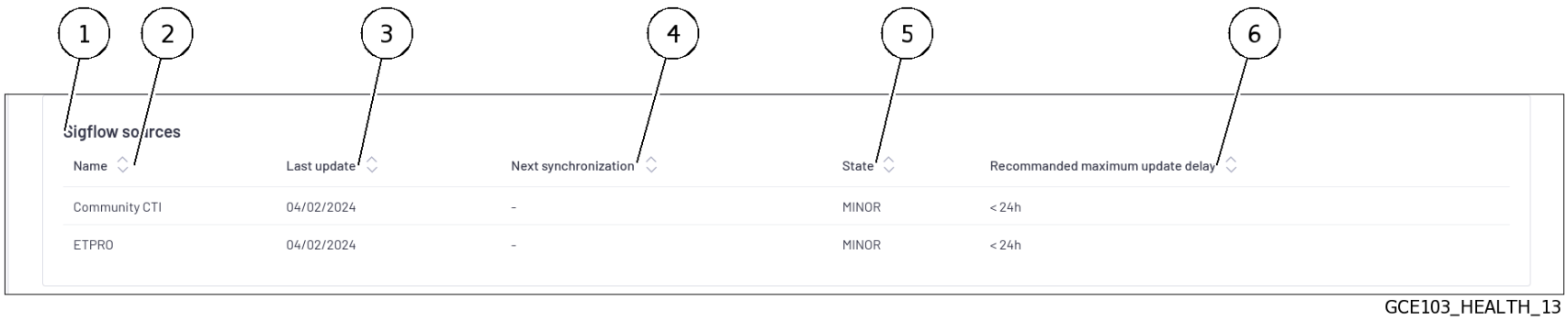


GCE103_HEALTH_12

Item	Name	Description
1	`IOC`	Displays the information about the IOC updates
2	• `Name`	• Name
3	• `Last update`	• Last update date
4	• `Next synchronisation`	• Next synchronisation date
5	• `State`	• State of the update
6	• `Recommanded maximum update delay`	• Recommanded maximum update delay

5.7.3.2.5.4 The `Sigflow sources` zone

The `Sigflow sources` zone includes:

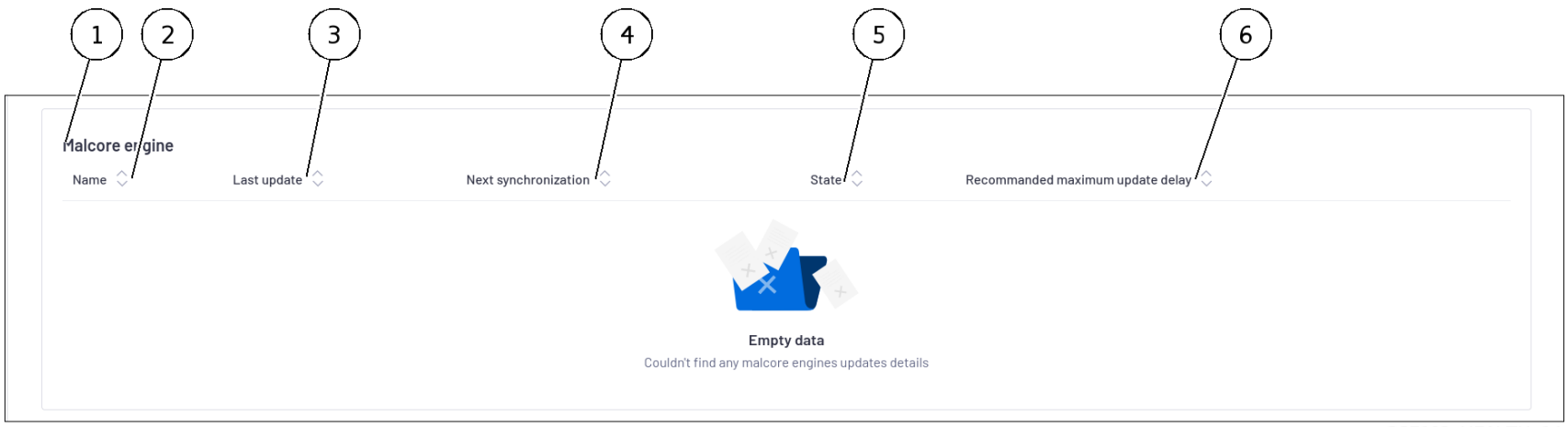


GCE103_HEALTH_13

Item	Name	Description
1	`Sigflow sources`	Displays the information about the Sigflow sources updates
2	`Name`	Name
3	`Last update`	Last update date
4	`Next synchronisation`	Next synchronisation date
5	`State`	State of the update
6	`Recommanded maximum update delay`	Recommanded maximum update delay

5.7.3.2.5.5 The `Malcore engine` zone

The `Malcore engine` zone includes:

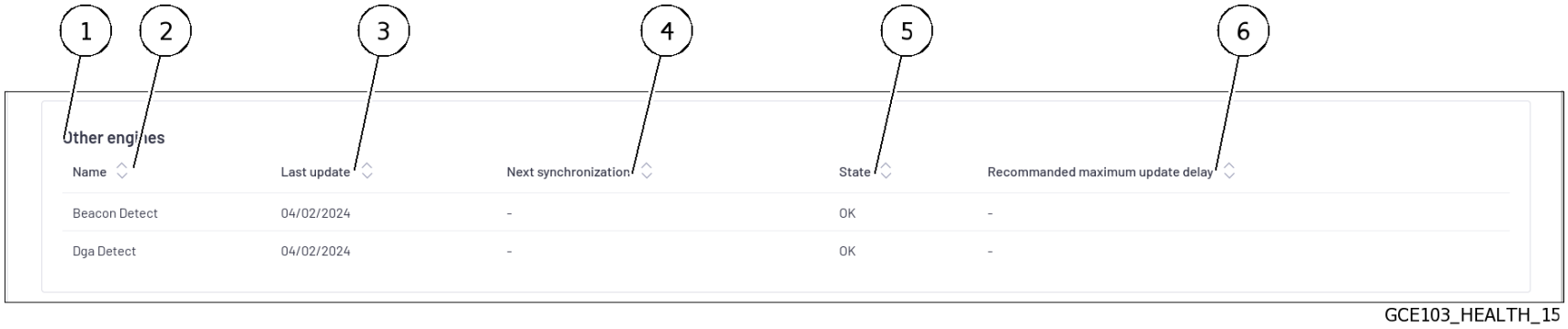


GCE103_HEALTH_14

Item	Name	Description
1	`Malcore engine`	Displays the information about the Malcore engine updates
2	`Name`	Name
3	`Last update`	Last update date
4	`Next synchronisation`	Next synchronisation date
5	`State`	State of the engine update
6	`Recommanded maximum update delay`	Recommanded maximum update delay

5.7.3.2.5.6 The `Other engines` zone

The `Other engines` zone includes:



GCE103_HEALTH_15

Item	Name	Description
1	Other engines	Displays the information about the Other engines updates
2	Name	Name
3	Last update	Last update
4	Next synchronisation	Next synchronisation
5	State	State
6	Recommanded maximum update delay	Recommanded maximum update delay

---

5.7.3.3 `Advanced metrics` screen of the Netdata User Interface (Gstats)

5.7.3.3.1 Introduction

The GCenter retrieves the GCap metrics.
The GCap and GCenter metrics are transmitted via Netdata to the Netdata server present on the GCenter.
The GCenter Gstats interface uses this data and allows to visualize it for an analysis of the state and consumption of the various physical and software components.

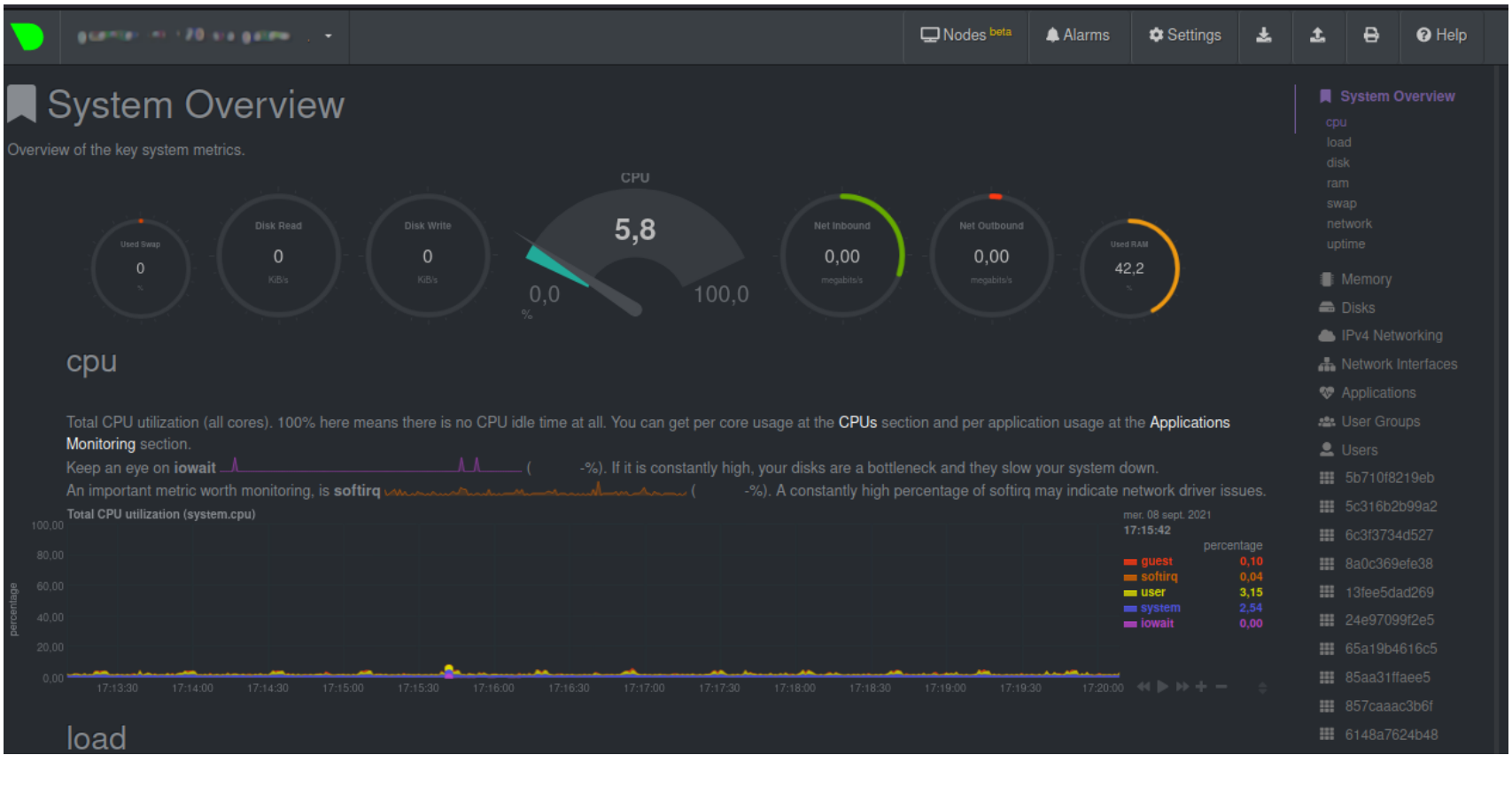
For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.
`.

5.7.3.3.2 Links associated

See the *Overview of the Netdata User Interface (Gstats)*.

5.7.3.3.3 Screen description

After pressing the `Advanced metrics` command on the `Health-Monitoring` menu, the `System Overview`` screen is displayed.



This Gstats interface provides administrators with a large number of metrics on different devices.
It is possible via the menu at the top of the page to select the equipment to be administered such as **GCenter** but also the paired GCaps.

Note:

Alternatively, this data will also be available from Kibana in tabs (or dashboards) accessible from the `Kibana` Dashboards menu.

5.7.3.4 The `System notifications`

5.7.3.4.1 Introduction

The notification system consists of two parts:

- The reduced part: it is present directly in the `Health` menu
- The full part is given in the `System notifications` screen

In both parts, the notification system:

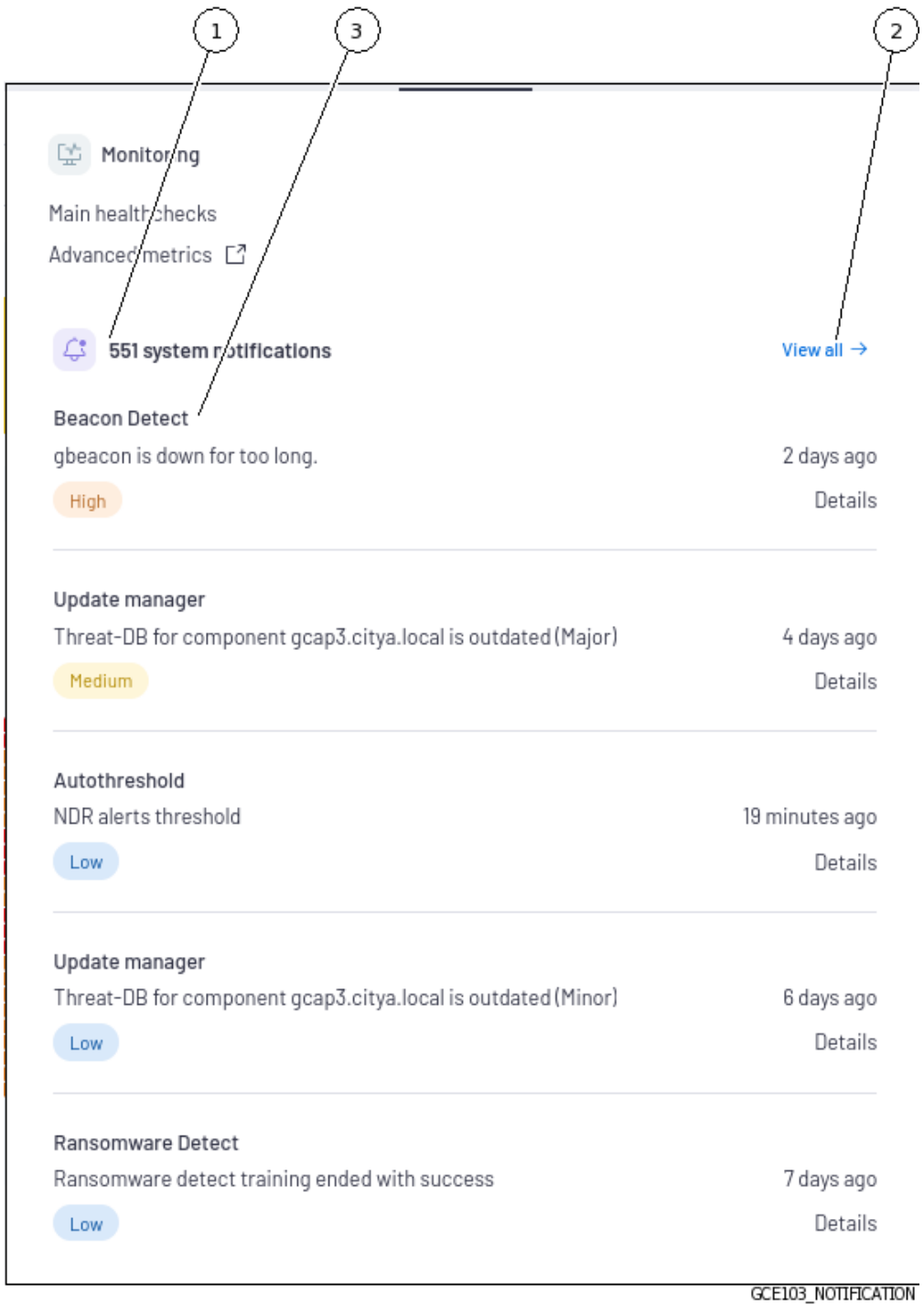
- Reporting alarms defined by a level of risk, among others
- Manages them (sorting, acknowledgement...)

This screen is only accessible to members of the *operator* group.

5.7.3.4.2 Links associated

None

5.7.3.4.3 Part `System notifications` of the `Health` menu



GCE103_NOTIFICATION

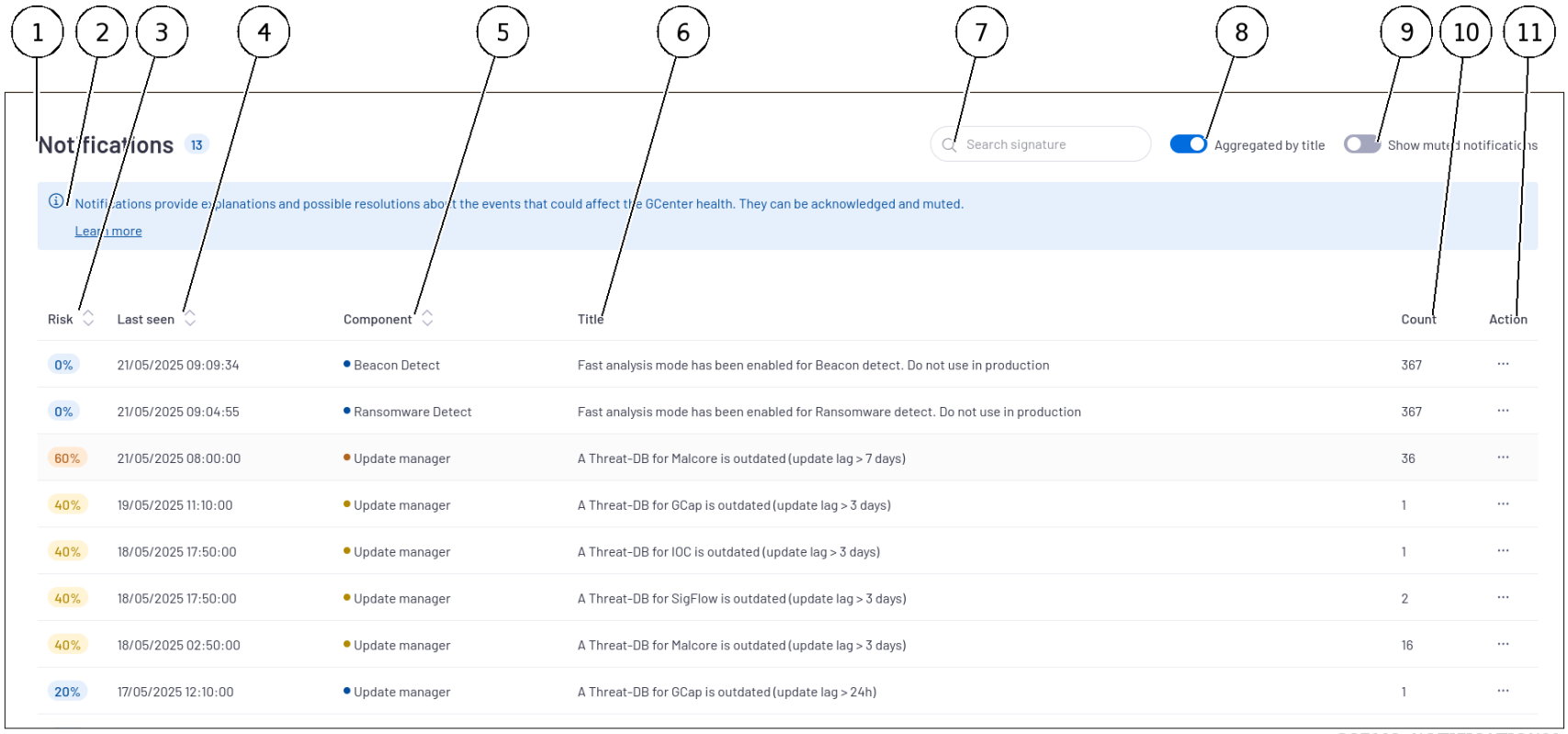
For *administrator* group members, the following message is displayed: `Error 403:Insufficient permissions`.

Item	Description
1	Total number of unpaid notifications
2	Link `View all` : opens the `System notifications` window
3	Last notification received. This notification displays: - A description - A risk level (High, Medium, Low) - The time of appearance - A link `Details` to display the notification detail window

---

5.7.3.4.4 `System notifications` screen

After clicking on the link `View all` in the `Health-Monitoring` menu, the `System notifications` screen is displayed.



GCE103_NOTIFICATION01

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

Item	Name	Function
1	`Notifications`	Number of notifications displayed; depends on aggregated or not (see 8)
2	Brief information on this screen.	The link `Learn more` opens the documentation integrated on the corresponding page.
3	`Risk`	Risk level of the notification
4	`Last seen`	Date and time of last appearance
5	`Component`	Notification issuer component
6	`Title`	Title of the notification
7	Search field	Search for text in categories
8	`Aggregated by name` selector	if used, aggregates the notifications. In this mode, the information fields are different (`Count` field present)
8	`Count`	Number of same notifications (displayed only in `Aggregated by name` mode)
9	`Muted` selector	If used, displays the muted notifications
11	`Action`	Displays the possible actions: - `Unmute` - `Mute related notifications` - `Acknowledge related notifications`

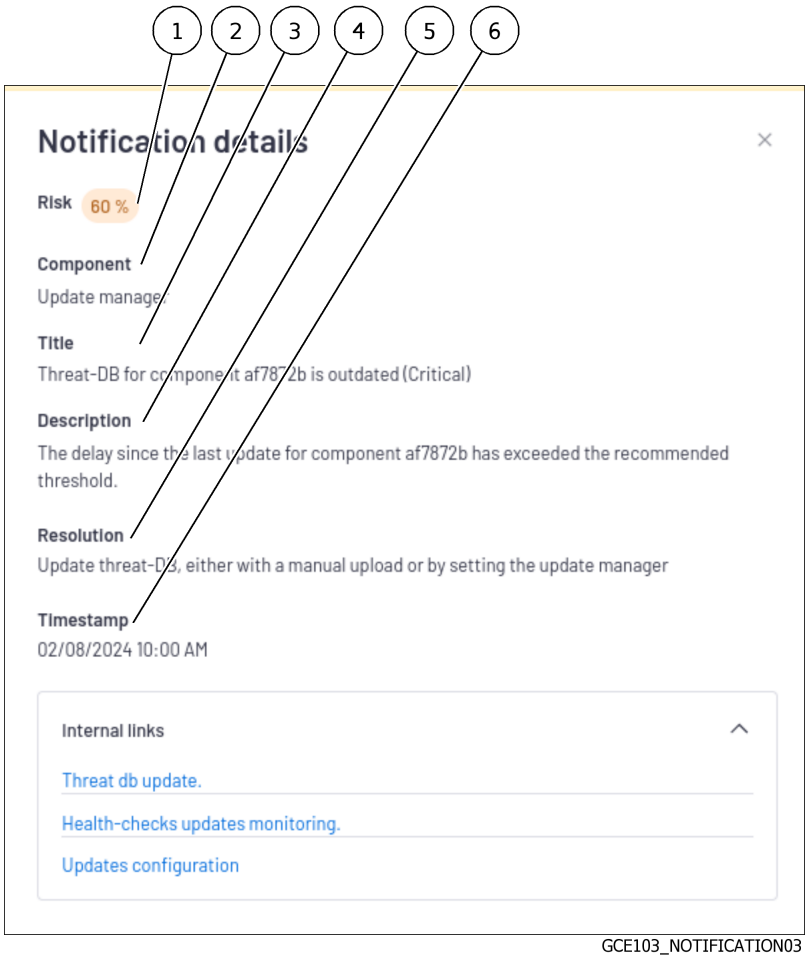
Note:

By clicking on the notification, the `Notification details` window is detailed.

5.7.3.4.5 `Notification details` window

The `Notification details` window is displayed:

- by clicking on the `Détails` link in the `System notifications` section of the `Health` menu
- either by clicking on the notification in the `System notifications` screen



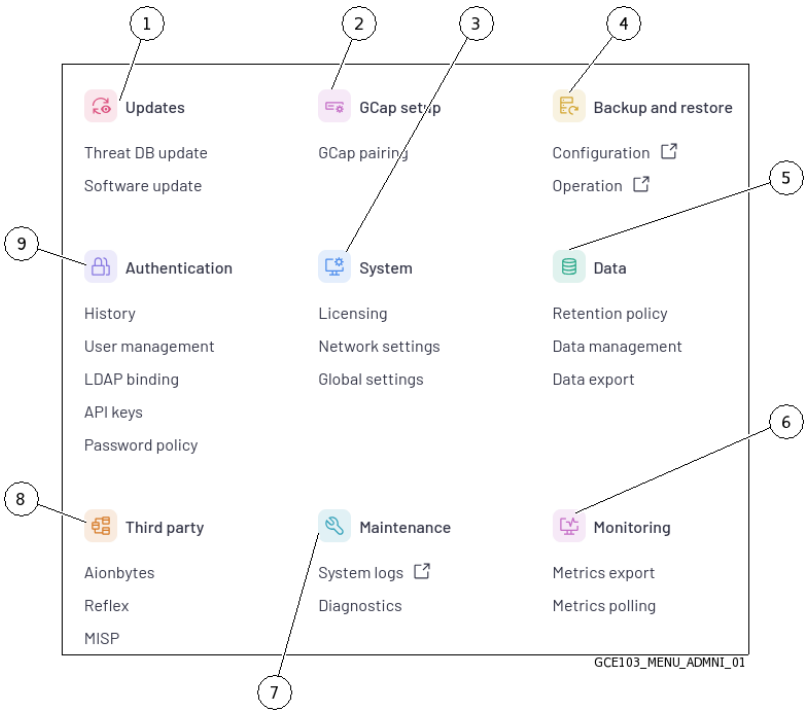
GCE103_NOTIFICATION03

Item	Name	Function
1	Risk	Risk level of the notification
2	`Component`	Notification issuer component
3	`Title`	Title of the notification
4	`Description`	Reason why the notification was created
5	`Résolution`	Advice on solving the problem
6	`Timestamp`	Date and time of notification

5.7.4 `Administration` menu

5.7.4.1 Overview of the `Administration` menu

The `Administration` menu consists of:



Item	Heading	Command	Description
1	`Updates`	`Threat-DB update` `Software update`	See *'Threat DB update' screen* See *'Software update' screen*
2	`Gcap setup`	`Gcap Pairing`	See *'GCaps Pairing' screen*

3	`System`	`Licensing`
		`Network setting`
		`Global settings`
			See *'License' screen*
			See *'Network settings' screen*
			See *'Global settings' screen*

4	`Backup and restore`	`Configuration` `Operation`	See *'Configuration' screen* See *'Backup operations' screen*

5	`Data`	`Retention policy`
		`Data management`
		`Log export`
			See *'Retention policy' screen*
			See *'Data Management' screen*
			See *'Data export' screen*

6	`Monitoring`	`Metrics export` `Metrics polling`	See *'Netdata Export Configuration' screen* See *'Netdata polling' screen*
7	`Maintenance`	`System logs` `Diagnostics`	See *'System logs' screen* See *'Diagnostics' screen*
8	`Third party`	`MISP`	See *'MISP settings' screen*

9	`Authentication`	`History`
		`Users management`
		`LDAP binding`
		`API keys`
		`Password policy`
			See *'History' screen*
			See *'Users management' screen*
			See *'LDAP binding' screen*
			See *'API keys' screen*
			See *'Password policy' screen*

5.7.4.2 `Threat DB update` screen

5.7.4.2.1 Introduction

The `Threat DB update` screen is used:

- To update manually signatures and/or anti-viral engines (update)
- To configure automatic update of signatures and/or anti-viral engines (update)
- To view package installation history and status

The packages that can be downloaded through this interface are:

- beacon.gwp package: this package contains beacon update
- cti.gwp package: this package contains update of the database of Indicators Of Compromise
- dga.gwp package: this package contains update to the DGA detect engine
- sigflow.gwp package: this package contains the sigflow engine update and the rules base updates
- malcore directory: this directory contains the updates of Malcore engines and their antivirus databases
- full package (full.gwp): this package is the sum of the previous packages

Note:

The malcore directory contains:

- One package for each antivirus engine named after the hash of the engine to which it relates, same hash as what is presented in malcore healthcheck
- A package of utilities named "common_utilities.gwp"

Important:

In this case, select a GWP package file, only from those of the solution's engines.
Hotfix and upgrade packages will not work in this interface.

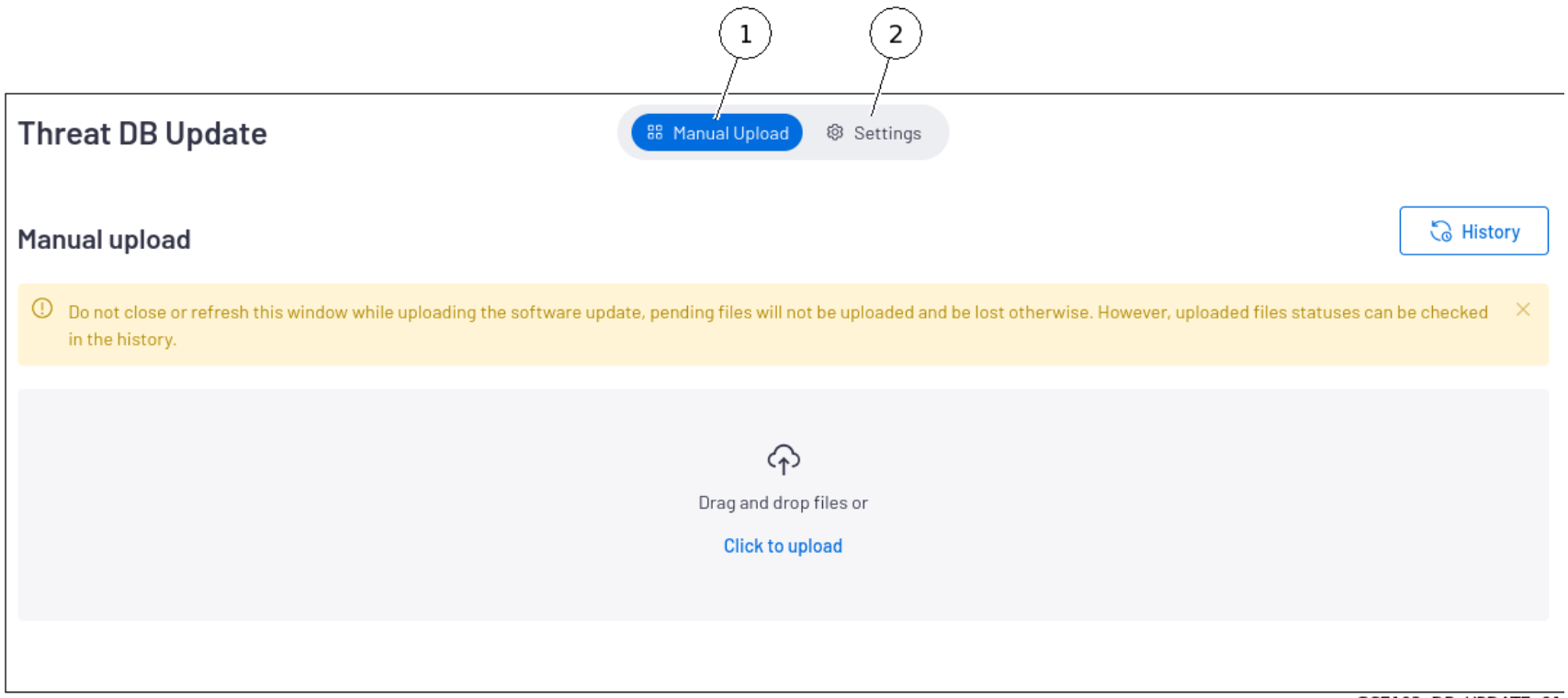
This screen is only accessible to members of the *administrator* group.

5.7.4.2.2 Links associated

See the *Update presentation*.
The update packages are available in the https://update.gatewatcher.com/update/.
For manual installation, see the *Installing an update manually* procedure.
For automatic update configuring, see the *Configuring automatic update of signatures and/or anti-viral engines* procedure.

5.7.4.2.3 Screen description

After pressing the `Threat DB update` command on the `Administration-Updates` menu, the `Threat DB update` screen is displayed.



GCE103_DB_UPDATE_01

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

The `Threat DB update` screen contains the following parts:

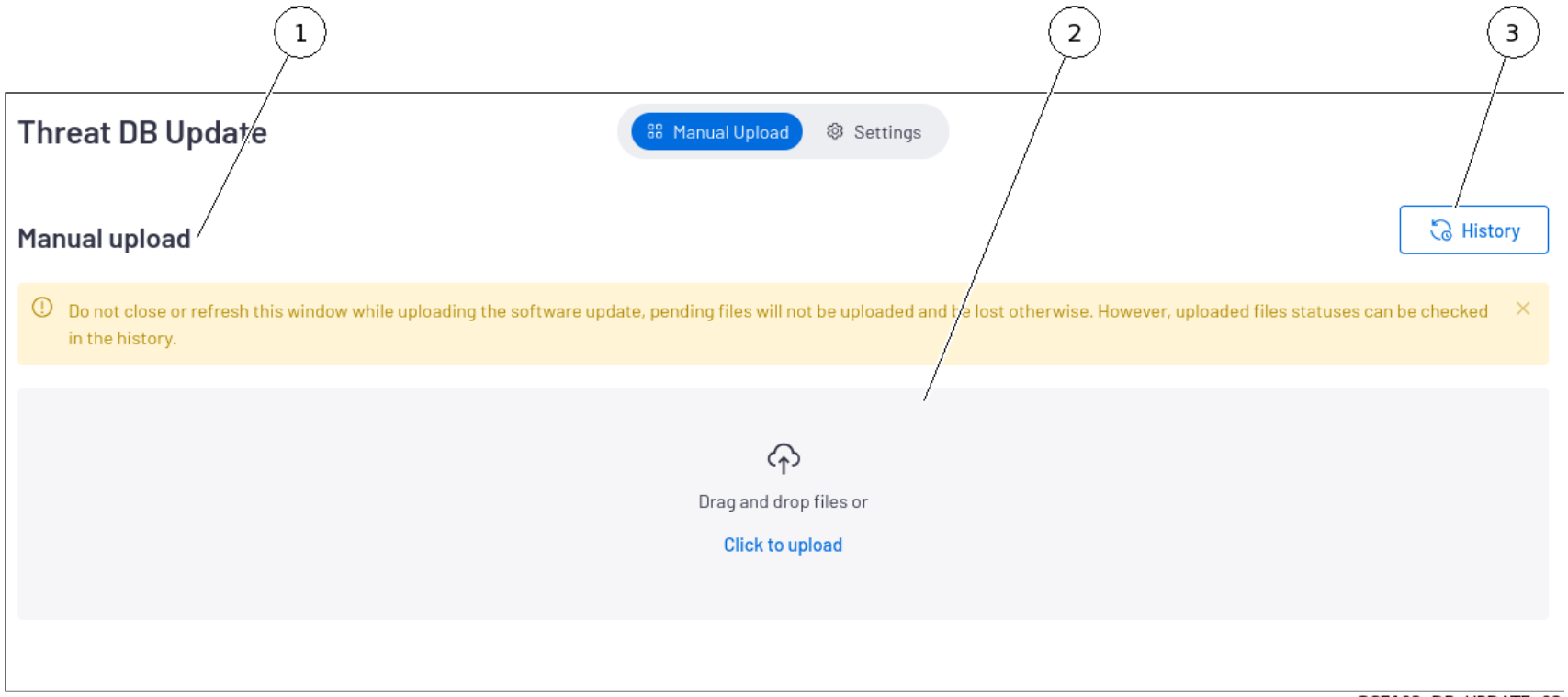
Item	Area	Function
1	`Manual Upload`	Area to upload a manual update
2	`Settings`	This area allows: - To set the schedule and setting of the automatic update - To test the connection - To active the automatic update

Note:

The cti.gwp package is updated hourly on update.gatewatcher.com
The other packages are updated every day.
It is not possible to download the full.gwp file in automatic mode.

5.7.4.2.3.1 Screen `Manual Upload` of the `Threat DB update` screen

This screen includes the following:



GCE103_DB_UPDATE_02

Item	Name	Function
1	`Manual Upload`	Part that allows manual update
2	`Drag and drop files or Click to upload`	Drop a package Open a window to select package to download
3	`History`	View download history

Important:

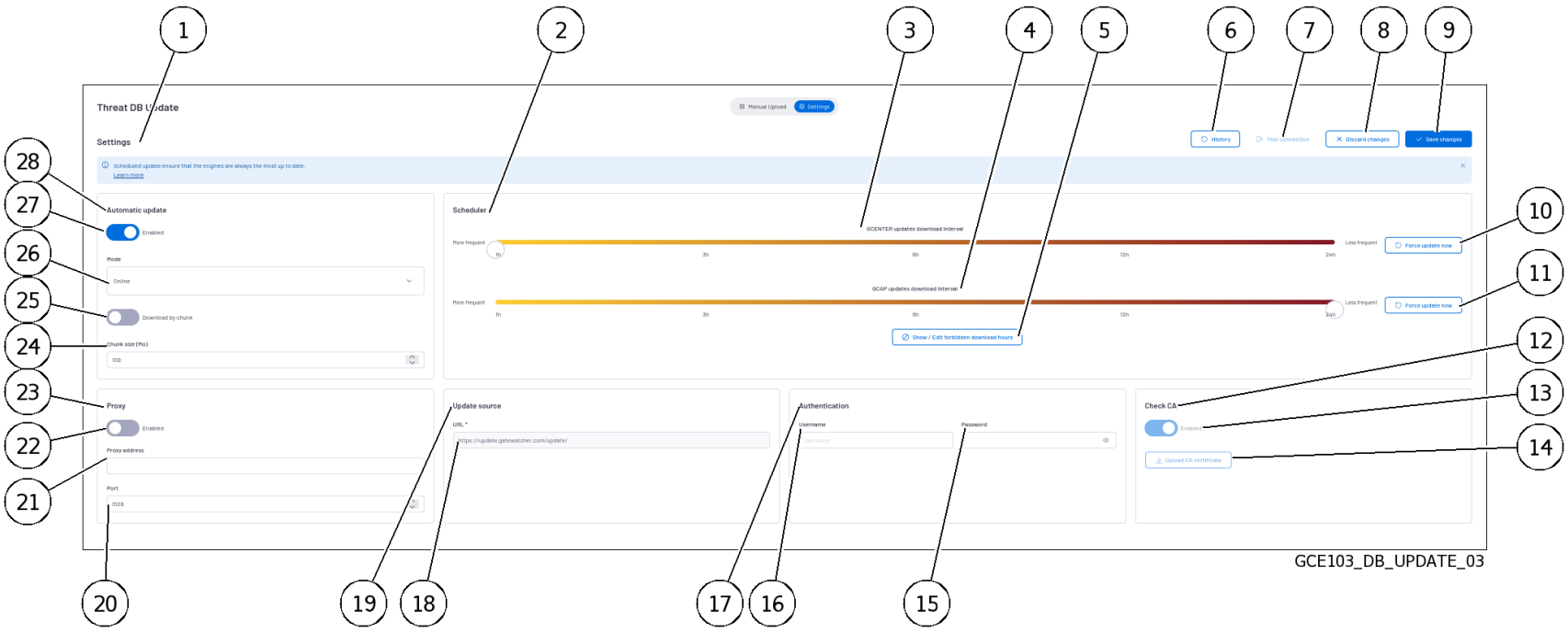
In this case, select a GWP package file, only from those of the solution's engines.
Hotfix and upgrade packages will not run in this interface.

5.7.4.2.3.2 Screen `Settings` of the `Threat DB update` screen

The options are different according to the automatic type mode:

- **Online** mode enables the automatic updates (from Gatewatcher servers)
- **Local** mode enables the updates to be made from a local repository

This screen includes the following:



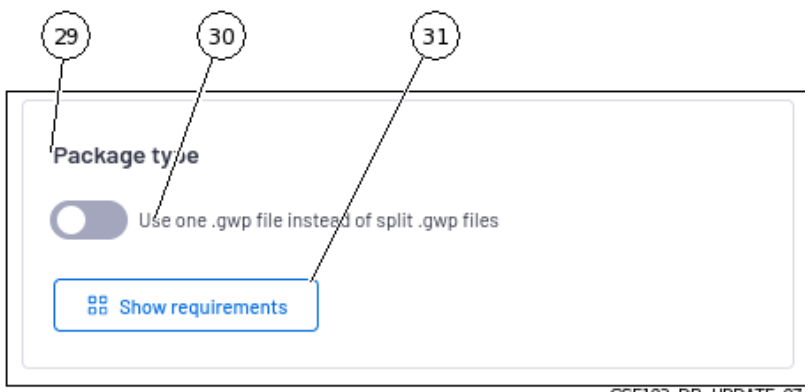
Item	Name	Function
1	`Settings` area	Area to set the configuration and testing of the automatic update
28	`Automatic update` area	Area to enable auto Update Feature
27	• `Enabled` selector	• Enables / disables the automatic update
26	• `Mode`	• Selects the type of update mode (local or Online) : here Online
25	• `Download by chunk` selector	• Enables the download packages in chunks
24	• `Chunk size (Mo)`	• Size of the pieces
23	• `Proxy (Mo)` area	• Area to set the proxy listed below
22	• `Enabled` selector	• Enables / disables the proxy feature
21	• `Proxy address`	• Enter the proxy server address as an IP address or FQDN in the `Proxy address` field
20	• `Port`	• Enter the Proxy Listening Port (1-65535)
2	`Scheduler` area	Area to set configuration of the planning appliances listed below
3	• `GCENTER updates download interval`	• Update time interval scheduling slider for the GCenter
10	• `Force update now` button	• Triggers immediate update for the GCenter
4	• `GCAP updates download interval`	• Update time interval planning slider for the GCap
11	• `Force update now` button	• Triggers immediate update for the GCap
5	• `Show / Edit forbidden download hours` button	• Displays or changes schedule of prohibited hours
6	`History` button	Displays installation history
7	`Test connection` button	Tests connection with or changes schedule of prohibited hours
8	`Discard changes` button	Cancels common changes
9	`Save changes` button	Saves changes

continues on next page

Table 38 – continued from previous page

Item	Name	Function
19	`Update source` area	Area to define the update source
18	• `URL`	• Viewing area of the URL made up: - Of the selected protocol with the cursor `SSL enabled` - Of the domain name/path defined in the field `Domain*`
17	`Authentication` area	Inputs authentication for access to package update site
16	• `Username`	• Access account name
15	• `Password`	• Access account password
12	`Check CA` area	Customer certificate verification area by CA: active only if Online mode (26) is selected
13	• `Enabled` selector	• Enables / disables this check
14	• `Upload CA file` button	• Downloads the certificate file

At the bottom of the screen, there is the following category:



Item	Name	Function
29	`Package type` area	Area to choose the package type
30	`Use one .gwp file instead of split .gwp files` selector	• If enabled, the file downloaded is the full.gwp file If disabled, the files downloaded are the engine .gwp files (one file per detection engines and one per Malcore engines)
31	`Show requirements` button	Views the files which will be downloaded

5.7.4.3 `Software update` screen

5.7.4.3.1 Introduction

The `Software update` screen enables to:

- Install upgrade
- Install patche (or hotfix)
- View installation history and status

Important:

In this case, a GWP package file must be selected and only those of the hotfix and upgrade type.
Update type packages will not work in this interface.

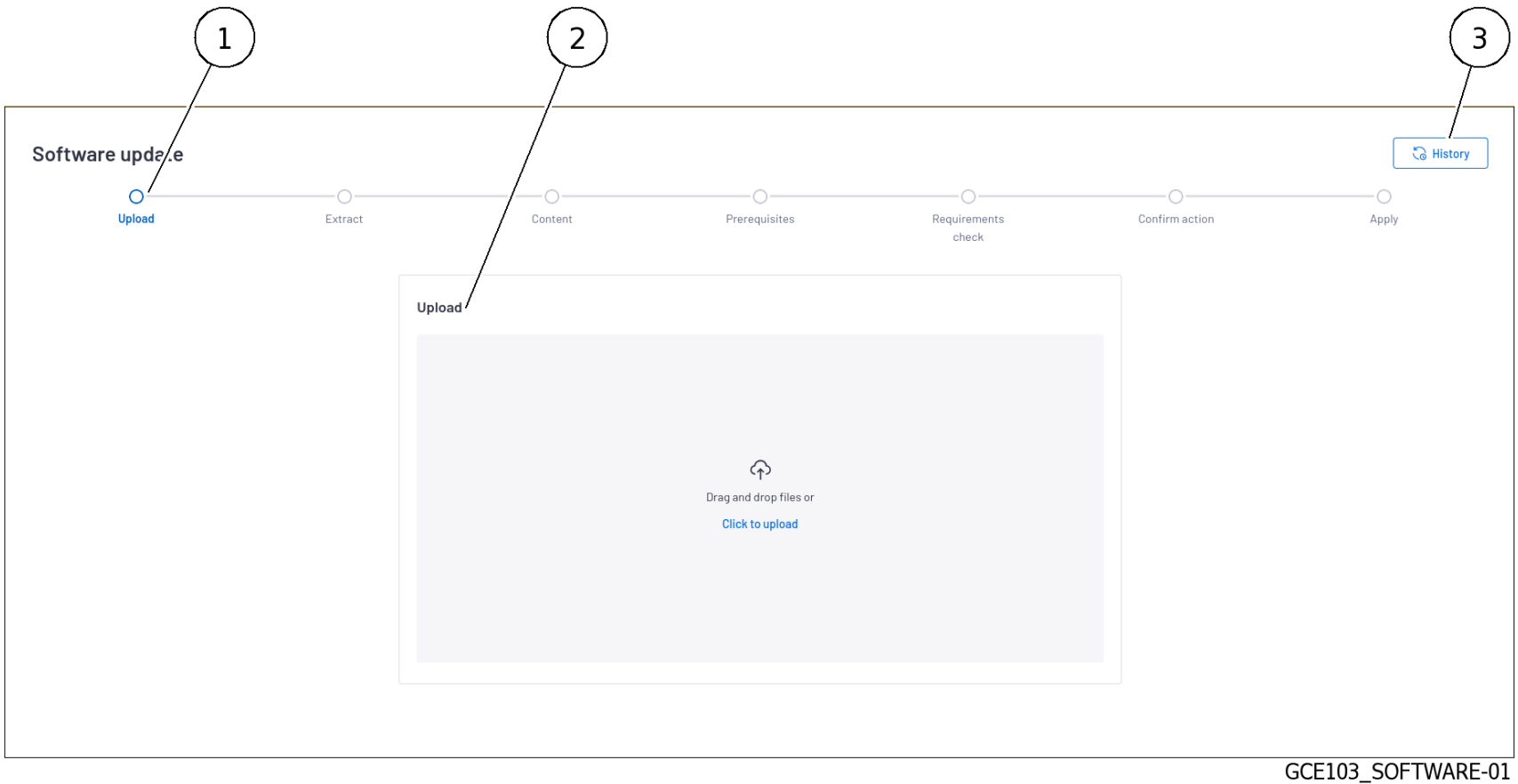
This screen is only accessible to members of the *administrator* group.

5.7.4.3.2 Links associated

See the *Upgrade presentation* or the *Hotfix presentation*.
The hotfix packages are available on https://update.gatewatcher.com/hotfix/.
For hotfix installation, see the *Installing a hotfix* procedure.
The upgrade packages are available on https://update.gatewatcher.com/upgrade/.
For manual upgrade installation, see the *Installing of an upgrade* procedure.

5.7.4.3.3 Screen description

After pressing the `Software update` command from the `Administration-Updates` menu, the following screen is displayed.



GCE103_SOFTWARE-01

Item	Name	Function
1	Installation Steps Viewer	Indicates the different stages of the installation and the current step The list of steps are: - `Upload`: load the package from the local pc to the GCenter - `Extract`: unwrap the gwp file and move the gwp content to the target folder - `Content`: check the files content - `Prerequisites`: check the patcher requirements - `Requirements check`: execute the requirements check - `Confirm action`: confirm the installation action - `Apply`: apply the installation action
2	`Upload` zone	Central window that evolves according to the current stage In the example, the Upload step is the current step. here then , either it is possible to click and drop the package or click in the window to display a download window.
3	`History` button	Displays installation history

5.7.4.4 `History` screen

5.7.4.4.1 Introduction

The History feature manages:

- The history of all authentications
- The history of all user creations or deletions
- The history of all user permissions

To do so, the `History` screen enables to:

- Activate the event history
- Configure the amount of event history
- View event history

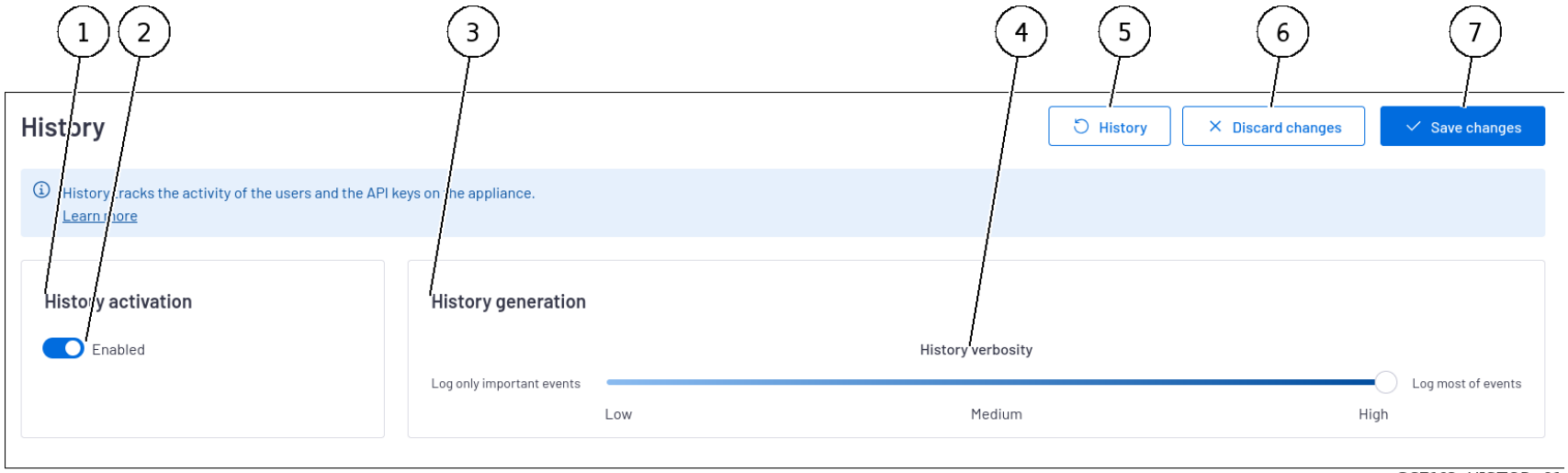
This screen is only accessible to members of the *administrator* group.

5.7.4.4.2 Links associated

For implementation, see the *Viewing the authentication history*.

5.7.4.4.3 Screen description

After pressing the `History` command on the `Administration-Authentication` menu, the `History` screen is displayed.



GCE103_HISTOR_01

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

Item	Name	Function
1	`History activation`	Area to active the historisation
2	`Enabled` selector	Enables the historisation function
3	`History generation`	Area to configure the history generation
4	`History verbosity` selector	Defines the quantity of historic events
5	`History` button	Explores history events in Kibana
6	`Discard changes` button	Cancels current changes
7	`Save changes` button	Saves current changes

5.7.4.5 `Users management` screen

5.7.4.5.1 Introduction

The `Users management` screen is used:

- To create and manage the accounts of locally defined GCenter users
- To display the LDAP accounts which are been used to open a session on the GCenter

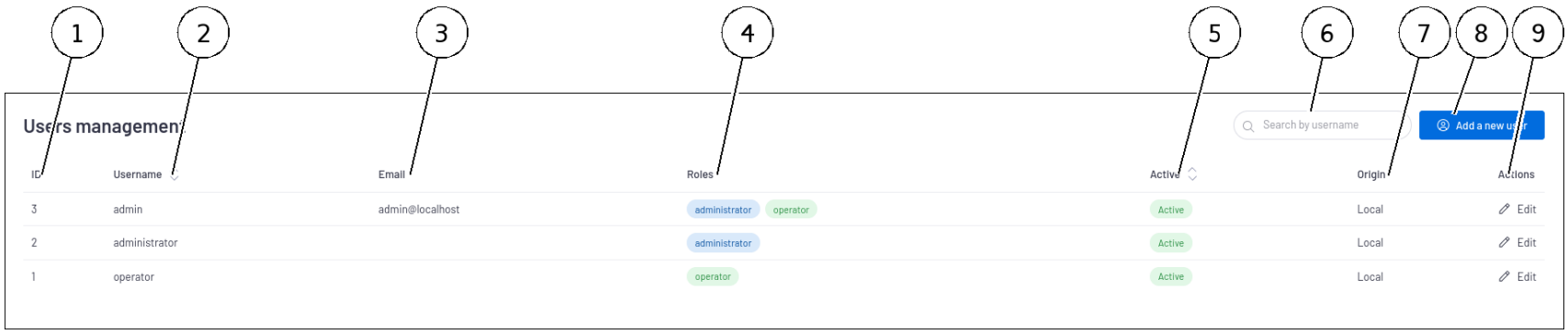
This screen is only accessible to members of the *administrator* group.

5.7.4.5.2 Links associated

For information, see the paragraph *Web interface accounts and their management*.
For implementation, see the *Creating local user* procedure.
For implementation, see the *Changing some of a local user's information* procedure.

5.7.4.5.3 Screen description

After pressing the `Users management` command on the `Administration-Authentication` menu, the `Users management` screen is displayed.



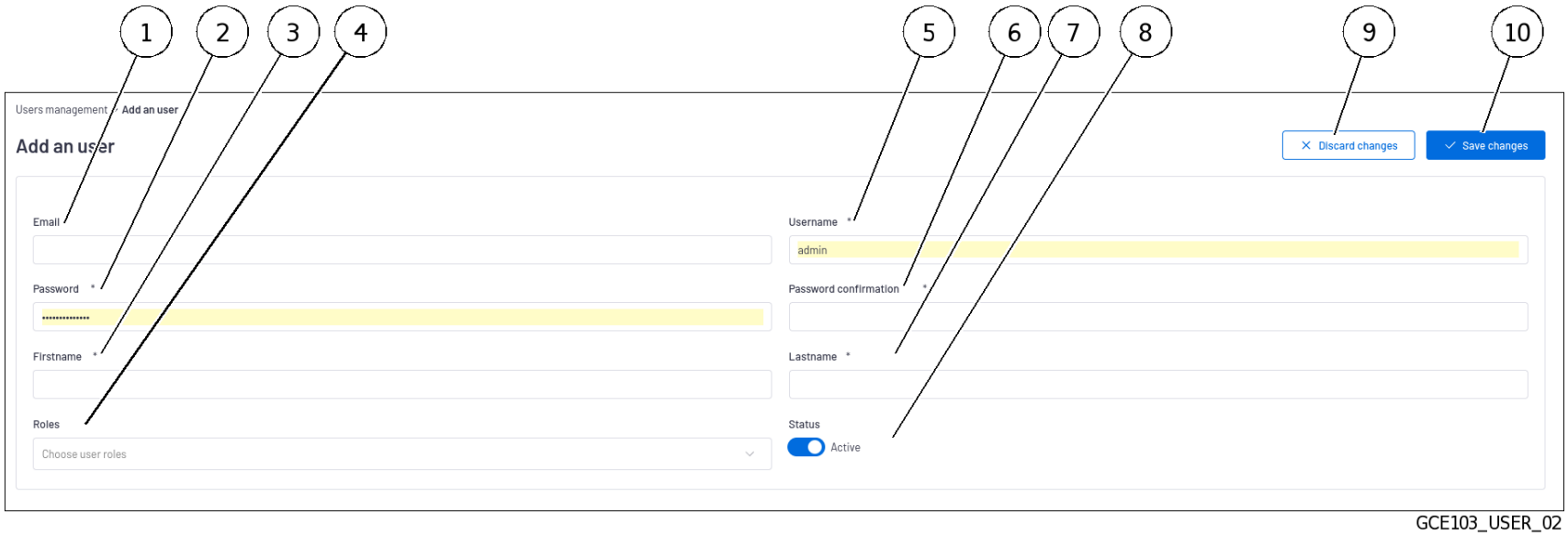
GCE103_USER_01

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

Item	Name	Function
1	`ID`	Unique account number
2	`Username`	Full name of new user Can only contain letters, numbers and characters [@/. /+/-/-/_.]
3	`Email`	Email address Keep the contact email of the user
4	`Roles`	Defines the roles granted to the account Possible roles are Operator and/or Administrator
5	`Active` Selector	Activates or deactivates the account
6	Search field	Find an account
7	`Origin`	Local indicates this account was created directly on the GCenter
8	`Add a new user` button	Creates a new user This is done via the `Add an user` screen described below.
9	`Actions`	Edits the selected account This is done via the `Edit` screen described below.

5.7.4.5.4 `Add an user` screen

The `Add an user` screen enables to enter a new user's information and includes the following:



GCE103_USER_02

Item	Name	Function	Mandatory or not field
1	`Email`	Email address Keeps the user's contact email	Optional field but the format is checked
2	`Password`	Password: this password must correspond to password policy	Mandatory field
3	`Firstname`	First name of the user	Mandatory field
4	`Roles`	Defines the roles granted to the account The possible roles are Operator and/or Administrator	Mandatory field
5	`Username`	Full name of new user. Can only contain letters, numbers and characters [@/. /+/-/-/_.]	Mandatory field
6	`Password confirmation`	Password identical to the `Password` field	Mandatory field
7	`Lastname`	Name of the user	Mandatory field
8	`Status` selector	Activates or deactivates the account	Mandatory field
9	`Discard changes` button	Cancels the current changes	NA
10	`Save changes` button	Saves current changes	NA

5.7.4.5.5 `Edit` screen

The `Edit` screen enables to view the information of an existing user and delete it if necessary.

GCE103_USER_03

Item	Name	Function
1	`User information`	This area displays the information of the selected account
2	`Id`	• Unique account number
3	`Username`	• User's full name. Can only contain letters, numbers and characters [@/. /+/-/-/_.] The username has to be unique in the list
4	`First name`	• First name of user
5	`Last name`	• User name
6	`Date joined`	• Account creation date
7	`Last login`	• Date of last account login
8	`User configuration`	This area displays the information of the selected account and allows you to modify each of these fields
9	`Email`	• Field indicating the email address
10	`Firstname`	• User first name
11	`Roles`	• Defines the roles granted to the account. The possible roles are Operator and/or Administrator.
12	`Status` selector	• Activates or deactivates the account
13	`Lastname`	• User name
14	`Delete user` button	Deletes current user
15	`Discard changes` button	Cancels current changes
16	`Save changes` button	Saves current changes

5.7.4.6 `LDAP binding` screen

5.7.4.6.1 Introduction

The `LDAP binding` screen enables the association between the GCenter and the LDAP server.

This screen is only accessible to members of the *administrator* group.

5.7.4.6.2 Links associated

For information about the accounts and the LDAP integration, see the *Web interface accounts and their management*.
For the viewing of the LDAP interconnection status, refer to *Displaying of the connection status between the GCenter and the LDAP server*.
For the implementation of the LDAP interconnection activation (LDAP authentication settings zone), see the procedure *Enabling the connection between the GCenter and the LDAP server*.
For the implementation of the LDAP settings, see the procedure *Configuring the connection between the GCenter and the LDAP server*.

5.7.4.6.3 Screen description

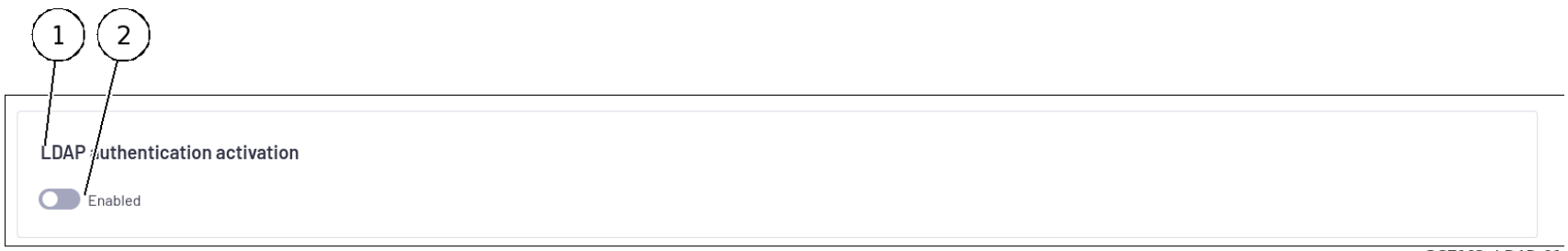
After pressing the `LDAP blinding` command on the `Administration-Authentication` menu, the `LDAP Configuration` screen is displayed.

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page. `.

Zone	Description	For more information see
`LDAP authentication activation`	Remote authentication server activation area	*`LDAP authentication activation` area*
`LDAP server binding settings`	Remote authentication server login information input area	*`LDAP server binding settings` area*
`LDAP users and groups mapping`	User and group mapping area between the GCenter and the remote authentication server	*`LDAP users and groups mapping` area*
`LDAP advanced settings`	Advanced configuration area connecting to a remote authentication server	*`LDAP advanced settings` area*

5.7.4.6.3.1 `LDAP authentication activation` area

This area enables the connection to a remote authentication server.



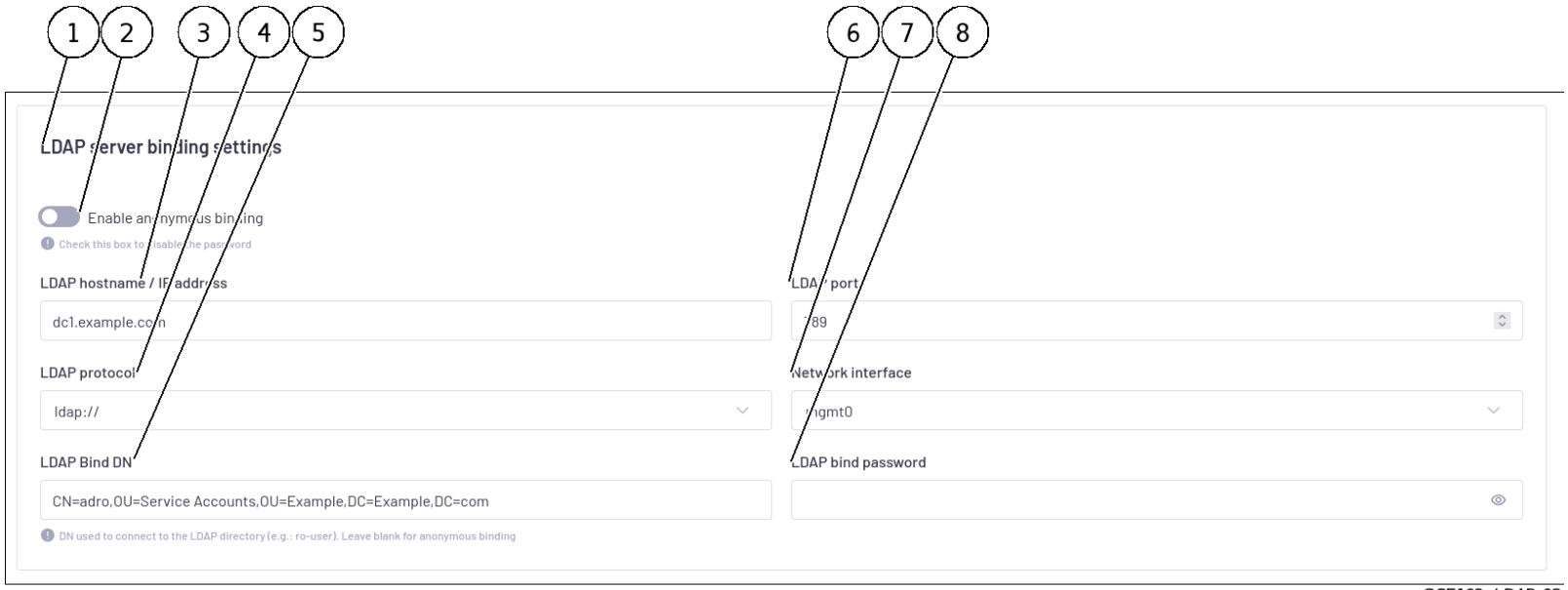
GCE103_LDAP-01

Item	Name	Function
1	`LDAP authentication activation`	Login Activation Area
2	`Enabled` selector	Enables authentication by a remote LDAP server

---

5.7.4.6.3.2 `LDAP server binding settings` area

This area enables the input of login information to a remote authentication server.

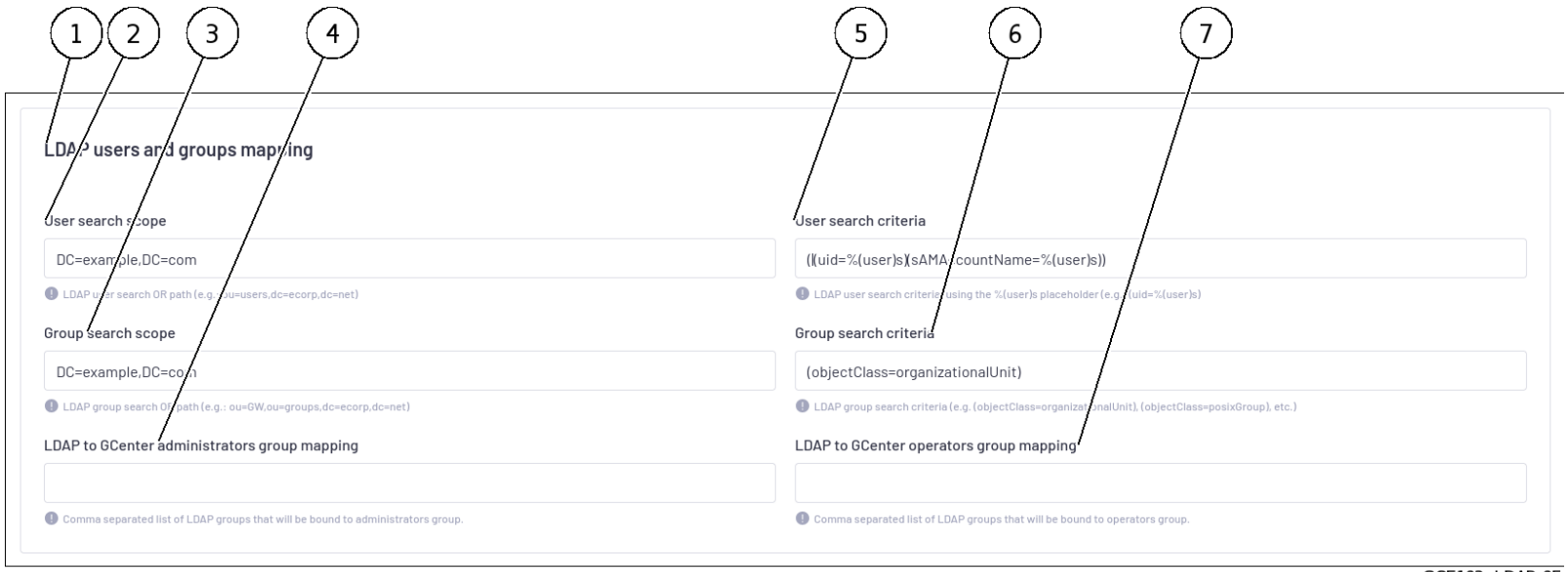


GCE103_LDAP-02

Item	Name	Function
1	`LDAP server binding settings`	Login information input area
2	`Enable anonymous binding` selector	• Enables not having to enter the login password
3	`LDAP hostname / IP address`	• Specifies the IP address or name of the remote server
4	`LDAP protocol`	• Chooses the protocol used for the connection ldap:// ou ldaps://
5	`LDAP binding DN`	• Specifies the user name for connecting to the remote server DN used to connect to the LDAP directory (e.g.: ro-user). Leave blank for anonymous binding
6	`LDAP port`	• Specifies the port of the remote server 389 for ldap or 636 for ldaps for example
7	`Network interface`	• Chooses the GCenter interface through which to communicate with the remote server mgmt0 by default
8	`LDAP binding password`	• Specifies the user's password for connecting to the remote server

5.7.4.6.3.3 `LDAP users and groups mapping` area

This area enables to specify the mapping of users and groups between the GCenter and the remote authentication server.

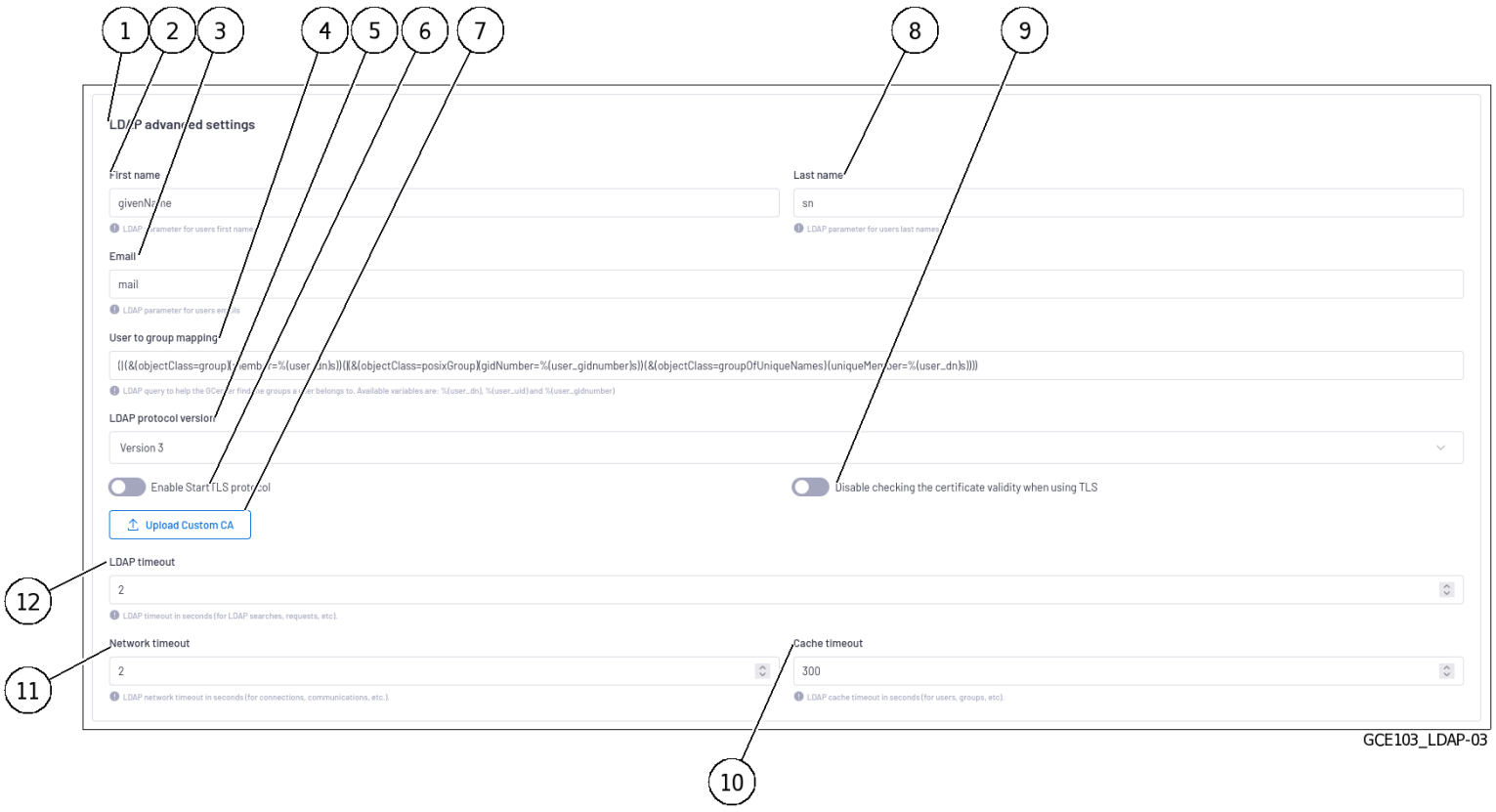


GCE103_LDAP-05

Item	Name	Function
1	`LDAP users and groups mapping`	Area to specify the mapping of users and groups between the GCenter and the remote authentication server
2	`User search scope`	• Specifies the search for users in the remote directory by default: DC=example, DC=com
3	`Group search scope`	• Specifies the search for groups in the remote directory by default: DC=example, DC=com
4	`LDAP to GCenter administrators group mapping`	• Specifies which groups will have the "administrator" role Groups of administrators for example
5	`User search criteria`	• Specifies the search criteria for users in the remote directory by default: *(|(uid=%(user)s) (sAMAccountName=%(user)s))*
6	`Group search criteria`	• [Specifies the search criteria for groups in the remote directory | by default: | (objectClass=organizationalUnit)
7	`LDAP to GCenter operators group mapping`	• Specifies which groups will have the "operator" role groups of analysts for example

5.7.4.6.3.4 `LDAP advanced settings` area

This area enables advanced configuration of the connection to a remote authentication server.



Item	Name	Function
1	`LDAP advanced settings`	Area of advanced configuration of the connection to a remote authentication server
2	`First name`	• Specifies the LDAP parameter for the first name of the users
3	`Email`	• Specifies the LDAP setting for the user's email
4	`User to group mapping`	• Enables entering an LDAP query to help the GCenter find the groups a user belongs to
5	`LDAP protocol version`	• Chooses the LDAP version of the remote server
6	`Enable StartTLS protocol` selector	• Enables or disables the StartTLS protocol
7	`Upload Custom CA` button	• Loads a certificate for LDAP use
8	`Last name`	• Specifies the LDAP parameter for the last name of the users
9	`Disable checking the certificate validity when using TLS` selector	• Enables or disables certificate validity checking (LDAPS)
10	`Cache timeout`	• Specifies the waiting time for LDAP users and groups
11	`Network timeout`	• Specifies the waiting time at the LDAP communications network level (by default: 2)
12	`LDAP timeout`	• Specifies the waiting time for LDAP queries (by default: 2)

5.7.4.7 `API keys` screen

5.7.4.7.1 Introduction

This screen manages API access tokens.

This screen is only accessible to members of the *administrator* group.

5.7.4.7.2 Links associated

For the implementation, see the *Managing an API access token*.

5.7.4.7.3 Screen description

After pressing the `API keys` command on the `Administration-Authentication` menu, the `API keys` screen is displayed.

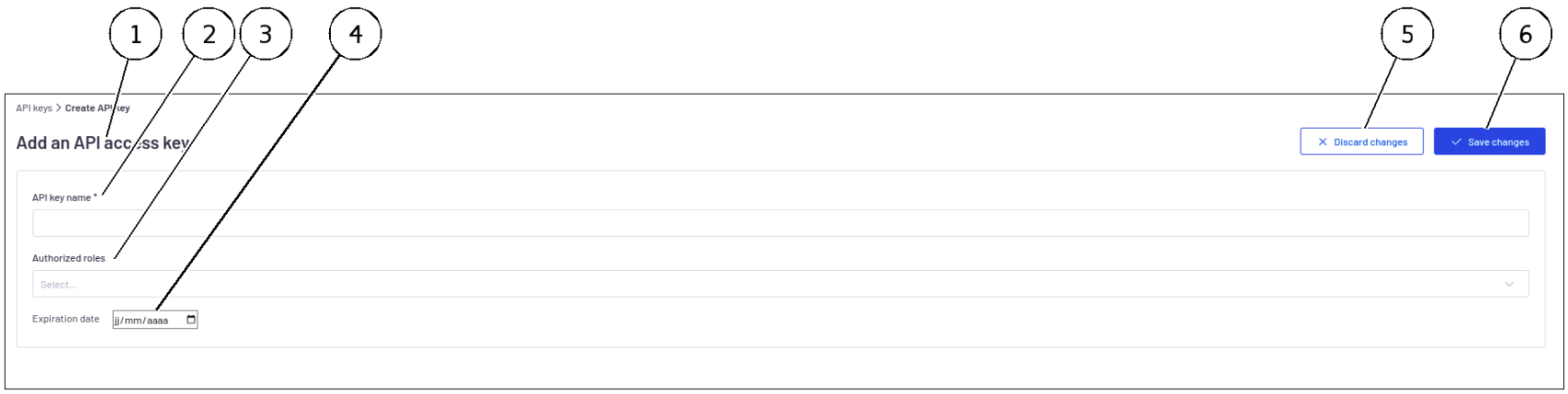
GCE103_API-1

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

Item	Name	Function
1	`API keys`	API key creation and management window
2	`3`	• Number of present API keys
3	`API keys provide authentication for programmatic interaction with the GCenter..`	• Short information about this screen. The Learn more link opens the embedded documentation on the corresponding page
4	`API Key ID``	• API key ID number
5	`API Key name`	• Name of the API key entered during the key creation
6	`Creation date`	• Creation date of the API key
7	`Expiration date`	• Expiration date of the API key
8	`Last used`	• Date of last use
9	`Creator`	• Account name which has created the APY key
10	`Role`	• Roles associated to the API keys (Operator and / or Administrator)
11	Search for a key name	• Enables entering a name to be searched
12	Search for a role	• Enables to select a role to filter the API keys
13	`Status`	• Api key status (active..)
14	`Add an API key` button	• Displays the `Add an API access key` window
15	`Action`	• Displays the possible action : here delete the current api key

5.7.4.7.4 `Add an API access key` screen

After pressing the `Add an API key` button of the `API keys` window, the `Add an API access key` screen is displayed.



GCE103_API-2

Item	Name	Function
1	`Add an API access key`	Fenêtre de création d'un nouvelle clé API
2	`API key name`	• Field to enter the name of the new API key
3	`Authorized roles`	• Field to select one or several roles associated to this API key
4	`Expiration date`	• Definition of the expiration date of the APY key
5	`Discard changes` button	• Cancels current changes
6	`Save changes` button	• Saves current changes

5.7.4.8 `Password policy` screen

5.7.4.8.1 Introduction

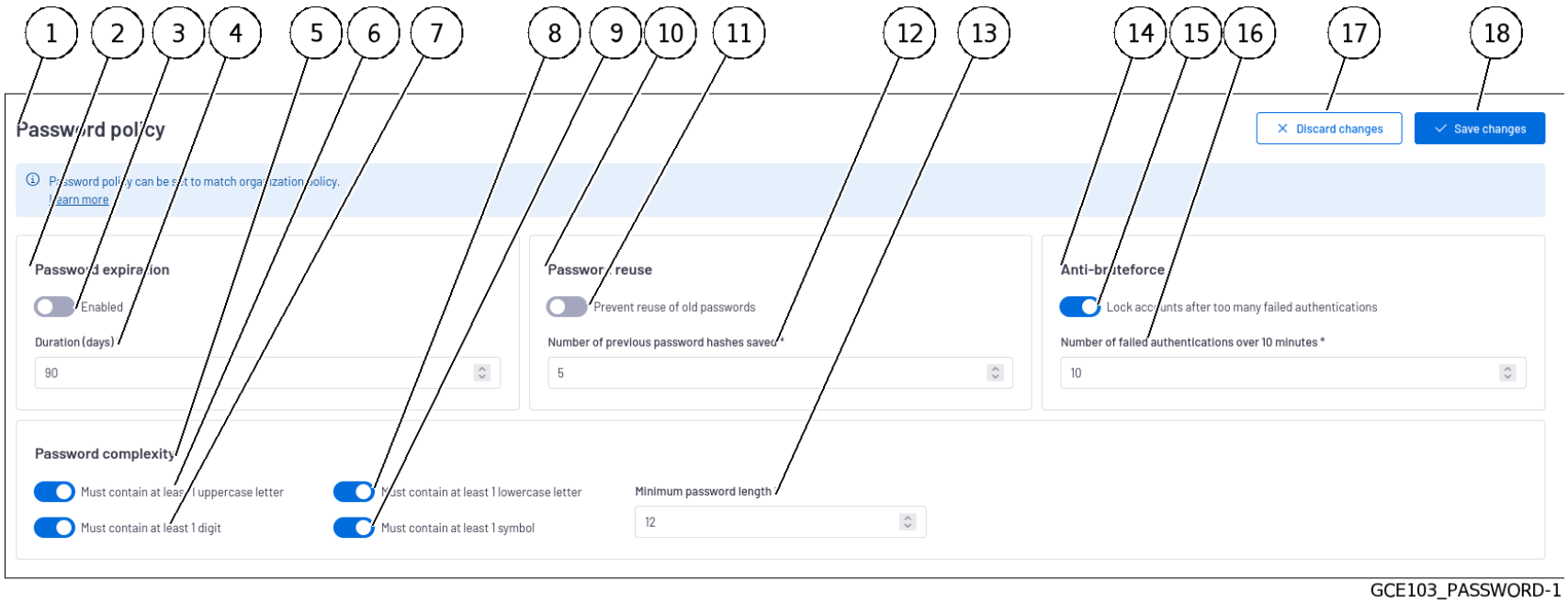
This screen is used to manage the password policy.
This screen is only accessible to members of the *administrator* group.

5.7.4.8.2 Links associated

For the implementation, see the procedure *Managing the password policy*.

5.7.4.8.3 Screen description

After pressing the `Password policy` command on the `Administration-Authentication` menu, the `Password Policy` screen is displayed.



GCE103_PASSWORD-1

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

Item	Name	Description
1	`Password Policy`	Screen to define the password policy
2	`Password expiration` Zone	Activates the password expiration
3	`Enabled` selector	• Activates the password expiration
4	`Duration (days)`	• Value of the password validity duration
5	`Password complexity` Zone	Defines the password
6	`Must contain at least 1 uppercase letter`	• At least one upper case letter
7	`Must contain at least 1 digit`	• At least one digit (0 to 9)
8	`Must contain at least 1 lowercase letter`	• At least one lower case letter
9	`Must contain at least 1 symbol`	• At least one symbol (i.e. neither a number nor a letter)
10	`Password reuse` Zone	Defines the password reuse
11	`Prevent reuse of old passwords`	• Prevents reuse of the same password
12	`Number of previous password hashes saved`	• Number of previous password hashes saved ie the last passwords cannot be reused
13	`Minimum password length`	Minimum password length (Default value: 12 characters)
14	`Anti-bruteforce` Zone	Defines the anti-bruteforce function
15	`Lock accounts after too many failed authentications` selector	• Activates the anti-bruteforce function
16	`Number of failed authentications over 10 minutes`	• Defines the number of the failed authentications over 10 minutes: after this limit, the account will be locked
17	`Discard changes` button	Cancels current changes
18	`Save changes` button	Saves current changes

5.7.4.9 `MISP settings` screen

5.7.4.9.1 Introduction

This screen is used to manage the connection between the GCenter and a Malware Information Sharing Platform (MISP) server in the local infrastructure.

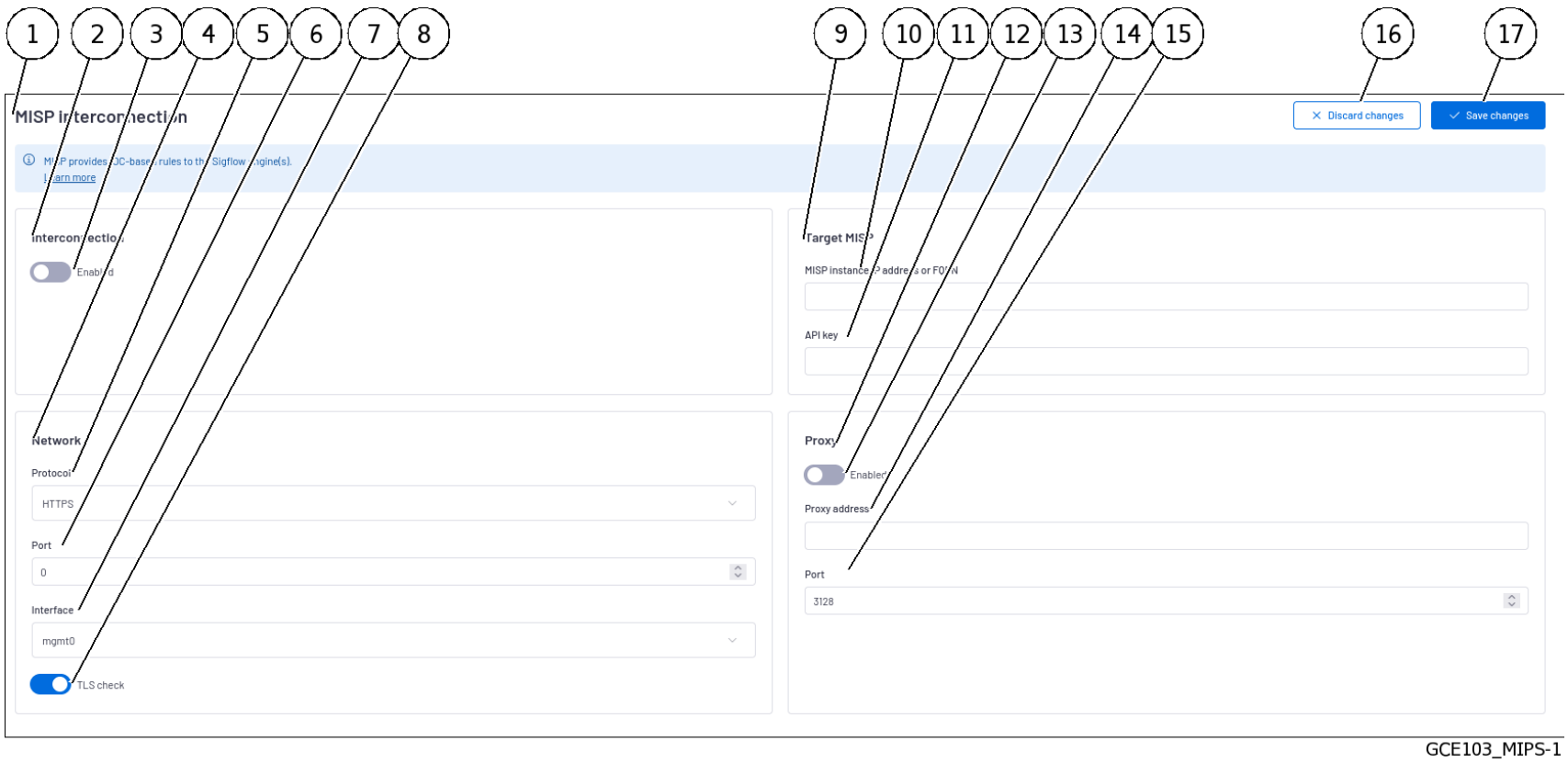
This screen is only accessible to members of the *administrator* group.

5.7.4.9.2 Links associated

For more information on MISP functions, see the presentation in *Connection to a MIPS server*.
For implementation, see the *Configuring the connection to the MISP* procedure

5.7.4.9.3 Screen description

After pressing the `MISP` command on the `Administration-Third party` menu, the `MISP settings` screen is displayed.



GCE103_MIPS-1

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

Item	Name	Function
1	`MISP interconnection`	This zone indicates the connection status with the MISP. It includes:
2	`Interconnection` zone	Activates the connection. It includes:
3	• `Enabled` button	• Enables the MISP feature
4	`Network` zone	Enables configuration the network parameters. It includes:
5	• `Protocol`	• Communication protocol to be used to contact the *MISP* instance. Two options are possible: 'HTTPS' and 'HTTP'
6	• `Port`	• MISP instance listening port
7	• `Interface`	• GCenter network interface for connection with MISP server
8	• `TLS check` selector	• if used, enables the TLS verification
9	`Target MISP` zone	Enables MISP configuration. It includes:
10	• `MISP instance IP address or FQDN`	• Domain name or IP address of the MISP instance
11	• `Api key `	• MISP instance API key
12	`Proxy` zone	Enables proxy configuration. It includes:
13	• `Enabled` selector	• If used, enables the proxy feature
14	• `Proxy address`	• IP address of the proxy
15	• `Port`	• Listening port
16	`Discard changes` button	Cancels current changes
17	`Save changes` button	Saves current changes

5.7.4.10 `GCaps Pairing` screen

5.7.4.10.1 Introduction

The GCap probe must be associated to the GCenter in order to receive the network flow.
Pairing enables configuring the IPSec tunnel between the GCap and the GCenter.
This screen is used to manage (add, remove or refresh) tunnels.

This screen is only accessible to members of the *administrator* group.

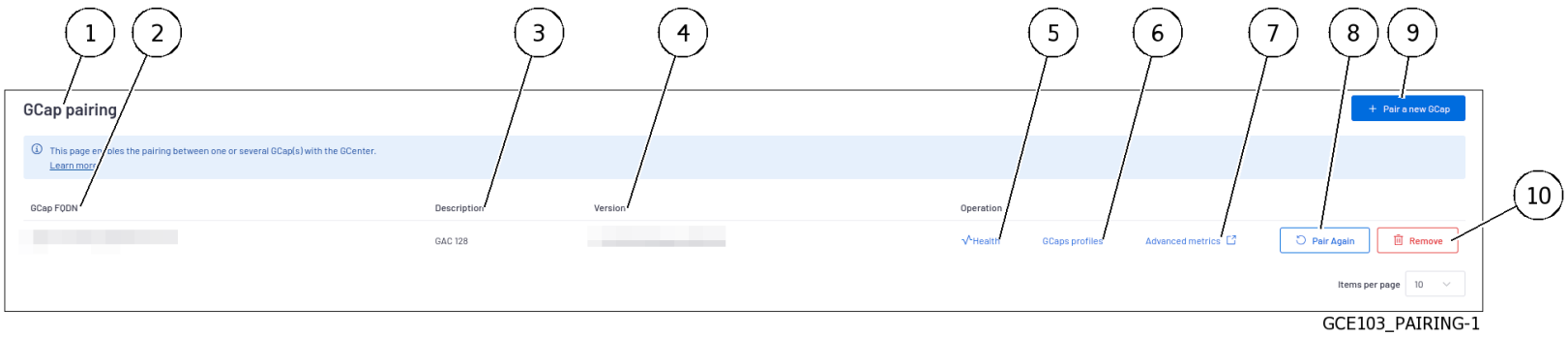
5.7.4.10.2 Links associated

For implementation, see :

- The *Pairing a GCap with the GCenter* procedure
- The *Pairing again a GCap* procedure

5.7.4.10.3 Screen description

After pressing the `GCap Pairing` command on the `Administration-GCap setup` menu, the `GCAP Pairing` screen is displayed.



GCE103_PAIRING-1

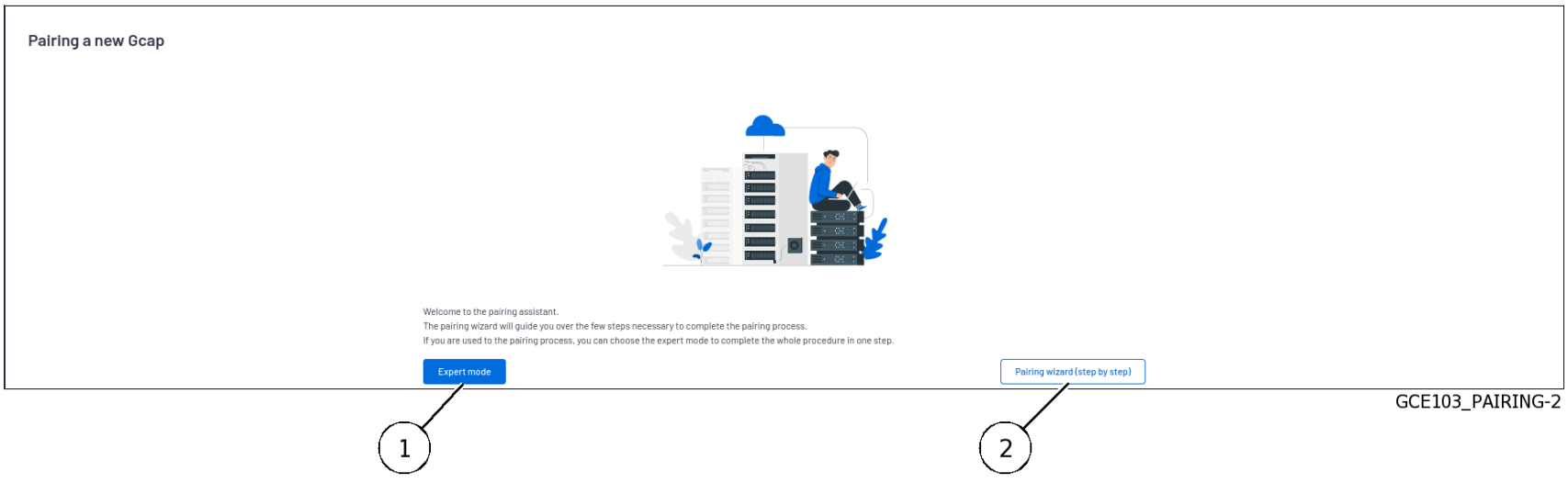
For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page. `.

This screen displays the list of the paired GCap

Item	Name	Function
1	`GCAP Pairing`	Window to manage the pairing
2	`FQDN`	• Fully Qualified Domain Name of the Gcap
3	`Description`	• Information entered during the pairing procedure
4	`Version`	• Gcap version
5	`Health` link	• Link to display the state of the VPN connection between the GCenter and the GCap (see the `Healthchecks` screen)
6	`GCaps profiles`	• Link to display the list and the configuration of the GCaps profiles
7	`Advanced metrics``	• Link to display the state of the VPN connection between the GCenter and the GCap (called Suricata status in the kibana interface)
8	`Pair Again` button	• Pairs again the selected GCap. The existing data is not lost.
9	`Pair a new GCap` button	• Starts the pairing of a new GCap. The `Pairing a new GCap` screen is displayed and is described below.
10	`Remove` button	• Removes the pairing

5.7.4.10.3.1 `Pairing a new GCap` screen

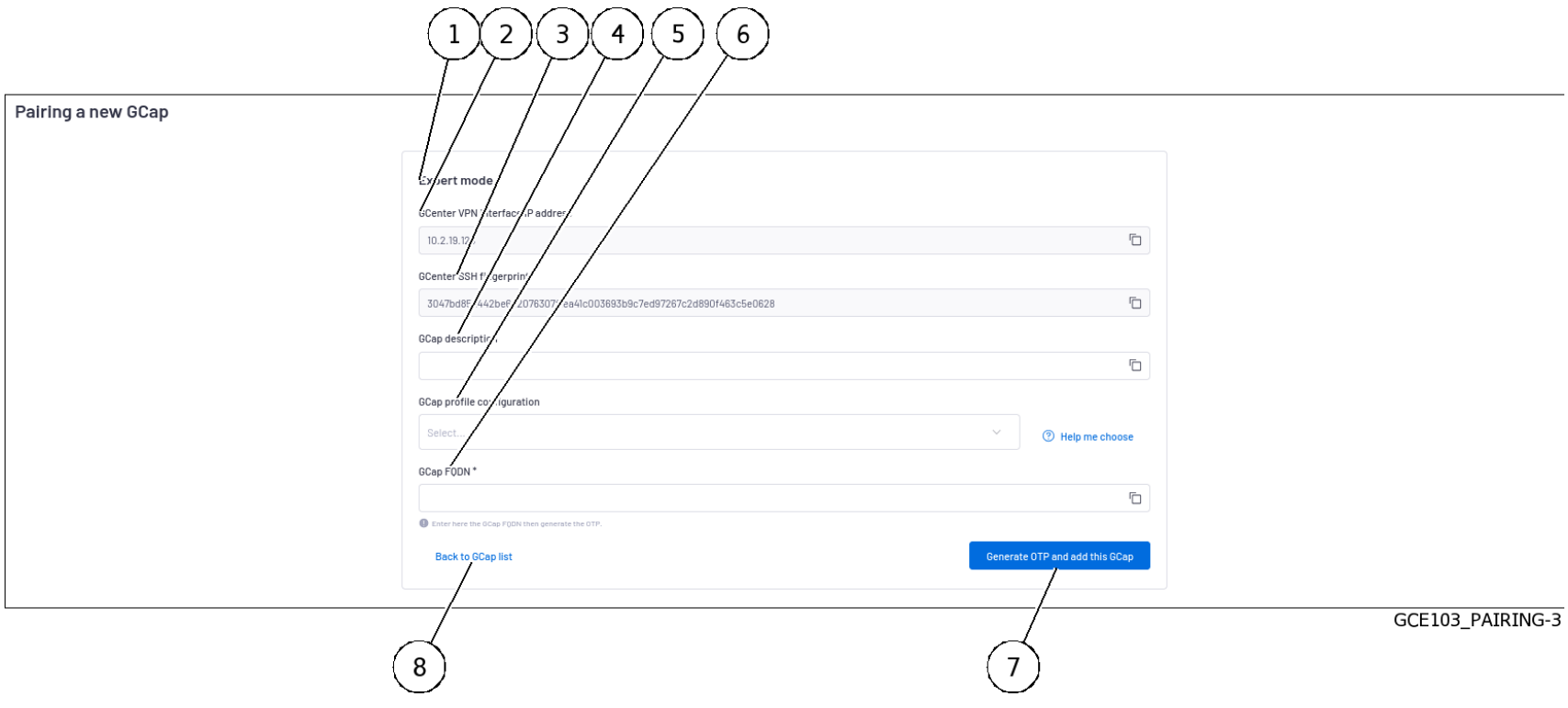
After clicking on the `Pair a new GCap` button, the following screen is displayed.
This screen displays two possibilities to pair a new GCap.



Item	Name	Function
1	`Expert mode` button	Completes the whole procedure in one step.
2	`Pairing wizard (step by step)` button	Launches the pairing wizard It will guide you over the few steps necessary to complete the pairing process.

5.7.4.10.3.2 `Pairing a new Gcap` screen in `Expert mode` mode

After clicking on the `Expert mode` button, the following screen is displayed.
This screen enables to enter all pairing parameters in only one screen.



Item	Name	Function
1	`Expert mode`	Zone to enter the parameters
2	`GCenter VPN interface IP address`	• IP address of the GCenter VPN interface
3	`GCenter SSH fingerprint` field	Displays the fingerprint of the GCenter useful during the pairing procedure
4	`GCenter SSH fingerprint` field	Enter a description of the GCap to be paired
5	`GCap profile configuration` field	Select a GCap profile to be applied
6	`GCap FQDN` field	Enter the FQDN (Fully Qualified Domain Name) of the GCenter
7	`Generate OTP and add this GCAP` button	Generates an OTP (One Time Password) and add this GCap
8	`Back to GCap list` button	Returns to the `GCAP Pairing` screen

5.7.4.11 `License` screen

5.7.4.11.1 Introduction

The `License` screen is used to obtain information about the current license, verify its validity and available features.
The `Gcenter license information` area enables obtaining information on:

- The material for which this license was issued via its model and serial number
- The period of validity of the license
- The associated contact address
- The type of license

The `License features` area provides information about enabling the various modules of the GCenter.
Finally, it is possible at the bottom of the page to enter a new license, and also to set the notification in the interface of a near expiry date by entering the number of days before the expiration.
Once the license is validated and activated, the content of the page updates and displays the details of the license.

Note:

To obtain a GCenter license, please contact GATEWATCHER business engineers or contact them at trade@GATEWATCHER.com.

The `Gatewatcher CTI License ` area enables obtaining information on:

- The material for which this license was issued via its model and serial number
- The validity of the license
- The associated contact address

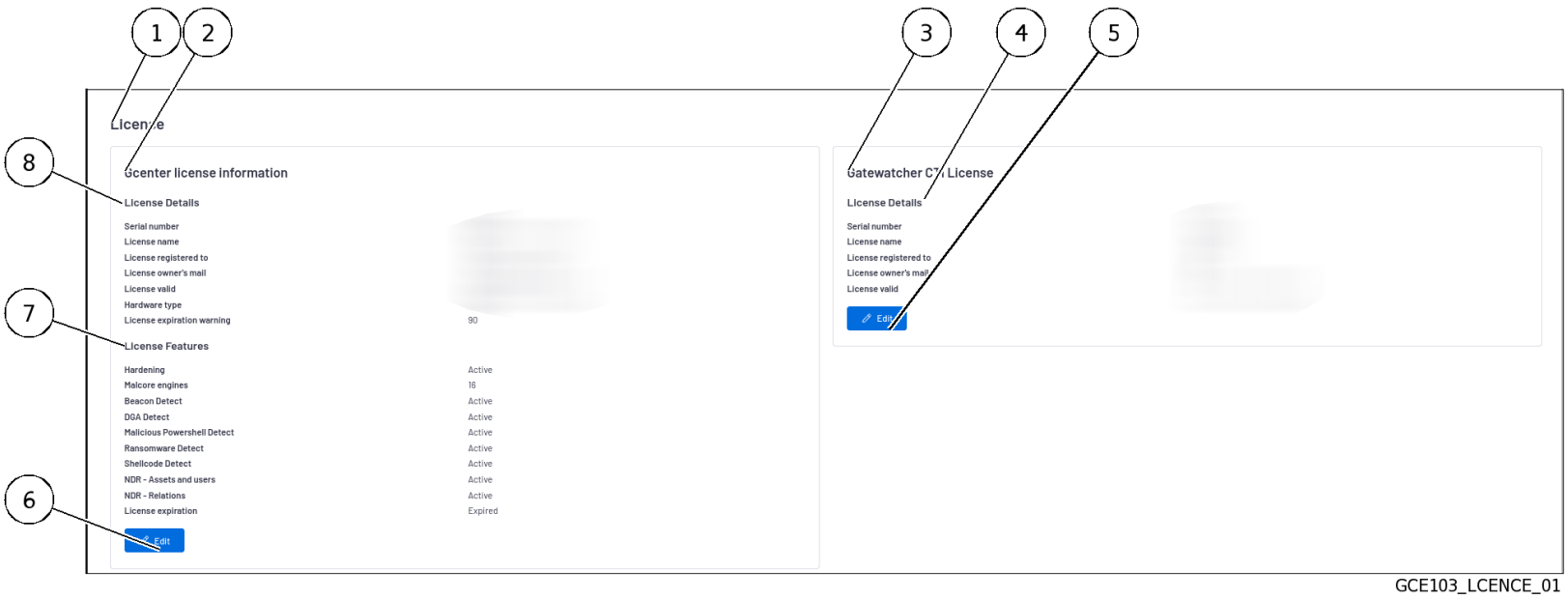
This screen is only accessible to members of the *administrator* group.

5.7.4.11.2 Links associated

For the implementation of a new license, refer to the *Managing the license* procedure.

5.7.4.11.3 Screen description

After pressing the `License` command on the `Administration-System` menu, the `License` screen is displayed.



For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.
`.

Item	Name	Function
1	`License` Window	Displays the licenses information or allows to enter a new license
2	`Gcenter license information` zone	• Displays the GCenter license information or enter a new license
8	`License Details` zone	• Displays the GCenter license details : - `Serial number` : server serial number - `License name`: Trackwatch Pro and Malcore. For further information about license, see paragraph below - `License registered to`: owner name - `License owner's mail`: owner mail - `License valid`: validity duration - `Hardware type`: virtual or hardware - `License expiration warning`: delay before warning to indicate the license expiration
7	`License Features` zone	• Indicates the list of active motors and features (depends of the license type): - `Hardening`: Active - `Malcore engines`: 1 or 16 - `Beacon Detect`: engine (Active or inactive) - `DGA Detect`: engine (Active or inactive) - `Malicious Powershell Detect`: engine (Active or inactive) - `Ransomware Detect`: engine (Active or inactive) - `Shellcode Detect`: engine (Active or inactive) - `NDR - Assets and users`: engine (Active or inactive) - `NDR - Relations`: engine (Active or inactive) - `License expiration`: status and number of days remaining in the license
6	`Edit` button	• Opens the Edit a GCenter license window. See presentation below.
3	`Gatewatcher CTI License` zone	Zone to view CTI license information or enter a new license
4	`License Details` zone	Displays the license details : - `Serial number` : Server serial number - `License name` : LastInfoSec - `License registered to` : owner name - `License owner's mail` : owner mail - `License valid` : validity duration
5	`Edit` button	• Opens the Edit a CTI license window. See presentation below.

5.7.4.11.3.1 Engine per license name

Table 39: License type

license name	Malcore	Shellcode detect	Powershell detect	Beacon detect	DGA detect	Ransomware detect	LastInfosec	AionBytes
AIONIQ	1 motor	NOK	NOK	NOK	NOK	NOK	NOK	NOK
AIONIQ Pro	1 motor	OK	OK	OK	OK	OK	Option	Option
AIONIQ Pro and Malcore	16 motors	OK	OK	OK	OK	OK	Option	Option

5.7.4.11.3.2 LastInfosec option

The LastInfosec option contents:

- The IOC specific source to create new rules used by the following engines
- The Active CTI engine
- The Retro hunt engine

5.7.4.12 `Network settings` screen

5.7.4.12.1 Introduction

The `Network settings` window displays the network configuration i.e:

- the Interface configuration
- the DNS configuration
- the NTP configuration
- the WebUI configuration
- the Hostname configuration
- the Session age configuration
- the SSH banner configuration

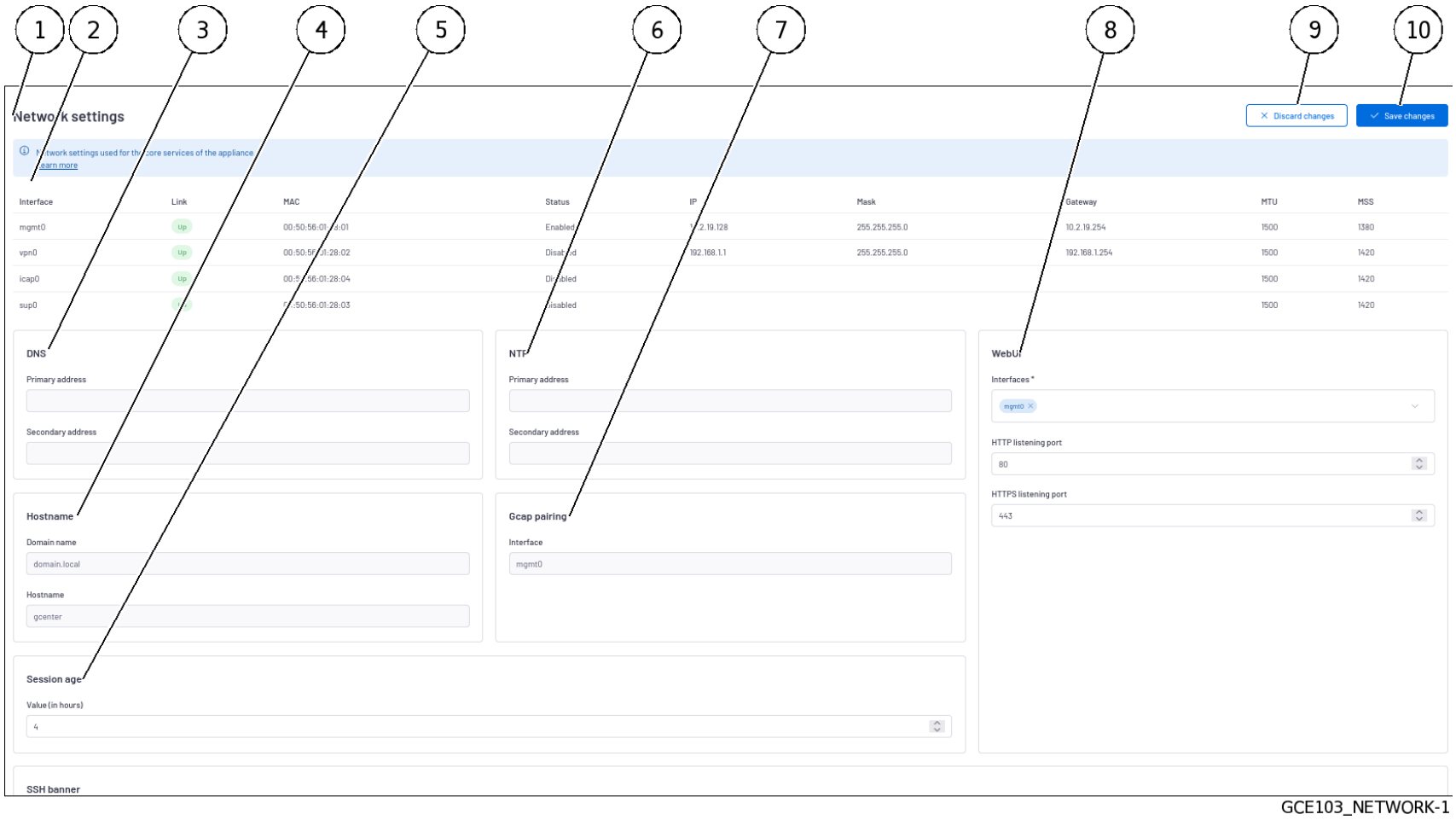
This screen is only accessible to members of the *administrator* group.

5.7.4.12.2 Links associated

To modify the network configuration, see the *`Network` command*

5.7.4.12.3 Screen description

After pressing the `Network settings` command on the `Administration-System` menu, the `Global settings` screen is displayed.



GCE103_NETWORK-1

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

Item	Name	Function
1	`Network settings` Window	To show the GCenter network settings
2	Interfaces parameters	• Displays the interface parameters. For each interface, the following parameters are displayed: - `Interface` column: interface name - `Link` column: link status - `MAC` column: MAC address - `Status` column: status - `IP` column: IP address - `Mask` column: mask address - `Gateway` column: gateway address - `MTU` column: MTU value - `MSS` column: MSS value
3	`DNS` parameters	• Displays the DNS parameters (`Primary address` and Secondary address)
4	`Hostname`	• Displays the hostname parameters: - `Domain name` - `Hostname`
5	`Session age`	• Displays the session age value
6	`SSH banner`	• Displays the SSH banner content
7	`NTP`	• Displays the NTP parameters (`Primary address` and Secondary address)
8	`Gcap pairing`	• Displays the interface NTP parameters (`Primary address` and Secondary address)
9	`WebUI`	• Displays the parameters of the interface used for the WebUI access: - `Interfaces`: name of the used interface - `HTTP listening port` - `HTTPS listening port`

5.7.4.13 `Global settings` screen

5.7.4.13.1 Introduction

The `Global settings` window enables to configure:

- the GScan feature
- the `Assets & Users tracking` feature
- the `Relationship tracking` feature
- the `General parameters & security` parameters
- the `Custom certificate` feature
- the `Dual authenticator` feature

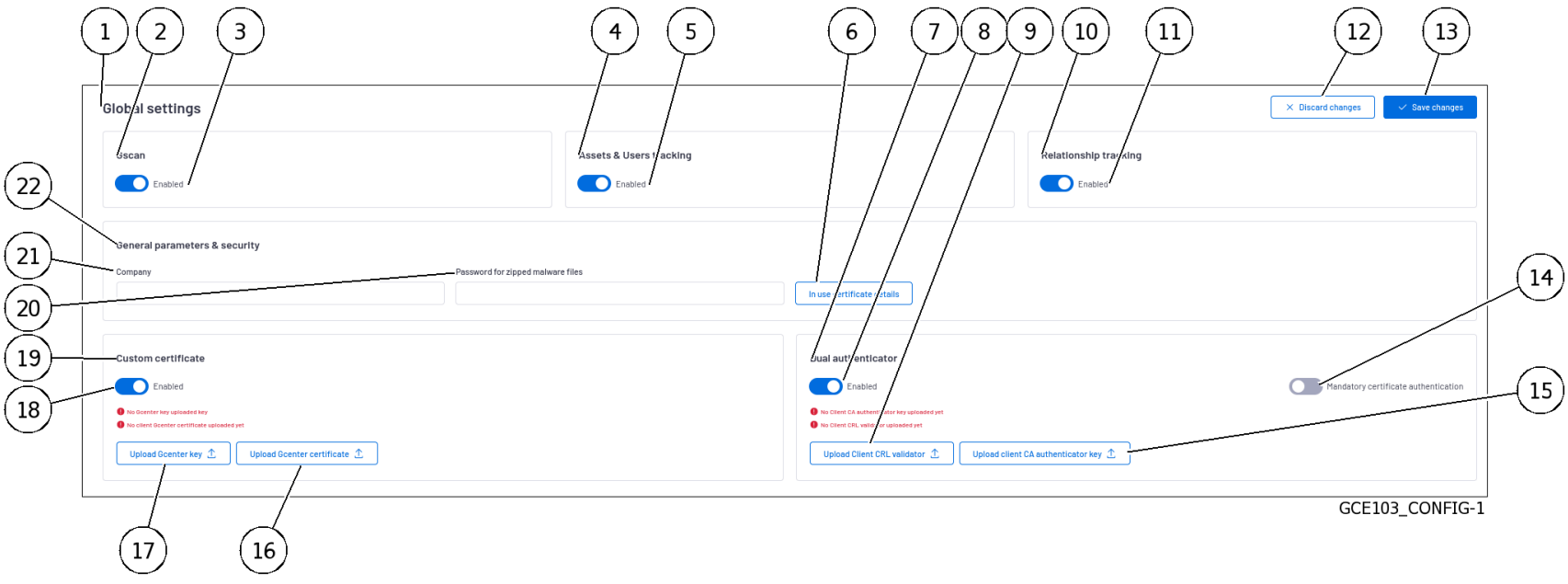
This screen is only accessible to members of the *administrator* group.

5.7.4.13.2 Links associated

For the implementation of the Global settings, see *Configuring the GCenter*

5.7.4.13.3 Screen description

After pressing the `Global settings` command on the `Administration-System` menu, the `Global settings` screen is displayed.



For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

Item	Name	Function
1	`Global settings` window	Defines the GCenter global settings
2	`Gscan` zone	Configures the GScan feature. This zone contents:
3	`Enabled` selector	• Enables real-time local scanning for malware or suspicious executables. Default value: enabled As part of the Military Programming Law, the GScan Function is disabled by default in this management interface.
4	`Assets & Users tracking` zone	Configures the `Assets & Users tracking` feature. This zone contents:
5	`Enabled` selector	• Enables the `Assets & Users tracking` feature
10	`Relationship tracking` zone	Configures the `Relationship tracking` feature. This zone contents:
11	`Enabled` selector	• Enables the `Relationship tracking` feature
12	`Discard changes` button	Cancels current changes
13	`Save changes` button	Saves current changes
22	`General parameters & security` zone	Configures the following parameters. This zone contents:
21	`Company`	• Adds the company name to be added to the detection analysis reports default value: empty These reports can be downloaded after making an association between the GCenter and the GBox
20	`Password for zipped malware files`	• Defines the password protecting the archive when downloading malware and unzipping it to avoid an unintentional click default value: empty This password will be the same for downloading shellcodes. The specifics of this functionality are described in more detail in the Malcore sections
7	`Dual authenticator` zone	Configures the dual authentication The dual authentication area enables mutual authentication (mTLS). This allows the user to verify the identity of the server as well as allowing the server to verify the identity of the user. This zone contents:
8	`Enabled` selector	• Enables the `Dual authenticator` feature
9	`Upload Client CRL validator` button	• Selects a file from the list of revoked certificates
15	`Upload Client CA authenticator key` button	• Selects a certificate file issued by the certification authority in PEM format
14	`Mandatory certificate authentication`	• Making it mandatory for users to hold a certificate issued by the certification authority
6	• `In use certificate details` button	Opens a screen to display information on the certificate currently on the following zones: * the `In use certificate details KEY` zone * the `In use certificate details PEM` zone * the `CA certificate information` zone
19	`Custom certificate` zone	Enables using a specific certificate. This is done by specifying the private key in the `GCenter Key` field and the PEM format certificate in the `GCENTER certificate` field and also by activating the `Enable Custom Certificate` selector.
18	`Enabled` selector	• Enables a personalized certificate
17	`Upload Gcenter Key` button	Selects a GCenter key file
16	`Upload Gcenter certificate` button	Selects a GCenter certificate

5.7.4.14 `System logs` screen

5.7.4.14.1 Introduction

The Kibana web interface allows to display the data present in the ElasticSearch indexes of the GCenter.
The `System logs` screen displays the information given by the `Administration` tab.

This screen is only accessible to members of the *administrator* group.

5.7.4.14.2 Links associated

For implementation, see the procedure *Using of the Kibana dashboards*.
This interface is described in the Kibana Interface section: see the *Overview of the Kibana GUI*.

5.7.4.15 `Diagnostics` screen

5.7.4.15.1 Introduction

In the event of an obstructing problem, it is necessary to access the solution logs in order to resolve the problem.
This information is used for diagnosis in collaboration with GATEWATCHER support.
The diagnostic function enables:

- Generating log files and uploading them for analysis by GATEWATCHER support.
  The export file log is protected by a password only known by the GATEWATCHER administrator team.
  Messages from all logs will be accessible as well as all system calls from the system.
- Generating the "Tech support" file and uploading it for analysis by an administrator.
  The "Tech support" file provides information on the health of the GCenter server although it does not contain any captured data.
  This file is not encrypted and is usable by the administrator.

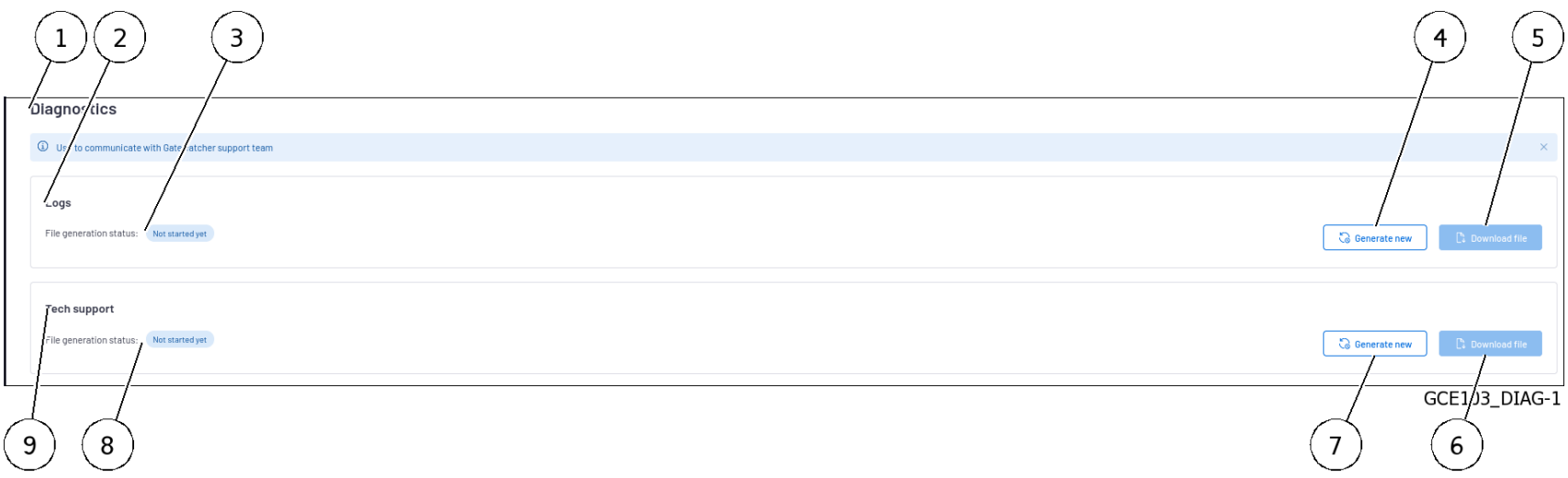
This screen is only accessible to members of the *administrator* group.

5.7.4.15.2 Links associated

For implementation, see the *Generating and loading files for diagnosis* procedure.

5.7.4.15.3 Screen description

After pressing the `Diagnostics` command on the `Administration-Maintenance` menu, the `Diagnostics` screen is displayed.



For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page. `.

Item	Name	Function
1	`Diagnostics` window	Generate files to diagnose
2	`Log` zone	Generates the log file
3	`File generation status:` field	• Indicates the status of the file generation
4	`Generate new` button	• Generates the Log file
5	`Download` button	• Downloads the Log file
9	`Tech support` zone	Generates the tech support file
8	`File generation status:` Field	• Indicates the status of the file generation
7	`Generate new` button	• Generates the Tech support file
6	`Download` button	• Downloads the Tech support file

5.7.4.16 `Configuration` screen

5.7.4.16.1 Introduction

This screen enables configuring the frequency and location of backups.

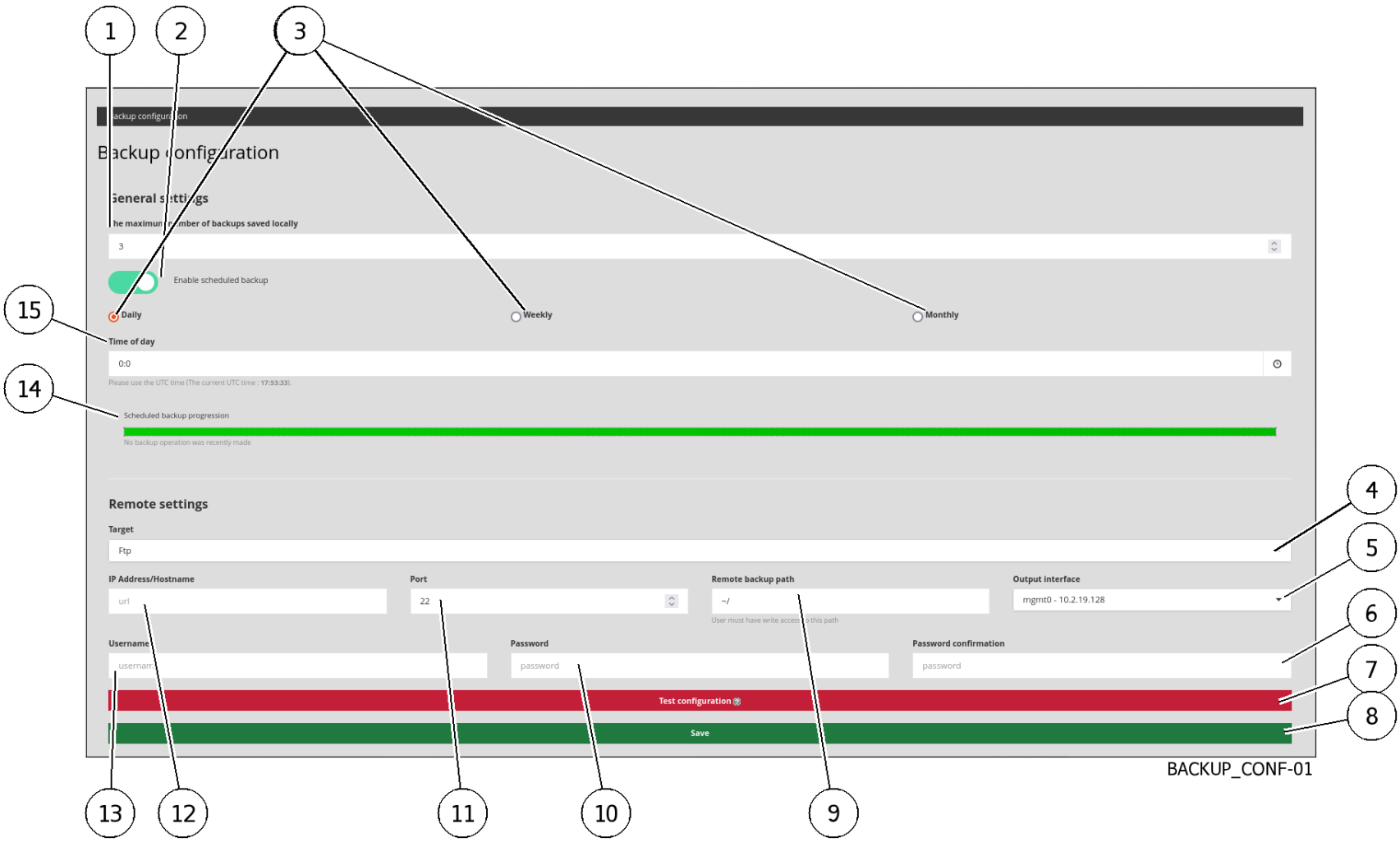
This screen is only accessible to members of the *administrator* group.

5.7.4.16.2 Links associated

For more information, see the *Overview of the backup and restoration*.
For implementation, see the *Setting the backup* procedure.

5.7.4.16.3 Screen description

After pressing the `Configuration` command on the `Administration-Backup and restore` menu, the `Backup configuration` screen is displayed.



For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

The `Backup configuration` screen contains the following sections:

- *`General settings` section*
- *`Remote settings` setting in `Local` version* for a local only backup (Gcenter backup partition)
- *`Remote settings` section in `FTP` version* for a backup on a remote SCP server and for a local backup
- *`Remote settings` section in `SCP` version* for a backup on a remote FTP server and for a local backup

---

5.7.4.16.4 `General settings` section

Item	Name	Function
1	`The maximum number of backups saved locally`	Maximum number of local backups
2	`Enable scheduled backup` selector	Activates the backup scheduler. Displays the zone below
3	`Daily`, `Weekly`, `Monthly` buttons	• Choice of the backup frequency
14	`Scheduled backup progression` field	• Backup progress bar
15	`Time of day` field	Choosing the time of the backup: this field is active when the `Daily` choice is selected
4	`Target` field	Choosing the backup location: `local`, `Scp`, `Ftp` Selecting Scp and Ftp will bring up additional parameters listed below

Note:

The time displayed under the `Time of day` field corresponds to the UTC time of the user's browser.

5.7.4.16.5 `Remote settings` setting in `Local` version

By selecting `Local` in parameter (4) `Target`, the `Remote settings` part contains the following:

Item	Name	Function
4	`Target` field	Choosing the backup location: `local`
8	`Save` button	Validates the information entered

By selecting this choice, the backup will run locally on the GCenter backup partition

---

5.7.4.16.6 `Remote settings` section in `FTP` version

The `Remote settings` section in the `FTP` version contains the following items:

Item	Name	Function
5	`Output interface` field	Name of the network interface used of the GCenter, including IP address
6	`Password confirmation` field	2nd entry of the confirmation password: must be identical to the mark (10)
7	`Test configuration` button	Triggers verifying the entered parameters and sending a test file to the specified directory The possible actions listed below depend on the context
8	`Save` button	Validates the information entered
9	`Remote backup path` field	Path of the backup on the remote server. The user account used should have read and write permissions on this path.
10	`Password` field	Entering the user's password of the remote server
11	`Port` field	Entering the server's listening port of the remote server
12	`IP Address` field	Entry of the IP address or FQDN of the remote server (Example: _72.14.192.0)
13	`Username` field	Entering the user name of the remote server

By selecting this choice, the backup will run on the network using the FTP protocol.

5.7.4.16.7 `Remote settings` section in `SCP` version

The `Remote settings` section in the `SCP` version contains the following items:

Name	Function
`IP Address`	Entry of the IP address or FQDN of the remote server (Example: _72.14.192.0)
`Port` field	Entering the server's listening port
`Remote backup path`	Path of the backup on the remote server. The user account used should have read and write permissions on this path.
`Output interface`	Name of the network interface used, including IP address
`Credentials type`	Remote server authentication mode (choice between `Password` or `Public_key`)
`Username`	Entering the user name of the remote server
`Password`	Only displayed if the `Password` choice is active in the `Protocols` field. Entering the user's password
`Password confirmation`	Only displayed if the `Password` choice is active in the `Protocols` field. 2nd entry of the confirmation password: must be identical to the mark (10)
`Backup host public key`	Enter the Public Key of the backup host server First, connect to the remote server to display its public key
`Gcenter public key`	GCenter public key
`Test the saved configuration` button	Triggers verifying the entered parameters and sending a test file to the specified directory of possible actions
`Save` button	Saves the entered parameters

By selecting this choice, the backup will run on the network using the SCP protocol.

5.7.4.17 `Backup operations` screen

5.7.4.17.1 Introduction

This screen enables:

- Manually performing a backup
- Manually restoring from a backup file located on the GCenter or on a remote PC
- Visualizing the correct operation of the backup schedule

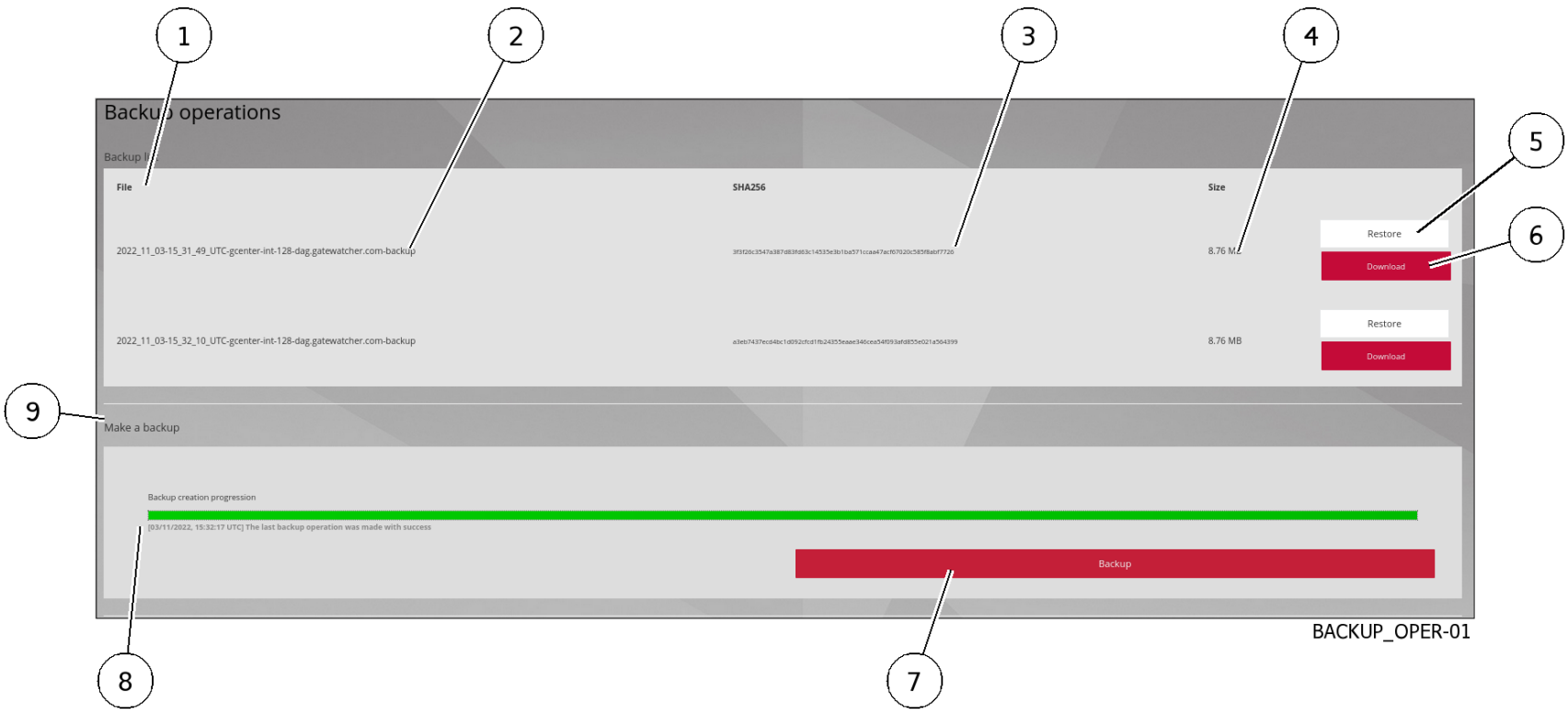
This screen is only accessible to members of the *administrator* group.

5.7.4.17.2 Links associated

For more information, see the *Overview of the backup and restoration*.
To perform a backup, see the procedure *Operating the backup*.
To perform a restoration, see the procedure *Operating the restoration*.

5.7.4.17.3 Screen description

After pressing the `Operation` command from the `Administration-Backup and restore` menu, the screen `Backup operations` is displayed.



For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page. `.

The `Backup operations` screen contains the following sections:

- *`Backup list` section*
- *`Make a backup` section*
- *`Restore operations` section*
- *`Scheduled backup` section*

5.7.4.17.4 `Backup list` section

The `Backup list` screen contains the following sections:

Item	Name	Function
1	`File` field	List of backup files. Each file has the following properties. - Name of the file (2) consisting of 'timestamp-GCENTER-version-backup' - Shasum `SHA256` (3) consisting of 'timesatamp-NomDuGCENTER.local-backup.gwc' - `Size` (4)
5	`Restore` button	Enables file restoration. Beware, the restoration starts immediately!
6	`Download` button	Downloads the backup file to the remote PC's download directory

---

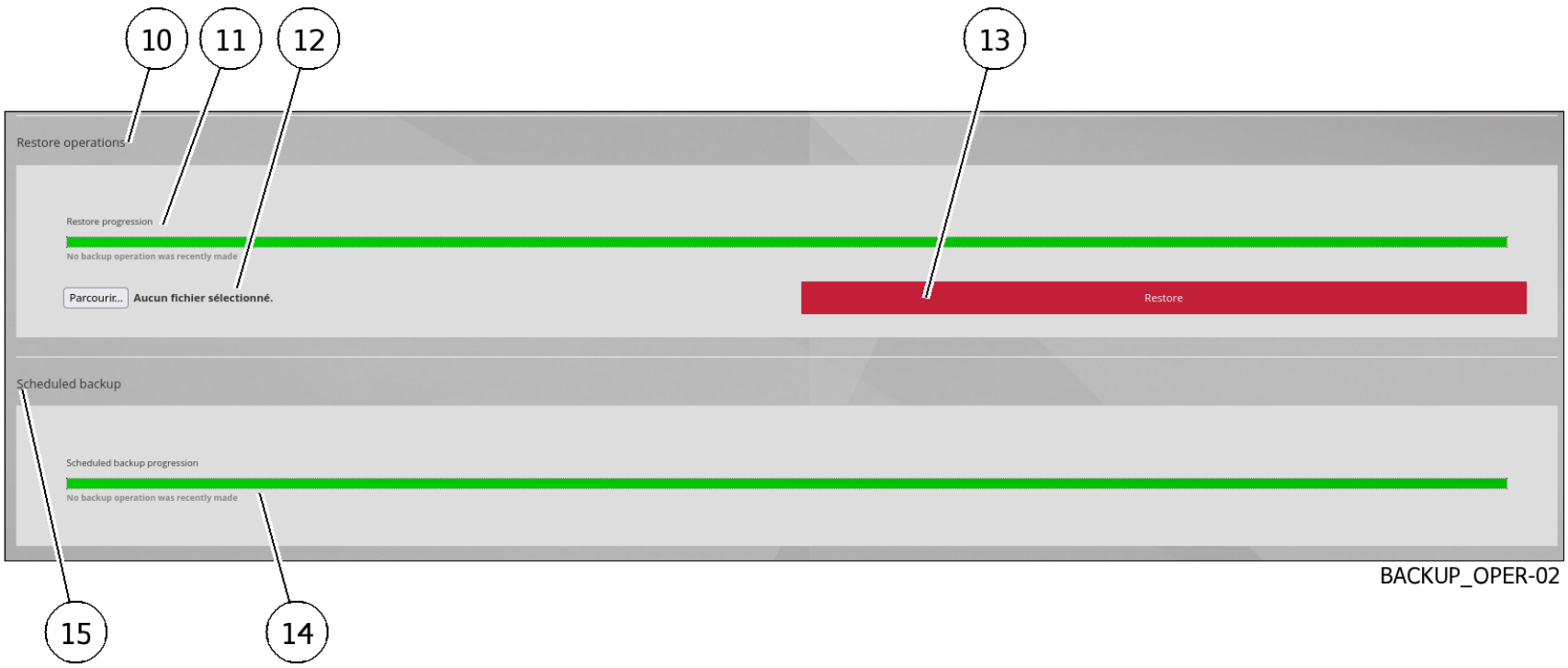
5.7.4.17.5 `Make a backup` section

The `Make a backup` screen (9) contains the following sections:

Item	Name	Function
7	`Backup` button	Enables either local or local and remote backup depending on the configuration. - Name of the file (2) consisting of 'timesatamp-GCENTER-version-backup' - Shasum `SHA256` (3) - `Size` (4)
8	`Backup creation progression`	The progress bar shows the status of the backup At the end of the backup, a message is displayed indicating the result
6	`Download` button	Downloads the backup file to the remote PC's download directory

---

5.7.4.17.6 `Restore operations` section



The `Restore operations` screen (10) contains the following sections:

Item	Name	Function
11	`Restore progression`	The progress bar shows the status of the restoration At the end of the backup, a message is displayed indicating the result
12	`Parcourir` button	Sélects a backup file on the remote PC
13	`Restore` button	Enables restoration from the selected file

5.7.4.17.7 `Scheduled backup` section

The `Scheduled backup` section (15) shows the status (14) of the scheduled backup:

- The progress bar shows the status of the restoration
- An information message about this status

5.7.4.18 `Retention policy` screen

5.7.4.18.1 Introduction

This screen enables the setting up elasticsearch data retention:

- Activating the function `Synchronize NDR boards with Elasticsearch retention`
- Changing the value of the retention time
- To define the value of TTL configuration

This screen is only accessible to members of the *administrator* group.

5.7.4.18.2 Links associated

For more information, see the *Overview of the backup and restoration*.
For implementation, see *Configuring the NDR*.

5.7.4.18.3 Screen description

After pressing the `Retention policy` command on the `Administration-Data` menu, the `Retention policy` screen is displayed.

The screen contains the following sections:

- *`Elasticsearch max data retention (in GiB)` zone*
- *`TTL configuration` section*
- *`Synchronize NDR boards with Elasticsearch retention` section*
- *`Resource allocations` section*

5.7.4.18.4 `Elasticsearch max data retention (in GiB)` zone

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

Item	Name	Function
1	`Retention policy` Window	Configures the NDR retention policy
2	`Elasticsearch max data retention (in Go)` zone	Configures the retention data
5	`Data retention: ...` cursor	• Sets the quantity of the retention data / total space.
7	`Discard changes` button	Cancels current changes
8	`Save changes` button	Saves current changes

5.7.4.18.5 `TTL configuration` section

Item	Name	Function
3	`TTL configuration` zone	Configures the TTL configuration
4	`Data max TTL (in days)`	Maximum Time To Live (in days)

5.7.4.18.6 `Synchronize NDR boards with Elasticsearch retention` section

The NDR database stores metadata about the alerts displayed in the dashboards (`Alerts`, `Assets`, `Users`, etc.), while Elasticsearch (Hunting) stores details about them.

Enabling this feature activates the synchronization of NDR dashboards with the data available in Elasticsearch.

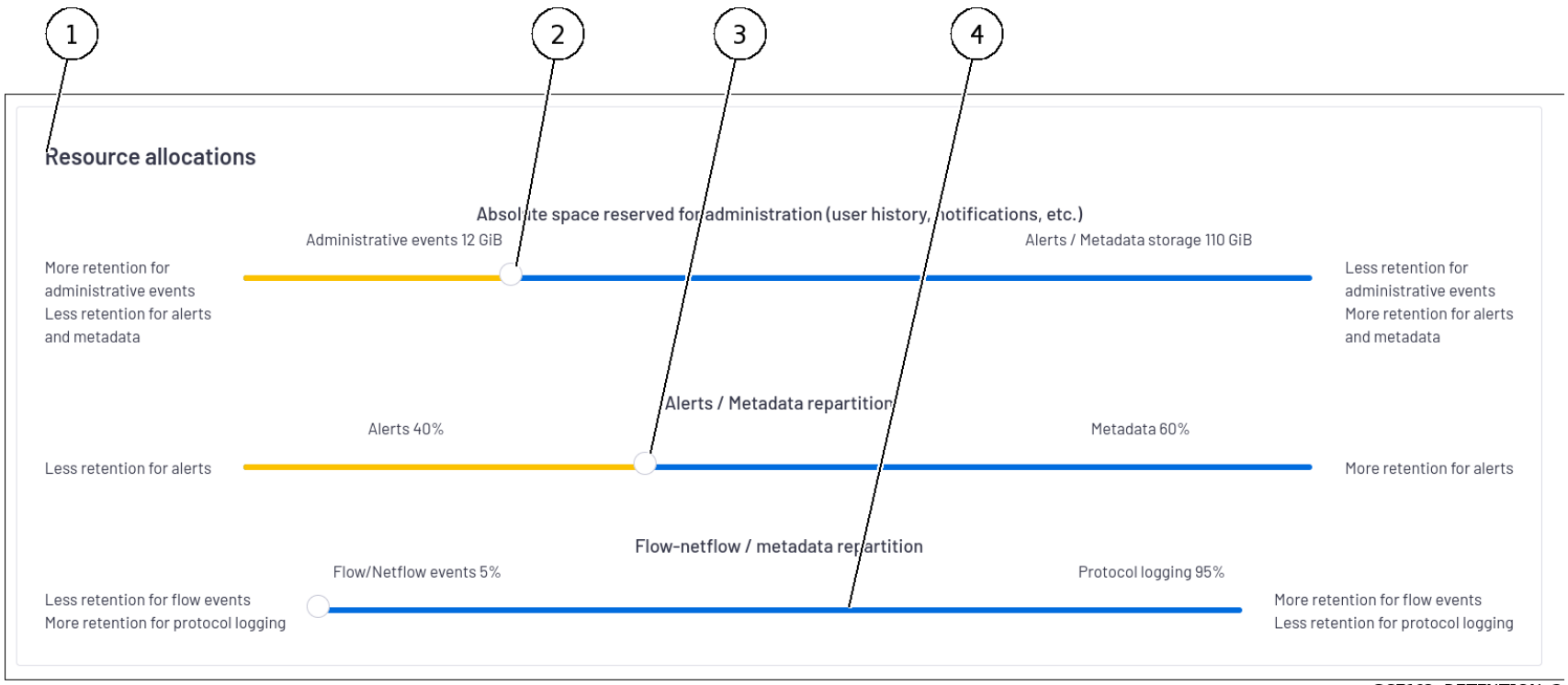
Disable this feature to continue to display alerts in NDR dashboards that are no longer stored in Elasticsearch. In this case, the alerts are available but the details cannot be displayed.

The retention time of Elasticsearch depends on the maximum space allocated in GB to store the logs

Therefore, the data retention period in elasticsearch depends on the amount of logs generated by the GCaps.

Item	Name	Function
6	`Synchronize NDR boards with Elasticsearch retention`	Zone to configure the synchronization of the NDR boards
9	`Enabled` selector	Synchronises the NDR dashboards with data in Elasticsearch (see text below the table)

5.7.4.18.7 `Resource allocations` section



GCE103_RETENTION_2

Item	Name	Function
1	`Resource allocations` zone	Configures the storage space allocation
2	`Absolute space reserved for administration (user history, notifications, etc.)` selector	Manages the allocation of disk space between event storage and alert and metadata storage
3	`Alerts / Metadata repartition` slider	For storage reserved for alerts and metadata, this slider manages the distribution between them
4	`Flow-netflow / metadata repartition` slider	For storage reserved for metadata, this slider manages the distribution between the flow/Netflow events and the protocol logging

5.7.4.19 `Data Management` screen

5.7.4.19.1 Introduction

This screen enables deleting all or part of the data on the GCenter.
In this screen, it is possible to choose the type of data to be permanently deleted from the GCenter.
The options enable:

- Choosing the time interval in which the deletion is to be carried out
- Choosing the type of data to be deleted

Important:

Data not yet processed will also be deleted.

This screen is only accessible to members of the *administrator* group.

5.7.4.19.2 Links associated

For details on data management, see the *Data use*.
For implementation of the configuration, see the procedure *Deleting data (log files)*.

5.7.4.19.3 Screen description

After pressing the `Data Management` command of the `Administration-Data` menu, the `Data Management` screen is displayed.

Item	Name	Function
1	`Data management`	Window to choose data to delete
2	`All data elements`. The data elements are composed of:	Check box to select all data elements on only one click
6	• `elasticsearch`	The elasticsearch data is grouped into the following data views: `Engines alerts`, `Engines flows`, `Engines metadata`, `Appliances logs`, `Appliances access`, `Appliances monitoring`, `Too large indexes`, `Indicator of compromise (IOC) indices`
9	• `system`	The `system` data is grouped into the `Gscan history` (8) and `Notifications` (7) categories
13	• `engine_history`	The `engine_history` data is grouped into the `Ransomware` (12), `DGA` (11), `Beacon` (10) categories
14	• `processed_data`	The `processed_data` data is grouped into the `Risk and alerts board`, `Assets and users` categories
20	• `samples`	The `samples` data is grouped into the `Malcore samples` (19), `Shellcode detect samples` (18), `Malicious Powershell detect samples` (17), `Sigflow samples` (16), `Retro hunt samples` (15) categories
3	Calendar	Displays the calendar to choose the data deletion period
4	`Any date` selector	Activates the data deletion period as any date
5	`Delete` button	Deletes selected data

5.7.4.20 `Data export` screen

5.7.4.20.1 Introduction

It is possible to export events from the GCenter to remote servers such as a SIEM by using the syslog protocol.
The number of Syslog servers is limited to two.
This screen enables configuring the connection to the two remote servers.

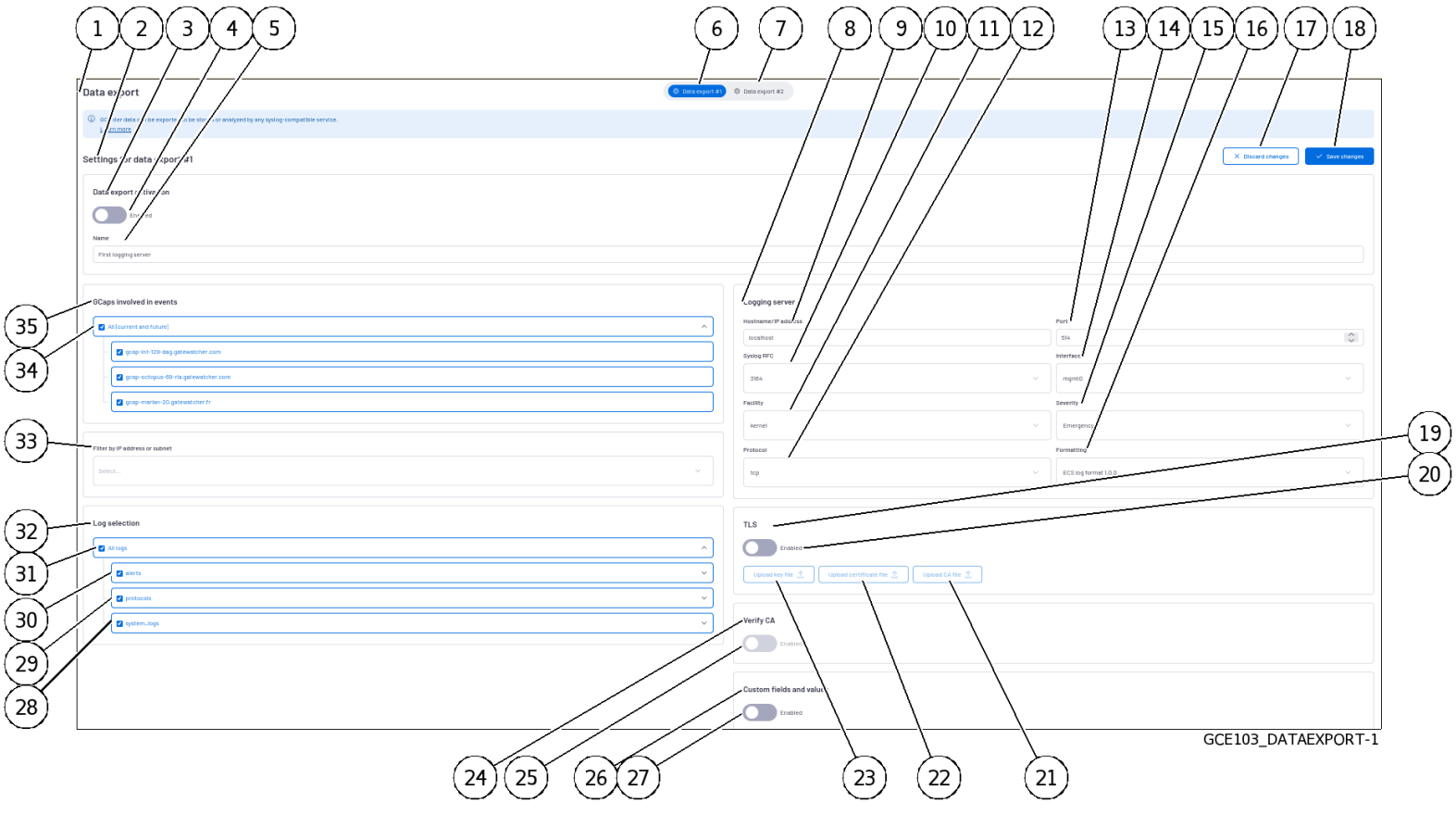
This screen is only accessible to members of the *administrator* group.

5.7.4.20.2 Links associated

For details on data management, see the *Data use*.
For more information of the syslog export, see the *Connection to Syslog servers*.
For implementation of the configuration, refer to *Configuring the export data to a SIEM via the syslog protocol*.

5.7.4.20.3 Screen description

After pressing the `Data export` command in the `Administration-Data` menu, the `Data export` screen is displayed.



Item	Name	Function
1	`Data export` window	Configures the data export. There are two usable connections selected by the buttons (6) or (7)
2	`Settings for data export #1` zone	Configures the connexion named `data export #1`
3	`Data export activation` zone	Enables the Syslog export
4	`Enabled` selector	• Enables the Syslog export
5	`Name`	• Name of the remote server assigned by the administrator (Example: _First logging server)
6	`Data export #1` button	Selects the Syslog connection to be configured: here it is the first connection
7	`Data export #2` button	Selects the Syslog connection to be configured: here it is the second connection

continues on next page

Table 40 – continued from previous page

Item	Name	Function
8	`Logging server` zone	Configures the connection This zone contents:
9	`Hostname/IP address`	• IP address or name of the remote server (Example: localhost or 192.168.199.1)
10	`Syslog RFC`	• Selects the corresponding RFC for the desired message normalisation (Example: _3164 or _5424)
11	`Facility`	• Message type used for sending to the Syslog server. The default value is a *kernel* (Example: kernel, user-level, mail, daemon, security/authorization, syslog, line printer, network news, uucp)
12	`Protocol`	• Protocol used for data transfer The default value is in TCP (Example: tcp, udp ou ssl_tcp)
13	`Port`	• Listening port of the remote server. The default value is 514.
14	`Interface`	• Selected output interface between the **GCenter** and the remote SIEM server (Example: mgmt0, sup0)
15	`Severity`	• Severity rate for Syslog messages. The default value is an emergency The list of choices is shown in the table **List of Facility field choices**
16	`Formatting`	• Choice between the log formatting: - ECS log format 1.0.0. for the Elastic Common Schema (ECS) format - Legacy retro-compatibility 2.5.3.102 for standard syslog export
17	`Discard changes` button	Cancels current changes
18	`Save changes` button	Saves current changes
19	` TLS` zone	Configures the TLS feature This zone contents:
20	• `Enabled` selector	• Enables the TLS service (Transport Layer Security). Disabled by default.
21	`Upload CA file` button	• Adds the file for the certification authority
22	`Upload certificate file` button	• Adds a certificate
23	`Upload key file` button	• Adds the related key
24	`Verify CA` Zone	Actives the checking the validity of the certificate This zone contents:
25	`Enabled` selector	• Checks the validity of the certificate when the TLS service is enabled. Disabled by default.
26	`Custom fields and values` zone	Feature of the custom fields and values This zone contents:

continues on next page

Table 40 – continued from previous page

Item	Name	Function
27	`Enabled` selector	• Activates the feature. Disabled by default.
32	`Log selection` Zone	Selects the log to be exported. This zone contents:
31	`All logs`	• Check box to select all logs The list of the log types is displayed. The log types are `alerts` (30), `protocols` (29), `system_logs` (28) The alerts types are detailed in the note below. The protocols types are detailed in the note below: these protocols are the Sigflow protocols. The system_logs has only one choice: notification.
33	`Filter by IP address or subnet`	Selects the events source with its IP address or subnet. By default, all data is sent to the remote server if the field is empty.
35	`Gcap involved in events` zone	Selects data to sent: all data from the GCap paired and selected to the GCenter is sent to the remote server This zone contents:
34	`All (current and futures)`	• Check box to select all known GCaps The list of the GCaps is displayed. Each GCap can be selected independently.

Note:

List of motors for the alert logs

The alerts type can be selected engine by engine or for all motors by using the `alerts` check box:

- active_cti
- beacon_detect
- dga_detect
- malicious_powershell_detect
- malcore
- malcore_retroanalyzer
- ransomware_detect
- retrohunt
- shellcode_detect
- sigflow

Note:

List of protocols for the protocol logs

unsupported_protocols, sigflow_alert, sigflow_dcerpc, sigflow_dhcp, sigflow_dnp3, sigflow_dns, sigflow_enip, sigflow_file, sigflow_ftp, sigflow_http, sigflow_http2, sigflow_ikev2, sigflow_krb5, sigflow_mqtt, sigflow_modbus, sigflow_netflow, sigflow_nfs, sigflow_ntp, sigflow_rdp, sigflow_rfb, sigflow_sip, sigflow_smb, sigflow_smtp, sigflow_snmp, sigflow_ssh, sigflow_tftp, sigflow_tls

Activate the `protocols` check box selects all listed protocols: a protocol that is not selected will not be exported.

If the GCap version is newer than that of the GCenter, some protocols may be missing.

Table 41: **List of choices for the `Facility` field**

Name	Description
Emergency	The system is unusable
Alert	Action must be taken immediately
Critical	Conditions are severe
Error	Failure conditions
Warning	Warning Conditions
Notice	Normal but significant condition
Informational	Explanatory messages
Debug	Repair level messages

Note:

SSL-TCP is mandatory if SSL encryption is enabled. Otherwise, it is disabled.

5.7.4.21 `Netdata Export Configuration` screen

5.7.4.21.1 Introduction

To export system data in real time to a remote Netdata server, a Netdata export interface is present in the GCenter and is reserved for this purpose.
This Netdata export interface must be configured with the necessary information.

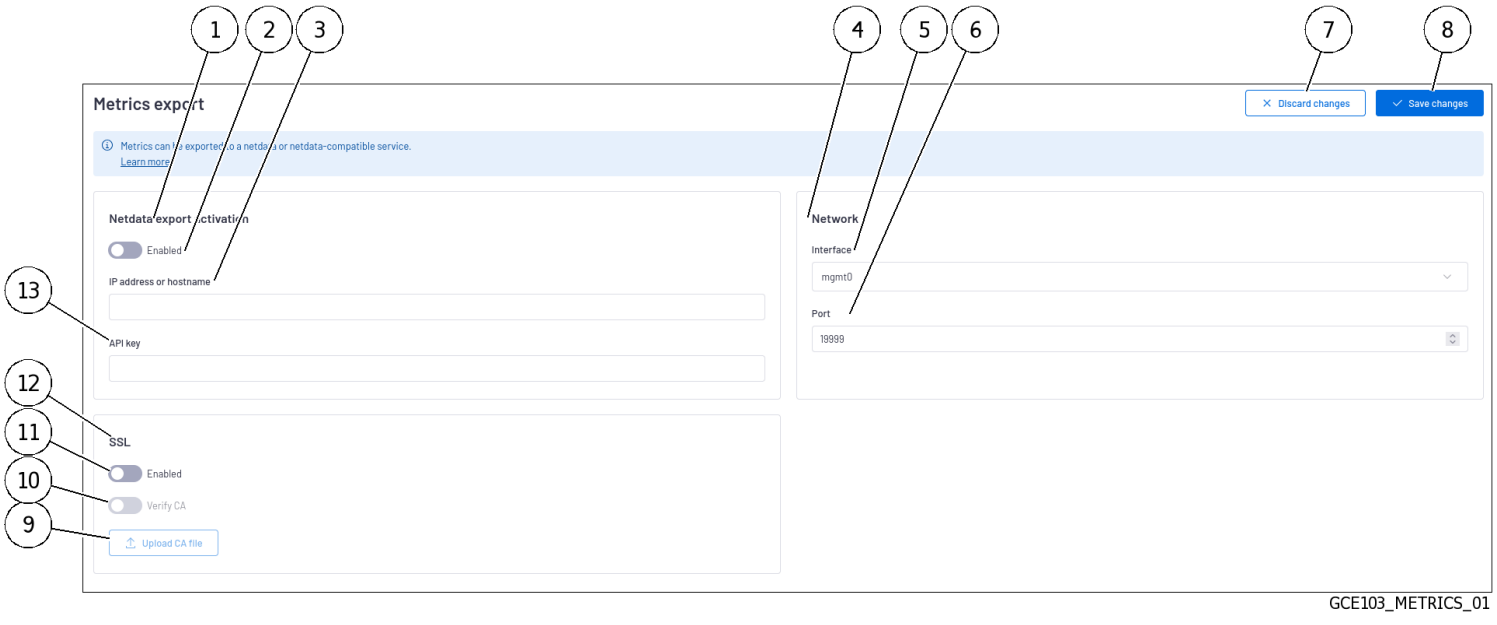
This screen is only accessible to members of the *administrator* group.

5.7.4.21.2 Links associated

For details on data management, see the *Data use*.
For implementation, see the procédure *Configuring the Netdata export interface*.

5.7.4.21.3 Screen description

After pressing the `Metrics Export` command of the `Monitoring` menu, the `Netdata Export Configuration` screen is displayed.



GCE103_METRICS_01

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

Item	Name	Function
1	`Netdata export activation` Zone	configuration of the Netdata export
2	`Enabled` selector	• Enables the netdata export
3	`IP address or hostname` field	• Enter the FQDN or IP address of the Netdata server
13	`API Key`	• Field to enter the API key of the Netdata server
4	`Network` Zone	Configuration of the Netdata network parameters
5	`Interface`	• Output interface used to reach the Netdata server

continues on next page

Table 42 – continued from previous page

Item	Name	Function
6	`Port`	• Listening port of the Netdata server
7	`Discard changes` button	Cancels current changes
8	`Save changes` button	Saves current changes
12	`SSL` zone	Configuration of the Secure Socket Layer (SSL) certificate
11	`Enabled` selector	• Enables the SSL feature
10	`Verify CA` selector	• Enables the certificate verification area by CA
9	`Upload CA file` button	• Downloads the certificate file

5.7.4.22 `Netdata polling` screen

5.7.4.22.1 Introduction

The `Netdata polling` screen configures the data access for a Nagios-like monitoring server. This reads the information on the input interface.
Authenticated users can poll the Netdata API, available on Gstats.
For simple automation, it is possible to enable a non-authenticated user to poll the API.
In this case, the API endpoint is redirected to http on the port specified below: http://<gcenter_fqdn>:<redirection_port>.
An access list restricts the client subnets for which this redirection is available.
Refer to the documentation for more help on how to use this API with monitoring tools such as Nagios.

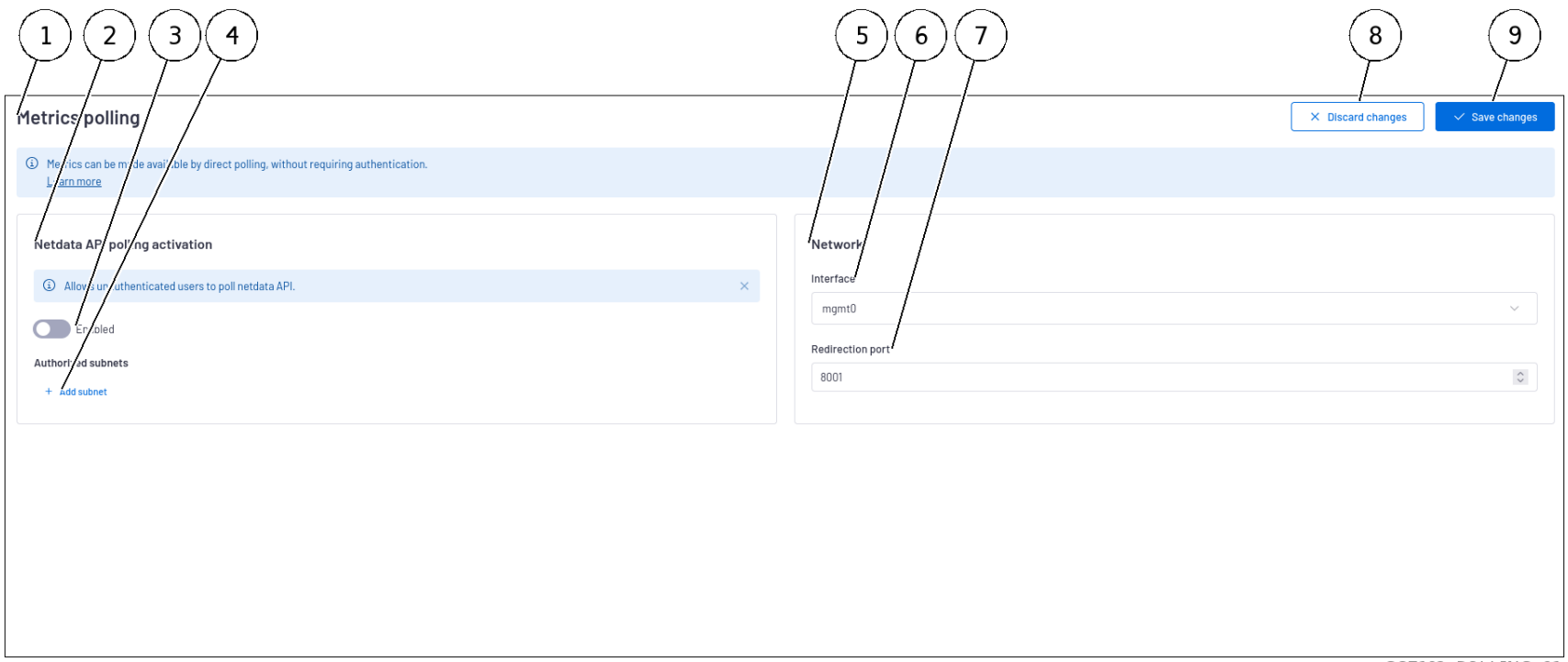
This screen is only accessible to members of the *administrator* group.

5.7.4.22.2 Links associated

For details on data management, see the *Data use*.
For implementation, see the *Configuring the Netdata polling interface*

5.7.4.22.3 Screen description

After pressing the `Metrics polling` command of the `Administration-Monitoring` menu, the `Metrics polling` screen is displayed.



GCE103_POLLING_01

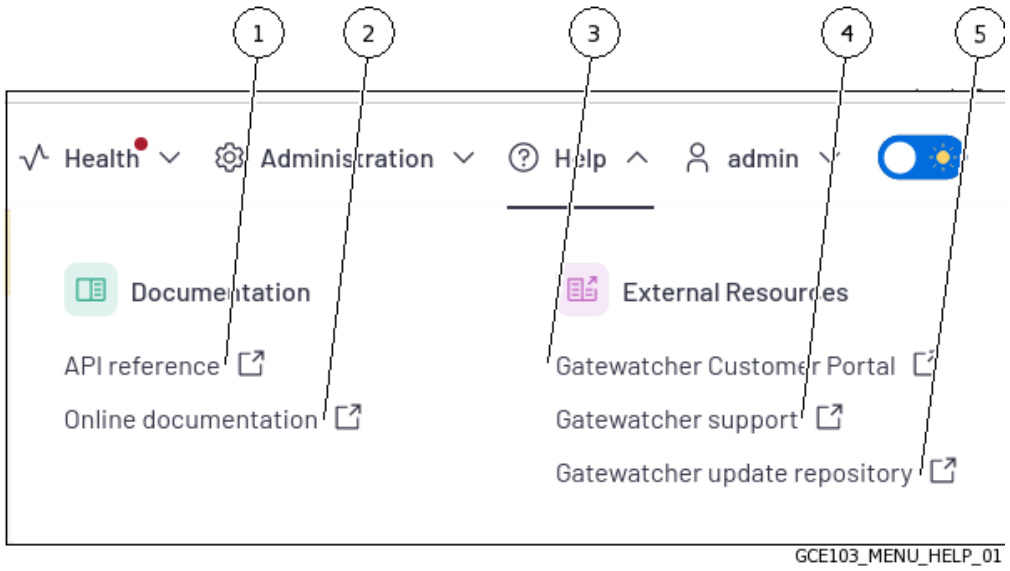
For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page.`.

Item	Name	Function
1	`Metrics polling` window	Configures the Metrics polling
2	`Netdata API polling activation` zone	Allows unauthenticated users to poll netdata API
3	`Enabled` selector	• Activates the feature
4	• `Add subnets` link	• Displays the field to enter the authorized subnets parameter
5	`Network` zone	Configures the interface to be used
6	`interface` field	• Gcenter used interface
7	`Redirection port` field	• Used redirection port
8	`Discard changes` button	Cancels current changes
9	`Save changes` button	Saves current changes

5.7.5 `Help` menu

5.7.5.1 Overview of the `Help` menu

The `Help` menu consists of the following:



Item	Heading	Command	Description
1	Documentation	`API reference`	Access to the Gatewatcher API See *`Gatewatcher API` screen*
2	Documentation	`Documentation`	Open the GCenter documentation See *`Gatewatcher API` screen*
3	External Resources	`Gatewatcher Customer Portal` site	Access to the Gatewatcher Customer Portal See *`Gatewatcher Customer Portal` screen*
4	External Resources	`Gatewatcher support` site	Access to the Gatewatcher support See *`Gatewatcher support` screen*
5	External Resources	`Gatewatcher update repository` site	Access to the Gatewatcher update repository See *`update.gatewatcher.com` screen*

5.7.5.2 `Gatewatcher API` screen

5.7.5.2.1 Introduction

The API is used:

- To display the list by theme of existing endpoints
- To be able to filter this list
- To know all the information of each endpoint
- To run the endpoint
- To Know its curl command
- To Know its URL request

Note:

The API is named swagger.

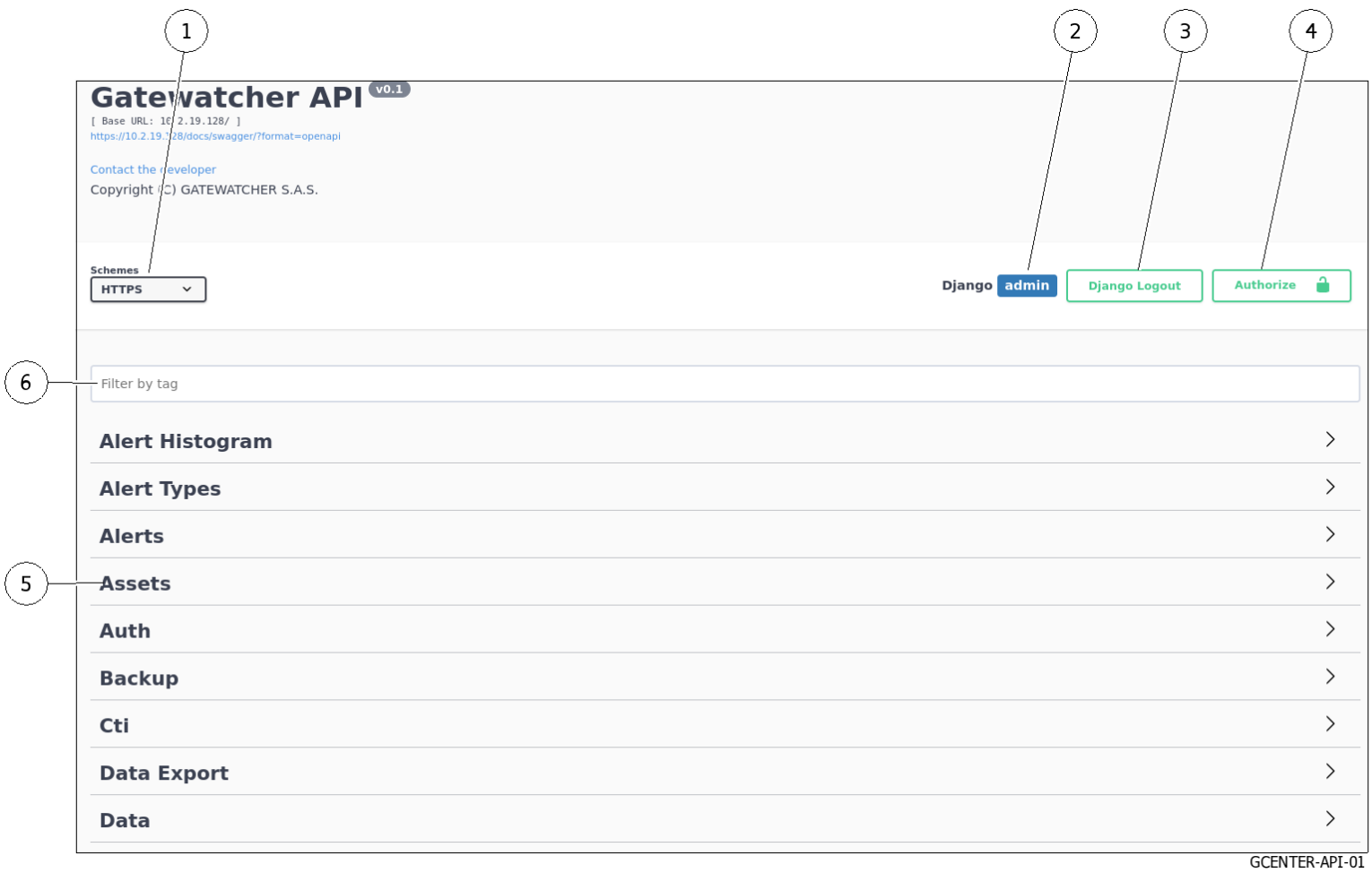
This screen is only accessible to members of the *administrator* group.

5.7.5.2.2 Links associated

For further details about the endpoints, see *Endpoints list*.

5.7.5.2.3 Screen description

After pressing the `API reference` command of the `Documentation` menu, the `Gatewatcher API` screen is displayed.



GCENTER-API-01

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page. `.

Item	Name	Function
1	`Schemes`	Parameter indicating the protocol used (HTTPS)
2	Current account name	Here account administrator
3	`Django Logout` button	Exits the API
4	`Authorize` button	Defines the necessary authentication in curl commands
5	`Assets`	Endpoints are sorted by theme (tag)
6	Filtration field	After enter the text, filters themes

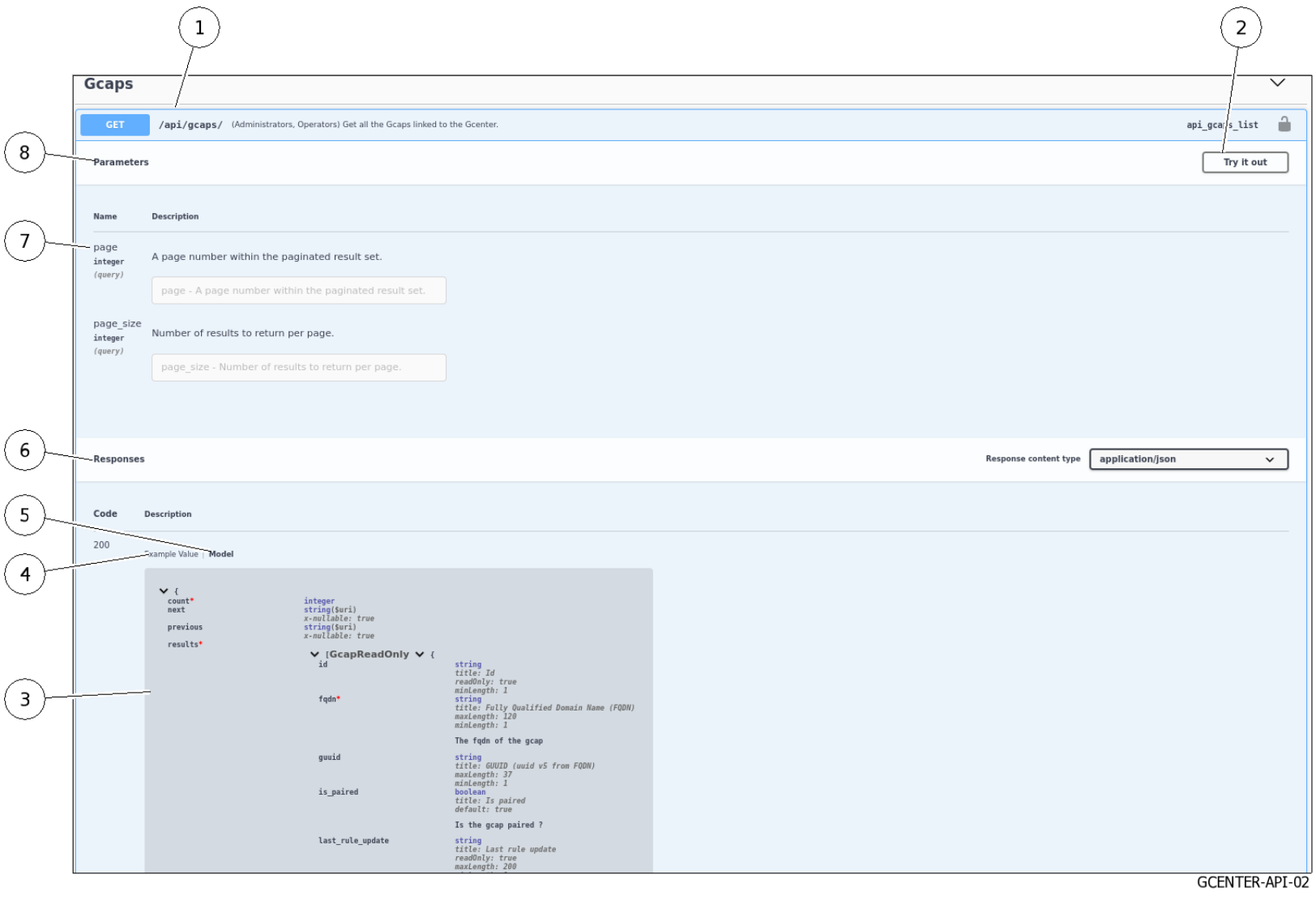
In this interface, all API endpoints are available and usable.
The use of the different endpoints is subject to the same rights as in the GCenter web interfaces.

Note:

A feature requiring administrator rights cannot be used by a user with only operator rights.

5.7.5.2.3.1 Detail for an endpoint

The information displayed for an endpoint is as follows:



GCENTER-API-02

Item	Description
1	Title line. It includes : - the action (here GET) - the name of the endpoint (here/api/gcaps) - the accesses (here Administrators and Operators) - the description of the endpoint
2	`Try it out` button: runs the endpoint with current parameters
8	Field `Parameters`: displays the optional or mandatory parameters to execute the query. For mandatory parameters, refer to the box (6). This area includes the parameters needed for the selected API. In this example, there are two: the page number and the number of results per page.
7	• Parameter `page`: enter a page number. This example depends on the API
6	• `Responses` area: area that displays information based on whether or not the `Try it out` button has been activated

Note:

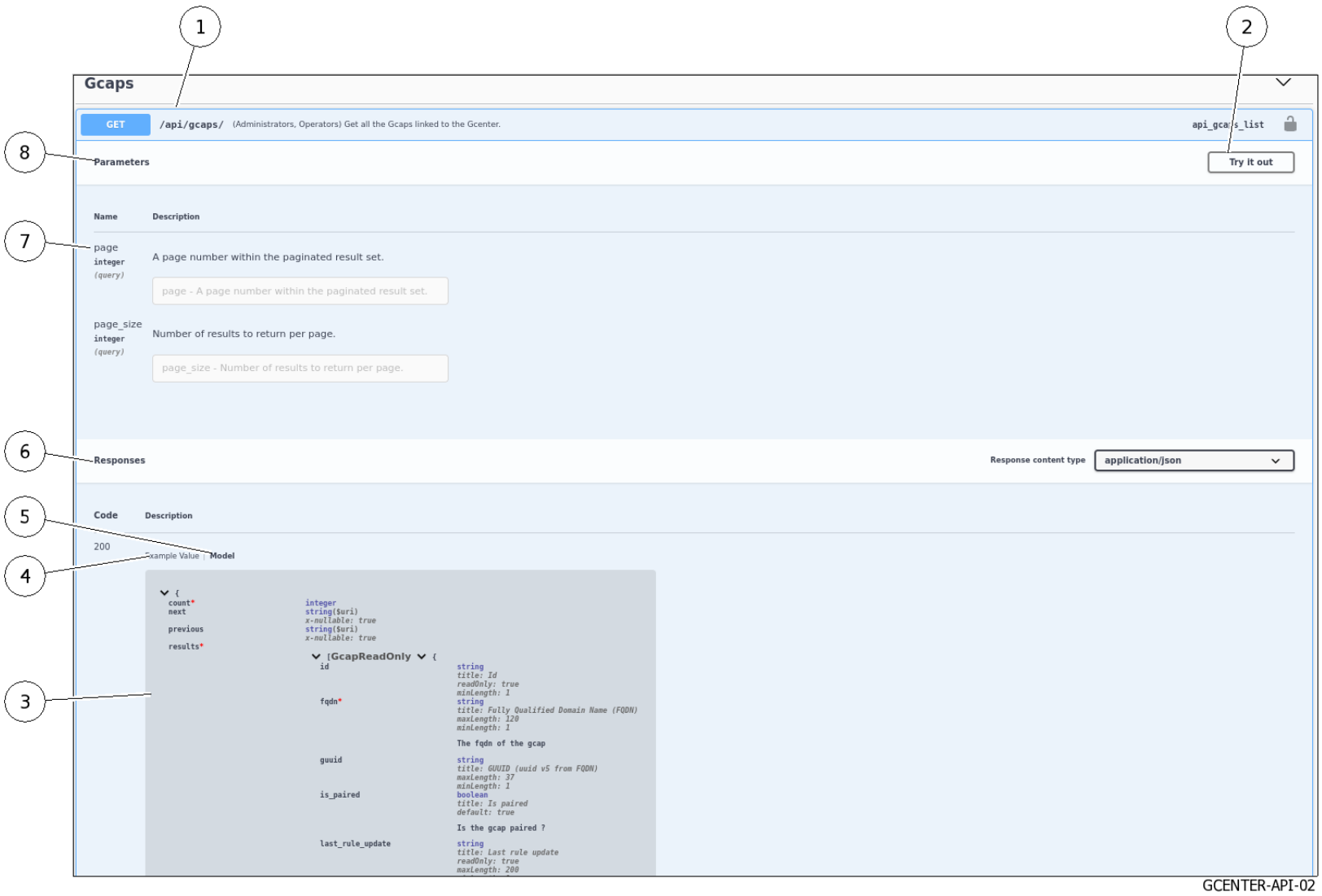
If a parameter is mandatory, an asterisk with `required` is displayed.

Note:

In this screen, it is not possible to enter parameters. To do this, you must execute the query.

5.7.5.2.3.2 Zone `Responses` if the `Try it out` button is not activated

If the `Try it out` button is not activated then the `Responses` zone contains the information for the expected response:



GCENTER-API-02

Item	Description
5	Link `Model`: by clicking on this text, the window (3) displays the model of the expected answer
4	Link `Example Value`: by clicking on this text, the window (3) displays an example of the expected response with values for example. Values are, for type **integer** (value 0), for type string (value = string), for type **boolean** (value = true)
3	Field of view: contains the content selected by the active option (4) or (5). An example of content is given below.

5.7.5.2.3.3 Sample Output Template

The output model gives the structure of the data that will be displayed as output after execution of the request.

GCENTER-API-04

Item	Description
1	`count`: number. For this parameter, its characteristics are indicated (integer).
2	`results`: expected results
3	`GcapReadOnly`: GCap settings For each parameter (id, fqdn,is_paired...), the characteristics are displayed

5.7.5.2.3.4 Example with default values

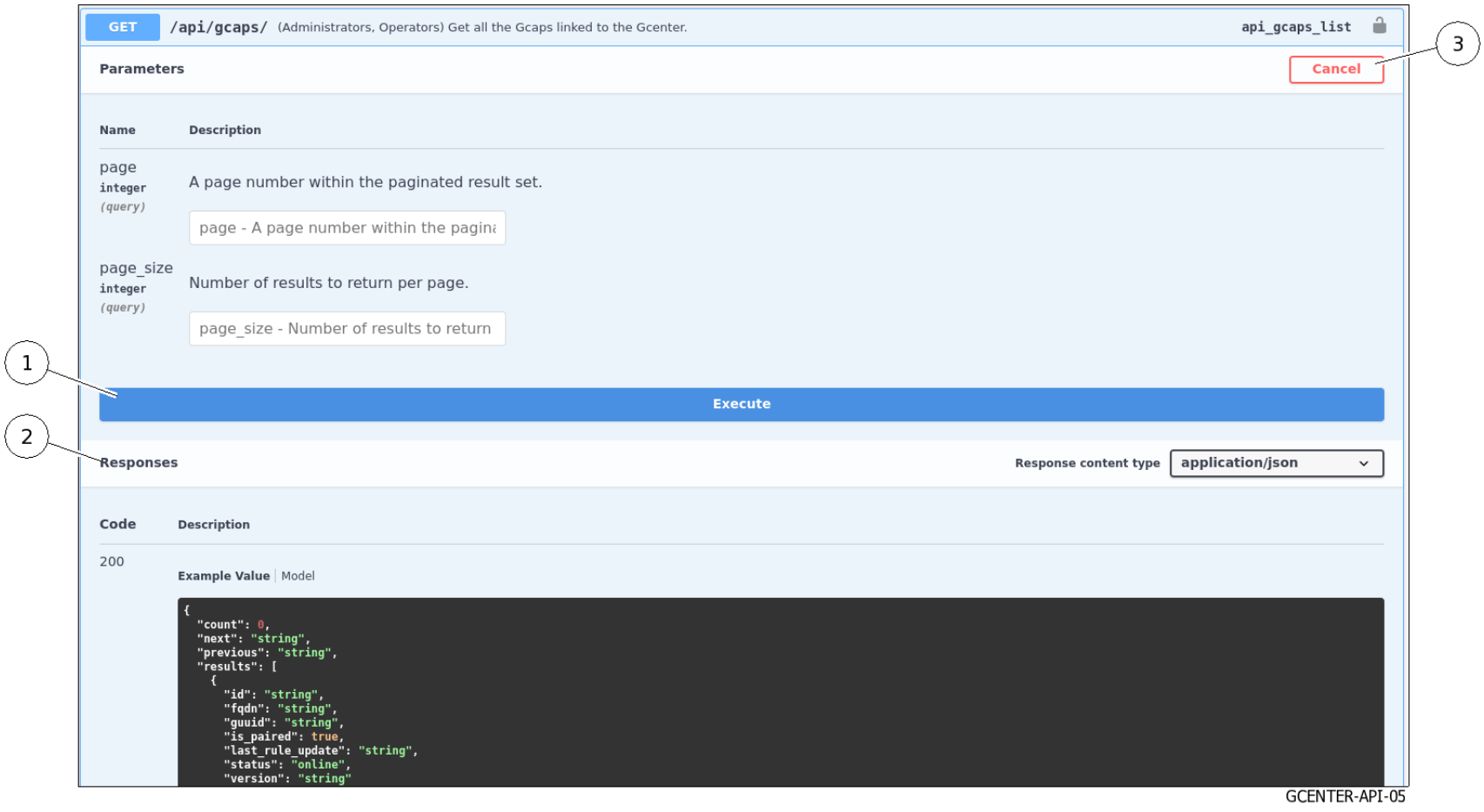
In this example, the information is displayed with the following defaults:

- Parameters of type **integer** are displayed with `0`
- Parameters of type **string** are displayed with `string` text
- Parameters of type **boolean** are displayed with `true` text

The marking is the same as in the output model.

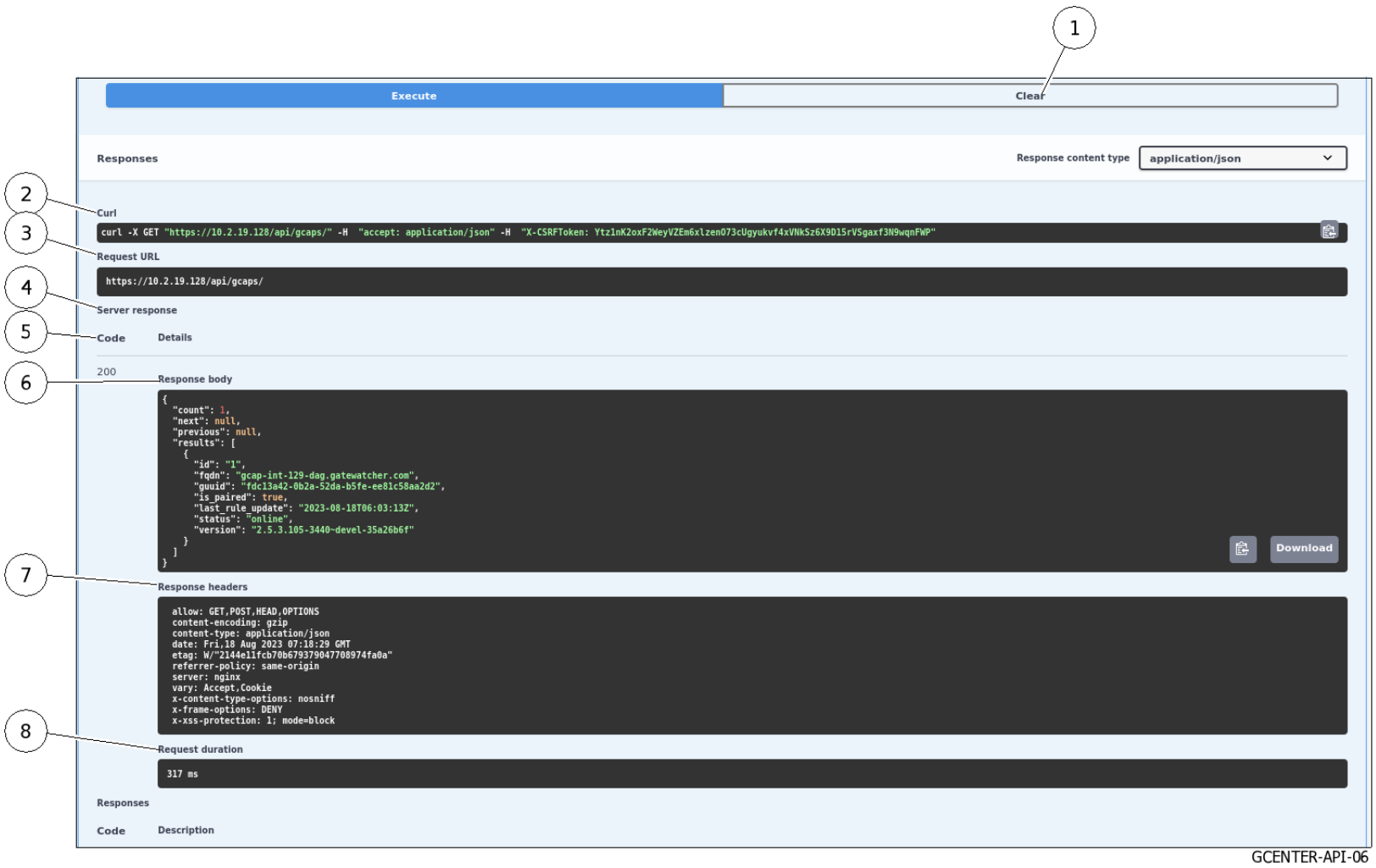
5.7.5.2.3.5 Zone `Responses` if the `Try it out` button is activated

After clicking the `Try it out` button, the parameter entry area is activated.
The following screen is displayed:



Item	Description
1	`Execute` button executes the query with the current parameters
2	`Cancel` button cancels the request
3	`Responses` zone displays the responses o the request after using the `Execute` button

After clicking the `Execute` button, the query is launched and the next window is displayed.



GCENTER-API-06

Bench-mark	Description
1	`Clear` button: returns to the state before execution
2	Display Area `Curl`: displays the Curl query
3	Display area `URL`: displays the URL request
4	Display Area `Server response`: displays the server response to the request. It includes the following
5	• `Code`: if code 200 then execution is ok. If the message `code 400 Undocumented Error Bad Request` is displayed, verify that the required parameters are entered.
6	• `Responses body`: in this section the information requested is displayed
7	• `Responses headers`: field detailing the answer header
8	• `Responses headers`: value in ms of the duration of the request

5.7.5.3 `Online documentation` screen

5.7.5.3.1 Introduction

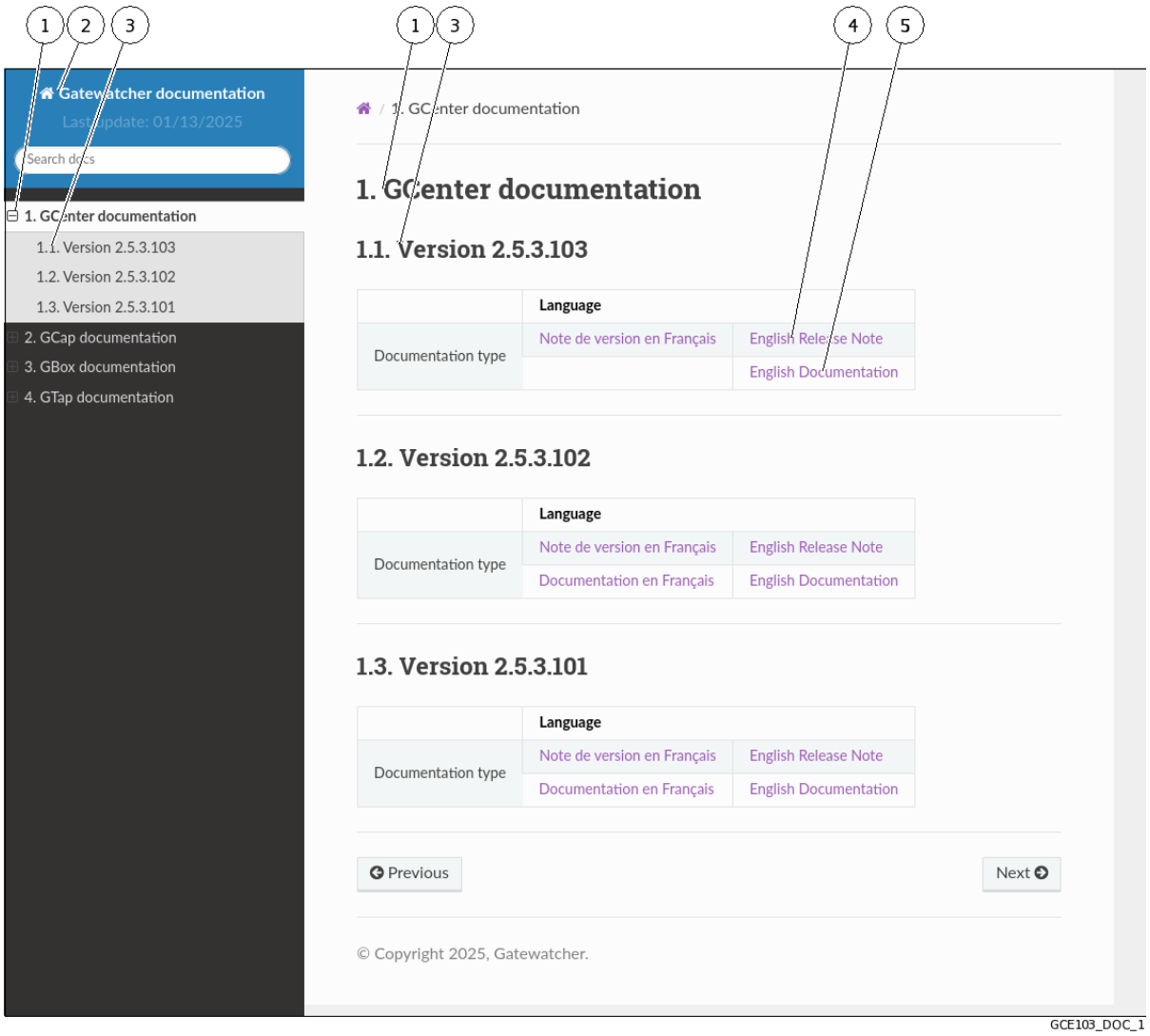
All product documentation are displayed in the https://docs.gatewatcher.com/ site.

5.7.5.3.2 Links associated

None

5.7.5.3.3 Screen description

After pressing the `Online documentation` command of the `Documentation` menu, the `GATEWATCHER DOCUMENTATION` screen is displayed.



GCE103_DOC_1

For members of the *operator* group, the following message is displayed: `Unauthorized- You don't have the permission to view this page. `.

Item	Name	Function
1	`GCenter documentation`	Link to open the list the Gcenter documentation
2	`atewatcher documentation`	Link to open the main screen
3	`Version 2.5.3.103`	List of the documentation for this version
4	`English Release Note`	Link to open this document in HTML format
5	`English Documentation`	Link to open this document in HTML format

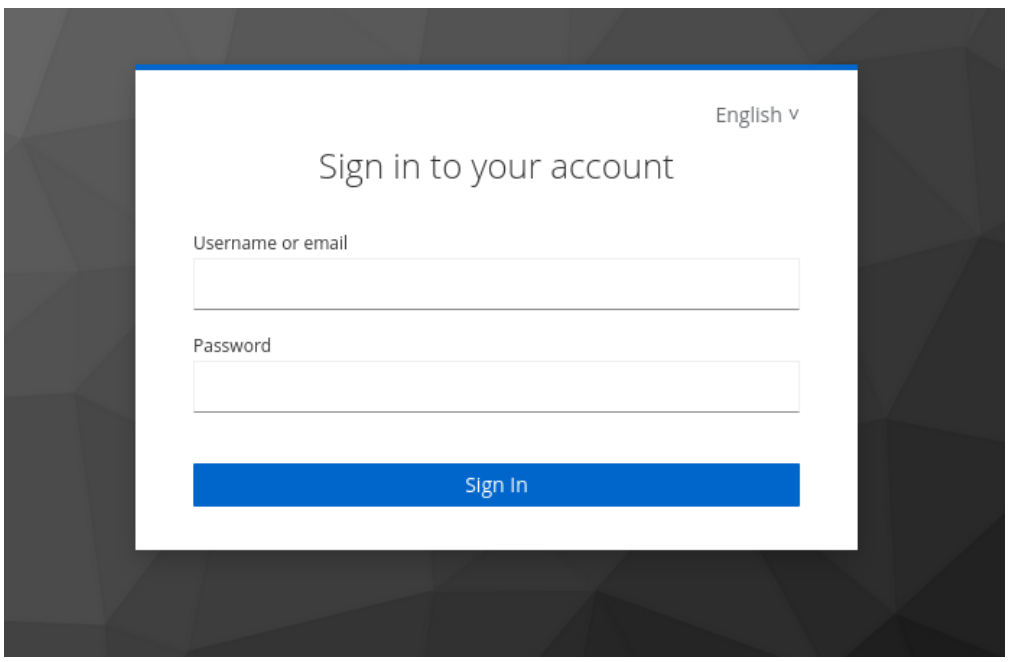
5.7.5.4 `Gatewatcher Customer Portal` screen

5.7.5.4.1 Introduction

The Gatewatcher customer portal give information to its customer with control access.

5.7.5.4.2 Screen description

After pressing the `Gatewatcher Customer Portal` command of the `Help` menu, the `Gatewatcher Customer Portal` screen is displayed.



- Enter the username or email
- Enter the password
- Validate with the `Sign In` button

To contact the Gatewatcher support use the mail tac@gatewatcher.com or https://tac.gatewatcher.com

---

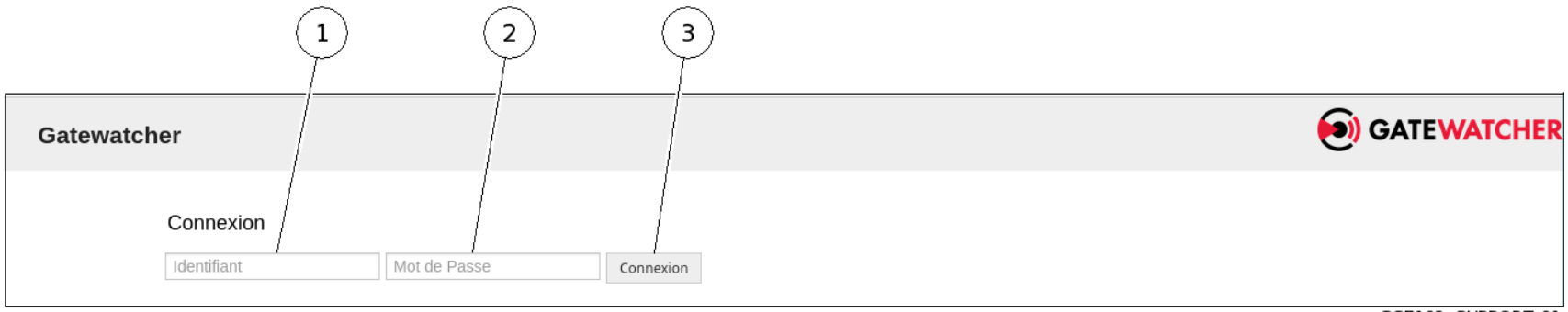
5.7.5.5 `Gatewatcher support` screen

5.7.5.5.1 Introduction

The site allows customers to contact support.

5.7.5.5.2 Screen description

After pressing the `Gatewatcher Customer Portal` command of the `Help` menu, the `Gatewatcher Customer Portal` screen is displayed.



GCE103_SUPPORT-01

- Enter the username (1).
- Enter the password (2).
- Validate with the `Connexion` button (3).

To contact the Gatewatcher support use the mail tac@gatewatcher.com or https://tac.gatewatcher.com

---

5.7.5.6 `update.gatewatcher.com` screen

5.7.5.6.1 Introduction

The `update.gatewatcher.com` site allows customers to upload the update files.

5.7.5.6.2 Screen description

After pressing the `Gatewatcher update repository` command of the `Help` menu, the Internet browser is opened and the control access is activated.

- Enter the username.
- Enter the password.
- Validate.

To contact the Gatewatcher support use the mail tac@gatewatcher.com or https://tac.gatewatcher.com

---

5.8 Graphical API

5.8.1 Overview of the API interface

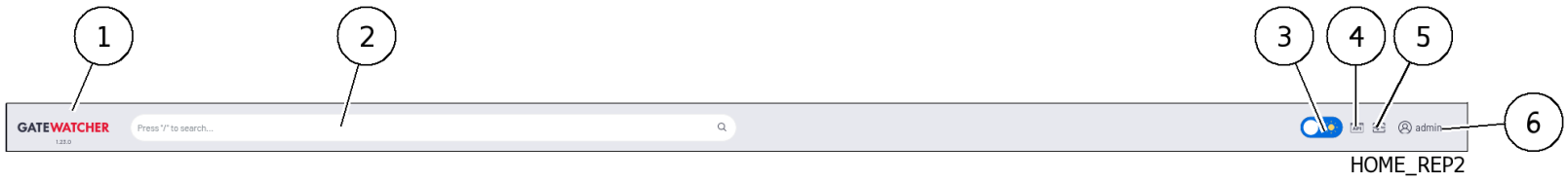
The API allows:

- To display the list by theme of existing endpoints
- To be able to filter this list
- To know all the information of each endpoint
- To run the endpoint,
- To know its curl command
- To know its URL request

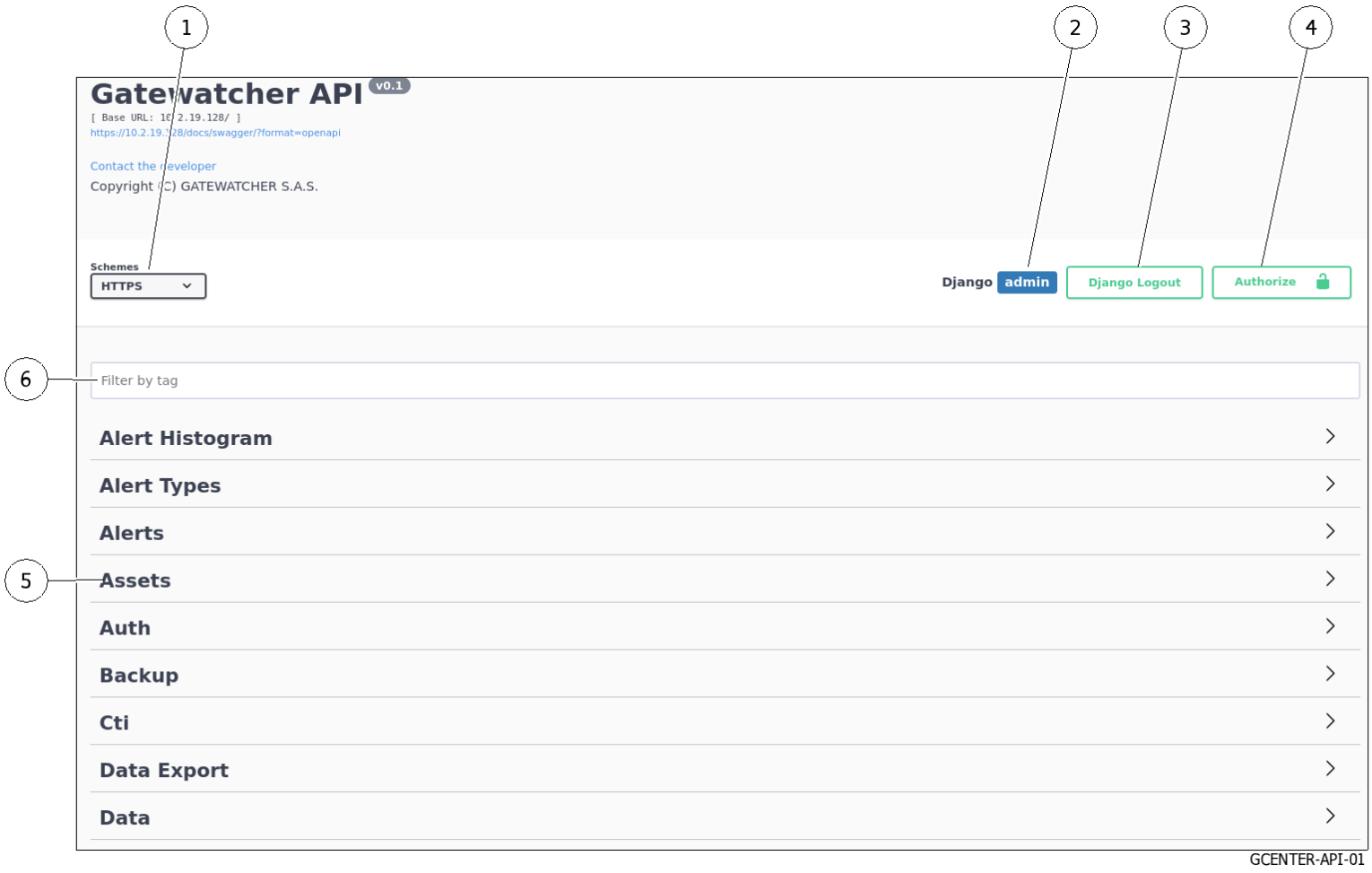
Note:

The API is named swagger.

Access to this interface is available in the title bar of the main interface.



After pressing the `API` button (4) of the title bar, the following screen is displayed.
The window includes:



Item	Description
1	`Schemes`: parameter indicating the protocol used (HTTPS)
2	Current account name: here account administrator
3	`Django Logout` button: allows to exit the API
4	Button `Authorize`: allows to define the necessary authentication in curl commands
5	Endpoints are sorted by theme (tag)
6	Filtration field: allows to filter themes

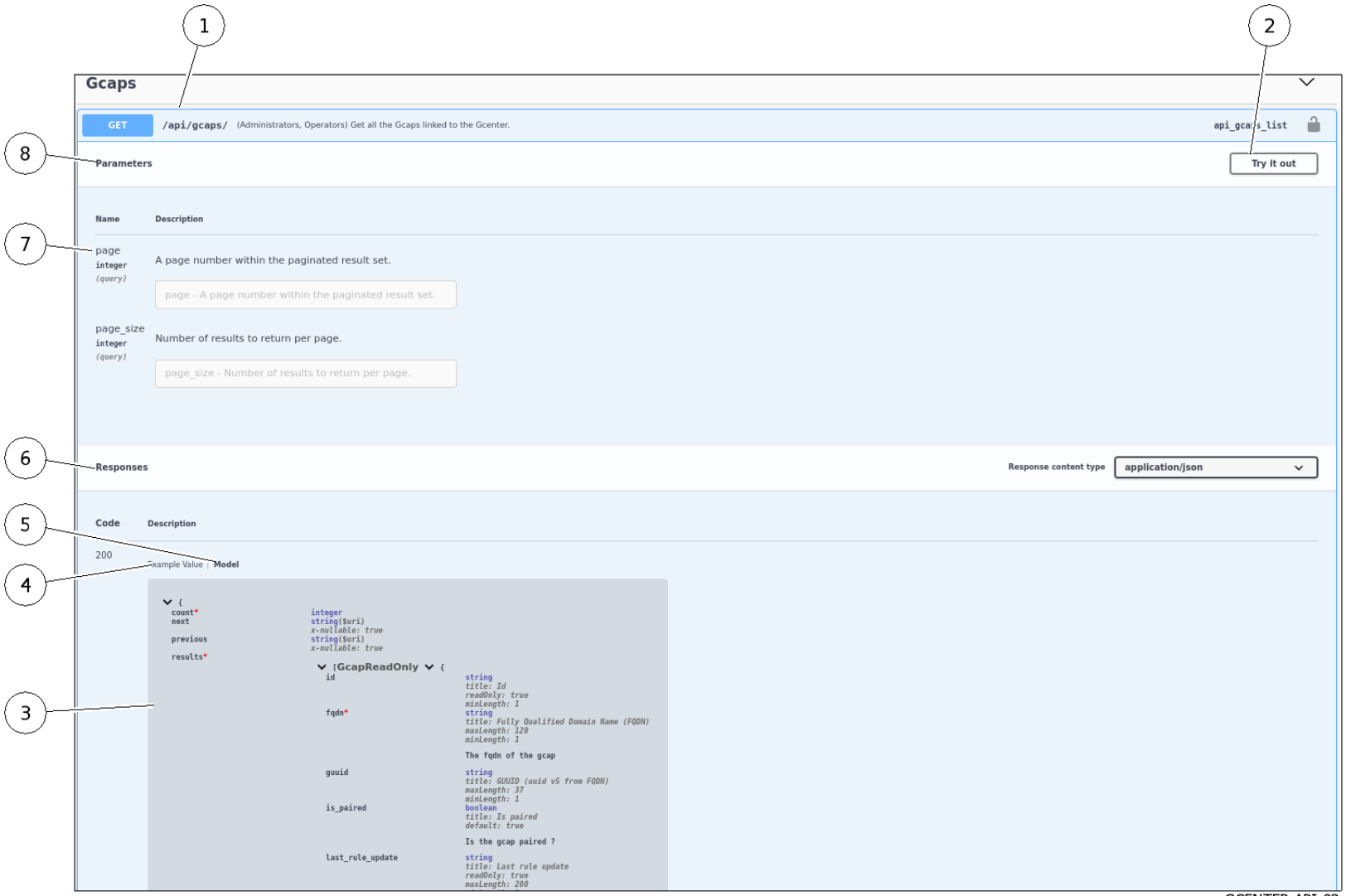
In this interface, all API endpoints are available and usable.
The use of the different endpoints is subject to the same rights as in the GCenter web interfaces.

Note:

A feature requiring administrator rights cannot be used by a user with only operator rights.

5.8.1.1 Detail for an endpoint

The information displayed for an endpoint is as follows:



Item	Description
1	Title line. It includes the action (here GET), the name of the endpoint (here/api/gcaps), the accesses (here Administrators and Opertors), the description of the endpoint
2	`Try it out` button: runs the endpoint with current parameters
8	Field `Parameters`: displays the optional or mandatory parameters to execute the query. For mandatory parameters, refer to the box (6). This area includes the parameters needed for the selected API. In this example, there are two: the page number and the number of results per page.
7	• Parameter `page`: enter a page number. This example depends on the API
6	• `Responses` area: area that displays information based on whether or not the `Try it out` button has been activated

Note:

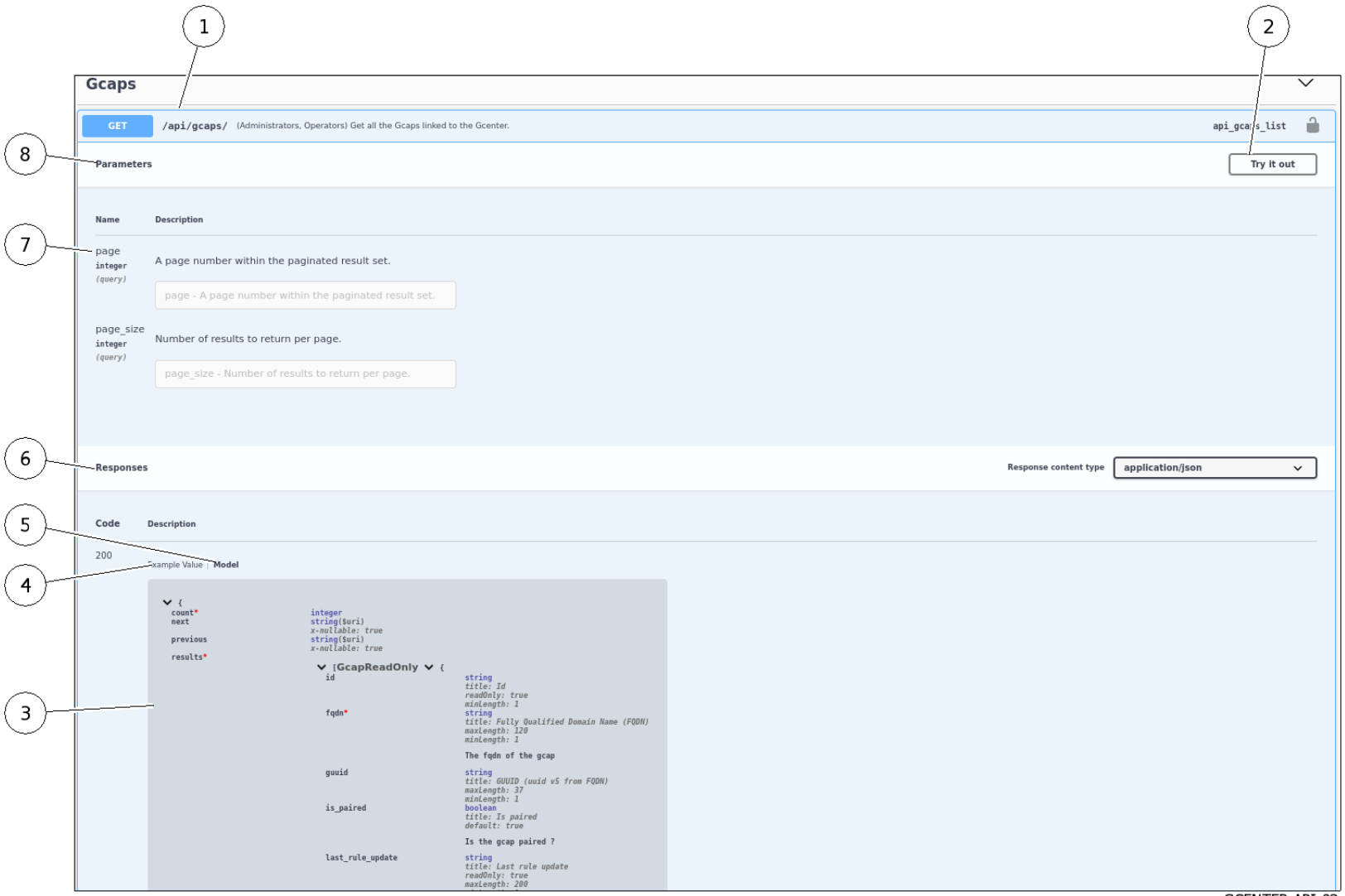
If a parameter is mandatory, an asterisk with `required` is displayed.

Note:

In this screen, it is not possible to enter parameters. To do this, you must execute the query.

5.8.1.1.1 Zone `Responses` if the `Try it out` button is not activated

If the `Try it out` button is not activated then the `Responses` zone contains the information for the expected response:



Item	Description
5	Link `Model`: by clicking on this text, the window (3) displays the model of the expected answer
4	Link `Example Value`: by clicking on this text, the window (3) displays an example of the expected response with values for example. Values are, for type **integer** (value 0), for type string (value = string), for type **boolean** (value = true)
3	Field of view: contains the content selected by the active option (4) or (5). An example of content is given below.

@Copyright: December 2024, Gatewatcher

5.8.1.1.1.1 Sample Output Template

The output model gives the structure of the data that will be displayed as output after execution of the request.

Item	Description
1	`count`: number. For this parameter, its characteristics are indicated (integer).
2	`results`: expected results
3	`GcapReadOnly`: GCap settings For each parameter (id, fqdn,is_paired...), the characteristics are displayed

5.8.1.1.2 Example with default values

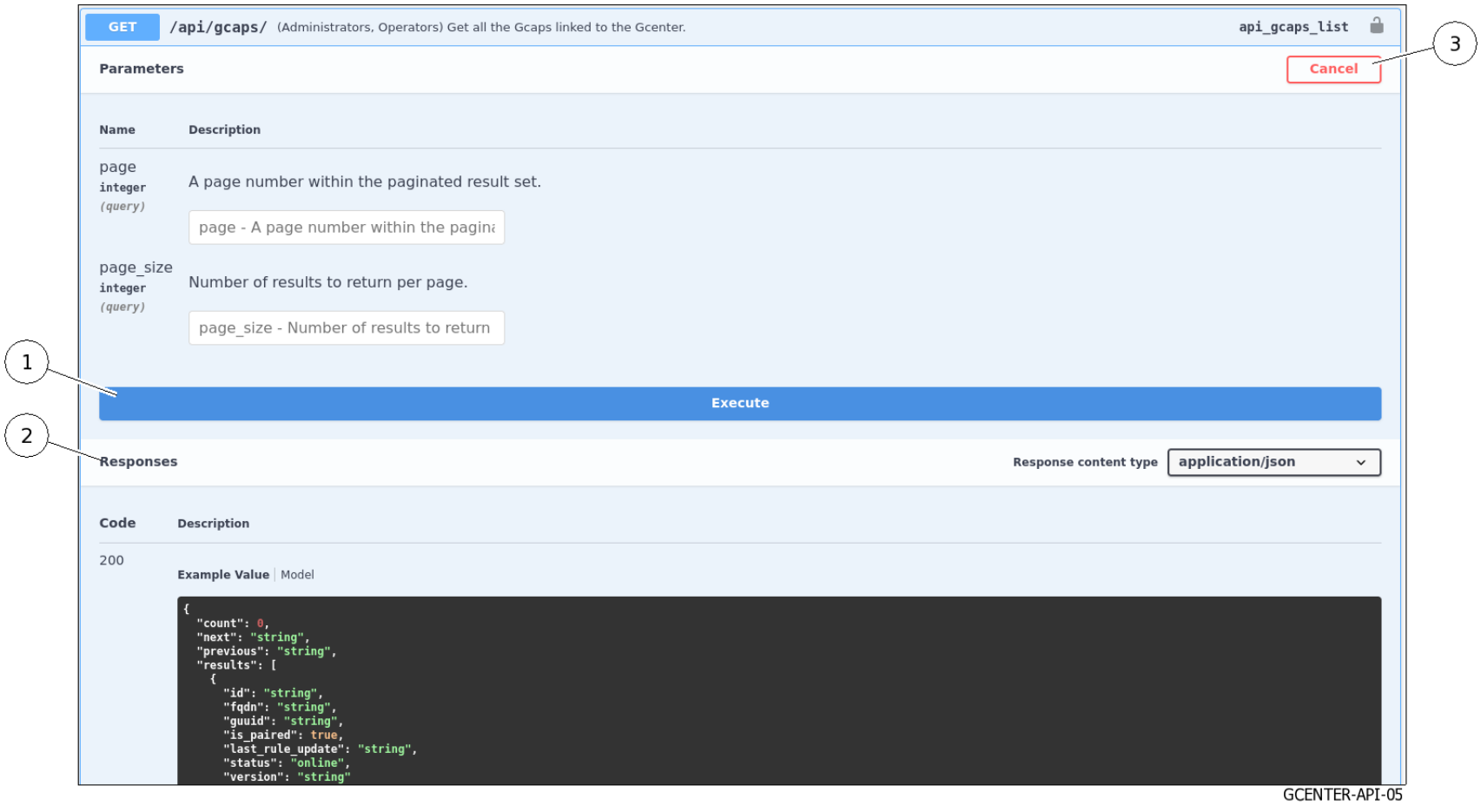
In this example, the information is displayed with the following defaults:

- Parameters of type **integer** are displayed with `0`
- Parameters of type **string** are displayed with `string` text
- Parameters of type **boolean** are displayed with `true` text

The marking is the same as in the output model.

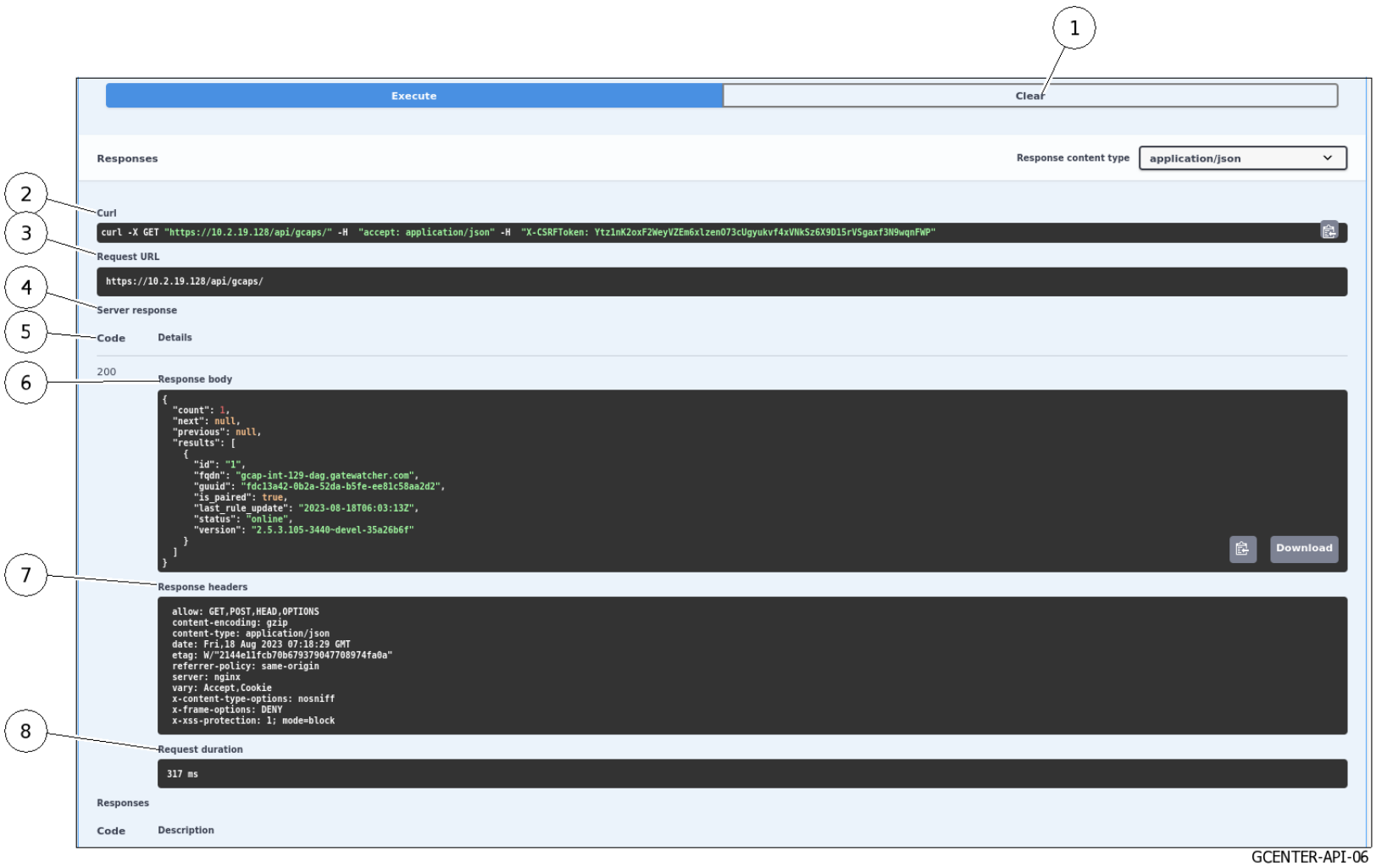
5.8.1.1.3 Zone `Responses` if the `Try it out` button is activated

After clicking the `Try it out` button, the parameter entry area is activated.
The following screen is displayed:



Item	Description
1	`Execute` button executes the query with the current parameters
2	`Responses` zone has not changed
3	`Cancel` button: cancels the request

After clicking the `Execute` button, the query is launched and the next window is displayed.



GCENTER-API-06

Item	Description
1	`Clear` button returns to the state before execution
2	Display Area `Curl` displays the Curl query
3	Display area `URL` displays the URL request
4	Display Area `Server response` displays the server response to the request. It includes the following
5	• `Code`: if code 200 then execution is ok. If the message `code 400 Undocumented Error Bad Request` is displayed, verify that the required parameters are entered.
6	• `Responses body`: in this section the information requested is displayed
7	• `Responses headers`: field detailing the answer header
8	• `Request duration`: value in ms of the duration of the request

5.8.2 Endpoints list

Note:

In the table below the legend is:
- Ope : operators role
- Adm : administrator role
- WAuth : Without Authentication
- AUser : Authenticated User

Table 43: Alert Histogram

Theme	Name	Verb	Role	Description
Alert Histogram	/alert-histogram/	GET	Ope	Returns a heat map aggregation

Table 44: Alert Types

Theme	Name	Verb	Role	Description
Alert Types	/alert-types/	GET	Ope	Get the sorted alert type by risk / number of alerts

Table 45: Alerts

Theme	Name	Verb	Role	Description
Alerts	/alerts/	GET	Ope	Get the alerts
Alerts	/alerts/	DELETE	Adm	Delete the alerts that occurred in the given date range
Alerts	/alerts/action/{action}/	PUT	Ope	Displays the alerts list
Alerts	/alerts/clusters/	GET	Ope	Return alert clusters
Alerts	/alerts/{pk_or_uuid}/	GET	Ope	Get one alert details
Alerts	alerts/{uuid}/note/	PUT	Ope	Update the note for a given instance
Alerts	/alerts/{uuid}/note/	DELETE	Ope	Clear the note content for a given instance
Alerts	/alerts/{uuid}/tags/	GET	Ope	Get the tags for a given instance
Alerts	/alerts/{uuid}/tags/	PUT	Ope	Update the tags for a given instance

Table 46: Assets

Theme	Name	Verb	Role	Description
Assets	/assets/	GET	Ope	Retrieves a list of assets
Assets	/assets/{asset_name}/	GET	Ope	Retrieve a specific asset data
Assets	/assets/{asset_name}/alerts/	GET	Ope	Get the alerts for a specific asset
Assets	/assets/{asset_name}/clusters/	GET	Ope	Return alert clusters for the corresponding asset
Assets	/assets/{asset_name}/ips/	GET	Ope	Get the list of ips related to an asset
Assets	/assets/{asset_name}/note/	PUT	Ope	Update the note for a given instance
Assets	/assets/{asset_name}/note/	DELETE	Ope	Clear the note content for a given instance
Assets	/assets/{asset_name}/tags/	GET	Ope	Get the tags for a given instance
Assets	/assets/{asset_name}/tags/	PUT	Ope	Update the tags for a given instance
Assets	/assets/{asset_name}/urls/	GET	Ope	Get the list of urls related to an asset through an alert

Table 47: Auth

Theme	Name	Verb	Role	Description
Auth	/auth/login/	POST	WAuth	Initiate a new session
Auth	/auth/logout/	POST	WAuth	Terminate session
Auth	/auth/tokens/	GET	Adm	Get all the API authentication Tokens
Auth	/auth/tokens/	POST	Adm	Generate an API authentication token
Auth	/auth/tokens/{id}/	GET	Adm	Get a API authentication token data
Auth	/auth/tokens/{id}/	DELETE	Adm	Delete an API authentication token

Table 48: Auto Threshold

Theme	Name	Verb	Role	Description
Auto Threshold	/auto-threshold/	GET	Ope	Displays the current auto thresholds
Auto Threshold	/auto-threshold/	PUT	Ope	Update the auto thresholds
Auto Threshold	/auto-threshold/presets/	GET	Ope	Displays the predefined auto thresholds
Auto Threshold	/auto-threshold/reset/	POST	Ope	Resets the predefined auto thresholds

Table 49: Backups

Theme	Name	Verb	Role	Description
Backups	/backups/	GET	Adm	Get the backup list
Backups	/backups/	POST	Adm	Create a backup
Backups	/backups/config/	GET	Adm	Get the Backup config
Backups	/backups/config/	PUT	Adm	Update the Backup config
Backups	/backups/config/check/	POST	Adm	Test the remote scheduled config
Backups	/backups/restore/	POST	Adm	Restore a backup with file upload
Backups	/backups/status/	GET	Adm	Get the backup status
Backups	/backups/{name}/download/	GET	Adm	Download a backup
Backups	/backups/{name}/restore/	POST	Adm	Restore a backup

Table 50: Beacon Detect

Theme	Name	Verb	Role	Description
Beacon Detect	/beacon-detect/settings/	GET	Ope	Get the Beacon detect settings
Beacon Detect	/beacon-detect/settings/	PUT	Ope	Update the Beacon detect settings
Beacon Detect	/beacon-detect/white-list/	GET	Ope	Get the Beacon detect destinations white list
Beacon Detect	/beacon-detect/white-list/	POST	Ope	Add a destination to the white list
Beacon Detect	/beacon-detect/white-list/hints	GET	Ope	Get destination hints for white list
Beacon Detect	/beacon-detect/white-list/{destination}	DELETE	Ope	Delete a destination from the white list

Table 51: CTI

Theme	Name	Verb	Role	Description
Cti	/cti/license/	GET	Adm	Get the LIS license key and details
Cti	/cti/license/	PUT	Adm	Update the LIS license key
Cti	/cti/settings/	GET	Ope	Get the current LIS configuration
Cti	/cti/settings/	PUT	Adm	Update the current LIS configuration

Table 52: Data Export

Theme	Name	Verb	Role	Description
Data Export	/data-export/netdata/	GET	Adm	Get the current netdata export configuration
Data Export	/data-export/netdata/	PUT	Adm	Update the current netdata export configuration
Data Export	/data-export/syslog/{id}/	GET	Adm	Get the current syslog export configuration
Data Export	/data-export/syslog/{id}/	PUT	Adm	Update the current syslog export configuration

Table 53: Data

Theme	Name	Verb	Role	Description
Data	/data/es/search/	POST	Adm, Ope	Execute an Elasticsearch Search on Gcenter data

Table 54: Delete Data

Theme	Name	Verb	Role	Description
Delete Data	/delete-data/	DELETE	Adm	Delete data
Delete Data	/delete-data/	OPTIONS	Adm	Defines the mapping of delete data names and their corresponding primary keys
Delete Data	/delete-data/status/	GET	Adm	Get the data deletion status

Table 55: Device Types

Theme	Name	Verb	Role	Description
Device Types	/device-types/	GET	Ope	Retrieves the list of asset types

Table 56: Dga Detection

Theme	Name	Verb	Role	Description
Dga Detection	/dga-detection/settings/	GET	Ope	Get the DGA detection management settings
Dga Detection	/dga-detection/settings/	PUT	Ope	Update the DGA detection management settings
Dga Detection	/dga-detection/top-domains/	GET	Ope	Get the DGA detection whitelist hints
Dga Detection	/dga-detection/{list_type}-list/	GET	Ope	Get the domain name white/black list
Dga Detection	dga-detection/{list_type}-list/	POST	Adm	Add a domain name to the white/black list
Dga Detection	/dga-detection/{list_type}-list/load	PUT	Adm	Update the white/black list from a csv file
Dga Detection	/dga-detection/{list_type}-list/{domain_name}	DELETE	Adm	Delete a domain name from the white/black list

Table 57: Diagnostics

Theme	Name	Verb	Role	Description
Diagnostics	/diagnostics/logs/	GET	Adm	Download the file
Diagnostics	/diagnostics/logs/	PUT	Adm	Generate/Update the file asynchronously
Diagnostics	/diagnostics/logs/status/	GET	Adm	Get the file's generation status
Diagnostics	/diagnostics/tech-support/	GET	Adm	Download the file
Diagnostics	/diagnostics/tech-support/	PUT	Adm	Generate/Update the tech support file asynchronously
Diagnostics	/diagnostics/tech-support/status/	GET	Adm	Get the file's generation status

Table 58: Entities

Theme	Name	Verb	Role	Description
Entities	/entities/	DELETE	Adm	Delete the entities records that occurred in the given date range
Entities	/entities/count/	GET	Ope	Retrieve the total count of the different entities for the given date range

Table 59: External Modules

Theme	Name	Verb	Role	Description
External Modules	/external-modules/gresponse/	GET	Adm, Ope	Get the GResponse settings
External Modules	/external-modules/gresponse/	PUT	Adm	Set the GResponse settings
External Modules	/external-modules/intelligence/	GET	Adm	Get the intelligence interconnection configuration
External Modules	/external-modules/intelligence/	POST	Adm	Test the interconnection with the current saved configuration
External Modules	/external-modules/intelligence/	PUT	Adm	Update the intelligence interconnection configuration
External Modules	/external-modules/intelligence/status/	GET	Adm,Ope	Get the intelligence status
External Modules	/external-modules/misp/	GET	Adm	Get the MISP configuration
External Modules	/external-modules/misp/	PUT	Adm	Update the MISP configuration
External Modules	/external-modules/misp/status/	GET	Adm, Ope	Get the MISP status
External Modules	/external-modules/misp/updates/	GET	Ope	Get all MISP generations
External Modules	/external-modules/misp/updates/	POST	Ope	Add a MISP generation
External Modules	/external-modules/misp/updates/settings/	GET	Ope	Get the automatic generation settings
External Modules	/external-modules/misp/updates/settings/	PUT	Ope	Set the automatic generation settings

Table 60: Gcaps Health Checks

Theme	Name	Verb	Role	Description
Gcaps Health Checks	/gcaps-health-checks/	GET	Adm, Ope	Get the health check

Table 61: Gcaps

Theme	Name	Verb	Role	Description
Gcaps	/gcaps/	GET	Adm, Ope	Get all the Gcaps linked to the Gcenter
Gcaps	/gcaps/	POST	Adm	Pair a new gcap
Gcaps	/gcaps/vpn/	GET	Adm	Get the VPN interface data used by the GCenter/Gcap connexion
Gcaps	/gcaps/{id}/	GET	Adm, Ope	Get a Gcap's data
Gcaps	/gcaps/{id}/	DELETE	Adm	Delete a GCap
Gcaps	/gcaps/{id}/files-rules/	GET	Ope	Get all files rules of a Gcap
Gcaps	/gcaps/{id}/files-rules/	POST	Ope	Create a Gcap files rule configuration
Gcaps	/gcaps/{id}/files-rules/load/	PUT	Ope	Update the gcap files rule from a csv file
Gcaps	/gcaps/{id}/files-rules/template/	GET	Ope	Get the csv template of the gcap files rules config
Gcaps	/gcaps/{id}/files-rules/{id_rule}/	GET	Ope	Get a Gcap files rule configuration
Gcaps	/gcaps/{id}/files-rules/{id_rule}/	PUT	Ope	Update a Gcap files rule configuration
Gcaps	/gcaps/{id}/files-rules/{id_rule}/	DELETE	Ope	Remove a Gcap files rule configuration
Gcaps	/gcaps/{id}/flows-timeouts/	GET	Ope	Get all flows timeouts of a Gcap
Gcaps	/gcaps/{id}/flows-timeouts/{id_flow}/	GET	Ope	Get a flows timeouts details of a Gcap
Gcaps	/gcaps/{id}/flows-timeouts/{id_flow}/	PUT	Ope	Update a flows timeouts details of a Gcap
Gcaps	/gcaps/{id}/interfaces	GET	Adm, Ope	Get the Gcap's available network interfaces
Gcaps	/gcaps/{id}/packet-filters	GET	Ope	Get the list of the packet filtering configuration of a Gcap
Gcaps	/gcaps/{id}/packet-filters/	POST	Ope	Add a packet filtering configuration for a Gcap
Gcaps	/gcaps/{id}/packet-filters/	OPTIONS	Ope	Get the list of protocols, each with a name and corresponding port configuration
Gcaps	/gcaps/{id}/packet-filters-default-vlans	GET	Ope	Get all the packet filters default vlan of gcap interfaces
Gcaps	/gcaps/{id}/packet-filters-default-vlans/{interface_name}	GET	Ope	Get the packet filters default vlan of a gcap interface
Gcaps	/gcaps/{id}/packet-filters-default-vlans/{interface_name}	PUT	Ope	Update the packet filters default vlan of a gcap interface
Gcaps	/gcaps/{id}/packet-filters/{packet}	GET	Ope	Get a packet filtering configuration of a Gcap
Gcaps	/gcaps/{id}/packet-filters/{packet}	DELETE	Ope	Remove a packet filtering configuration of a Gcap
Gcaps	/gcaps/{id}/profile/	GET	Ope	Get a Gcap's profile configuration
Gcaps	/gcaps/{id}/profile/	PUT	Ope	Update a Gcap's profile configuration

continues on next page

Table 61 – continued from previous page

Theme	Name	Verb	Role	Description
Gcaps	/gcaps/{id}/profile/	OPTIONS	Ope	Get the profile
Gcaps	/gcaps/{id}/profile/apply/	POST	Ope	Apply a gcap configuration if changed
Gcaps	/gcaps/{id}/profile/memcap/	GET	Ope	Get a Gcap's memcap profile configuration
Gcaps	/gcaps/{id}/profile/memcap/	PUT	Ope	Update a Gcap's memcap profile configuration
Gcaps	/gcaps/{id}/repair/	POST	Adm	Repair a GCap
Gcaps	/gcaps/{id}/reset-profile/	POST	Ope	Reset the gcap profile
Gcaps	/gcaps/{id}/reset-tenant/	POST	Ope	Reset the single/multi tenant configuration
Gcaps	/gcaps/{id}/tenants/	GET	Ope	Get the tenant list
Gcaps	/gcaps/{id}/tenants	POST	Ope	Add a new tenant
Gcaps	/gcaps/{id}/tenants-settings/	GET	Ope	Get the tenants settings
Gcaps	/gcaps/{id}/tenants-settings/	PUT	Ope	Update the tenants settings
Gcaps	/gcaps/{id}/tenants/{id_tenant}	PUT	Ope	Update a tenant
Gcaps	/gcaps/{id}/tenants/{id_tenant}	DELETE	Ope	Remove a tenant
Gcaps	/gcaps/{id}/tenants/{tenant_pk}/variables	GET	Ope	Get all ruleset variables of a Gcap tenant
Gcaps	/gcaps/{id}/tenants/{tenant_pk}/variables	POST	Ope	Create a new ruleset variables of a Gcap tenant
Gcaps	/gcaps/{id}/tenants/{tenant_pk}/variables-settings/	GET	Ope	Get the ruleset network variable settings of a Gcap tenant
Gcaps	/gcaps/{id}/tenants/{tenant_pk}/variables-settings/	PUT	Ope	Update the ruleset variables settings of a Gcap tenant
Gcaps	/gcaps/{id}/tenants/{tenant_pk}/variables/{id_net}	GET	Ope	Get a ruleset variable of a Gcap tenant
Gcaps	/gcaps/{id}/tenants/{tenant_pk}/variables/{id_net}	PUT	Ope	Update ruleset variables of a Gcap tenant
Gcaps	/gcaps/{id}/tenants/{tenant_pk}/variables/{id_net}	DELETE	Ope	Delete a ruleset variables of a Gcap tenant

Table 62: Gcenter

Theme	Name	Verb	Role	Description
Gcenter	/gcenter/ssh-rsa-key/	GET	Adm	Get the GCenter pub key

Table 63: Gscan

Theme	Name	Verb	Role	Description
Gscan	/gscan/histories/	GET	Ope	Get all the previous Gscan results
Gscan	/gscan/histories/{id}/	GET	Ope	Get a previous Gscan history result's details
Gscan	/gscan/malcore/	POST	Ope	Scan a file with malcore
Gscan	/gscan/powershell/	POST	Ope	Scan a file with powershell
Gscan	/gscan/settings/	GET	Adm	Get the gscan settings configuration
Gscan	/gscan/settings/	PUT	Adm	Update the gscan settings configuration
Gscan	gscan/shellcode/	POST	Ope	Scan a file with shellcode
Gscan	/gscan/shellcode/deep-config/	GET	Ope	Get the shellcode deep scan configuration
Gscan	/gscan/shellcode/deep-config/	PUT	Ope	Update the shellcode deep scan configuration

Table 64: Gum

Theme	Name	Verb	Role	Description
Gum	/gum/config/	GET	Adm	Get the gum config
Gum	/gum/config/	POST	Adm	Try to run the scheduled update gum task config now
Gum	/gum/config/	PUT	Adm	Change the gum config
Gum	/gum/config/	OPTIONS	Adm	Get the needed remote files for the local repository
Gum	/gum/config/check/	POST	Adm	Test the remote scheduled config
Gum	/gum/software-updates/	GET	Adm	Get the last software updates status
Gum	/gum/software-updates/	POST	Adm	Upload a new software update gwp file
Gum	/gum/software-updates/{id}/	GET	Adm	Get a software updates status
Gum	/gum/software-updates/{id}/continue/	POST	Adm	Continue the operation
Gum	/gum/software-updates/{id}/end/	POST	Adm	Stop the operation
Gum	/gum/threat-db-updates/	GET	Adm	Get the last threat db updates status
Gum	/gum/threat-db-updates/	POST	Adm	Upload a new threat db update gwp file
Gum	/gum/threat-db-updates/{id}/	GET	Adm	Get a threat db updates status

Table 65: Health Checks

Theme	Name	Verb	Role	Description
Health Checks	/health-checks/	GET	Adm, Ope	Get the health checks

Table 66: Ignore Lists

Theme	Name	Verb	Role	Description
Ignore Lists	/ignore-lists/asset-names/	GET	Ope	Get all the ignored asset names
Ignore Lists	/ignore-lists/asset-names/	POST	Ope	Add a new ignored asset name
Ignore Lists	/ignore-lists/asset-names/{id}/	DELETE	Ope	Remove one ignored asset name
Ignore Lists	/ignore-lists/hints/asset-ips/	GET	Ope	Get all the asset IP ignore hints (IP associated to more than 4 assets)
Ignore Lists	/ignore-lists/hints/asset-mac-addresses/	GET	Ope	Get all the asset MAC ignore hints (MAC associated to more than 4 assets)
Ignore Lists	/ignore-lists/hints/kuser-ips/	GET	Ope	Get all the kerberos user IP ignore hints (IP associated to more than 4 kusers)
Ignore Lists	/ignore-lists/kuser-ips/	GET	Ope	Get all the ignored kerberos user IPs
Ignore Lists	/ignore-lists/kuser-ips/	POST	Ope	Add a new ignored kerberos user IP
Ignore Lists	/ignore-lists/kuser-ips/{id}/	DELETE	Ope	Remove one ignored kerberos user IP
Ignore Lists	/ignore-lists/kuser-names/	GET	Ope	Get all the ignored kerberos user names
Ignore Lists	/ignore-lists/kuser-names/	POST	Ope	Add a new ignored kerberos user name
Ignore Lists	/ignore-lists/kuser-names/{id}/	DELETE	Ope	Remove one ignored kerberos user name
Ignore Lists	/ignore-lists/mac-addresses/	GET	Ope	Get all the ignored MAC addresses
Ignore Lists	/ignore-lists/mac-addresses/	POST	Ope	Add a new ignored MAC address
Ignore Lists	/ignore-lists/mac-addresses/{id}/	DELETE	Ope	Remove one ignored MAC address

Table 67: Kusers

Theme	Name	Verb	Role	Description
Kusers	/kusers/	GET	Ope	Retrieves a list of Kerberos Users
Kusers	/kusers/{kuser_name}/	GET	Ope	Retrieve a specific user data
Kusers	/kusers/{kuser_name}/alerts/	GET	Ope	Get the alerts for a specific kerberos user
Kusers	/kusers/{kuser_name}/clusters/	GET	Ope	Return alert clusters for the corresponding kerberos user
Kusers	/gukusers/{kuser_name}/ips/	GET	Ope	Get the list of ips related to a user
Kusers	/kusers/{kuser_name}/note/	PUT	Ope	Update the note for a given instance
Kusers	/kusers/{kuser_name}/note/	DELETE	Ope	Clear the note content for a given instance
Kusers	/kusers/{kuser_name}/tags/	GET	Ope	Get the tags for a given instance
Kusers	/kusers/{kuser_name}/tags/	PUT	Ope	Update the tags for a given instance
Kusers	/kusers/{kuser_name}/urls/	GET	Ope	Get the list of urls related to a user through an alert

Table 68: Ldap

Theme	Name	Verb	Role	Description
Ldap	/ldap/	GET	Adm	Get the LDAP settings
Ldap	/ldap/	POST	Adm	Test the saved configuration
Ldap	/ldap/	PUT	Adm	Update the LDAP settings
Ldap	/ldap/certificate/	GET	Adm	Get the LDAP custom CA file name
Ldap	/ldap/certificate/	PUT	Adm	Update the LDAP custom CA file
Ldap	/ldap/certificate/	DELETE	Adm	Delete the LDAP custom CA file

Table 69: License

Theme	Name	Verb	Role	Description
License	/license/	GET	Adm, Ope	Get the GCenter license key and details
License	/license/	PUT	Adm	Update the GCenter license key and expiry alert

Table 70: Main Domains

Theme	Name	Verb	Role	Description
Main Domains	/main-domains/	GET	Adm, Ope	Get all the main domains
Main Domains	main-domains/	POST	Adm, Ope	Add a new main domain
Main Domains	main-domains/{id}/	GET	Adm, Ope	Get one main domain
Main Domains	main-domains/{id}/	PUT	Adm, Ope	Update one main domain
Main Domains	main-domains/{id}/	DELETE	Adm, Ope	Remove one main domain

Table 71: Malcore

Theme	Name	Verb	Role	Description
Malcore	/malcore/engine-ignore-list/	GET	Ope	Get the Malcore sensitive engine ignorelist
Malcore	/malcore/engine-ignore-list/	POST	Ope	Add a sensitive engine to the ignorelist
Malcore	/malcore/engine-ignore-list/{engine_id}/	DELETE	Ope	Delete a sensitive engine from the ignorelist
Malcore	malcore/filename-{list_type}-list/	GET	Ope	Get the Malcore filename white/black list
Malcore	malcore/filename-{list_type}-list/	POST	Ope	Add a filename to the white/black list
Malcore	/malcore/filename-{list_type}-list/{id}	DELETE	Ope	Delete a filename the white/black list
Malcore	/malcore/hash-{list_type}-list/	GET	Ope	Get the Malcore sha256 white/black list
Malcore	/malcore/hash-{list_type}-list/	POST	Ope	Add a sha256 to the white/black list
Malcore	/malcore/hash-{list_type}-list/load	PUT	Ope	Update the sha256 white/black list from a csv file
Malcore	/malcore/hash-{list_type}-list/{sha256}	DELETE	Ope	Delete a sha256 from the white/black list
Malcore	/malcore/health-checks/	GET	Adm, Ope	
Malcore	malcore/profiles/	GET	Ope	Get the Malcore profiles list
Malcore	malcore/profiles/{name}/	GET	Ope	Get the settings of a Malcore profile
Malcore	malcore/profiles/{name}/	PUT	Ope	Update the settings of a Malcore profile
Malcore	malcore/settings/	GET	Ope	Get the Malcore settings
Malcore	malcore/settings/	PUT	Ope	Update the Malcore settings
Malcore	/malcore/yara/settings/	GET	Ope	Get the yara settings
Malcore	/malcore/yara/settings/	PUT	Ope	Update the yara settings

Table 72: Mitre

Theme	Name	Verb	Role	Description
Mitre	/mitre/	GET	Ope	Get the mitres with the alerts aggregation

Table 73: Ndr

Theme	Name	Verb	Role	Description
Ndr	/ndr/settings/	GET	Adm, Ope	Get the NDR settings
Ndr	/ndr/settings/	PATCH	Adm	Update the NDR settings

Table 74: Net

Theme	Name	Verb	Role	Description
Net	/net/certificate/	POST	Adm	Get a certificate file's data
Net	/net/dns/	GET	Adm	Get the dns service configuration
Net	/net/dns/	PUT	Adm	Update the dns service configuration
Net	/net/interfaces/	GET	Adm	Get the Gcenter's available network interfaces
Net	/net/interfaces/{name}/	GET	Adm	Get a Gcenter's network interface data
Net	/net/ntp/	GET	Adm	Get the ntp service configuration
Net	/net/ntp/	PUT	Adm	Update the ntp service configuration

Table 75: Netdata Polling

Theme	Name	Verb	Role	Description
Netdata Polling	/netdata-polling/	GET	Adm	Get the netdata polling global configuration
Netdata Polling	/netdata-polling/	PUT	Adm	Update the netdata polling global configuration

Table 76: Notifications

Theme	Name	Verb	Role	Description
Notifications	/notifications/	GET	Adm, Ope	Get detailed notifications
Notifications	/notifications/	POST	Adm, Ope	Acknowledge notifications
Notifications	/notifications/aggregated/	GET	Adm, Ope	Get aggregated notifications
Notifications	/notifications/aggregated/{action}/	POST	Adm	Mute/unmute notifications aggregates

Table 77: Powershell

Theme	Name	Verb	Role	Description
Powershell	/powershell/settings/	GET	Ope	Get the current Powershell configuration
Powershell	/powershell/settings/	PUT	Ope	Update the current Powershell configuration

Table 78: Ransomware Detect

Theme	Name	Verb	Role	Description
Ransomware Detect	/ransomware-detect/	GET	Ope	Get the Ransomware detect engine properties
Ransomware Detect	/ransomware-detect/predictions-graph/	GET	Ope	Get data to build predictions graph
Ransomware Detect	/ransomware-detect/settings/	GET	Ope	Get the Ransomware detect settings
Ransomware Detect	/ransomware-detect/settings/	PUT	Ope	Update the Ransomware detect settings
Ransomware Detect	/ransomware-detect/train/	POST	Ope	Launch Ransomware detect engine training
Ransomware Detect	/ransomware-detect/white-list/	GET	Ope	Get the Ransomware detect source IP white list
Ransomware Detect	/ransomware-detect/white-list/	POST	Ope	Add a source IP to the white list
Ransomware Detect	/ransomware-detect/white-list/hints	GET	Ope	Get source IP hints for white list
Ransomware Detect	/ransomware-detect/white-list/{source_ip}	DELETE	Ope	Delete a source IP from the white list

Table 79: Raw Alerts

Theme	Name	Verb	Role	Description
Raw Alerts	/raw-alerts/{id}/	GET	Ope	Get a raw alert data
Raw Alerts	/raw-alerts/{id}/analysis-report/	GET	Ope	Download the malcore alert analysis report file
Raw Alerts	/raw-alerts/{id}/file/	GET	Ope	Download the related alert file
Raw Alerts	/raw-alerts/{id}/graph/	GET	Ope	Download the shellcode alert graph file
Raw Alerts	/raw-alerts/{id}/hexdump/	GET	Ope	Generate the related codebreaker alert file hexdump
Raw Alerts	/raw-alerts/{id}/remote-report/	POST	Ope	Generate the malcore alert remote report file

Table 80: Relations

Theme	Name	Verb	Role	Description
Relations	/relations/	GET	Ope	Get the graph of relations between users/assets
Relations	/relations/top/	GET	Ope	Get the graph of the relations between users/assets for the top N items by risk

Table 81: Search

Theme	Name	Verb	Role	Description
Search	/search/autocomplete/	GET	Ope	Search the alerts info
Search	/search/autocomplete/recent/	GET	Ope	Get the user last search results
Search	/search/autocomplete/recent/	POST	Ope	Add one search result to the user's history
Search	/search/autocomplete/recent/all/	DELETE	Ope	Remove all user's search history

Table 82: Settings

Theme	Name	Verb	Role	Description
Settings	/settings/	GET	Adm	Get the global settings configuration
Settings	/settings/	PUT	Adm	Update the global settings configuration
Settings	/settings/	OPTIONS	Adm	Get all the available import/export urls
Settings	/settings/webui/	GET	Adm	Get the global settings configuration
Settings	/settings/webui/	PUT	Adm	Update the global settings configuration
Settings	/settings/zip_password/	DELETE	Adm	Remove the zip password

Table 83: Shellcode

Theme	Name	Verb	Role	Description
Shellcode	/shellcode/settings/	GET	Ope	Get the current Shellcode configuration
Shellcode	/shellcode/settings/	PUT	Ope	Update the current Shellcode configuration

Table 84: Sigflow

Theme	Name	Verb	Role	Description
Sigflow	/sigflow/rulesets/	GET	Adm, Ope	Get all the sigflow rulesets
Sigflow	/sigflow/rulesets/{id}/	GET	Adm, Ope	Get a sigflow ruleset data

Table 85: Signatures

Theme	Name	Verb	Role	Description
Signatures	/signatures/	GET	Ope	Get signatures
Signatures	/signatures/action/{action}/	PUT	Ope	

Table 86: Ssl

Theme	Name	Verb	Role	Description
Ssl	/ssl/	GET	Adm	SSL global settings(ONLY for import/export)
Ssl	/ssl/	PUT	Adm	SSL global settings(ONLY for import/export)
Ssl	/ssl/custom-certificate/	GET	Adm	Get the Gcenter SSL Custom Certificate status
Ssl	/ssl/custom-certificate/	PUT	Adm	Update the Gcenter SSL Custom Certificate
Ssl	/ssl/custom-certificate/	DELETE	Adm	Reset the Gcenter SSL Custom Certificate
Ssl	/ssl/details/	GET	Adm	Get the Gcenter SSL security details
Ssl	/ssl/mutual-authentication/	GET	Adm	Get the Gcenter SSL mutual authentication configuration
Ssl	/ssl/mutual-authentication/	PUT	Adm	Update the Gcenter SSL mutual authentication configuration
Ssl	/ssl/mutual-authentication/	DELETE	Adm	Reset the Gcenter SSL mutual authentication configuration

Table 87: Static Ip Asset Name

Theme	Name	Verb	Role	Description
Static Ip Asset Name	/static-ip-asset-name/	GET	Adm, Ope	Get all the IP bound to a specific asset
Static Ip Asset Name	/static-ip-asset-name/	POST	Adm, Ope	Add a new IP bound to a specific asset
Static Ip Asset Name	/static-ip-asset-name/{id}/	DELETE	Adm, Ope	Remove unbound an IP from a specific asset

Table 88: Status

Theme	Name	Verb	Role	Description
Status	/status/api/	GET	WAuth	Check if the API is working
Status	/status/gcenter/	GET	Adm	Get the engine status
Status	/status/hardware/raid/	GET	Adm	Download the hardware diagnostic report file
Status	/status/user/	GET	WAuth	Get the User status

Table 89: Tags

Theme	Name	Verb	Role	Description
Tags	/tags/	GET	Adm, Ope	Get all the tags
Tags	/tags/	POST	Adm	Create a new tag
Tags	/tags/{id}/	GET	Adm	Get a tag content
Tags	/tags/{id}/	PUT	Adm	Update a tag content
Tags	/tags/{id}/	DELETE	Adm	Delete a tag

Table 90: Throttling

Theme	Name	Verb	Role	Description
Throttling	/throttling/	GET	Adm, Ope	Get throttling settings
Throttling	/throttling/	PUT	Adm, Ope	Update throttling settings

Table 91: Updates Health Checks

Theme	Name	Verb	Role	Description
Updates Health Checks	/updates-health-checks/	GET	Adm, Ope	Get the updates health checks

Table 92: Users

Theme	Name	Verb	Role	Description
Users	/users/	GET	Adm	Get all Gcenter's users
Users	/users/	POST	Adm	Create a new user
Users	/users/history/	GET	Adm	Logging history settings view set
Users	/users/history/	PUT	Adm	Logging history settings view set
Users	/users/me/	GET	Adm, Ope	Get your user data
Users	/users/me/	PUT	Adm, Ope	Update your user data
Users	/users/me/password/	GET	Adm, Ope	Get password suggestions
Users	/users/me/password/	PUT	Adm, Ope	Update your user password
Users	/users/password-policy/	GET	Adm, Ope	Get the current password policy configuration
Users	/users/password-policy/	PUT	Adm	Update the current password policy configuration
Users	/users/session-age/	GET	Adm	Get the session age configuration
Users	/users/session-age/	PUT	Adm	Update the session age configuration
Users	/users/{id}/	GET	Adm	Get a user data
Users	/users/{id}/	PUT	Adm	Update a user data
Users	/users/{id}/	DELETE	Adm	Delete a user
Users	/users/{id}/password/	PUT	Adm	Reset the password of a user

Table 93: Version

Theme	Name	Verb	Role	Description
Version	/version/	GET	Adm, Ope	Get the Gcenter version

Chapter 6

Use case of the configuration menu: setup account

6.1 Direct connection to the GCenter configuration menu with keyboard and monitor

6.1.1 Introduction

The first connection to a GCenter can be made via a direct connection with a keyboard and monitor.
This is necessary if the network configuration is not yet completed on the GCenter or if the network address is not known.
This procedure enables the network parameters (iDRAC) to be known if they exist or to modify them.
Subsequent accesses will generally be made remotely.

6.1.2 Preliminary operations

- Connect the power cables.
- Connect the network cables (see *Presentation of the GCenter*).

6.1.3 Procedure to connect the monitor and keyboard

- Connect the monitor to the VGA connector.
- Connect the keyboard to one of the USB connectors.
- Switch on the server.

6.1.4 Procedure to find out or changing the iDRAC network settings via the BIOS

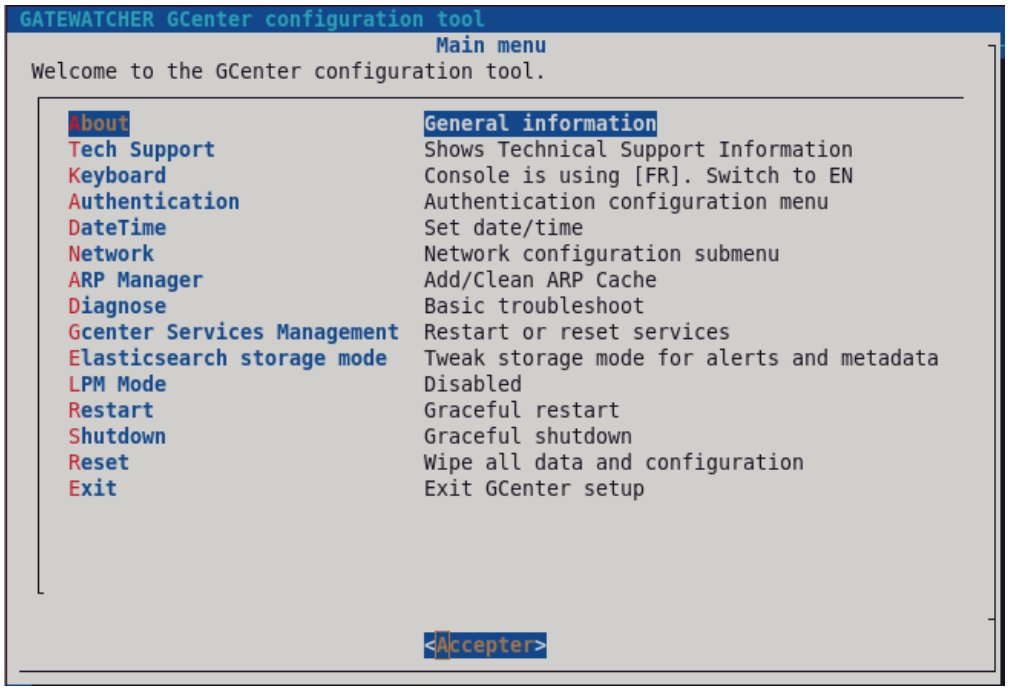
- Press **F2** during the boot up self-test (POST).
- On the `` `System Setup Main Menu` `` page (main menu of the configuration of the system), click on `` `iDRAC Settings` ``.
  The `` `iDRAC settings` `` page appears.
- Click on `` `Network` ``.
  The `` `IDRAC Settings. Network` `` page is displayed.
- Note the network settings in the `` `Network Settings` `` configuration or modify these settings.
- After noting down the network settings, exit the BIOS.
- Successively click the `` `Back` `` button and then the `` `Finish` `` button.
- In the `` `Warning` `` window prompting you to save changes, click the `` `No` `` button.
- In the `` `System Setup` `` screen, click the `` `Finish` `` button.
- In the `` `Warning` `` window prompting you to confirm the exit, click the `` `Yes` `` button.
  The server restarts...
- Unplug the monitors and keyboard if necessary.

Note:

The first time a user logs in via the *setup* account, the system prompts to change the password.
The following message is displayed: `` `You are required to change your password immediately (administrator enforced).` ``
In this case:

- Enter a new password in the appropriate format
- Re-enter the new password

The main menu is displayed.



Note:

Press the first letter of a command for quick access.
Press the `OK` button to confirm the selected choice.

6.2 Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)

6.2.1 Introduction

This procedure describes the remote connection from a distant computer using:

- The network connection to the iDRAC port of the GCenter
- A Web browser

This connection is not the normal way to access the GCenter but enables access to the GCenter in the event of problems.
To carry out this procedure, it is necessary:

- That the iDRAC has an accessible IP in order to be able to connect to it
- To know the login name and password to access iDRAC

From the iDRAC web page, it is possible to:

- View the material resources, their status, and the BIOS configurations
- Interact with the server to turn it on, off, and restart it
- Connect to the GCenter via the console

6.2.2 Preliminary operations

- Carry out the iDRAC's network configuration.

6.2.3 Procedure

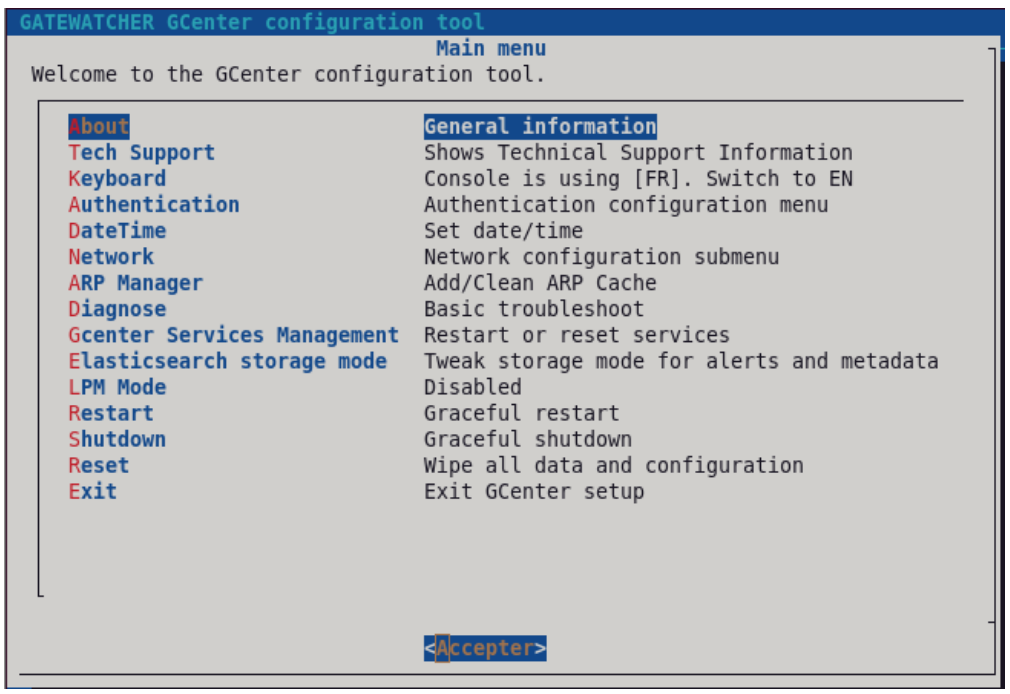
- On the remote computer, open a web browser.
- Enter the IP address of GCenter's iDRAC interface and confirm.
  The `Login` window is displayed.
- Enter the requested parameters:
  - `Username` : ID
  - `Password` : password of the entered login
  - `Domain` : select `This IDRAC`
- Click on the `Log In` button.
- Initiate the virtual console (`Virtual console` area, `Launch Virtual console` button).
  Following this action, a new page will open. It will be possible to interact with the GCenter.

Note:

The first time a user logs in, the system prompts to change the password.
The following message is displayed: `You are required to change your password immediately (administrator enforced).`
In this case:

- Enter a new password in the appropriate format
- Re-enter the new password

The main menu is displayed.



Note:

Press the first letter of a command for quick access.
Press the `OK` button to confirm the selected choice.

6.3 Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode

6.3.1 Introduction

This procedure describes the remote connection from a distant computer using:

- The network connection to the iDRAC port of the GCenter
- A connection tool via SSH

This connection is not the normal way to access the GCenter but enables access to the GCenter in the event of problems.
To carry out this procedure, it is necessary:

- That the iDRAC has an accessible IP in order to be able to connect to it
- To know the login name and password to access iDRAC

From the interface, it is possible to:

- View the operating system messages
- Connect to the GCenter via the console

6.3.2 Preliminary operations

- Carry out the iDRAC's network configuration.

6.3.3 Procedure on the remote PC running Linux

- Open a command prompt.
- Enter the command `` `ssh identifiant@ip_adress` ``.
  For example, `` `ssh setup@x.x.x.x` `` where
  - `` `setup` `` is the identifier and
  - x.x.x.x is the IP address of the GCenter iDRAC port
- Validate the command.
- Enter the password of the entered login.
- Press `` `Enter` `` to display all available commands and a short explanation.

6.3.4 Procedure on the remote PC running Windows

- Open an SSH client software, such as Putty.
- Enter the IP address of GCenter's iDRAC interface and confirm.
- Enter the following command `` `racadm>>console com2` ``.
- Validate.
  The system now displays the graphical interface of the device.
  Following this action, a new page will open. It will be possible to interact with the GCenter.

6.4 Direct connection to the GCenter configuration menu via SSH

6.4.1 Introduction

This procedure describes how to connect from a remote computer securely using an SSH tunnel.

6.4.2 Preliminary operations

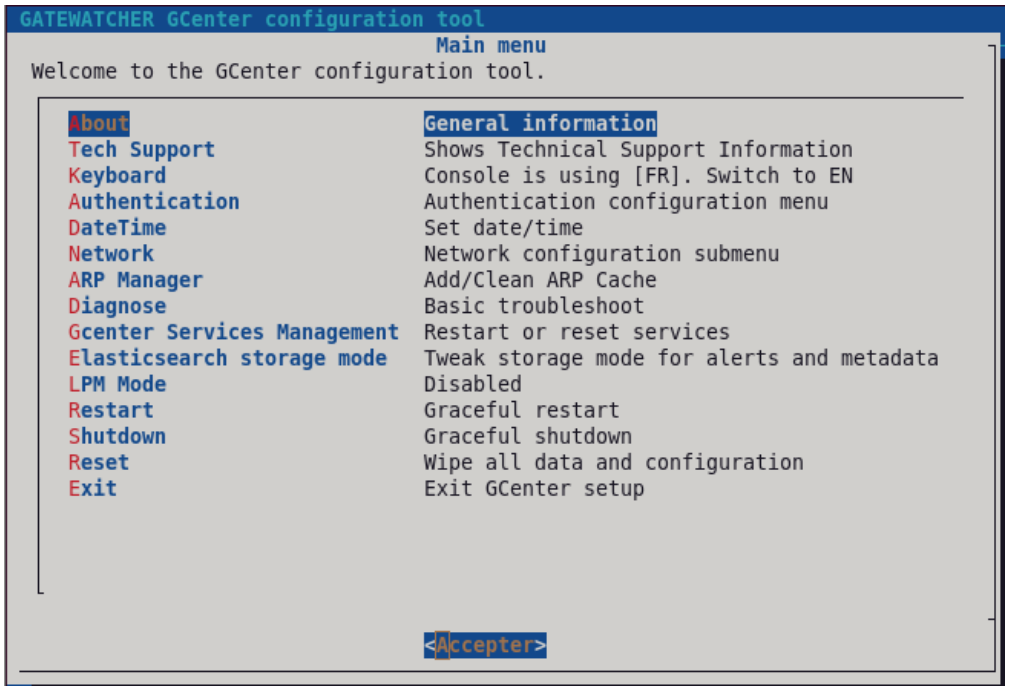
- Make an initial connection to the GCenter (see *Direct connection to the GCenter configuration menu with keyboard and monitor*).
- Know the name of the GCenter or its IP address.

6.4.3 Procedure on the remote PC running Linux

- Open a command prompt.
- Enter the command `` `ssh identifiant@adresse_ip_GCenter` `` or `` `ssh identifiant@FQDN_GCenter` ``.
  For example, `` `ssh setup@gcenter` `` where:
- The identifier is `` `setup` `` and
- The FQDN is `` `gcenter` ``.
- Validate the command.
- Enter the password.

6.4.4 Procedure on the remote PC running Windows

- Open an SSH client software, such as Putty.
- Enter the IP address of GCenter's interface and confirm.
- Enter the login and password.
  The main menu is displayed.



Note:

Press the first letter of a command for quick access.
Press the `OK` button to confirm the selected choice.

6.5 `About` command

6.5.1 Introduction

The `About` command displays the following information:

- `Gcenter Name` : name of the GCenter
- Version: the software version of the GCenter
- The GCenter's IP address characteristics for the mgmt0 interface

- `IP Address`: 192.168.1.1
- `Subnet Mask`: 255.255.255.0
- `Default Gateway`: 192.168.1.254

6.5.2 Prerequisites

- User: setup

6.5.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.5.4 Procedure

The configuration menu is displayed.

- Select the `About` line or press the letter **A**.
- Click on the `OK` button.
  The `About` window is displayed:

```
Gcenter Name            :    gcenter-name
Version                 :    number
IP Address              :    192.168.1.1
Subnet Mask             :    255.255.255.0
Default Gateway         :    192.168.1.254
```

- Press the `Enter` key to return to the menu.

6.6 `Tech Support` command

6.6.1 Introduction

The `Tech Support` command generates a text report of the GCenter's status.
As the report's data is in plain text, it enables the data to be anonymized if required.
The main sections of this report are:

- Appliance Version
- Interfaces
- Containers statuses
- Containers Health checks
- Health checks
- Containers processes statuses
- Appliance Version
- Services statuses
- NTP
- GCaps / Sigflow
- License
- Logical Volumes
- Disk Free
- Mounted FS
- Scheduled updates
- Latest Update Package sha256sum
- Scheduled backups
- File count in /data/extraction/geyego
- Tree structure of data and backups partitions
- Snapshot top
- Monitoring
- Geyego Stats

6.6.2 Prerequisites

- User: setup

6.6.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

@Copyright: December 2024, Gatewatcher

6.6.4 Procedure

The configuration menu is displayed.

- Select the `Tech Support` line or press the letter **T**.
- Click on the `OK` button.
  The system creates the technical report, displaying it on the screen.
- Press the `Enter` key to return to the menu.

6.7 `Keyboard` command

6.7.1 Introduction

The `Keyboard` command declares the language of the keyboard used:

- choice EN for English keyboard
- choice FR for a French keyboard

6.7.2 Prerequisites

- User: setup

6.7.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.7.4 Procedure

The configuration menu is displayed.
The system shows:

- The current configuration
- And, if the line is pressed, the switch to the other language.
  For example: the `Keyboard` line shows: `Now using [EN]. Switch to FR`.
  In this case, the keyboard used is declared as EN keyboard (English).
- Select the `Keyboard` line or press the letter **K**.
- Click on the `OK` button.
  The system changes the keyboard language.
  In this case, the keyboard used is declared as keyboard FR (French).

6.8 `Authentication` command

6.8.1 Introduction

The `Authentication` command enables to configure:

- the setup access account password
- the ssh keys

6.8.2 Prerequisites

- User: setup

6.8.3 Preliminary operations

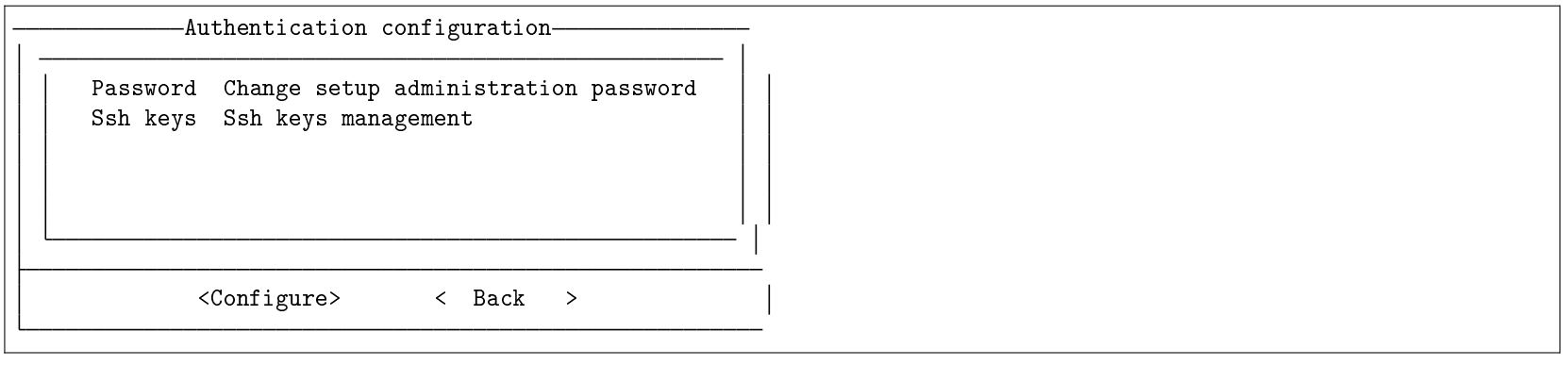
Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.8.4 Procedure to change the setup account password

The configuration menu is displayed.

- Select the `Authentication` line or press the letter **A**.
- Click on the `Configure` button.
  The following window is displayed.



- Select the `Password` line or press the letter **P**.
- Click on the `Configure` button.
  The following message is displayed:

```
You are about to change the password of the administrative user account (setup) granting access to this␣
↪configuration tool.
This change will be effective immediately.
Are you sure to want to continue?
```

- Press the `Yes` button to change the password or the `No` button to cancel.
  If the `Yes` button has been pressed, the following message is displayed:

```
Password complexity rules:
  Minimum different characters between old and new passwords: 2
  Minimum length: 12
  Lowercase character required: yes
  Uppercase character required: yes
  Digit required: yes
  Other character class required: yes

(current) LDAP Password:
```

- Enter the current password and confirm.
  The following message is displayed: `New password:`
- Enter new password and validate.
- Re-enter password and validate.

Note:

In case of an error, the following message is displayed:

```
An error has occurred during the password change invite.
You may have mistyped the current password of the password confirmation.
The password has NOT been changed.
Do you want to retry a password change?
```

- Click on the `Yes` button to restart the password change procedure or the `No` button to cancel.

6.8.4.1 Procedure to modify the ssh keys

The configuration menu is displayed.

- Select the line `Ssh keys` or press the letter **S**.
- Press the `Configure` button.
  The `Ssh saved keys` window is displayed.
  The window displays 16 saved key possibilities numbered from 1 to 16.
  For each of these keys, it is possible to configure or delete it.
- To set up a key:
  - Select a key number
  - Click on the `Configure` button
    The `Configure key x` window is displayed:

```
Comment
Key type
Key
```

  - Fill in the various fields
  - Click on the `Save` button

Note:

If the key type is not recognized, the system displays the list of recognized types

```
──────────────────────────Warning──────────────────────────
zd is not a supported key. Gcenter supports these types:
- ecdsa-sha2-nistp521
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp521-cert-v01@openssh.com
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp256-cert-v01@openssh.com
- rsa-sha2-512
- rsa-sha2-256
- rsa-sha2-512-cert-v01@openssh.com
- rsa-sha2-256-cert-v01@openssh.com
- sk-ecdsa-sha2-nistp256@openssh.com
- sk-ecdsa-sha2-nistp256-cert-v01@openssh.com
- ssh-ed25519
- ssh-ed25519-cert-v01@openssh.com
- sk-ssh-ed25519@openssh.com
- sk-ssh-ed25519-cert-v01@openssh.com
- ssh-rsa
- ssh-rsa-cert-v01@openssh.com
──────────────────────────────────────────────────────────
```

Note:

If the key does not match the type entered, the system indicates this with the message `Invalid SSH key format detected`.

6.9 `DateTime` command

6.9.1 Introduction

The `DateTime` command enables changing the date and time of the GCenter.

Note:

It is highly recommended to use a functioning NTP server to maintain an accurate date and time configuration.
Some features may not work as expected if the date and time are incorrect.

Note:

Before pairing between the GCap and the GCenter, it is necessary to ensure that both systems are at the same time.
The GCap and GCenter times must be the same within 1 minute.
If there is a discrepancy, the GCap time should be changed.
The adjustment is necessary for the establishment of the IPsec tunnel.
Once the pairing is functional, the GCenter acts as the NTP server for the GCap so that the clocks of the equipment are synchronized.

6.9.1.1 Prerequisites

- User: setup

6.9.1.2 Preliminary operations

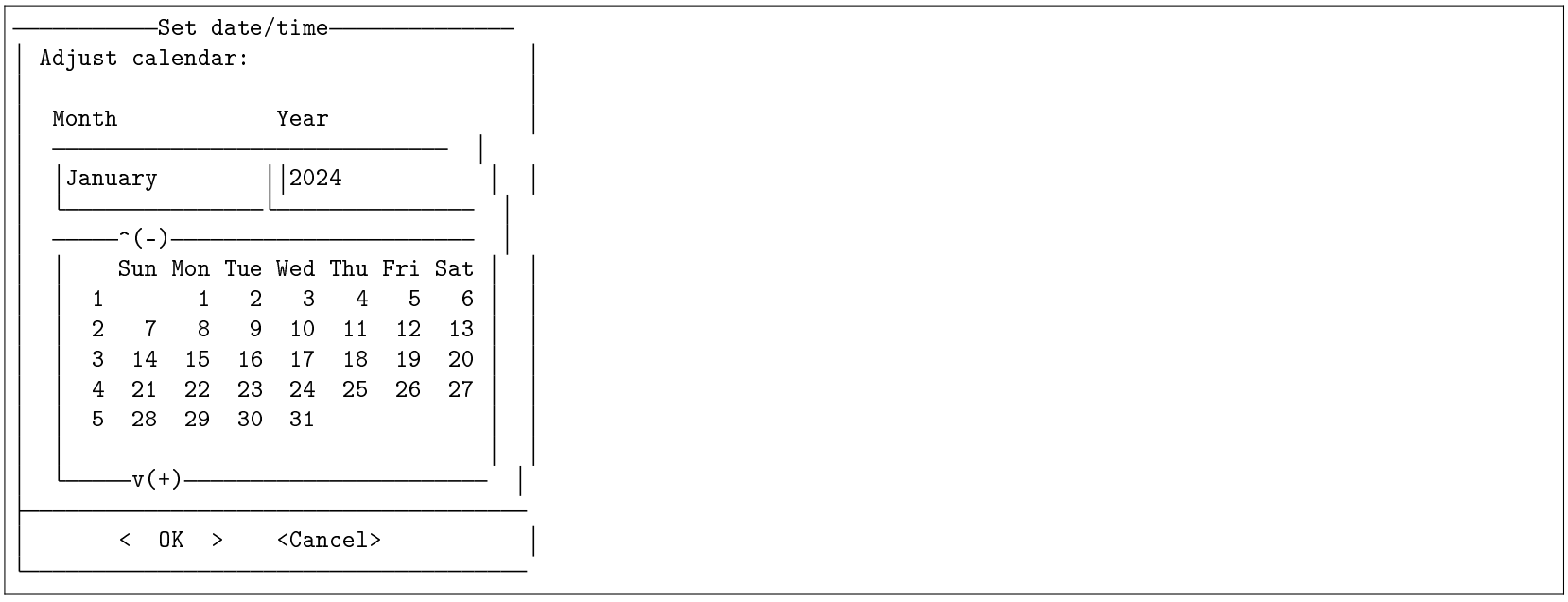
Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.9.1.3 Procedure

The configuration menu is displayed.

- Select the line `DateTime` or press the letter **D**.
- Press the `OK` button.
  The system displays the calendar and is set to the current date.



- To change the date, use the <-> or <+> keys.
- Validate after modification.
- To select a field, use the side arrows > or <
- To change a value, use the upper and lower arrows
- Validate after modification.
  The following message is displayed:

```
It is strongly recommended that you use a working NTP server to maintain an accurate date and time␣
↪configuration.
Some features may not work as expected if the date and time are incorrect.
```

The system displays the new date and time in UTC.

- Validate if necessary.

6.10 `Network` command

6.10.1 Introduction

The `Network` command enables viewing and modifying the GCenter network settings:

- GCenter name (hostname)
- domain name
- IP address for mgmt0 (with mask and gateway)
- IP address for vpn0 (with mask and gateway)
- IP address for icap0 (with mask and gateway)
- IP address for sup0 (with mask and gateway)
- DNS servers (primary and secondary)
- NTP servers (primary and secondary)

Attention:

If an interface used by certain services is deactivated, the latter will no longer be functional.

Note:

refer to *Presentation of the GCenter* to known the list of GCenter inputs outputs.

6.10.2 Prerequisites

- User: setup

6.10.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.10.4 Procedure to access the network interface configuration menu

The configuration menu is displayed.

- Select the `Network` line or press the letter **N**.
- Click on the `OK` button.
  The `Hostname configuration` window is displayed:

```
   Hostname configuration
   Interface configuration: mgmt0  Enabled
   Interface configuration: vpn0   Disabled
   Interface configuration: icap0  Disabled
   Interface configuration: sup0   Disabled
   DNS configuration
   NTP configuration

   ___________________________________________

         <Configure>       <Back>

For each of the 4 interfaces, the system displays its status.
```

- Use one of the following procedures if necessary:

- *Procédure to configure the hostname*
- *Procedure to configure an interface*
- *Procedure to configure the DNS*
- *Procedure to configure the NTP*

6.10.5 Procédure to configure the hostname

- Select the line `Hostname configuration` or press the letter **H**.
- Click the `Configure` button.
  The `Hostname configuration` window is displayed:
  The following settings are displayed by default:

```
Hostname         : gcenter
DNS domain name  : domain.local
```

- If necessary, change the displayed values.
- Press the `Next` button to move to the subsequent settings.

Note:

Press the `Back` button to return to the preceding screen.

6.10.6 Procedure to configure an interface

- For the interface to be configured:
  - Select it
  - click on the button `Configure`
    The window `IP address configuration` is displayed.

```
Configure here the IPv4 settings for the mgmt0 network interface.
Please note that modifying the interface configuration may have an impact on SSH access, WebUI and␣
↪pairing access.

Note: Only dot-decimal IPv4 for is accepted.

 ──────────────────────────────────────────────────────────────────────────────
 IP address  192.168.1.1
 Netmask     255.255.255.0
 Gateway     192.168.1.254
 MTU         1500
 TCP MSS     1380
 
                        <Enable >              <Disable>              <Disable>
 ──────────────────────────────────────────────────────────────────────────────
```

  - Enter or modify the requested parameters.
  - To validate, click on the `Enable` button.
    To cancel the entry, click on the `Disable` button.
    To return to the previous screen, click on the `Back` button.

6.10.7 Procedure to configure the DNS

- Select the line `DNS configuration` or press the letter **D**.
- Click on the `Configure` button.
  The `DNS servers configuration` window is displayed:

```
Configure DNS servers

Note: Only dot-decimal IPv4 format is accepted

  DNS server #1 : 192.168.1.251
  DNS server #2 :
```

- If necessary, change the displayed values.
- To validate, click on the `Save` button.
  To return to the previous screen, click on the `Back` button.

6.10.8 Procedure to configure the NTP

- Select the line `NTP configuration` or press the letter **N**.
- Click on the `Configure` button.
  The `NTP configuration` window is displayed:

```
Configure NTP servers

Note: Only dot-decimal IPv4 format is accepted

  NTP server #1 : 192.168.1.251
  NTP server #2 :
```

- If necessary, change the displayed values.
- To validate, click on the `Save` button.
  To return to the previous screen, click on the `Back` button.

6.11 `Arp Manager` command

6.11.1 Introduction

The `Arp Manager` command is used:

- To add an entry to the GCenter ARP table
- To delete an ARP entry made via the ARP Manager
- To clear the ARP cache of entries made via the ARP Manager

Note:

It is used in specific cases, for example if a diode is found between the GCenter and a piece of equipment on the network.

6.11.2 Prerequisites

- User: setup

6.11.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.11.4 Procedure to access to the `Arp Manager` submenu

The configuration menu is displayed.

- Select the `Arp Manager` line or press the letter **A**.
- Click on the `OK` button.
  The `Arp Manager` window is displayed:

```
Choose a task

      Add entry         Adds an ARP entry
      Delete entry      Deletes an ARP entry
      Clean cache       Cleans all the ARP cache
```

Several choices are available:

Choice	See
`Add entry`	*Procedure A: Adding an ARP entry*
`Delete entry`	*Procedure B: Delete an ARP entry*
`Clean cache`	*Procedure C: Clearing the ARP cache*

- Press the `Exit` key to return to the menu.

6.11.5 Procedure A: Adding an ARP entry

The `Arp Manager` window is displayed:

```
Choose a task

    Add entry         Adds an ARP entry
    Delete entry      Deletes an ARP entry
    Clean cache       Cleans all the ARP cache
```

- Select the `Add entry` line or press the letter **A**.
- Click on the `OK` button.
  The `Add ARP entry` window is displayed:

```
Add an IP Address and its corresponding MAC address
     MAC Address
     IP  address
```

- Enter the parameters.
- Press the `Add` button to confirm the selected choice.
  or Press the `Exit` key to return to the menu.
  The `Add ARP entry` window is displayed to indicate the addition of the new ARP entry.
- Press the `Exit` key to return to the menu.

6.11.6 Procedure B: Delete an ARP entry

The `Arp Manager` window is displayed:

```
Choose a task

    Add entry         Adds an ARP entry
    Delete entry      Deletes an ARP entry
    Clean cache       Cleans all the ARP cache
```

- Select the line `Delete entry` or press the letter **D**.
- Press the `Accept` button.
  The `Delete ARP entry` window is displayed:

```
──────────────Delete ARP Entry─────────────────
│ Please select an IP Address:                 │
│ ──────────────────────────────────────────── │
│ │ [ ] 192.168.x.x      a2:bb:36:5b:9c:34   │ │
│ │                                          │ │
│ │                                          │ │
│ │                                          │ │
│ └──────────────────────────────────────────┘ │
│──────────────────────────────────────────────│
│         <Accept>     <  Exit  >              │
└──────────────────────────────────────────────┘
```

Note:

If there is no entry then the message `Nothing to delete` is displayed. Press the `Accept` button.

- Select an IP address to delete by checking the line and press the `Accept` button.
  The `Delete ARP entry` window is displayed:

```
────────────Delete ARP entry────────────────
│ ARP entries successfully deleted from    │
│ table                                    │
│──────────────────────────────────────────│
│               <Accept>                   │
└──────────────────────────────────────────┘
```

- Press the `Accept` button.

6.11.7 Procedure C: Clearing the ARP cache

The `Arp Manager` window is displayed:

```
Choose a task

    Add entry         Adds an ARP entry
    Delete entry      Deletes an ARP entry
    Clean cache       Cleans all the ARP cache
```

- Select the line ` Clean cache` or press the letter **C**.
- Press the `Accept` button.
  The `Clean cache` window is displayed:

  Note:

  If there is no data to clean then the `Nothing to clean` message is displayed.

- Click on the `Accept` button.

6.12 `Diagnose` command

6.12.1 Introduction

The `Diagnose` command enables various actions to be tested on the network in order to validate the GCenter's correct configuration.
The tests performed are as follows:

- Ping the default gateway
- Ping the primary DNS server
- Ping of the secondary DNS server
- Ping the primary NTP server
- Ping of the secondary NTP server
- Query to primary DNS server
- Query to secondary DNS server
- Registration of the GCenter in the DNS
- Resolution of the Intelligence site
- Ping intelligence.gatewatcher.com
- Connect to intelligence.gatewatcher.com
- NTP synchronisation
- Internal DNS running
- Web server running

6.12.2 Prerequisites

- User: setup

6.12.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.12.4 Procedure

The configuration menu is displayed.

- Select the `Diagnose` line or press the letter **D**.
- Click on the `OK` button.
  The `Gatewatcher Diagnostics` window is displayed:

```
Select a timeout for each network test.
Value must be between 1 and 10 sec:
```

- Enter a value between 1 and 10 then validate.
  The system displays the tests carried out and then the test results:

```
──────────────Gatewatcher Diagnostics - Tests results──────────────
│  Ping default gateway                                    [ OK ]  │
│  Ping DNS server #1                                     [ NOK ]  │
│  Ping DNS server #2                                     [ NOK ]  │
│  Ping NTP server #1                                     [ NOK ]  │
│  Ping NTP server #2                                     [ NOK ]  │
│  Querying DNS server #1                                 [ NOK ]  │
│  Querying DNS server #2                                 [ NOK ]  │
│  GCenter registered in DNS                              [ NOK ]  │
│  Resolving intelligence site                             [ OK ]  │
│  Ping intelligence.gatewatcher.com                       [ OK ]  │
│  Connect to intelligence.gatewatcher.com                [ NOK ]  │
│  Syncing NTP                                             [ OK ]  │
│  Internal DNS running                                    [ OK ]  │
│  Web Backend running                                     [ OK ]  │
│                                                                  │
├──────────────────────────────────────────────────────────────────┤
│                           < Done >                               │
└──────────────────────────────────────────────────────────────────┘
```

- Analyze the results obtained.
- Press the `Enter` key to return to the menu.

6.13 `GCenter Services Management` command

6.13.1 Introduction

The `GCenter Services Management` command enables:

- Rebooting a GCenter application
- Resetting a GCenter application
- Restarting a GCenter service

The applications that can be restarted include the following:

App name	Detail
gabana	Kibana service
gbeacon	beacon detect engine
gcti	Retro hunt engine
gdgadetect	DGA engine
gesmaster	ES Master Service
geyego	Threat analysis and retroactive orchestration service
gfilebeat_eve	Ingester Service - Sigflow
gfilebeat_export_0	Ingester Service - export data 0
gfilebeat_export_1	Ingester Service - export data 1
ggcc	WebUI Service #1
glogstash	Threat logging service
gmalcorev2	Malware analysis engine
goasm	Vulnerability exploitation scanning engine
gpostgres	Database service
gproxy	Connection Manager
gps	Powershell scanning engine (Malicious Powershell Detect)
gransomware	Ransomware Detect engine
gredis	Ephemeral data service
gredis cache	Ephemeral data service (Used for caching)
gstats	Monitoring service
gunpoint	GCap gateway service
gweb	WebUI Service #2

The applications that can be reset include the following:

App name	Detail
Reset Webui configuration to default	Reset HTTP / HTTPS ports and interface to default configuration
Clear & Restart Webui service	Reset web server to default configuration
Wipe Elasticsearch index	Removes all internal indexes
Reset Elasticsearch Database	Resetting the Elasticsearch database and erasing all data

The services that can be restarted include the following:

App name	Detail
nginx	Restarting the web service
uwsgi	Restarting the application management service
celery	Restart the GCenter queue service
redis	Restart ephemeral data management service
unbound	Restart the DNS resolution service
sshd	Restart the GCenter ssh service
sshd_gcap	Restart the GCap-related ssh service
GCenter-healthchecks-daemon	Restarting the GCenter health check service
GCenter-docker-orchestrator	Restarting the docker orchestration service

---

6.13.2 Prerequisites

- User: setup

6.13.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.13.4 Procedure to access to `GCenter Services Management` sub-menu

The configuration menu is displayed.

- Select the `GCenter Services Management` line or press the letter **G**.
- Click on the `OK` button.

  The `GCenter Services Management` window is shown:

```
Restart a GCenter App
Reset a GCenter App
Restart a GCenter Service
```

  Several choices are available:

Choice	see
Restart a GCenter App	*Procedure A: Restarting an application*
Reset a GCenter App	*Procedure B: Reset a service*
Restart a GCenter Service	*Procedure C: Restarting a service*

- Click on the `Exit` key to return to the menu.

6.13.5 Procedure A: Restarting an application

The `GCenter Services Management` window is displayed:

- Select the `Restart a GCenter App` line or press the letter **R** .
- Validate.
  The `Restart a GApp` window is displayed:
- Select the line of the application to be restarted.
- Click on the `OK` button.

Note:

For example, for the ggcc service:
The system displays the following message `You are about to restart ggcc. Are you sure?`

- Click on the `Yes` button.
  A message indicates the restart is in progress.
  Then the system displays the following message `ggcc restarted successfully`.
- Click on the `OK` button.

6.13.6 Procedure B: Reset a service

The `GCenter Services Management` window is displayed:

- Select the `Reset a GCenter App` line or press the letter **R** .
- Validate.
  The `Reset a GApp` window is displayed:

```
Choose a GApp to reset:

Reset Webui configuration      This will reset HTTP / HTTPS and interface to default configuration
Clear & Restart Webui service  This will set webserver to default config
Wipe Elesticsearch index       Delete all internals index
Reset Elasticsearch Database   Reset elasticsearch service and clear all data
```

- Select the action to execute or press the corresponding letter.
- Click on the `OK` button.

Note:

For example, for the line `Reset WebUI to default configuration`:
The system displays the following message:

```
──────────────────────────Reset WebUI to default configuration──────────────────────────
│ You are about to change WebUI ports and inbound interface to default configuration.  │
│ After this :                                                                         │
│     HTTP port will be set to 80.                                                     │
│     HTTPS port will be set to 443.                                                   │
│     Inbound interface will be set to mgmt0.                                          │
├──────────────────────────────────────────────────────────────────────────────────────┤
│                              < Yes >              < No >                             │
└──────────────────────────────────────────────────────────────────────────────────────┘
```

- Click on the `Yes` button.
  A message indicates to wait... then the menu is displayed

6.13.7 Procedure C: Restarting a service

The `GCenter Services Management` window is displayed:

- Select the `Restart a GCenter Service` line or press the letter **R** .
- Validate.
  The `Reset a Service` window is displayed:
- Select the line of the service to be restarted or press the corresponding letter.
- Click on the `OK` button.

Note:

For example, for the `nginx` service:
The system displays the following message `You are about to restart nginx. Are you sure?`.

- Click on the `Yes` button.
  A message indicates the restart is in progress.
  Then the system displays the following message `nginx restarted successfully`.
- Click on the `OK` button.

6.14 `Elasticsearch storage mode` command

6.14.1 Introduction

The `Elasticsearch storage mode` command modifies the storage mode for the alerts and the metadata.
Choosing slow storage for elasticsearch will increase the potential retention duration, but it will negatively impact the performances and speed of the GCenter.
It is strongly recommended to keep elasticsearch on fast storage.

Note:

Storage type switch will preserve your data.
Moving high amount of data can greatly reduce the performances of your GCenter during the operation, and take up to one hour.
Indexation will be paused while it is occurring.
The migration process will allocate the default data retention size on the target storage (see numbers above).
This allocation can later be extended to the maximum size for the target storage: see the configuration in the WebUI screen following Admin>Configuration>Global settings>Elasticsearch max data retention.

6.14.2 Prerequisites

- User: setup

6.14.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.14.4 Procedure

The configuration menu is displayed.

- Select the line `Elasticsearch storage mode`` or press the letter **E**.
- Click on the `OK` button.
  The window `Elasticsearch storage mode` is displayed.

```
Choosing slow storage for elasticsearch will increase the potential retention duration,
but it will negatively impact the performances and speed of the gcenter.
It is strongly recommended to keep elasticsearch on fast storage.
Current storage type: fast
Maximum size on fast storage for elasticsearch: 15G
Maximum size on slow storage for elasticsearch: 99G
Current space used by elasticsearch: 1.0G`
```

- To change the current storage mode, press the `Switch storage type`.
  The screen becomes:

```
Storage type switch will preserve your data.
Moving high amount of data can greatly reduce the performances of your gcenter during the operation, and take up to one␣
↪hour.
Indexation will be paused while it is occurring.
The migration process will allocate the default data retention size on the target storage (see numbers above).
This allocation can later be extended to the maximum size for the target storage:
see WebUI configuration in Admin>Configuration>Global settings>Elasticsearch max data retention.

Maximum size for target storage type: 99G
Default data retention size on target storage type: 99G
Current space used by elasticsearch: 1,0G
```

- To start the operation, press the `Switch storage type and launch data migration`.
  The following message is displayed indicating the progress of the operation.

```
Elasticsearch storage mode configuration is running, this can take a while.
Storage mode reconfiguration preparation: Running
Amount of data on target storage / origin storage: Not running
Reconfigure storage mode: Not running
```

Note:

In case of error, the following message is displayed. In this case, contact the Gatewatcher support.

```
An error has been encountered during the procedure. As a result, the
GCenter could become unstable. Please, contact the gatewatcher support
quickly.
```

In case, validate the error message.

At the end of the operation, the storage type changed (in this example, it changed to `slow`).

```
Choosing slow storage for elasticsearch will increase the potential retention duration, but it will negatively impact␣
↪the performances and speed of the gcenter.
It is strongly recommended to keep elasticsearch  on fast storage.
Current storage type: slow
Maximum size on fast storage for elasticsearch: 15G
Maximum size on slow storage for elasticsearch: 999G
Current space used by elasticsearch: 1.0G
```

- Click on the `Back` button to return to the general menu.

6.15 `LPM Mode` command

6.15.1 Introduction

The `LPM Mode` command enables or disables MPL mode.
The current status is indicated. For example, `Disabled` indicates that LPM Mode is disabled.

Note:

For more information on the LPM, refer to *Military Programming Law (MPL)*.

6.15.2 Prerequisites

- User: setup

6.15.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.15.4 Procedure

The configuration menu is displayed.

- Select the `LPM Mode` line or press the letter **L**.
- Click on the `OK` button.
  The system displays the following message `Changing LPM mode will need to reboot the appliance. Are you sure?`.
- Click on the `Yes` button.

Important:

Please note! The system will reboot when the above operation is performed.
After this reboot, the GCenter will enter the selected mode.

6.16 `Restart` command

6.16.1 Introduction

The `Restart` command enables restarting the GCenter.

6.16.2 Prerequisites

- User: setup

6.16.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.16.4 Procedure

The configuration menu is displayed.

- Select the `Restart` line or press the letter **R**.
- Click on the `OK` button.
  The `Rebooting` window is displayed:

```
Rebooting in 10 seconds
You can still abort reboot by pressing <ESC> or <Cancel> button.
```

- Press:
- The `Reboot now` button to return to the menu
- The `Cancel` button to abort the reboot

6.17 `Shutdown` command

6.17.1 Introduction

The `Shutdown` command enables turning off the GCenter.

6.17.2 Prerequisites

- User: setup

6.17.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.17.4 Procedure

The configuration menu is displayed.

- Select the `Shutdown` line or press the letter **S**.
- Click on the `OK` button.
  The `Shutdown` window is displayed:

```
Shutting down in 10 seconds
You can still abort reboot by pressing <ESC> or <Cancel> button.
```

- Press:
- The `Shutdown now` button to return to the menu
- The `Cancel` button to abort the shutdown

6.18 `Reset` command

6.18.1 Introduction

The `Reset` command enables resetting the GCenter to its factory settings.
All configurations and data will be deleted.

6.18.2 Prerequisites

- User: setup

6.18.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu via SSH*
- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.18.4 Procedure

The configuration menu is displayed.

- Select the `Reset` line or press the letter **R**.
- Click on the `OK` button.
  The `Reset GCenter Appliance` window is displayed:

```
Warning
This tool will WIPE ALL DATA.
This means that you will loose connectivity and data.
It will restart the GCenter automatically.
```

- Press:
  - The `Yes` button to continue
  - The `Cancel` button to abort.

6.19 `Exit` command

6.19.1 Introduction

The `Exit` command enables closing the configuration menu.

6.19.2 Prerequisites

- User: setup

6.19.3 Preliminary operations

Depending on the situation:

- Either use *Direct connection to the GCenter configuration menu with keyboard and monitor*
- Either use *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
- Either use *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*

6.19.4 Procedure

The configuration menu is displayed.

- Select the `Exit` line or press the letter **E**.
- Click on the `OK` button.

Note:

If the connection to the GCenter is remote, it will be closed.
If the connection is made via iDRAC, the menu will close and the login page will be displayed.

6.20 Switching to a double interface configuration

6.20.1 Introduction

For further details on the single interface configuration and the double interface configuration, see the *`MGMT0` and `VPN0` network interfaces*.
This procedure outlines the switchover from a single interface configuration to a double interface configuration.

Important:

The user will lose the session if the connection between the GCenter and the user's PC is made remotely via SSH.
In order to avoid this disconnection, connect to the GCenter (see the Preliminary operations).

6.20.2 Prerequisites

- **User:** setup

6.20.3 Preliminary operations

- As appropriate, refer to:
  - The *Direct connection to the GCenter configuration menu with keyboard and monitor*
  - The *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
  - The *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*
- Stop the detection engine (see the GCap documentation)

6.20.4 Procedure for displaying the current configuration

The configuration menu is displayed.

- Select the *Network* line or press the letter N.
- Click on the *OK* button.

  The *Hostname configuration* window is displayed:

```
Hostname configuration
Interface configuration: mgmt0  Enabled
Interface configuration: vpn0   Disabled
Interface configuration: icap0  Disabled
Interface configuration: sup0   Disabled
DNS configuration
NTP configuration

_____________________________________________

      <Configure>       <Back>
```

For each of the 4 interfaces, the system displays its status.

The single interface configuration is indicated by :

- the status of mgmt0: Enabled
- the status of vpn0: Disabled
  - **Single interface configuration**

    SSH and VPN connections are handled by the mgmt0 interface.

    In this case, the system displays:

```
Hostname configuration
Interface configuration: mgmt0  Enabled
Interface configuration: vpn0   Disabled
```

    In this example, the current configuration is single-interface, vpn0 is Disabled In this case, continue with this procedure.
  - **Double interface configuration**

    The SSH connection for GCenter management is handled by the `mgmt0` interface.

    The VPN communication is controlled by the `vpn0` interface.

    In this case, the system displays:

```
   Hostname configuration
   Interface configuration: mgmt0  Enabled
   Interface configuration: vpn0   Enabled

In this case, there is nothing to do.
```

6.20.5 Procedure for switching from single to double interface configuration

- First of all, unpair the GCap: to do so, refer to the GCap documentation
- Use the network command to modify the status of the VPN0 (from disable to enable) : to do so , refer to the *`Network` command*
- Rewire the network cables if necessary.
- On the GCap; use `the Pairing between a GCap and a GCenter` procedure.

6.21 Switching to a single-interface configuration

6.21.1 Introduction

For further details on the single interface configuration and the double interface configuration, see the *`MGMT0` and `VPN0` network interfaces*.
This procedure outlines the switchover from a double interface configuration to a single interface configuration.

Important:

The user will lose the session if the connection between the GCenter and the user's PC is made remotely via SSH.
In order to avoid this disconnection, connect to the GCenter (see the Preliminary operations).

6.21.2 Prerequisites

- **User:** setup

6.21.3 Preliminary operations

- As appropriate, refer to:
  - The *Direct connection to the GCenter configuration menu with keyboard and monitor*
  - The *Direct connection to the GCenter configuration menu in HTTP via iDRAC (DELL server)*
  - The *Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode*
- Stop the detection engine (see the GCap documentation)

6.21.4 Procedure for displaying the current configuration

The configuration menu is displayed.

- Select the *Network* line or press the letter N.
- Click on the *OK* button.
  The *Hostname configuration* window is displayed:

```
Hostname configuration
Interface configuration: mgmt0  Enabled
Interface configuration: vpn0   Enabled
Interface configuration: icap0  Disabled
Interface configuration: sup0   Disabled
DNS configuration
NTP configuration

_____________________________________________

      <Configure>       <Back>
```

For each of the 4 interfaces, the system displays its status.

The double interface configuration is indicated by:

- The status of mgmt0: Enabled
- The status of vpn0: Enabled
  - **Single interface configuration**
    SSH and VPN connections are handled by the mgmt0 interface.
    In this case, the system displays:

```
Hostname configuration
Interface configuration: mgmt0  Enabled
Interface configuration: vpn0   Disabled
```

In this example, the current configuration is single interface, vpn0 is Disabled

In this case, there is nothing to do.

- **Double interface configuration**

  The SSH connection for the GCenter management is handled by the `mgmt0` interface.

  The VPN communication is controlled by the `vpn0` interface.

  In this case, the system displays:

```
Hostname configuration
Interface configuration: mgmt0  Enabled
Interface configuration: vpn0   Enabled
```

In this case, continue with this procedure.

6.21.5 Procedure for switching from double to single interface configuration

- First of all, unpair the GCap: to do so, refer to the GCap documentation
- Use the network command to modify the status of the VPN0 (from enable to disable): to do so , refer to the *`Network` command*
- Rewire the network cables if necessary.
- On the GCap; use `the Pairing between a GCap and a GCenter` procedure.

Chapter 7

Use cases at the operator or analyst level

7.1 Connection to the GCenter web interface via a web browser

7.1.1 Introduction

This procedure describes connecting from a remote computer to the GCenter web interface via a web browser.
This connection is the nominal way to access the web interface of the equipment.

7.1.2 Prerequisites

- User: all users

7.1.3 Preliminary operations

- Know the name of the GCenter or its IP address.
- Access GCenter from your workstation.

7.1.4 Procedure

On the remote PC:

- Open a web browser
- Enter the IP address or FQDN of the GCenter
- Validate.
  The GCenter login window is displayed.
- Enter the login name
- Enter the password
- Validate.
  The GCenter graphical interface is displayed.

Note:

During the first login, it is necessary to change the password.
Passwords must comply with the password policy (see *Password management policy*).

7.2 Managing current user

This section describes how to manage the current user on the GCenter.
For more details on the accounts, see *Web interface accounts and their management*.

7.2.1 Changing the checking account password

7.2.1.1 Introduction

This procedure describes how to change the current user's password.
To enter a new password consistent with the policy to be applied, the system proposes six passwords.
A `REGENERATE` button enables six new passwords to be generated.

7.2.1.2 Links associated

For information, see the paragraphe *Web interface accounts and their management*.
For presentation of the screen, see the *`Profile / Edit Password` screen*.

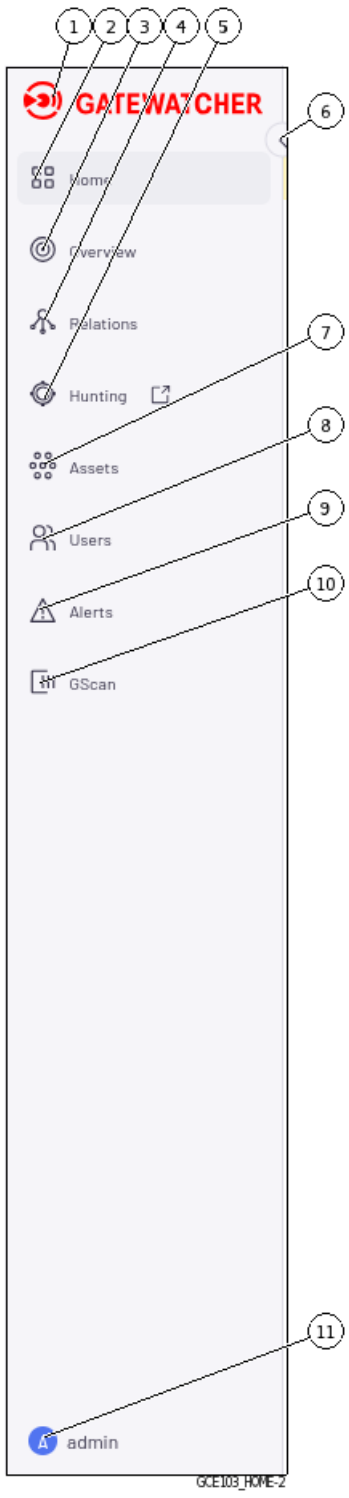
7.2.1.3 Prerequisites

Not Applicable

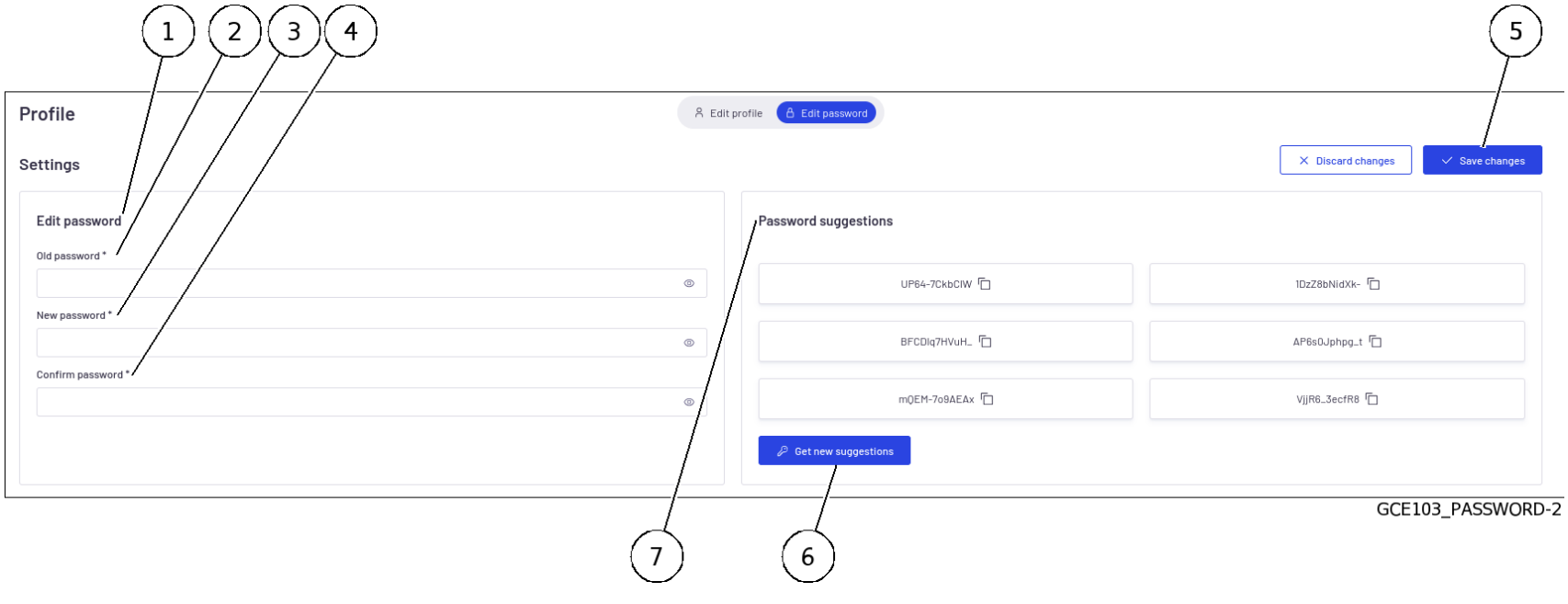
7.2.1.4 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

7.2.1.5 Procedure



- In the GCenter interface, click on the checking account button (11).
- Click on the `Edit password` command.



- Enter the previous password in the `Old password` field (2).
- Enter the new password in the `New password` field (3).

- Enter the new password in the `Confirm password` field (4).
  The password entered must match the *Password management policy*.
  The system checks the password against the verification policy.
  If the password does not meet the verification policy, one of the following messages will be displayed:
  - `Minimal length 12`: indicates a password that is too short (12 characters minimum)
  - `Uppercase`: indicates the lack of a capital letter
  - `Lowercase`: indicates the lack of a small letter
  - `Symbol`: indicates the lack of a special character
  - `Digit`: indicates the lack of a digit

  Note:

  To copy one of the proposed passwords, click on the right side of the password.
  A window will appear informing that the password is copied to the clipboard.
  To paste the password, right-click and then paste into each of the two fields.
  Make sure to note down the password before saving.

- Click on the `Save changes` button (5).

Note:

If the following message is displayed `you used this password recently, please choose a different one.`, enter a password that has not been used before.

7.2.2 Changing some of the current user's information

7.2.2.1 Introduction

This procedure describes how to modify local users:

- Email address
- First name
- Last name

7.2.2.2 Links associated

For information, see the *Web interface accounts and their management*.
For presentation of the screen, see the *`Profile / Edit profile` screen*.

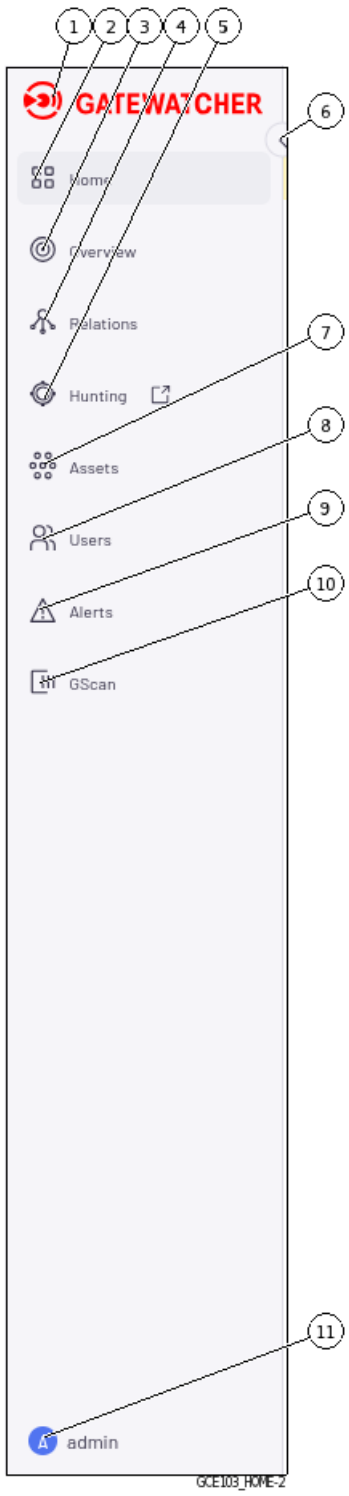
7.2.2.3 Prerequisites

Not Applicable

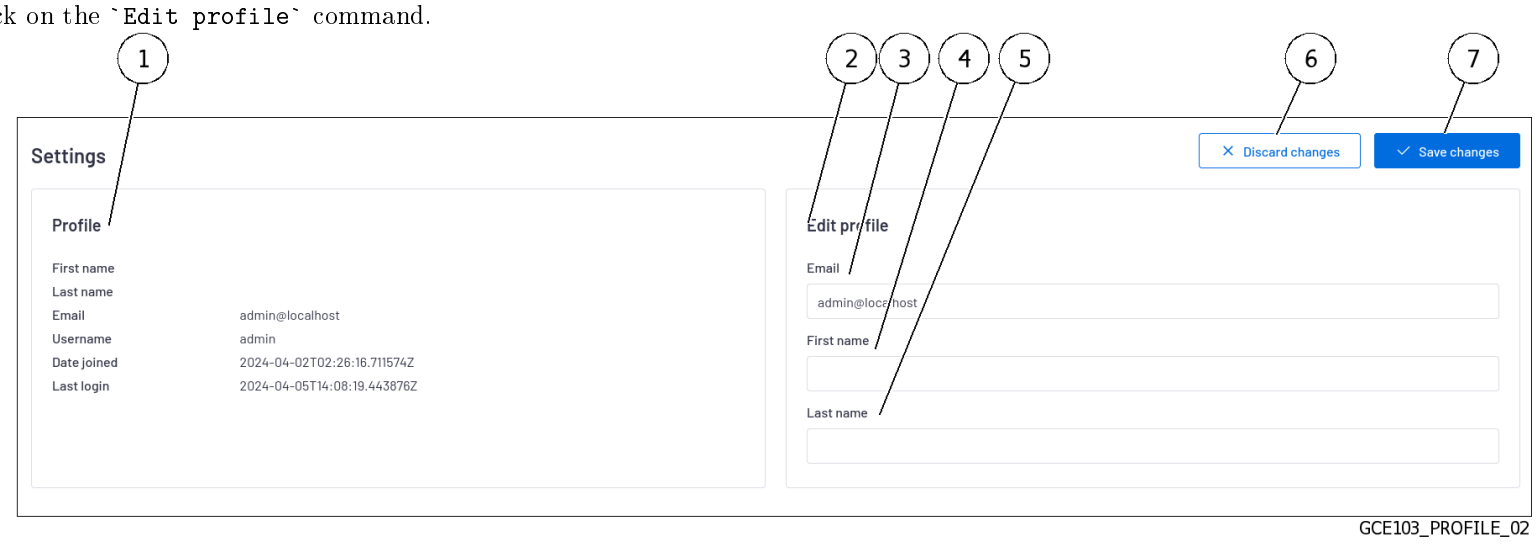
7.2.2.4 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

7.2.2.5 Procedure



- In the GCenter interface, click on the checking account button (11).
- Click on the `Edit profile` command.



The `Profile` area (1) shows account information such as username, creation date, and last login.

- Enter or modify the data found in the `Edit Profile` area (2):
- In the `Email ` field (3)
- In the `First name` field (4)
- In the `Last name` field (5)

- Confirm the changes using the `Save changes` button (7).
  A confirmation window displays the message `Profile successfully saved!`.

7.3 Configuring the Sigflow engine

This section describes the GCap configurations from the GCenter.

7.3.1 Managing the Sigflow engine rule sources

7.3.1.1 Introduction

A source is broken down as follows:

- Detection rules are found in categories
- Categories are found in sources
- Sources are in rulesets

Note:

Categories are not mandatory.
They enable improved organisation of the source.

This procedure describes:

- Managing the existing sources
- Managing the categories and rules made available in the sources
- Adding public or customized sources

Note:

Sources should be added to a **Ruleset** that will then be made available to the GCap.

For...	Successively apply the...
Visualise existing sources	- *Procedure to open the `Sources` window* - *Procedure to view the existing sources*
Add a public source	- *Procedure to open the `Sources` window* - *Procedure to add a public source*
Add a custom source	- *Procedure to open the `Sources` window* - *Procedure to add a custom source*
Delete a source	- *Procedure to open the `Sources` window* - *Procedure to delete a source*
Edit a source	- *Procedure to open the `Sources` window* - *Procedure to edit a source*
Update a source	- *Procedure to open the `Sources` window* - *Procedure to update a source*

7.3.1.2 Links associated

The rules and their organization are described in the *Organizing the rules* paragraph.
The graphic interface is described in the *`Rulesets` screen*.
See the *Updating rules sources*.

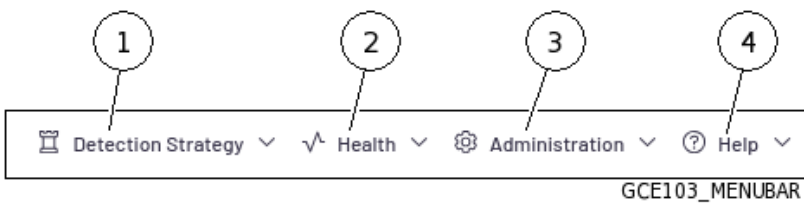
7.3.1.3 Prerequisites

- User: member of **Operator** group

7.3.1.4 Preliminary operations

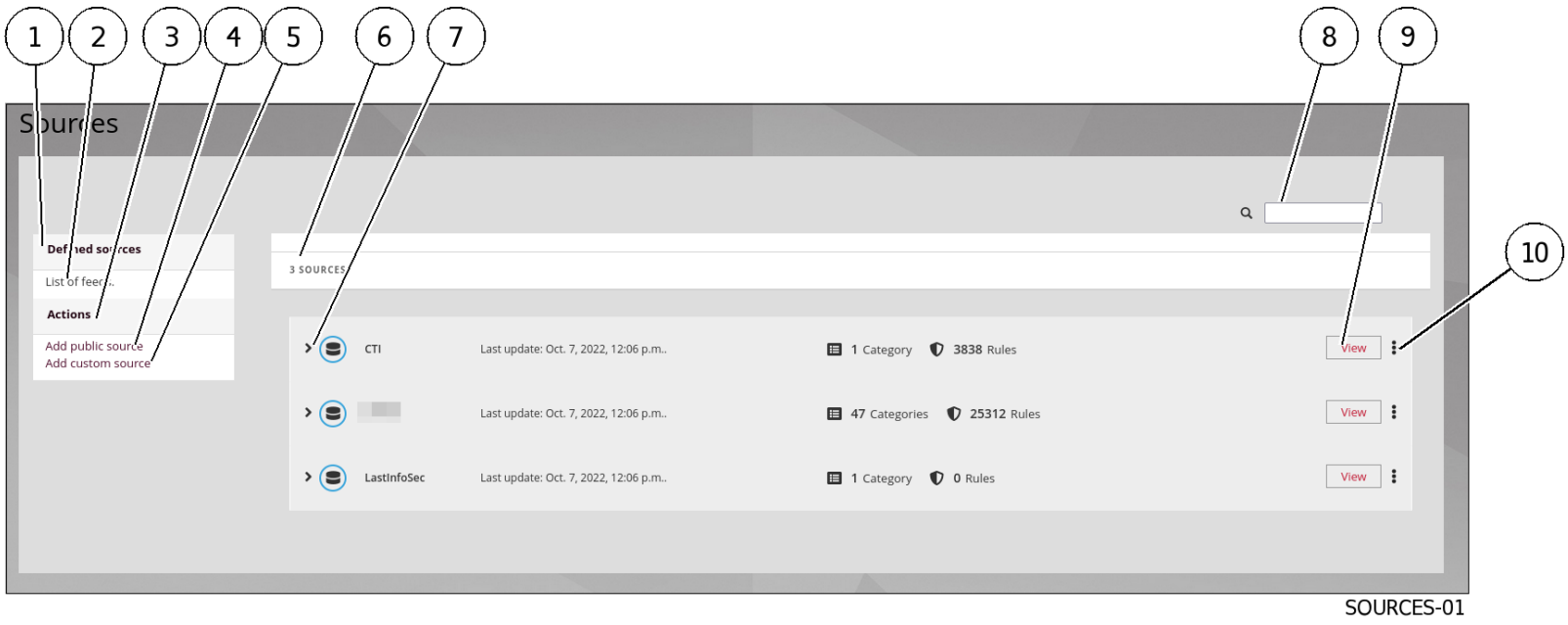
- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

7.3.1.5 Procedure to open the `Sources` window



- Click successively on :
  - The `Detection Strategy` menu (1)
  - The `Sources` command of the `Sigflow rules manager` heading
    The `Sources` window is displayed.

7.3.1.6 Procedure to view the existing sources



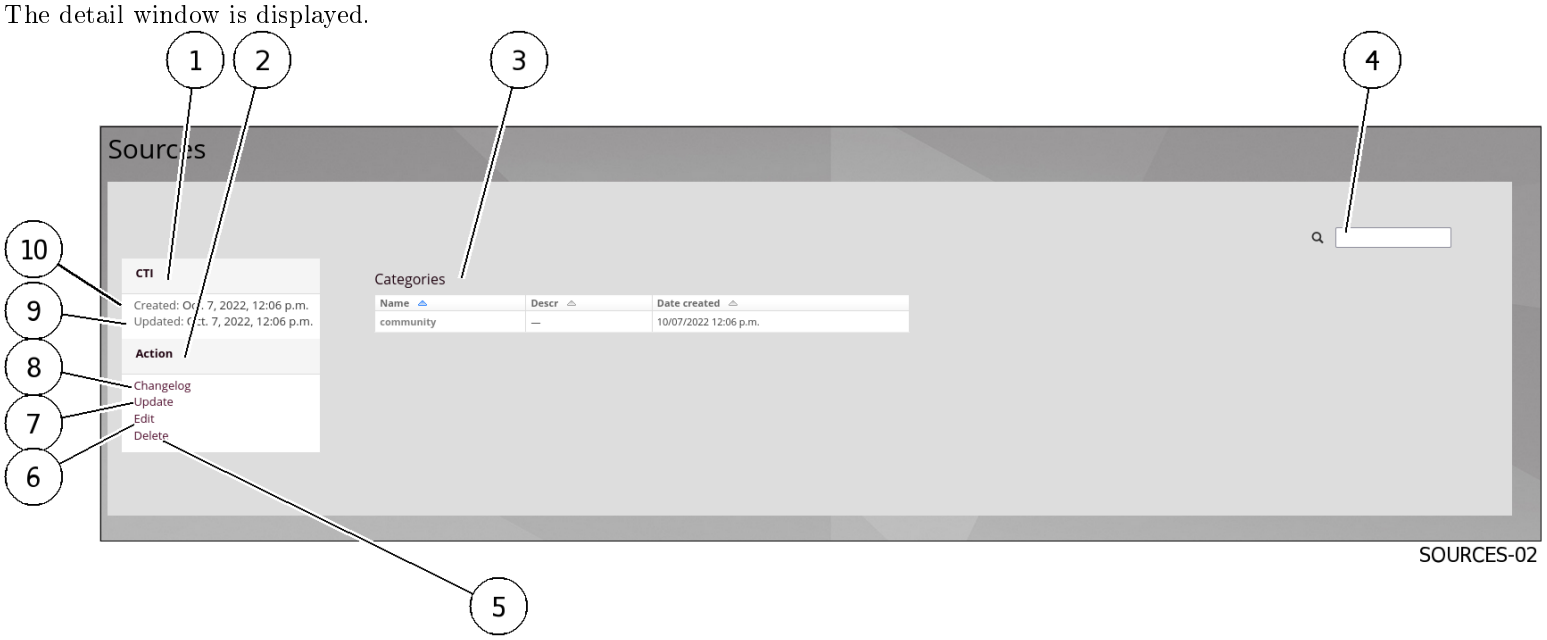
From the source management interface, the available sources are displayed (7).
The following types of information are displayed:

- The name of the source (CTI, Gatewatcher CTI...)
- The date and time of the last update
- The number of categories and signatures

Note:

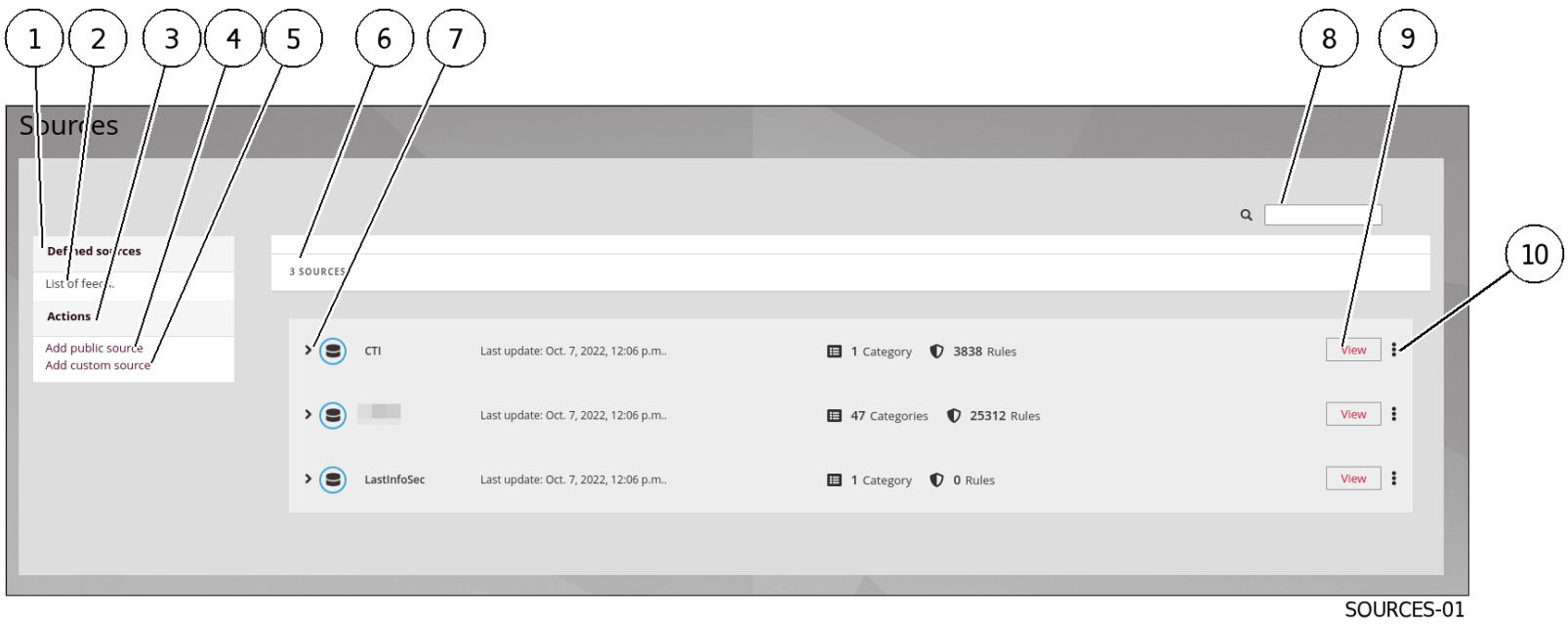
It is possible to add a MISP source.
For this, contact the administrator.

- To view the contents of the desired source, click on the `View` button (9).
  The detail window is displayed.

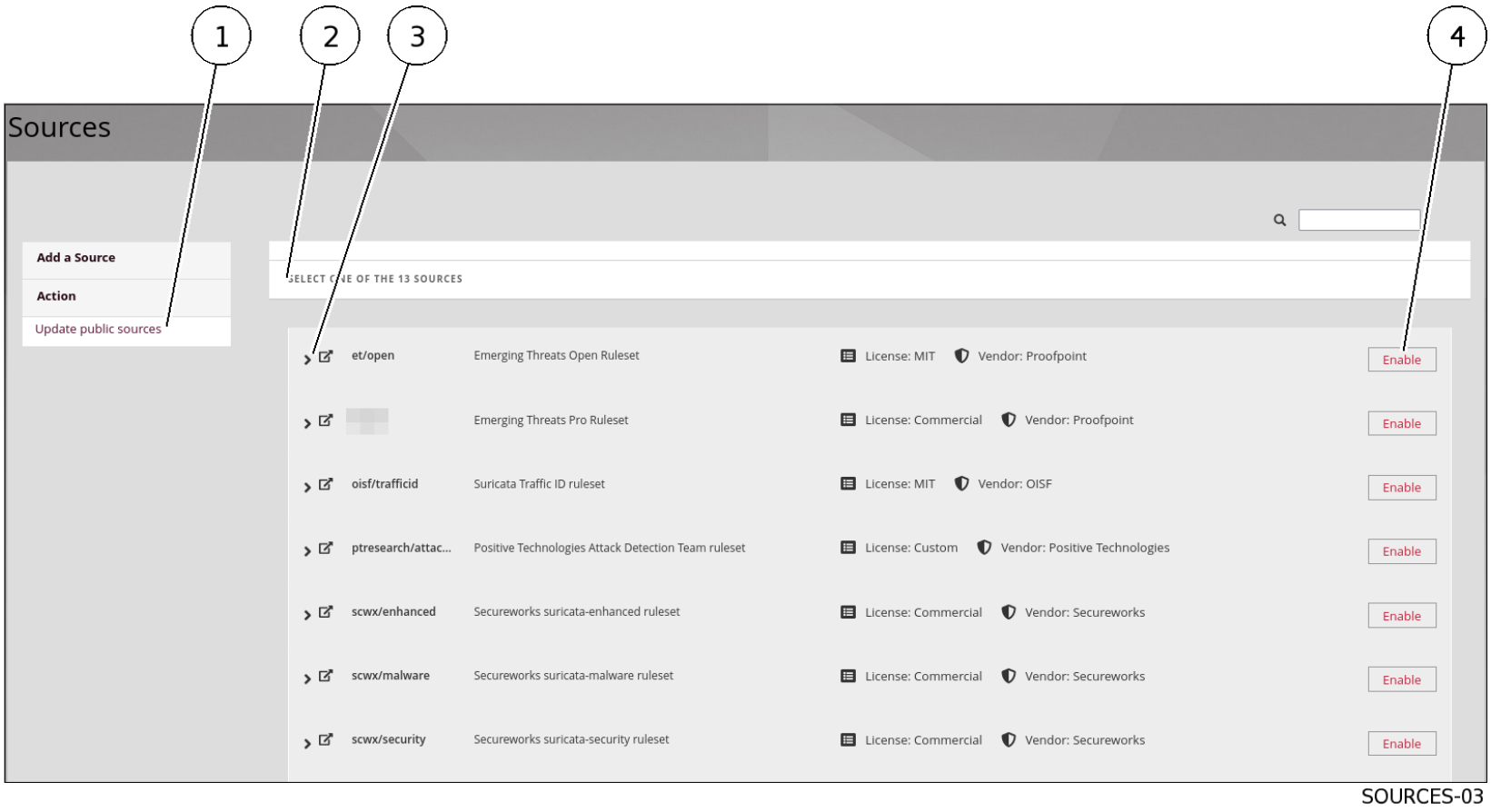


The source detail is detailed in *`Rulesets` screen*.

7.3.1.7 Procedure to add a public source



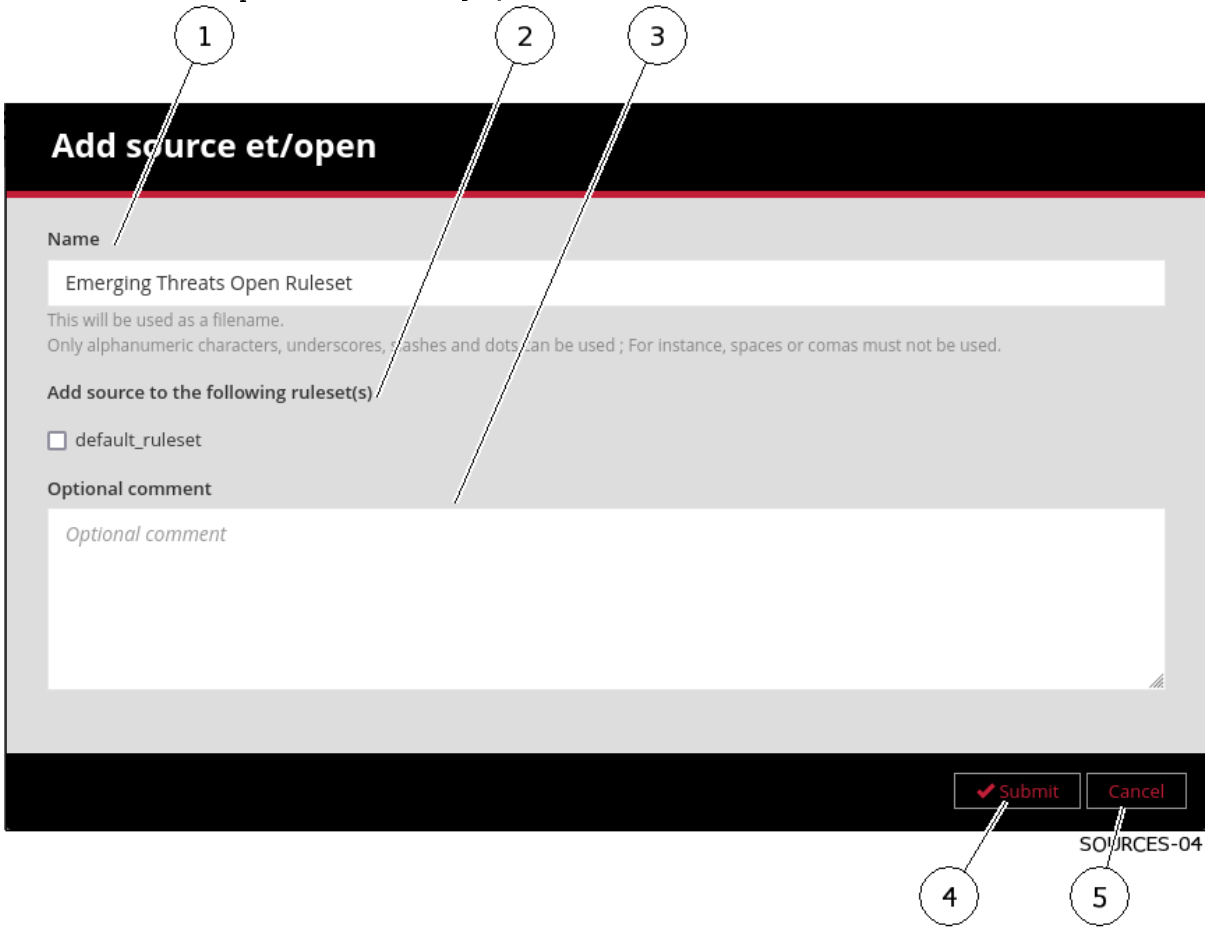
- Click on the `Add public source` link (4).
  The `Sources` window is displayed.



SOURCES-03

The window displays the list of available sources (2) when connecting to the Internet.
If the Internet connection is not active then an error message is displayed.

- Activate the desired public source (for example item 3) by clicking on the `Enable` button (4).
The `source and/open` window is displayed.



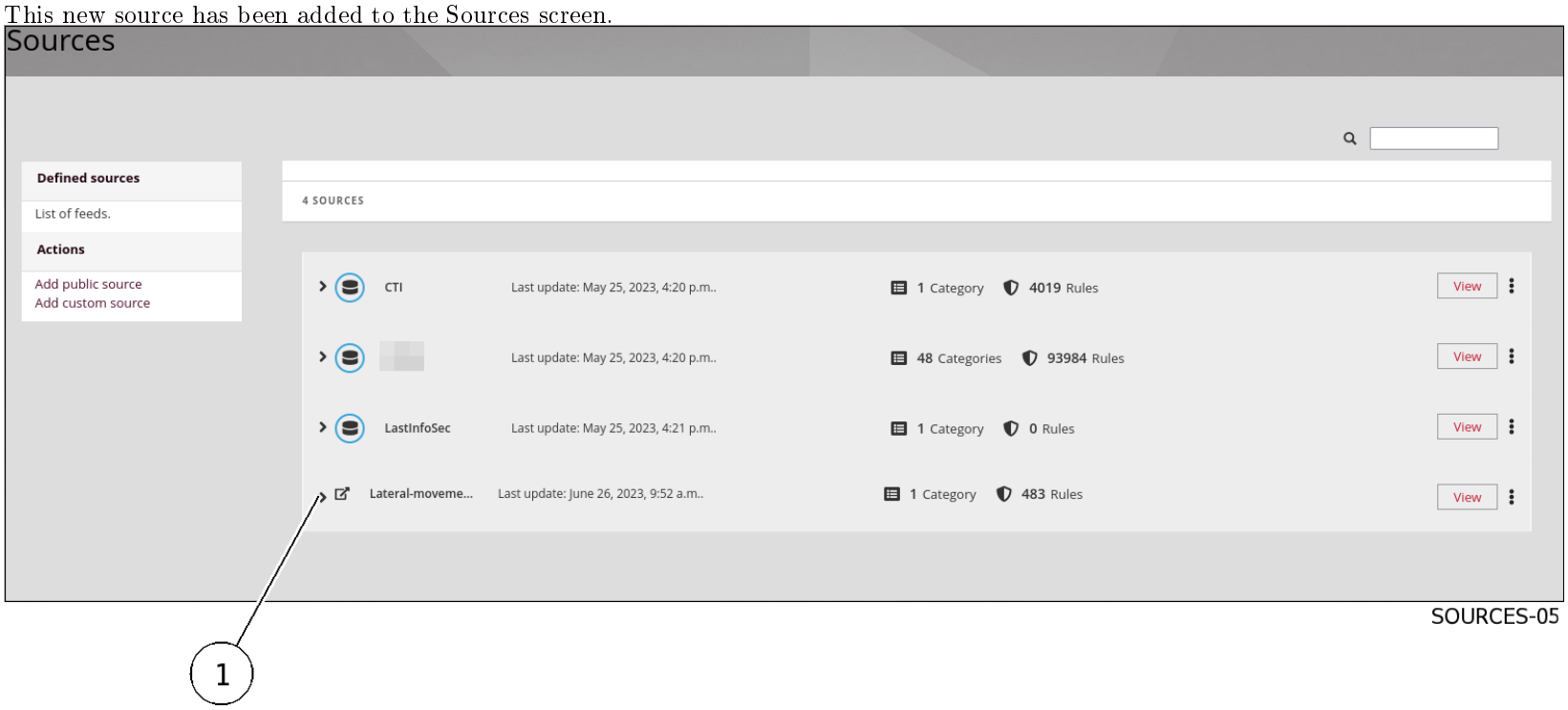
- Change source name (1) if needed.

Note:

The name is also the file name so only alphanumeric characters, underscore, slash and dot can be used. However, spaces and commas should not be used.

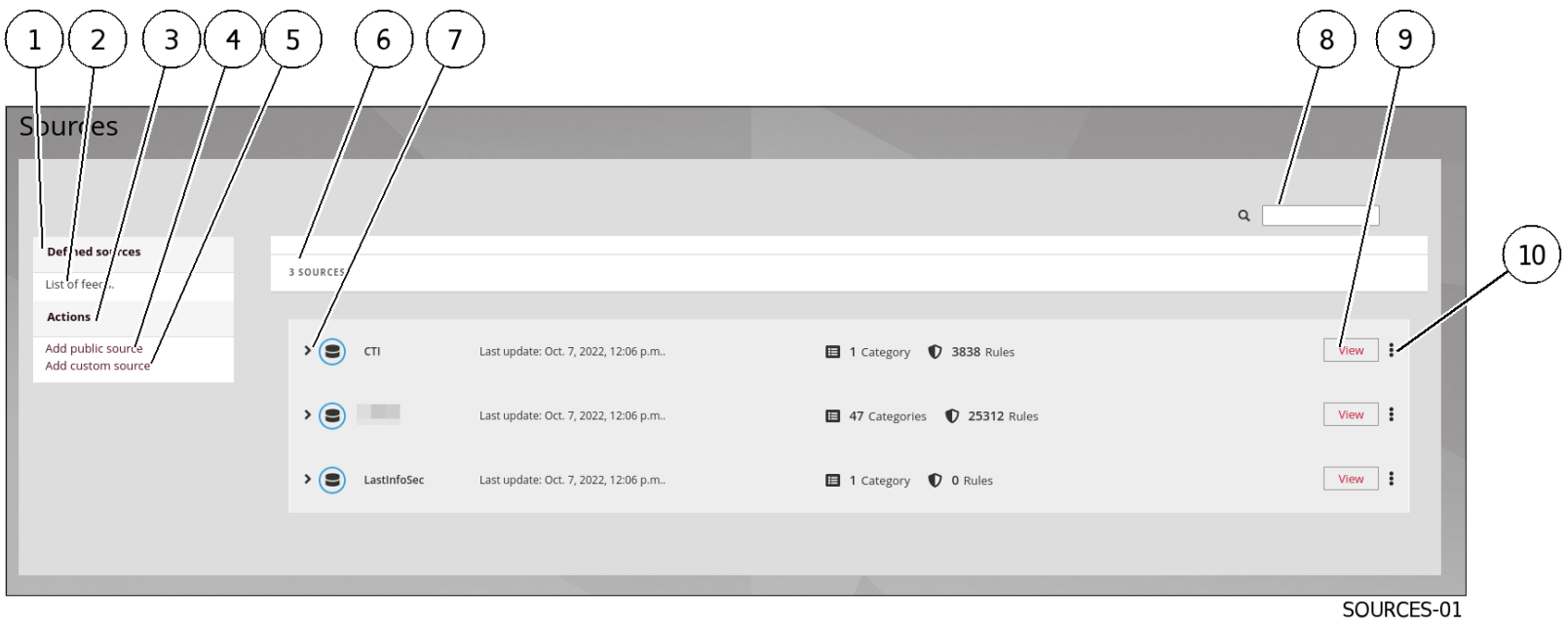
- Add the source to the default ruleset (2) if needed.
- Add a comment (3) if needed.
- Enter the source editor token if necessary.
- Validate the entry by clicking on the `Submit` button (4) or cancel with the `Cancel` button (5).

The message `Source fully activated` is displayed.
The message `Source updated` is displayed.
The `Source is valid` message is displayed.
A link is active to display the details of this new source.
This new source has been added to the Sources screen.



SOURCES-05

7.3.1.8 Procedure to add a custom source



SOURCES-01

Two methods are possible:

- Method 1: HTTP URL **or**
- Method 2: Upload

- **Method 1**: HTTP URL
  From the source management interface:

- Click on the `Add custom source` link (5)
- Enter a name for the added source
- Choose the `HTTP URL` method
- Choose the file format of the added rules: TAR archive (Signatures files in tar archive) or plain text file (Individual Signatures file)
- Enter the URL of the target file on the remote HTTP server
- Tick the ruleset in which to add the source - multiple ticks are possible
- If necessary, add a comment (optional)
- Click on the `Submit` button

- **Method 2**: Upload
  From the source management interface:

  - Click on the `Add custom source` link (5)
  - Enter a name for the added source
  - Choose the `Upload` method

- Choose the file format of the added rules: TAR archive (Signatures files in tar archive) or plain text file (Individual Signatures file)
- Tick the ruleset in which to add the source - multiple ticks are possible
- Choose the rules file to be added
- If necessary, add a comment (optional)
- Click on the `Submit` button

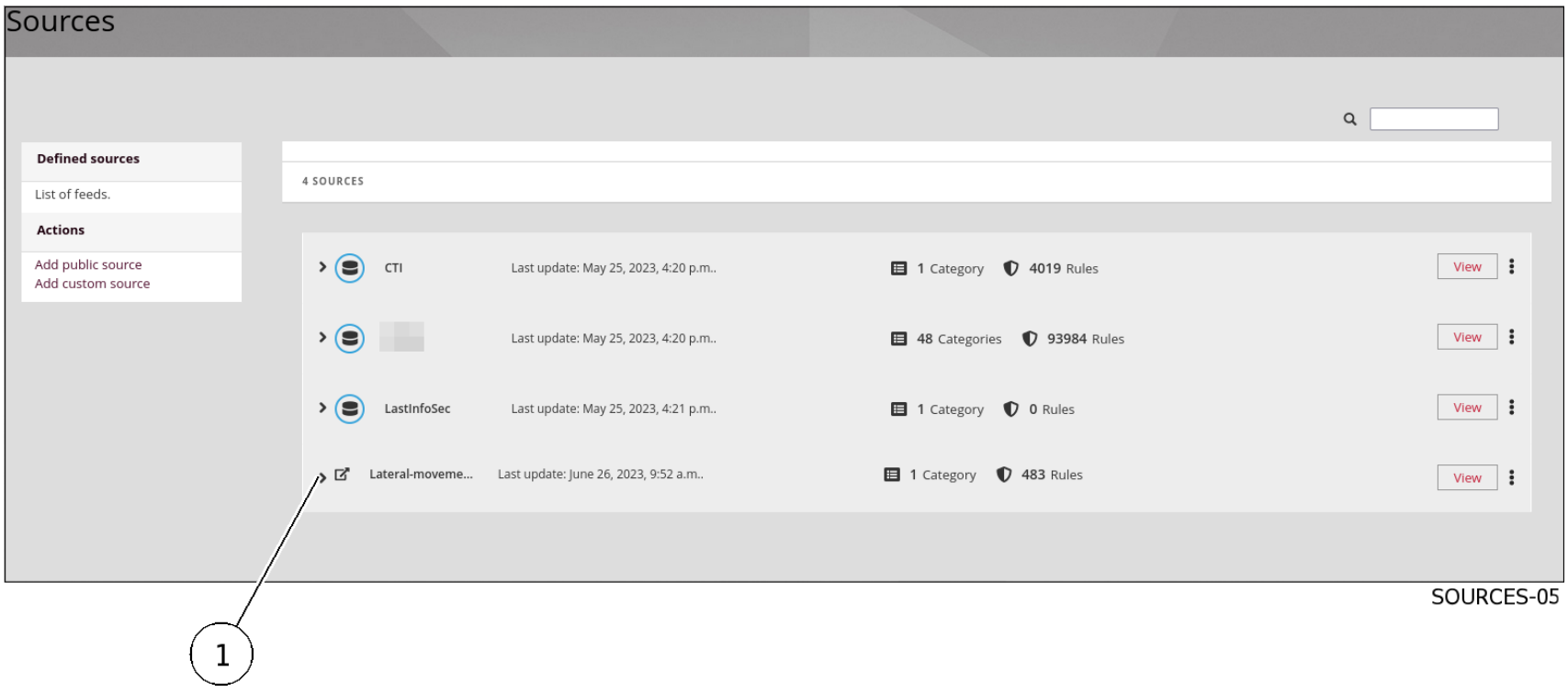
Checks are made, for example:

- the message `Error during source update: Invalid URL 'toto.com': No scheme supplied. Perhaps you meant http://toto.com?` indicates an error when entering the URL
- the message `Invalid filename` indicates that the source name format is not a file name

Note:

The rule files in the TAR archive enable creating categories within the source. The sub-folders in the archive will be the future source categories.

7.3.1.9 Procedure to delete a source



SOURCES-05

- Click on the three vertical points of the source to be deleted (1).
- Click on the `Delete source` command.

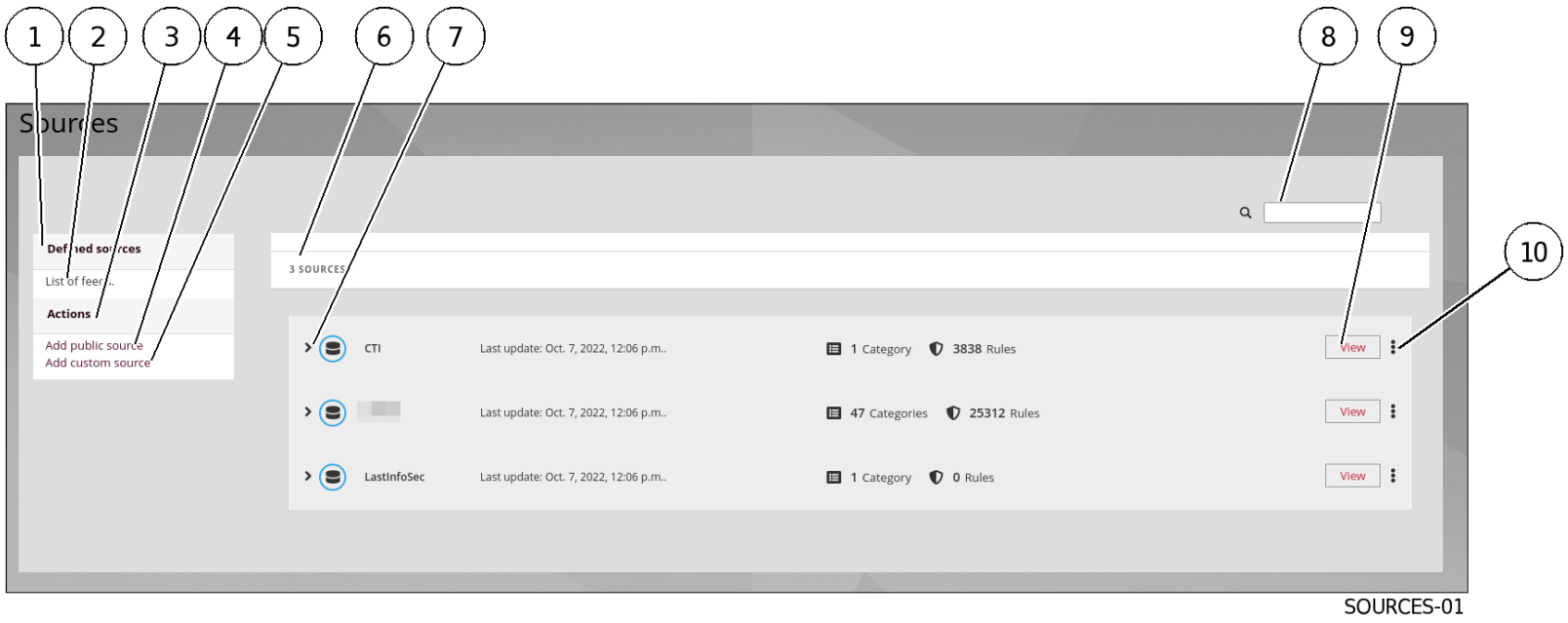
  A message `Are you sure you want to delete object ***?` is displayed.
- If necessary, add a comment (optional).
- Click on the `Delete object` button.

Or

- Click on the `View` button of the desired source
- Click on the `Delete` link, in the list of actions on the left.

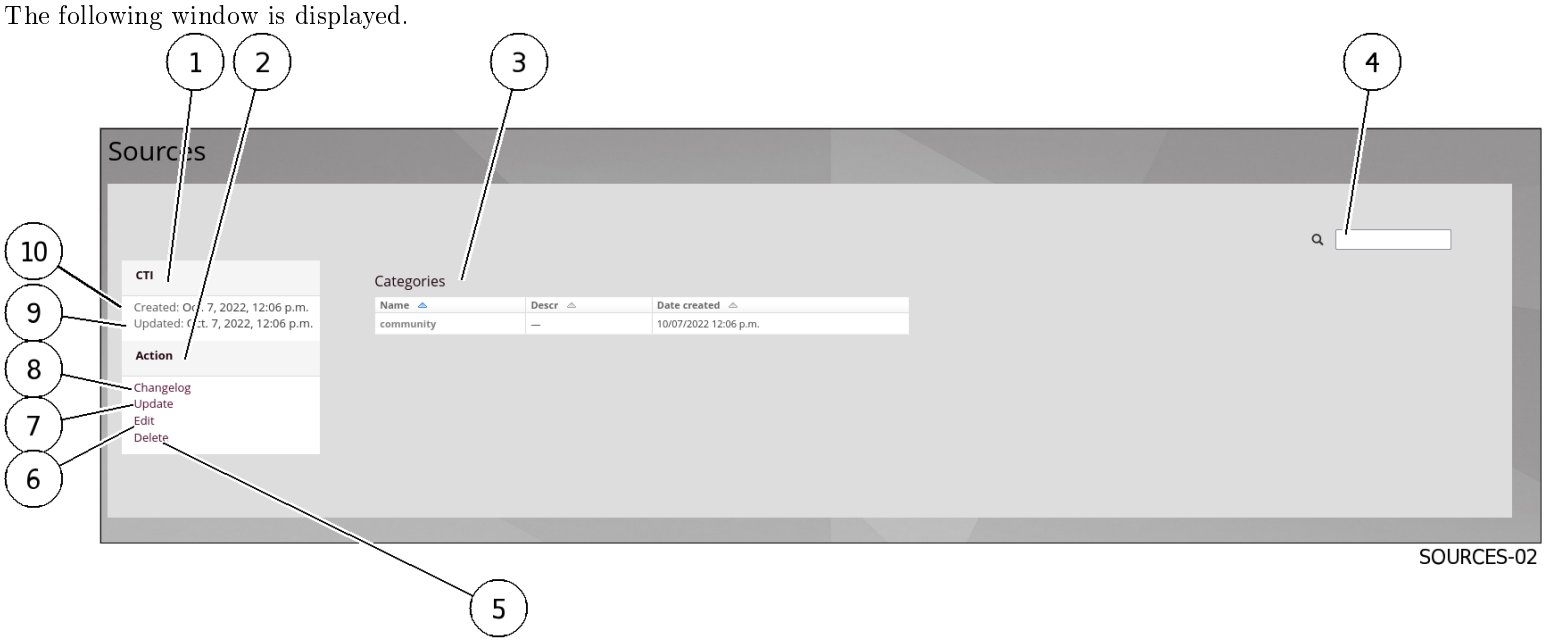
  A message `Are you sure you want to delete object ***?` is displayed.
- If necessary, add a comment (optional).
- Click on the `Delete object` button.

7.3.1.10 Procedure to edit a source



SOURCES-01

- Click on the `View` button (9) of the desired source.
  The following window is displayed.



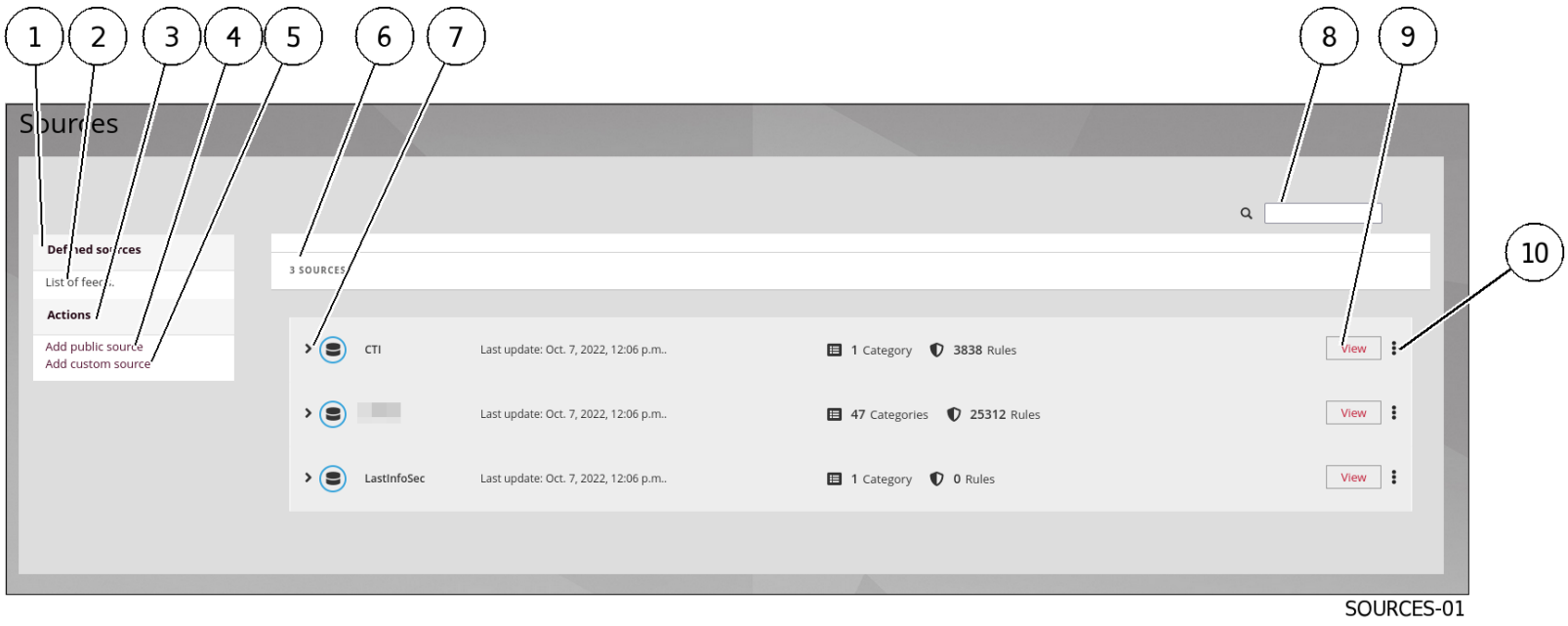
SOURCES-02

- Click on the `Edit` command (6).
- Change the desired parameters: method, file type, public source, and rules file.
- Add a comment if necessary - optional.
- Click on the `Submit` button.

7.3.1.11 Procedure to update a source

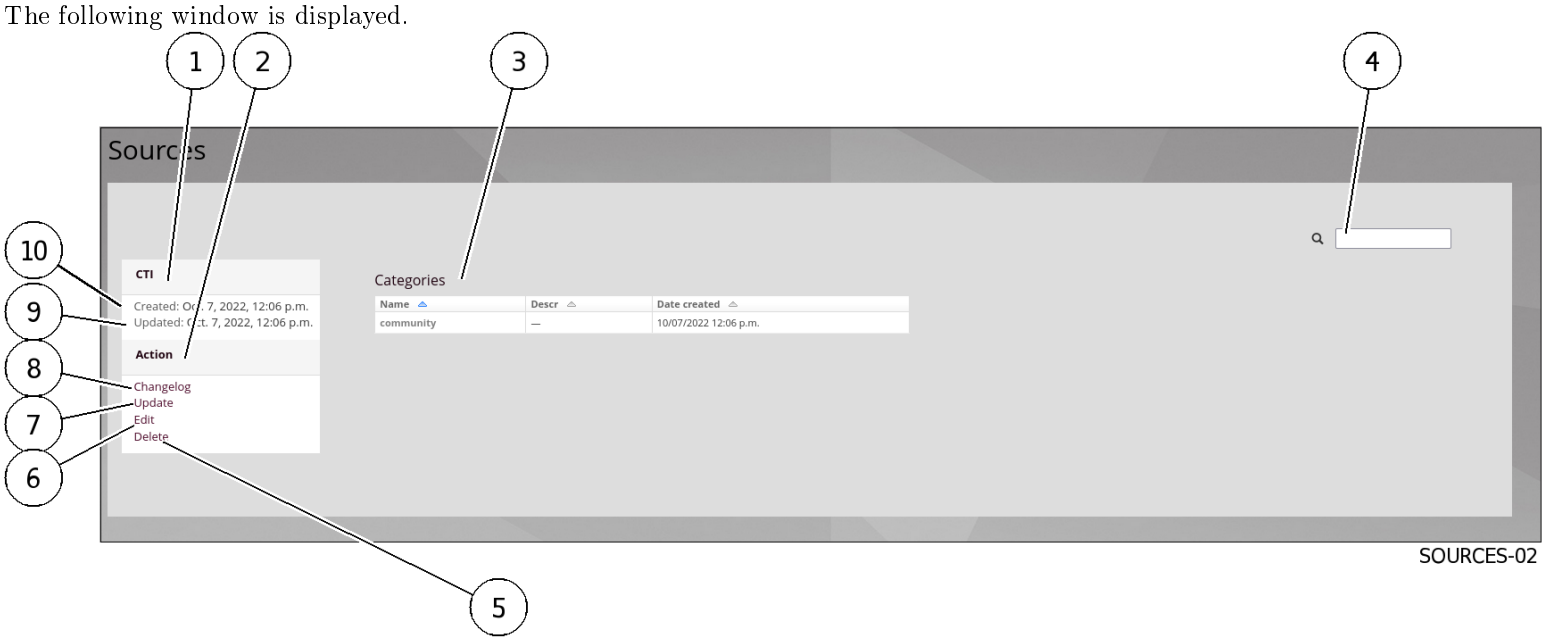
Note:

Updating sources via this procedure only applies to customized or public sources.
The update is performed if the rules file of the remote server or editor has been itself updated.



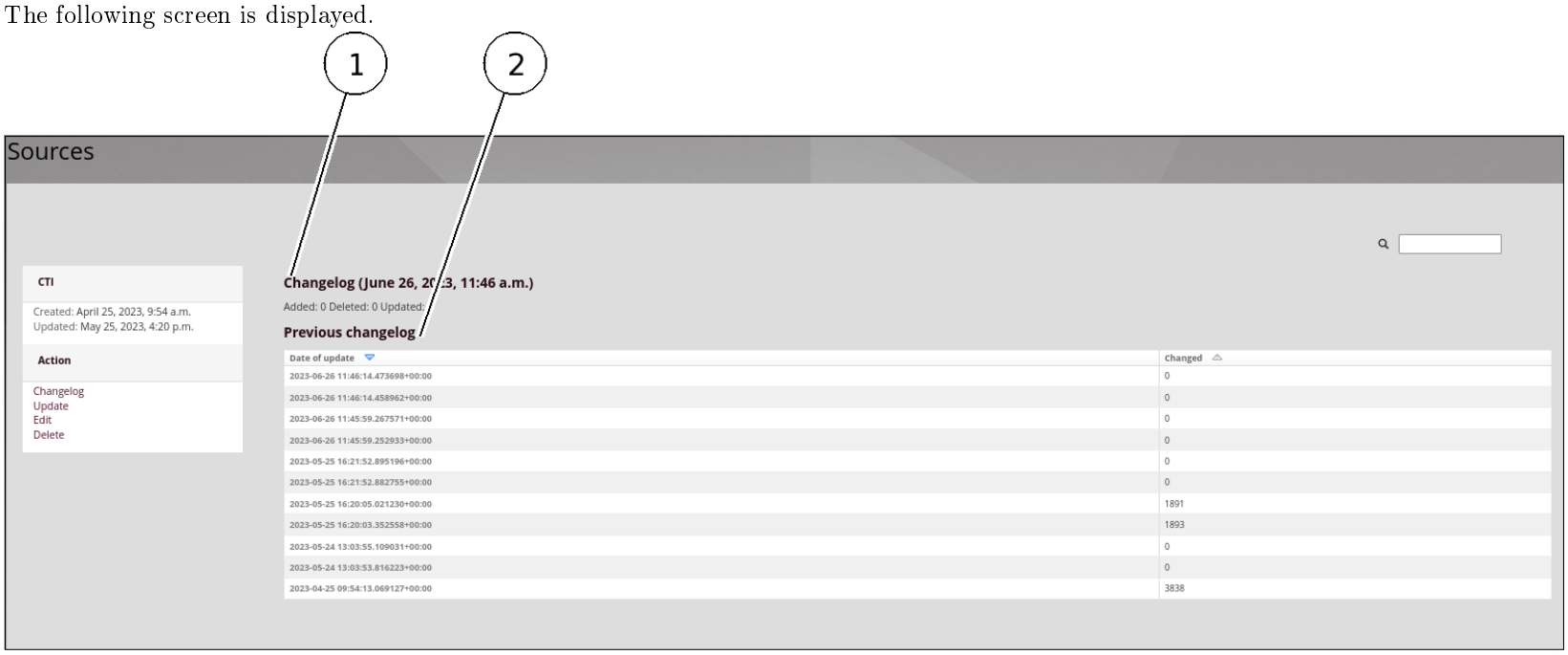
SOURCES-01

- Click on the `View` button (9) of the desired source.
  The following window is displayed.



SOURCES-02

- Click on `Update` command (7)
  The following screen is displayed.



SOURCES-06

The window shows:

- The summary (1)
- History (2)

It is possible to click on a changelog to view the content.

7.3.2 Managing a Sigflow engine ruleset

7.3.2.1 Introduction

The security policy in detection terms is held in what is called a ruleset.
The ruleset contains the rule sources enabling detection.
The detection rules in the ruleset will enable the GCap to raise security alerts on the traffic being scanned.
Multiple rulesets can be used to apply multiple security policies to the various capture points.

Note:

Managing a ruleset is only available to users assigned the role of operator.

This procedure describes different procedures to manage rulesets i.e:

For	Go to
Displaying a ruleset	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to display information about an existing ruleset*
Creating a ruleset	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to create a ruleset*
Copying a ruleset	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to copy a ruleset*
Deleting a ruleset	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to delete a ruleset*
Editing a ruleset	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to edit a ruleset*
Exporting a ruleset	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to export a ruleset*
Updating a ruleset	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to update a ruleset*

7.3.2.2 Links associated

For more information on Sigflow and its rules, see the paragraph *Sigflow engine*.
This configuration interface is described in the *`Rulesets` screen*.

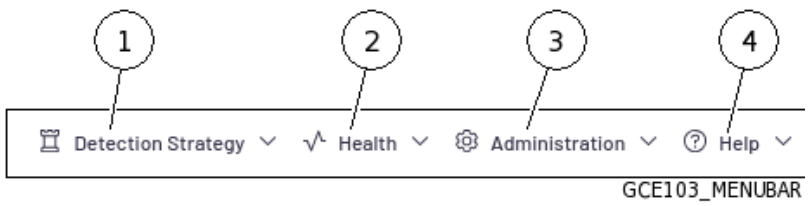
7.3.2.3 Prerequisites

User: member of **Operator** group

7.3.2.4 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

7.3.2.5 Procedure to open the `Rulesets` window



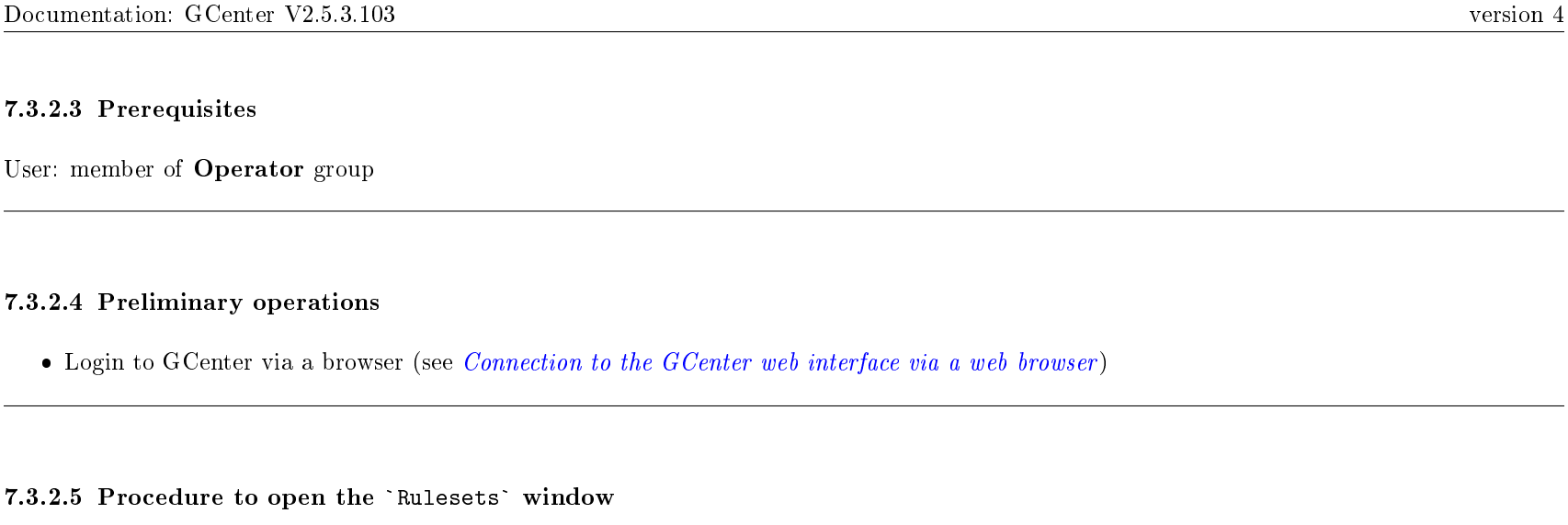
GCE103_MENUBAR

- From the navigation bar, click successively on:
- The `Detection Strategy` menu (1)
- The `Rulesets` command of the `Sigflow rules manager` sub menu.
  The `Rulesets` window is displayed.

7.3.2.6 Procedure to create a ruleset

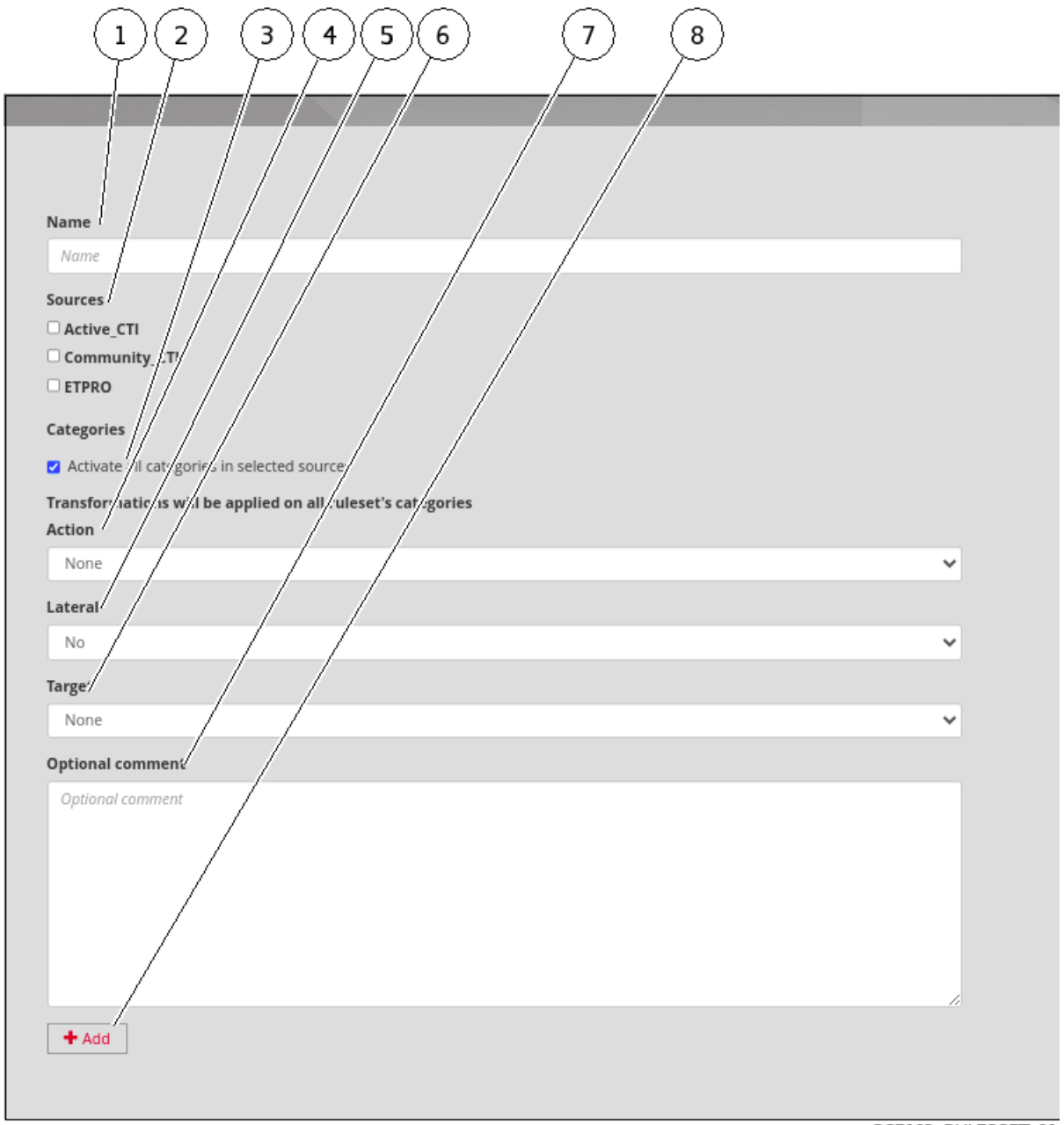
This procedure describes the creation of a ruleset i.e define:

- The ruleset name
- The selection of the sources
- The transformation rules if needed
- An optional comment



GCE103_RULESSET-06

- Click on the `Add` link (4) of the `Action` menu (3).
  The following screen is displayed.



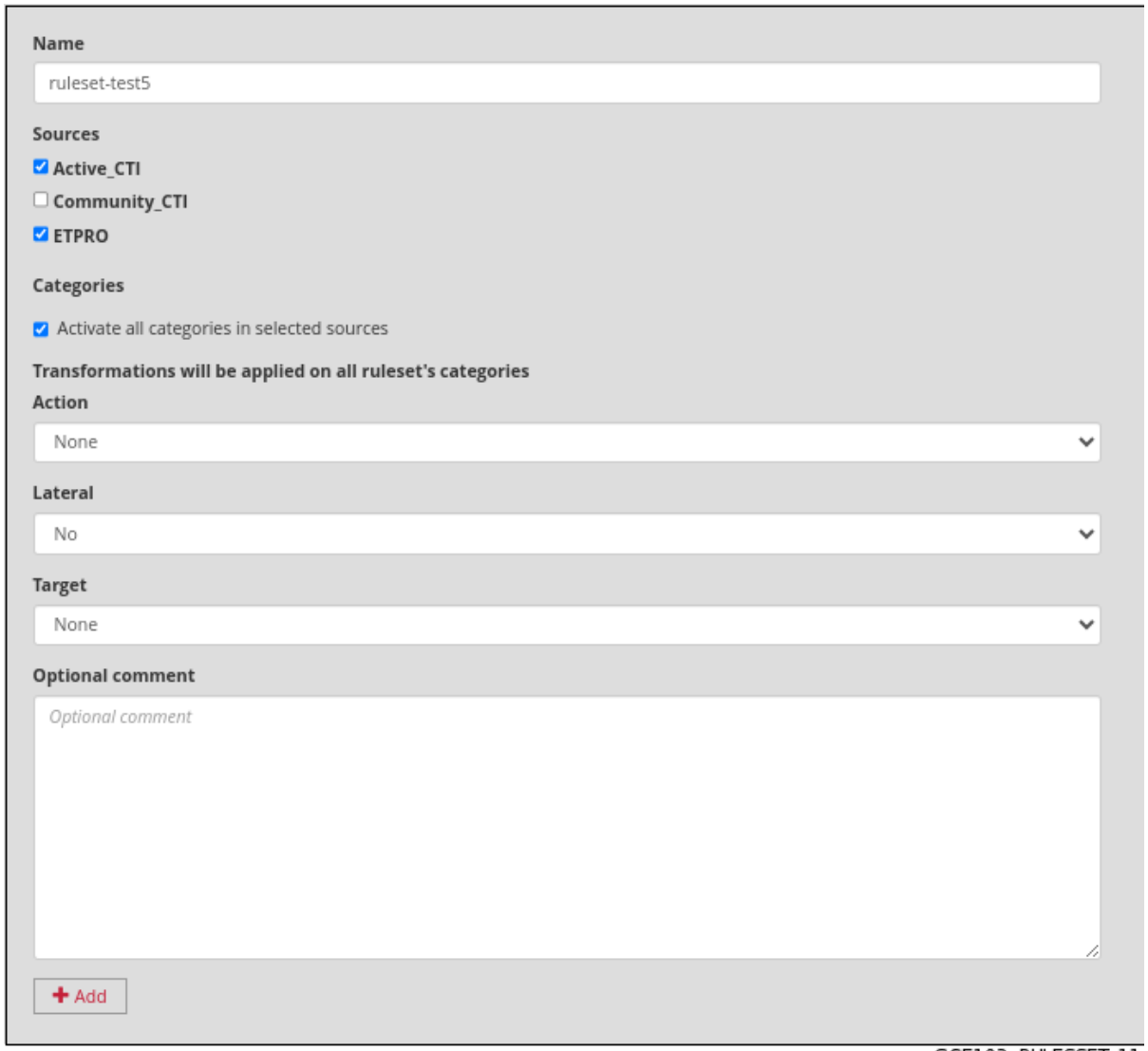
GCE103_RULESSET-01

- Enter a name of the created ruleset in the field (1), ruleset-test5 for example.
- Tick the sources (2) to be added.
- Leave the `Activate all categories in selected sources` checkbox ticked (3).

> **Note:**
>
> To have further information about these transformation rules, refer to *Transform rule*.

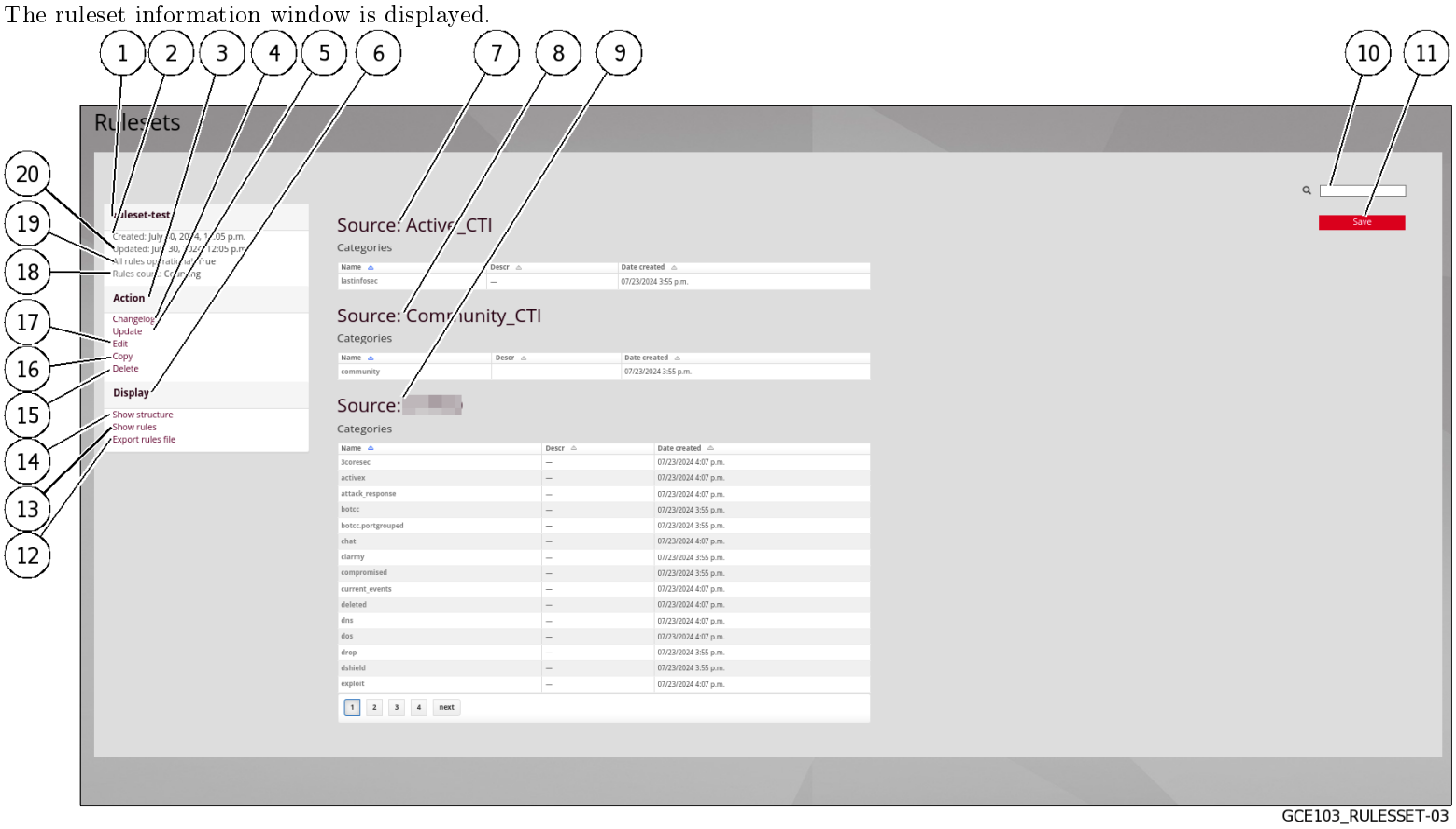
- Leave the `Action` (4), `Lateral` (5) , and `Target` (6) transformation fields as default.
- If necessary, add a comment (optional) (7).

  After entered, an example below is displayed.



GCE103_RULESSET-11

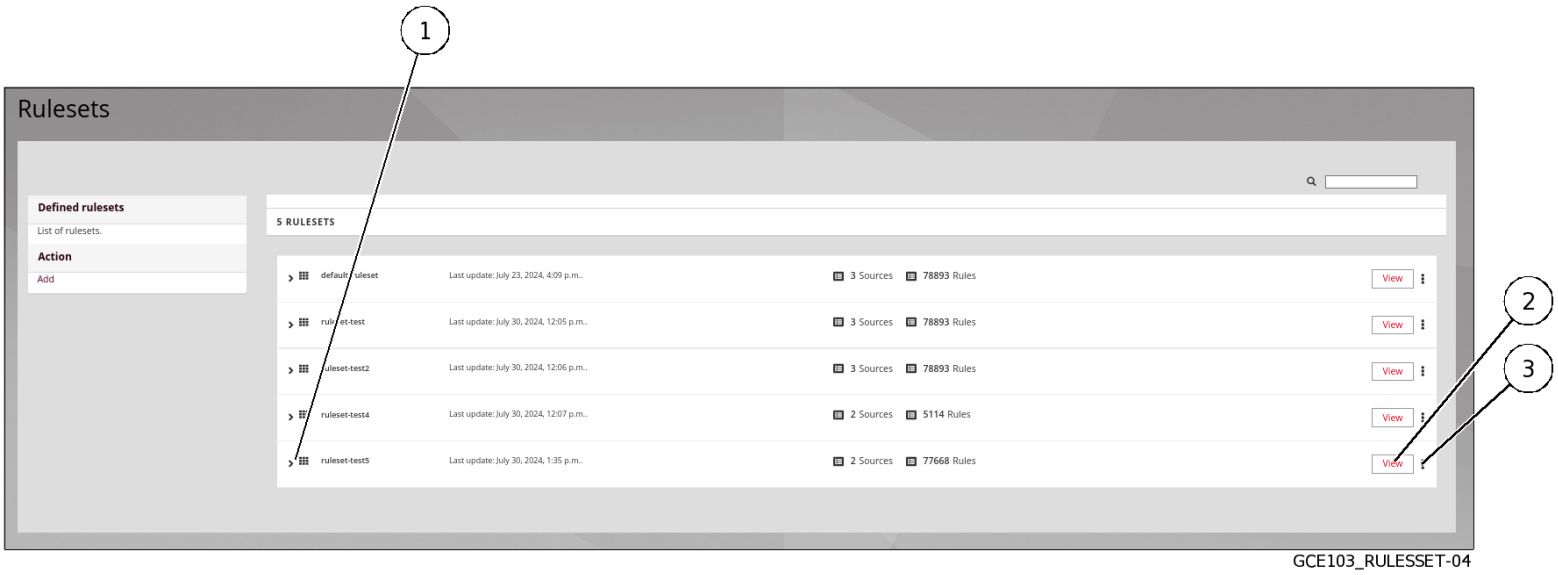
- Click on the `+ Add` button (8).
  The ruleset information window is displayed.



GCE103_RULESSET-03

This window gives information about the created ruleset.

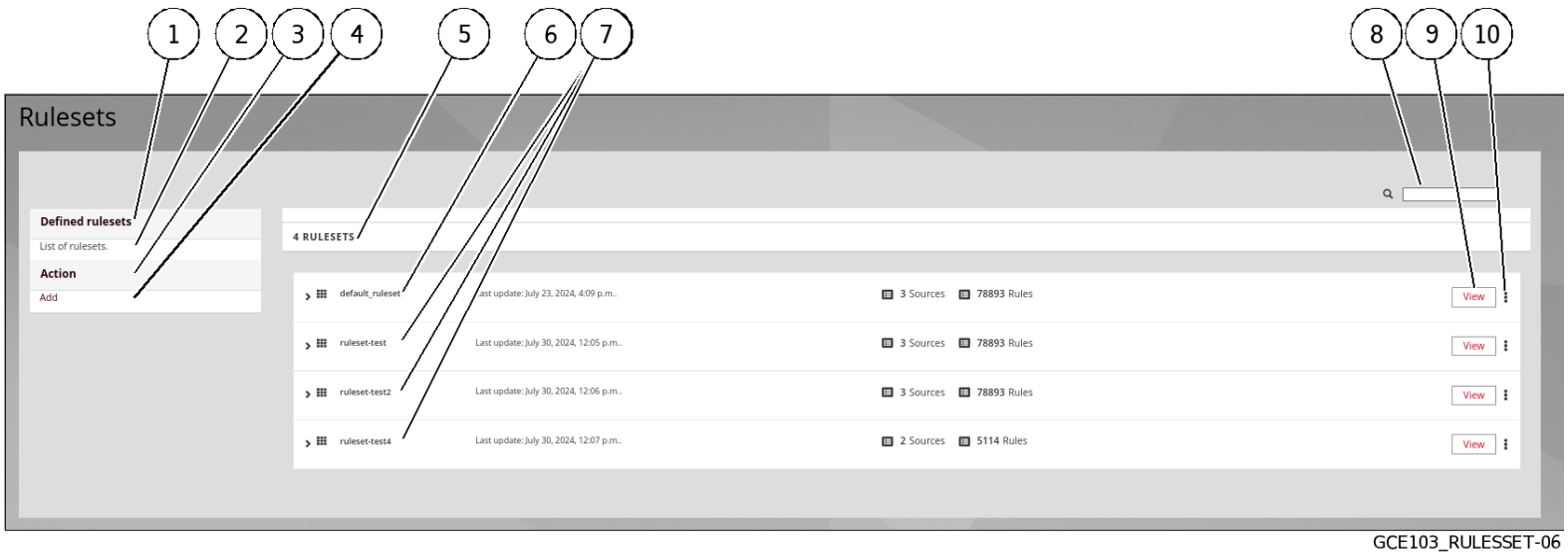
- Click on the `Save` button (11).



The new ruleset (1) is now displayed.

7.3.2.7 Procedure to display information about an existing ruleset

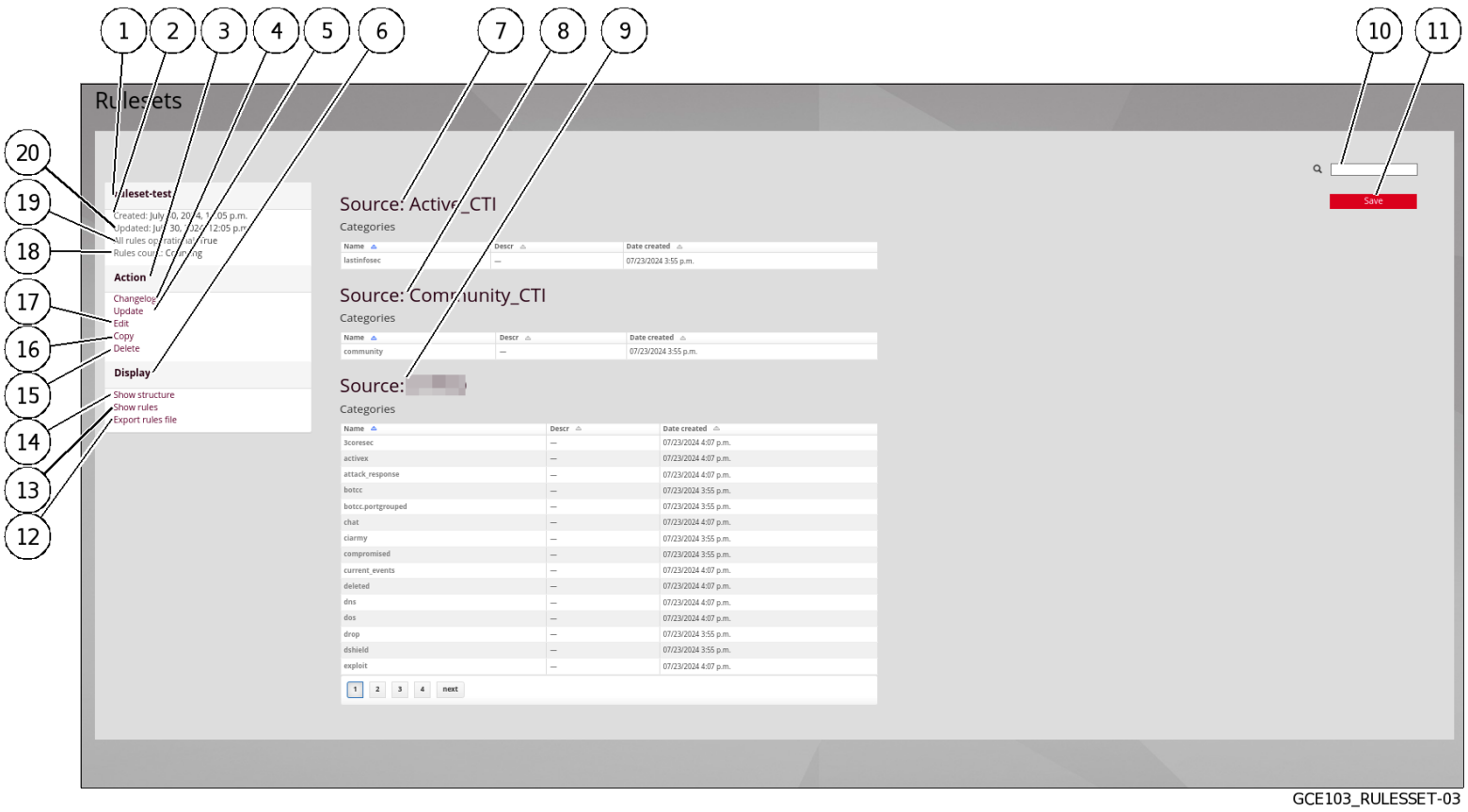
This procedure describes the ruleset information.



This screen displays:

- The ruleset number (5)
- The list of existing rulesets (6 and 7)

- Click on the `View` button (9) of the chosen ruleset.

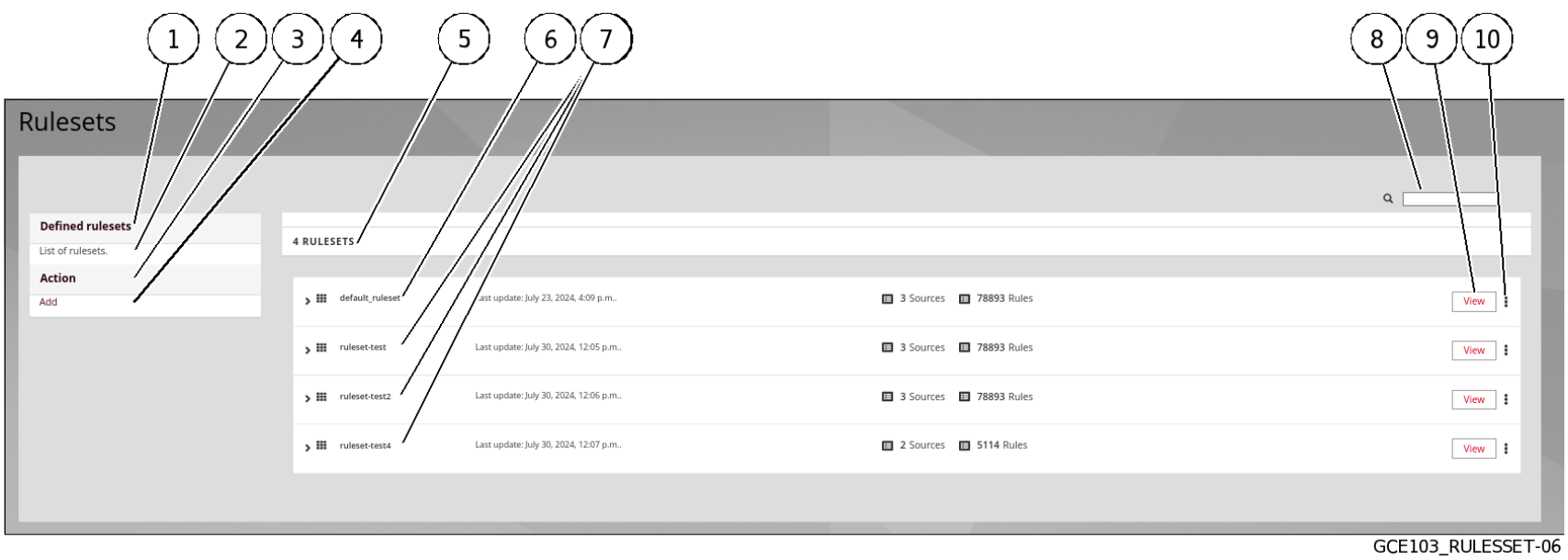


This window gives information:

- The left part of the window (General information) enables:
- Displaying general information (area 1) about the ruleset
- Displaying actions (3) with the commands of the `Action` menu
- Displaying specific information (6) with the commands of the `Display` menu
- The central part of the window (General information) displays:
- Source list (7 to 9)
- For each source, the categories list with the created date
- For each category, the ruleset list with the last updated date
- For each rule, the rule detail

7.3.2.8 Procedure to copy a ruleset

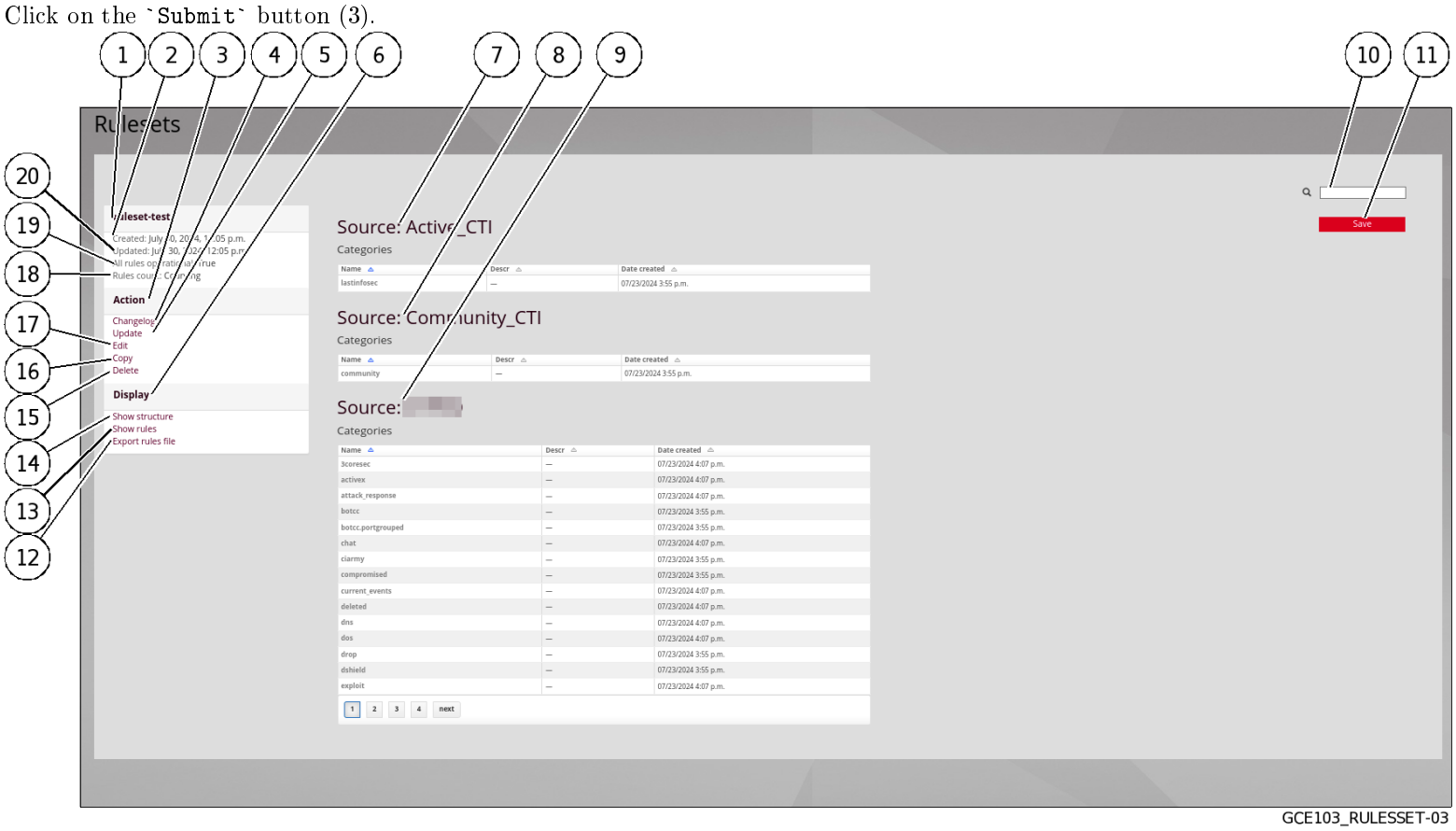
This procedure describes the ruleset copy: the copy will take into account the sources associated with the ruleset.
The administrator can decide to make a duplicate of the ruleset in order to assign it to another probe **GCap** for example according to the network flows that transit.
The ruleset is specific and must be optimized according to the probe to which it will be assigned.



- Click on the three vertical dots (10) of the ruleset to copy.
- Click on the `Copy ruleset` command.

GCE103_RULESET-07

- Enter the desired name for the new ruleset in the `Name` field (1).
- If necessary, add a comment (optional) in the `Optional comment` field (2).
- Click on the `Submit` button (3).



GCE103_RULESET-03

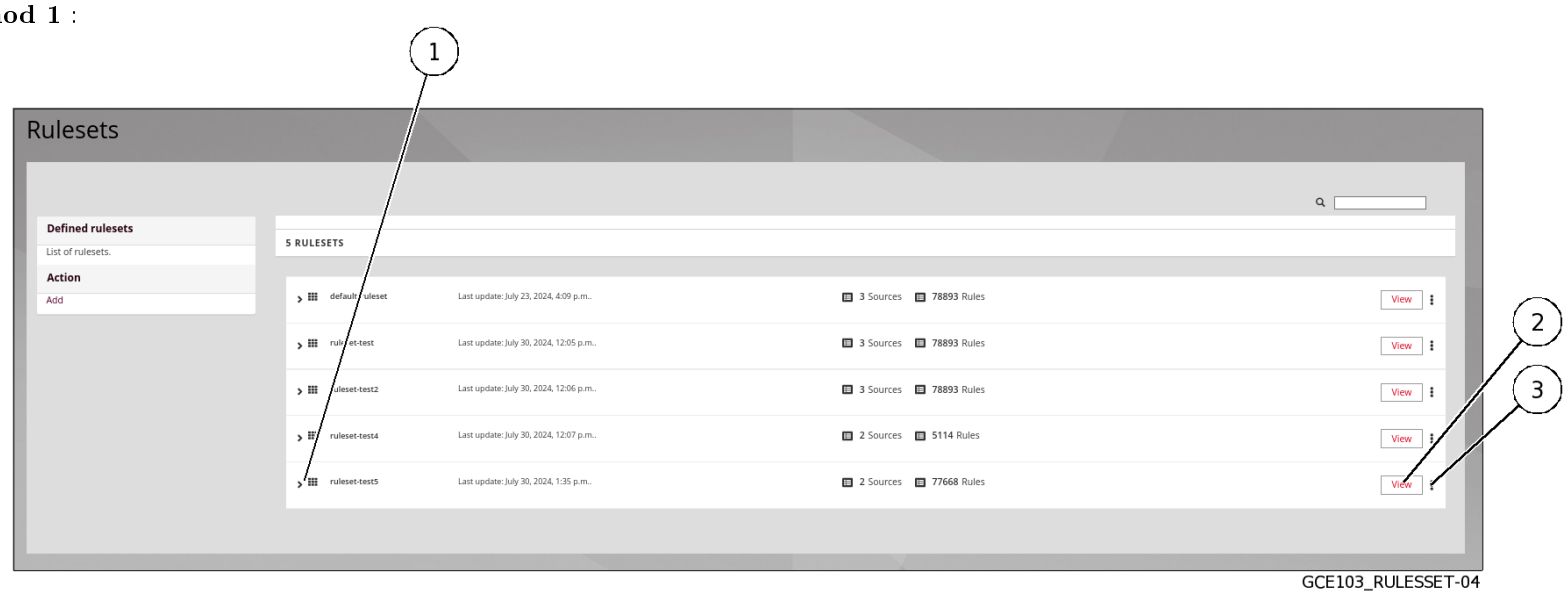
The windows resumes sources and their rules contained in this new ruleset

- Click on the `Save` button (11).
  The new ruleset is now displayed.

7.3.2.9 Procedure to delete a ruleset

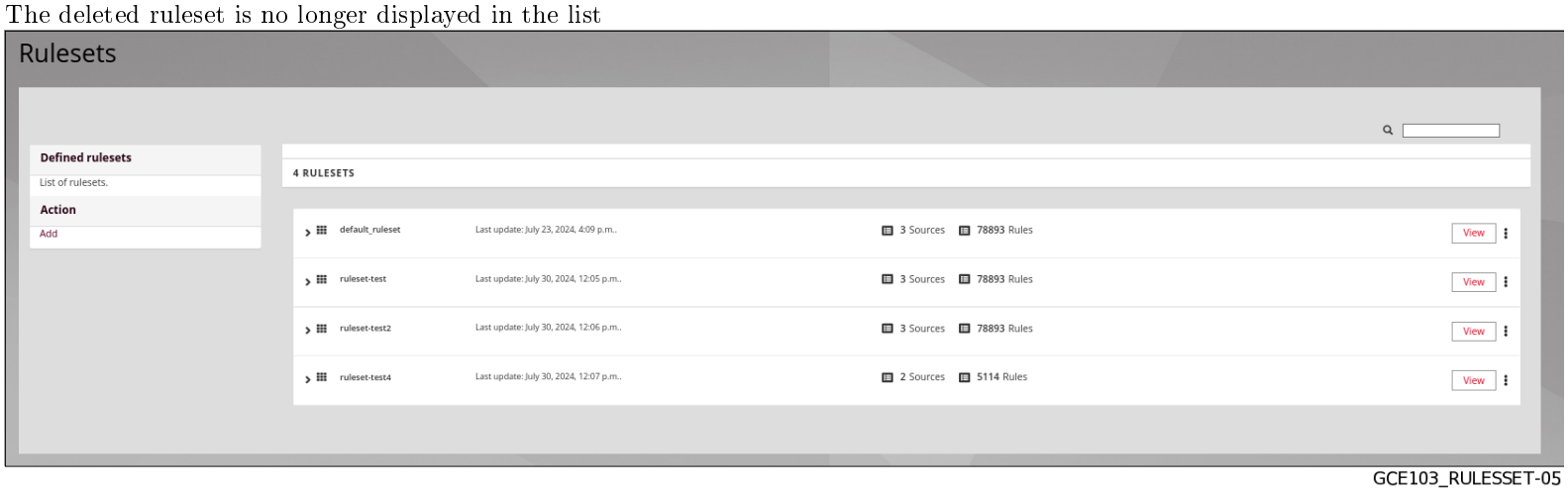
This procedure describes the ruleset deletion.
Deleting the ruleset is irreversible but will not cause the deletion of the sources and signatures that were linked to the ruleset.

- **Method 1** :



GCE103_RULESSET-04

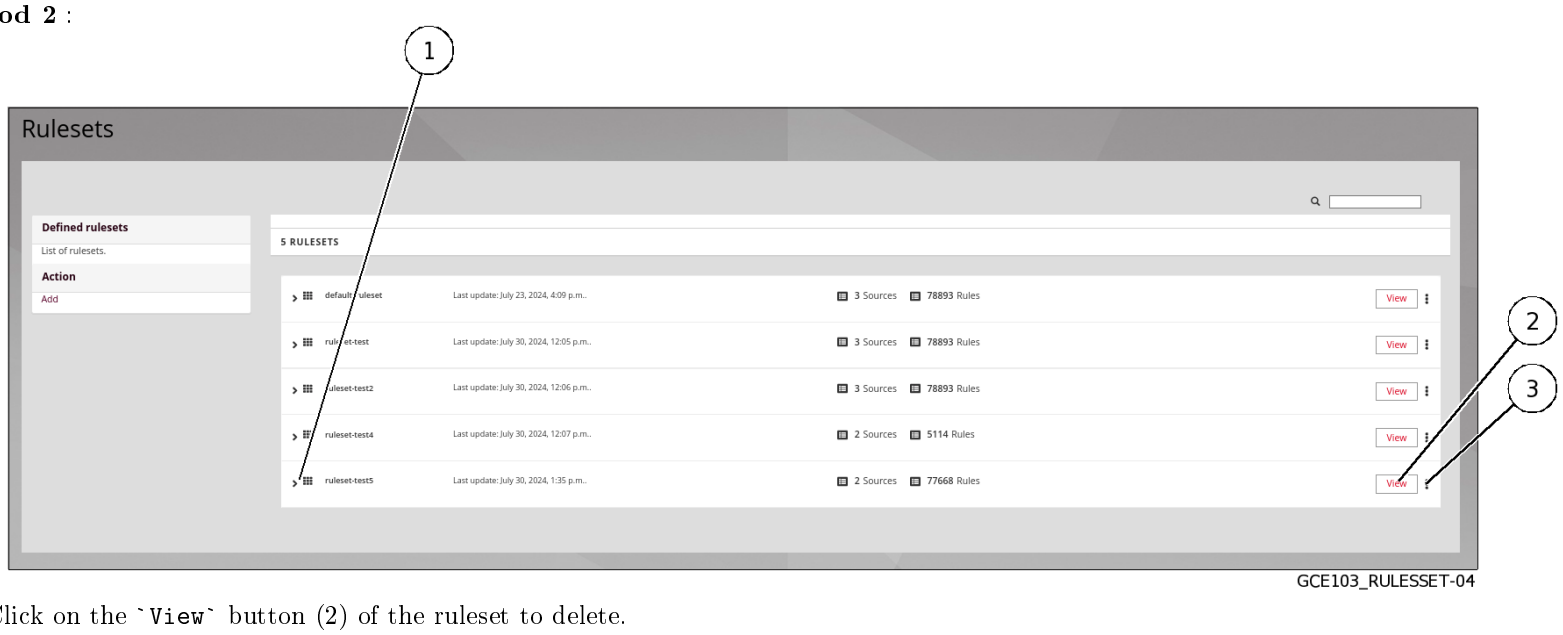
- Click on the three vertical dots (3) of the ruleset to delete.
- Click on the `Delete ruleset` command.
  The `Are you sure you want to delete object xxx?` window is displayed.
- If necessary, add a comment (optional).
- Click on the `Delete object` button
  The deleted ruleset is no longer displayed in the list



GCE103_RULESSET-05

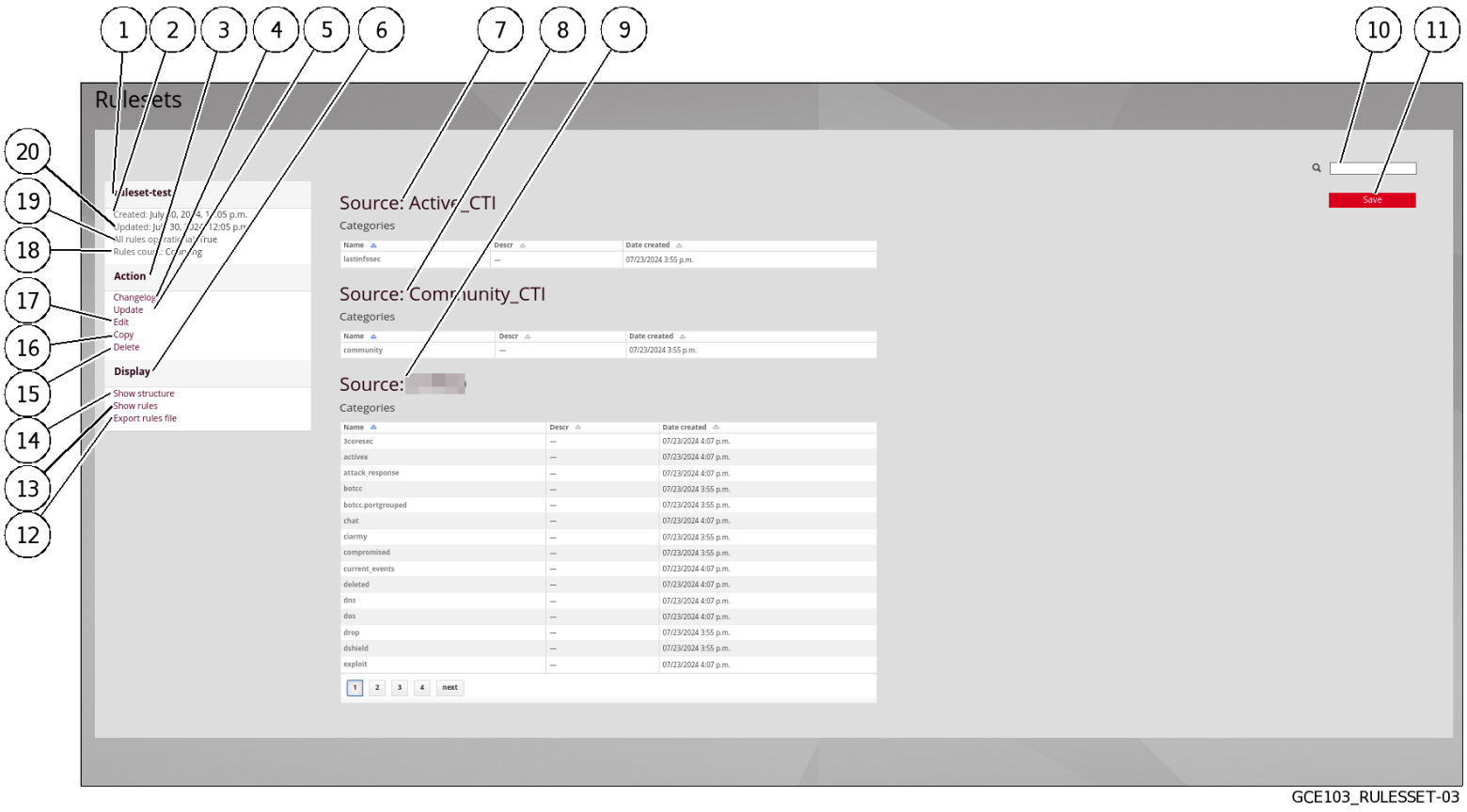
Or

- **Method 2** :



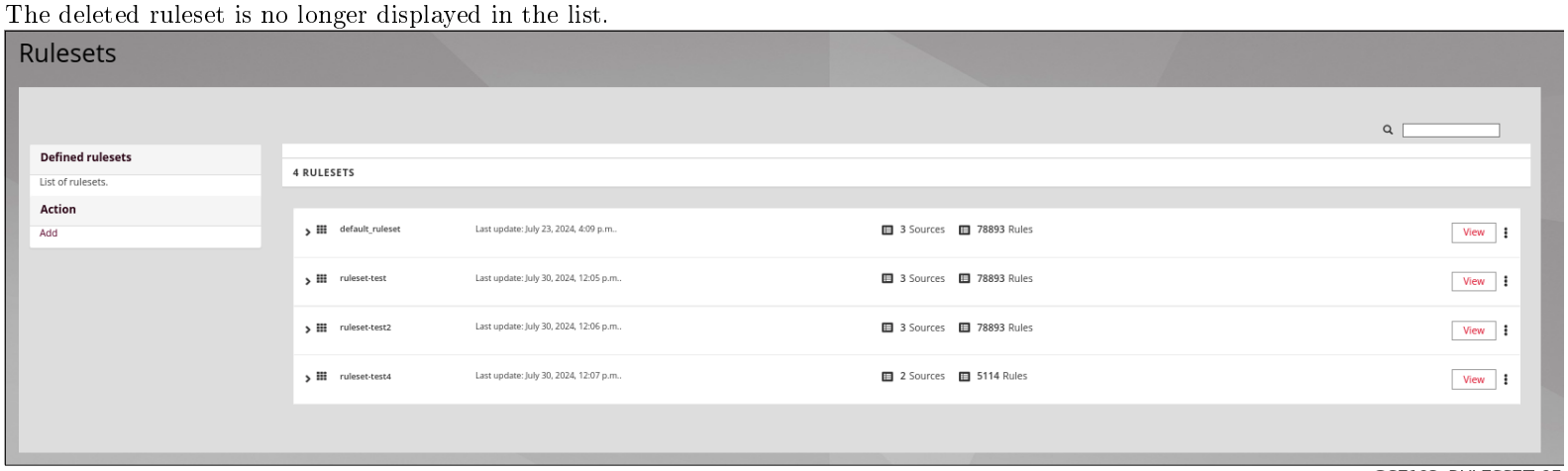
GCE103_RULESSET-04

- Click on the `View` button (2) of the ruleset to delete.



GCE103_RULESSET-03

- Click on the `Delete` link (15) in the list of actions on the left.
  The `Are you sure you want to delete object xxx?` window is displayed.
- If necessary, add a comment (optional).
- Click on the `Delete object` button.
  The deleted ruleset is no longer displayed in the list.



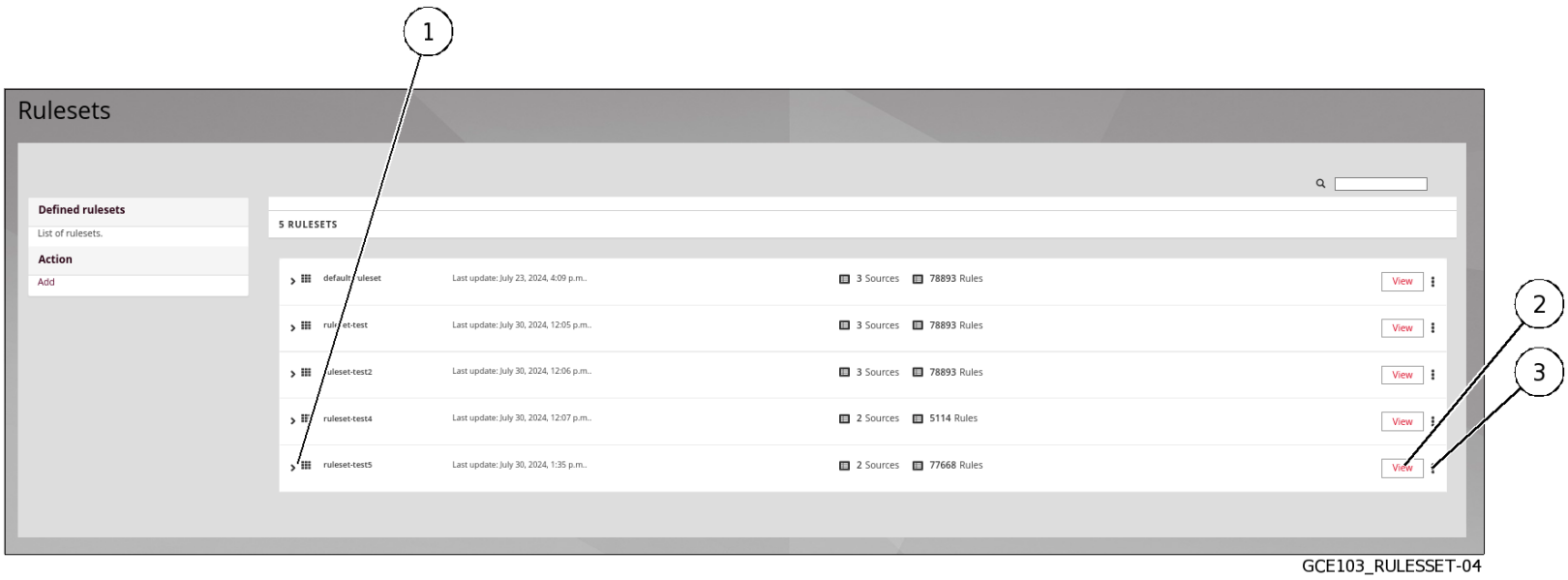
GCE103_RULESSET-05

7.3.2.10 Procedure to edit a ruleset

This procedure describes the ruleset edition.
A ruleset can be edited so that the operator can make changes to the sources, categories or rules present in the ruleset.
These changes can be made to the rules in order to adapt a public rule to specific information system requirements, or to a specific need.

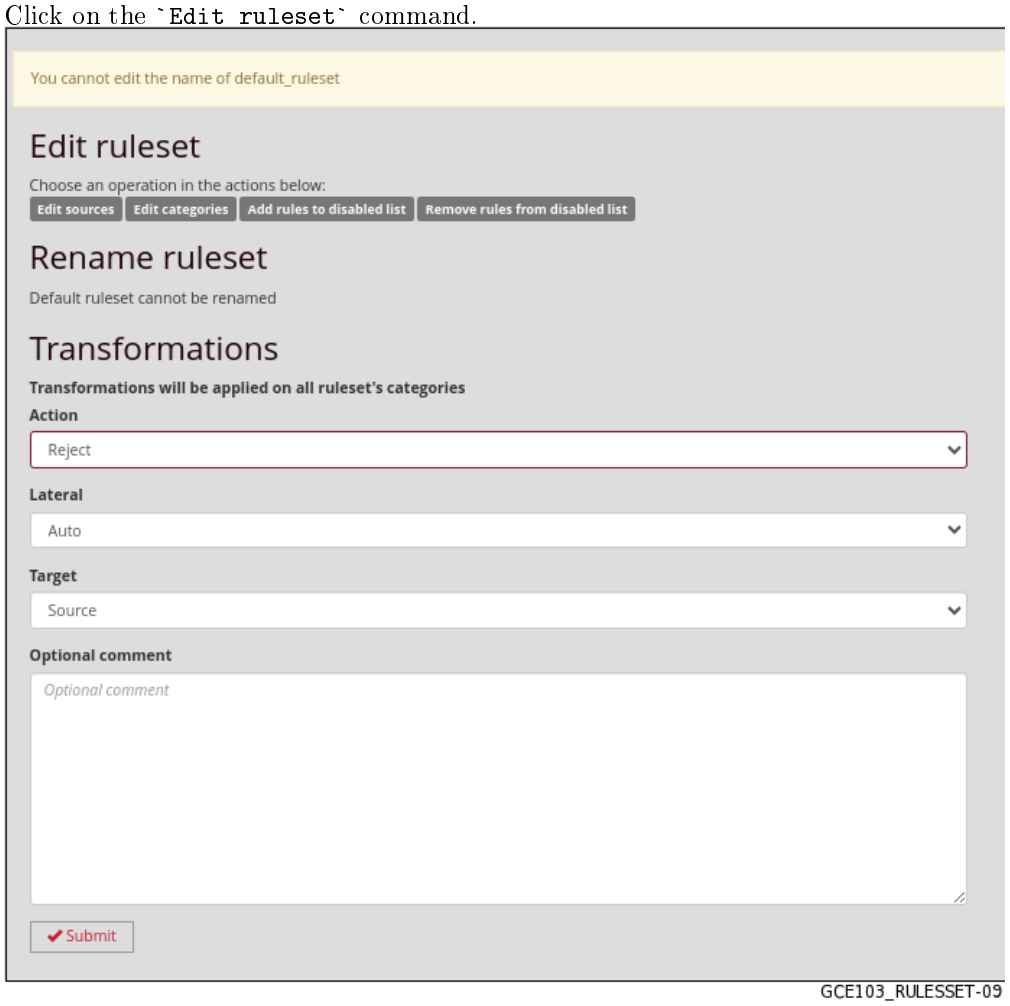
Note:

Using the options of this feature requires a good knowledge of the product: do not hesitate to contact Gatewatcher support to help you.
To contact the Gatewatcher support use the mail tac@gatewatcher.com or https://tac.gatewatcher.com



GCE103_RULESSET-04

- Click on the three vertical dots (3) of the ruleset.
- Click on the `Edit ruleset` command.



GCE103_RULESSET-09

Once in this window, it is possible to:

- From the commands of the `Edit ruleset` part:
- Add or remove sources from the ruleset via the `Edit Sources` link
  This option is used to manually enable or disable an existing source on a ruleset.
  Once unchecked, signatures will no longer be matched by specific streams and will no longer raise alerts on the interface.
- Add or remove categories from a ruleset source via the `Edit categories` link
  This option is used to manually enable or disable an existing category on a ruleset.
  Once unchecked, signatures will no longer be matched by specific streams and will no longer raise alerts on the interface.
- Add rules to the disabled list via the `Add rules to disabled list` link
  It is possible to disable a signature associated with a ruleset. Disabling a rule does not permanently delete it.
- Remove rules from the disabled list via the `Remove rules from disabled list` link
  The rule returns to the active ruleset rules.
- From the `Rename ruleset` part, change the name of the ruleset.
- From the `Transformations` part:
  - Change the `Action`, `Lateral`, and `Target` transformation fields.

Note:

For further information, see the *Transform rule* paragraph:

- Change the comment

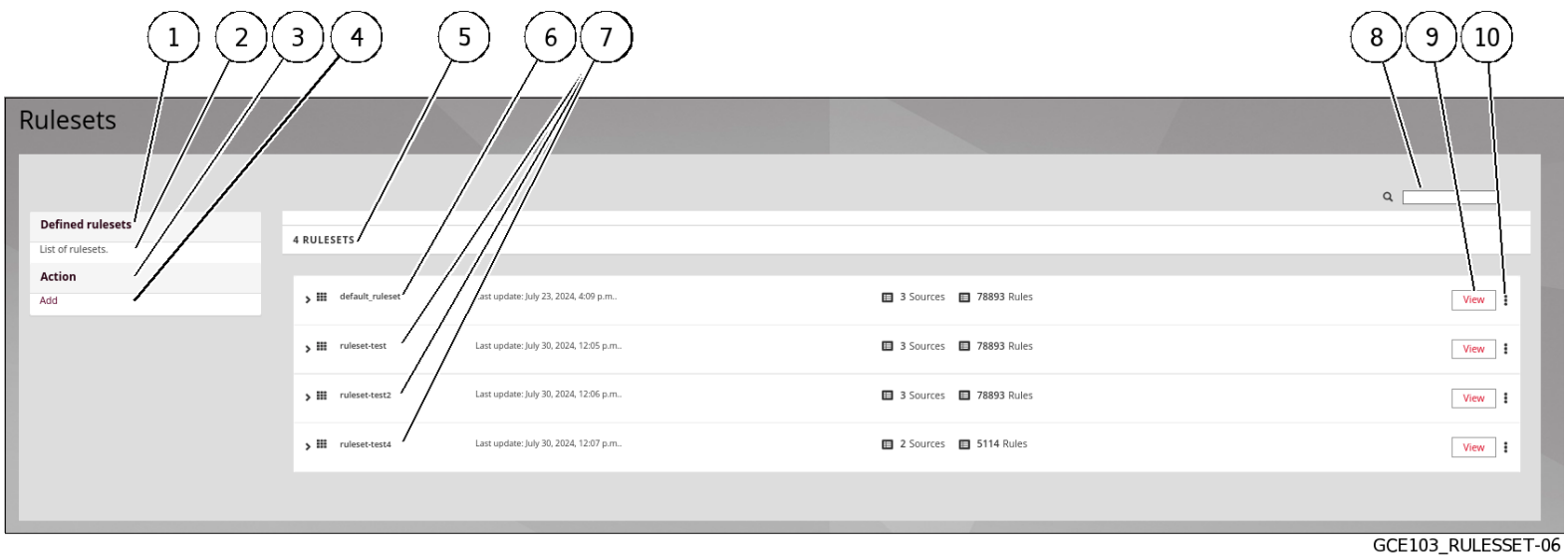
- Click on the `Submit` button to validate the changes.

Note:

When adding a source, it is necessary to manually add the categories of this source so they are present in the source.
If this is not done, the ruleset source will be empty.

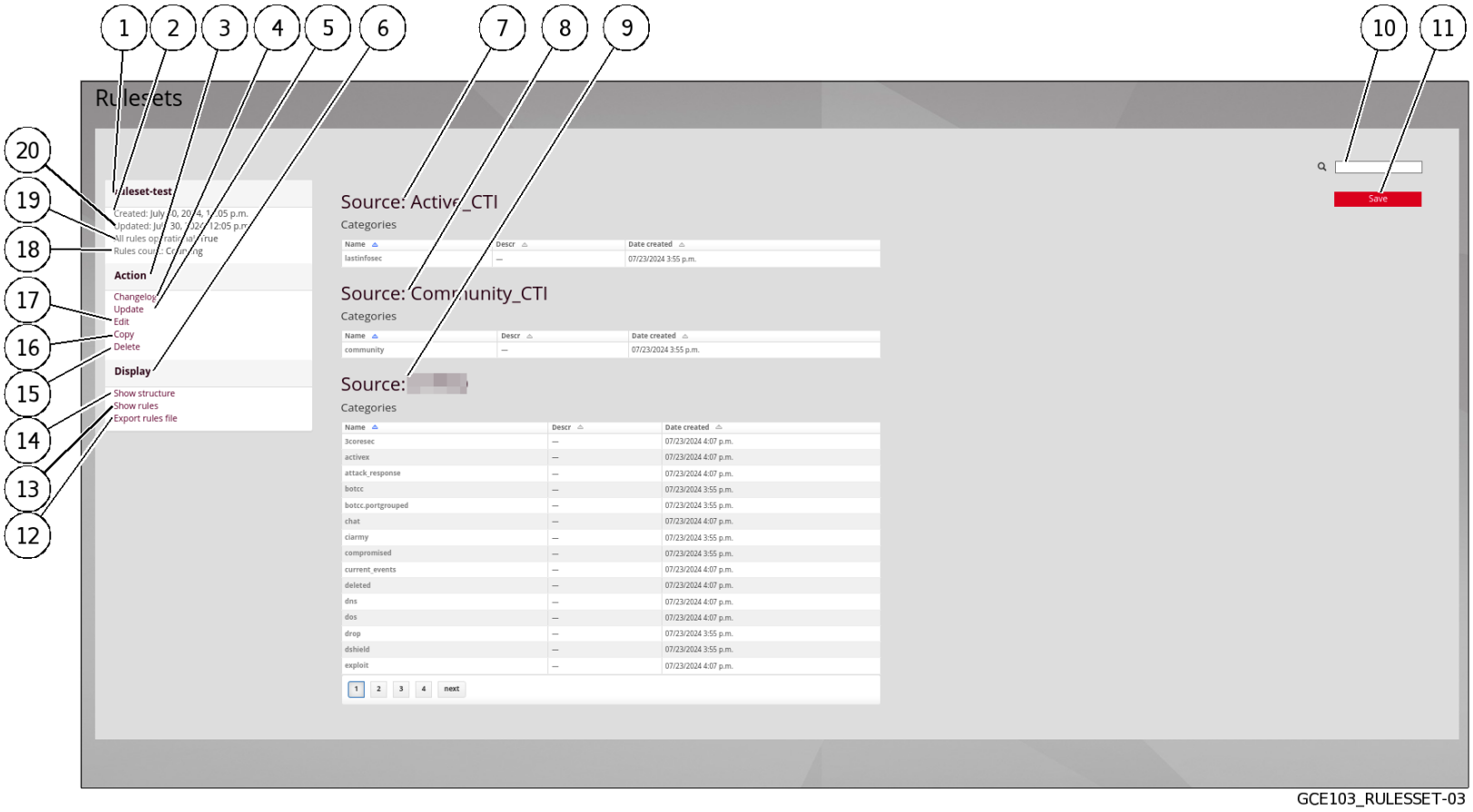
7.3.2.11 Procedure to export a ruleset

Exporting the ruleset enables downloading a ".rules" file containing all the rules of the ruleset in question.
This may enable some rules to be reimported into other tools.



GCE103_RULESSET-06

- Click on the `View` button (9).



GCE103_RULESSET-03

- Click on the `Export rules file` link (12).
  A ruleset named (rulesetname.rules) is downloaded on the local PC.

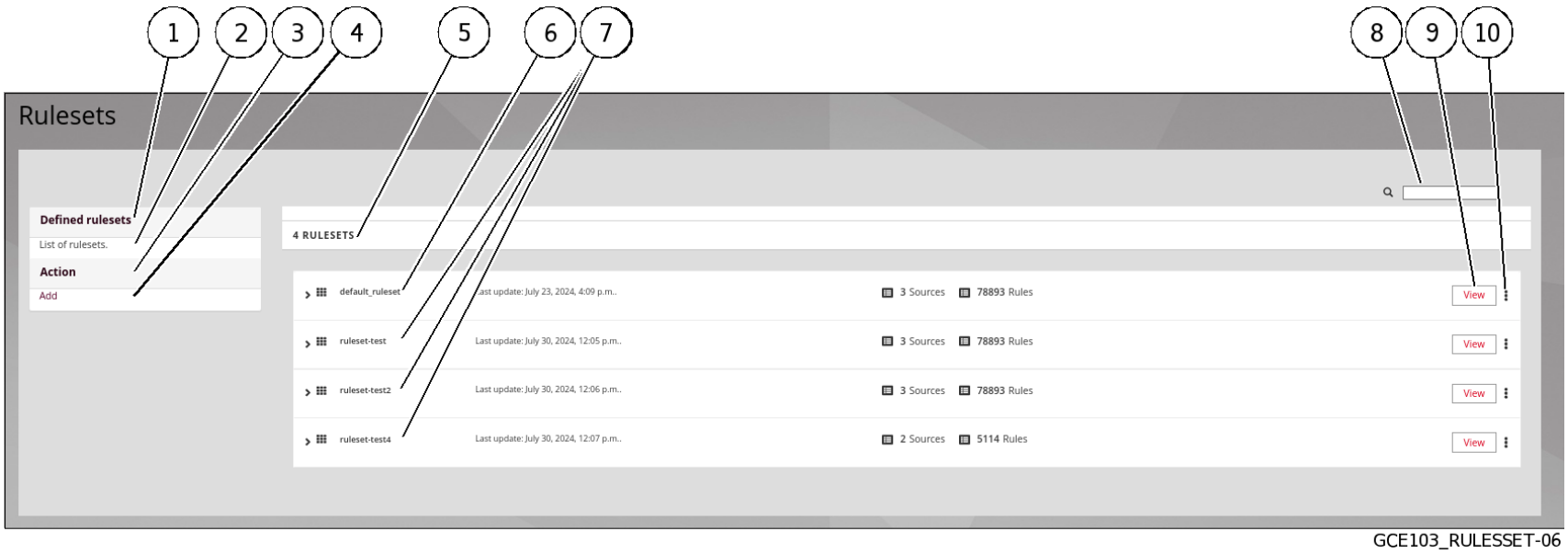
Important:

This feature does not serve as a ruleset backup.
It is not possible to import the exported file back into GCenter as is.
This would result in duplicate rules.

7.3.2.12 Procedure to update a ruleset

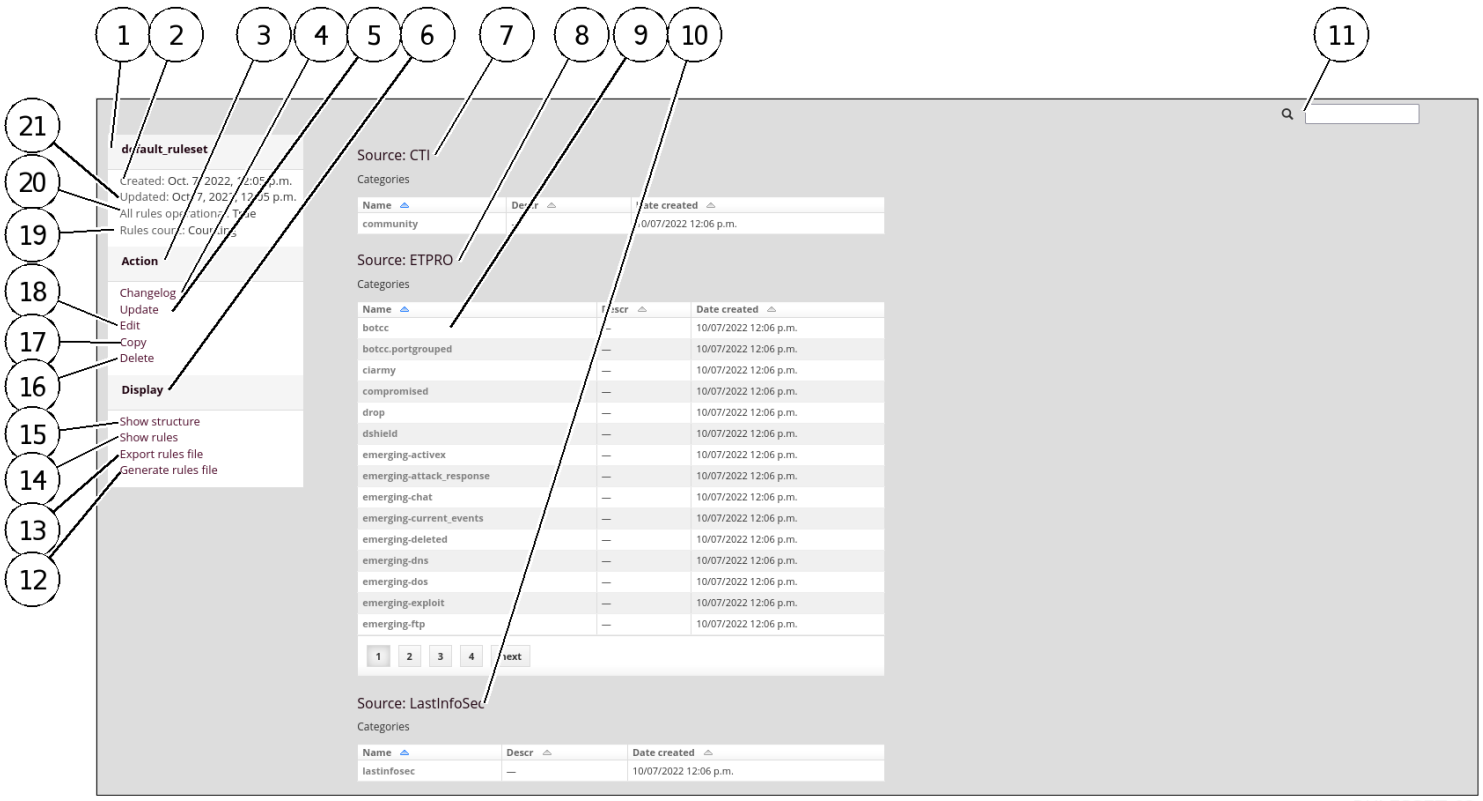
Note:

The update via this procedure only concerns the custom or public sources of the ruleset.
The update is performed if the ruleset file of the remote server or editor has been updated.



GCE103_RULESSET-06

- Click on the `View` button (9) of the desired ruleset.



RULESSET-02

- Click on the `Update` link (5).
  The message `Sigflow is updating ruleset. This window will close when update is over.` is displayed.
- Wait until this message is closed.

Note:

Other Method

- Click on the three vertical dots (9).
- Click on the `Update ruleset` command.

7.3.3 Updating rules sources

7.3.3.1 Introduction

Rulesets are created from rules sources that need to be updated.
To do this, follow the following procedure.

To	Go to
Update all sources defined in a ruleset	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to update all sources defined in a ruleset*
Update all sources defined in the GCenter	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to update all sources defined in the GCenter*

7.3.3.2 Links associated

For more information on Sigflow and its rules, refer to the *Sigflow engine*.
This configuration interface is described in the *`Rulesets` screen*.

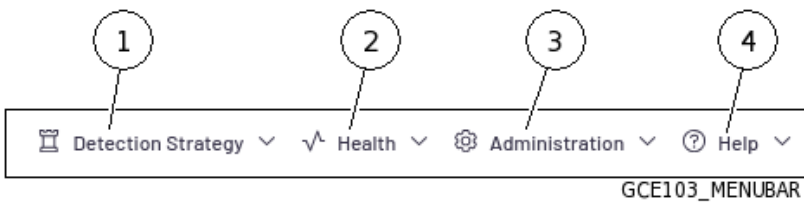
7.3.3.3 Prerequisites

User: member of **Operator** group

7.3.3.4 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

7.3.3.5 Procedure to open the `Rulesets` window



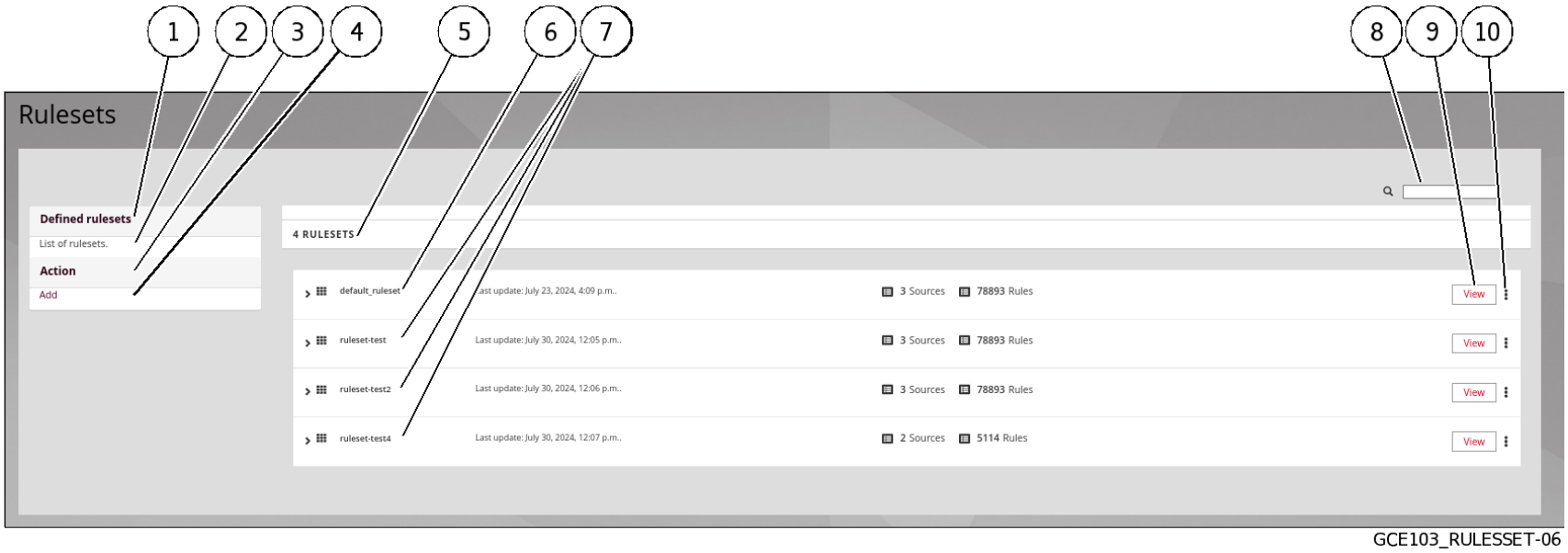
From the navigation bar, click successively on:

- The `Detection Strategy` menu (1)
- The `Rulesets` command of the `Sigflow rules manager` sub menu.
  The `Rulesets` window is displayed.

7.3.3.6 Procedure to update all sources defined in a ruleset

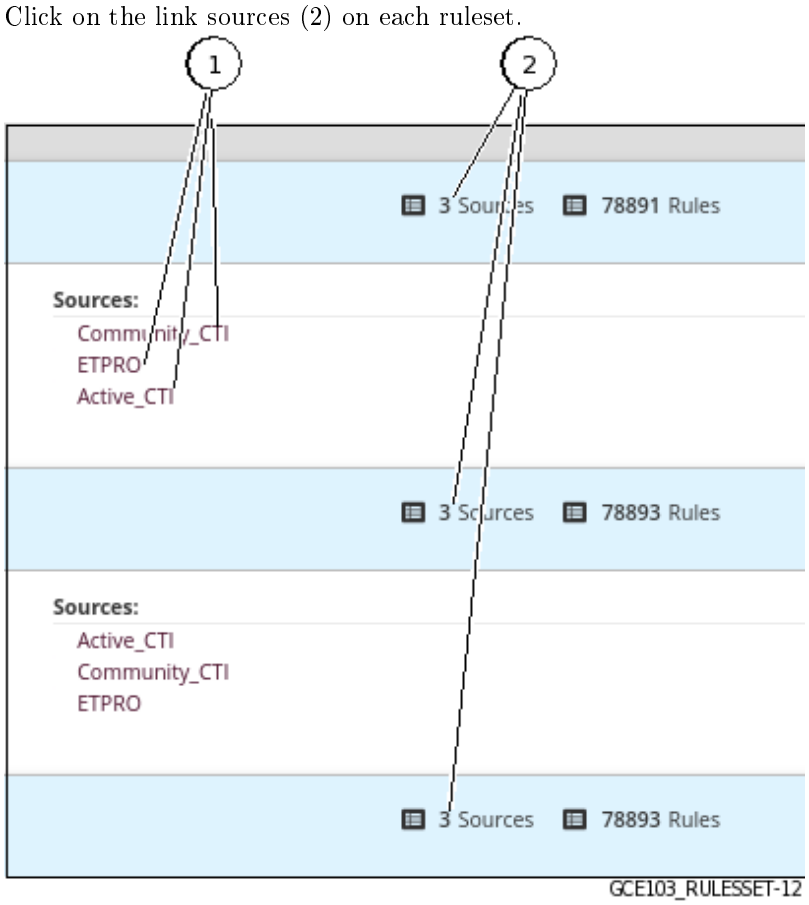
This procedure is described in the *Procedure to update a ruleset*.

7.3.3.7 Procedure to update all sources defined in the GCenter



GCE103_RULESSET-06

- Click on the link sources (2) on each ruleset.



GCE103_RULESSET-12

  The sources (1) of each ruleset are shown.

- For each source (1), apply the *Procedure to update a source*.

7.3.4 Modifying Sigflow engine rules

7.3.4.1 Introduction

Detection rules are what enable the GCap to raise alerts on monitored traffic.
As a reminder:

- Rules are found in categories
- Categories are found in sources
- Sources are placed in rulesets

It is possible to directly influence the operation of a rule, from the **Sigflow** tool, by limiting or deleting alerts for the rule within a ruleset.
The various actions possible for modifying the behavior of a rule are the following:

- The implementation of a transform rule (see the *Transform rule* paragraph) for:

  - The disabling of a transform rule
  - The enabling of a transform rule
- The implementation of a threshold rule (see the *Threshold rule* paragraph)
- The implementation of a suppress rule (see the *Suppress rule* paragraph)

Note:

In order to find a rule to be modified, it is possible to use the search function in the top right-hand corner of all the pages of the Sigflow menu.
It is enough to search for the SID or the name of the desired rule.

7.3.4.1.1 Transform rule

7.3.4.1.1.1 Concept

The transformation rules or "Transform rules" allow to modify the behavior of the rule by modifying its content.
This amendment may be made on a rule-by-rule basis. In this case, the amendment applies only to this rule.
This change can:

- Modify the content of a rule, for example, modify the action of a rule by replacing the **Alert** action defined in the rule with another action of type **drop** or **reject**
  This change is defined in the transformation rule.
- Add a keyword to the rule (**bypass** or **filestore**) defined in the transformation rule
- Change the content of the rule by inheritance.
  By configuring the rule with the default setting (**category default**) of the container (the category), the rule inherits the contents of this parameter.
  This can be done at the category level.
- In this case, the changes are applicable for all rules contained in this category.
  Change handling is the same as at the rule level except the default setting is **ruleset default** set at the ruleset level.
- This can be done at the ruleset level
  In this case, the changes are applicable for all rules contained in all categories of the ruleset.
  Change management is the same as category level except that there is no default setting.

7.3.4.1.1.2 Parameters

The various possible parameters are:

- The `Action` field determines the measure to be applied to the rule
  For example, modifying the action of a rule by replacing the **Alert** action defined in the rule with another action of type **drop** or **reject** or add a keyword to the rule (bypass/filestore):
  - `Filestore`: if a rule matches then the file defined in the flow will be processed by Sigflow and stored like any other package.
    And this even if there is no rule for file generation by filemagic/extension.
  - `Bypass`: if a rule contains a 'bypass', the flow defined by that rule will not be analyzed regardless of its content.
  - `None`: no transformation is carried out.
  - `Category Default`: the rule applies the change defined at the category level and inherits this configuration.
  - `Ruleset`: the category applies the change defined at the ruleset level and inherits this configuration.
  - For choices `Reject` and `Drop`: as a reminder, the GCap is in IDS mode and not IPS i.e:
  - in IPS (Prevention) mode, the network flow passes through the detection system which can let it pass but also reject it (action `Reject`) or delete it (action `Drop`)
  - in IDS (Detection) mode, the network flow is copied by the TAP to the GCap so none of the actions `Reject` or `Drop` make sense since the GCap does not have any action on the main flow.

Note:

The default action in the solution is **alert**. As GCap is an IDS, not an IPS, normally there is no need to change this value.

- The `Lateral` field enables the scope of the rule to be changed at the network variable level
  If a rule has a source $HOME_NET and a destination $EXTERNAL_NET and both sides of the traffic being analyzed are in $HOME_NET, then the rule will not raise an alert and lateral movements will no longer be detected.
  Thus, the transformation enables the value of the variable to be changed from "$EXTERNAL_NET" to "any" in order to broaden the scope to detect lateral movements.
  Here are the possible values:
- `Auto`: substitution is made if the signature checks certain properties

- `None`: the replacement is not performed
- `Yes`: $EXTERNAL_NET is replaced by any other IP (any)
- `Category Default`: the rule applies the change defined at the category level and inherits this configuration
- `Ruleset Default`: the category applies the change defined at the ruleset level and inherits this configuration

- The field `Target` adds the field "target:[src_ip dest_ip]" in the rule
  It generates additional metadata indicating who is the target of the attack.
  Possible values are:

- `Auto`: an algorithm is used to determine the target if one is present
- `Destination`: the target is the receiving IP
- `None`: the replacement is not performed
- `Ruleset Default`: the category applies the change defined at the ruleset level and inherits this configuration
- `Source`: the target is the originating IP

7.3.4.1.2 Threshold rule

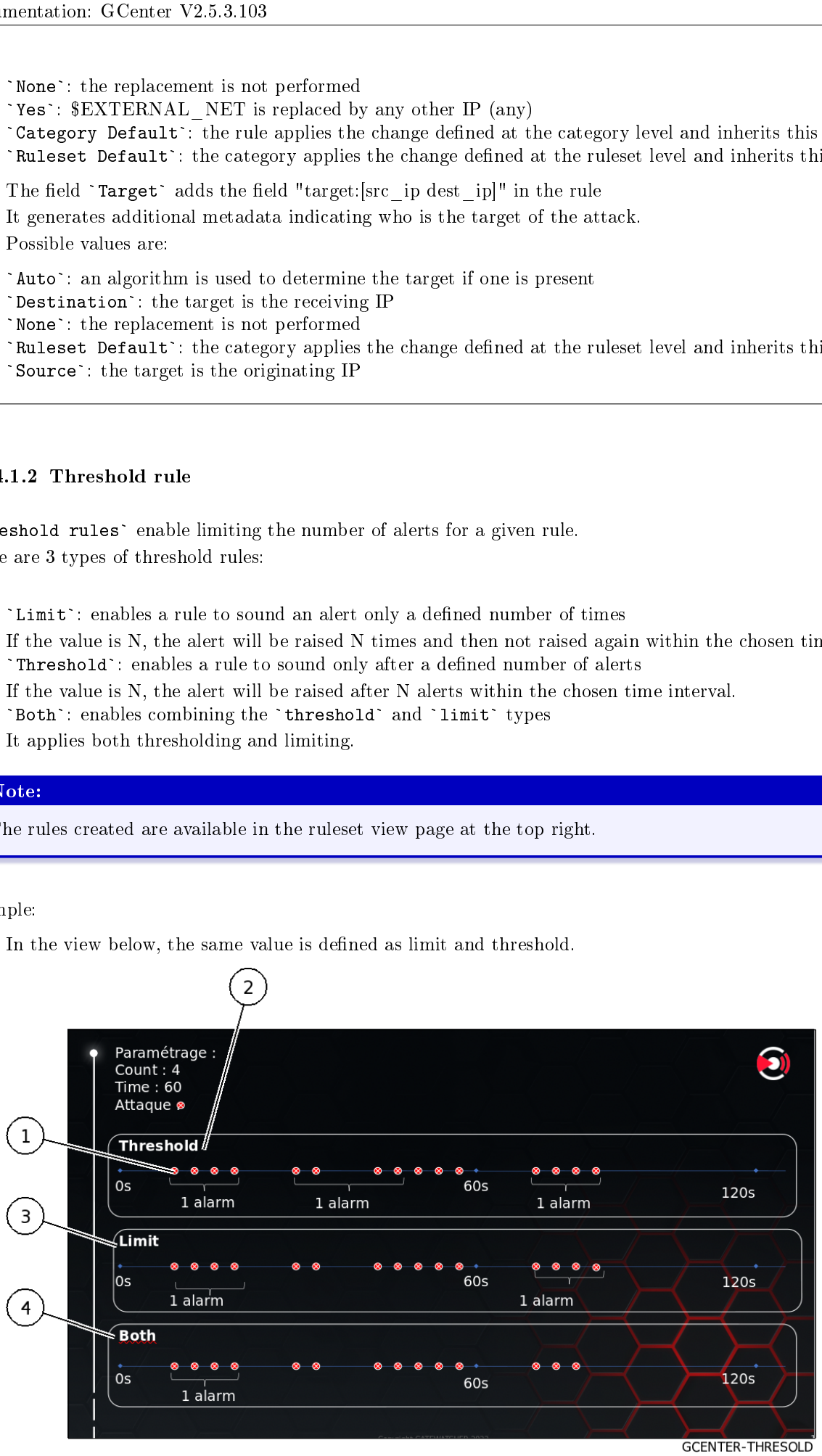
`Threshold rules` enable limiting the number of alerts for a given rule.
There are 3 types of threshold rules:

- `Limit`: enables a rule to sound an alert only a defined number of times
  If the value is N, the alert will be raised N times and then not raised again within the chosen time interval.
- `Threshold`: enables a rule to sound only after a defined number of alerts
  If the value is N, the alert will be raised after N alerts within the chosen time interval.
- `Both`: enables combining the `threshold` and `limit` types
  It applies both thresholding and limiting.

Note:

The rules created are available in the ruleset view page at the top right.

Example:
In the view below, the same value is defined as limit and threshold.



In the `Threshold` zone (2), the threshold counter is set to four. So for the period considered (here 60 seconds), an alarm (1) is activated every 4 attacks.
In the `Limit` zone (3), the limit counter is set to four. So for the period considered (here 60 seconds), an alarm is activated only for the first 4 attacks.
In the `Both` field (4), the counter is set to four. So for the period considered (here 60 seconds), an alarm is activated only for the first 4 attacks (limit value reached).

7.3.4.1.3 Suppress rule

Suppress rules allow disabling alerts for a rule on a specific network or IP.
Multiple networks or IPs can be added separated by ' ,'.

Example:

A rule raises 10 alerts every hour from the same IP source.
It turns out that this is a false positive and that these alerts are irrelevant.
In this case, it is appropriate to disable the rule for the IP source in question.
The rule remains active on the rest of the network.

Note:

The rules created are available in the ruleset view page at the top right.

To	Go to
Transform a rule	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to setup a transformation rule*
Disable a rule	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to disable a rule*
Enable a rule	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to enable a rule*
Setup a threshold rule	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to setup a threshold rule*
Setup a suppress rule	1 - *Procedure to open the `Rulesets` window* 2 - *Procedure to setup a suppress rule*

7.3.4.2 Links associated

This configuration interface is described in *`Rulesets` screen*.

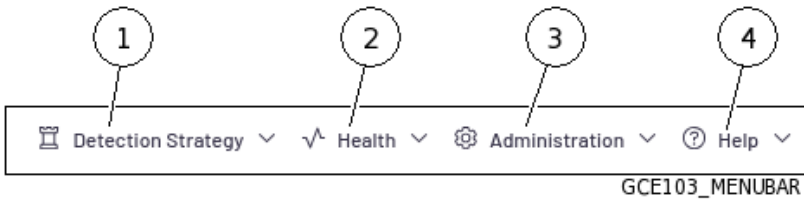
7.3.4.3 Prerequisites

User: member of **Operator** group

7.3.4.4 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

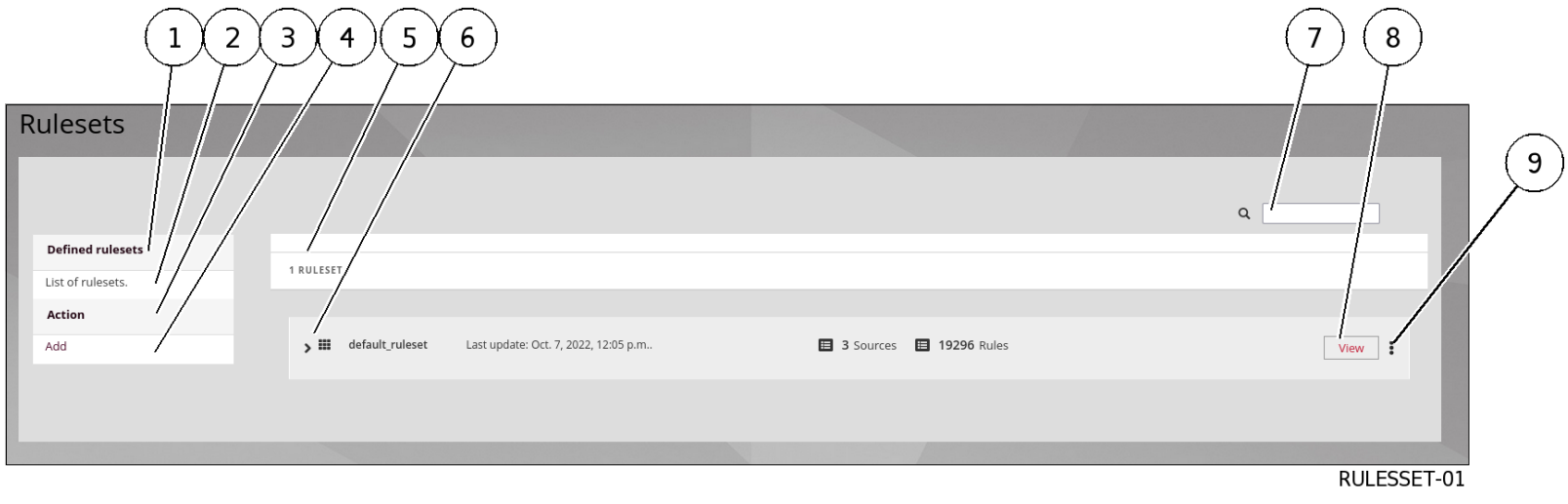
7.3.4.5 Procedure to open the `Rulesets` window



From the navigation bar, click successively on:

- The `Detection Strategy` menu (1)
- The `Rulesets` command of the `Sigflow rules manager` sub menu.
  The `Rulesets` window is displayed.

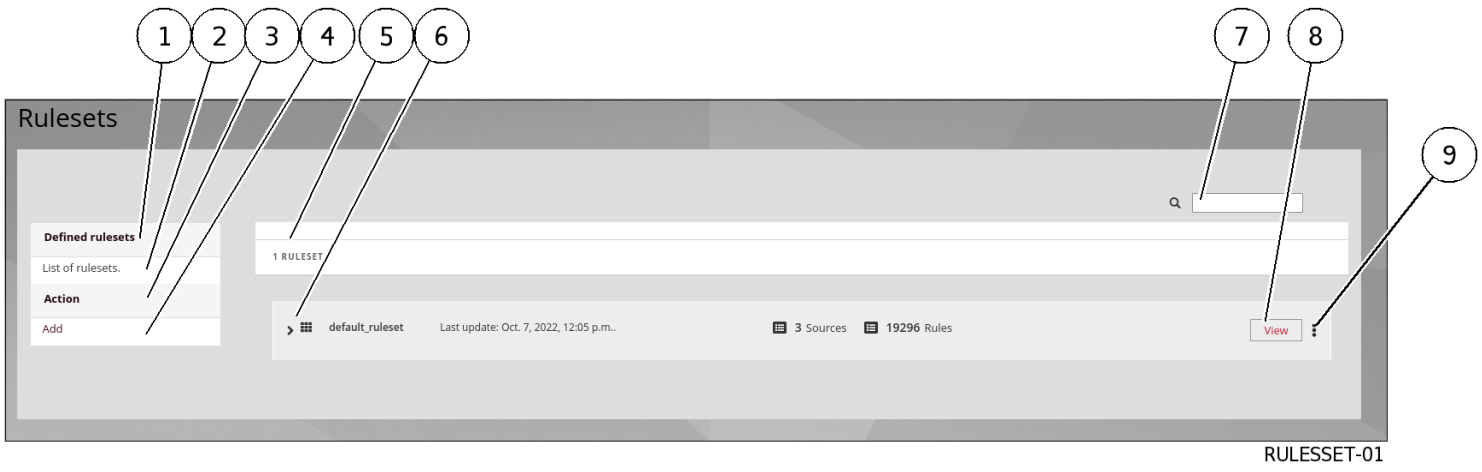
7.3.4.6 Procedure to setup a transformation rule



From the ruleset management interface:

- Look for the SID of the rule to be modified in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Edit rule` link to display the edit menus
- Make sure to be in the `Transform rule` menu
- Tick the rule(s) in which the rule transformation is to be applied
- Change the `Action`, `Lateral`, and `Target` fields as required
- If necessary, add a comment (optional)
- Click on the `Valid` button.

7.3.4.7 Procedure to disable a rule



From the ruleset management interface:

- **method 1** :

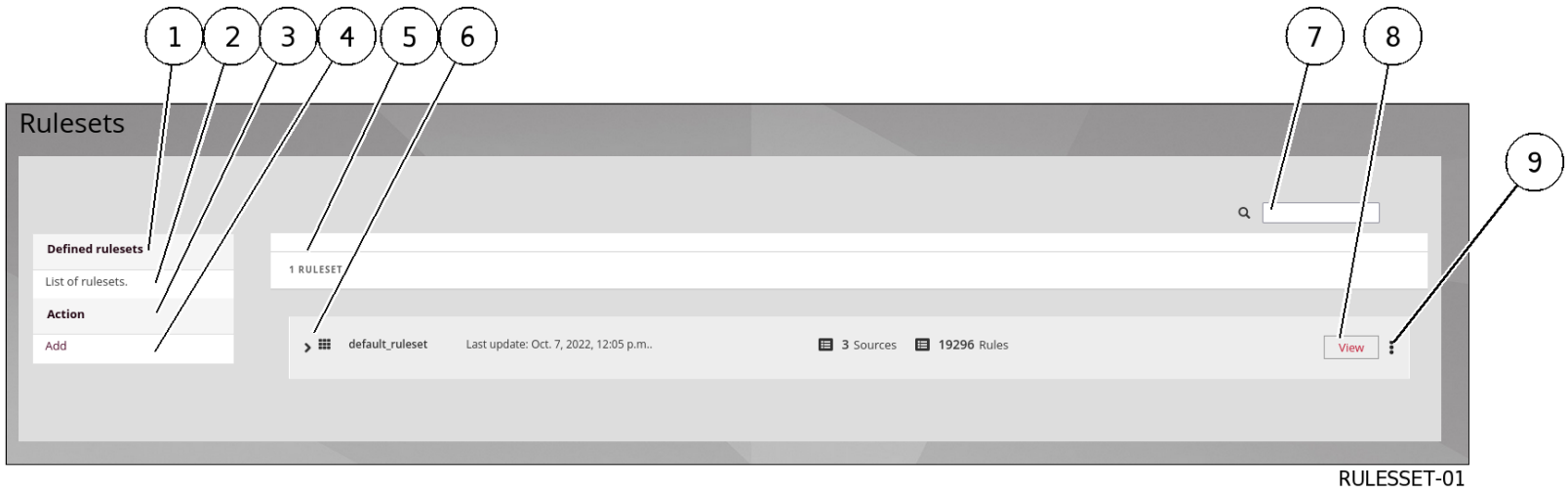
- Look for the SID of the rule to be disabled in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Disable rule` link
- Tick the rule(s) in which the rule should be disabled
- If necessary, add a comment (optional)
- Click on the `Disable` button

Or

- **method 2** :

- Look for the SID of the rule to be disabled in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Edit rule` link to display the edit menus
- Click on the `Disable rule` link
- Tick the ruleset(s) in which the rule should be disabled
- If necessary, add a comment (optional)
- Click on the `Disable` button

7.3.4.8 Procedure to enable a rule



From the ruleset management interface:

- **method 1** :

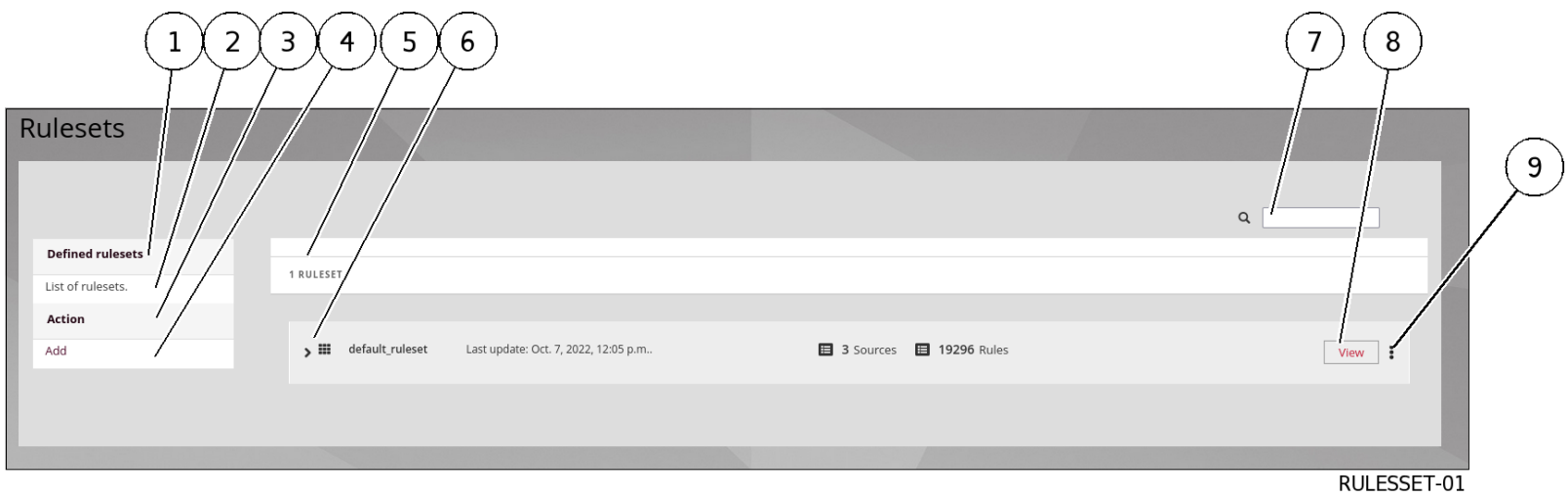
- Look for the SID of the rule to be enabled in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Enable rule` link
- Tick the ruleset(s) in which the rule should be enabled
- If necessary, add a comment (optional)
- Click on the `Enable` button

Or

- **method 2** :

- Look for the SID of the rule to be enabled in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Edit rule` link to display the edit menus
- Click on the `Enable rule` link
- Tick the ruleset(s) in which the rule should be enabled
- If necessary, add a comment (optional)
- Click on the `Enable` button

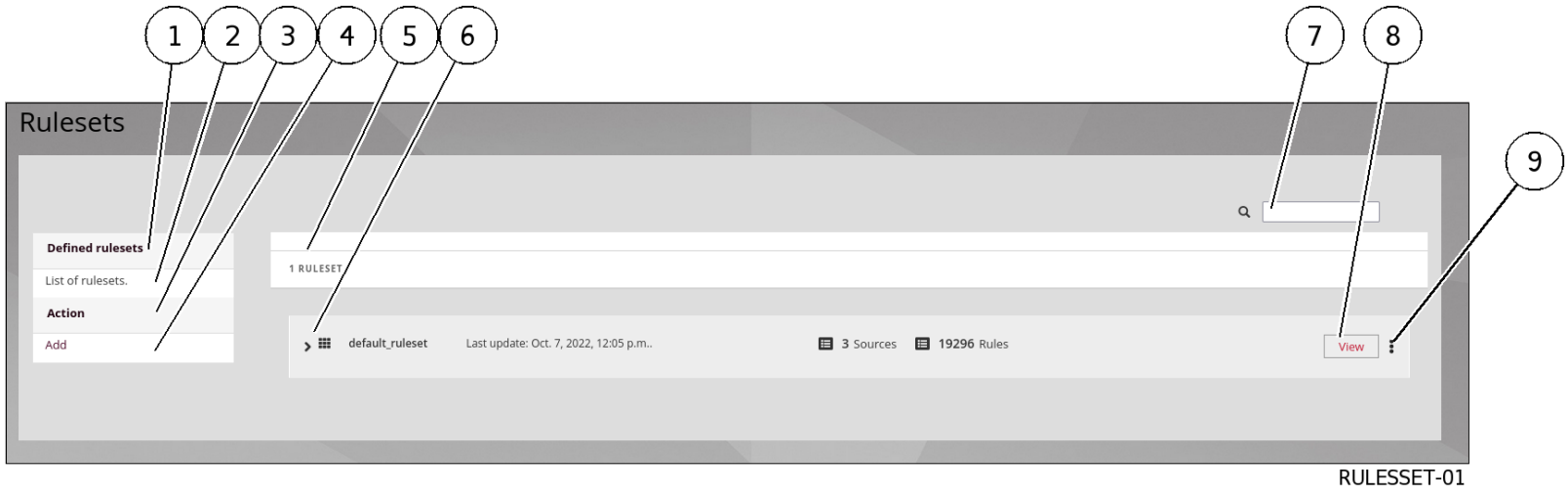
7.3.4.9 Procedure to setup a threshold rule



From the ruleset management interface:

- Look for the SID of the rule to be modified in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Edit rule` link to display the edit menus
- Click on the `Threshold rule` link
- Select the type of threshold desired `threshold`, `limit`, or `both`
- Select whether the threshold should apply to the source or the destination
- Enter the desired threshold value. The impact will be different depending on the type of threshold chosen
- Enter the value of the desired time interval in which the threshold will apply
- Tick the ruleset(s) in which the rule threshold is to be applied
- If necessary, add a comment (optional)
- Click on the `Valid` button

7.3.4.10 Procedure to setup a suppress rule



RULESSET-01

From the ruleset management interface:

- Look for the SID of the rule to be modified in the top right-hand bar (7)
- Click on the SID of the rule among the search results
- Click on the `Edit rule` link to display the edit menus
- Click on the `Suppress rule` link
- Select the type of threshold desired `threshold`, `limit`, or `both`
- Select whether the threshold should apply to the source or the destination
- Enter the IP address or network on which the rule will be disabled
- Tick the ruleset(s) in which the deletion rule is to be applied
- If necessary, add a comment (optional)
- Click on the `Valid` button

7.3.5 Creation of automatic alarm limits

7.3.5.1 Introduction

- The number of alerts for one or more GCaps can be controlled by limitation
- The GCenter counts alerts during an observation period and compares them to a programmable trigger point
- The GCenter determines the rules that generated this threshold exceeding and based on the selected criterion (filter type), GCenter automatically creates alarm limits
- These limits grouped by the GCap are communicated to the Sigflow engine present in each GCap to implement these limitations

There are several types of filtration:

- `by_src`: the limitation is applied to alerts with the same source IP address
- `by_dst`: the limitation is applied to alerts with the same destination IP address
- `by_rule`: the limitation is applied to all alerts triggered by the rule
- `by_both`: the limitation is applied to alerts with the same IP pair source address + destination

---

7.3.5.2 Links associated

For more information, refer to the description given in *`Auto-threshold` screen*.

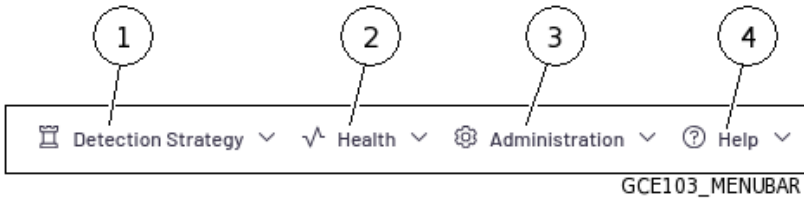
7.3.5.3 Prérequis

User: member of **Operator** group

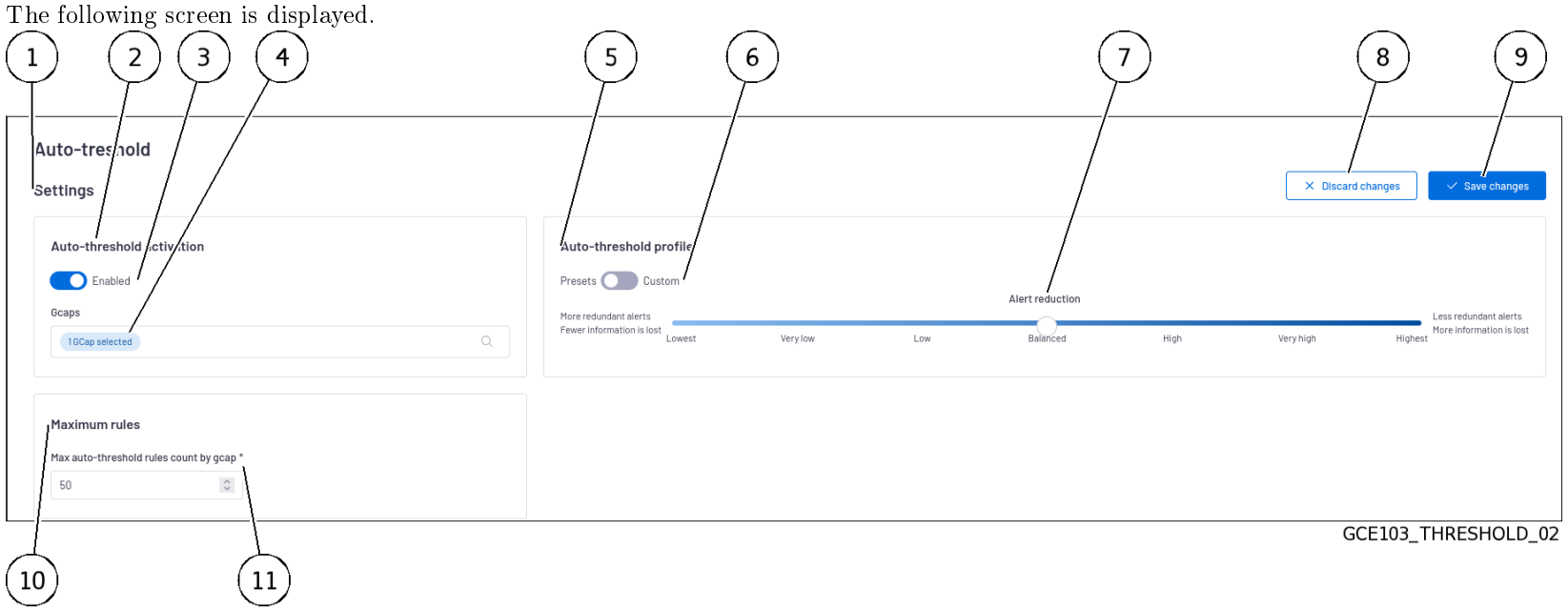
7.3.5.4 Opérations préliminaires

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

7.3.5.5 Procedure to access to the `Auto-threshold` window

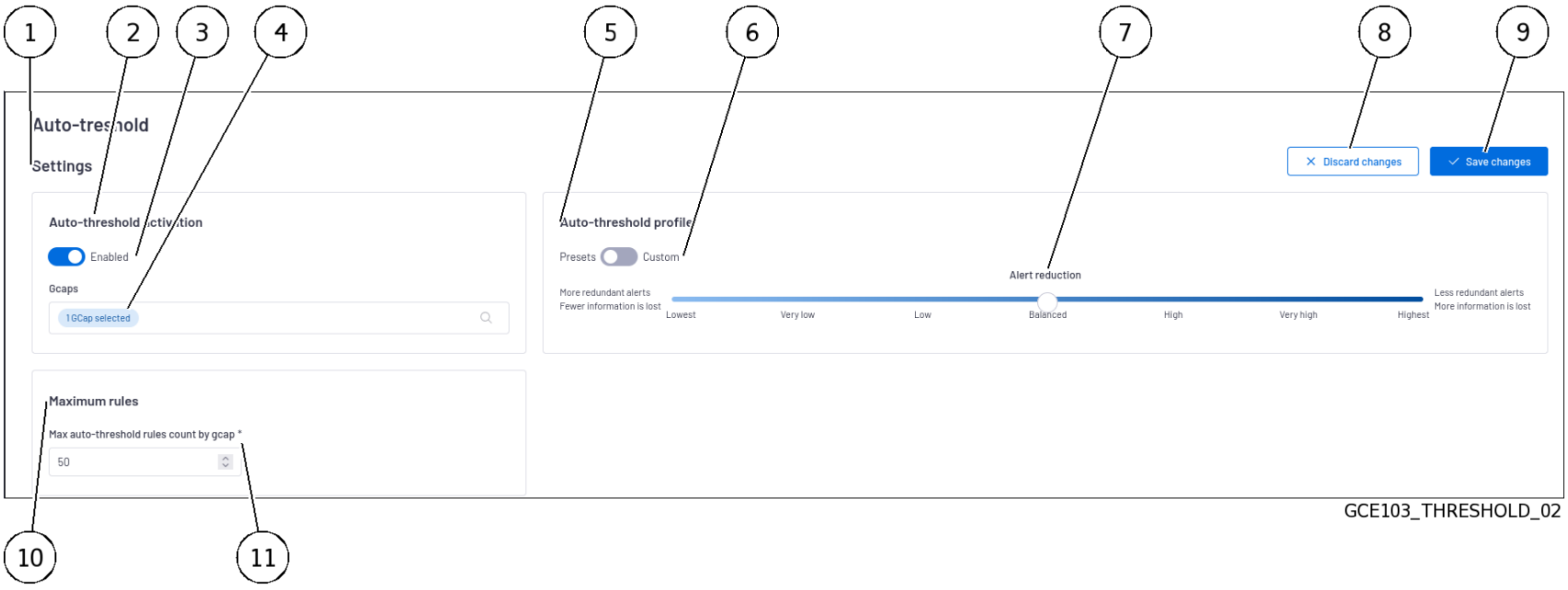


- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `Auto-threshold profile` command from the `Sigflow rules manage` submenu.
  The following screen is displayed.



- Continue with:
  - the *Procedure to create automatically thresholds using the presets profile*
  - the *Procedure to create automatically thresholds using the custom profile*

7.3.5.6 Procedure to create automatically thresholds using the presets profile



GCE103_THRESHOLD_02

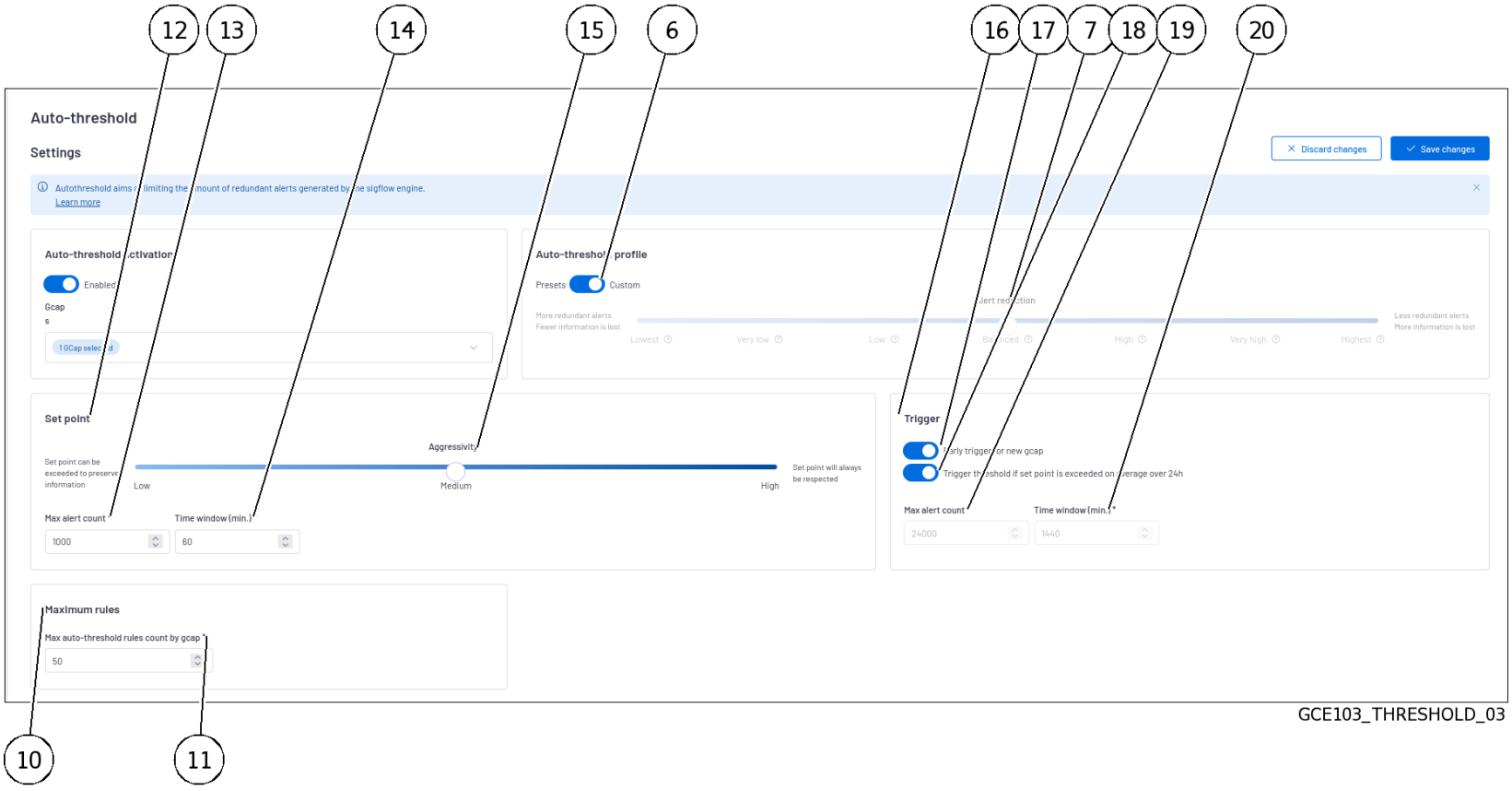
- Active the `Auto-threshold activation` feature (2) by clicking on the `Enabled` selector (3).
- Select the GCap concerned by the creation of automatic thresholds using the field (4).
- In the `Auto-threshold profile` area, put the `Presets / Custom` selector on the `Presets` position.
  This function enables to use pre-existing and editable profiles using the cursor (7).
- Select one profil with the `Alert reduction` cursor.

Profile	Trigger	Central value	Aggressiveness (selection criterion)
`Lowest`	96k alerts per 24 hours	4k alerts per hour	1
`Very low`	48k alerts per 24 hours	2k alerts per hour	1
`Low`	24k alerts per 24 hours	1k alerts per hour	1
`Balanced (default)`	24k alerts per 24 hours	1k alerts per hour	2
`High`	12k alerts per 24 hours	500 alerts per hour	2
`Very high`	12k alerts per 24 hours	500 alerts per hour	3
`Highest`	1200 alerts per 24 hours	50 alerts per hour	3

- Configure the Maximum number of limits per GCcap (11).
  The system can continuously create new limits and keep the ones that trigger the most.

7.3.5.7 Procedure to create automatically thresholds using the custom profile

- Active the `Auto-threshold activation` feature (2) by clicking on the `Enabled` selector (3).
- Select the GCap concerned by the creation of automatic thresholds using the filed (4).
- In the `Auto-threshold profile` area, put the `Presets / Custom` selector on the `Custom` position.
  This function enables to configure threshold parameters.
  To do so, the `Set point` and `Trigger point` sections are displayed.



GCE103_THRESHOLD_03

- Select one profil with the `Alert reduction` cursor (7).

Profile	Trigger	Central value	Aggressiveness (selection criterion)
`Lowest`	96k alerts per 24 hours	4k alerts per hour	1
`Very low`	48k alerts per 24 hours	2k alerts per hour	1
`Low`	24k alerts per 24 hours	1k alerts per hour	1
`Balanced (default)`	24k alerts per 24 hours	1k alerts per hour	2
`High`	12k alerts per 24 hours	500 alerts per hour	2
`Very high`	12k alerts per 24 hours	500 alerts per hour	3
`Highest`	1200 alerts per 24 hours	50 alerts per hour	3

- Configure the limit pivot value definition with the cursor (15) in the `Set point` area (12):
  - Configure the `Aggressivity` level to select the alarm type criterion to limit.

    The settings are:
    - *Low Setting*
    - *Medium Setting*
    - *High Setting*

    The default level is: low
  - Enter the maximum number of alerts sent in the `Max alert count` field (13).
  - Enter the time window during the maximum number of alerts reported applies in the `Time window (min)` field (14).
- Configure the `Trigger` (16) to begin the analyze period.

  The following parameters define the trigger parameters:
  - Use the `Trigger threshold if set point is exceeded on average over 24h` selector (18)
    - If the selector `Trigger threshold if set point is exceeded on average over 24h` is activated, the GCenter counts alerts by rule and when a rule exceeds the pivot value set in the `Max alert count` (19) parameter reduced to 24 hours measured over 24 hours.

      This option is enabled by default.

      For example: for a value of 1000 in the `Max alert count` parameter (19) and a value of 60 in the `Time window` parameter (20) then the system triggers the automatic creation from the appearance of 24000 alerts during the last 24 hours.
    - If the selector is disabled, the system triggers from the value set in the `Max alert count` parameter (19) that appeared during the `Time window` (20) parameter value.
  - Use the `Early trigger for new GCap` selector (17) if needed
  - Enter the maximum number of automatic thresholds applied on a GCap (11) in the `Maximum rules` area (10).
- Click on the `Save changes` button.

7.4 Configuring GCaps using the `GCaps Profiles`

This section describes the GCap configurations from the GCenter.

7.4.1 Customizing the setting of the GCap profile

7.4.1.1 Introduction

When the GCap was paired, a predefined profile has been selected and sent to it.
The default profiles are :

- Essential
- Balanced
- Deep
- Paranoid
- Performance

The parameters given by the profil selected can be modified by using the following procedure.

7.4.1.2 Links associated

The setting values are described in the *GCAP Profiles*.
The details of the customisation options are provided in the *`GCaps profiles` screen*.

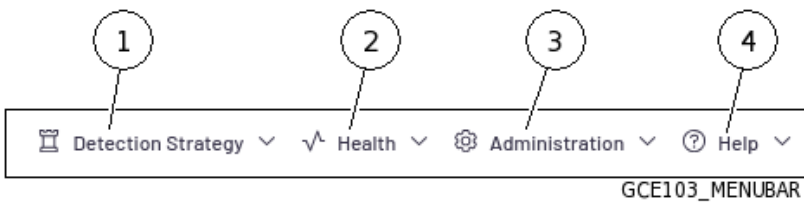
7.4.1.3 Prerequisites

- User: member of **Administrator** group

7.4.1.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)
- Know the **Fully Qualified Domain Name FQDN** (FQDN) of the GCap and its IP address (for example: 'gcapname.domaine.com')

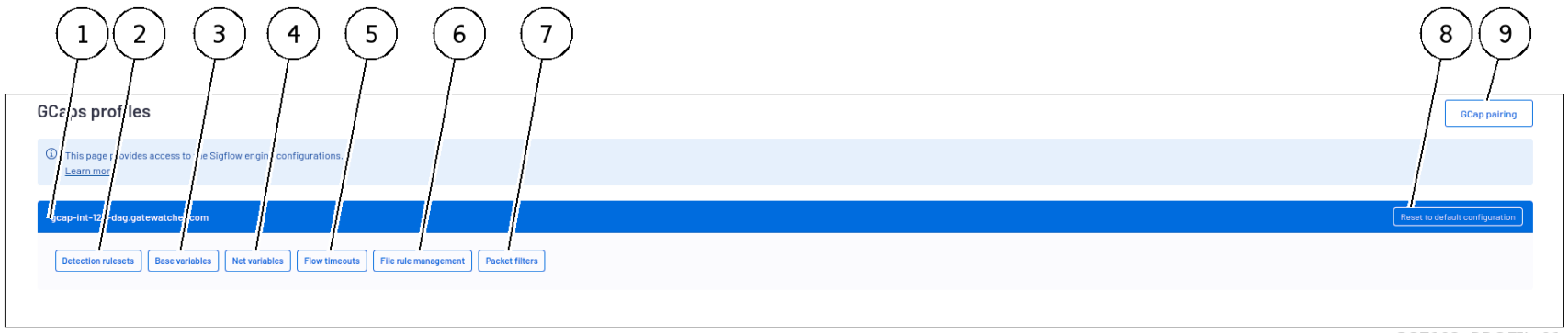
7.4.1.5 Procedure to open the `GCaps profiles` window



- From the navigation bar, click successively on:
- The `Detection strategy` button (1)
- The `GCaps profiles` button of the `Sigflow engine` category
  The `GCaps profiles` window is displayed.

7.4.1.6 Procedure to customise the default profile

- Select the GCap (1) for which profile parameters should be modified



GCE103_PROFIL-01

- To each category (item 2 to 7), see the corresponding procedure given in the following table.

Item	Function	For further details, see the description...	and the procedure
1	FQDN GCap name paired with GCenter		
2	`Detection Rulesets` button Manages the rulesets to the paired GCaps	*`Detection Rulesets` section of the `GCaps profiles` screen*	*Configuring the detection rulesets via the GCap profile*
3	`Base variables` button Manages configuration of advanced GCap settings	*`Base variables` Section of the `GCaps profiles` screen*	*Configuring the Base variables parameters via the GCap profile*
4	`Net variables` button Manages network variables used in Sigflow rules	*`Net variables` section of the `Config Gcaps profiles` menu*	*Configuring the network variables parameters via the GCap profile*
5	`Flow timeouts` button Configures how long Sigflow keeps a stream in memory based on its state	*`Flow timeouts` section of the `GCaps profiles` screen*	*Configuring the flow timeouts via the GCap profile*
6	`File rule management` button Configures the file types that the GCap will extract for a given protocol	*`File rules` section of the `GCaps profiles` screen*	*Configuring the file reconstruction rules via the GCap profile*
7	`Packet filters` button Adjusts the GCap capture settings with advanced Sigflow features	*`Packet filters` section of the `Gcaps profiles` screen*	*Configuring filters on targeted parts of the analyzed traffic via the GCap profile*
8	`Reset to default configuration` button Resets the configuration and loads the selected predefined profile in `GCaps pairing and status`		
9	`GCap pairing` button Displays the screen to manage the pairing of a GCap	Reserved to the administrator	

- Use the `APPLY` button to trigger the transmission of the global configuration to the selected GCap.

Note:

The `Reset to default configuration` button (8) resets the configuration and loads the profile selected in the `GCaps pairing and status` screen.

7.4.2 Configuring the detection rulesets via the GCap profile

7.4.2.1 Introduction

The `Detection Rulesets` section defines the management of the network interfaces and the ruleset(s) used to inspect the captured traffic on the GCap paired with the GCenter.

Note:

It is necessary to generate rules for a ruleset before applying it to GCaps. Failure to do so will result in no rules being applied.

As a reminder, the `Tenant mode` area has three configuration options:

- `Single tenant`:
- Assigning a ruleset to inspect the traffic whatever interface is present
- `Multi-tenant by interface`:
- Assigning a ruleset per GCap monitoring interface
- Assigning a default ruleset for undefined GCap monitoring interfaces
- `Multi-tenant by VLAN`:
- Assigning one ruleset per VLAN
- Assigning a ruleset for the default VLAN for those VLANs not created via the interface

Note:

These configuration options are exclusive.
This means that it will not be possible to apply a single tenant and multi-tenant by VLAN configuration at the same time.

For	go to the
View or modify the single-tenant configuration	1- *Procedure to open the `GCaps profiles` window* 2- *Procedure to setup the `Single-tenant` mode*
View or modify the multi-tenant by interface configuration	1- *Procedure to open the `GCaps profiles` window* 2- *Procedure to setup the `Multi-tenant by interface` mode*
View or modify the multi-tenant by VLAN configuration	1- *Procedure to open the `GCaps profiles` window* 2- *Procedure to setup the `Multi-tenant by VLAN` mode*

7.4.2.2 Links associated

The rulesets and the GCap profiles are presented in *Sigflow engine*.
To manage the rules, see the *Configuring the Sigflow engine* menu.
The graphic interface is described in the *`Detection Rulesets` section of the `GCaps profiles` screen*.

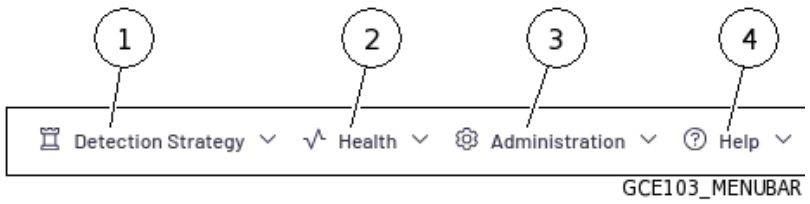
7.4.2.3 Prerequisites

User: member of **Operator** group

7.4.2.4 Preliminary operations

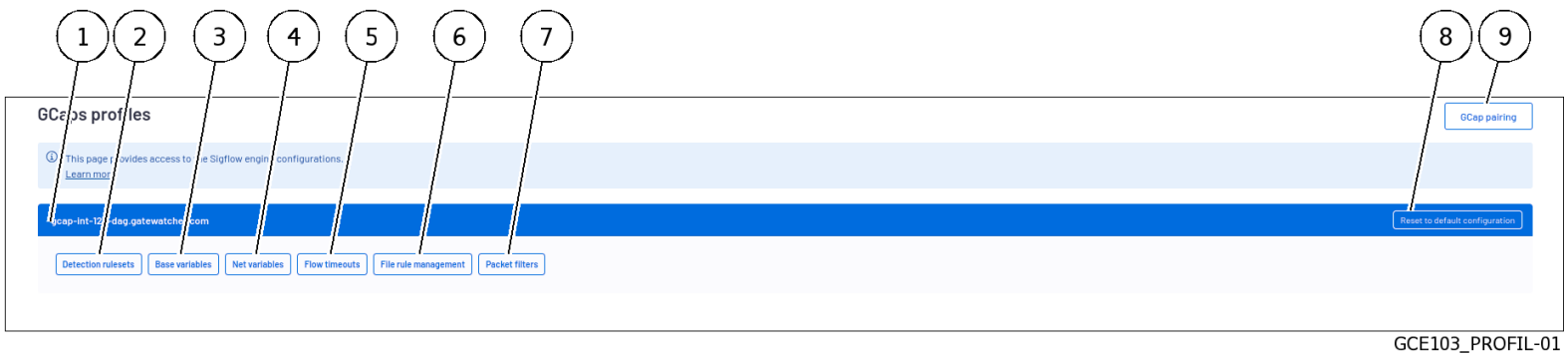
- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

7.4.2.5 Procedure to open the `GCaps profiles` window

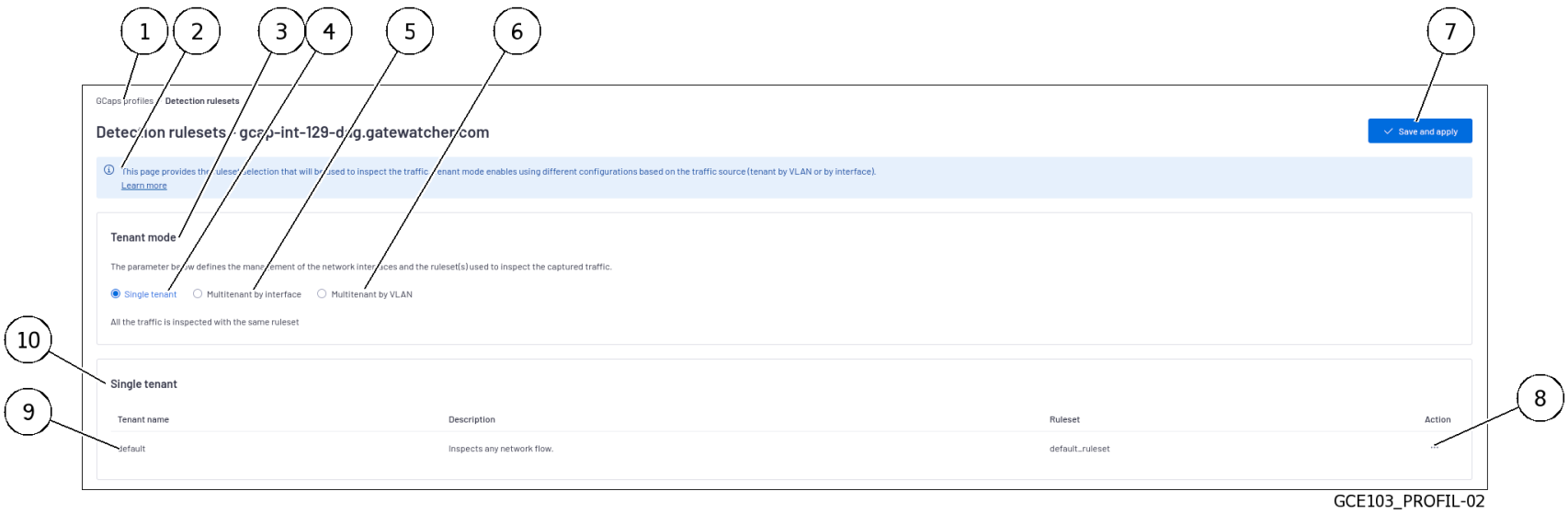


- From the navigation bar, click successively on:
- The `Detection strategy` button (1)
- The `GCaps profiles` button of the `Sigflow engine` category
  The `GCaps profiles` window is displayed.

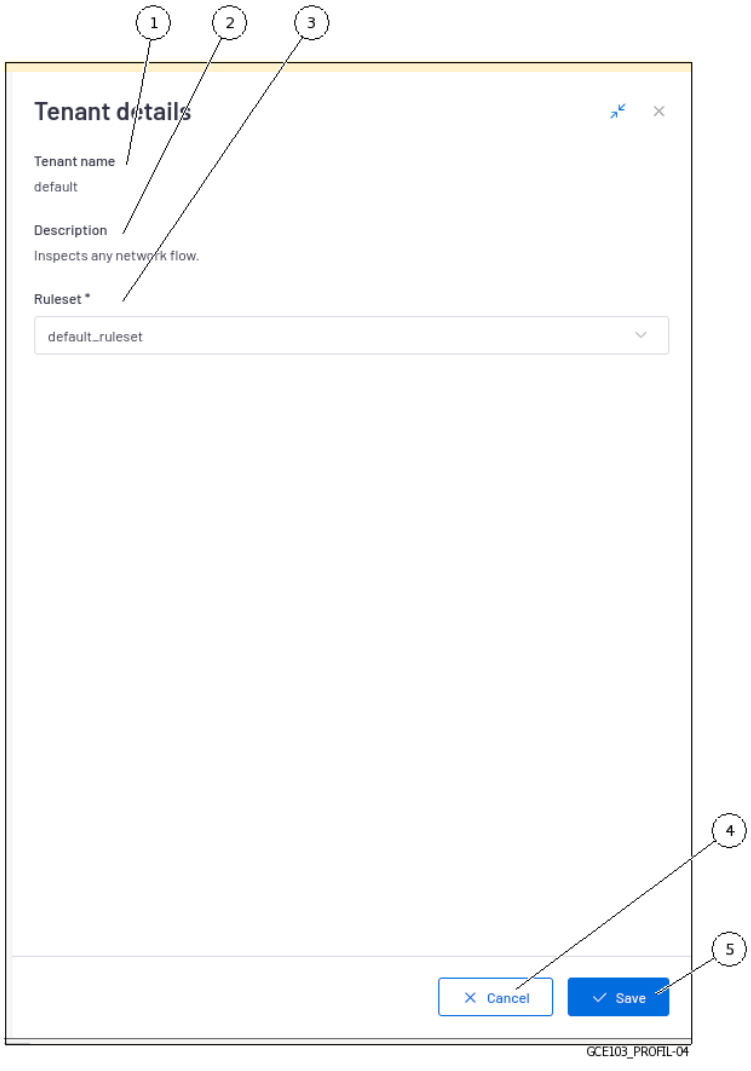
7.4.2.6 Procedure to setup the `Single-tenant` mode



- Click on the `Detection rulesets` button (2).



- Select on the `Single-tenant` choice (4) of the `Tenant mode` (3).
  The `Single tenant` part displays the parameters of this configuration.
- If the ruleset defined in the `Ruleset` field is ok, there is nothing to do.
  Otherwise, apply the following procedure:
  - Click on the `Edit tenant` command of the `Action` field (8).
    The `Tenant details` window enables to modify the ruleset to be used.

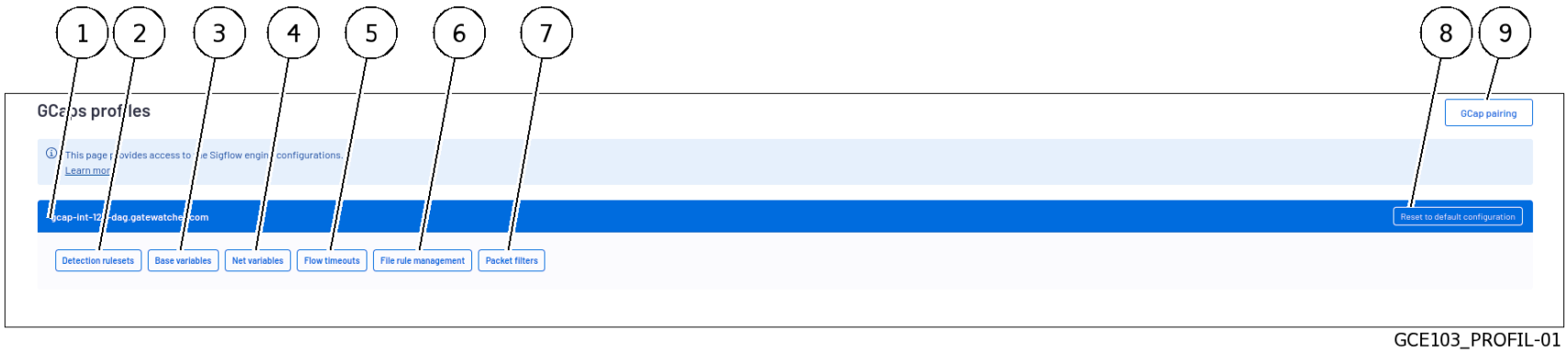


- Select the ruleset to be used on the `Ruleset` field (3).
- Click on the `Save` button (5).
  The following message is displayed:

```
Success
Your data has been saved
```

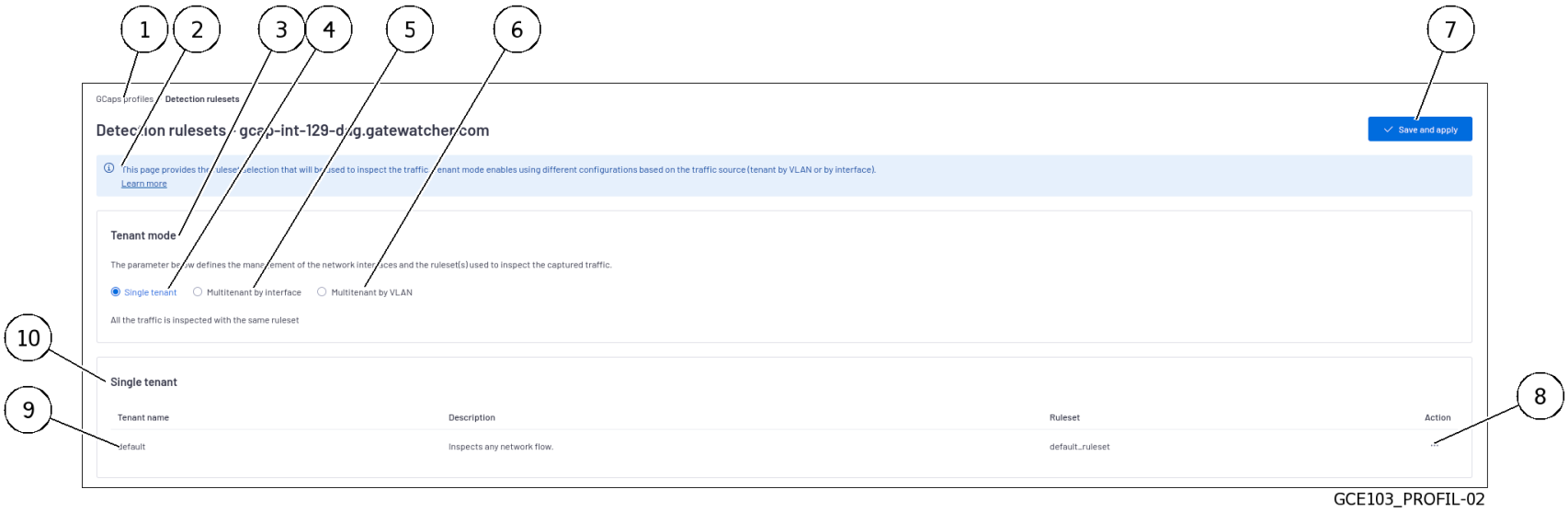
- If the configuration of the GCap profile is finished then click on the `Save and apply` button to send the new GCap profile to the GCap. Otherwise, continue the configuration by using another GCap profiles procedure.

7.4.2.7 Procedure to setup the `Multi-tenant by interface` mode



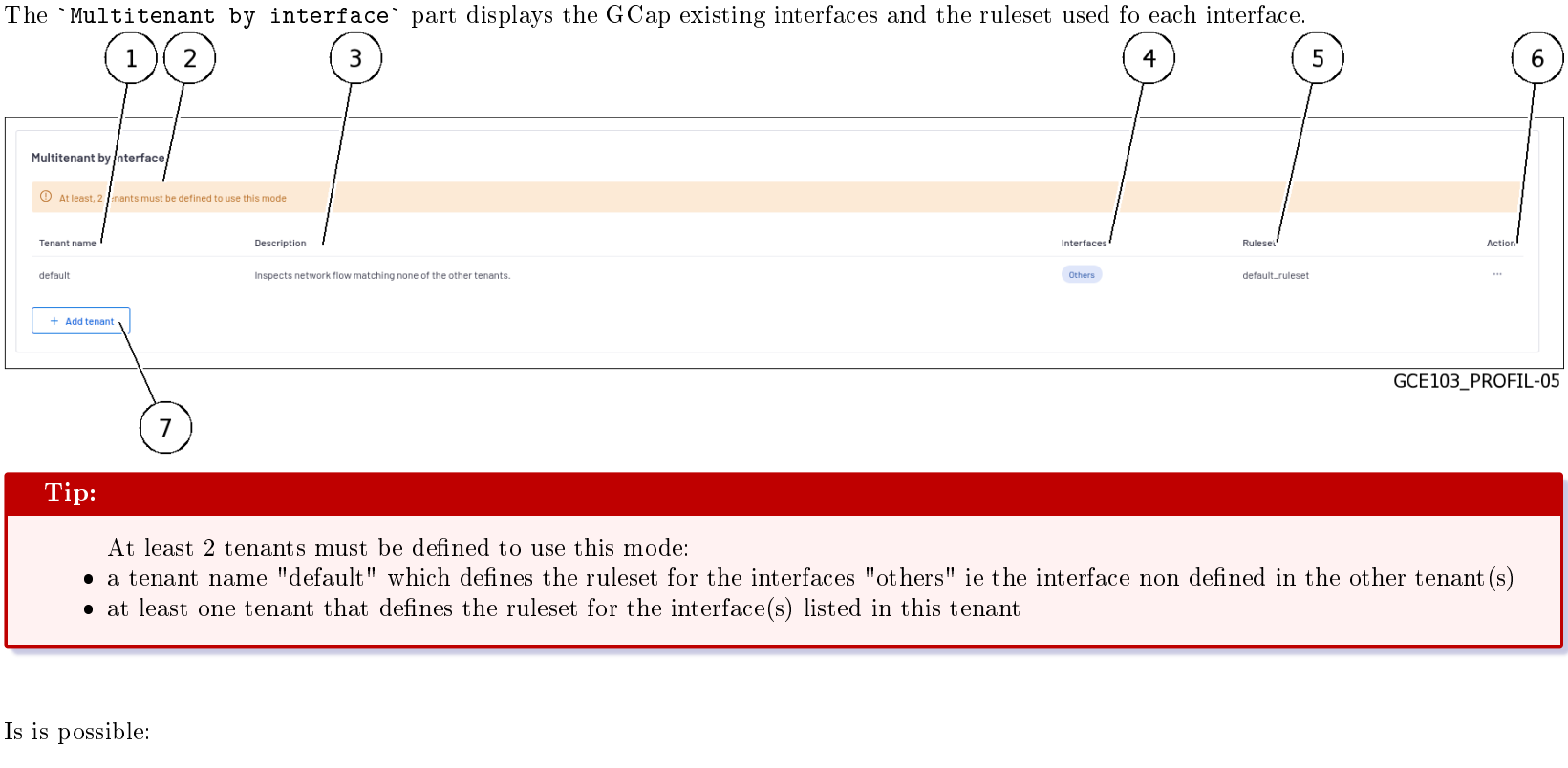
GCE103_PROFIL-01

- Click on the `Detection rulesets` button (2).



GCE103_PROFIL-02

- Click on the `Multi-tenant by interface` choice (5) of the `Tenant mode` (3).
  The `Multitenant by interface` part displays the GCap existing interfaces and the ruleset used fo each interface.



GCE103_PROFIL-05

Tip:

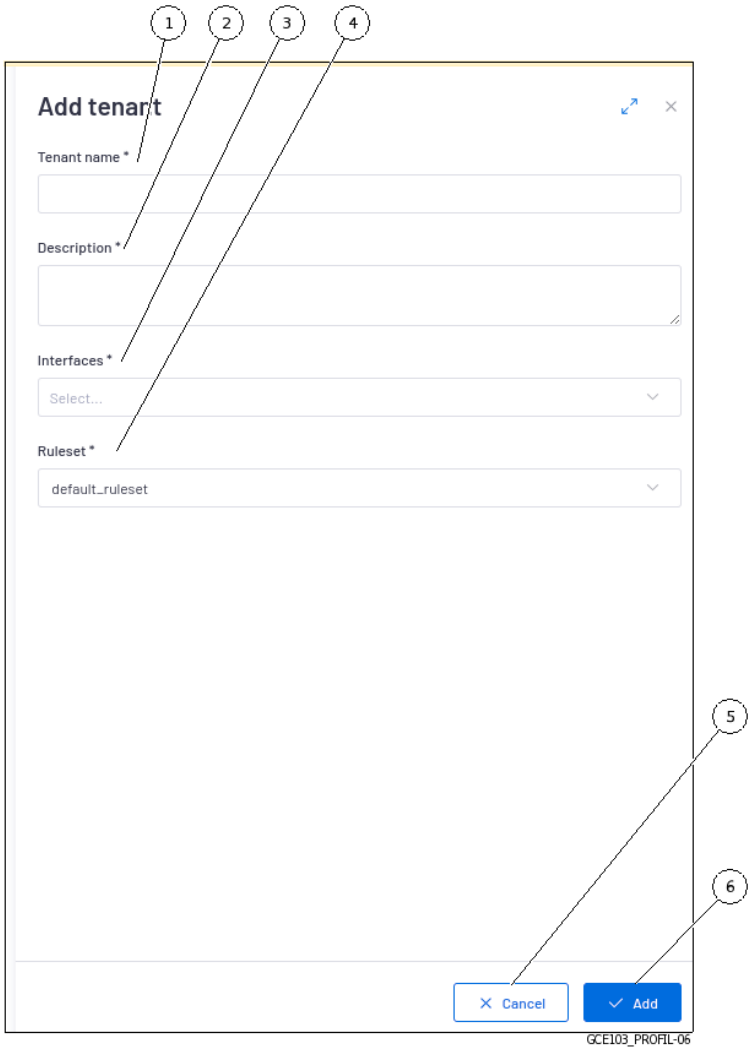
At least 2 tenants must be defined to use this mode:

- a tenant name "default" which defines the ruleset for the interfaces "others" ie the interface non defined in the other tenant(s)
- at least one tenant that defines the ruleset for the interface(s) listed in this tenant

Is is possible:

- To modify the ruleset used for an existing interface
- To create a new interface then select the ruleset to be applied

- If the ruleset defined in the `Ruleset` field for each defined interface is ok, there is nothing to do.
  Otherwise, apply the following procedure to add a new tenant:
  - Click on the `Add tenant` button (7).
    The `Add tenant` window enables to select or modify the ruleset to be used in this configuration.



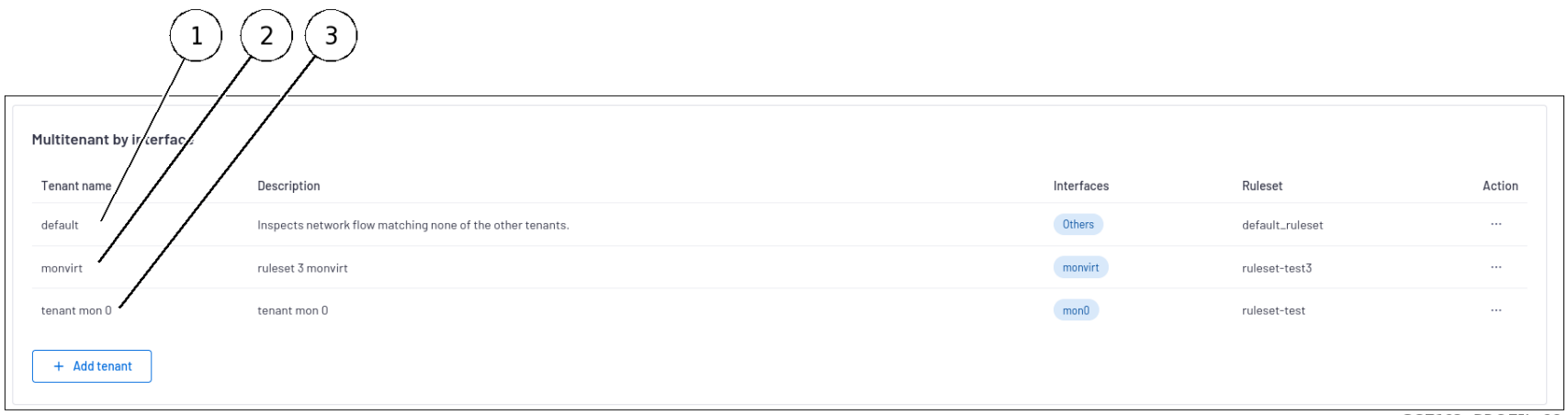
- Enter the tenant name in the `Tenant name` field (1).
- Enter the description name in the `Description` field (2).
- Select the interface to be used in the `Interfaces` field (3).
- Select the ruleset to be used in the `Ruleset` field (4).
- Click on the `Add` button (6).

  The following message is displayed:

```
Success
Your data has been saved
```

- If the configuration of the GCap profile is finished then click on the `Save and apply` button to send the new GCap profile to the GCap. Otherwise, continue the configuration by using another GCap profiles procedure.

Configuration example:



In this example, there are three tenants:

- The tenant named `default` (1) enables:
- To analyze the traffic coming from interfaces not defined by other tenants (indicated by the name `Others`)
- To configure the Sigflow engine with rules defined in ruleset named with default_ruleset
- The tenant named `monvirt` (2) enables:
- To analyze the traffic coming from the monvirt interface (indicated by the name `monvirt`)
- To configure the Sigflow engine with rules defined in ruleset named with ruleset-test3
- The tenant named `tenant mon0t` (3) enables:
- To analyze the traffic coming from the mon0 interface (indicated by the name `mon0`)
- To configure the Sigflow engine with rules defined in ruleset named with ruleset-test

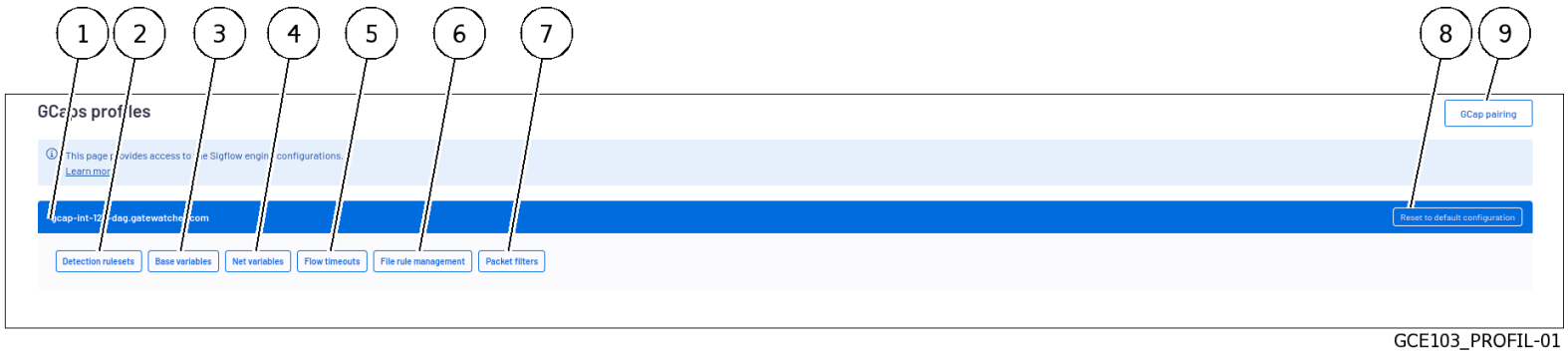
Note:

Detection will differ between traffic received on interfaces mon0 and mon1 because the rulesets themselves are different.

Note:

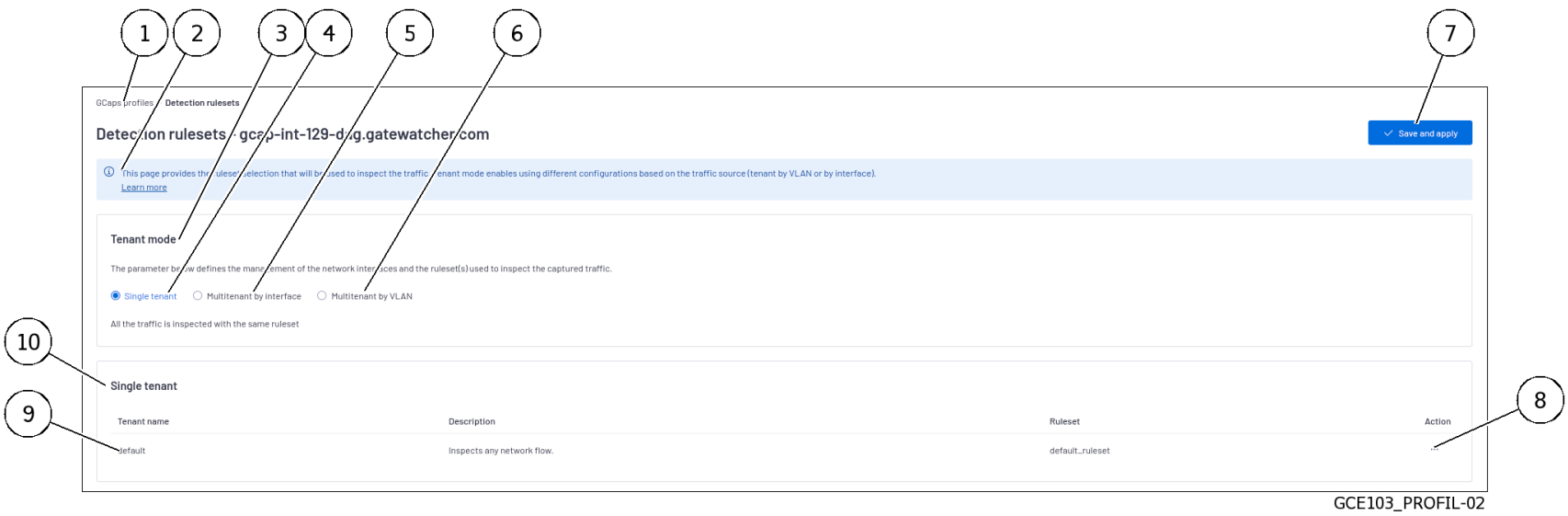
To modify an existing tenant, apply the same procedure by using the `Edit tenant` command of the `Action` field.

7.4.2.8 Procedure to setup the `Multi-tenant by VLAN` mode



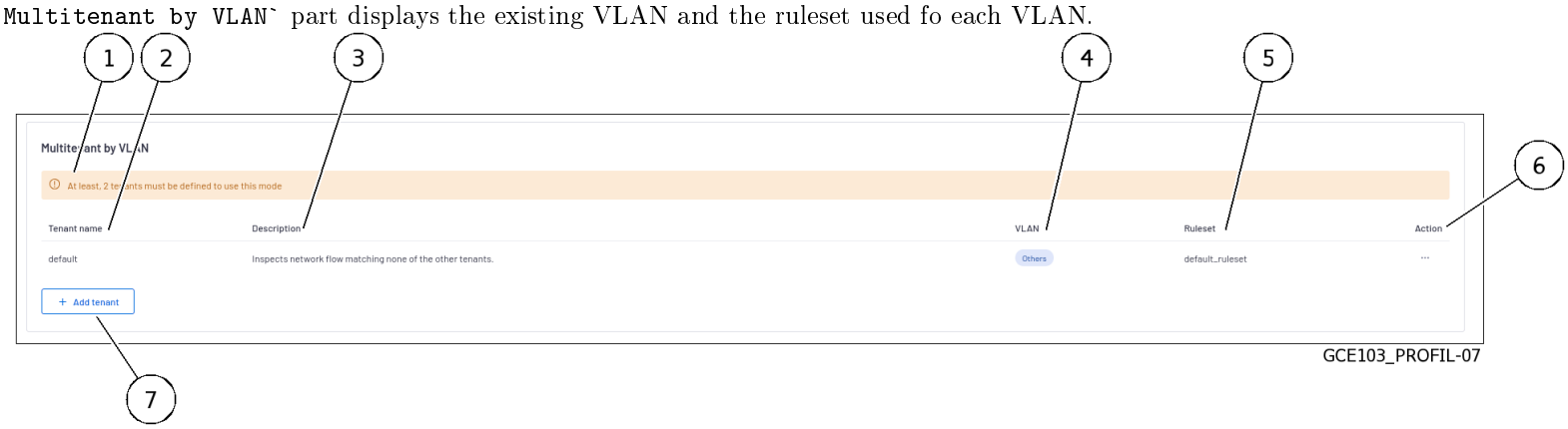
GCE103_PROFIL-01

- Click on the `Detection rulesets` button (2).



GCE103_PROFIL-02

- Click on the `Multi-tenant by VLAN` choice (6) of the `Tenant mode` (3).
  The `Multitenant by VLAN` part displays the existing VLAN and the ruleset used fo each VLAN.



GCE103_PROFIL-07

Tip:

At least 2 tenants must be defined to use this mode:

- a tenant name "default" which defines the ruleset for the VLAN "others" ie the interface non defined in the other tenant(s).
- at least one tenant that defines the ruleset for the VLAN(s) listed in this tenant

Is is possible:

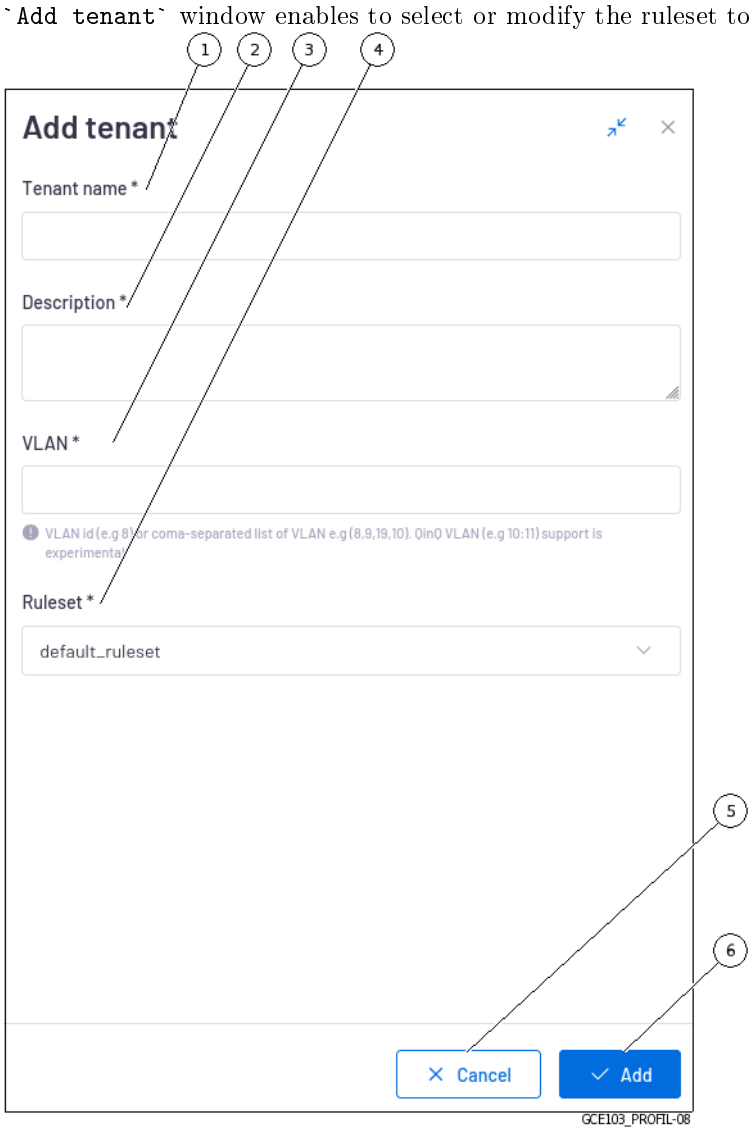
- To modify the ruleset used for an existing VLAN
- To create a new VLAN then select the ruleset to be applied

- If the ruleset defined in the `Ruleset` field for each defined VLAN is ok, there is nothing to do.

Otherwise, apply the following procedure to add a new tenant:

- Click on the `Add tenant` button (7)

  The `Add tenant` window enables to select or modify the ruleset to be used in this configuration.



  - Enter the tenant name in the `Tenant name` field (1)
  - Enter the description name in the `Description` field (2)
  - Select the VLAN to be used in the `VLAN` field (3)
  - Select the ruleset to be used in the `Ruleset` field (4)
  - Click on the `Add` button (6)

    The following message is displayed:

```
Success
Your data has been saved
```

- If the configuration of the GCap profile is finished then click on the `Save and apply` button to send the new GCap profile to the GCap. Otherwise, continue the configuration by using another GCap profiles procedure.

Note:

To modify an existing tenant, apply the same procedure by using the `Edit tenant` command of the `Action` field.

7.4.3 Configuring the Base variables parameters via the GCap profile

7.4.3.1 Introduction

The `Base variables` section enables configuring the parameters of the predefined profil selected during the pairing of each GCap paired to this GCenter.
The different configuration parameters are the following:

Attention:

Changing some of these parameters will cause the detection engine to restart, making the capture unavailable for the duration of the restart.

To	go to the
- Change in file reconstruction size - Set the size of the streams and files reconstructed by the GCap	1 - *Procedure to open the `GCaps profiles` window* 2 - *Procedure to change the reconstruction size of files*
Set the HTTP Proxy parameters	1 - *Procedure to open the `GCaps profiles` window* 2 - *Procedure to change the HTTP Proxy parameters*
Set fields in events such as payload, payload printable, packet, HTTP body and HTTP body printable	1 - *Procedure to open the `GCaps profiles` window* 2 - *Procedure to configure the fields present in the events*
Set the `Community ID` field	1 - *Procedure to open the `GCaps profiles` window* 2 - *Procedure to configure the `Community ID` parameters*
Set the alerting and logging of the different protocols available on the GCap	1 - *Procedure to open the `GCaps profiles` window* 2 - *Procedure to configure the alerting and logging protocols*

7.4.3.2 Links associated

The rulesets and the GCap profiles are presented in *Sigflow engine*.
To manage the rules, see the *Configuring the Sigflow engine* menu.

The graphic interface is described in the *`Base variables` Section of the `GCaps profiles` screen*.

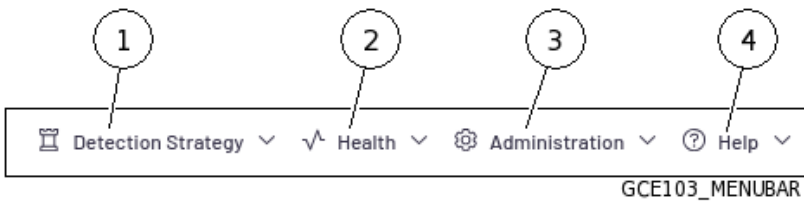
7.4.3.3 Prerequisites

User: member of **Operator** group

7.4.3.4 Preliminary operations

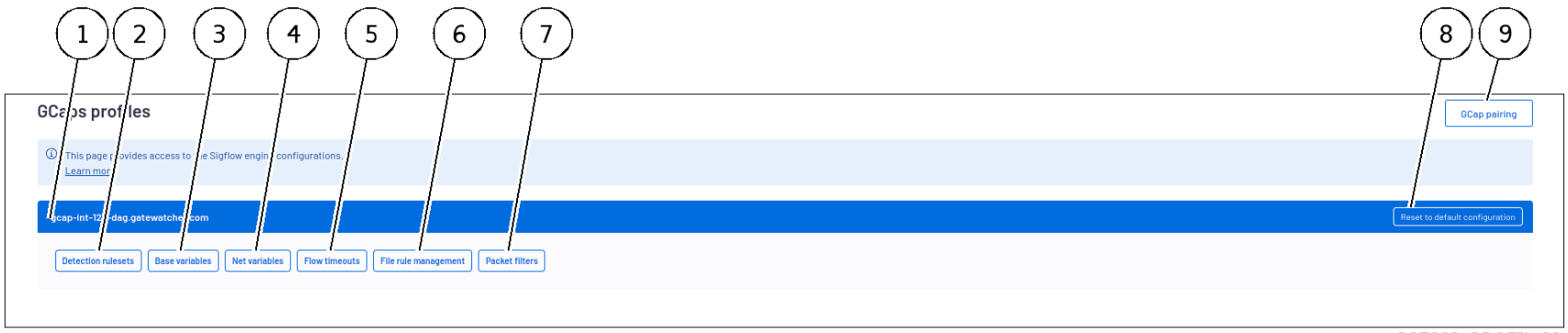
- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

7.4.3.5 Procedure to open the `GCaps profiles` window



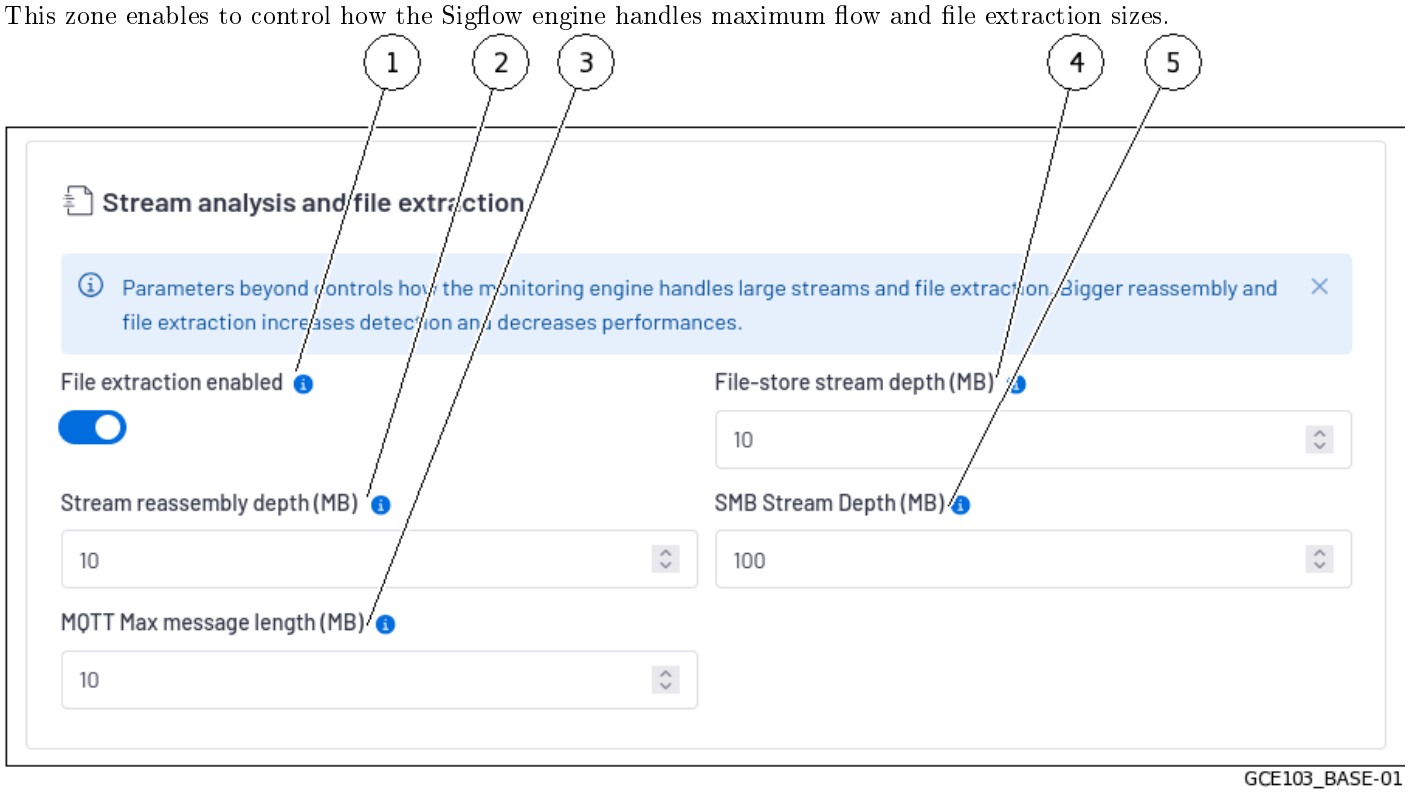
- From the navigation bar, click successively on:
- The `Detection strategy` button (1)
- The `GCaps profiles` button of the `Sigflow engine` category
  The `GCaps profiles` window is displayed.

7.4.3.6 Procedure to change the reconstruction size of files



GCE103_PROFIL-01

- Click on the `Base variables` button (3).
  For further information about the parameters, see the *`Stream analysis and file extraction` zone*
- From the `Stream analysis and file extraction` section:
  This zone enables to control how the Sigflow engine handles maximum flow and file extraction sizes.



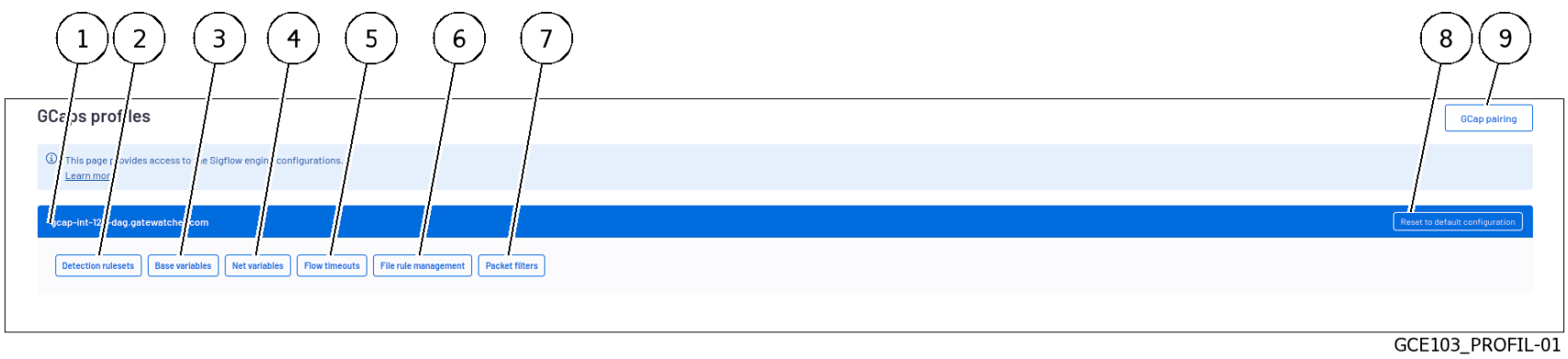
GCE103_BASE-01

  - Check the `File extraction enabled` choice (1) is activated
  - Change the value of the `File-store stream depth (MB)` field (4) (default is 10MB)
- Click on the `Apply configuration` button

Note:

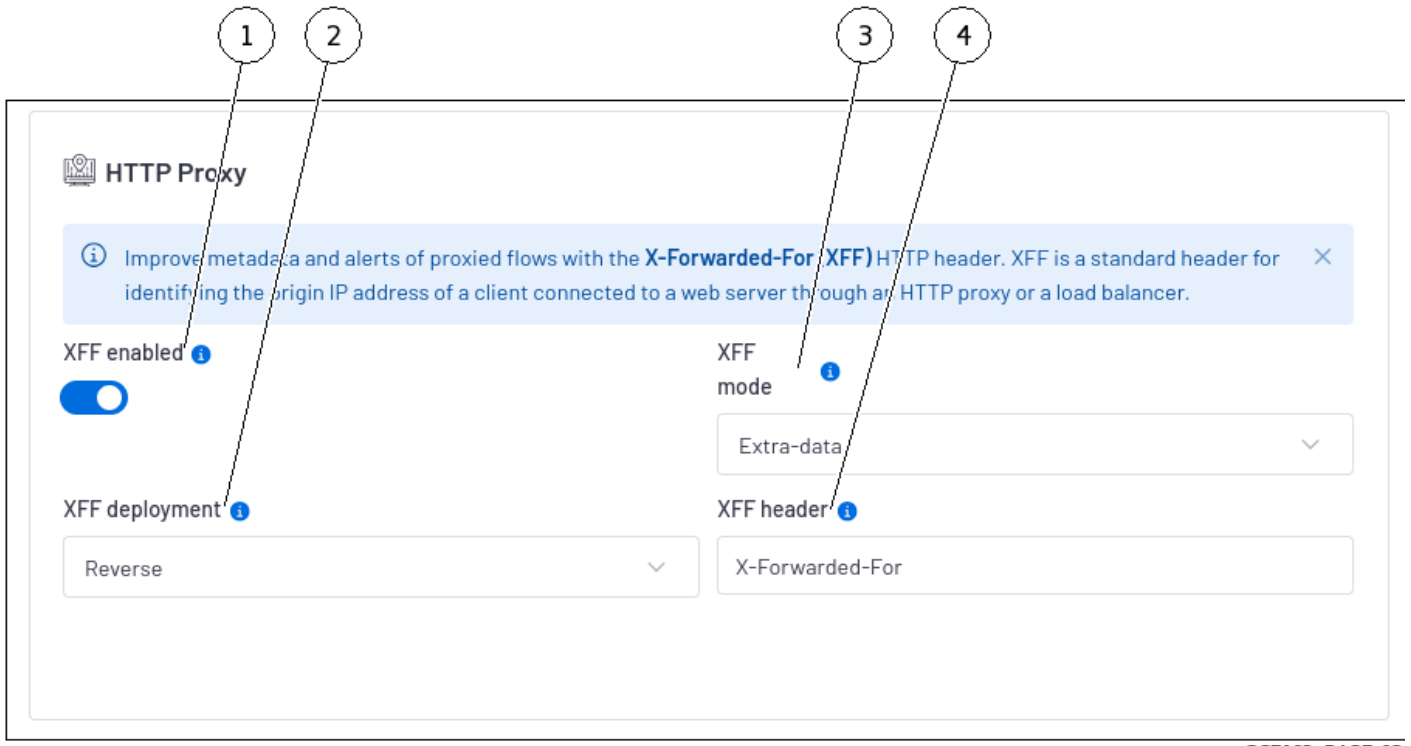
The value choice is important: the higher the value configured, the greater the impact on performance.

7.4.3.7 Procedure to change the HTTP Proxy parameters



GCE103_PROFIL-01

- Click on the `Base variables` button (3).
  For further information about the parameters, see the *`HTTP Proxy` Zone*
- From the `HTTP Proxy` section:
  This zone improves the metadata and alerts of the mandated streams with the X-Forwarded-For (XFF) http header.

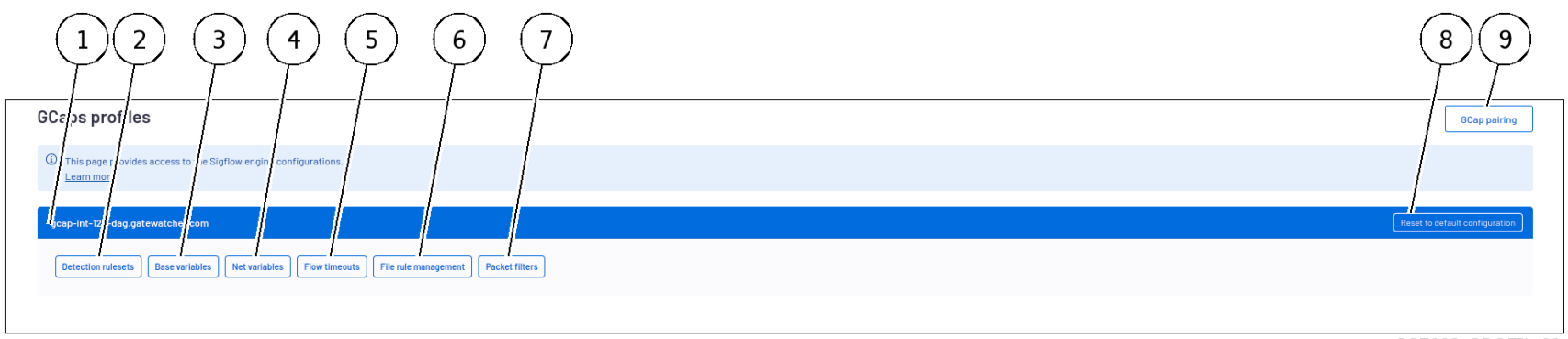


GCE103_BASE-02

- Select the `XFF enabled` (1) on the enable position
- Select the parameters (items 2 to 4)

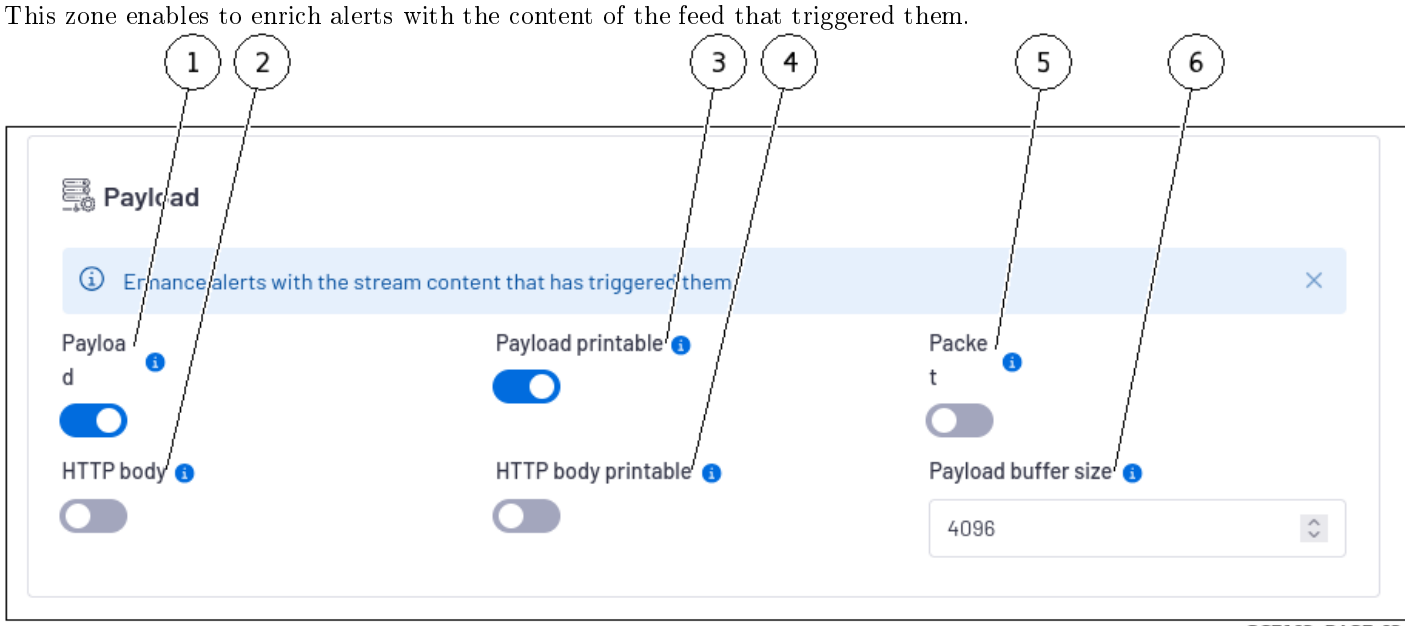
- Click on the `Apply configuration` button

7.4.3.8 Procedure to configure the fields present in the events



GCE103_PROFIL-01

- Click on the `Base variables` button (3).
  For further information about the parameters, see the *`Payload` zone*.
- From the `Payload` section:
  This zone enables to enrich alerts with the content of the feed that triggered them.



GCE103_BASE-03

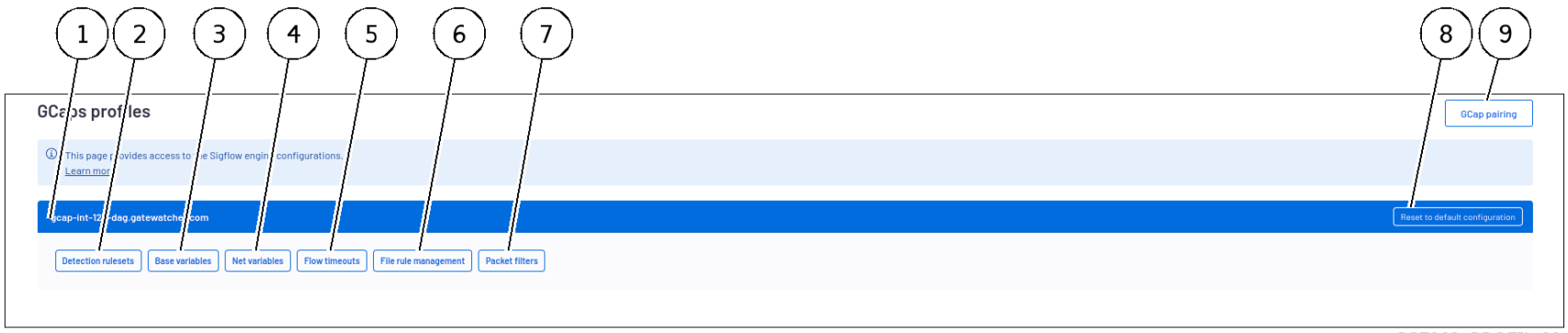
- Enable or disable fields (items 1 to 5) that will not appear in events
- If needed change the `Payload buffer size` selector (6)

- Click on the `Apply configuration` button

Note:

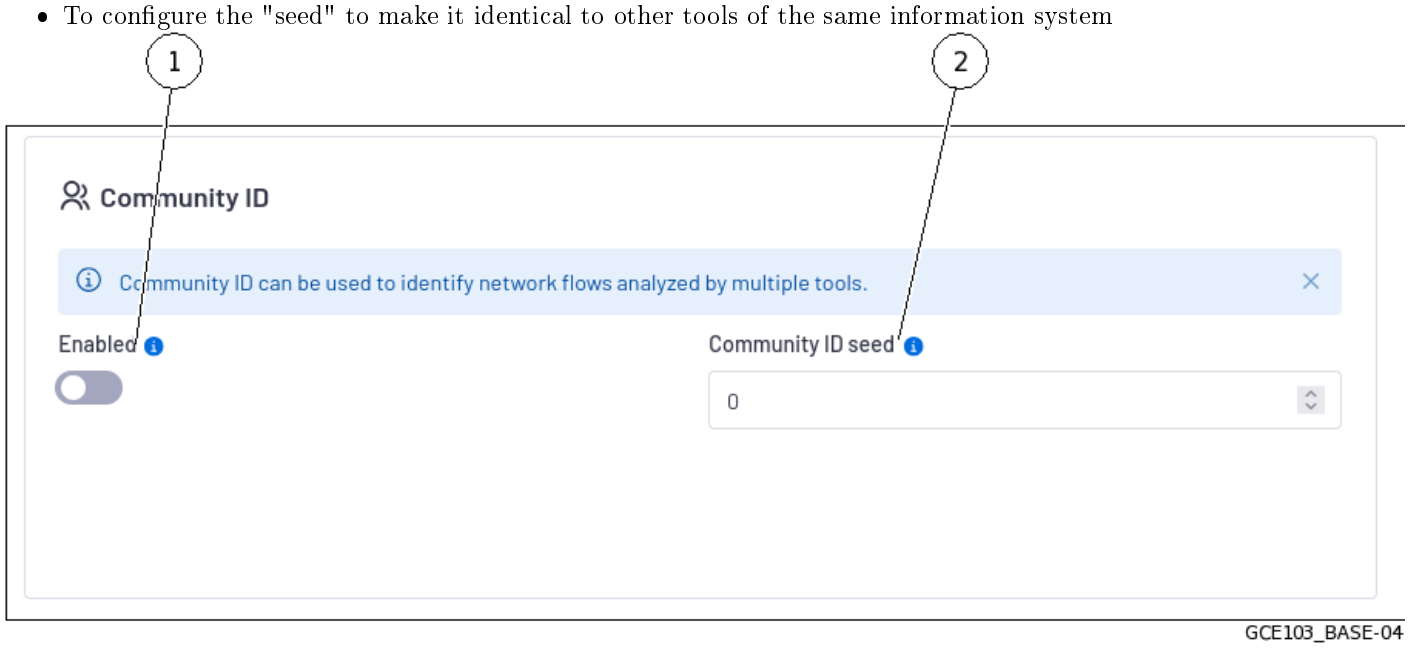
In some SIEMs, too high an event size can lead to truncation.

7.4.3.9 Procedure to configure the `Community ID` parameters



GCE103_PROFIL-01

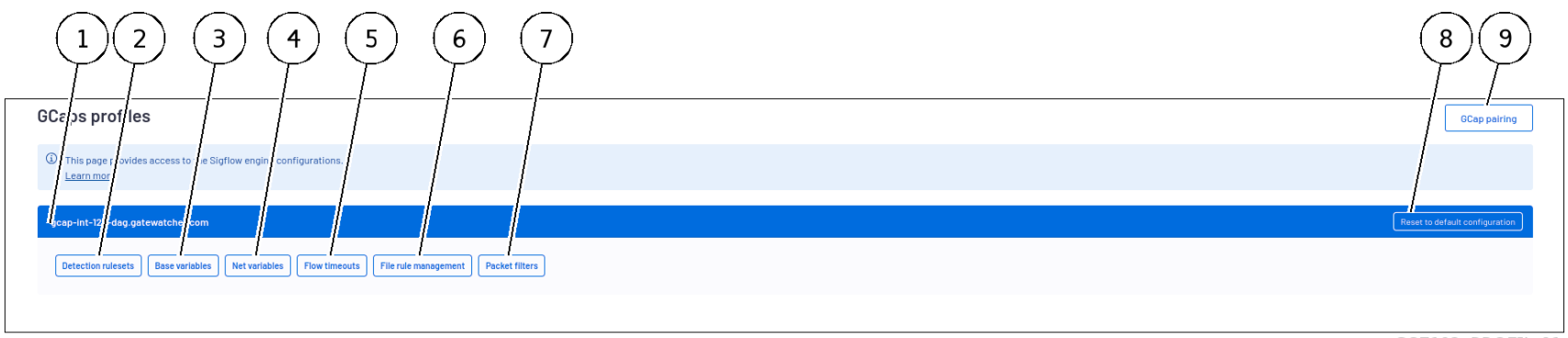
- Click on the `Base variables` button (3).
  For further information about the parameters, see the *`Community ID` zone*.
- From the `Community ID` section:
  This zone enables:
  - To activate the `Community ID` field in the events.
    The latter identifies the network flows analyzed*
  - To configure the "seed" to make it identical to other tools of the same information system



GCE103_BASE-04

  - Select the `Enabled` (1) on the enable position
  - Enter the `Community ID seed` parameter (2)
- Click on the `Apply configuration` button

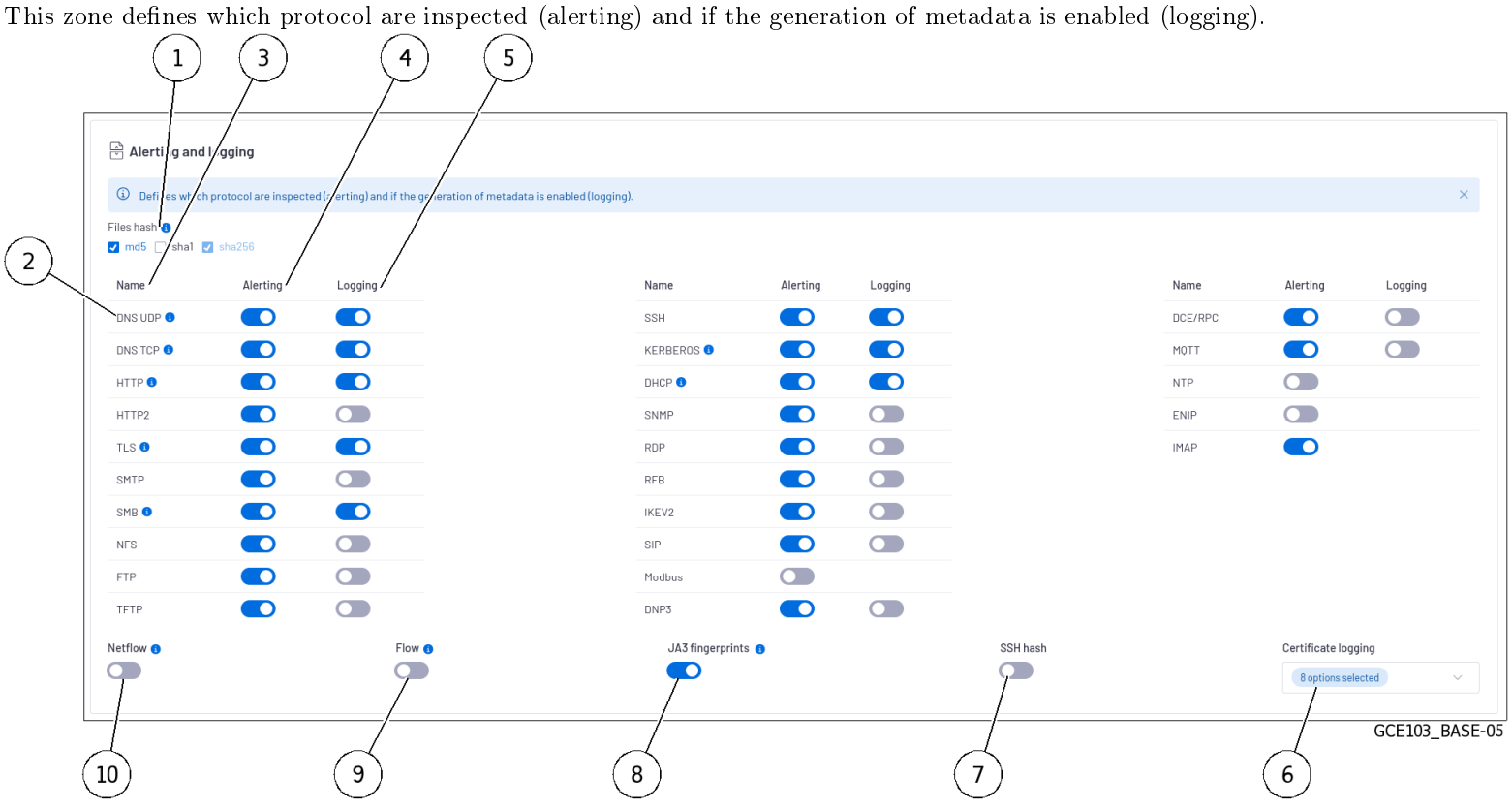
7.4.3.10 Procedure to configure the alerting and logging protocols



GCE103_PROFIL-01

- Click on the `Base variables` button (3).
  For further information about the parameters, see the *Description of the `Alerting and logging` zone*.
- From the `Alerting and logging` section:

This zone defines which protocol are inspected (alerting) and if the generation of metadata is enabled (logging).



- Tick the hash types that will appear in events (md5, sha1 and sha256) (1)
- Enable alerting for protocols that will raise alerts (4)
- Disable alerting for protocols that will not raise alerts (4)
- Enable logging for protocols that will need to raise metadata (5)
- Disable logging for protocols that should not raise metadata (5)
- If needed, use the options:
- `` `SSH hash` `` (7)
- `` `fingerprint JA3` `` (8)
- `` `Flow` `` (9)
- `` `Netflow` `` (10)

- Click on the `` `Apply configuration` `` button

7.4.4 Configuring the network variables parameters via the GCap profile

7.4.4.1 Introduction

The `` `Base variables` `` section enables configuring the network variables used by the GCap detection rules.
These variables correspond to the internal networks, external networks, and the various server types in the monitored environment.

7.4.4.2 Links associated

The rulesets and the GCap profiles are presented in *Sigflow engine*.
To manage the rules, see the *Configuring the Sigflow engine* menu.

The graphic interface is described in the *`Net variables` section of the `Config Gcaps profiles` menu*.

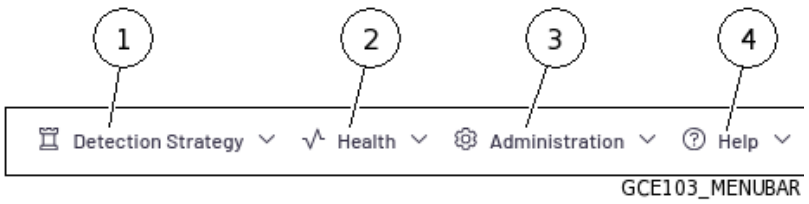
7.4.4.3 Prerequisites

User: member of **Operator** group

7.4.4.4 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)
- Select the tenant mode

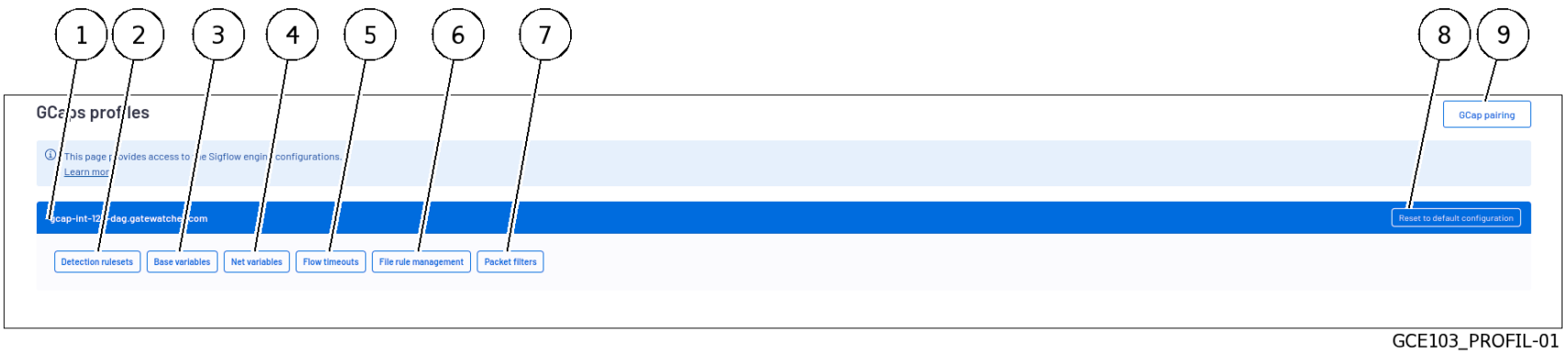
7.4.4.5 Procedure to open the `GCaps profiles` window



GCE103_MENUBAR

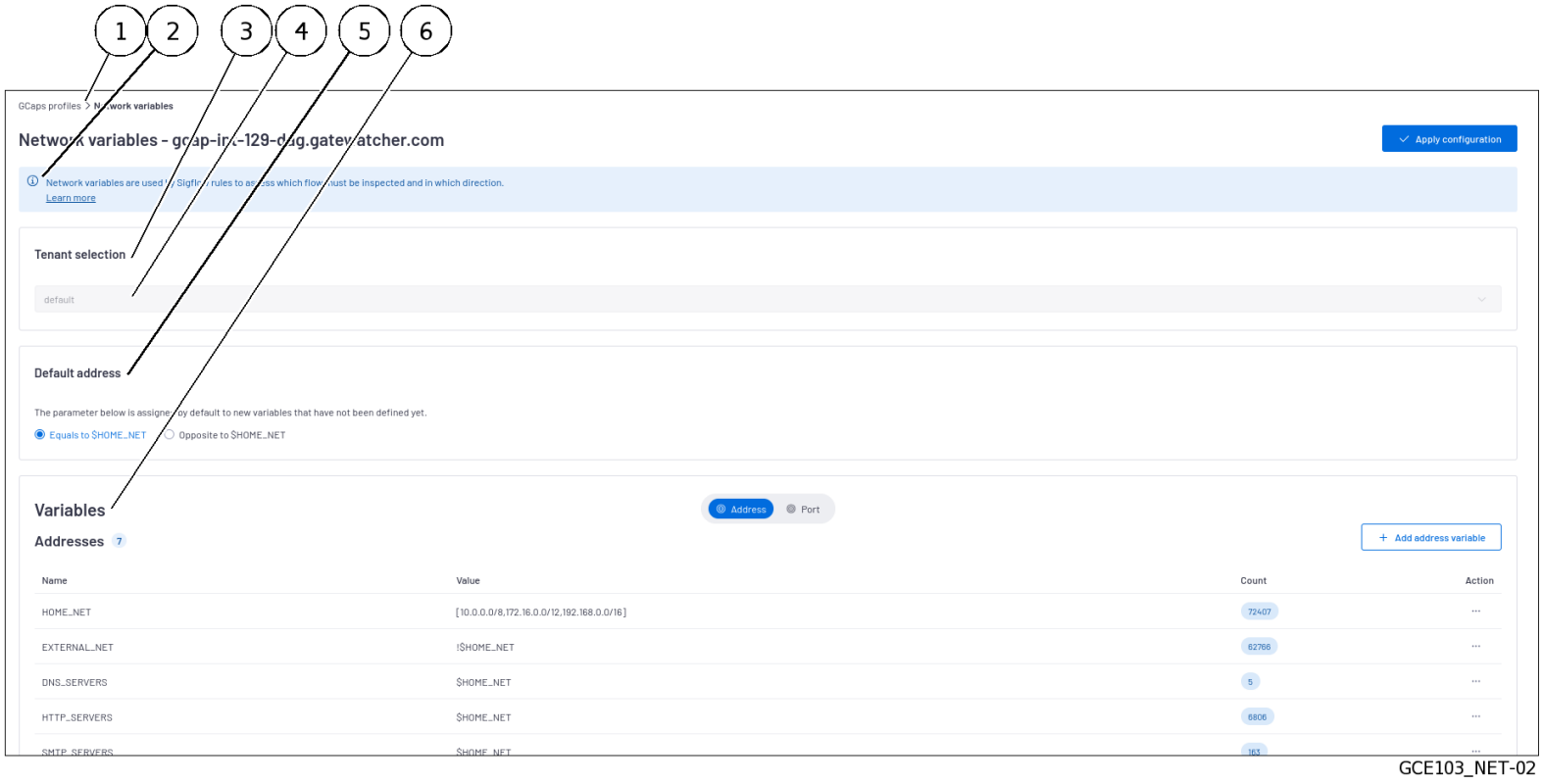
- From the navigation bar, click successively on:
- The `Detection strategy` button (1)
- The `GCaps profiles` button of the `Sigflow engine` category
  The `GCaps profiles` window is displayed.

7.4.4.6 Procedure to setup the network variables



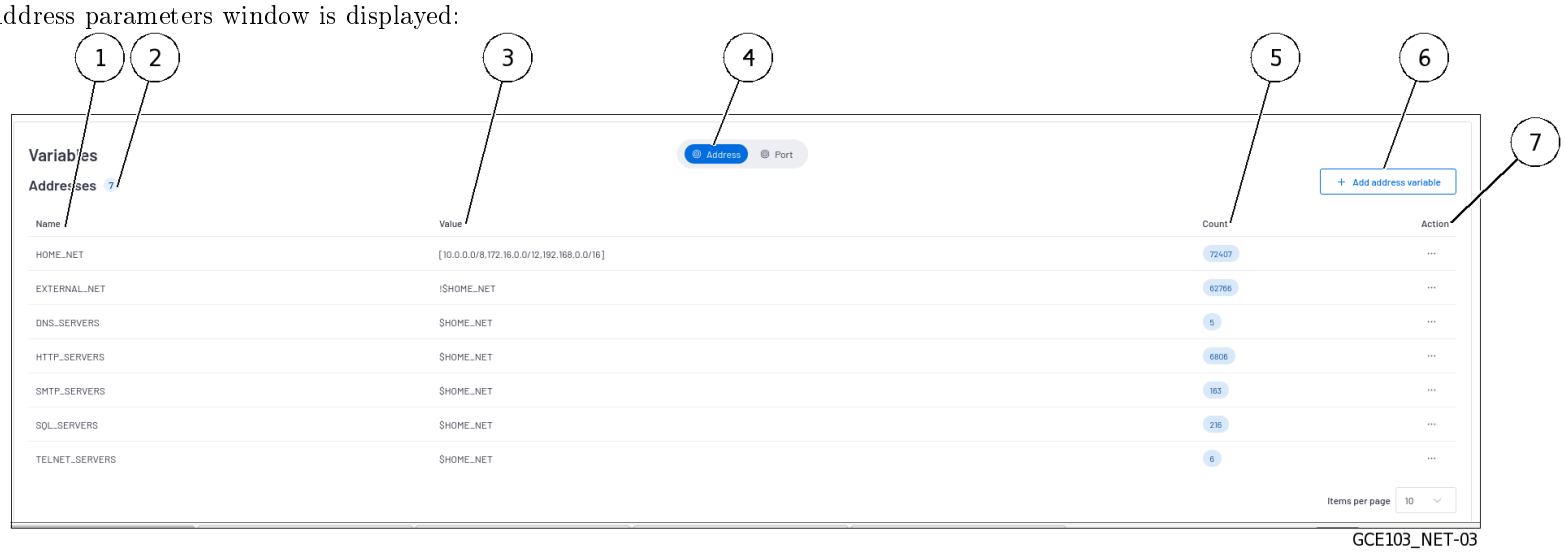
GCE103_PROFIL-01

- Click on the `Net variables` button (4).
  Network variables are used by Sigflow rules to assess which flow must be inspected and in which direction.
  In the structure of a rule, just after 'alert' and the protocol keyword, it is possible to use variables that will enable defining groups of IP addresses.



GCE103_NET-02

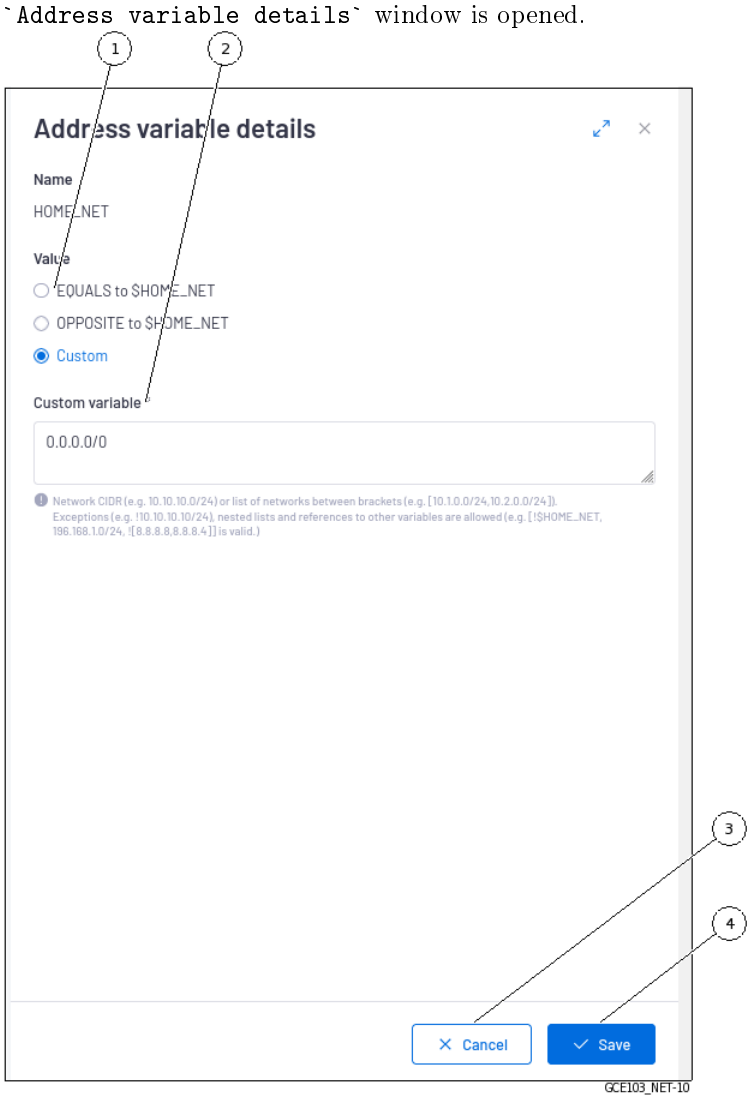
- According the tenant mode, select the tenant (interface or VLAN) in the `Tenant selection` zone (3).
- Select the `Default address` zone (5): choice `Equals to $HOME_NET` or `Opposite to $HOME_NET`.
- To manage the address parameters of the `Variables` zone (6) :
- Click on the `Address` button (4).
  The Address parameters window is displayed:



GCE103_NET-03

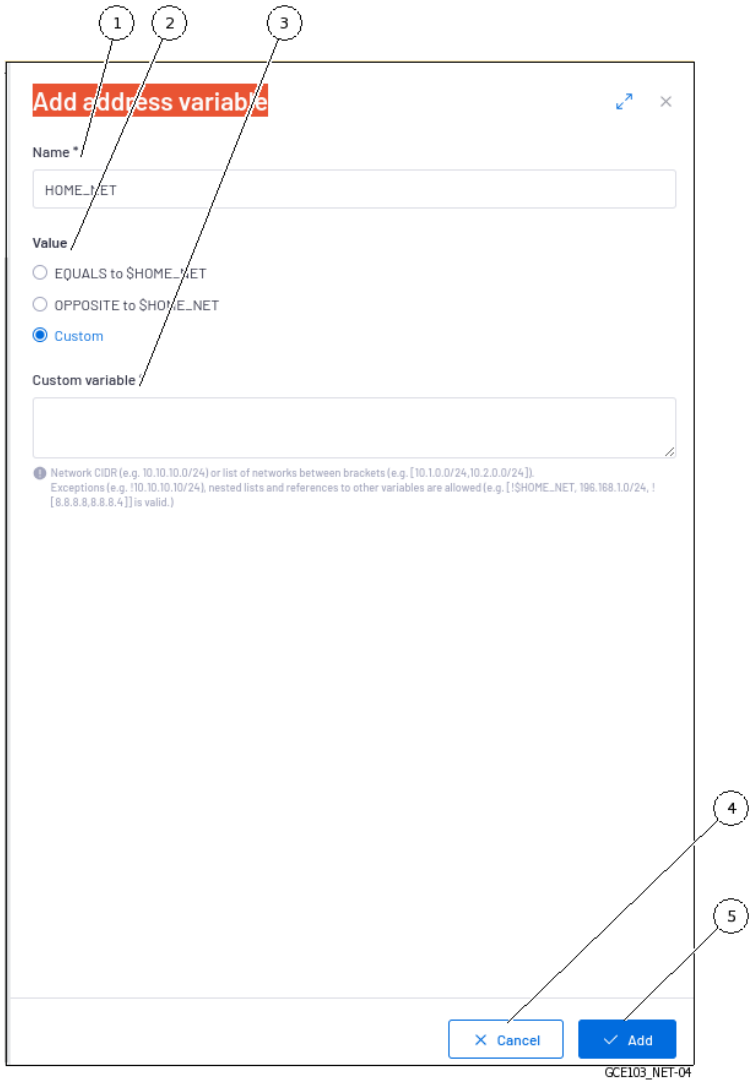
The window shows the current value of each parameter and the current count.

- To modify an existing parameter:
  - Click on the `Edit` command of the `Action` menu (7)
    The `Address variable details` window is opened.



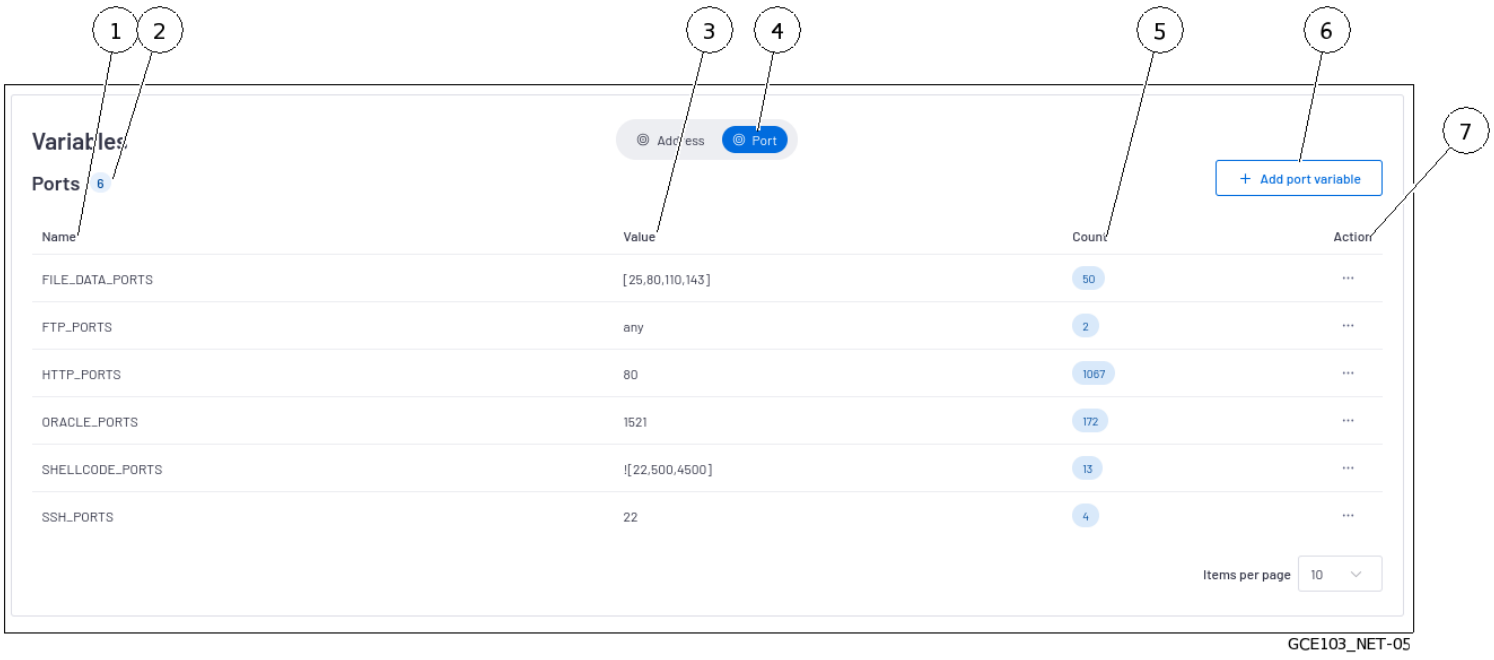
GCE103_NET-10

  - Select the `value` field (1) and if needed, the address in the `Custom variable` field (2).
  - Click on the `Save` button (4).
- To add a new parameter:
  - Click on the `Add address variable` button (6) of the `Variables-Adresses` zone.
    The `Add address variable` window is opened.



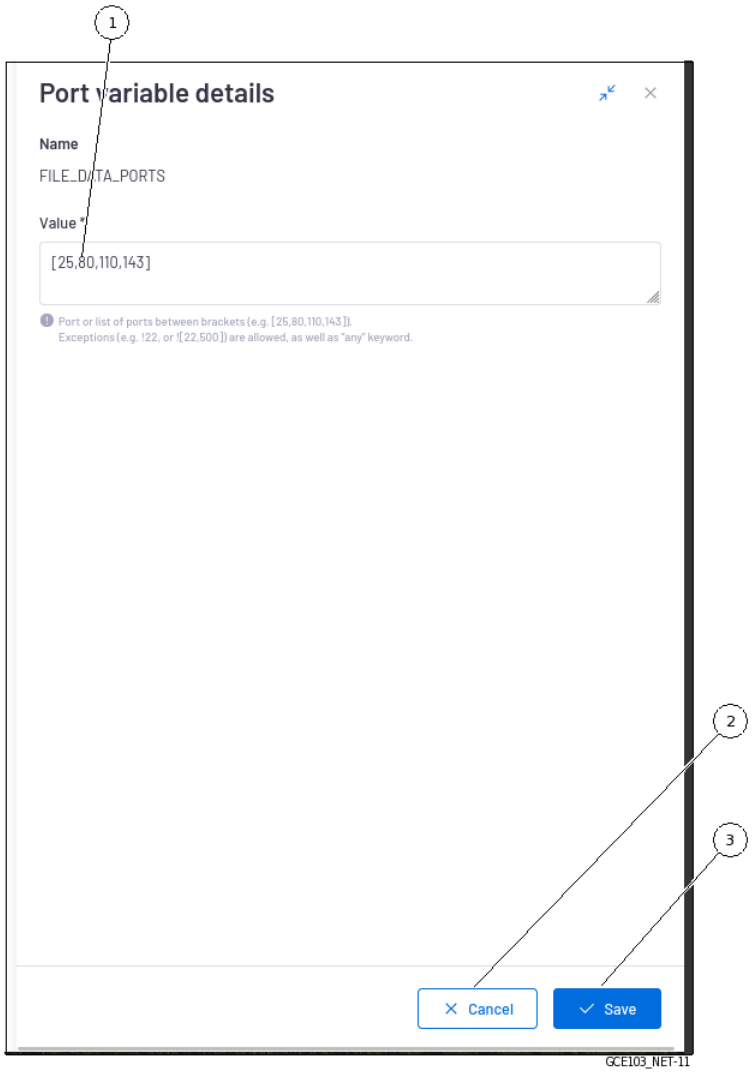
- Enter the name of the new parameter in the `Name` field (1)
- Select the `Value` field (2) and if needed, the address in the `Custom variable` field (3).
- Click on the `Add` button (5).

- To manage the port parameters of the `Variables` zone (6) :
  - Click on the `Port` button (4).



- To modify an existing parameter:
  - Click on the `Edit` command of the `Action` menu (7)

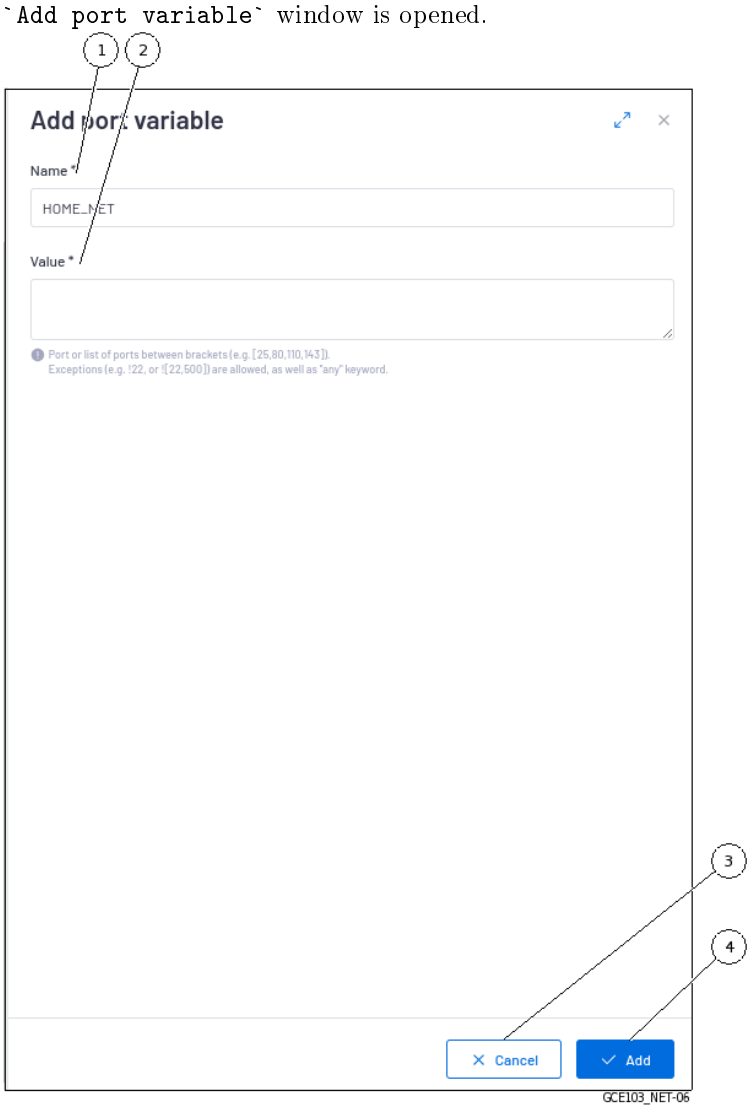
    The `Port variable details` window is opened.



- Modify the value in the `Value` field (1).
- Click on the `Save` button (3).

- To add a new parameter:
  - Click on the `Add port variable` button (6) of the `Variables-Ports` zone.

The `Add port variable` window is opened.



- Enter the name of the new parameter in the `Name` field (1)
- Select the `Value` field (2).

- Click on the `Add` button (4).

7.4.5 Configuring the flow timeouts via the GCap profile

7.4.5.1 Introduction

The `Flow timeouts` section sets the timeouts of the different states (New, Established and closed) for the listed protocols.

7.4.5.2 Links associated

The rulesets and the GCap profiles are presented in *Sigflow engine*.
To manage the rules, see the *Configuring the Sigflow engine* menu.

The graphic interface is described in the *`Flow timeouts` section of the `GCaps profiles` screen*.

7.4.5.3 Prerequisites

User: member of **Operator** group

7.4.5.4 Preliminary operations

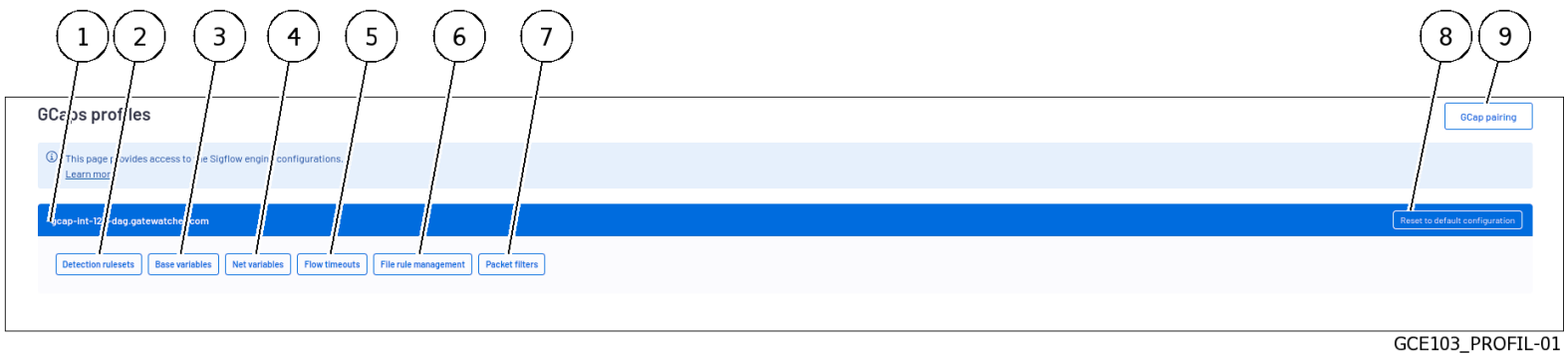
- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)
- Select the tenant mode

7.4.5.5 Procedure to open the `GCaps profiles` window

The rulesets and the GCap profiles are presented in *Sigflow engine*.
To manage the rules, see the *Configuring the Sigflow engine* menu.

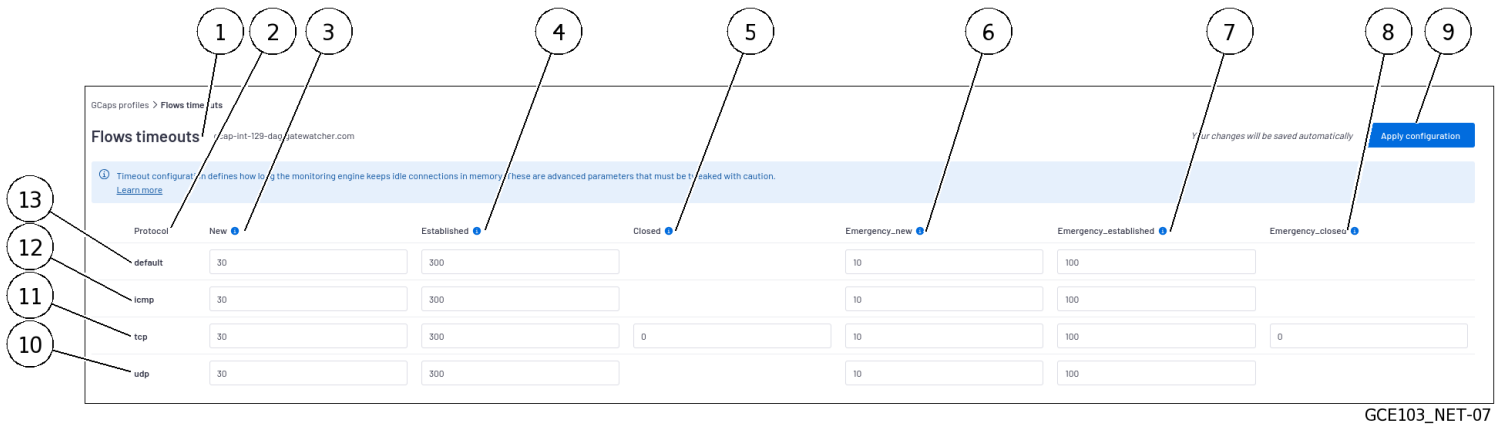
The graphic interface is described in the *`Flow timeouts` section of the `GCaps profiles` screen*.

7.4.5.6 Procedure to setup the flow timeouts



GCE103_PROFIL-01

- Click on the `Flow timeouts` button (5).



GCE103_NET-07

- For each protocol listed (10 to 13), modify if needed the parameters (3 to 8).
- Click on the `Apply configuration` button (9).

7.4.6 Configuring the file reconstruction rules via the GCap profile

7.4.6.1 Introduction

The `File rule management` section enables configuring the file reconstruction rules used by the GCap detection engine.
Reconstruction is based on several parameters: the protocol, the file type, and the file type value.

To	go to the
Set the file reconstruction by using the GCenter WebUI	1- *Procedure to open the `GCaps profiles` window* 2- *Procedure to set up the file reconstruction by using the GCenter WebUI*
Set the file reconstruction by using the csv editor	1- *Procedure to open the `GCaps profiles` window* 2- *Procedure to set up the file reconstruction by using the csv editor*
Save the current configuration	1- *Procedure to open the `GCaps profiles` window* 2- *Procedure to save the current configuration*
Load a saved configuration	1- *Procedure to open the `GCaps profiles` window* 2- *Procedure to load a saved configuration*
Add a reconstruction rule	1- *Procedure to open the `GCaps profiles` window* 2- *Procedure to add a file reconstruction rule*

7.4.6.2 Links associated

The rulesets and the GCap profiles are presented in *Sigflow engine*.
To manage the rules, see the *Configuring the Sigflow engine* menu.

The graphic interface is described in the *`File rules` section of the `GCaps profiles` screen*

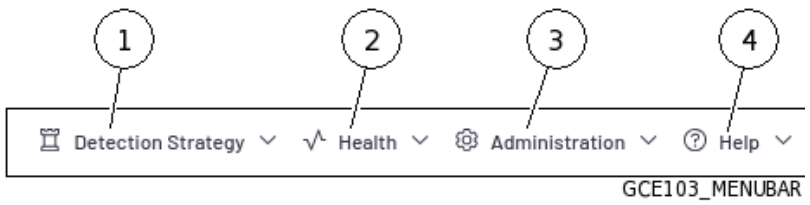
7.4.6.3 Prerequisites

User: member of **Operator** group

7.4.6.4 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

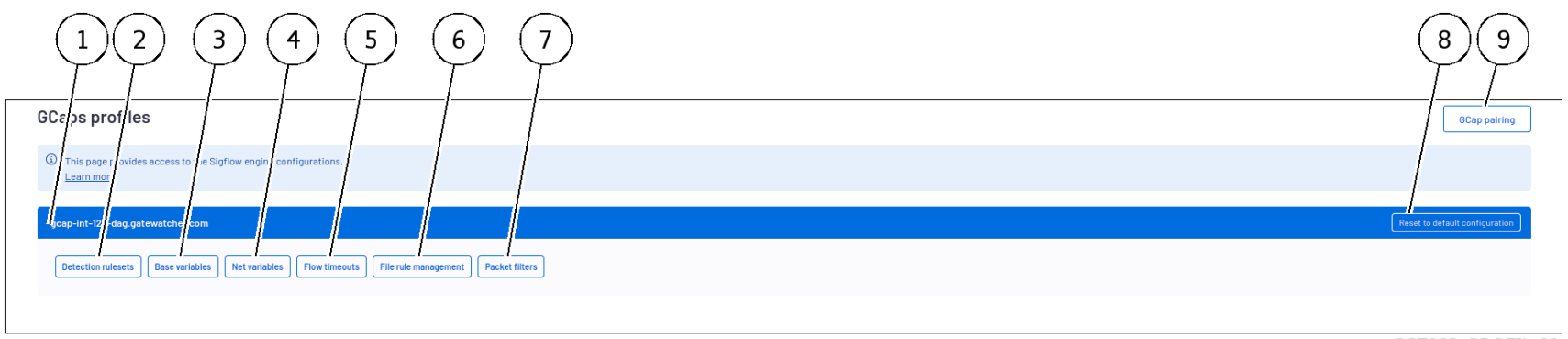
7.4.6.5 Procedure to open the `GCaps profiles` window



GCE103_MENUBAR

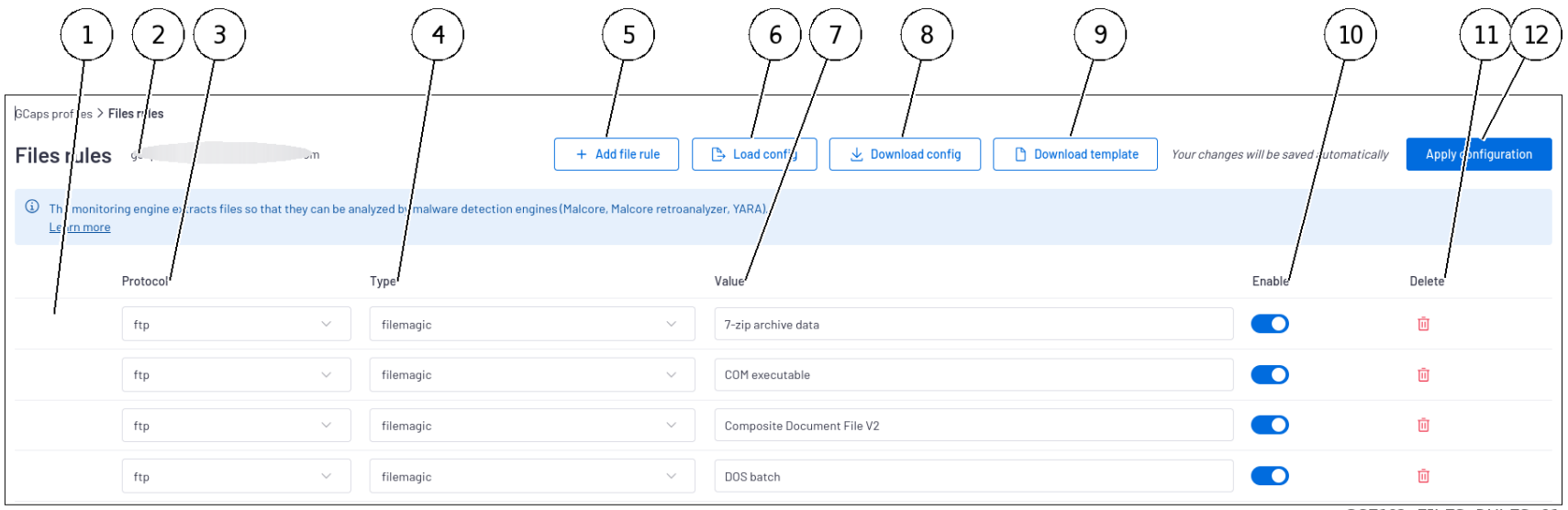
- From the navigation bar, click successively on:
- The `Detection strategy` button (1)
- The `GCaps profiles` button of the `Sigflow engine` category
  The `GCaps profiles` window is displayed.

7.4.6.6 Procedure to set up the file reconstruction by using the GCenter WebUI



GCE103_PROFIL-01

- Click on the `File rule management` button (6).



GCE103_FILES_RULES_01

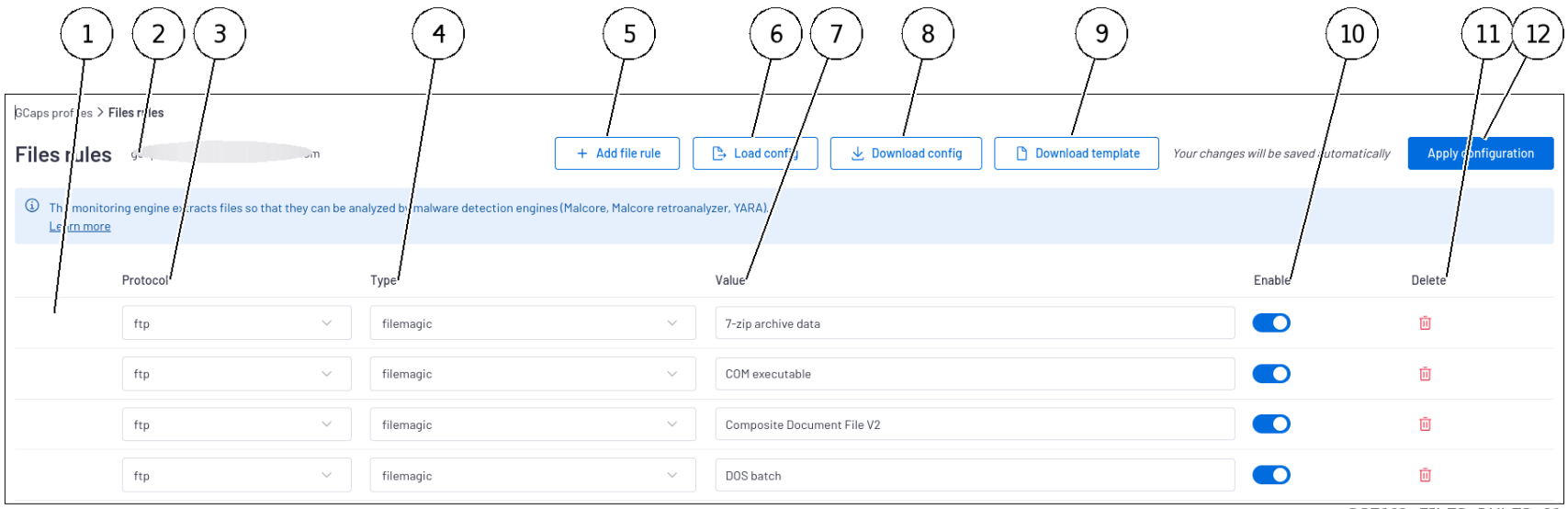
Note:

The rules displayed are those of the predefined profile previously loaded into the GCap during its pairing.
The rule list is given in paragraph *Rules applied depending on the GCap profile used*.

- For each rule, validate that the `protocol` (3), `type` (4), `value` (7) fields match the desired values.
- Enable or disable the desired rules using the enable button in the `Enable` (10) field.
- Completely remove the unnecessary rules.

- If necessary, insert rules using the `Add file rule` button (5) (see the *Procedure to add a file reconstruction rule*).
- Click on the `Apply configuration` button (12).

7.4.6.7 Procedure to set up the file reconstruction by using the csv editor



GCE103_FILES_RULES_01

Note:

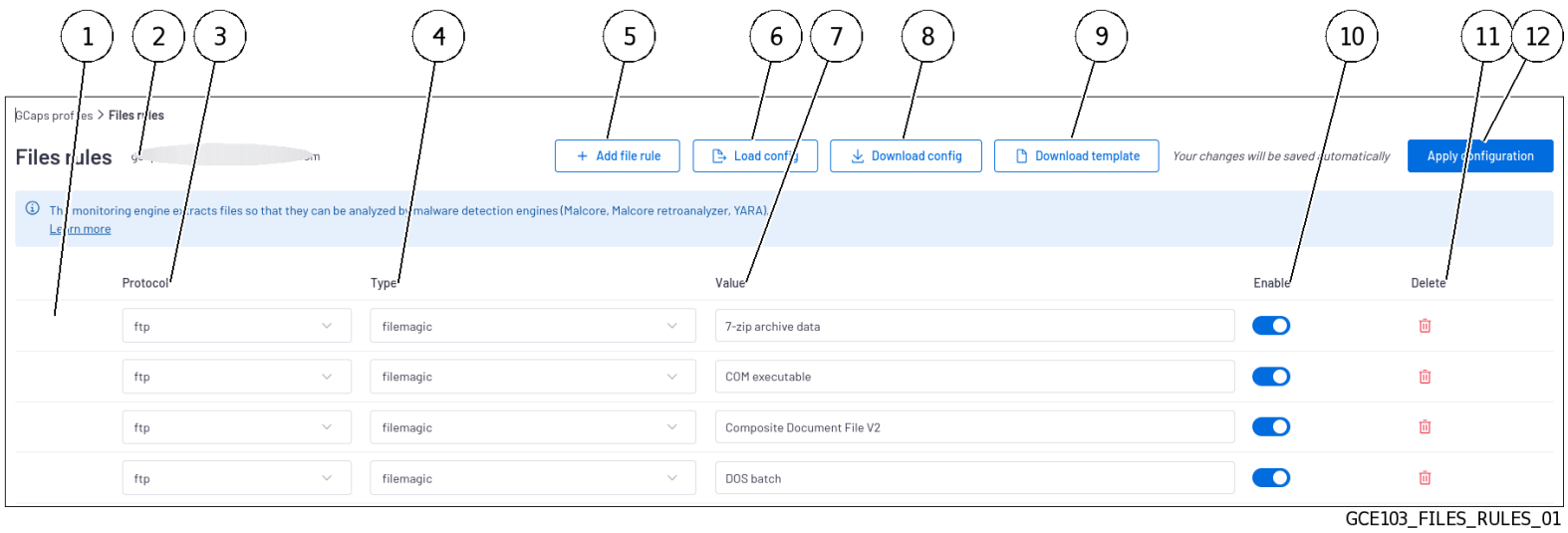
The rules displayed are those of the predefined profile previously loaded into the GCap during its pairing.
The rule list is given in paragraph *Rules applied depending on the GCap profile used*.

- Use the `Download config` button (8) to download the current configuration from the GCenter to the local PC.
  The file is named *1_files-rules-config.csv*.
- Or use the `Download template` button to download the template file from the GCenter to the local PC.
  The file is named *1_files-rules-template.csv*.
- Complete the csv file by using a csv editor.
  Here is a sample template file:

```
1 enabled,file_type,id,protocol,value
2 true,filemagic,,ftp,Microsoft Excel
3 true,extension,,http,exe
4 true,filemagic,,http2,7-zip archive data
```

- Save the file after modifications.
- Upload the file by using the `Load config` button (6).
  The file is checked during the importation.
  For example of an error: `Your line number x is invalid, please use the provided template`.
  After importation, the GCenter uses the downloaded configuration.

7.4.6.8 Procedure to save the current configuration



GCE103_FILES_RULES_01

- Click on the `Download config` button (8).
  The downloaded file is named *1_files-rules-config.csv*.

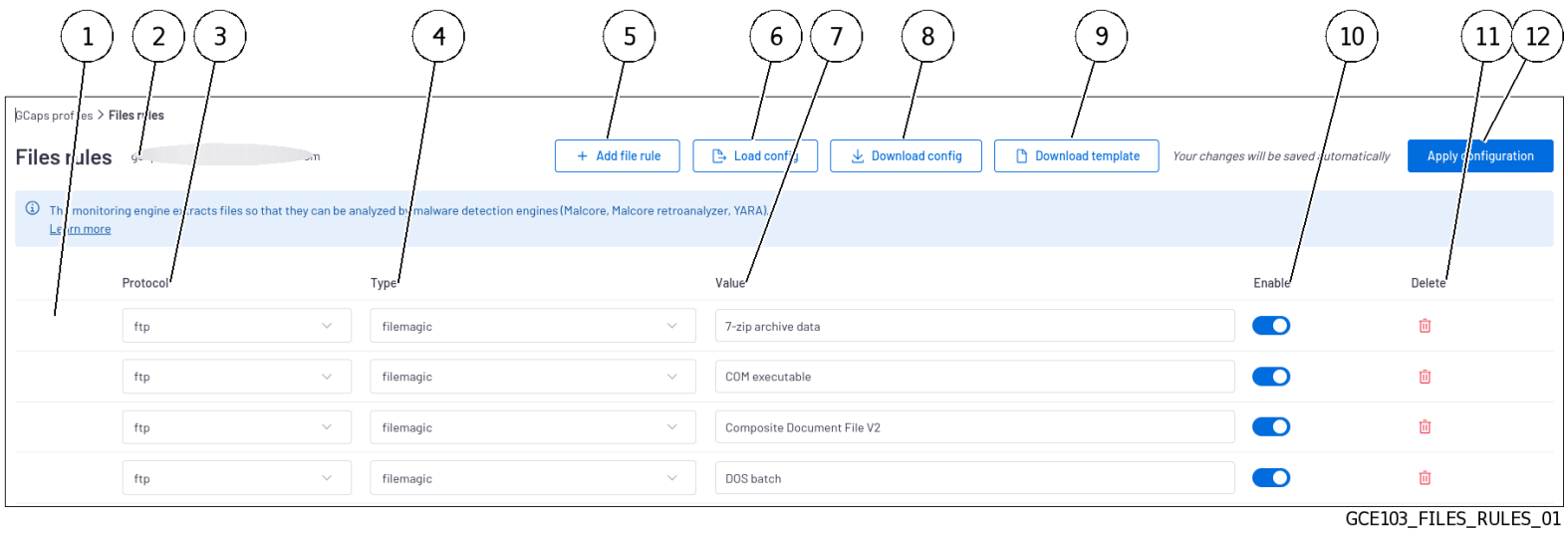
Note:

Locate the file in a directory which the name is composed by the GCap FQDN and the date.

7.4.6.9 Procedure to load a saved configuration

Note:

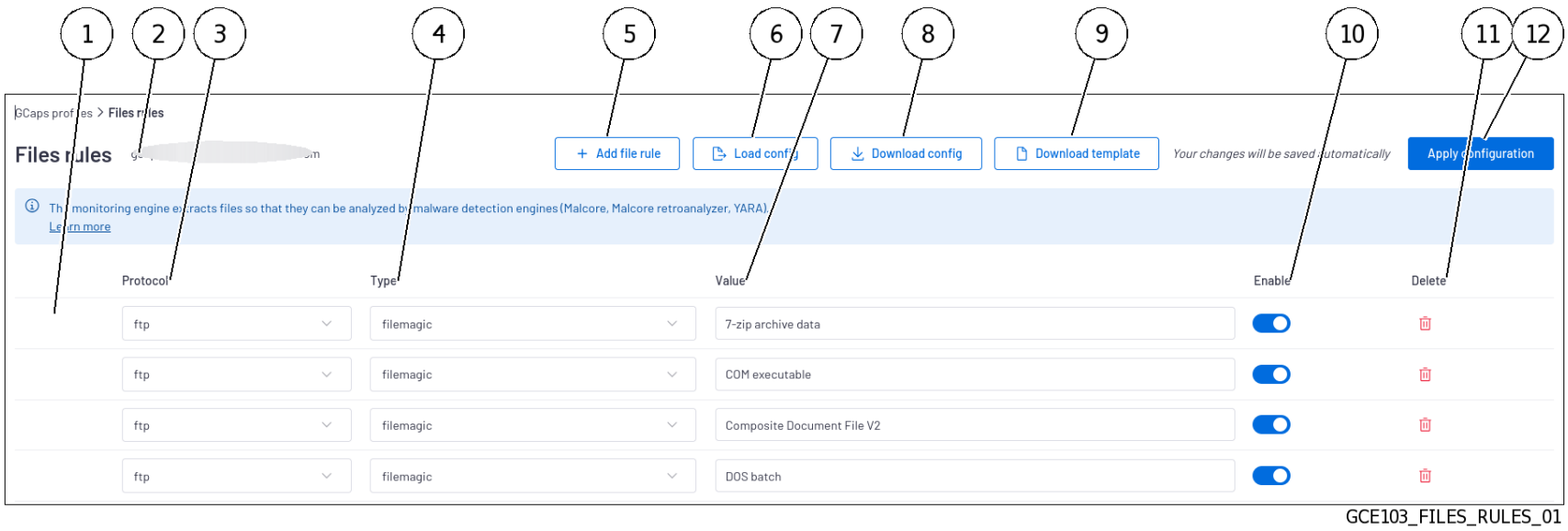
This procedure can be used to load the configuration from one GCap to another or to save the configuration.



GCE103_FILES_RULES_01

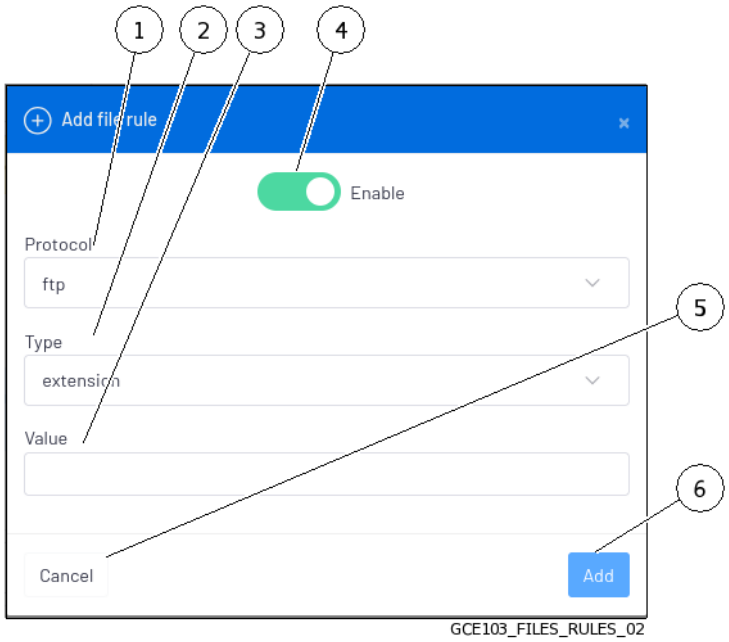
- Click on the `Load config` (7) button and select the configuration file corresponding to this GCap.
- Click on the `Apply configuration` button (12).

7.4.6.10 Procedure to add a file reconstruction rule



GCE103_FILES_RULES_01

- Click on the `Add file rule` button (5).



In the popup that appears:

- Enable or disable the rule (4)
- Specify the protocol (1) on which the rule will be applied
- Choose the type of reconstruction (2) - by extension or by filemagic
- Enter the value (3) corresponding to the type chosen above
- Click on the `Add` button (6)

- Click on the `Apply configuration` button (12).

7.4.7 Configuring filters on targeted parts of the analyzed traffic via the GCap profile

7.4.7.1 Introduction

The `Packet filters` section enables filters to be set on targeted parts of the traffic being analyzed so they are not processed.

To	go to the
Add a filter	1- *Procedure to open the `GCaps profiles` window* 2- *Procedure to set up the filter*
Change of native VLAN	1- *Procedure to open the `GCaps profiles` window* 2- *Procedure to configure the VLAN*

7.4.7.2 Links associated

The rulesets and the GCap profiles are presented in *Sigflow engine*.
To manage the rules, see the *Configuring the Sigflow engine* menu.

The graphical integration is described in the *`Packet filters` section of the `Gcaps profiles` screen*.

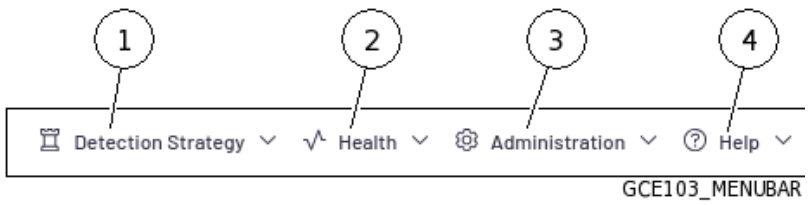
7.4.7.3 Prerequisites

User: member of **Operator** group

7.4.7.4 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

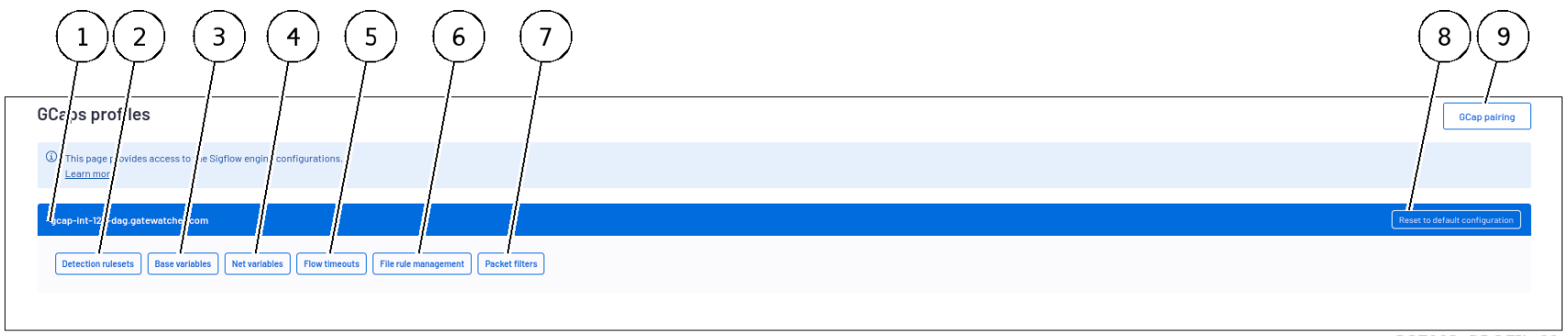
7.4.7.5 Procedure to open the `GCaps profiles` window



GCE103_MENUBAR

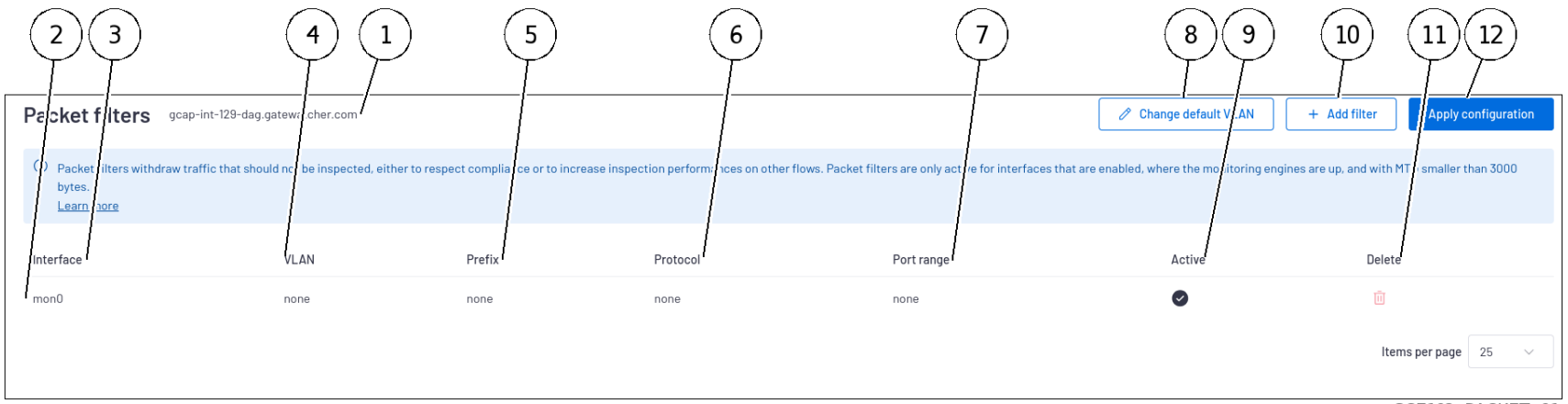
- From the navigation bar, click successively on:
- The `Detection strategy` button (1)
- The `GCaps profiles` button of the `Sigflow engine` category
  The `GCaps profiles` window is displayed.

7.4.7.6 Procedure to set up the filter



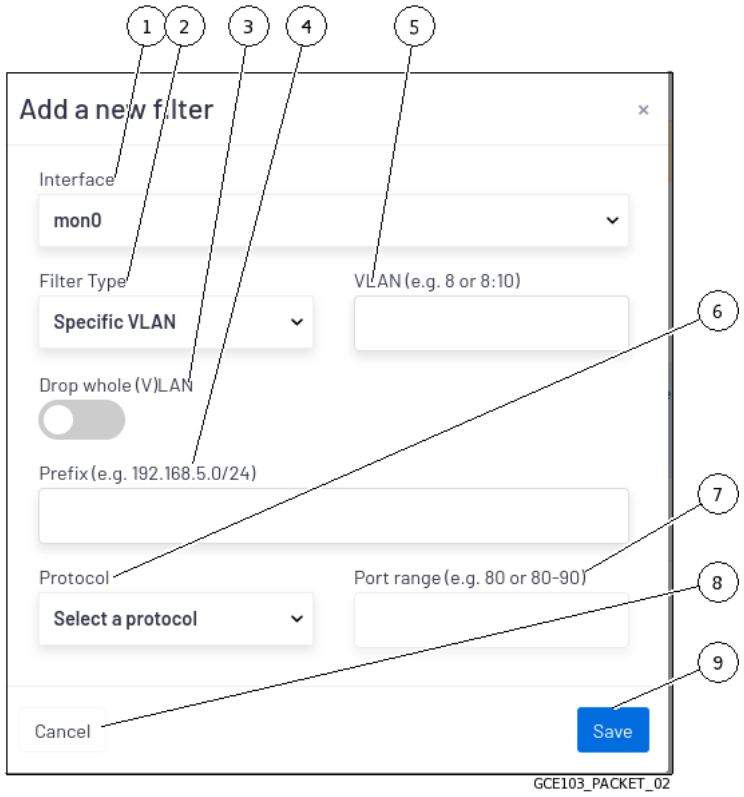
GCE103_PROFIL-01

- Click on the `Packet filters` button (7).



GCE103_PACKET_01

- Click on the `Add filter` button (10).



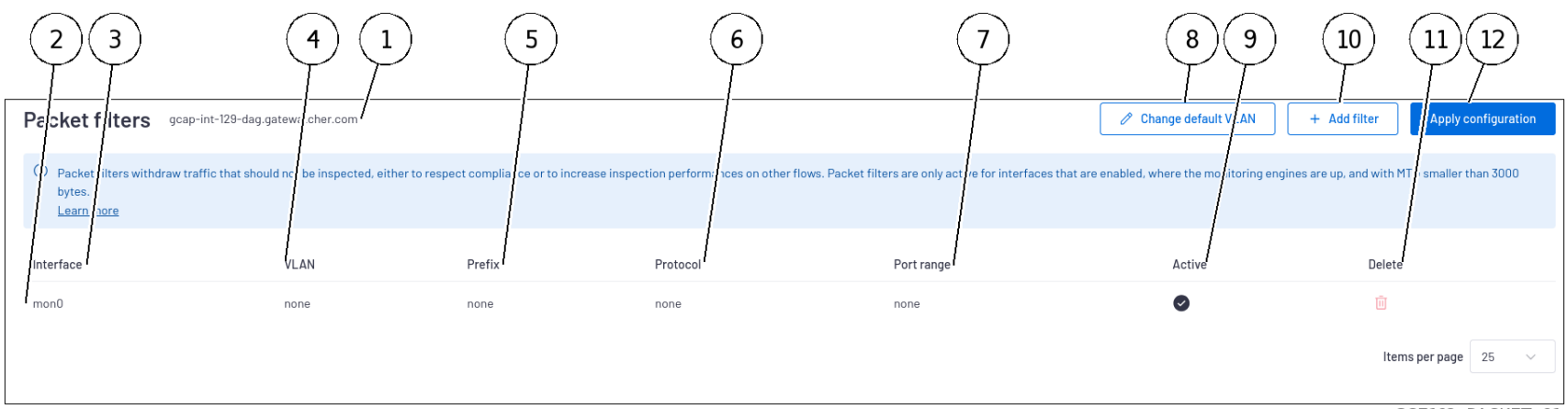
In the popup that appears:

- Choose the desired interface (1): it must be enabled
- In the `Filter Type` field (2), choose between `Specific VLAN` and `Default VLAN & untagged traffic`.
- In the `VLAN` field (5), enter the value of the desired VLAN.
  If the "Filter Type" field is set to `default VLAN & untagged traffic` the box is not editable.
- In the `Drop whole LAN` field (3), choose whether the filter applies to the whole vlan (enable) or a part of the vlan (disable).
- In the `Prefix` field (4), enter the network to apply the filter to.
  If the `Drop whole LAN` field is enabled, this box is not editable.
- In the `Protocol` field (6), enter the protocol to apply the filter to.
  If the `Drop whole LAN` field is enabled, this box is not editable.
- In the `Port range` field (7), choose the port or port range to apply the filter to.
  If the `Drop whole LAN` field is enabled, this box is not editable.
- Click on the `Save` button (9).
- Click on the `Apply configuration` button (12).

Note:

When `Drop whole LAN` (3) is enabled:
- If the `Filter Type` field is set to `Specific VLAN`, all traffic associated with this VLAN will drop
- If the `Filter Type` field is set to `default VLAN & untagged traffic`, all VLAN traffic associated with default and all traffic that is not part of any VLAN will be dropped

7.4.7.7 Procedure to configure the VLAN



- Click on the `Change default VLAN` button (8).
  In the popup that appears:
- Choose the desired interface: it must be enabled
- Enter the desired value in the `Default VLAN` field

- Click on the `Save` button
- Click on the `Apply configuration` button (12).

7.5 Analyzing the engine alerts

7.5.1 Analyzing the Malcore alerts

7.5.1.1 Introduction

For information, see the following paragraphs:

- *For what types of threats is this engine designed?*
- *How does this particular engine detect threats?*
- *How does Malcore engine work in the GCenter?*

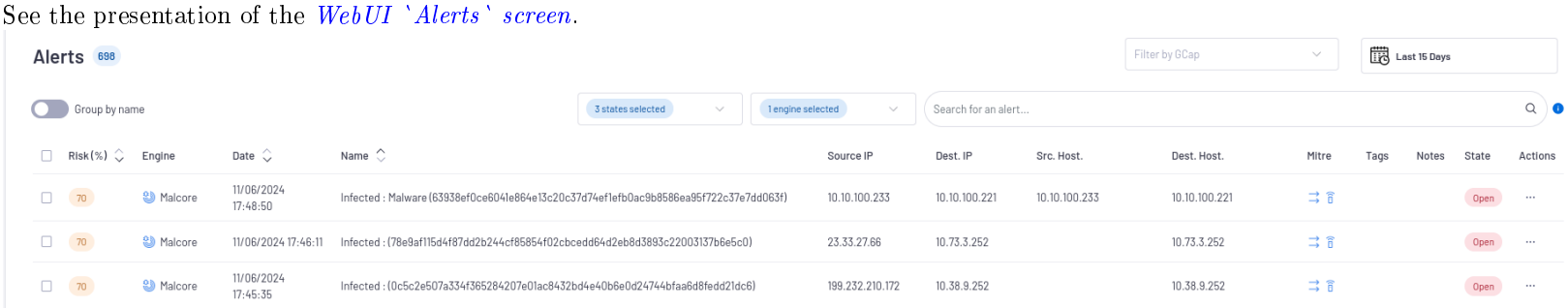
7.5.1.1.1 Management of the Malcore engine

For engine informations, see the paragraph see the *Viewing the engine status*
For information on update engine, see the paragraph *Engine update*
For information on engine configuration, see the paragraph *Malcore configuration and management of the ignored list feature*

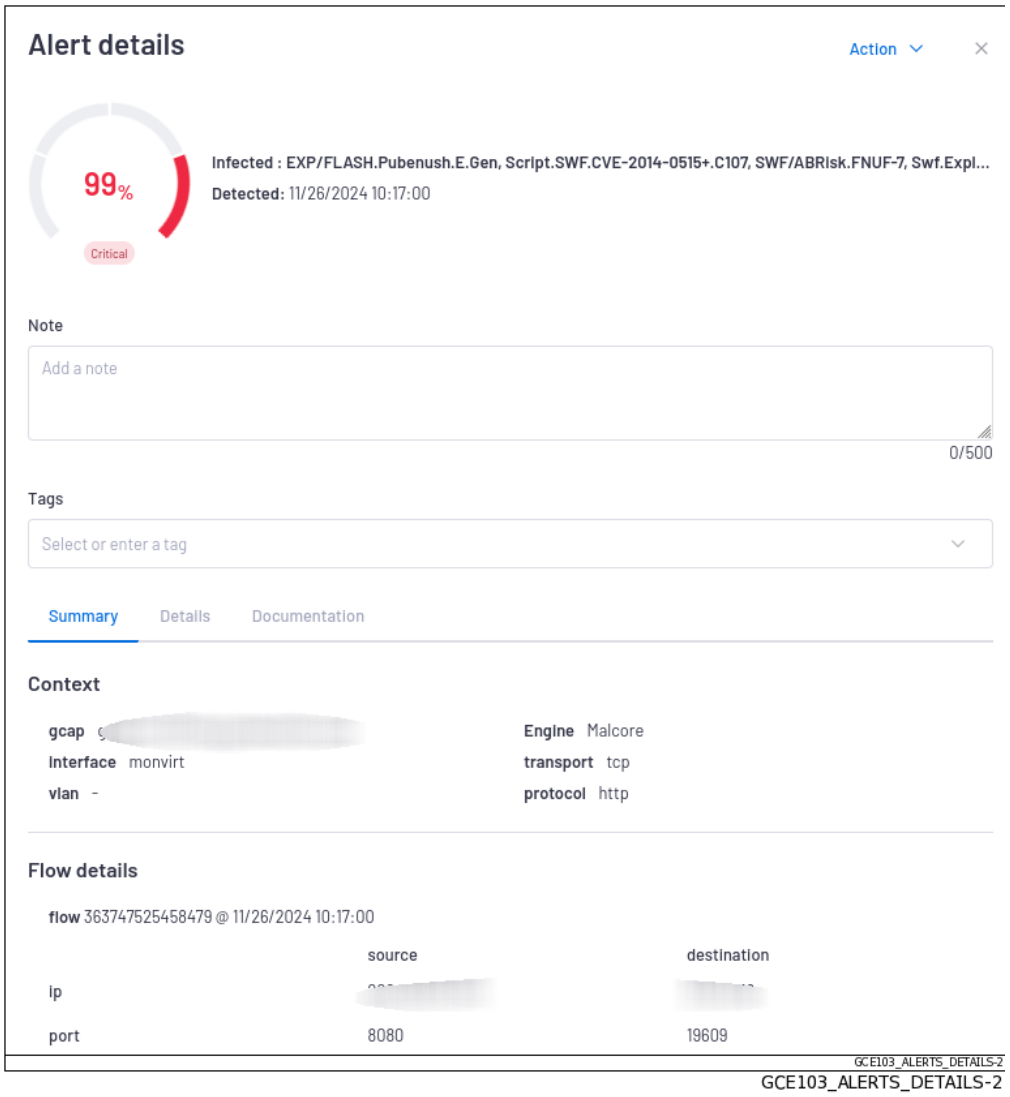
7.5.1.1.2 Events generated by the engine

Events generated by the Malcore engine are **alerts**.
Events generated by the Yara engine are included with the Malcore **alerts**.
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen:
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
- To view the alerts, select the `Malcore` engine filter.
  See the presentation of the *WebUI `Alerts` screen*.



- Click on the selected alert.
  The `Alert details` window is displayed.



GCE103_ALERTS_DETAILS-2

The following counters are displayed and give information on the alert category:

- `total found:`
- `threat:`

- If the `total found:` is 0/16 and the `threat:` is Yara Rule Matched then the alert category is **yara**
  Example of a Yara alert:

```
Malcore summary
state: Yara Rule Matched
total found: 0/16
file description: Adobe Portable Document Format
threat: Yara Rule Matched
```

  In this case, see the procedure *Analyzing the Yara alerts*.

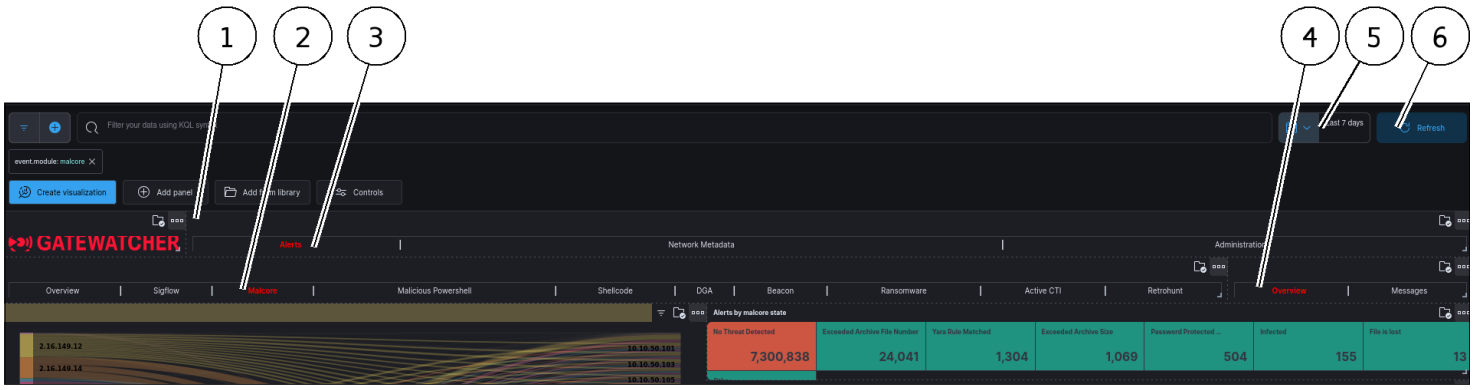
- If the `total found:` is different to 0/16 then the alert category is **malcore**
  Example of a Malcore alert:

```
Malcore summary
state: Infected
total found: 1/16
file description
threat
Infected: pdf/malicious_confidence_100
```

  The detailed information of this alert is displayed in *Example of a Malcore alert in the WebUI*.
  The displayed counters are given in the *Engine log data structure* appendix.

  In this case, the `total found` counter is different to 0/10, i.e at least one Malcore engine result is not CLEAN
- If the `Group by name` mode is activated, the name of the aggregated alerts and their number are displayed.
  Click on a grouping of alerts to display the list.
- When the `Group by name` mode is disabled, different Source and Destination information is displayed for each alert.
  `Tags` and `Notes` are also visible and editable.
  The various Quick Access `Actions` are available for each alert.

- In the **Kibana UI** interface
  - To view only the Malcore alerts without the Yara alerts:
    See the presentation of the *WebUI `Alerts` screen*.
    - Click on the `Hunting` icon of the `WebUI`.

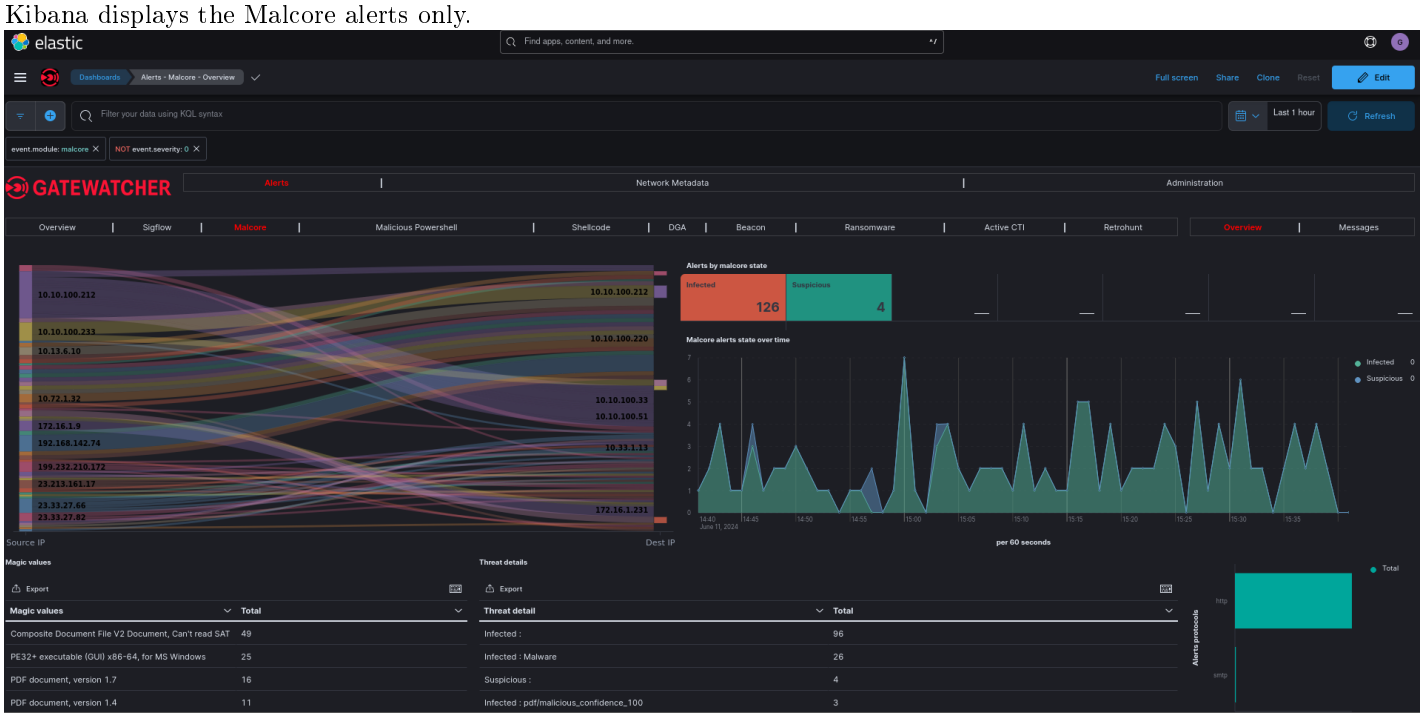


GCE103_MALCORE_ALERT_10

The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

- Click on the `Malcore` tab (2) of the `Alerts` category (3).
- Select the `Overview` tab (4).
- Select the time range (5) to display data.
- To filter the Malcore alerts without the Yara alerts on Kibana, enter the following command `event.module : "malcore" and NOT malcore.state : "Yara Rule Matched"` in the search field (1).
- Validate wih the `Refresh` button (6).

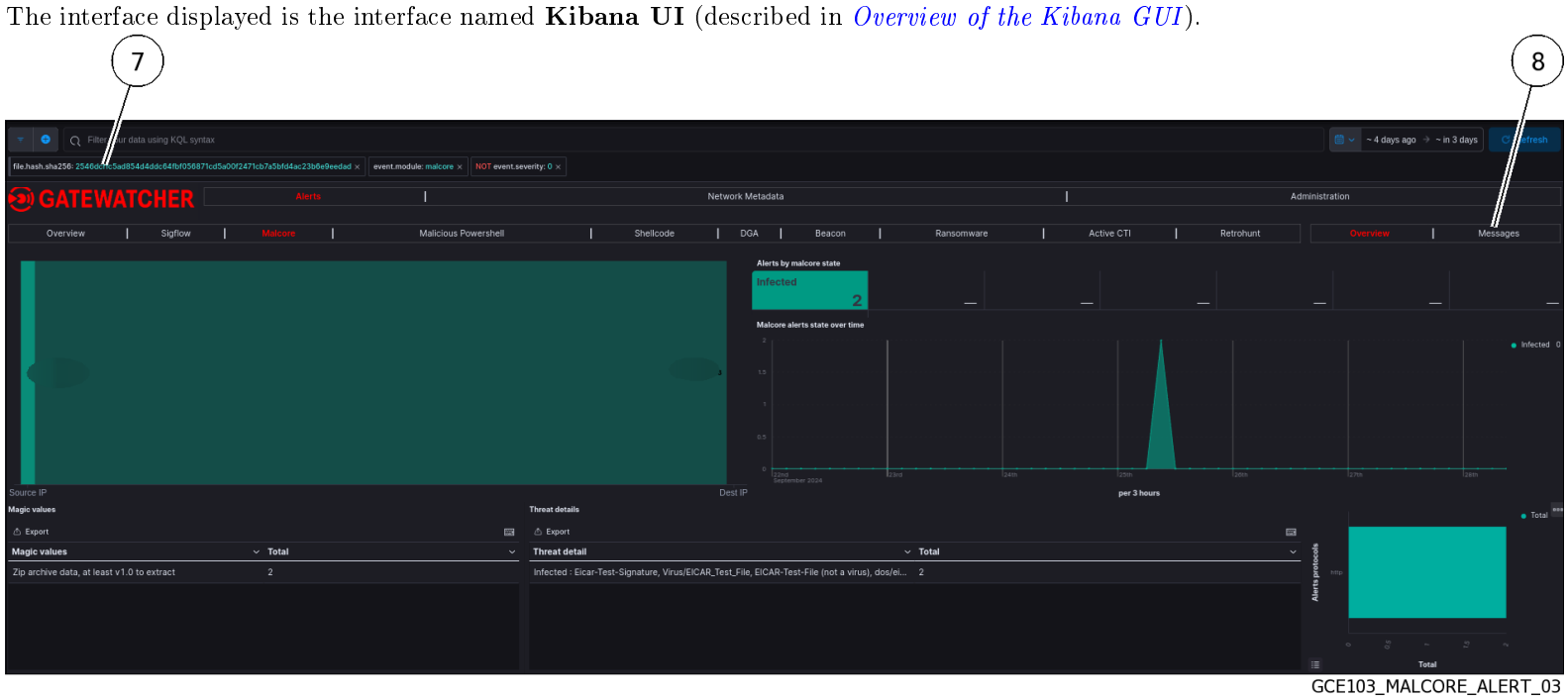
  Kibana displays the Malcore alerts only.



- To consult information about a specific alert:
- On the main interface **WebUI**, after clicking on an alert, click on the `Open malcore file transaction` command of the `Actions` menu.

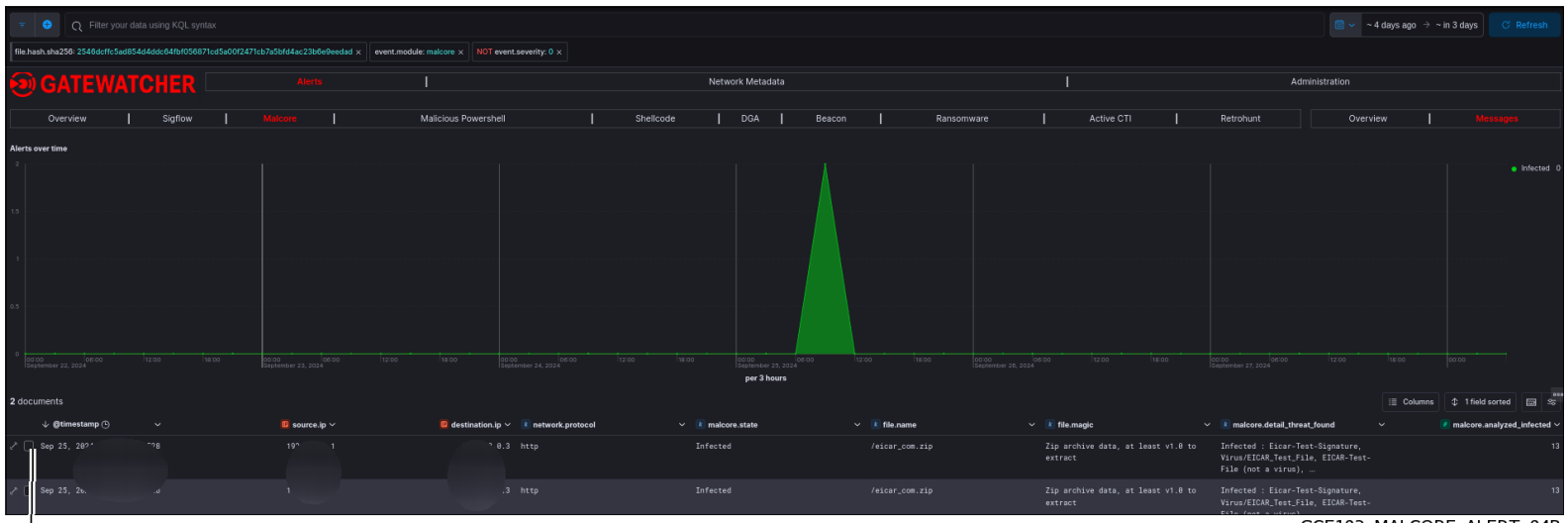
  Kibana is opened on the `Malcore` tab of the `Alerts ` section: in the `Overview` tab, the database is filtered on the `file.hash.sha256` parameter (7).

  The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).



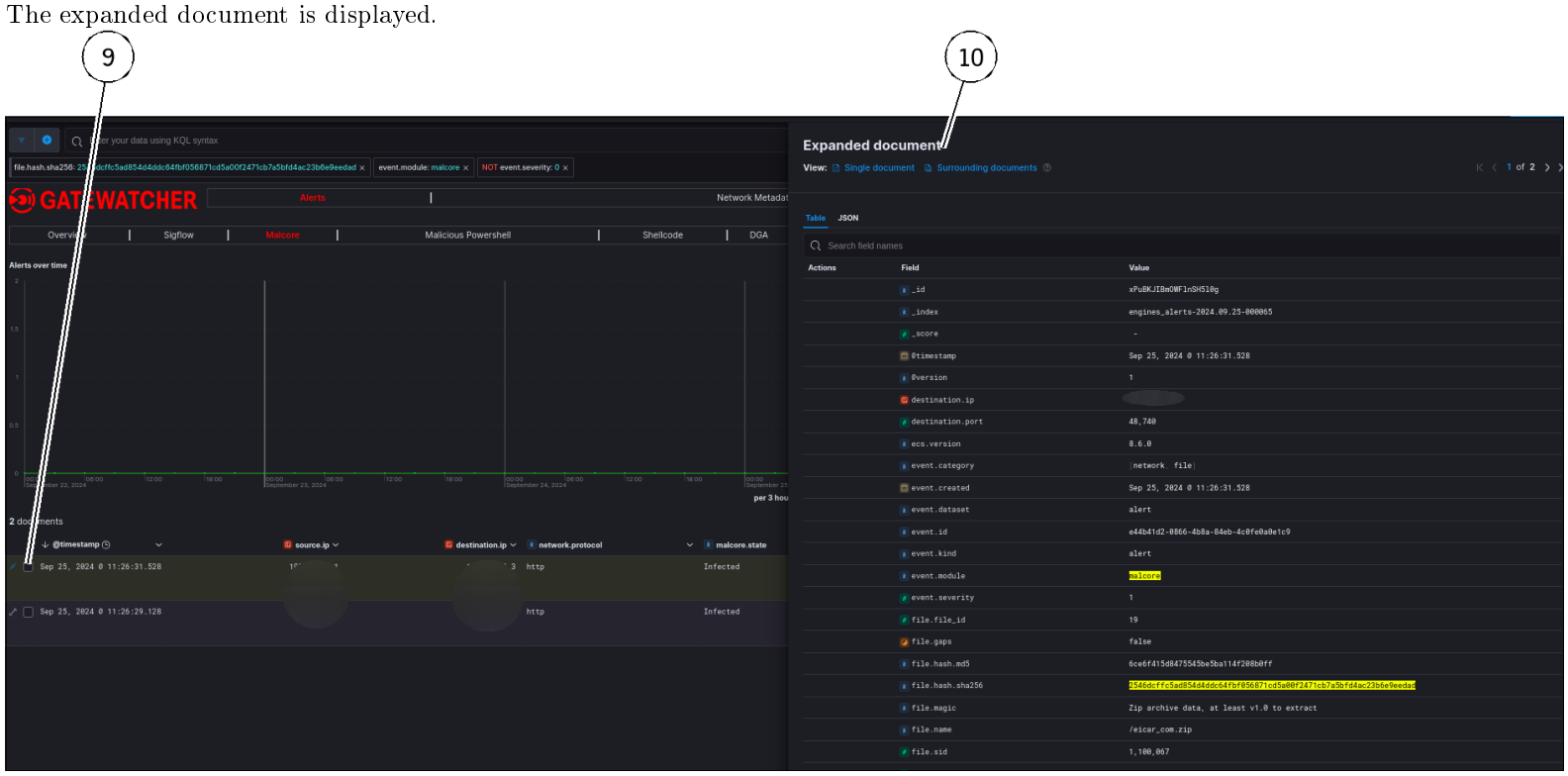
GCE103_MALCORE_ALERT_03

- Click on the `Messages` tab (8).



GCE103_MALCORE_ALERT_04B

- Click on the toggle icon on the left of the Alert (9).
  The expanded document is displayed.



GCE103_MALCORE_ALERT_05B

The detailed information of this alert can be viewed in table or json format (see the *Malcore log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

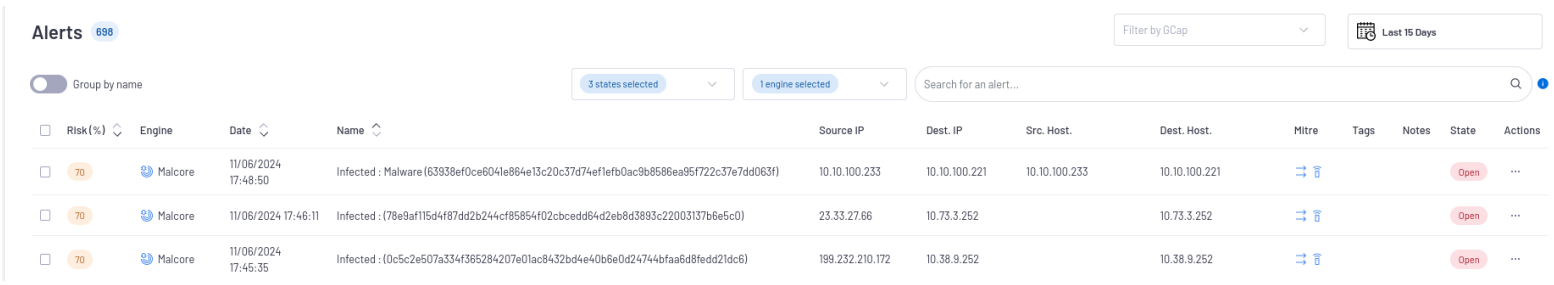
Note:

The **Kibana UI** can also be accessed without any filters via the `Hunting` icon on the left side menu bar in the WebUI.

7.5.1.1.3 Essential information to understand the context of the alert

7.5.1.1.3.1 What are the key fields of an alert and their meaning?

Before undertaking any investigation or qualification of the alert, it is essential to start by observing several elements that will provide essential information to understand the context of the alert.
These elements can be found either in the **WebUI** interface or in the **Kibana UI** interface (for more information, refer to the previous paragraph).



In the information displayed on the WebUI `Alerts` screen, these key elements include:

- `Engine:`
  The alerts related to the Malcore engine include the term `Malcore` for the `Engine` field.
- `Date:`
  The date when the Malcore engine rose an alert in the local timezone.
  The UTC date is accessible in the alert detail under *.event.created*
- `Name:`
  At the beginning of this field is indicated the result of the Malcore scan.
  It can be set to INFECTED or SUSPICIOUS.
  Its result is changed to "Infected" when a single engine qualifies the file as infected.
  Next to it, the name of the threat is indicated.
- `Source IP` and `Dest.IP`
  The IP addresses associated with the alert, whether source or destination, provide information about the network communication involved in the incident.
- `Src. Host.` and `Dest.Host.`
  The source and destination hosts associated with the alert provide information about the systems involved in the network communication of the incident.

More information is available on the **Alert Details** screen after clicking on an alert in the `Alerts` screen of the **WebUI**.

- Click on the `Details` tab (3).

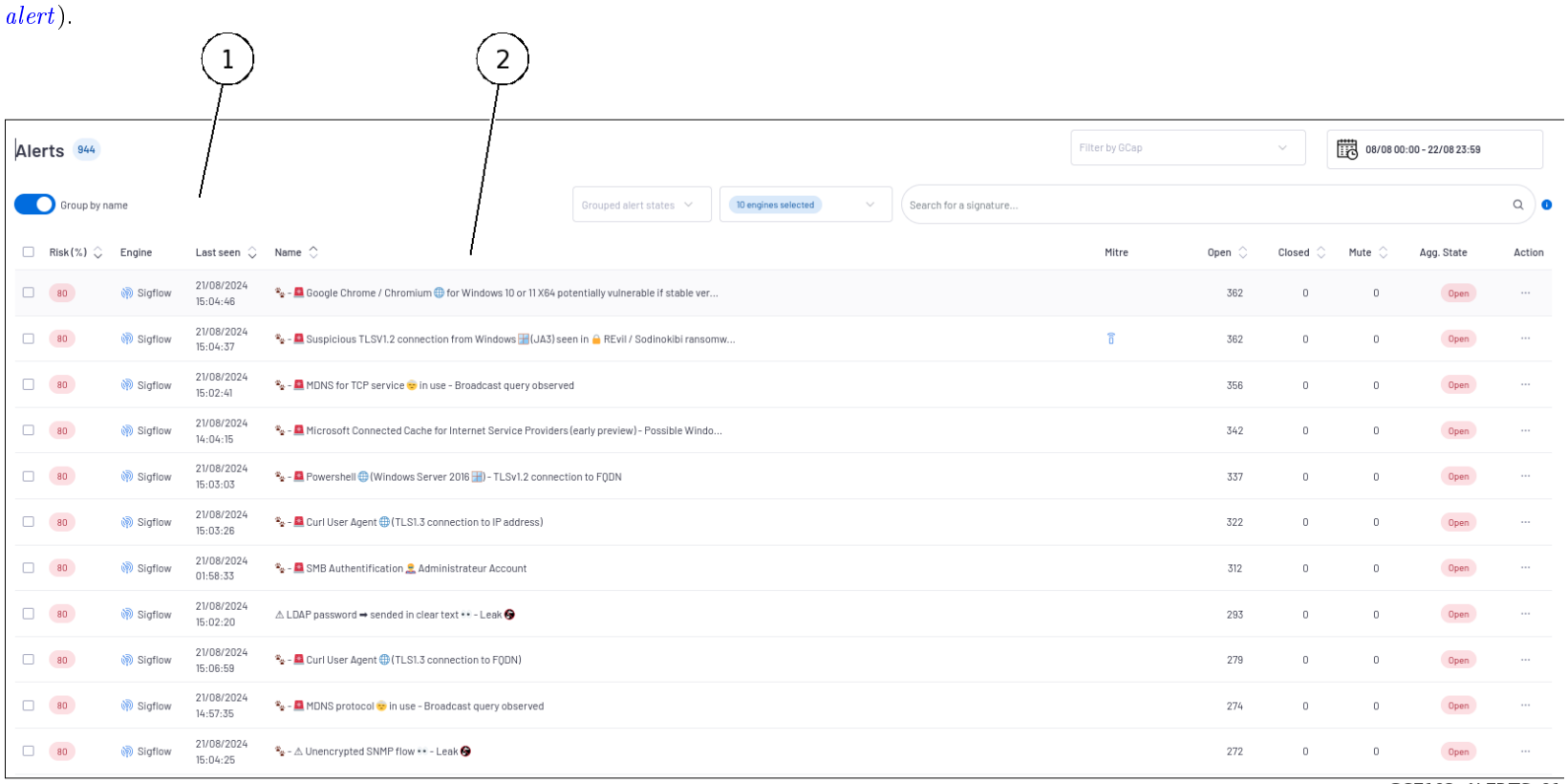
- `analyzed_clean`, `analyzed_infected`, `analyzed_suspicious`, `analyzed_error`, `analyzed_other`
  These fields present a summary of the sample analysis' result.
  The number associated is the number of engine with this verdict (Eg. `analyzed_clean: 13` means that 13 engines found this sample to be clean/not malicious).
- `analyzers_up`
  This field is the number of engine available at the moment of the scan.
  It helps to understand the results of the above fields.
- `engines_last_update_date`
  This date indicates the latest update of Malcore engines.
  It is important to understand the relevance of the signatures used for detection.
- `detail_threat_found`
  This section lists the names of threats detected by Malcore.
  Threat names are usually separated by commas, allowing for quick identification of the malicious elements involved.
  For example: "Infected: Trojan.GenericKD.70868911 (B), Trojan/Win.Generic, Ransom.Stop.P5".
- `protocol`
  This field indicates the protocol through which the file was observed on the network.
  This information can help identify how the file was delivered or offer a way to gather more protocol-specific information.
- `magic details`
  This is the file format detected by Malcore.
  The file format is not detected based on filename or extension but rather by the content of the file.
  This information can help to understand the nature of the malicious file in question, in particular the platforms that are targeted and it sometimes allow to reveal the real nature of a file.
  For example: "PE32 executable (GUI) Intel 80386, for MS Windows".
  In this example, "PE32 executable" indicates that it is an executable file in Portable Executable format, commonly used for Windows programs.
- `total found`
  This field indicates the number of Malcore antivirus engines that detected the file as infected or suspicious, divided by the total number of engines.
  For example: "13/16" means that 13 of the 16 engines identified the file as a threat.
- `file.name`
  This field indicates original filename used during the delivery.
- `file.hash.md5` and `file.hash.sha256`
  These fields indicate the checksum respectively in MD5 and SHA256 of the sample.
  This checksum is a unique value representing the content of a file.

7.5.1.2 Alert handling procedure

7.5.1.2.1 How do you verify the accuracy of an alert and determine if it represents a real threat?

To assess the accuracy of an alert and determine whether it represents a real threat, several steps can be taken.
Here is an overview of the actions frequently taken when analyzing an alert generated by the Malcore engine:

- Click on the alert to be analyzed in the **Alert details** window (for more information, see the *Procedure to retrieve information related to an alert*).



GCE103_ALERTS_01

- Click on the `Open malcore file transaction` command of the `Actions` menu.
  The command enables the viewing in Kibana the number of times a file has been analyzed by Malcore using its unique fingerprint in SHA-256 format.
  The interface `Kibana:` is opened in the `Overview` section of the `Malcore` tab.
  This feature is especially useful for tracking the activity of a specific file within your environment.
  The database is filtered by the parameter `fileinfo.sha256:`.
  Below is an illustrative example of the request made in Kibana:

```
fileinfo.sha256:"d17d874a4a3c6b2b4f20afbaea7a3609b988adc20d0400390a555e43a934fb88"
```

  This view provides a summary view of various information essential for the future, such as:

  - The name of the file concerned
  - The protocol on which the file was observed
  - As well as the number of antivirus engines that qualified the file as infected

  This view can be useful to gather information about this sample.
  For exemple:

  - Multiple occurrence of this sample always around the same time with the same source may indicate a backup
  - A checksum displayed on different assets at different time may indicate a propagation of the threat
- Click on the `Download Malware` command of the `Actions` menu.
  The `Download Malware` command enables to download the compressed file locally to the user's workstation.
  The file is **zipped for security**, to avoid inadvertently executing the file.
  The archive name matches the **UUID _file.zip** (file UUID).
  Below is an illustrative example of a downloaded file name:

```
526cfdd1-b13c-4917-a8c0-e2b52250970b_file.zip
```

  This feature is particularly useful:

  - When the threat is proven and there is a desire to better understand their behavior and clarify their capabilities
  - Later in the further processing of the incident, for further investigation, for example through reverse engineering

7.5.1.2.2 How to categorize the threat based on the information collected?

To categorize the threat, explore several avenues:

- **Check the number of antivirus**:
  - Examine how many antivirus engines built into Malcore qualify the file as malicious.
    If multiple engines indicate that the file is malicious, it increases the probability that the threat is real.
- **Verify the original IP address**:
  - If the alert is linked to an external IP address, review the reputation level of that address.
    An IP address with a bad reputation is more likely to be associated with malicious activity.
  - Note also that just because it is an internal IP address does not make it a false positive.
- **Check the file hash**:
  - To assess the nature of the file, consult sources of Threat Intelligence (CTI) such as LIS or other external platforms such as VirusTotal (VT).
    Hashing the file through these resources helps determine whether the file is known to be malicious or has been previously identified by security analysts.
- **Analyze the file name**:
  - Carefully review the file name.
  - Check if it matches legitimate file names known to be used by common operating systems or software.
    Some legitimate files may trigger alerts due to file names similar to known malware.
    If the file name matches a legitimate file, it may indicate a potential false positive.
  - However, do not rely solely on the file name and consider other threat indicators for a more accurate assessment.
- **Assess the consistency with assets**:
  - Carefully examine the coherence between the detected threat and the assets in the environment.
    For example, if the alert concerns a malicious PE file, but the affected server is a Linux system, this could indicate an inconsistency.
- **View the alert history**:
  - Consult the history of similar alerts generated by Malcore.
    If similar alerts have been confirmed as real threats in the past, it increases the likelihood that the current alert is also a threat.
    Depending on the observations, the threat can be categorized as real or not.
  - if necessary, use the *File transactions* functionality presented in the previous paragraph to obtain the majority of this information via a condensed view.

7.5.1.2.3 What answers are needed if the threat is confirmed?

Note:

This procedure enables to deepen the investigation and assess the extent of the incident after confirmation of a threat generated by the Malcore engine.

- **Isolate the system**: immediately isolate the contaminated system and ensure it cannot cause further damage
- **Notify**: inform relevant parties of threat detection
- **Dynamic analysis**: if possible, run the file in a secure environment (sandbox) to observe its behavior (a GBox for example)
- **Collect information**: gather essential information such as file hash, file name, source and location
- **Neutralize the threat** by deleting the file, blocking the original IP address, etc
- **Reverse engineering (if necessary)**: if the threat is particularly complex, reverse engineering can be considered to understand in depth its internal functioning
  This can help identify exploited vulnerabilities and propagation mechanisms
  The feature `` `Download Malware` ``, presented previously, enables to recover the file for analysis
- **Analyze logs**: review system and network logs to trace the spread of the threat

---

7.5.1.2.4 What if an alert from this engine is identified as a false positive?

If an alert from this engine is identified as a recurring false positive, it is recommended to add the file to the whitelist (see the *Managing the Ignore list of the Malcore engine*).

7.5.2 Analyzing the Shellcode detect alerts

7.5.2.1 Introduction

For information, see the following paragraphs:

- *For what types of threats is this engine designed?*
- *How does this particular engine detect threats?*
- *How does Shellcode Detect engine work in the GCenter?*

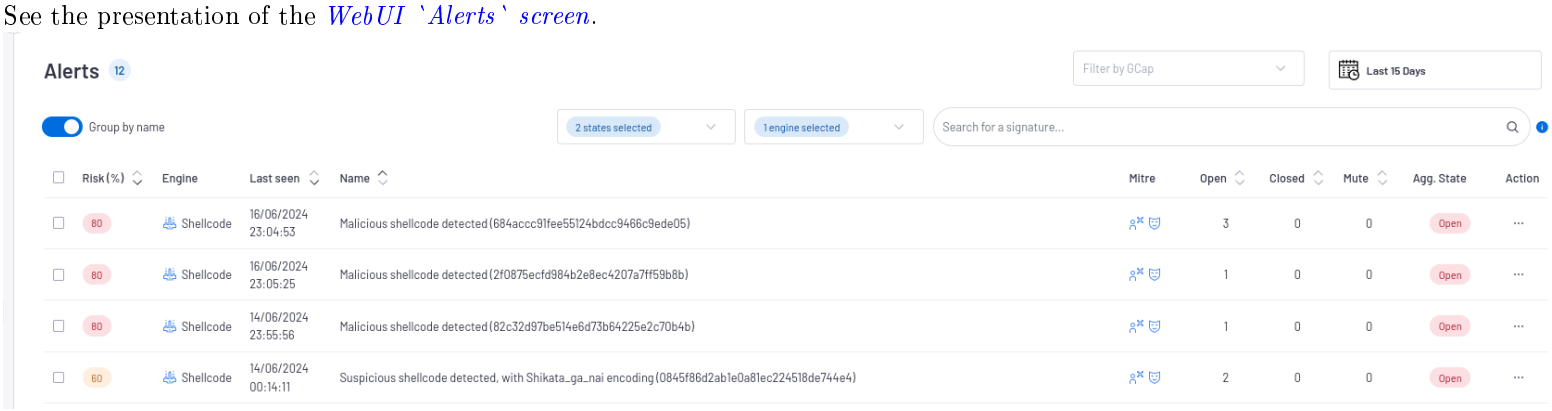
7.5.2.1.1 Management of the Shellcode detect engine

For engine informations, see the paragraph *Viewing the engine status*
For information on engine upgrade, see the paragraph *Engine update*
For information on engine configuration, see the paragraph *Engine configuration*.

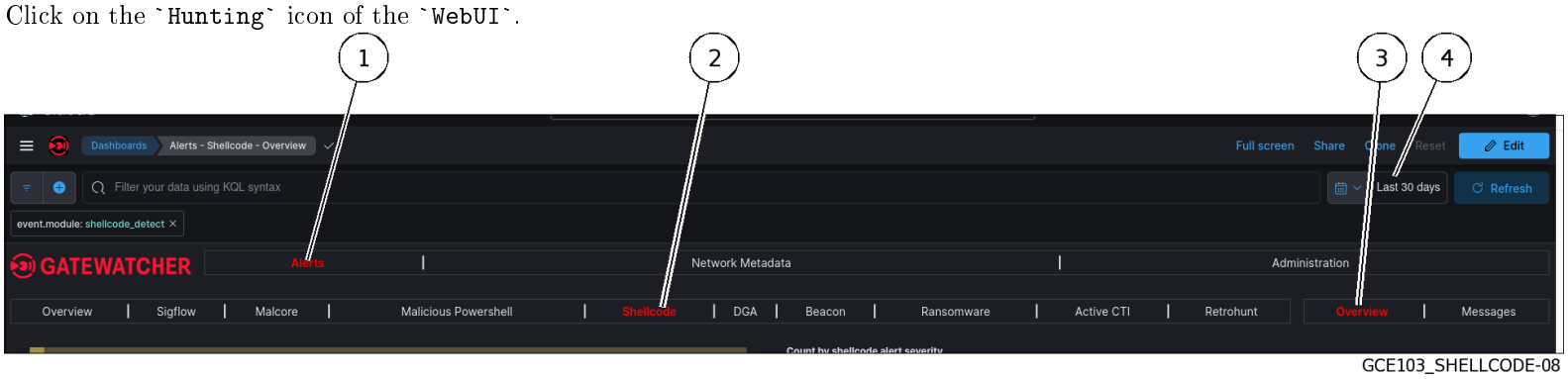
7.5.2.1.2 Events generated by the engine

Events generated by the Shellcode detect engine are **alerts** only.
These are displayed:

- In the main interface named **WebUI** on the GCenter in the `Alerts` screen
  The main interface named **WebUI** is described in the *Overview of the WEB UI*.
  - To display only these alerts, select the `Shellcode` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.



  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed in *Example of a Shellcode alert in the WebUI*.
    The displayed counters are given in the *Engine log data structure* appendix.
- In the interface named **Kibana UI**
  - Click on the `Hunting` icon of the `WebUI`.

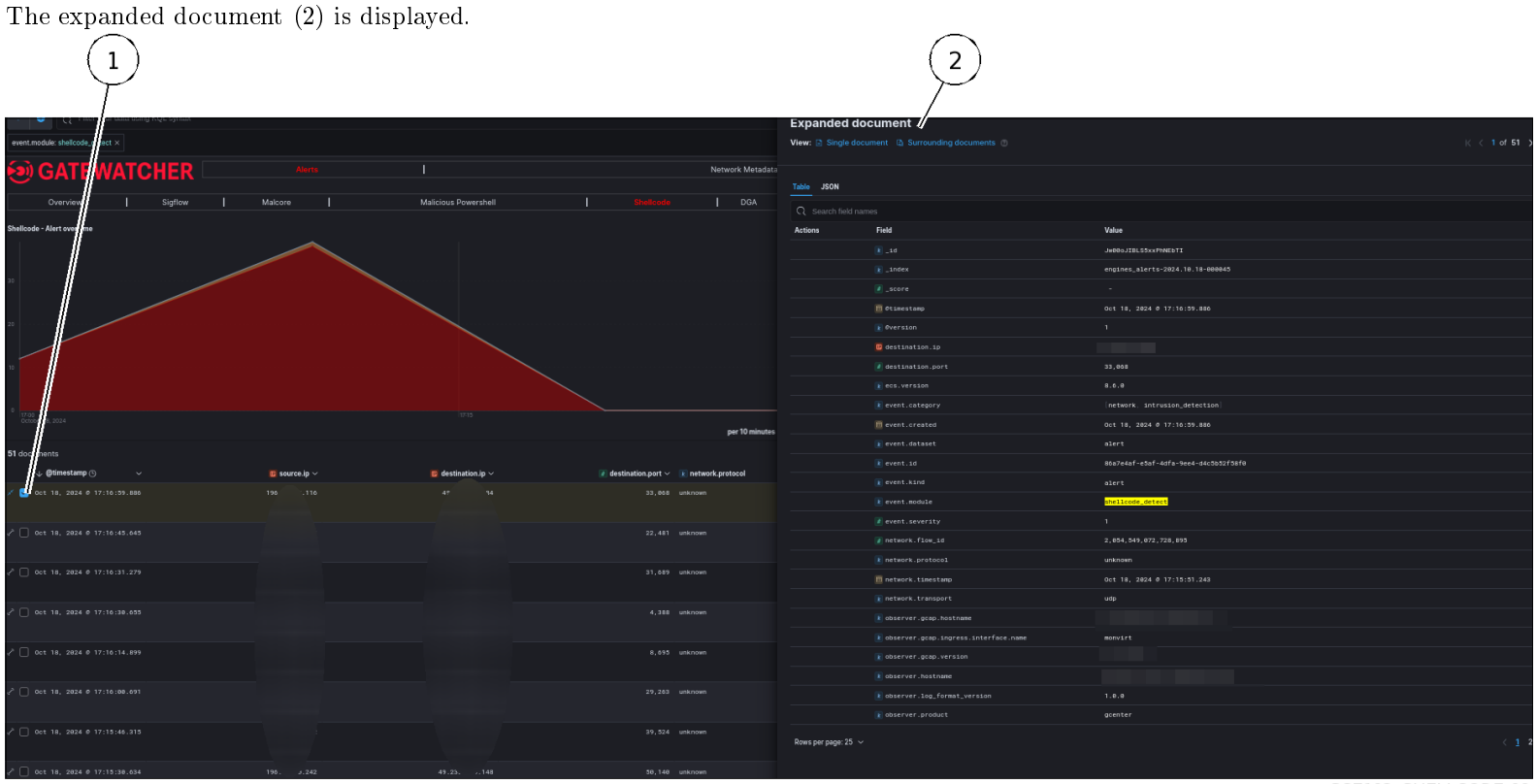


GCE103_SHELLCODE-08

    The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

    - Click on the `Shellcode` tab (2) of the `Alerts` category (1).
    - Select the `Overview` tab (3).
    - Select the time range (4) to display data.
      It is then possible to filter on certain values for, for example:
      - Do not display healthy machines (filter false positives)
      - Show only alerts from a particular IP
      - Do not display alerts from a specific GCap
- To consult information about a specific alert:
  - Click on the toggle icon (1) on the left of the Alert.

The expanded document (2) is displayed.



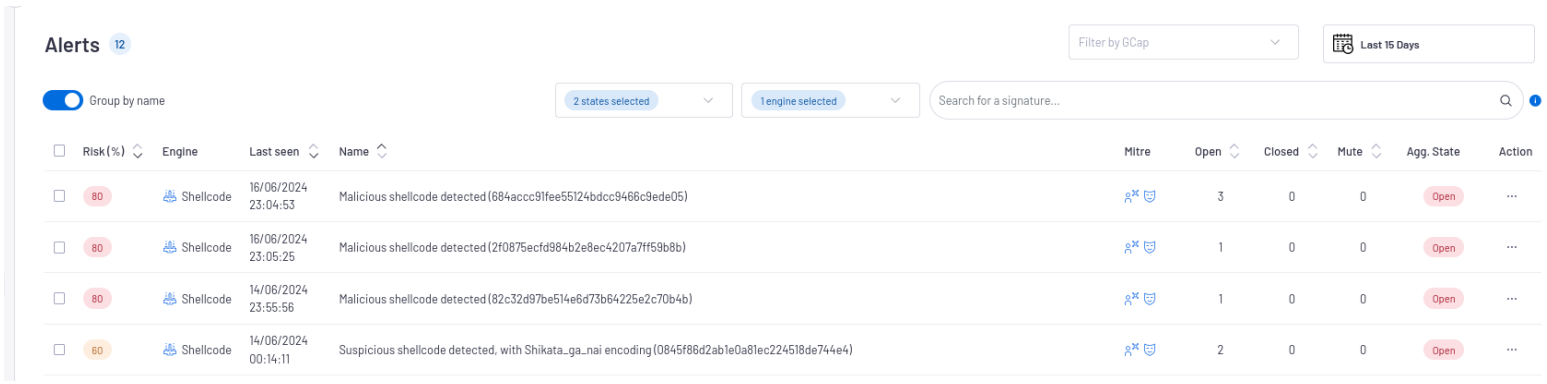
GCE103_SHELLCODE-09

The detailed information of this alert can be viewed in table or json format (see the *Shellcode log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

7.5.2.1.3 Essential information to understand the context of the alert

7.5.2.1.3.1 What are the key fields of an alert and their meaning?

Before undertaking any investigation or qualification of the alert, it is essential to start by observing several elements that will provide essential information to understand the context.
These elements can be found either in the **WebUI** interface or in the **Kibana UI** interface.



The following are the main fields that will appear in the `Alerts` view of the `WebUI` when **Aggregated** is disabled:

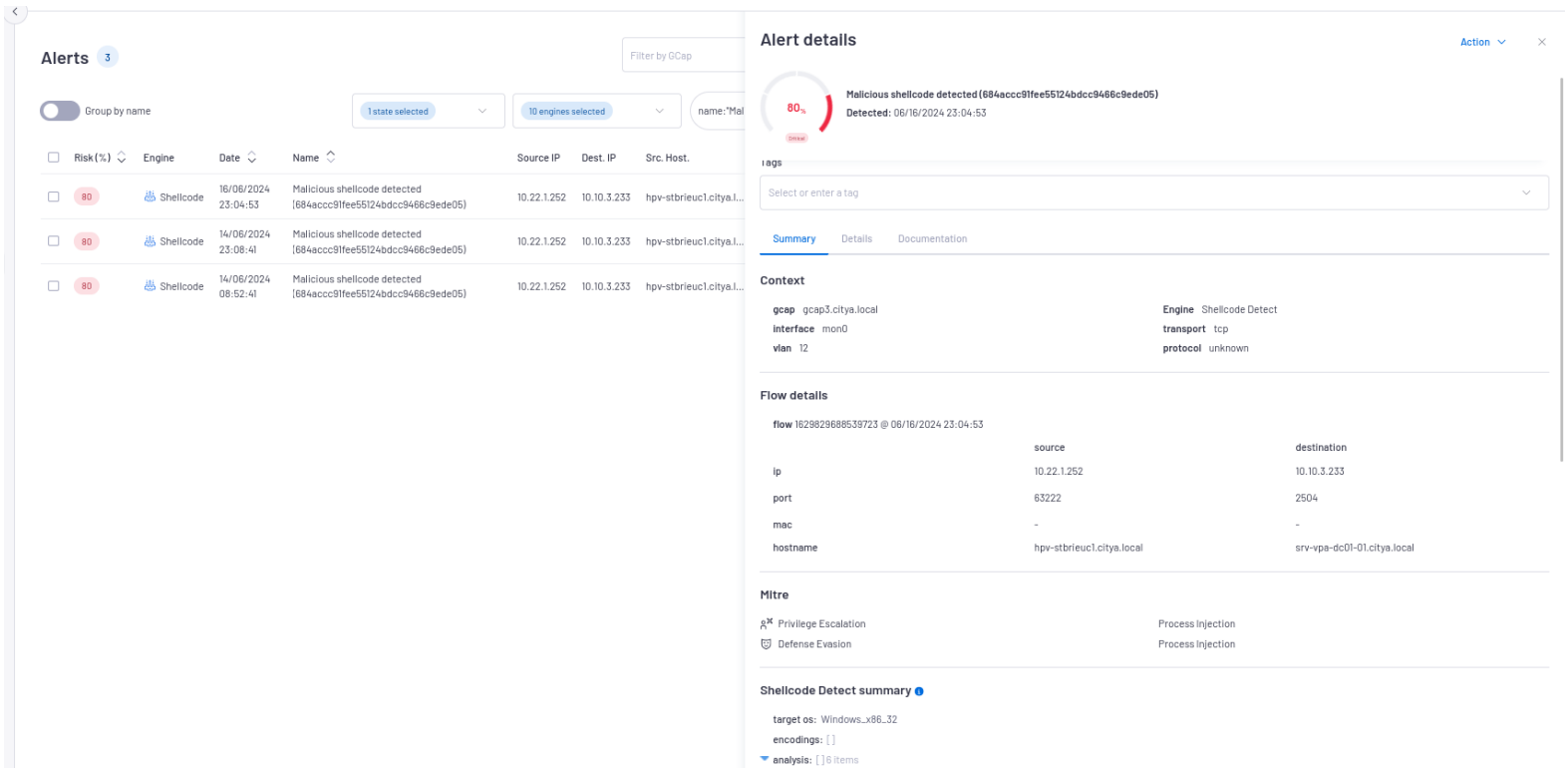
- `Risk`
  The risk score of the alert, it depends on the success of the analysis of the **Shellcode**.
  If the analysis fails but an encoding has been identified, the alert is raised with a lower *risk*.
- `Date:` (**event.created**)
  The date and time the alert was raised by the engine.
- `Name:`
  This is the threat description based on the analysis. It consists of:
  - The alert severity:

    If the risk is 80% then the alert is indicated as `Malicious`
    If the risk is 60% then the alert is indicated as `Suspicious`
  - From engine name: `shellcode_detected` (**event.module**)
  - The encoder name (**shellcode.encodings[0][name]**)
  - An identifier based on the details of the analysis (**shellcode.id**)
- `Source IP` and `Dest. IP` (**source.ip** and **destination.ip**)

The source and destination IP address associated with the alert generated

- `Src. Host.` and `Dest. Host.`
  When the information is available, it is the name of the machines linked to the IP associated with the alert.

More information is available in the `Alert Details` panel by clicking on an alert:



- In the `Shellcode detect summary` section of the `Summary` tab:
  - **target os**
    The target Operating system of the shellcode
  - **Encodings** (**shellcode.encodings**)
    The list of identified encodings
  - **call** (**shellcode.analysis**)
    List of system functions called by the **Shellcode** during analysis
- Click on the `Details` tab (3).
  - `event.severity`
    The threat score of the alert, it depends on the success of the analysis of the **Shellcode** and is generally worth `1` (the maximum).
    If the analysis fails but an encoding has been identified, the alert is raised with a *severity* to `2`.
    This is regularly the case when detecting an antiviral DB stream.
  - `network.timestamp`
    The date and time the file was extracted by the GCap.
  - `shellcode.sub_type`
    Corresponding to the target OS listed above
  - `shellcode.id`
    An identifier based on the analysis details, to group similar alerts.
  - `shellcode.sample_id`
    The unique identifier of the analyzed *sample*, composed of the extraction date, a random number, and the GCap name.

7.5.2.2 Alert handling procedure

7.5.2.2.1 How do you verify the accuracy of an alert and determine if it represents a real threat?

In some cases, a **Shellcode** alert may not be a real threat.
To evaluate it, several actions can be carried out:

- Check the sample content: Antiviral DB
  The first step is to inspect the contents of the extracted *sample*.
  The *shellcode_ detect* engine frequently categorizes as malicious flows of antivirus database updates, or similar, passing unencrypted over the network.
  These feeds contain signatures that can trigger an alert, but they also contain the names of these signatures.
  It is therefore generally easy to identify them:
  1. On the WebUI interface, open a **Shellcode** alert.
  2. Click on the `Show Hexdump` command of the `Action` menu.
  3. Search into the right column for keywords similar to signature names.
  4. If enough (3-4) different keywords are identified, it is certainly an antiviral database.

  These signature names can be truncated depending on the type of stream being extracted.

It is possible to find the related threat by carrying out a search on the Internet, or on the Microsoft site:
https://www.microsoft.com/en-us/wdsi/threats
Examples:

- *Pshdlexec* ("TrojanDownloader:X97M/Pshdlexec")
- *!##.. 32/Hikiti.GIC ("Backdoor:Win32/Hikiti")*
- *...64/Meterpreter. R("Trojan:Win64/Meterpreter")*
- *Y2V:Costin_Raiu_Kaspersky_Lab/loki2crypto*

- Check flow type: Backup
  A **Shellcode** may be detected in a virtual machine backup stream.
  This means that there is a **Shellcode** on the machine disk.
  This is an alert that is less urgent to investigate, and that will depend on the use of this machine.
  For example, a cybersecurity expert could keep such files on his machine.

  To know if it is a backup flow, we can:

  - Compare ports (`source.port`, `destination.port`) with your virtualization tool documentation
  - Check if the IP matches a storage server
  - Check if many similar flows occur at the same time
  - Contact the infrastructure staff

7.5.2.2.2 How to categorize the threat based on the information collected?

- Check the target machine.
  The *shellcode_detect* engine is able to identify Windows and Linux shellcodes.
  Thus, when an alert is raised, the information is present in the Target OS (shellcode.sub_type) field.
  It is then possible to check if the target machine matches the architecture of the detected **Shellcode**.
  If so, it is likely that the machine has been infected.
  If this is not the case, it can be an intermediate machine, or an automatic attack that did not identify the machine system.
- Check the analysis results.
  It happens under certain conditions that the sample is truncated, which prevents the analysis from succeeding.
  In this case, a **Shellcode** alert is raised if an encoding has been detected (`shellcode.encodings`).
  However, there will be no system function detected (`shellcode.analysis`).
  Generally, we get this kind of results when matching on antiviral database update streams.
  Otherwise, it will be necessary to treat this alert as a real threat and carry out the necessary investigations.

  In most cases, the analysis will be at least partially complete.
  It is then possible to look at the list of detected system functions and their arguments (`shellcode.analysis`).
  Generally, the names will be explicit enough to qualify the urgency of the threat.
  - Example of high threat (irrelevant information have been removed):
    Windows backdoor: opens port 28876 and gives command prompt access
    ws2_32_bind('name': '0.0.0.0:28876')
    ws2_32_listen()
    ws2_32_accept() -> 24
    kernel32_CreateProcessA('lpCommandLine': 'cmd', lpStartupInfo': '[hStdOutput: 24, hStdInput: 24, hStdError: 24])
  - Example of low threat (irrelevant information have been removed):
    Windows : execute *calc.exe* ; probably harmless
    kernel32_WinExec('lpCmdLine': 'calc.exe')
- Correlate with other engines.
  It is interesting to check the presence of alerts from other engines from information identified by **shellcode_detect**.

1. Note some information that may be present in other alerts.
   For example:
   - IP Source
   - IP Destination
   - If a file has been uploaded: its name and url
   - If a port has been opened: its value
   - If an IP was contacted: IP and port
2. In the `Alerts` menu of the WebUI, select all engines except Shellcode detect and filter on the collected information.
3. This investigation can also be conducted in Kibana UI.

7.5.2.2.3 What answers are needed if the threat is confirmed?

- **Isolate the system**: immediately isolate the contaminated system and ensure it cannot cause further damage
- **Notify**: inform relevant parties of threat detection
- **Collect information**: gather essential information such as IP addresses and domain name
- **Analyze logs**: review system and network logs to trace the spread of the threat

---

7.5.2.2.4 What if an alert from this engine is identified as a false positive?

There is no whitelist for the Shellcode detect engine.
It is possible to add a tag "False positive" and a note indicating the reason.
It is not recommended to use the action "Mute all similar alerts" since it will not take into account the source and destination IPs.

7.5.3 Analyzing the Malicious Powershell detect alerts

7.5.3.1 Introduction

For information, see the following paragraphs:

- *For what types of threats is this engine designed?*
- *How does this particular engine detect threats?*
- *How does Malicious Powershell Detect engine work in the GCenter?*

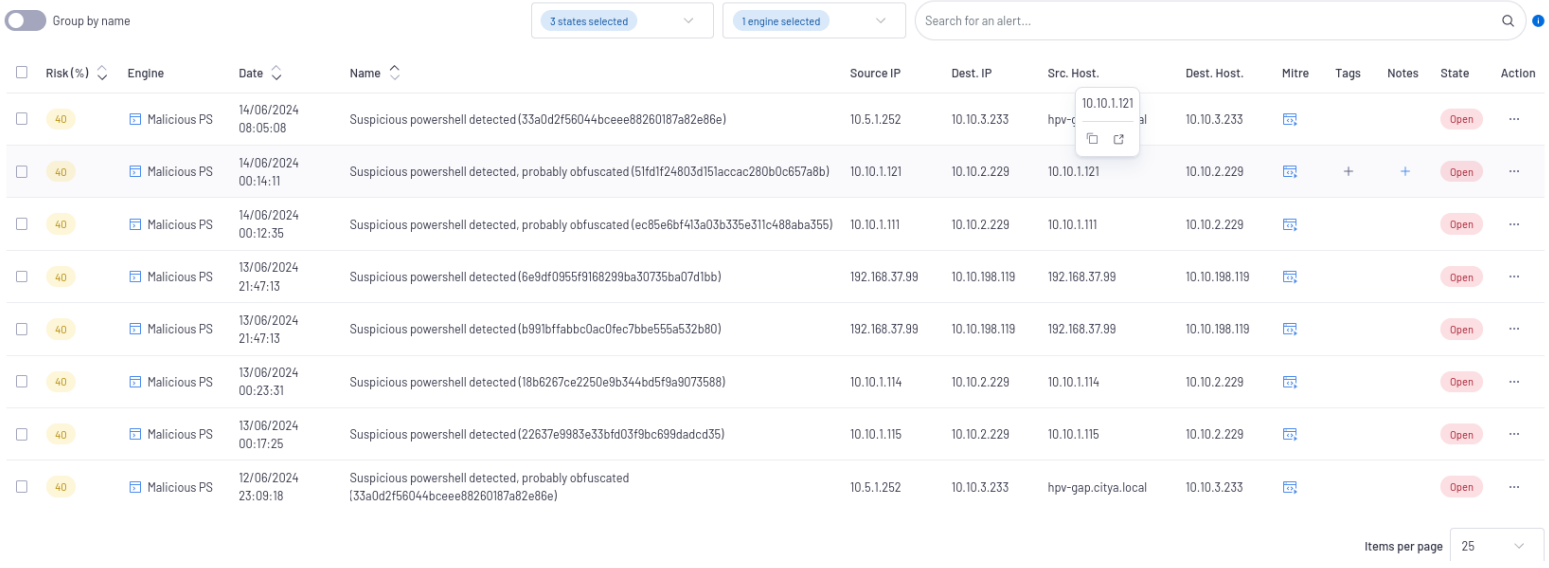
7.5.3.1.1 Management of the Malicious Powershell Detect engine

For engine informations, see the paragraph *Viewing the engine status*.
For information on engine upgrade, see the paragraph *Engine update*.
For information on engine configuration, see the paragraph *Engine configuration*.

7.5.3.1.2 Events generated by the engine

Events generated by the Malicious Powershell Detect engine are **alerts**.
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen:
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
  - To display only these alerts, select the `Malicious Powershell` engine filter then validate.
    See the presentation of the *WebUI `Alerts` screen*.

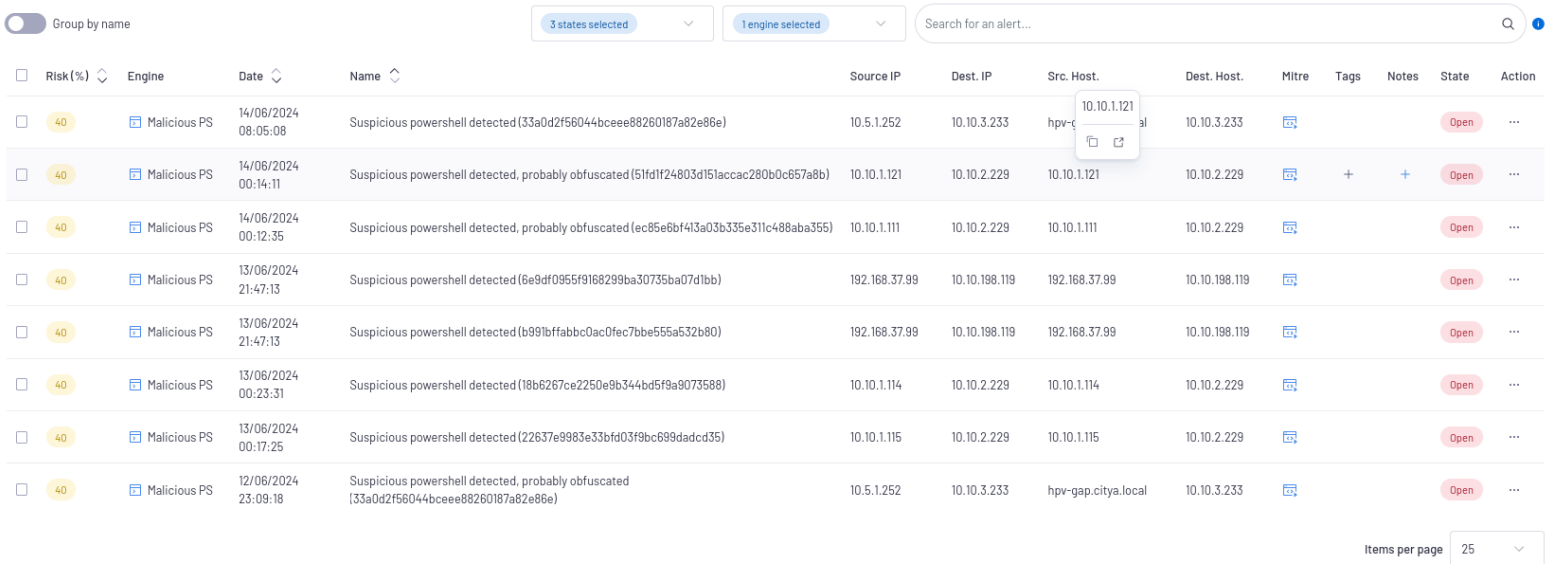


  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed in *Example of a Malicious Powershell detect alert in the WebUI*

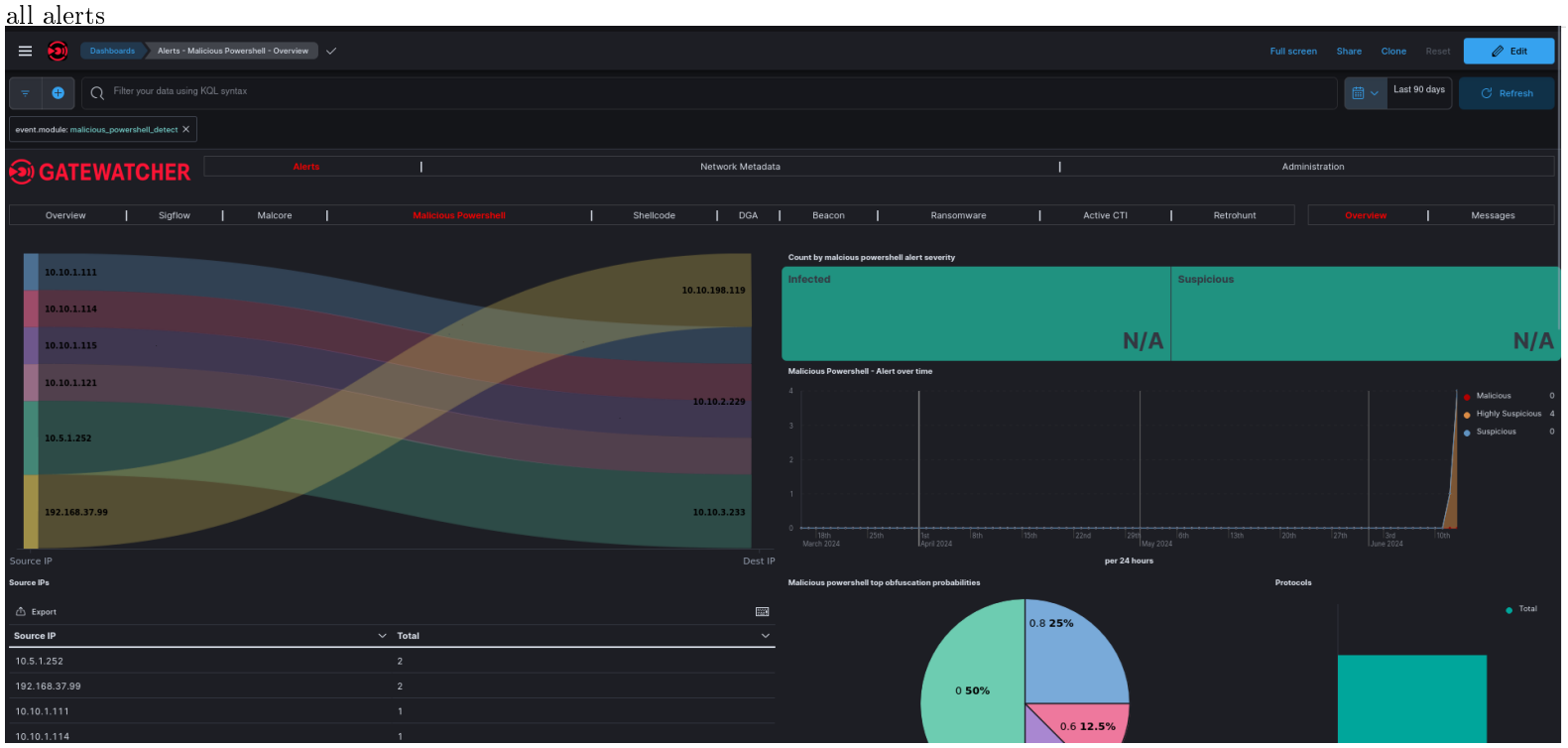
The displayed counters are given in the *Engine log data structure* appendix.

- If the `Group by name` mode is activated, the name of the aggregated alerts and their number are displayed.
  Click on a grouping of alerts to display the list.
- When the `Group by name` mode is disabled, different Source and Destination information is displayed for each alert.
  `Tags` and `Notes` are also visible and editable.
  The various Quick Access `Actions` are available for each alert.

- In the interface named **Kibana UI**:
  - In the `Alerts` screen of the **WebUI**, select the `Malicious Powershell` engine filter then validate.
    See the presentation of the *WebUI `Alerts` screen*.



  - After selecting the alert, click on the `Open powershell engine analytics` command of the `Actions` menu.
    Kibana is opened on the `Malicious Powershell` category of the `Alerts ` section: in the `Overview` tab, the database displays all alerts

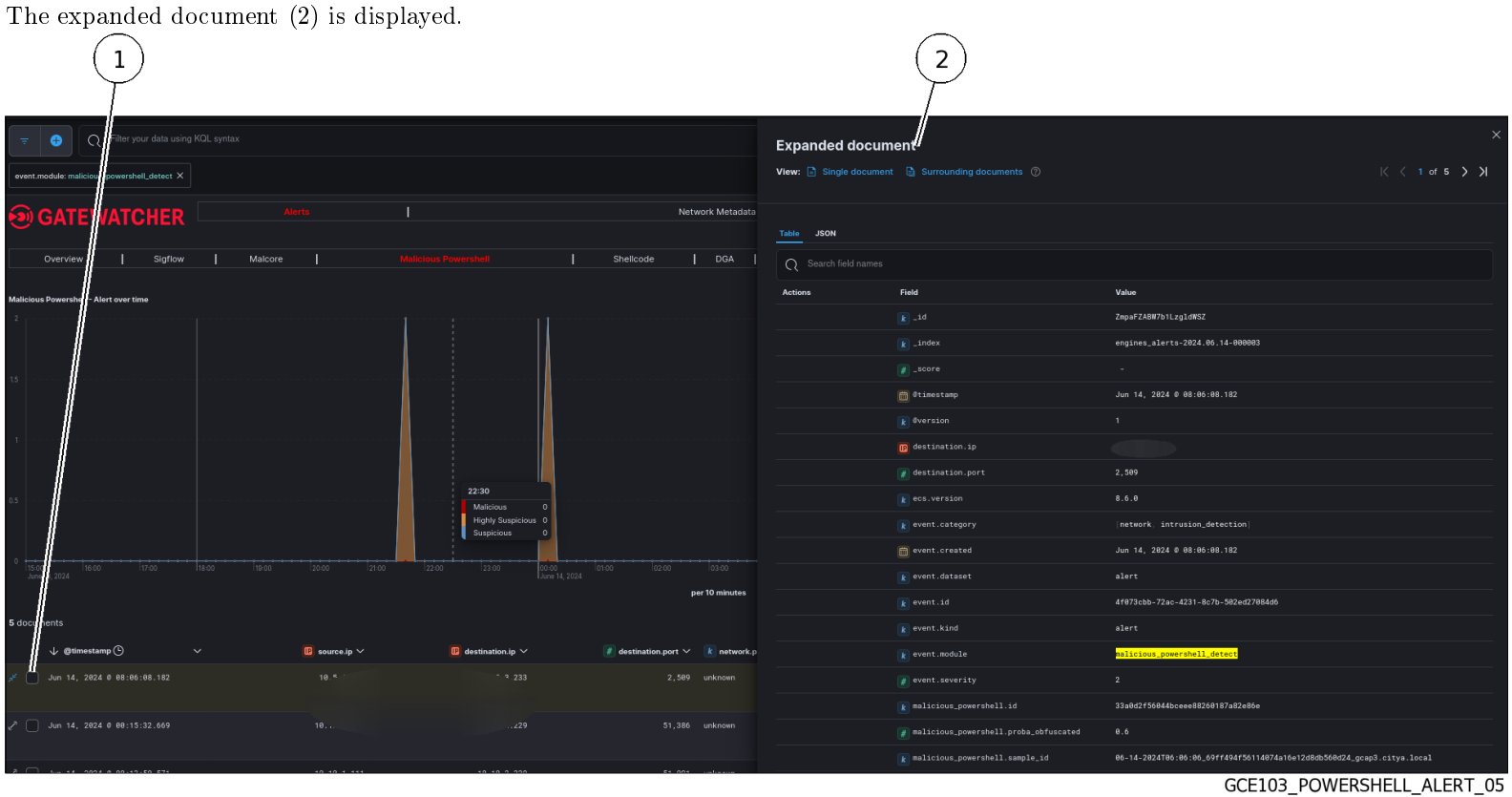


The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

- Click on the `Messages` tab (1).

GCE103_POWERSHELL_ALERT_04

- To consult information about a specific alert:
  - Click on the toggle icon (1) on the left of the Alert.
    The expanded document (2) is displayed.



GCE103_POWERSHELL_ALERT_05

The detailed information of this alert can be viewed in table or json format (see the *Malicious Powershell log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

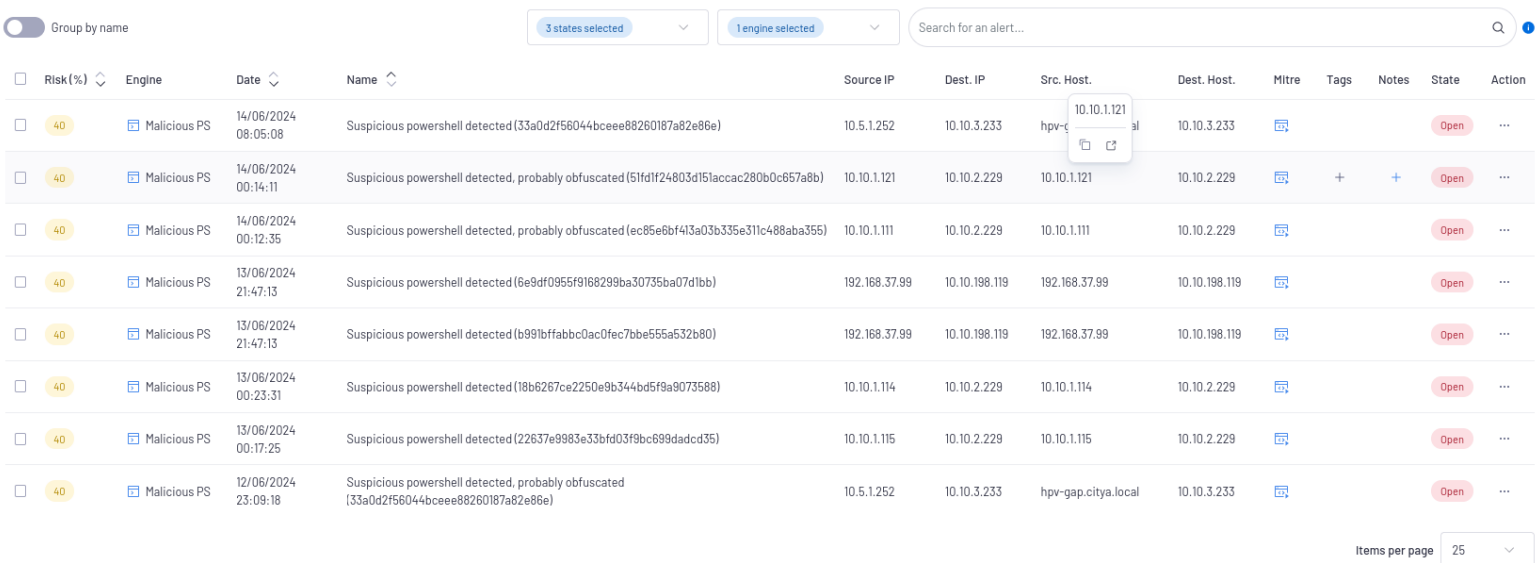
Note:

The **Kibana UI** can also be accessed without any filters via the `Hunting` icon on the left side menu bar in the WebUI.

7.5.3.1.3 Essential information to understand the context of the alert

7.5.3.1.3.1 What are the key fields of an alert and their meaning?

Before undertaking any investigation or qualification of the alert, it is essential to start by observing several elements that will provide essential information to understand the context.
These elements can be found either in the **WebUI** interface or in the **Kibana UI** interface.



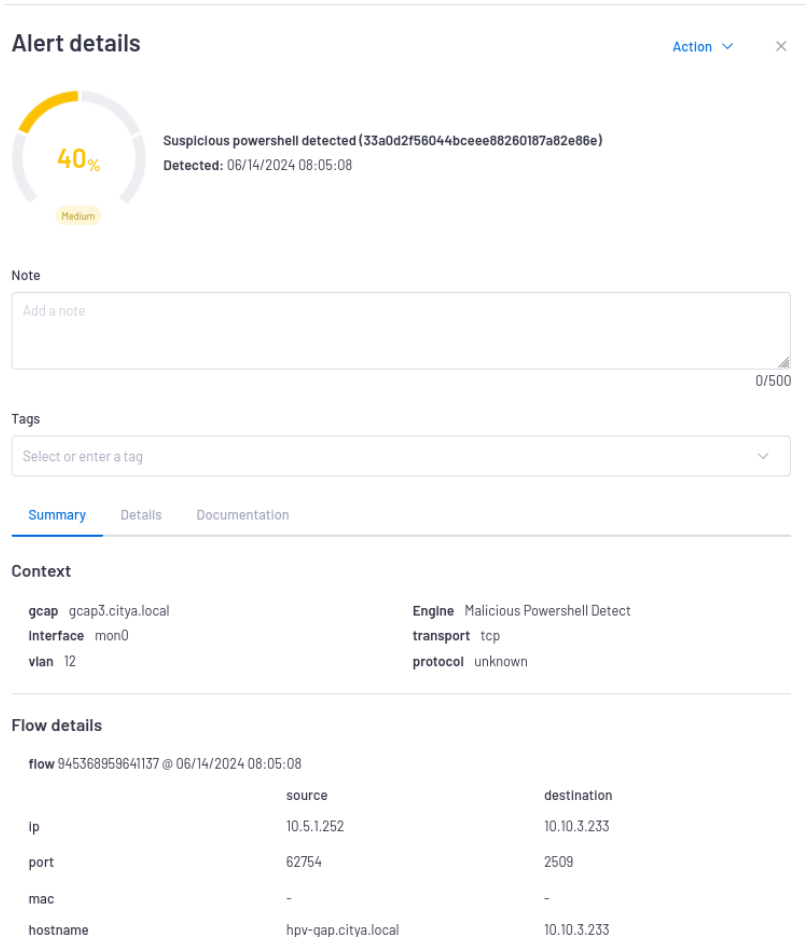
Here are the main fields that will be found in the `Alerts` view of the `WebUI`, when the selector `Group by name` is disabled:

- `Risk`
  The risk score of the alert, it depends on the success of the analysis of the **Shellcode**.
- `Date` (**event.created**)
  The date and time the alert was raised by the engine.
- `Name:`
  This is the threat description based on the analysis. It consists of:
  - Malicious powershell detected, probably obfuscated (60b656e17bec0a97f5638790c78a3124)
  - The alert severity:

    If the risk is 70% then the alert is indicated as `Malicious`

    If the risk is 40% then the alert is indicated as `Suspicious`
  - Engine name: `powershell_detected` (**event.module**)
  - The probability of obfuscation: if the score is superior to 0.75 then the `probably obfuscated` information is displayed
  - An identifier based on the details of the analysis (**malicious_powershell.id**)
- `Source IP` and `Dest. IP` (**source.ip** and **destination.ip**)
  The source and destination IP address associated with the alert.
- `Src. Host.` and `Dest. Host.`
  When the information is available, it is the name of the machines linked to the IP associated with the alert.

More information is available in the `Alert Details` panel by clicking on an alert:



- In the `Malicious Powershell Detect summary` section of the `Summary` tab:
  - Scores - Proba obfuscated (**obfuscation probability:**)
    This is the probability of obfuscation, a score of 1 indicates a high probability of obfuscation that can prevent the detection of suspicious commands.
    The more obfuscated the Powershell script, the more likely it is to be malicious.
  - Scores - Analysis (**score**)
    This is the synthetic score of malice, a score greater than `100` indicates the presence of several techniques considered malicious.
- Click on the `Details` tab (3).
  - Scores - Others (**malicious_powershell.score_details**)
    The score of the different techniques sought during the analysis, used to calculate the analysis score.
  - `event.severity`
    The threat score of the alert, it depends on the values **malicious_powershell.proba_obfuscated** and **malicious_powershell.score**.
    If these values are high enough, this score will have the value `1`, meaning a high probability of malice.
    If these values do not allow to decide on the threat, this score will have the value of `2`.
  - `network.timestamp`
    The date and time the file was extracted by the GCap.
  - `malicious_powershell.id`
    An identifier based on the analysis details, to group similar alerts.
  - `malicious_powershell.sample_id`
    The unique identifier of the analyzed *sample*, composed of the extraction date, a random number, and the GCap name.

7.5.3.2 Alert handling procedure

7.5.3.2.1 How do you verify the accuracy of an alert and determine if it represents a real threat?

In some cases, a **Malicious Powershell** alert may not be a real threat.
To evaluate it, several actions can be taken.

- Check sample content: legitimate tool
  Sometimes legitimate **Powershell** code is confused with malicious code.
  A number of tools are installed using **Powershell** commands as malware might do.

  For example, *chocolatey*, a package manager for windows, installs with the following command.
  iex ((New-Object System.Net.WebClient).DownloadString('https://community.chocolatey.org/install.ps1')
  This kind of command is often used in a malicious framework to download in memory and run malware on a Windows machine.
  The only clue to conclude a legitimate order is the url, by performing a search on the Internet.

  This is usually easy to identify:

1. On the WebUI interface, open a **Malicious Powershell** alert.
2. Click on the `Show Hexdump` command of the `Action` menu.
3. Search the right column for keywords known as legitimate tools.
4. Search the right column for any suspicious content.
5. If in doubt, contact administrators for confirmation.

- Check sample content: Antiviral DB

  The *malicious_powershell* engine often categorizes anti-viral database update streams, or similar, as malicious over the network.

  These feeds contain signatures that can trigger an alert, but they also contain the names of these signatures.

  It is therefore generally easy to identify them:

  1. On the WebUI interface, open a **Malicious Powershell** alert.
  2. Click on the `Show Hexdump` command of the `Action` menu.
  3. Search the right column for keywords similar to signature names.
  4. If enough (3-4) different keywords are identified, it is certainly an antiviral database

  Names can be truncated depending on the type of stream being extracted.

  Generally, just search for keywords on Microsoft's website: https://www.microsoft.com/en-us/wdsi/threats

  Examples:

  - *Pshdlexec* ("TrojanDownloader:X97M/Pshdlexec")
  - *!##..32/Hikiti.GIC* ("Backdoor:Win32/Hikiti")
  - *...64/Meterpreter.R* ("Trojan:Win64/Meterpreter")
  - *Y2V:Costin_Raiu_Kaspersky_Lab/loki2crypto*

- Check flow type: Backup

  It is possible for a malicious Powershell script to be detected in a virtual machine backup stream.

  This means that there is a **malicious Powershell** on the machine disk.

  This is an alert that is less urgent to investigate and will depend on the use of this machine.

  For example, a cybersecurity expert could keep such files on his machine.

  To know if it is a backup flow, we can:

  - Compare ports (source.port, destination.port) with your virtualization tool documentation
  - Check if the IP matches a storage server
  - Check if many similar flows occur at the same time
  - Contact the infrastructure staff

7.5.3.2.2 How to categorize the threat based on the information collected?

- Check the target machine.

  Powershell scripts require the Powershell interpreter to be installed on the machine, which is still the case on Windows, but very rare for Linux or MacOS.

  In addition, the capabilities of the Powershell framework are limited for them, reducing its interest in a malicious framework.

  Thus, when a **Malicious Powershell** alert is raised, it is interesting to check that the target machine is indeed under Windows.

  If so, it is likely that the machine has been infected.

  If not, it may be a intermediate machine or a false positive.

- Check detailed scores in alert.

  In the alert, consult the list of detailed analysis scores to determine the actions taken by the `powershell` code.

  The `malicious_powershell.score_details` subfields indicate the score related to the types of commands detected.

  Obfuscation techniques detected:

  - `FmtStr`

    Reassembly of multiple values into a formatted string
  - `StrCat`

    Concatenation of multiple strings
  - `StrJoin`

    Concatenating multiple strings with `-join`
  - `CharInt`

    Creating characters from integers with ``[Char]`
  - `Base64`

    Presence of Base64 encoded strings
  - `StrReplace`

    Changing strings by replacing patterns

  Detected commands related to the download:

  - `WebClientInvokation`
  - `InvokeWebRequest`
  - `InvokeRestMethod`
  - `StartBitsTransfer`

  Detected commands related to file interaction:

- `GetContent`
- `SetContent`
- `AddContent`
- `StreamReader`
- `StreamWriter`
- `SystemIOFile`

Detected commands related to order execution:

- `InvokeExpression`

Thus, we can deduce behaviors from this information.
For example an alert with the following results:

- `malicious_powershell.score_details.InvokeExpression: 50`
- `malicious_powershell.score_details.InvokeWebRequest: 20`

Indicates a download and execution of `powershell` code as a `string`.
This is probably a dropper that downloads code to run.

- Manually analyze the Powershell script
  It is often useful and effective to access the sample content to view the detected powershell code and categorize the threat.
  1. On the WebUI interface, open a **Malicious Powershell** alert.
  2. Click on the `Show Hexdump` command of the `Action` menu.
  3. Identify the Powershell code detected by a `powershell` text search.
  4. Extract script manually for better reading.
     Typically, the powershell code is intercepted as one or more orders placed directly to the powershell.
     In this case, isolate the code after the `-Command` or `-c` argument.
     It is not uncommon for the script to be partial, "perforated", or strewn with non-printable characters due to various network-related factors.

     The powershell code may also have been intercepted in base64.
     In this case, the base64 character string containing the code located after the `-EncodedCommand` or `-e` and extract it.
     This tool can be used: CyberChef - getEncodedCommand

     If the `powershell` code was intercepted as a *.ps1* file, the code should be readable and isolated without further action.
  5. Read code to understand purpose
     The Powershell language is relatively intuitive to read with basic programming, if it is not too obfuscated.
     The purpose of this first reading is to identify interesting commands like those indicated in the previous section.
     We can also be interested in external commands or windows executables, for example:
     - `regedit.exe`: import/export registry keys
     - `reg add`: add a registry key
     - `schtasks /Create`: create a scheduled task
     - `net start/stop`: starts/stops a service
     - `wmic`: obtaining or changing the configuration of a remote machine
     - `netsh advfirewall`: obtaining or changing firewall configuration
     - `wusa /kb:{numero}`: uninstall package by KB number

     Help can usually be found to understand these commands on the Internet.

     Overall, these commands can identify whether the script looks malicious or legitimate.
     If the code is too difficult to understand, it is possible to use an AI (eg chatGPT, Mistral, Phind, etc.) provided that the extraction is of good enough quality.

  6. Look for information that may contain indicators of compromise or threat details such as:
     - URLs (e.g. search `http://`)
     - IP addresses
     - File paths (e.g., search for `c:\`, `%AppData%` or `%windir%`)
     - Registry key paths (e.g. search `HKLM`, `HKCU`, `CurrentVersion`)
     - Messages to the victim (e.g. “Your sensitive data has been stolen”)

     It is common for this information to be obfuscated in order to avoid pattern detection.
     Here are the main techniques encountered along with tools to solve them:
     - simple concatenation: `"abc"+"def"` (recette CyberChef strcat) ou `("abc", "def") -join ""` (recette CyberChef strjoin)
     - base64: `WW91ciBkYXRhIGhhcyBiZWVuIHN0b2xlbg==` (recette CyberChef base64)
       This tool extracts only the viewable text, if the base64 starts with `TVqQ` it is probably a windows executable.
     - complex concatenation: `([char]0x61,[char]0x62,[char]0x63,[char]0x64,[char]0x65,[char]0x66) -join ""` (recette CyberChef charint)
     - search-replace: `"aXzYZf" -replace "XzYZ", "bcde"` (recette CyberChef strReplace)
     - format string: `"{1}{2}{0}" -f "ef","ab","cd"`

     Most `string` obfuscation techniques are easy to undo with the right recipe `CyberChef`
     When CyberChef or similar tools are not enough, it is possible to use an AI (eg chatGPT, Mistral, Phind, etc.) in order to obtain

the obfuscated code.
As a last resort, **be careful to copy only the obfuscation code**, execute the obfuscation code snippet in a `powershell` interpreter.
This `powershell` interpreter must have **as few rights as possible** to limit the risks in case of false manipulation.
PS C: Users Guest> "aXzYZf" -replace "XzYZ", "bcde" -> abcdef

- Correlate with other engines
  It is interesting to check the presence of alerts from other engines from information identified by *Malicious Powershell Detect*.

1. Note some information that may be present in other alerts.
   For example:
   - IP Source: `x.y.z.1`
   - IP Destination: `x.y.z.2`
   - URL or IP contacted by the script
   - File downloaded by script
2. In the `Alerts` menu of the WebUI, select all engines except Malicious Powershell Detect and filter on the collected information.
   Some examples of filters:
   - Filter 1: `ip:x.y.z.1`
   - Filter 2: `ip:x.y.z.2`

   Note:

   It is important to note that the source IP identified by Malicious Powershell Detect may have been identified by another engine as an IP Destination.

   The most suspicious alerts will be related to the compromise of the source IP: executable files, privilege elevation, connection to bad reputation IPs among others.
3. It is also possible to perform this investigation in Kibana UI.
   The previous filters then become:
   - `source.ip:x.y.z.1 or destination.ip:x.y.z.2) and event.module:"sigflow_alert"`
   - `source.ip:x.y.z.1 or destination.ip:x.y.z.2) and event.module:"sigflow_alert"`

- Correlate with windows logs
  - If a malicious Powershell script was run on a Windows machine, there is a good chance of finding a trace of it in the event logs.
  - If the feature is enabled, Windows records all executed powershell commands.
    To do this, open "Event Viewer", then go to "Application and Service Logs", "Microsoft", "Windows", "Powershell".

7.5.3.2.3 What answers are needed if the threat is confirmed?

- **Isolate the system**: immediately isolate the contaminated system and ensure it cannot cause further damage.
- **Notify**: inform relevant parties of threat detection.
- **Collect information**: gather critical information such as IP addresses, or information in the Hexdump.
- **Neutralize the threat** by blocking the IP address.
- **Analyze logs**: review system and network logs to trace the spread of the threat.

7.5.3.2.4 What if an alert from this engine is identified as a false positive?

If an alert from this engine is identified as a recurring false positive, it is recommended to `mute` the alert signed.
There is no whitelist for the Malicious Powershell Detect engine.

7.5.4 Analyzing the Sigflow alerts

7.5.4.1 Introduction

For information, see the following paragraphs:

- *For what types of threats is this engine designed?*
- *How does this particular engine detect threats?*
- *How does Sigflow engine work in the GCenter?*

7.5.4.1.1 Management of the Sigflow engine

For engine informations, see the paragraph *View the status of Sigflow*
For information on engine upgrade, see the paragraph *Engine update*
For information on engine configuration, see the paragraph *Sigflow configuration*

7.5.4.1.2 Events generated by the engine

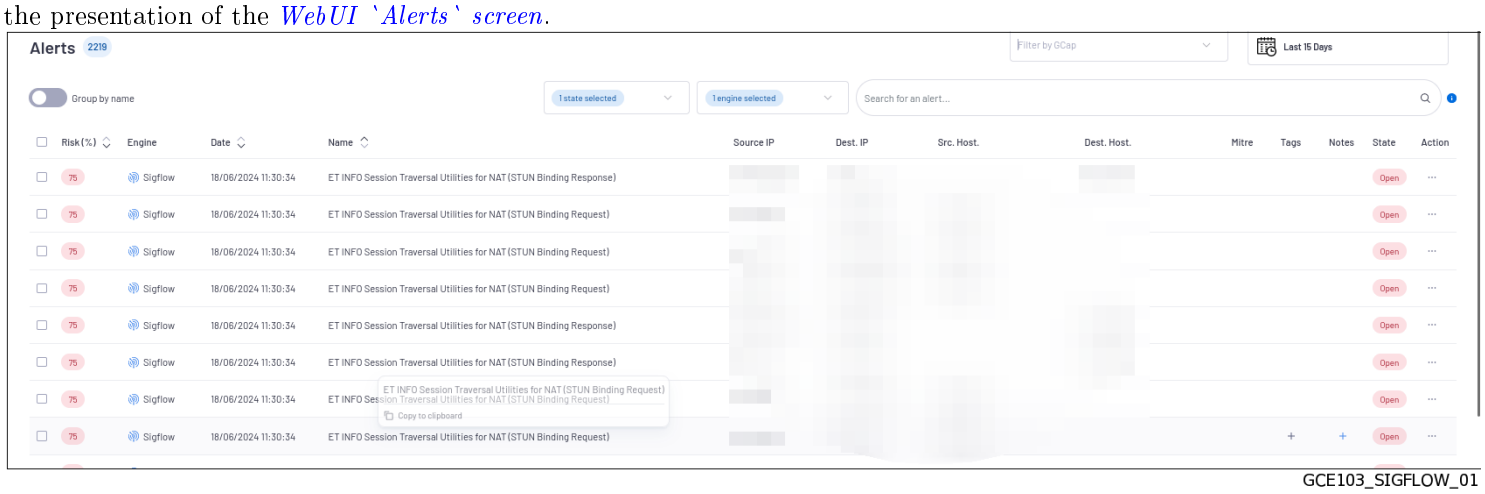
The events generated by Sigflow are:

- Events of type "alert" when the engine has found a match with the signature defined in the alert rules
- Events of type "fileinfo" when the Sigflow engine has reconstructed the network flow **files**
- Events of type "metadata" when the Sigflow engine has recognized the network flow **protocols**

7.5.4.1.2.1 Events of type "alert"

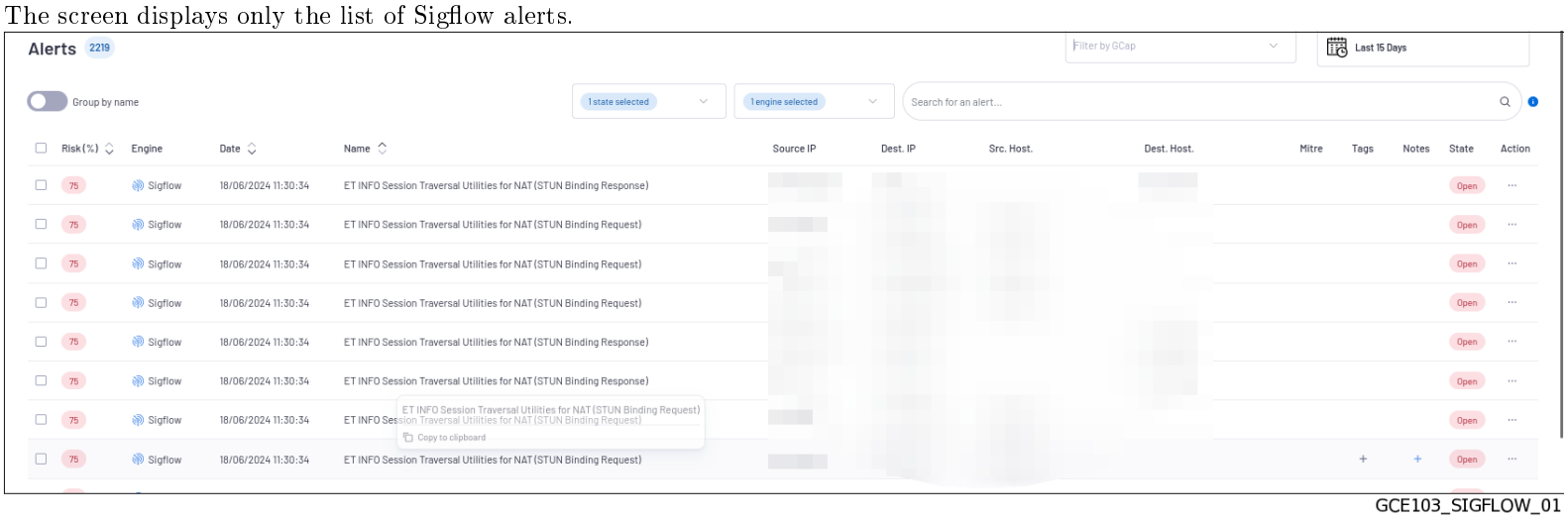
Events of type "alert" are generated when the engine has found a match with the signature defined in the alert rules.
These are displayed:

- In the main interface named **WebUI** on the GCenter in the `Alerts` screen
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
  It is possible to view the found signature and its definition.
  - To view the alerts, select the `Sigflow` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.



GCE103_SIGFLOW_01

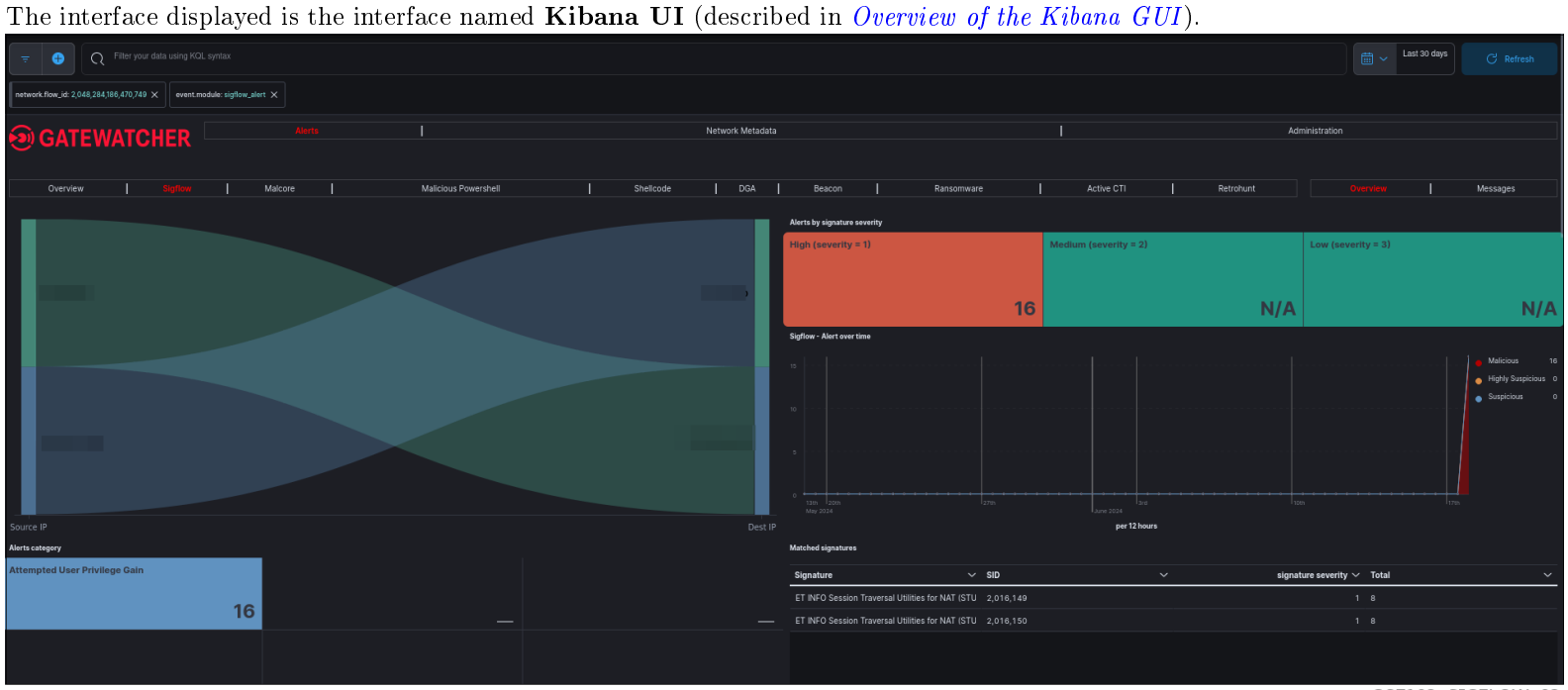
  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed: see *Example of a Sigflow alert in the WebUI*.
    The displayed counters are given in the *Engine log data structure* appendix.
- In the interface named **Kibana UI**
  - In the main interface **WebUI**, to view the alerts, select the `Sigflow` engine filter.
    The screen displays only the list of Sigflow alerts.



GCE103_SIGFLOW_01

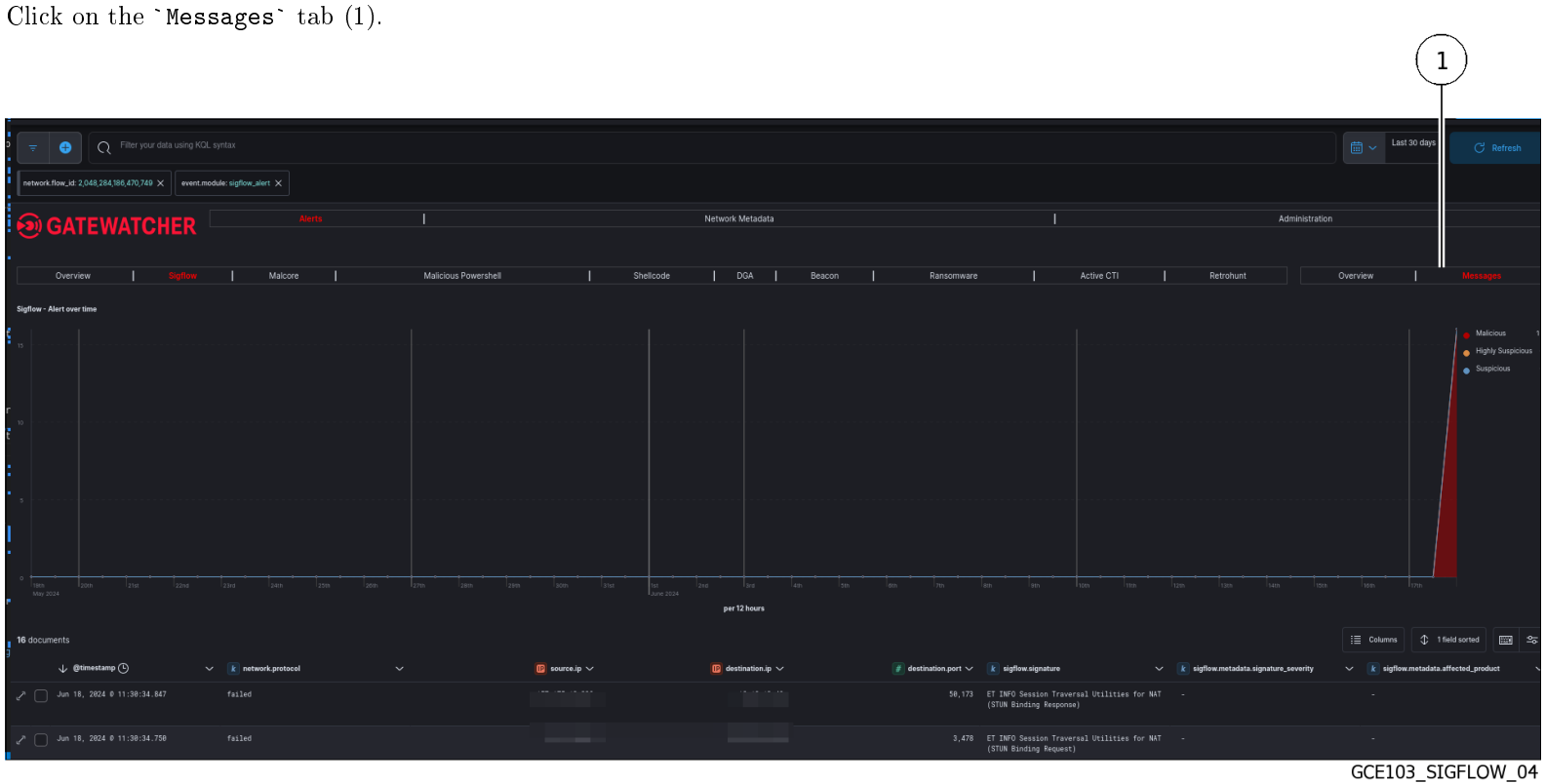
  - After selecting the alert, click on the `Open flow details` command of the `Actions` menu.
    See the presentation of the *WebUI `Alerts` screen*.
    Kibana is opened on the `Sigflow` category of the `Alerts ` section.

The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).



GCE103_SIGFLOW_03

- Click on the `Messages` tab (1).



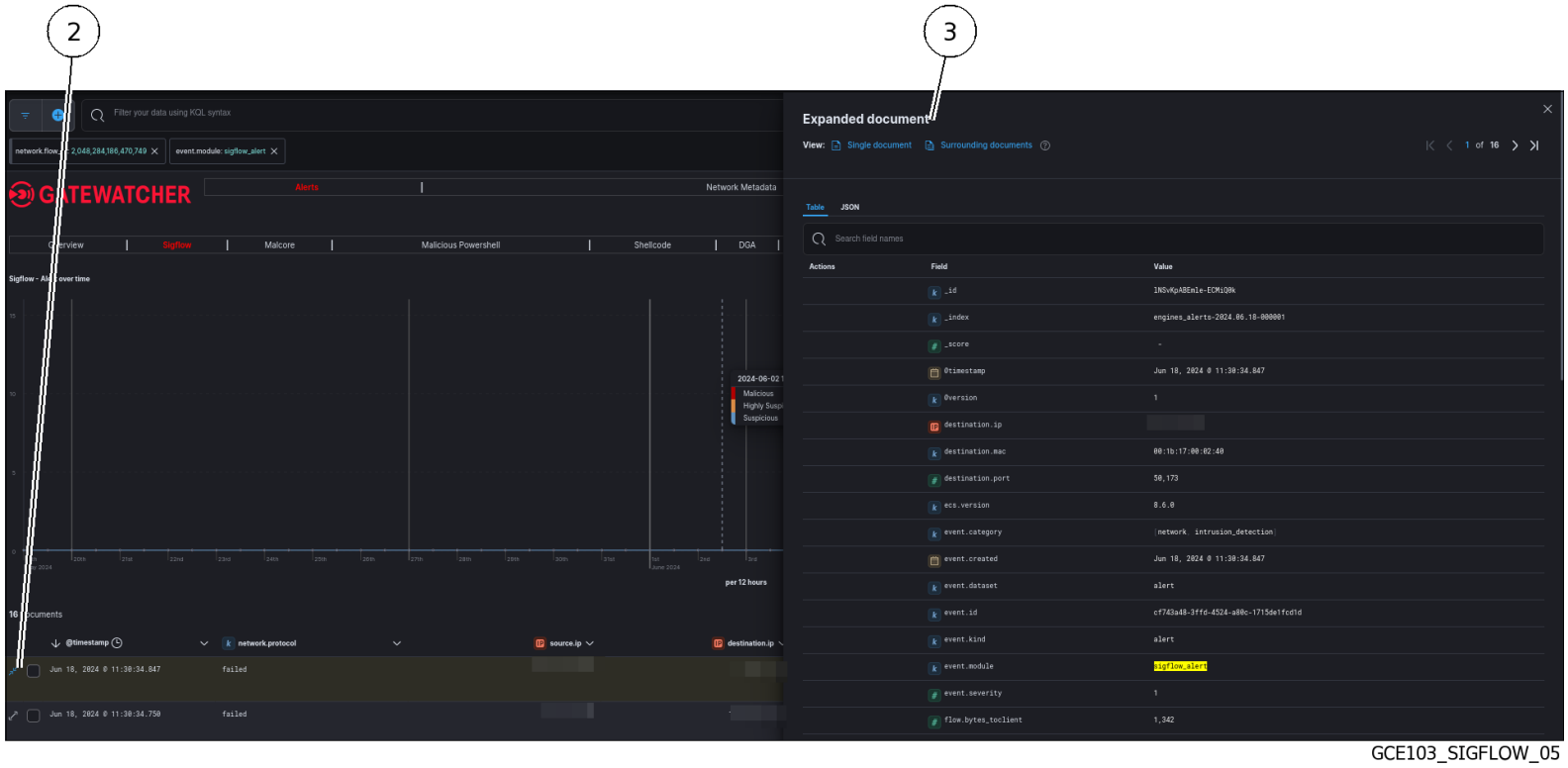
GCE103_SIGFLOW_04

The Kibana database is filtered with the filters:

- network.flow_id: unique ID of the flow selected
- event.module: sigflow_alert

This page displays all alerts detected by Sigflow in this network flow (whatever the IP addresses or the direction).

- Click on the toggle icon on the left of the alert (2).
  The `Expanded document` window (3) is displayed.



GCE103_SIGFLOW_05

The detailed information of this alert can be viewed in table or json format (see the *Events of type "alert"*).
The displayed counters are given in the *Engine log data structure* appendix.

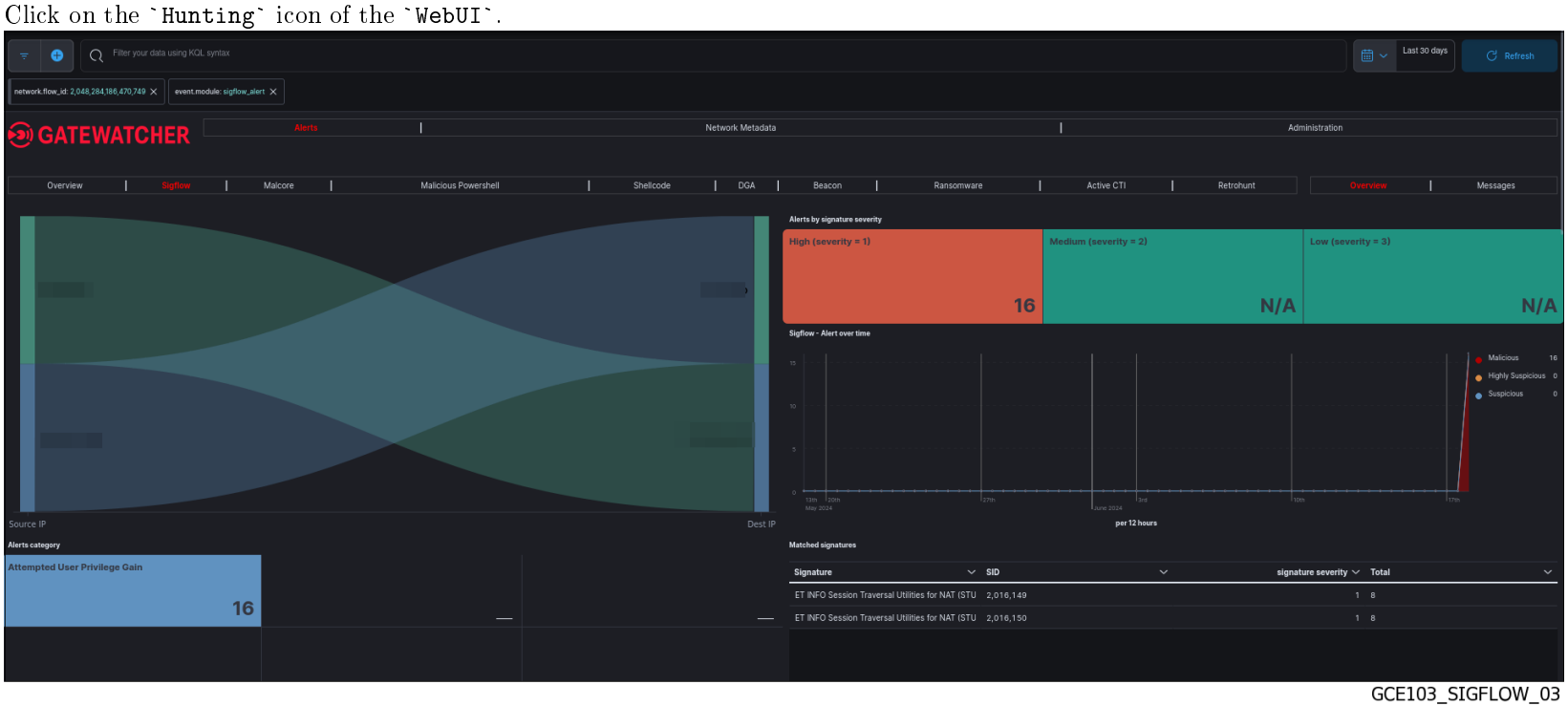
Note:

The **Kibana UI** can also be accessed without any filters via the `Hunting` icon on the left side menu bar in the WebUI.

7.5.4.1.2.2 Events of type "fileinfo"

Events of type "fileinfo" are generated when the Sigflow engine has reconstructed the network flow **files**.
These fileinfo events are visible in the Kibana interface.

- Click on the `Hunting` icon of the `WebUI`.



GCE103_SIGFLOW_03

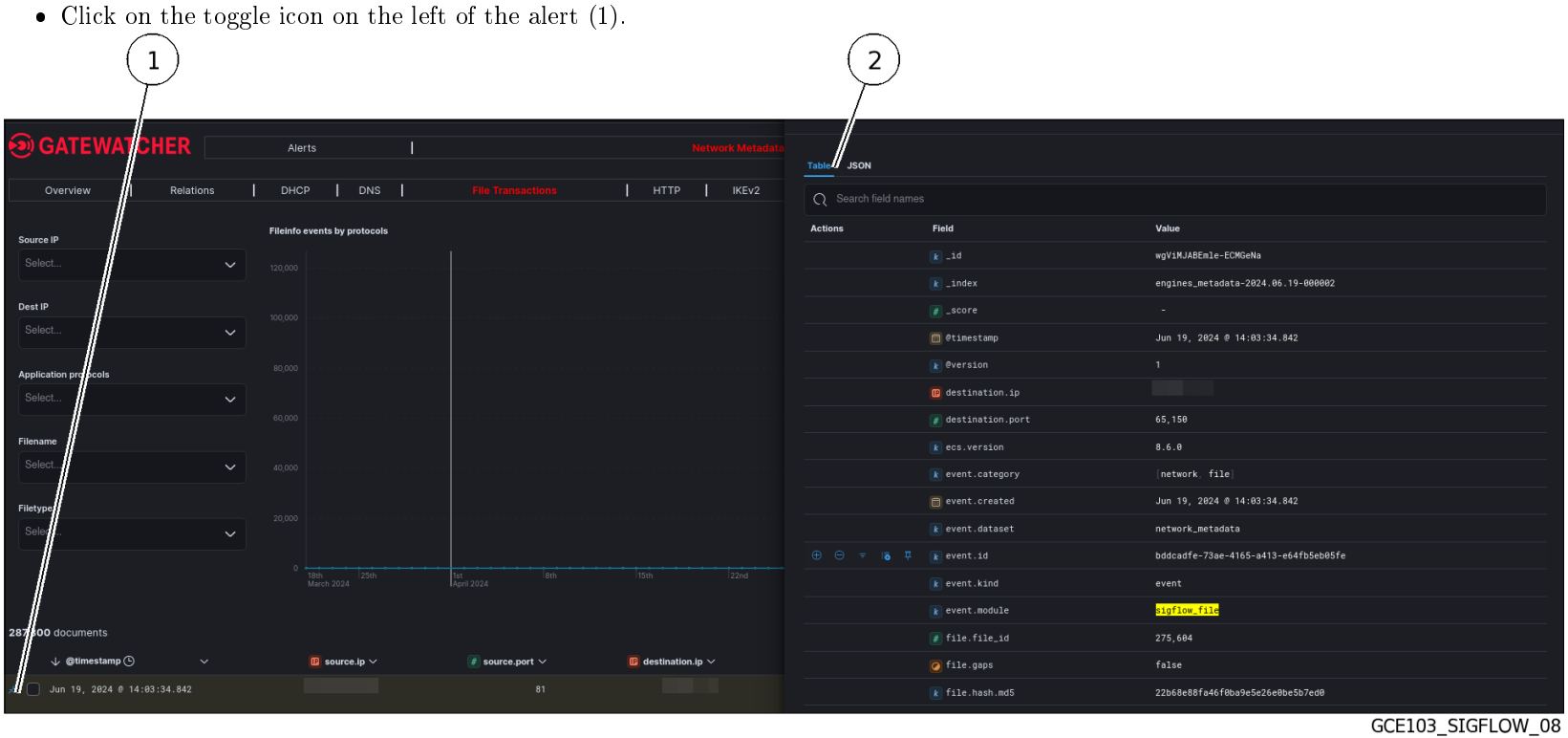
The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

- Click on the `Network Metadata` section (2) then the `File Transactions` category (1).
- Click on the `Messages` tab (3).

GCE103_SIGFLOW_07

This page displays all events of fileinfo type corresponding to the reconstructed files in this network flow.

- Click on the toggle icon on the left of the alert (1).



GCE103_SIGFLOW_08

The detailed information (2) of this event can be viewed in table or json format.

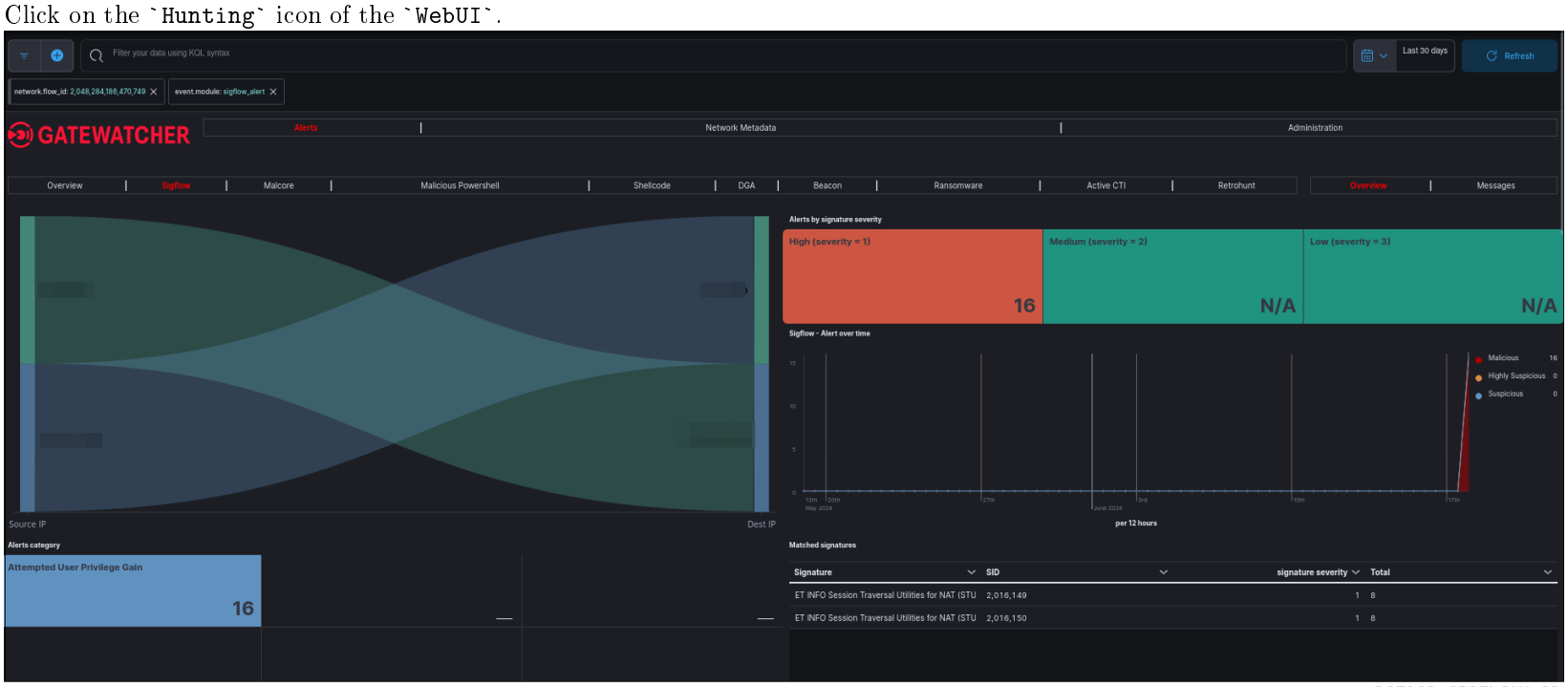
Note:

The **Kibana UI** can also be accessed without any filters via the `Hunting` icon on the left side menu bar in the WebUI.

7.5.4.1.2.3 Events of type "metadata"

Events of type "metadata" are generated when the Sigflow engine has recognized the network flow **protocols**.
These metadata events are visible in the Kibana interface.

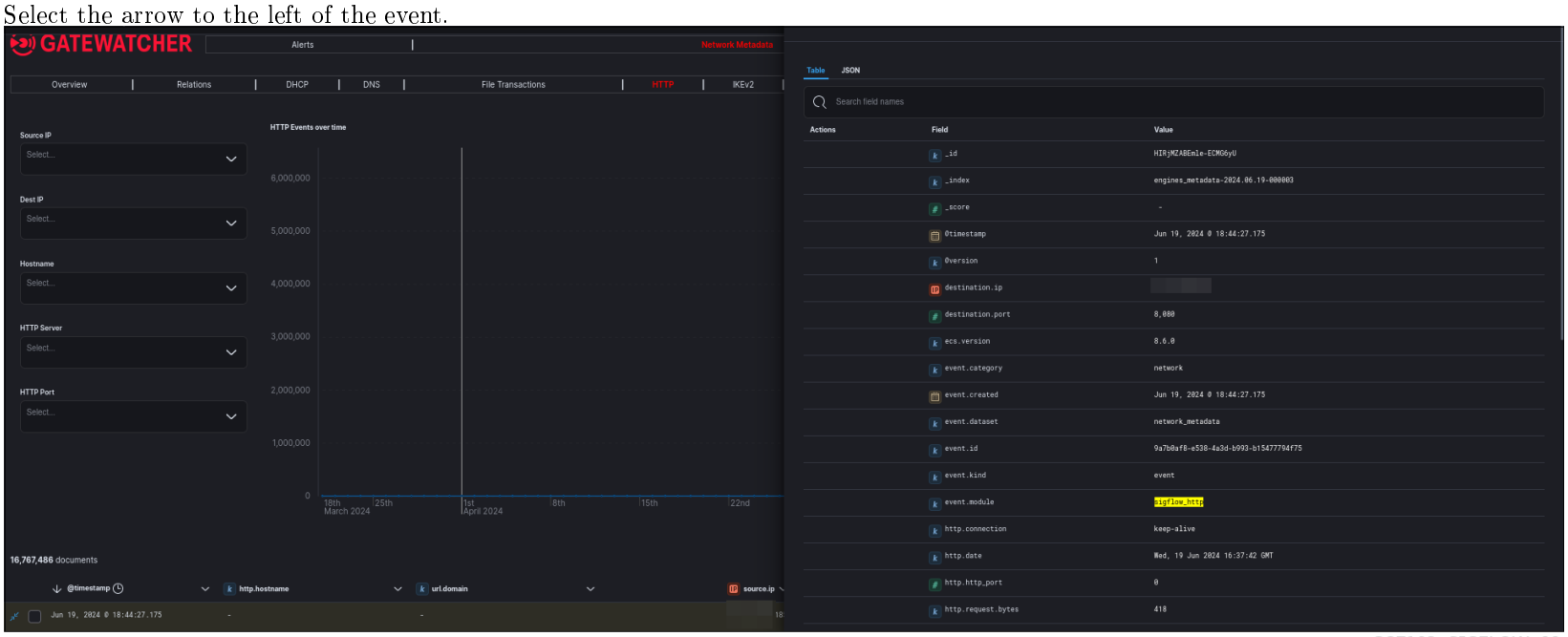
- Click on the `Hunting` icon of the `WebUI`.



GCE103_SIGFLOW_03

The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).

- Click on the `Network Metadata` section then the protocol category (HTTP for example).
- Click on the `Messages` tab.
  This page displays all events of metadata type (metadata) corresponding to the detected protocol in this network flow.
- Select the arrow to the left of the event.



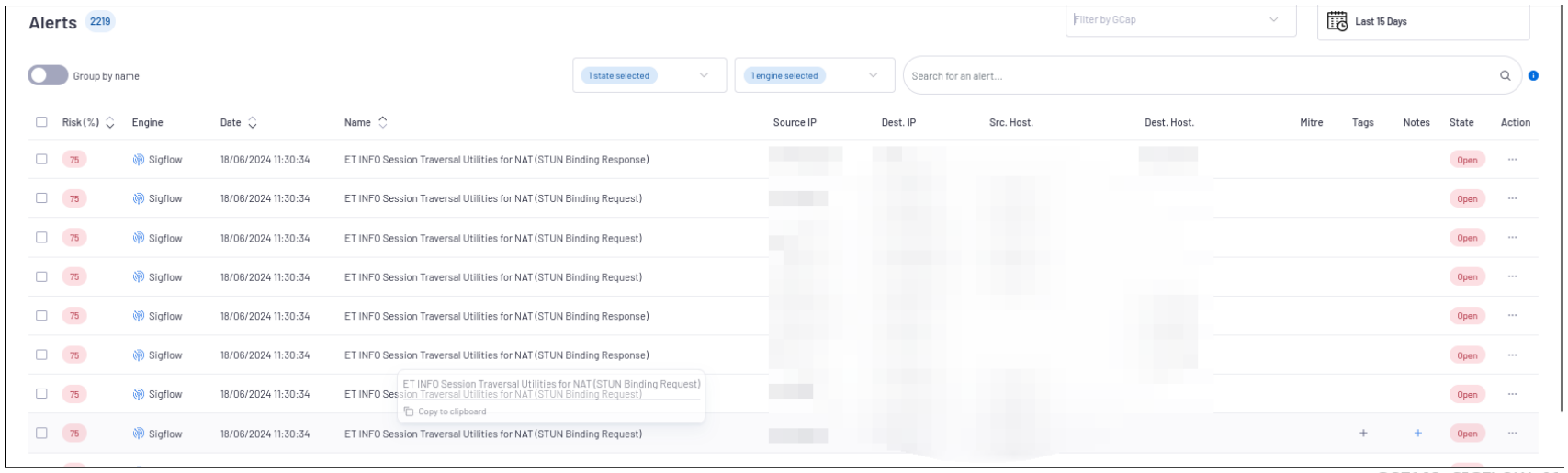
GCE103_SIGFLOW_09

The detailed information of this event can be viewed in table or json format.

7.5.4.1.3 Essential information to understand the context of the alert

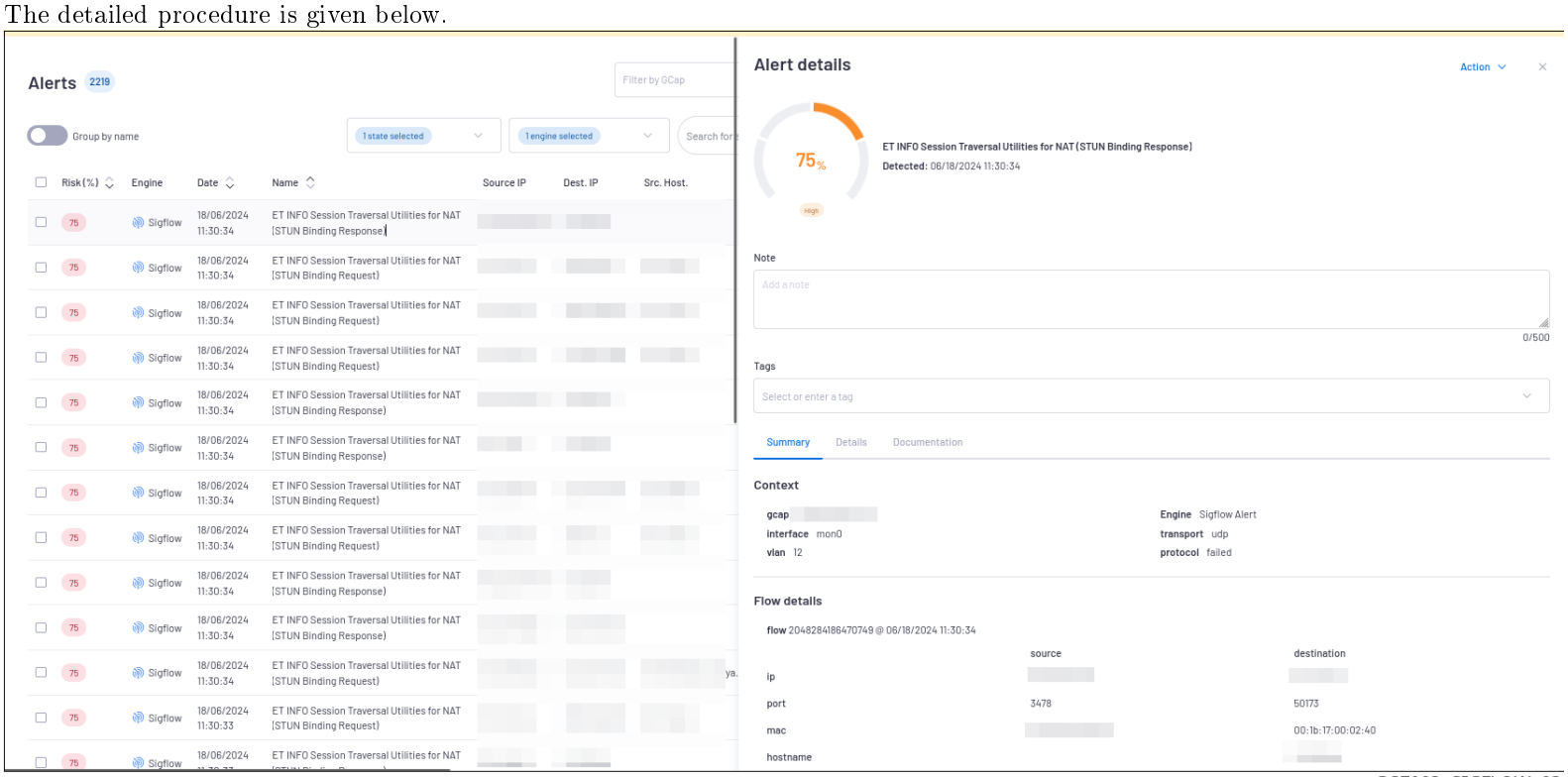
7.5.4.1.3.1 What are the key fields of an alert and their meaning?

Before undertaking any investigation or qualification of the alert, it is essential to start by observing several elements that will provide essential information to understand the context of the alert.
These elements can be found either in the **WebUI** interface or in the **Kibana UI** interface.



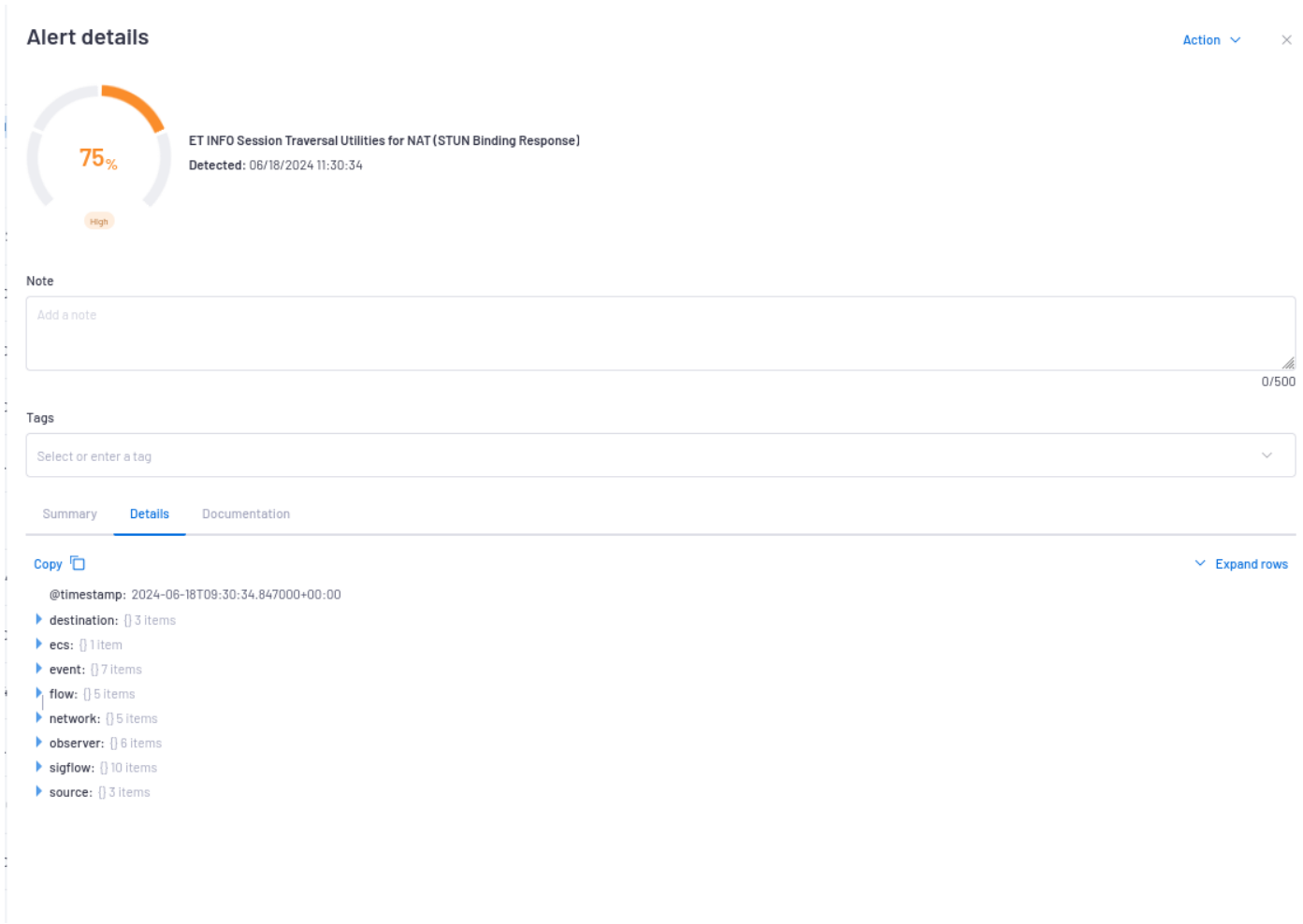
GCE103_SIGFLOW_01

- In the main interface named **WebUI** of the GCenter.
  - Open the `Alert details` window.
    The detailed procedure is given below.



GCE103_SIGFLOW_02

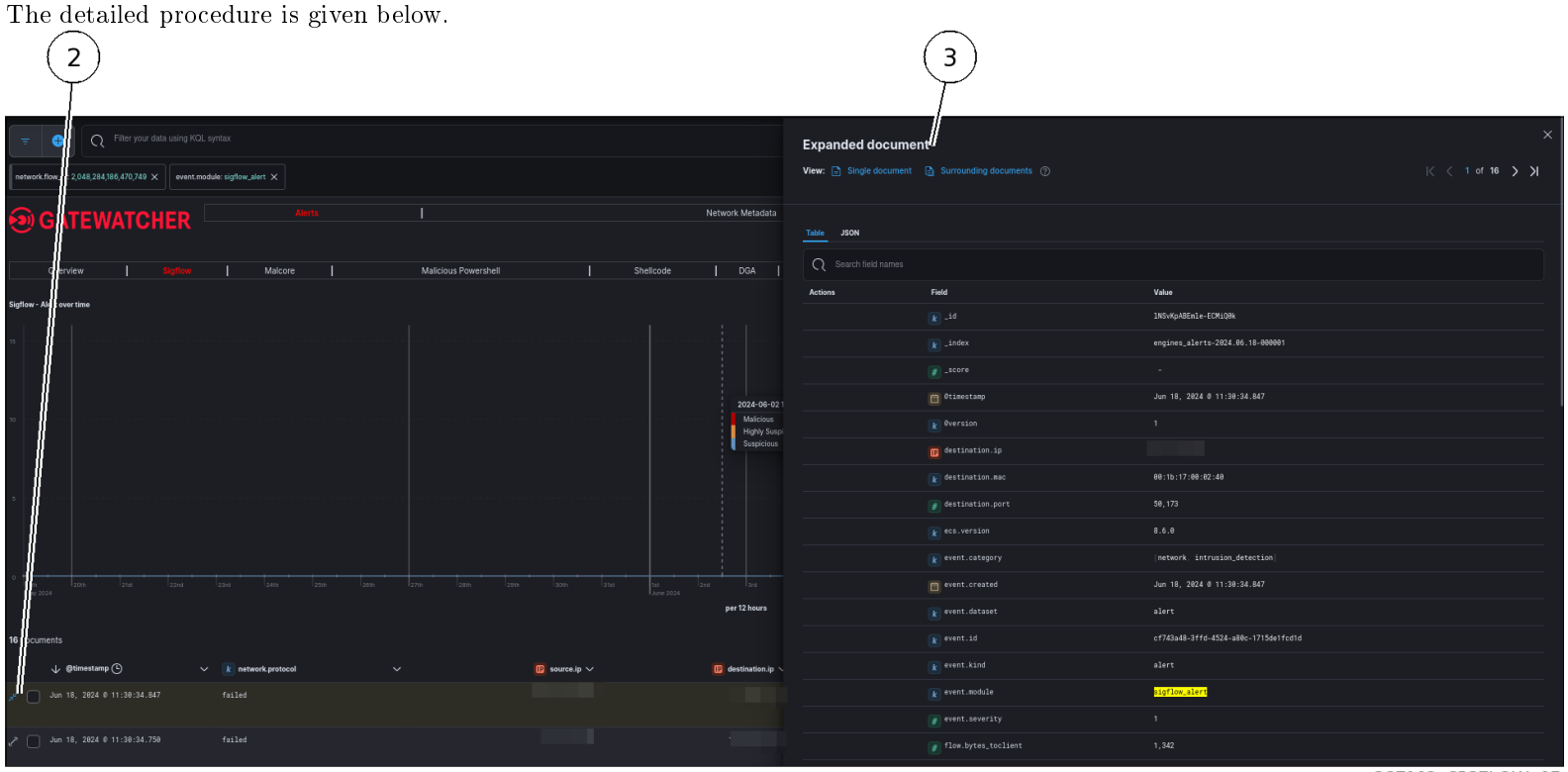
- Click on the `Details` tab.



The following key elements are:

- `category` to know the alert id and severity, useful for classifying alerts.
- `sigflow` to have important information about the triggering of the alert.
  The `metadata` section displays precisely the payload that triggers the alert.
  - `Network` for information on the protocol used to trigger the alert and also the vlan used.
  - `source` and `destination` to have the elements concerning the port and ip address for the source and destination.
  - For the rest of the elements, the most interesting field will be the `start` of the `flow`.
    It allows you to select a time window to perform searches.
- In the **Kibana UI** interface
  - Open the `Alerts-Sigflow - Messages` window.

  The detailed procedure is given below.



The following key elements are:

- `timestamp:`
  This field corresponds to the time of detection.
- `Source IP` and `Dest. IP`

The IP addresses associated with the alert, source or destination, provide information about the network communication involved in the incident.

- `Source Port` and `Dest. Port`
  The port associated with the alert, source or destination, provides information about the network communication involved in the incident.
- `Sigflow affected product`
  Where possible, there is a product specification in relation to the alert.
  The accuracy of this field is very relative, it can be an apache version or elements like `Web_Browsers` or `Windows_XP_Vista_7_8_10_Server_32_64_Bit`
- `Sigflow.signatures`
  This will display the alert title, the "msg" part that describes the item detected by the alert.
  For information, if this field contains `ET POLICY` or `ET INFO`, consider this alert as an information alert or a low profile alert.
  They show that there is a configuration that does not correspond to good practices.
  They can be used for additional context on other alerts.

7.5.4.2 Alert handling procedure

7.5.4.2.1 How do you verify the accuracy of an alert and determine if it represents a real threat?

Sigflow uses rules to make detections.
The subject of verifying the accuracy of a Sigflow alert must be addressed and whether it represents a real threat or not involving a combination of analysis techniques.
Here are some steps to take:

- **Understanding the alert:**
  - Understand the rule that triggered the alert, source and destination IP addresses, port numbers and any additional information provided.
  - All this information can be found in GCenter:
    - In the WebUI, in the `Alert details` window of the `Alert` screen: carefully review the details of the Sigflow alert
    - In Kibana, to better understand the alert, open the `Expanded document` window of the `Alerts ` section, `Sigflow` category, `Messages` tab
  - **For the record, if you have an alert containing the labels `ET POLICY` or `ET INFO`, take it as an information alert.**
    They show the fact that there is a configuration that does not correspond to best practices.
    They can be used for additional context on other alerts.
- **Rules analysis:**
  - Review the rule that generated the alert.
    Understand the conditions that triggered the alert and the level of severity assigned to it.
    Some rules may be more generic and generate false positives, while others may be more specific.
  - Different elements concerning false positives:
  - True false positive is a rule that has been triggered and indicates a threat when there is none.
  - Noisy signature is an alert triggered by normal activity that is identified but the rule has not been deleted.
    This can happen when, for example, a script performs automatic actions that can be associated with malicious activity if it is not performed by the monitoring machine.
- **Historical analysis and reference comparison:**
  - Examine historical data and trends.
    Analyze if similar alerts have been issued in the past and if there is a trend of recurring threats.
    Historical analysis can help identify persistent or evolving threats.
  - Aggregate all alerts by machine or check the regularity of the event over time.
  - By aggregating the view of alerts, look for the appearance of alerts to see if it is the only alert of this type.
    In case of multiple alert on this host, record it and qualify this alert.
    Sometimes alerts are too important and can be triggered even if there is nothing to fear.
  - If there are doubts about false positives, look at the following point in the documentation «What happens if an alert from this engine is identified as a false positive» ?
  - Once the assessment is complete and after determining whether the alert is recurring or not, drill down to the payload analysis.
- **Payload Analysis:**
  - Analyze the payload associated with the alert.
    This information will be found in the alert details (seen in the first point).
  - To analyze the payload, use the following fields `Sigflow.payload_printable`.
    For example, to identify a malicious domain.
  - Also use the `Sigflow.payload` field when the payload is coded.
    For example, to reconstruct and look inside an archive sent by stealer to its C2 and encode in b64.
- **Correlation with other events:**
  - It is mandatory to cross-reference alerts with logs from other engines.
    A tiered approach can help confirm the validity of an alert.
  - To help you in this task, reduce the scope of the analysis by exploring the IP sources/destinations, the port and a time window on which the first alert was identified
- **Threat intelligence integration:**
  - To be safe and have more information to act, obtain details on orroborate alerts with known indicators of compromise (ICOs) from threat intelligence sources.

- **Incident Response Procedures:**
  - If an alert is deemed genuine, follow your organization's response plan to mitigate and contain the threat.
  - Some ideas for a more in-depth analysis of events are given in the section «What answers are needed if the threat is confirmed?»

7.5.4.2.2 How to categorize the threat based on the information collected?

The categorization of threats based on the information produced by the Sigflow engine implies:

- To analyze alerts
- To classify them under different threat categories

The information will have to be cross-checked to initiate other actions.
To categorize threats:

- **Severity Levels:**
  - Start by reviewing the severity levels assigned to Sigflow alerts.
    Many rules have predefined severity levels (e.g., high, medium, low).
    Use these severity levels as an initial indicator of the potential threat.
  - All this information can be found in the GCenter:
    - In the WebUI, in the `Alert details` window of the `Alert` screen: carefully review the details of the Sigflow alert
    - In Kibana, to better understand the alert, open the `Expanded document` window of the `Alerts ` section, `Sigflow` category, `Messages` tab
- **Classification of rules:**
  - Classify rules into different categories according to their purpose and the type of threats they detect.
    For example, rules may focus on malware, suspicious network activity, exploit attempts, or known vulnerabilities.
  - For the record, if an alert contains the `ET POLICY` or `ET INFO` labels, take it as an information alert.
    They show the fact that there is a configuration that does not correspond to best practices.
    They can be used for additional context on other alerts.
  - All this information can be found in the GCenter:
    - In the WebUI, in the `Alert details` window of the `Alert` screen: carefully review the details of the Sigflow alert
    - In Kibana, to better understand the alert, open the `Expanded document` window of the `Alerts ` section, `Sigflow` category, `Messages` tab
  - For the record, if an alert contains the `ET POLICY` or `ET INFO` labels, take it as an information alert.
    They show the fact that there is a configuration that does not correspond to best practices.
    If necessary, report the alert to your security organization.
- **Payload Analysis:**
  - Examine the payload of network packets associated with each alert.
    Payload analysis can reveal the nature of the threat, such as specific malware signatures, command and control communication, or malicious payload patterns.
    For example, to identify a malicious domain.
  - Also use the field `Sigflow.payload`, it depends on the case.
    For example, to reconstruct and look inside an archive sent by stealer to its C2 and encode in b64.
- **Compromise Indicator Analysis (IOC):**
  - Look for indicators of compromise in alerts, such as IP addresses, domain names, file hashes or patterns specific to known malware.
    Cross-reference these indicators with threat intelligence flows to determine the nature of the threat.
  - All this information can be found in the GCenter, in the `Alert` panel or in Kibana, in Sigflow under the `Messages` panel.
  - All this information can be found in the GCenter:
    - in the Webui, in the `Alert details` window of the `Alert` screen: carefully review the details of the Sigflow alert
    - in Kibana, to better understand the alert, open the `Expanded document` window of the `Alerts ` section, `Sigflow` category, `Messages` tab
- **Behavioral analysis:**
  - Analyze the network traffic behavior that triggered Sigflow alerts.
    Identify patterns of suspicious or malicious behavior, such as port analysis, brute force attacks or abnormal communication patterns.
  - For this part, expand the time windows and look for other alerts to better understand the behavior.
    You won't necessarily find the beginning of the attack, but with this behavioral analysis, you can use killchain to identify the stage of the attack.
- **Background information:**
  - Consider contextual information, such as source and destination IP addresses, ports and protocols.
    This information can provide information about the specific type of threat and the potential impact on the network.
  - Also use another detection engine to help in this task.
    For example, Sigflow cross-reference alerts and the Malcore engine let you know what malware you are dealing with.
- **Incident Response Classification:**
  - If an alert is confirmed as a real threat, classify it according to your organization's response classification system.
    This may involve categorizing incidents as low, medium or high impact and prioritizing response actions accordingly.
- **Documentation and Reporting:**
  - Document findings and create reports that summarize threat categorization.
    Clear documentation helps to understand the nature of threats, improve response procedures and share information with relevant stakeholders.

7.5.4.2.3 What answers are needed if the threat is confirmed?

Note:

This procedure allows to deepen the investigation and assess the extent of the incident after confirmation of a threat generated by the Sigflow engine.

Follow incident response procedures if an alert is deemed genuine:

- Follow your organization's response plan to mitigate and contain the threat.
- In the absence of an incident response procedure:
  - **Reporting and Classification:**
    - Record findings
    - Classify the incident as low, medium or high impact
    - Prioritize intervention measures accordingly
  - **Isolate the system**:
    - Isolate contaminated system immediately
    - Ensure that it cannot cause further damage
  - **Go after threats**:
    - Proactive threat hunting
    - Use alerts as a starting point for investigating potential threats
    - Conduct in-depth analysis to uncover hidden or advanced threats that may not be immediately apparent

Because the Sigflow engine allows us to find an item on the network, with this network survey, a compromised host survey must be initiated.

7.5.4.2.4 What if an alert from this engine is identified as a false positive?

Sometimes alerts are too important and can be triggered even if there is nothing to fear.
In this case:

- Check that the traffic generating the alert:
  - Is legitimate
  - Aligns with the normal behavior of the network
- If it appears that some rules produce too many false positives, disable them by changing the ruleset.

Important:

Disabling a rule means that the threat for which the rule was created will no longer be detected.
We advise you to closely assess the risk of this operation with all stakeholders responsible for the security of the organization.

7.5.5 Analyzing the DGA detect alerts

7.5.5.1 Introduction

For information, see the following paragraphs:

- *For what types of threats is this engine designed?*
- *How does this particular engine detect threats?*
- *How does this DGA detect engine work in the GCenter?*

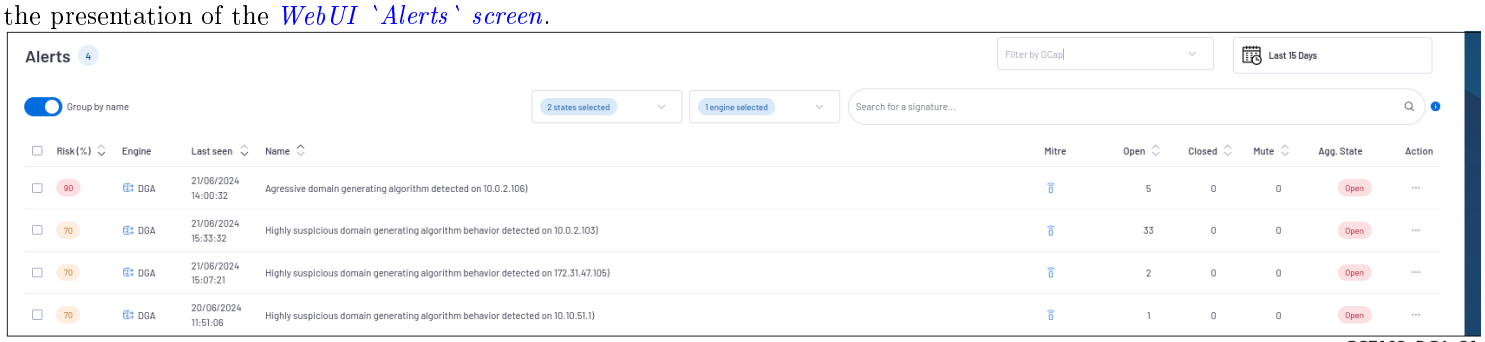
7.5.5.1.1 Management of the DGA Detect engine

For engine informations, see the paragraph *Viewing the engine status*
For information on engine upgrade, see the paragraph *Engine update*
For information on engine configuration, see the paragraph *Configure the DGA detect engine and manage the list of ignored files*

7.5.5.1.2 Events generated by the engine

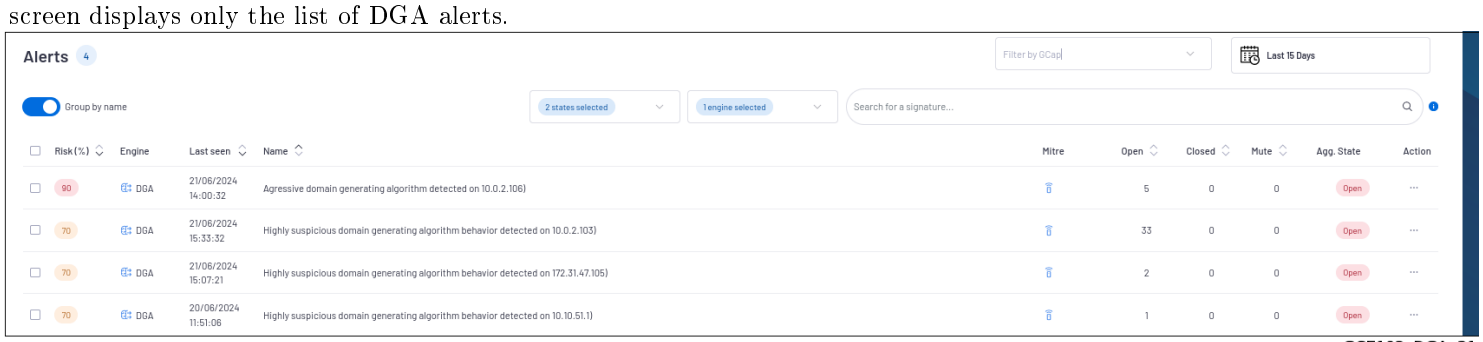
Events generated by the DGA detect engine are **alerts**.
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen.
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
  - To view the alerts, select the `DGA` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.



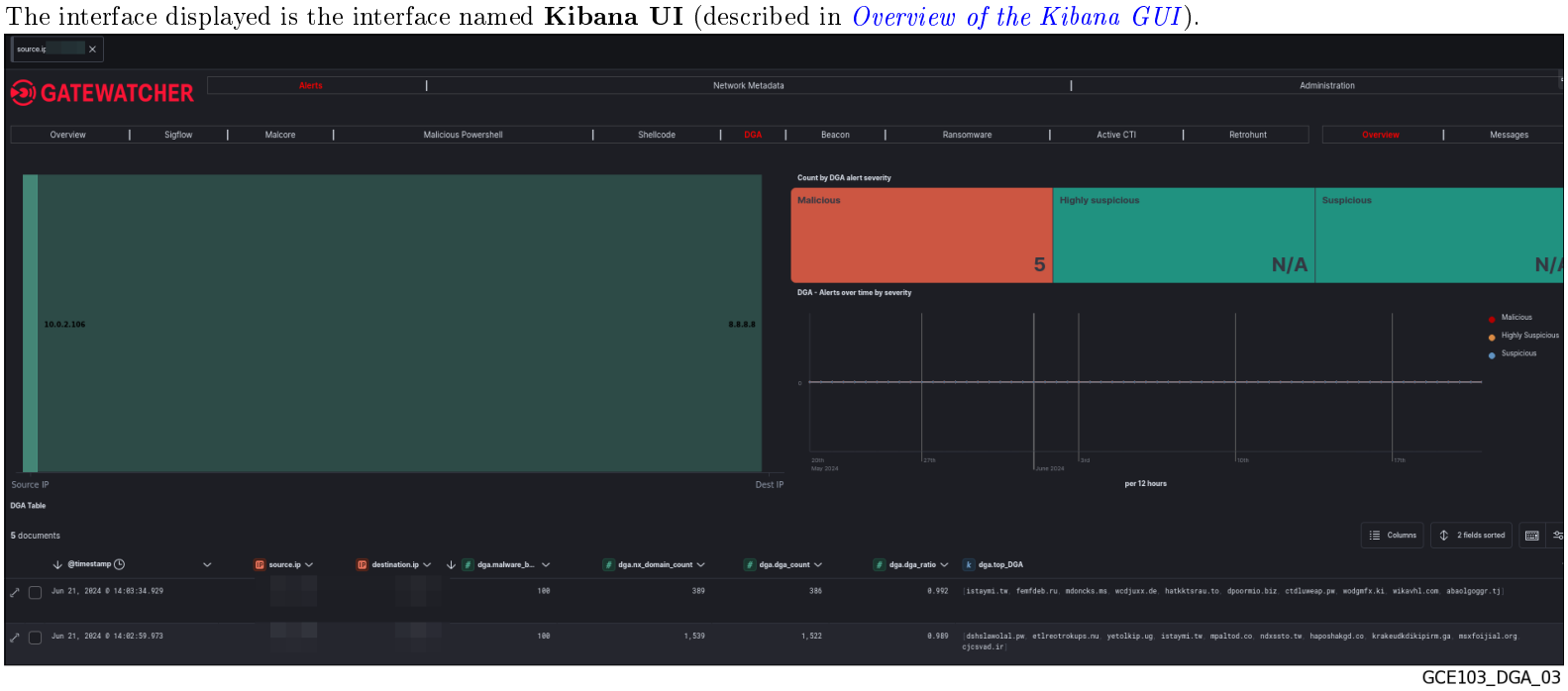
GCE103_DGA_21

  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed in *Example of a DGA detect alert in the WebUI*.
- In the interface named **Kibana UI**
  - To view the alerts, select the `DGA` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.
    The screen displays only the list of DGA alerts.



GCE103_DGA_21

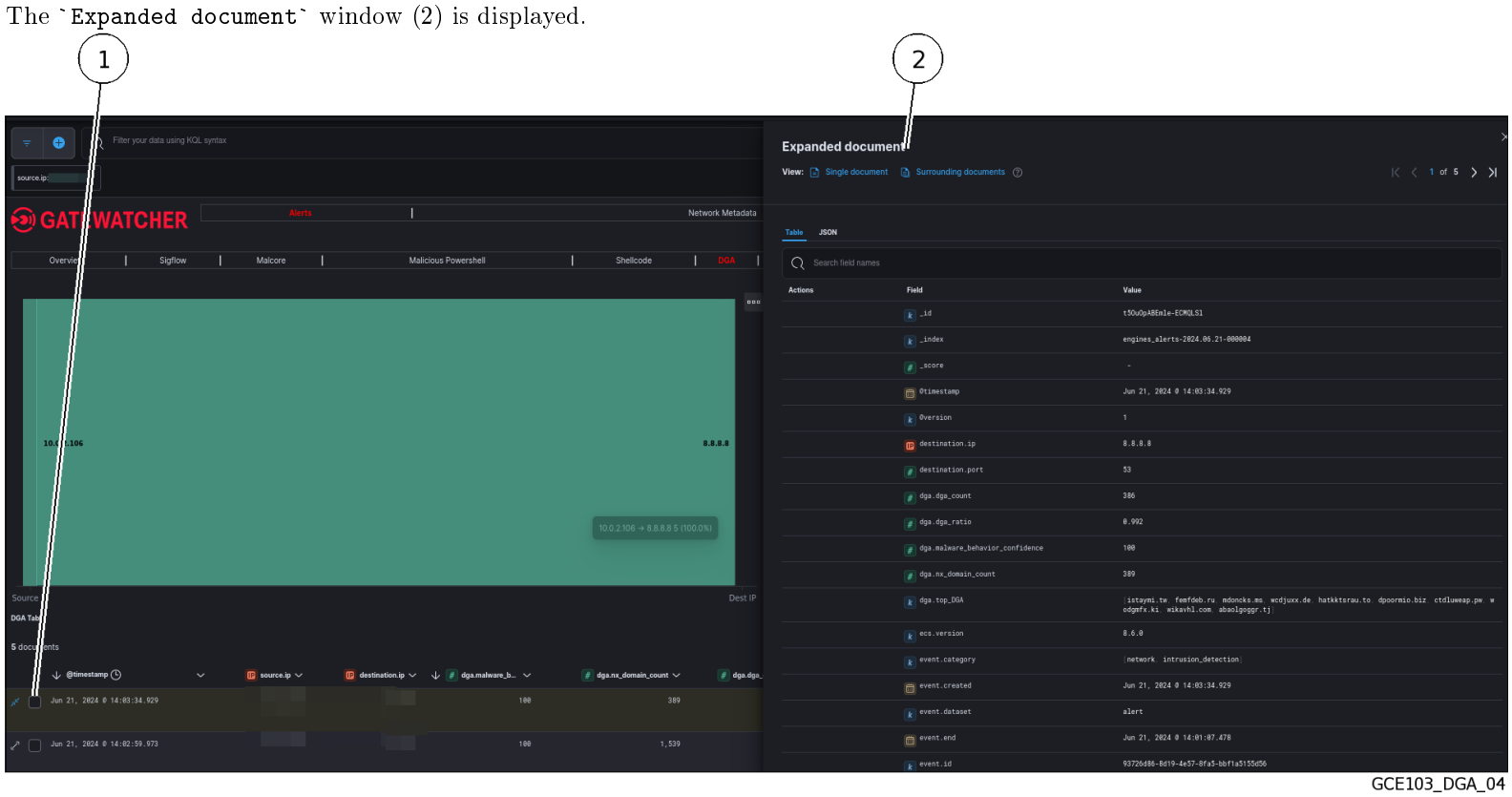
- After selecting the alert, click on the `Open DGA activity` command of the `Actions` menu.
  Kibana interface is opened in the `Overview` tab, the `DGA` category of the `Alerts ` section.
  The database is filtered on the `source.ip:` parameter which sends the DGA request.
  The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).



GCE103_DGA_03

This page displays all alerts from this IP address detected by DGA.

- Click on the toggle icon (1) on the left of the alert.
  The `Expanded document` window (2) is displayed.



GCE103_DGA_04

The detailed information of this alert can be viewed in table or json format (see the *DGA detect log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

Note:

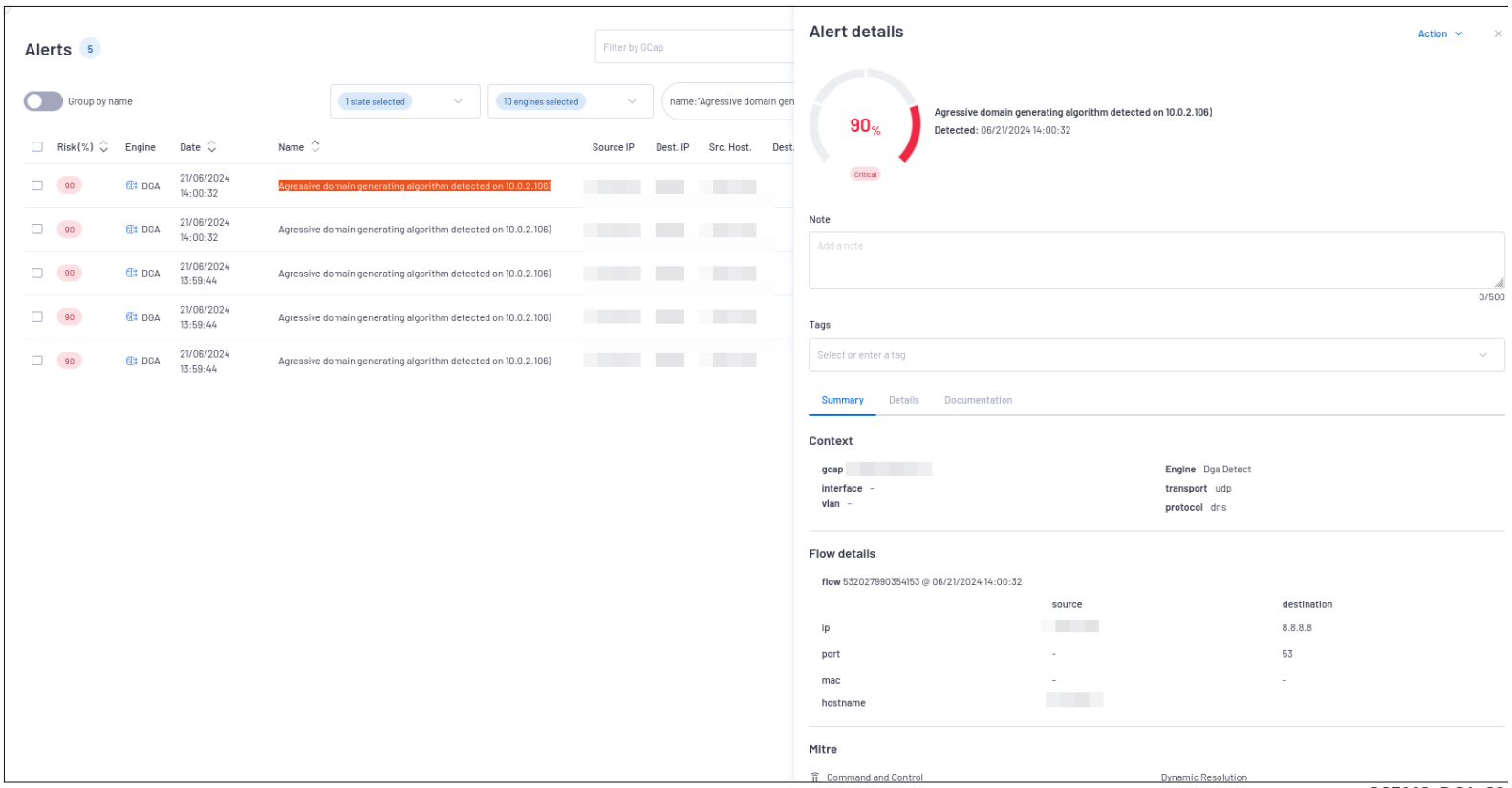
If a GCap oversees several networks or if several GCaps supervise several networks, it is possible that a domain name that appears several times will generate only one alert.

7.5.5.1.3 Essential information to understand the context of the alert

7.5.5.1.3.1 What are the key fields of an alert and their meaning?

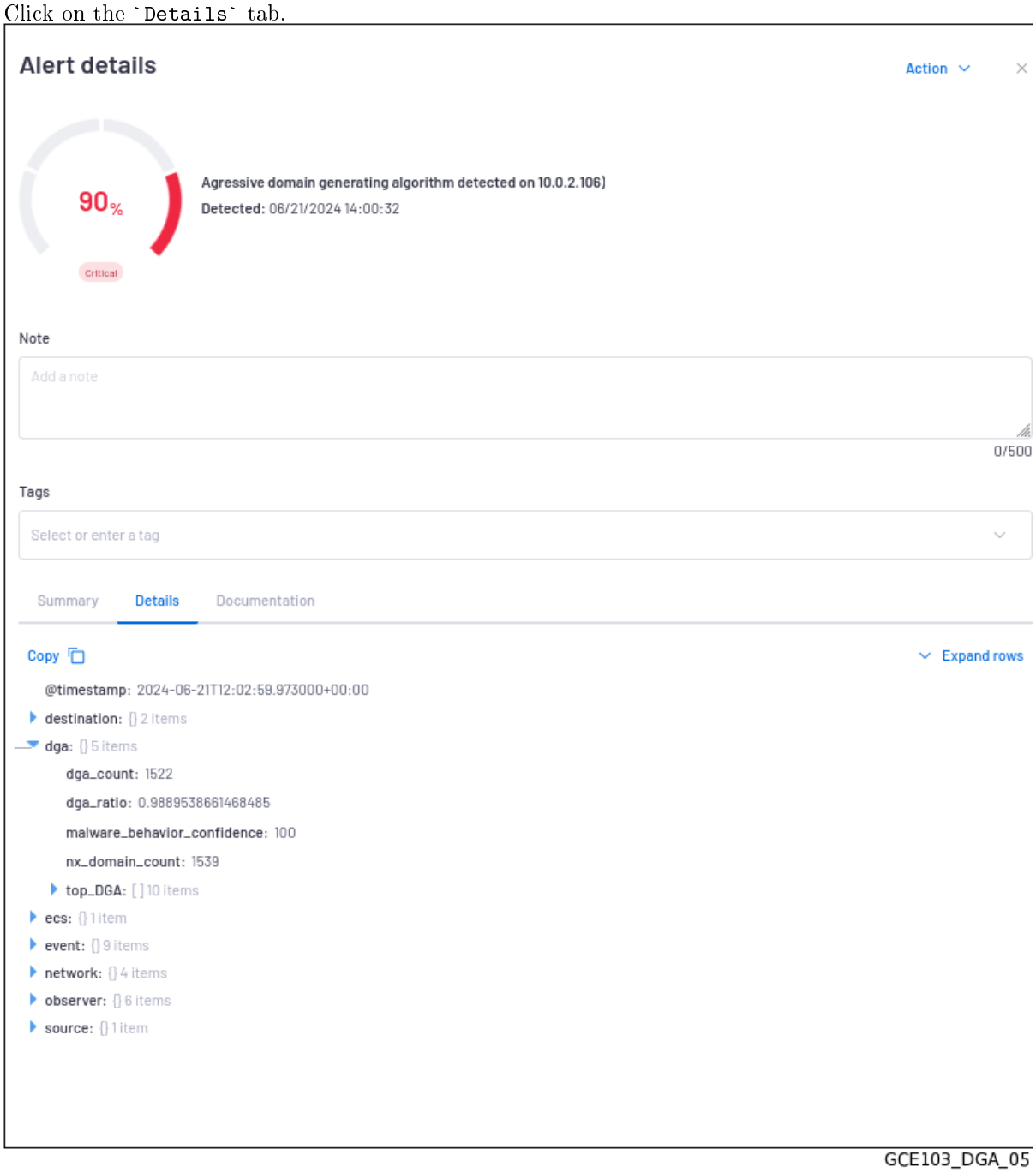
Before undertaking any investigation or qualification of the alert, it is essential to start by observing several elements that will provide essential information to understand the context of the alert.
These elements can be found either in the **WebUI** interface or in the **Kibana UI** interface.

- In the main interface named **WebUI** of the GCenter.
  - Open the `Alert details` window.
    The detailed procedure is given below.



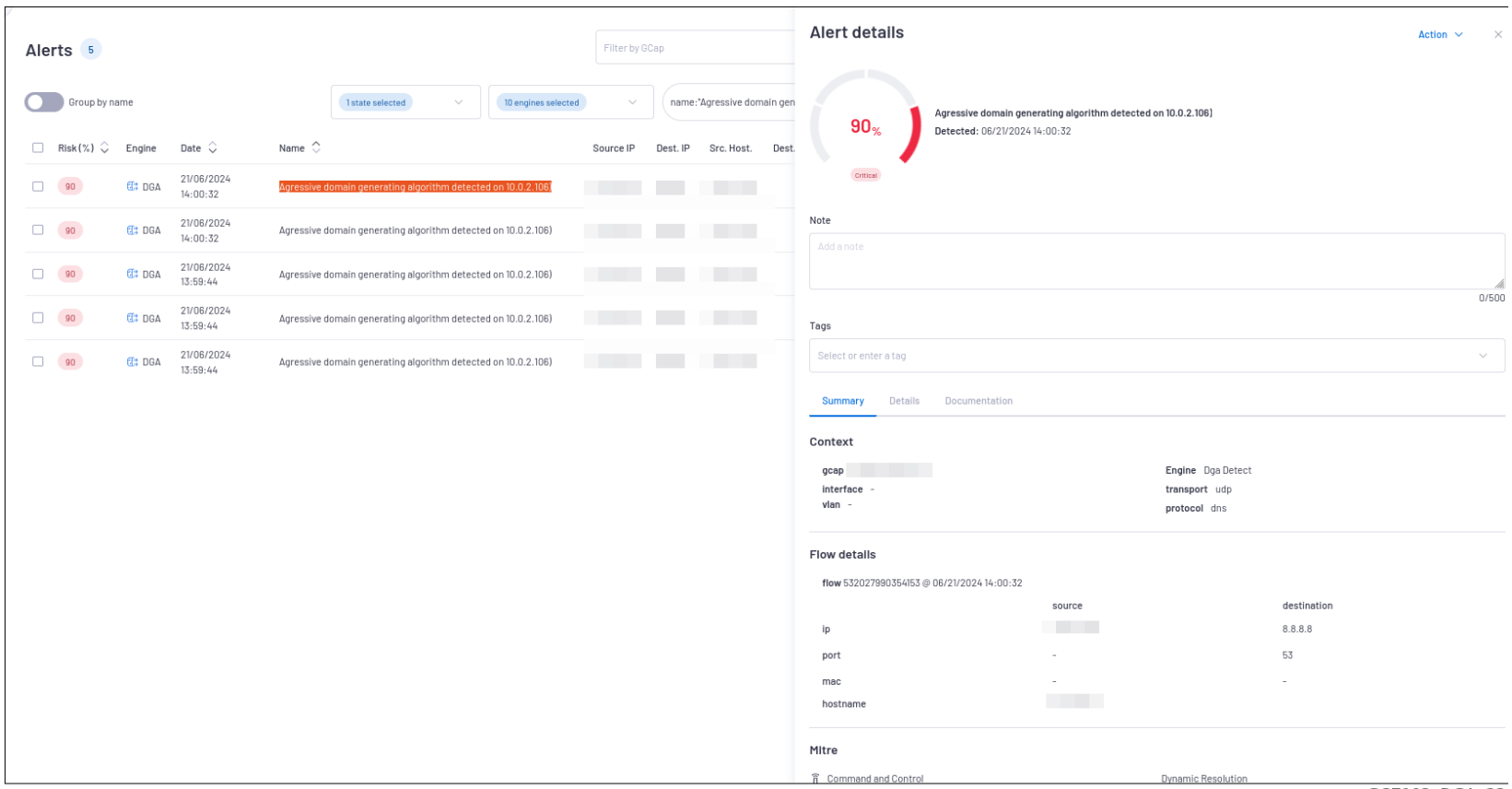
GCE103_DGA_22

- Click on the `Details` tab.



GCE103_DGA_05

- In the **Kibana UI** interface
  - Open the `Expanded document` window of the alert displayed on the `Alerts- DGA - Overview` window. The detailed procedure is given below.



GCE103_DGA_22

- Click on the toggle icon on the left of the alert.
  The expanded document is displayed.

The following key elements are:

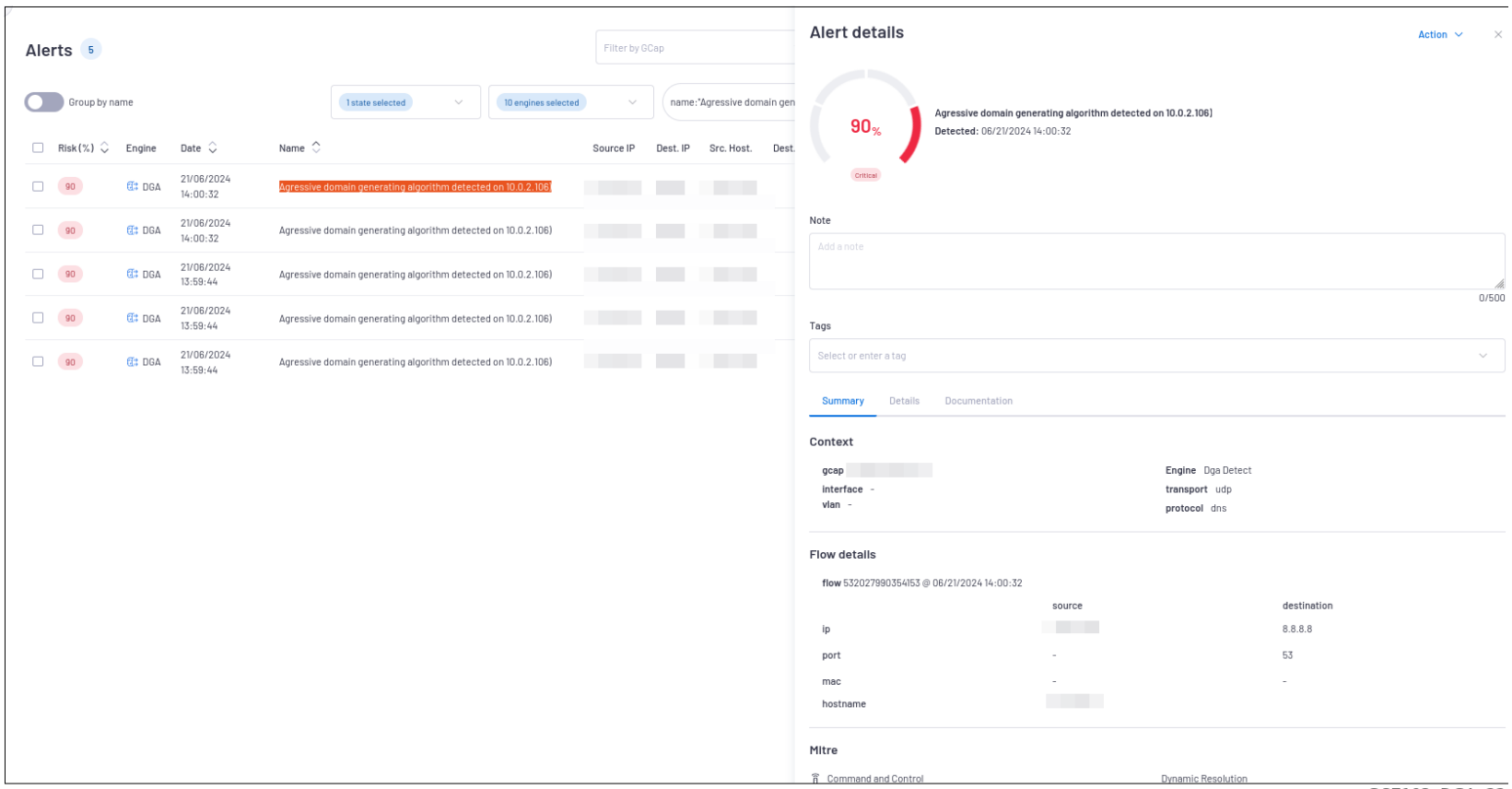
```
"dga" : {
    "nx_domain_count" : int,
    "dga_count": int,
    "dga_ratio" : float,
    "malware_behavior_confidence" : int,
    "top_DGA" : [
 ]
}
```

7.5.5.2 Alert handling procedure

7.5.5.2.1 How do you verify the accuracy of an alert and determine if it represents a real threat?

To assess the accuracy of an alert and determine whether it represents a real threat, several steps can be taken.
Here is an overview of the actions frequently taken when analyzing an alert generated by the DGA detect engine:

- In the **WebUI**, click on the alert to be analyzed in the `Alert details` window of the `Alert` screen.



GCE103_DGA_22

Domain names produced by a Domain Generating Algorithm (DGA) (whose top 10 appears in the top_DGA list of an alert) can be an indication that an alert is a false positive:

- In particular, if the domain names (and in particular the corresponding root domain) that appear are client-specific
- If a healthy domain name (or root domain) often triggers an alert then it is possible to add it to the ignore list

Note:

In the case where there is no indication to conclude, it is difficult to assess whether a domain name is a DGA or not.
A thorough analysis (especially on root domains) can give indications (for example, with experience, on the DGA family concerned).

7.5.5.2.2 How to categorize the threat based on the information collected?

To categorize the threat, **verify the original IP address**:

- If the alert is linked to an external IP address, review the reputation level of that address.
  An IP address with a bad reputation is more likely to be associated with malicious activity.
- Note also that just because it is an internal IP address does not make it a false positive.
- Analyze the domains from "top_DGA":
  - If they are internal, it is likely a false positive.
  - If they seem unusual or have a poor score reputation according to external resource, the investigation has to be continued.
- Is the host the only one having requested these strange domains ? If they are often requested by many asset, it could be a global misconfiguration.
- Analyze the behavior of the host : are NXDOMAIN answer usual? Does it seam that an unusual event has occurred? Are there new alerts of new behavior on the host since the DGA alert has been created?

7.5.5.2.3 What answers are needed if the threat is confirmed?

Note:

This procedure allows to deepen the investigation and assess the extent of the incident after confirmation of a threat generated by the DGA detect engine.

- **Isolate the system**: immediately isolate the contaminated system and ensure it cannot cause further damage.
- **Notify**: inform relevant parties of threat detection.
- **Collect information**: gather essential information such as source IP address.
- **Neutralize the threat** by deleting the file, blocking the original IP address, etc.
- **Reverse engineering (if necessary)**: if the threat is particularly complex, reverse engineering can be considered to understand in depth its internal functioning.

This can help identify exploited vulnerabilities and propagation mechanisms.
- **Analyze logs**: review system and network logs to trace the spread of the threat.
- **Cut off access to C&C**: possibly cut off communications with C&C if we can locate the DGA domain name that has been resolved and thus find the IP address of the attacker's server.
  However, by principle of the use of DGAs, this cut is effective only in the short term (in practice, less than a day).

7.5.5.2.4 What if an alert from this engine is identified as a false positive?

If an alert from this engine is identified as a recurring false positive, it is recommended to add the file to the `Ignore list`.
See the *Managing the Ignore list of the Malcore engine* procedure.

7.5.6 Analyzing the Malcore retroanalyzer alerts

7.5.6.1 Introduction

For information, see the following paragraphs:

- *For what types of threats is this engine designed?*
- *How does this particular engine detect threats?*
- *How does Malcore retroanalyzer work in the GCenter?*

7.5.6.1.1 Management of the Malcore retroanalyzer engine

For engine informations, see the paragraph *Viewing the engine status*
For information on engine upgrade, see the paragraph *Engine update*
For information on engine configuration, see the paragraph *Configuration of Malcore retroanalyzer engine*

7.5.6.1.2 Events generated by the engine

Events generated by the Malcore retroanalyzer engine are **alerts** only.
Alerts are displayed in the `Alerts` screen and are displayed as detected by the Malcore engine.

7.5.6.1.3 Essential information to understand the context of the alert

For more information about the way these events are displayed or how to analyze these kinds of event please refer to the *Analyzing the Malcore alerts*.

7.5.6.2 Alert handling procedure

Refer to the *Analyzing the Malcore alerts*.

7.5.7 Analyzing the Active CTI alerts

7.5.7.1 Introduction

For information, see the following paragraphs:

- *For what types of threats is this engine designed?*
- *How does this particular engine detect threats?*
- *How does Active CTI work in the GCenter?*

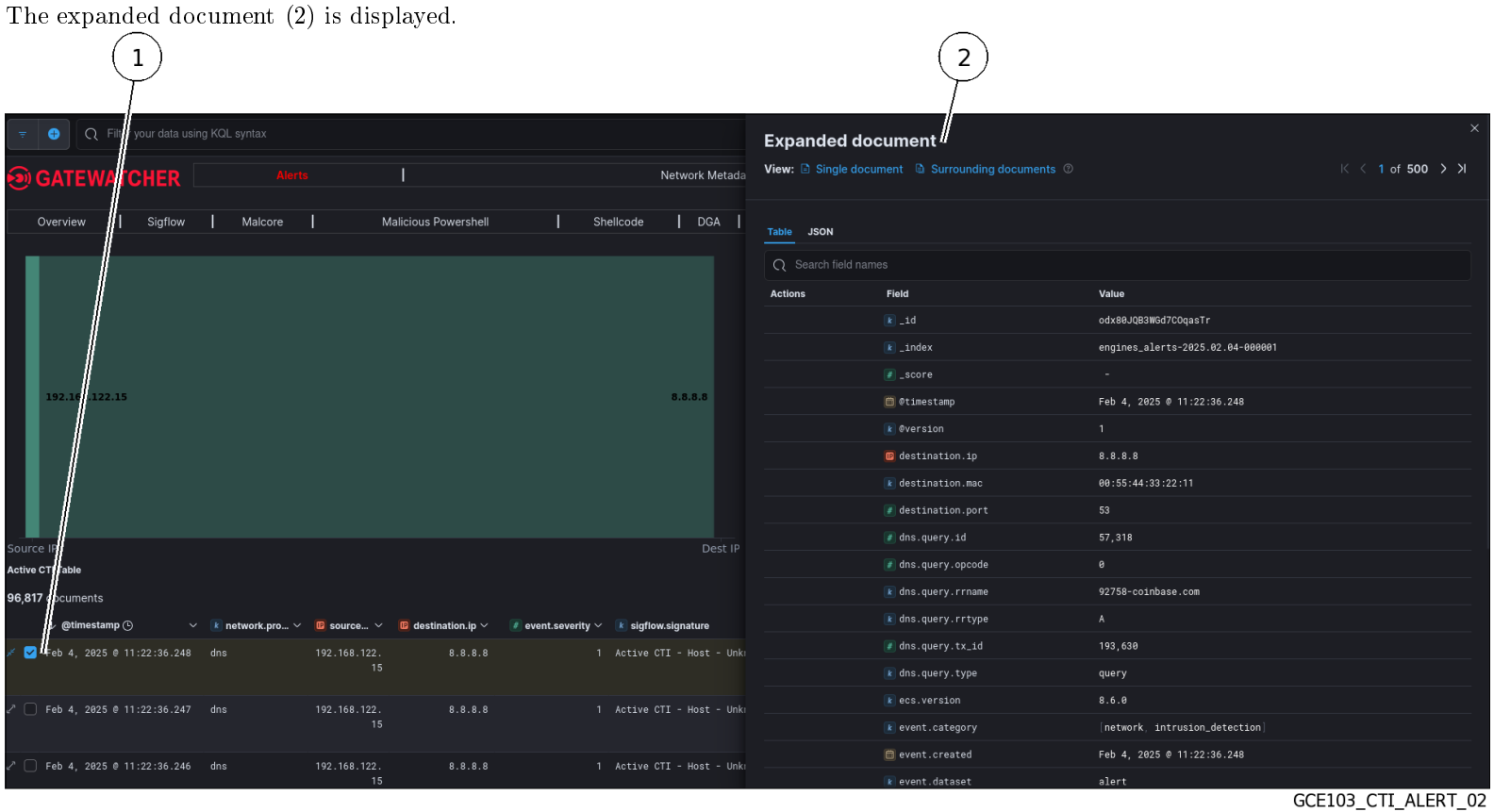
7.5.7.1.1 Management of the Active CTI engine

For engine informations, see the paragraph *Viewing the engine status*
For information on engine upgrade, see the paragraph *CTI update*
For information on engine configuration, see the paragraph *Active CTI engine configuration*

7.5.7.1.2 Events generated by the engine

Events generated by the engine are **alerts** of the Sigflow type.
They will therefore be available in the ACTIVE CTI dashboards.
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
  - To view the alerts, select the `Active CTI` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.
  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed in *Example of an Active CTI alert in Kibana*.
    The displayed counters are given in the *Engine log data structure* appendix.
- In the interface named **Kibana UI**:
  - In the main interface **WebUI**, click on the `Hunting` icon.
    The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).
  - Click on the `Active CTI` category of the `Alerts` section then the `Overview` or `Messages` tab.
- To consult information about a specific alert:
  - Click on the toggle icon (1) on the left of the Alert.
    The expanded document (2) is displayed.



GCE103_CTI_ALERT_02

The detailed information of this alert can be viewed in table or json format (see the *Active CTI logs data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

Active CTI alerts are alerts that can be filtered by searching for the term *event.module: active_ cti* in the Kibana search bar.

Note:

The **Kibana UI** can also be accessed without any filters via the `Hunting` icon on the left side menu bar in the WebUI.

7.5.7.1.3 Essential information to understand the context of the alert

7.5.7.1.3.1 What are the key fields of an alert and their meaning?

In order to undertake the investigation or qualification of the alert, it is necessary to search for the IoC on the OpenCTI platform of Gatewatcher CTI to obtain more information about the threat and understand the context.
To do this, you must first determine what the IoC is:

- If the alert is raised on a DNS packet, the value of the IoC is in the ``dns.query.rrname`` field of the alert
- If the alert is raised on an HTTP packet, the value of the IoC is in the ``http.hostname`` field of the alert

Note:

These elements can be found in the `Alert details` window.

It is also possible to search for IoC on the OpenCTI platform.
To this end:

- Search for the IoC value in the general search bar at the top right of the home page
- then select the IoC from the IoC present after searching

On the IoC page, you can find:

- Its description

  The IoC description consists of:
  - Its value
  - The type of IoC

    In the case of an ActiveCTI alert, alerts are associated with domains or URLs, but generally the platform includes file hashes, file names and IPs.
- If **Detection** or not, see the *Alert handling procedure*
- Its labels, which may correspond to:
  - The type of threat involved

    This field can take different values including **phishing**, **trojan**, **hacktool** depending on how the threat was categorized by Gatewatcher CTI.
  - On behalf of the associated malware

    In the case of a file hash or a URL or domain that downloads a file, if that file is categorized as belonging to a malware family, then the name will appear in the labels.

    For example: **mirai**, **qbot**, **redline stealer**.
  - On behalf of the associated threat actor

    In the same way as for malware, if the threat is associated with a threat actor, its name will appear in the labels.

    For example: **ta505**, **lockbit**, **lazarus group**.
- Its external references

  These are external articles or analyzes in which the IoC is present and which provide additional context.

7.5.7.2 Alert handling procedure

7.5.7.2.1 How do you verify the accuracy of an alert and determine if it represents a real threat?

To assess the accuracy of an alert and determine whether it represents a real threat, several steps can be taken.
Here is an overview of the actions frequently taken when analyzing a generated alert.
The first item to check is the usage_mode field of the alert in Kibana.
It can take two values: `detection` or `hunting`.

- If the usage_mode of the IoC mode has the `hunting` value which may be the case for a domain or an IP address, it means that the resource has not been contacted anymore.
  On a network, this can happen for example when a malicious resource tries to contact a domain that is no longer active.
- On the other hand, if the usage_mode has the `detection` value, the IoC is still active and represents in this case a current threat.

7.5.7.2.2 How to categorize the threat based on the information collected?

To categorize the threat, explore several avenues:

- **Check the threat type**:
  - In the case of a URL or domain, the associated threats are most often phishing or downloading a malicious file.
    This information is present in the IoC labels.
    If the labels do not determine the type of threat, the IoC value can give the information.
    Phishing URLs usually contain keywords that betray an attempt to spoof a service or company, where downloading a malicious file is often done from an IP and whose file name can be specified in the path.
    In other cases, IoC may refer to a domain of **Command and Control**, characterized by a specific malware name.
- **Search for threat on external CTI platforms**:
  - For more information on the level of malicious activity or to download the threat in which of a file, turn to external Threat Intelligence platforms such as VirusTotal or MalwareBazaar.
- **Verify the original IP address of the alert in the GCenter**:
  - If the alert is linked to an external IP address, review the reputation level of that address.
    An IP address with a bad reputation is more likely to be associated with malicious activity.
  - Note also that just because it is an internal IP address does not make it a false positive.
- **View the alert history**:
  - View the history of similar alerts generated by ActiveCTI.
    If similar alerts have been confirmed as real threats in the past, it increases the likelihood that the current alert is also a threat.
    Depending on the observations, the threat can be categorized as real or not.
  - If necessary, use the *File transactions* functionality presented in the previous paragraph to obtain the majority of this information via a condensed view.

7.5.7.2.3 What answers are needed if the threat is confirmed?

Note:

This procedure allows further investigation and evaluation of the extent of the incident after confirmation of a threat generated by the ActiveCTI engine.

In general, it is appropriate to:

- **Determine extent of infection**: identify machines infected by the threat
- **Isolate the system**: immediately isolate the contaminated system and ensure it cannot cause further damage
- **Notify**: inform relevant parties of threat detection

Depending on the case, different approaches are taken:

- if the threat is a domain or IP associated with the download of a malicious resource, in this case it is probably the transfer of a malicious tool to or within the infected environment:
  - Remove file or malware from infected machine(s)
  - Scan the machine from which the request was made to the malicious server, which would have been infected before the request
- if the threat is associated with a **Command and Control** server, this implies that one or more infected machines communicate with the said server:
  - Remove the malicious tag that originated communications to the infected machine(s) server
- if the threat is associated with phishing:
  - Identify the target of phishing
  - Ask the employee or employees about the details of the attack to assess the extent of the information communicated to the attacker

In a second step, it is also necessary to look at the relations associated with the IoC via the *relations* field or via the *external_links* for:

- Anticipate the actions of the attacker
- Monitor / block IoC related items

7.5.7.2.3.1 What if an alert from this engine is identified as a false positive?

If an alert from this engine is identified as a recurring false positive, it is recommended to *mute* the alert signed. There is no whitelist for the Active CTI engine.

7.5.8 Analyzing the Retrohunt alerts

7.5.8.1 Introduction

For information, see the following paragraphs:

- *For what types of threats is this engine designed?*
- *How does this particular engine detect threats?*
- *How does Retro hunt work in the GCenter?*

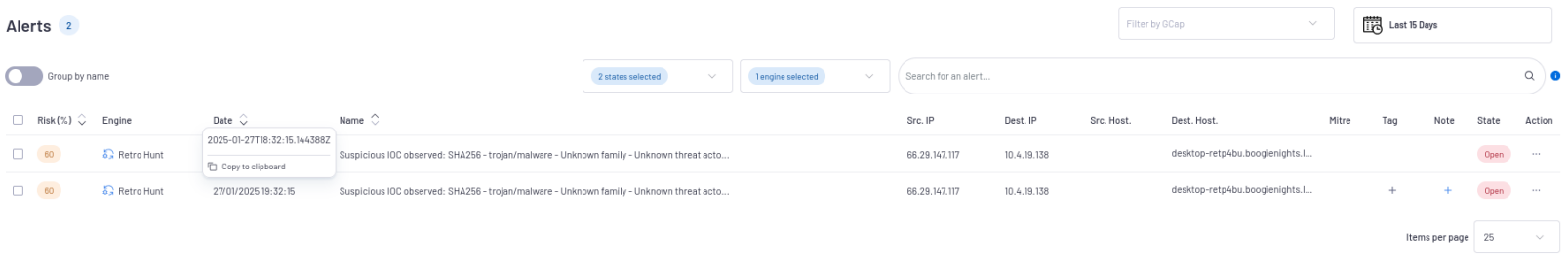
7.5.8.1.1 Management of the Retrohunt engine

For engine informations, see the paragraph *Viewing the engine status*
For information on engine upgrade, see the paragraph *CTI update*
For information on engine configuration, see the paragraph *Engine configuration*

7.5.8.1.2 Events generated by the engine

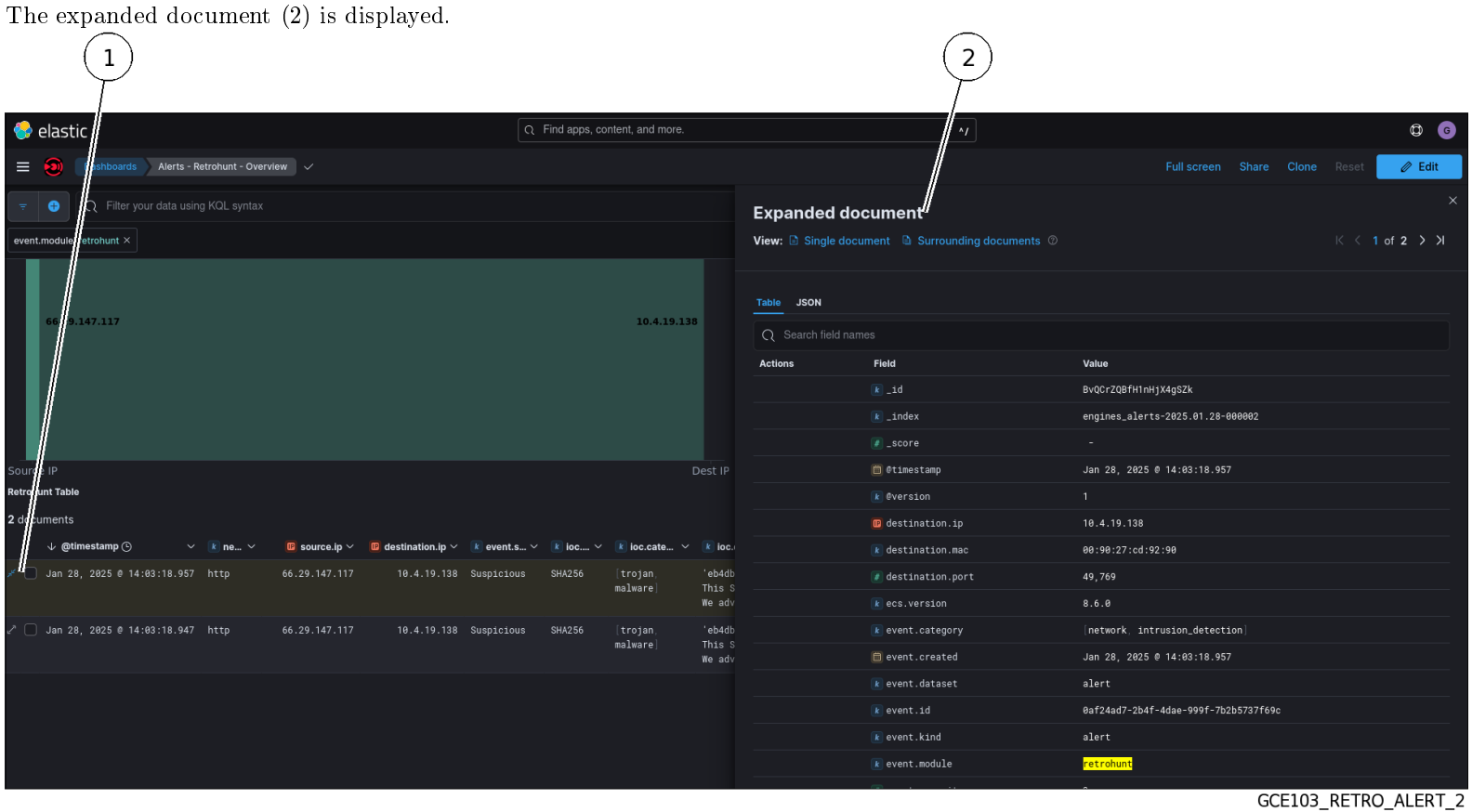
Events generated by the Retrohunt engine are **alerts**.
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen:
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
- To view only these alerts, select the `Retrohunt` engine filter.
  See the presentation of the *WebUI `Alerts` screen*.



- Click on the selected alert.
  The `Alert details` window is displayed
  The detailed information of this alert is displayed in *Example of a Retro hunt alert in the WebUI*.
- In the interface named **Kibana UI**:
  - Click on the `Hunting` icon on the left side menu bar in the WebUI.
    The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).
  - Select the `Retro hunt` category of the `Alerts` section in Kibana then the `Overview` or the `Messages` tab.
  - Click on the `Messages` tab.
- To consult information about a specific alert:
  - Click on the toggle icon (1) on the left of the Alert.

The expanded document (2) is displayed.



GCE103_RETRO_ALERT_2

The detailed information of this alert can be viewed in table or json format (see the *Retro hunt logs data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

7.5.8.1.3 Essential information to understand the context of the alert

7.5.8.1.3.1 What are the key fields of an alert and their meaning?

In order to undertake the investigation or qualification of the alert, it is necessary to search for the IoC on the OpenCTI platform of Gatewatcher CTI to obtain more information about the threat and understand the context.
To do this, you must first determine what the IoC is:

- If the alert is raised on a DNS packet, the value of the IoC is in the ``dns.query.rrname`` field of the alert
- If the alert is raised on an HTTP packet, the value of the IoC is in the ``http.hostname`` field of the alert

> **Note:**
>
> These elements can be found in the `Alert details` window.

It is also possible to search for IoC on the OpenCTI platform.
To this end:

- Search for the IoC value in the general search bar at the top right of the home page
- then select the IoC from the IoC present after searching

On the IoC page, you can find:

- Its description
  The IoC description consists of:
  - Its value
  - The type of IoC
    In the case of an ActiveCTI alert, alerts are associated with domains or URLs, but generally the platform includes file hashes, file names and IPs.
- If **Detection** or not, see the *Alert handling procedure*
- Its labels, which may correspond to:
  - The type of threat involved
    This field can take different values including **phishing**, **trojan**, **hacktool** depending on how the threat was categorized by Gatewatcher CTI.

  - On behalf of the associated malware

    In the case of a file hash or a URL or domain that downloads a file, if that file is categorized as belonging to a malware family, then the name will appear in the labels.

    For example: **mirai**, **qbot**, **redline stealer**.
  - On behalf of the associated threat actor

    In the same way as for malware, if the threat is associated with a threat actor, its name will appear in the labels.

    For example: **ta505**, **lockbit**, **lazarus group**.
- Its external references

  These are external articles or analyzes in which the IoC is present and which provide additional context.

In the information displayed in the Kibana alerts, the key elements include:

- `` `type` ``

  This is the type of IoC reported. This field can be SHA256, SHA1, MD5, Filename, URL, Host.
- `` `value` ``

  Corresponds to the value of the IoC, that is, the IoC itself.
- `` `signature` ``

  When available, the signature consists of the following fields:
  - `` `type` ``: if it is a hash, an IP, a domain.
  - `` `categories` ``: threat category corresponding to the IoC. For example: phishing, trojan, ransom, backdoor.
  - `` `families` ``: malware family corresponding to IoC. For example: Cobalt Strike, Mirai, gh0st RAT.
  - `` `threat_actor` ``: threat actor associated with IoC. For example: TA505, Medusa, SilverTerrier.
  - `` `relations` ``: corresponds to other IoCs present in the platform associated with IoC.

7.5.8.2 Alert handling procedure

7.5.8.2.1 How do you verify the accuracy of an alert and determine if it represents a real threat?

To assess the accuracy of an alert and determine whether it represents a real threat, several steps can be taken.
Here is an overview of the actions frequently taken when analyzing a generated alert.
The first item to check is the usage_mode field of the alert in Kibana.
It can take two values: `` `detection` `` or `` `hunting` ``.

- If the usage_mode of the IoC mode has the `` `hunting` `` value which may be the case for a domain or an IP address, it means that the resource has not been contacted anymore.

  On a network, this can happen for example when a malicious resource tries to contact a domain that is no longer active.
- On the other hand, if the usage_mode has the `` `detection` `` value, the IoC is still active and represents in this case a current threat.

7.5.8.2.2 How to categorize the threat based on the information collected?

To categorize the threat, explore several avenues:

- **Check the threat type**:
  - In the case of a URL or domain, the associated threats are most often phishing or downloading a malicious file.

    This information is present in the IoC labels.

    If the labels do not determine the type of threat, the IoC value can give the information.

    Phishing URLs usually contain keywords that betray an attempt to spoof a service or company, where downloading a malicious file is often done from an IP and whose file name can be specified in the path.

    In other cases, IoC may refer to a domain of **Command and Control**, characterized by a specific malware name.
- **Search for threat on external CTI platforms**:
  - For more information on the level of malicious activity or to download the threat in which of a file, turn to external Threat Intelligence platforms such as VirusTotal or MalwareBazaar.
- **Verify the original IP address of the alert in the GCenter**:
  - If the alert is linked to an external IP address, review the reputation level of that address.

    An IP address with a bad reputation is more likely to be associated with malicious activity.
  - Note also that just because it is an internal IP address does not make it a false positive.
- **View the alert history**:
  - View the history of similar alerts generated by ActiveCTI.

    If similar alerts have been confirmed as real threats in the past, it increases the likelihood that the current alert is also a threat.

    Depending on the observations, the threat can be categorized as real or not.
  - If necessary, use the *File transactions* functionality presented in the previous paragraph to obtain the majority of this information via a condensed view.

7.5.8.2.3 What answers are needed if the threat is confirmed?

Note:

This procedure allows further investigation and evaluation of the extent of the incident after confirmation of a threat generated by the ActiveCTI engine.

In general, it is appropriate to:

- **Determine extent of infection**: identify machines infected by the threat
- **Isolate the system**: immediately isolate the contaminated system and ensure it cannot cause further damage
- **Notify**: inform relevant parties of threat detection

Depending on the case, different approaches are taken:

- if the threat is a domain or IP associated with the download of a malicious resource, in this case it is probably the transfer of a malicious tool to or within the infected environment:
  - Remove file or malware from infected machine(s)
  - Scan the machine from which the request was made to the malicious server, which would have been infected before the request
- if the threat is associated with a **Command and Control** server, this implies that one or more infected machines communicate with the said server:
  - Remove the malicious tag that originated communications to the infected machine(s) server
- if the threat is associated with phishing:
  - Identify the target of phishing
  - Ask the employee or employees about the details of the attack to assess the extent of the information communicated to the attacker

In a second step, it is also necessary to look at the relations associated with the IoC via the *relations* field or via the *external_links* for:

- Anticipate the actions of the attacker
- Monitor / block IoC related items
- If the threat is a hash corresponding to a file:
  - Neutralize the threat by deleting the file, blocking the original IP address, etc.
  - Dynamic analysis: if possible, run the file in a secure environment (sandbox) to observe its behavior (a GBox for example).
  - Reverse engineering (if necessary): if the threat is particularly complex, reverse engineering can be considered in order to fully understand its internal functioning.
    This can help identify exploited vulnerabilities and propagation mechanisms.
  - Analyze the logs: review system and network logs to trace threat spread.

In a second step, it is also necessary to look at the relations associated with the IoC via the *relations* field or via the *external_links* for:

- Anticipate the actions of the attacker
- Monitor / block IoC related items

7.5.8.2.3.1 What if an alert from this engine is identified as a false positive?

If an alert from this engine is identified as a recurring false positive, it is recommended to *mute* the alert signed. There is no whitelist for the Retro hunt engine.

7.5.9 Analyzing the Ransomware detect alerts

7.5.9.1 Introduction

For information, see the following paragraphs:

- *For what types of threats is this engine designed?*
- *How does this particular engine detect threats?*
- *How does Ransomware detect work in the GCenter?*

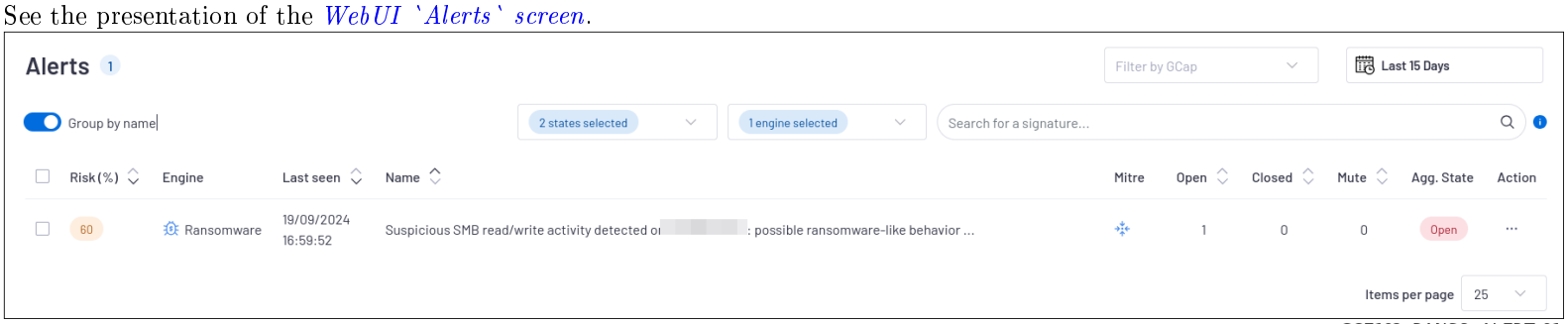
7.5.9.1.1 Management of the Ransomware detect engine

For engine informations, see the paragraph *Viewing the engine status*
For information on engine upgrade, see the paragraph *Engine update*
For information on engine configuration, see the paragraph *Ransomware detect configuration and management of the ignored list feature*

7.5.9.1.2 Events generated by the engine

Events generated by the Ransomware engine are **alerts**.
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
  - To view the alerts, select the `Ransomware` filter and view the list of alerts
    See the presentation of the *WebUI `Alerts` screen*.

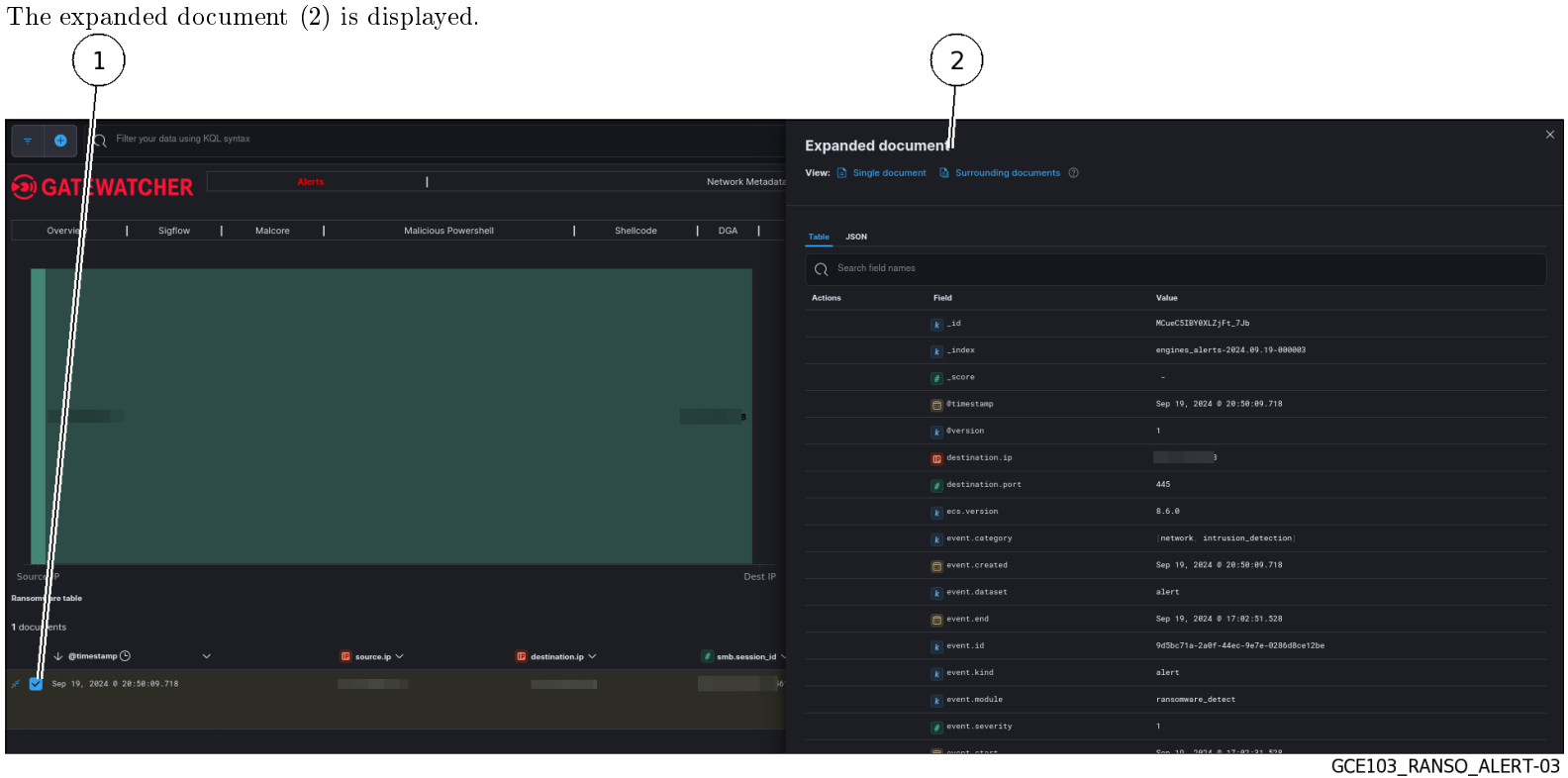


GCE103_RANSO_ALERT-01

  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed in *Example of Ransomware detect alert in the WebUI*.
- In the interface named **Kibana UI**
  - In the main interface **WebUI**, to view the alerts, select the `Ransomware` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.
  - After selecting the alert, click on the `Open host SMB activity` command of the `Actions` menu.
    Kibana is opened on the `Ransomware` category of the `Alerts ` section.
    The interface displayed is the interface named **Kibana UI** (described in the *Overview of the Kibana GUI*).

    In the `Overview` tab, the database is filtered on the `source.ip:` parameter.

- Click on the toggle icon (1) on the left of the Alert.
  The expanded document (2) is displayed.



GCE103_RANSO_ALERT-03

The detailed information of this alert can be viewed in table or json format (see the *Ransomware detect log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

Note:

The **Kibana** user interface is also accessible without a filter via the `Hunting` icon in the left menu bar.

7.5.9.1.3 Essential information to understand the context of the alert

7.5.9.1.3.1 What are the key fields of an alert and their meaning?

Before undertaking any investigation or qualification of the alert, it is essential to begin by observing several elements that will provide essential information to understand the context of the alert. These elements can be found either in the **WebUI** interface or in the **Kibana UI** interface (for more information, refer to the previous paragraph).
Each global Ransomware detect engine alert is associated with an SMB session.
In the information displayed on the Kibana `Alerts` screen, these key elements include:

```
"ransomware" : {
    "session_id" : int,
    "score" : int,
    "alert_threshold" : int
}
```

7.5.9.2 Alert handling procedure

7.5.9.2.1 How do you verify the accuracy of an alert and determine if it represents a real threat?

The session contains at least one READ and one WRITE.
In particular, an SMB session with only READ commands cannot be a ransomware.

To assess the accuracy of an alert and determine whether it represents a real threat, several steps can be taken.
Here is an overview of the actions frequently taken when analyzing an alert generated by the Ransomware detect engine:

- Click on the alert to be analyzed in the `Alerts` screen of the main WebUI interface.
- Click on the `Open host SMB activity` command of the `Actions` menu.
- Analyze the corresponding SMB session in Kibana, over the time period corresponding to the alert:
  - Filter *READ* and *WRITE* commands
  - If the session contains only *READ*` (+), then it cannot be a *ransomware*, so it is a **false positive**
  - If file names are accessible, see if a particular extension (suffix) was added in the write events.
    Some *ransomware* use specific extensions. Public extension lists of known *ransomware* are available:
    - https://github.com/mthcht/awesome-lists/blob/main/Lists/ransomware_extensions_list.csv

(+) this case can happen if the SMB session is very different from those seen during training.
In this case it is considered an anomaly.

7.5.9.2.2 How to categorize the threat based on the information collected?

To categorize the threat, explore several avenues:

- **Verify original IP address**:
  - If the alert is linked to an external IP address, review the reputation level of that address.
    An IP address with a bad reputation is more likely to be associated with malicious activity.
  - Note also that just because it is an internal IP address does not make it a false positive.

7.5.9.2.3 What answers are needed if the threat is confirmed?

Note:

This procedure allows further investigation and assessment of the extent of the incident after confirmation of a threat generated by the Ransomware detect engine

- **Isolate the system**: immediately isolate the contaminated system and ensure it cannot cause further damage
- **Notify**: inform relevant parties of threat detection
- **To do**: identify the *malware* (*ransomware*) on the target workstation: use the NDR
- **Neutralize the threat** by deleting the file, blocking the original IP address, etc.
- **Analyze logs**: review system and network logs to trace the spread of the threat

---

7.5.9.2.4 What if an alert from this engine is identified as a false positive?

If an alert from this engine is identified as a recurring false positive, it is recommended to add the source IP to the whitelist.

7.5.10 Analyzing the Beacon detect alerts

7.5.10.1 Introduction

- *For what types of threats is this engine designed?*
- *How does this particular engine detect threats?*
- *How does the Beacon detect engine work in the GCenter?*

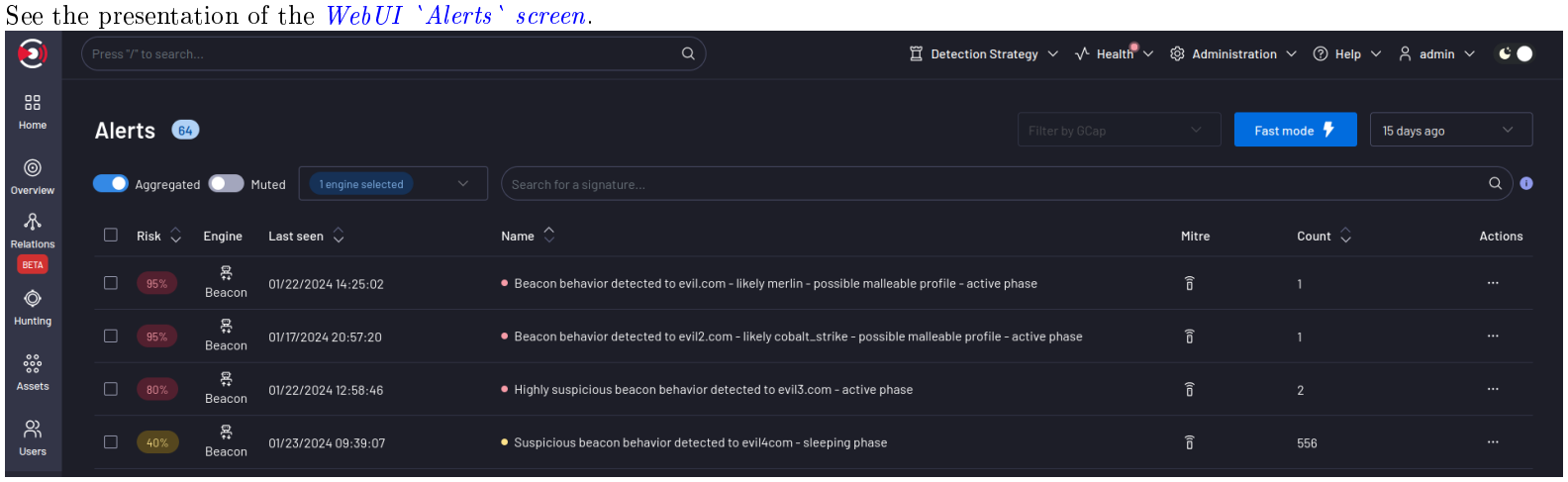
7.5.10.1.1 Management of the Beacon detect engine

For engine informations, see the paragraph see the *Viewing the engine status*.
For information on update engine, see the paragraph *Engine update*
For information on engine configuration, see the paragraph *Beacon detect configuration engine and management of the ignored destination list*

7.5.10.1.2 Events generated by the engine

Events generated by the Beacon detect engine are **alerts** only.
These are displayed:

- In the main interface named **WebUI** of the GCenter in the `Alerts` screen.
  The main interface named **WebUI** is described in the *Overview of the WEB UI*.
  - To display the beacon alerts, select the `Beacon` engine filter.
    See the presentation of the *WebUI `Alerts` screen*.

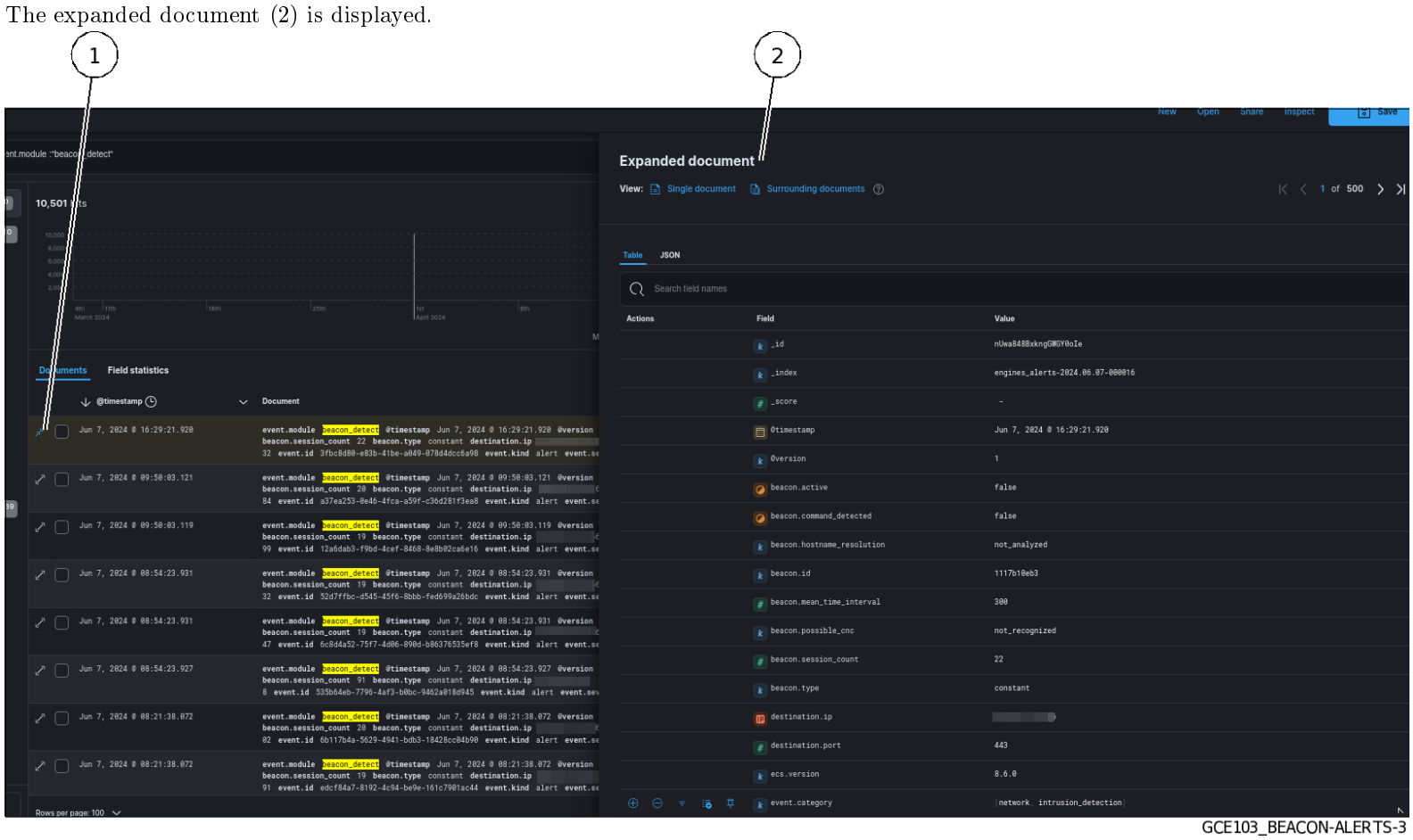


  - Click on the selected alert.
    The `Alert details` window is displayed.
    The detailed information of this alert is displayed in *Example of a Beacon detect alert in Kibana*.
- In the interface named **Kibana UI**:

- Click on the `Hunting` icon of the `WebUI`.
  The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).
- Click on the icon and then on `Discover`
- Select the `engines_alerts*` choice in the Data View
- In the search field, enter `event.module :"beacon_detect"` filter to display only the alerts of the Beacon detect engine

GCE103_BEACON-ALERTS-1

- Click on the toggle icon (1) on the left of the Alert.
  The expanded document (2) is displayed.



GCE103_BEACON-ALERTS-3

The detailed information of this alert can be viewed in table or json format (see the *Beacon detect log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

7.5.10.1.3 Essential information to understand the context of the alert

7.5.10.1.3.1 What are the key fields of an alert and their meaning in the WebUI?

Before undertaking any investigation or qualification of the alert, it is essential to start by observing several elements that will provide essential information to understand the context of the alert.
Here are the main fields displayed in the `Alerts` screen of the WebUI of the GCenter:

- `Risk`
  This is the risk score of the alert.
  It depends on the identification of detection evasion techniques used by C&C and features specific to some known C&C frameworks.
- `Name`
  This is the threat description based on the analysis. It consists of:
  - The alert severity:
    - `Beacon behavior detected to` is displayed if a specific C&C server has been identified
    - `Highly suspicious beacon behavior detected to` is displayed if a generic C&C behavior has been identified
    - `Suspicious beacon behavior detected to ` is displayed when a periodic communication pattern has been identified
  - The Server Name Indication (tls.sni)
  - The Domain
  - The destination.ip

Note:

A `malleable profile` is a configuration file used by the C&C Cobalt Strike to easily usurp a domain name.

7.5.10.1.3.2 What are the key fields of an alert and their meaning in Kibana?

In the information displayed on the Kibana `engine_alerts` screen, these key elements include:

Table 3: Beacon detect log key field table

Field	Description	Value or example
event.severity	Analysis result code	Between 1 and 3 1 = specific C&C identified 2 = Generic C&C behavior 3 = Periodic communication identified
event.module	The engine responsible for the alert	Only `beacon_detect` value is possible for Beacon Detect
beacon.mean_time_interval	Time period (in seconds) of time intervals between each communication to the server	Example: `1`
beacon.active	Presence of beacon activity markers: execution of commands or change of communication rhythm	Can take values: [`true`, `false`]
beacon.session_count	Number of sessions established between beacon and server	Example: `26096`
beacon.hostname_resolution	Analysis status to identify a C&C detection evasion method based on domain name spoofing	Can take values: [`not_analyzed`, `found`, `not_found`] `not_analyzed` = analysis disabled `found` = no spoofing detected `not_found` = spoofing detected
beacon.type	Identifies beacon as periodic or offended (escape method)	Can take values: [`constant`, `obfuscated`] `constant` = periodic communication `obfuscated` = offended periodic communication
beacon.command_detected	Presence of commands to execute that were sent to the beacon by the server	Can take values: [`true`, `false`]
beacon.possible_cnc	Identifies specific C&C detected	Can take values: [`not_recognized`, `cobalt_strike`, `caldera`, `powershell_empire`, `brute_ratel_c4`, `sliver`]

7.5.10.2 Alert handling procedure

7.5.10.2.1 How do you verify the accuracy of an alert and determine if it represents a real threat?

To assess the accuracy of an alert and determine whether it represents a real threat, several steps can be taken.

- **Correlate with other engines**
  It is interesting to check the presence of alerts from other engines based on the information identified by Beacon Detect.
  1. Note some information that may be present in other alerts.
     For example:
  - IP Source: `` `10.1.1.1` ``
  - IP Destination: `` `10.1.1.2` ``
  - Domain name: `` `example.com` ``
  - The name of the specific C&C if indicated in the beacon.possible_cnc field: `` `cobalt_strike` ``
  2. In the `` `Alerts` `` menu, select all engines except Beacon detect and filter on the collected information.
     Some examples of filters:
     - Filter 1: `` `ip:10.1.1.1` ``
     - Filter 2: `` `ip:10.1.1.2` ``
     - Filter 3: `` `dest_hostnames:example.com` ``
     - Filter 4: `` `Description:Cobalt` ``

     Note:

     It is important to note that the source IP identified by Beacon detect may have been identified by another engine as an IP Destination.

     The most suspicious alerts will be related to the compromise of the source IP: executable files, privilege elevation, connections to bad reputation IP among others.
     An alert from an engine other than Beacon detect indicating the name of a C&C will be very suspicious.
     The C2Matrix website (https://howto.thec2matrix.com/) maintains an up-to-date list of the most active C&C.
     Some behaviors, such as using self-signed certificates or using non-standard ports may also be suspicious.
     To go further, a list of the techniques used by C&C is available on the Mitre website (https://attack.mitre.org/) : Tactic Command And Control (id:TA0011).

  3. It is also possible to perform this investigation in Kibana UI.
     The previous filters then become:
  - `` `(source.ip:10.1.1.1 or destination.ip:10.1.1.2) and event.module:"sigflow_alert"` ``
  - `` `(source.ip:10.1.1.1 or destination.ip:10.1.1.2) and event.module:"sigflow_alert"` ``
  - `` `(tls.client.server_name :  "example.com" or http.hostname:"example.com") and event.module:"sigflow_alert"` ``
  - `` `sigflow.signature:*Cobalt*` ``
- **Verify domain and IP reputation identified**
  1. Check reputation of identified Source and Destination IPs.
     A public destination IP with a bad reputation will be suspicious.
     A public source IP belonging to your company and recently exposed to the Internet will be suspicious.
  2. Check the domain's presence in Kibana UI's past logs.
     A domain that appeared recently will be more suspicious than an older domain.
  3. For an external domain name: check the domain's reputation and age.
     A newly created domain will be more suspicious than an older domain.
- **Ignore list check**
  Not all periodic connections are malicious.
  Some servers may behave like a beacon by making regular connections: keep-alives, synchronization.
  Most of these legitimate servers should be identified and ignored automatically by the filters provided in the configuration menu.
  However, depending on the particular infrastructure or configuration chosen, some manual additions to the ignore list may be necessary for optimal engine operation.
  1. Check the relationship between the domain name and the company
     Let's take the example of an alert where the domain name is: `` `example1.mycompany.com` ``.
     If the `` `example1.mycompany.com` `` Top Level Domain (TLD) belongs to the company, a known business partner or a customer, it may be reasonable to add this domain name in the ignore list.

     Note:

     Warning: an attacker may use a domain name similar to those used by the company to hide. For example, missing or additional letters in the domain name will make it particularly suspicious.

  2. Internally: check the association between the IP Destination and the domain name in the IPAM

If the identified domain name is associated with the Destination IP identified in the IPAM or on internal DNS servers then it is reasonable to add this domain name in the ignore list.

7.5.10.2.2 How to categorize the threat based on the information collected?

Following the previous investigation, two cases can be distinguished:

1. No suspicious items were identified.
   In the absence of additional evidence, the alert could reasonably be considered a false positive.
   The domain name associated with the alert can then be added in the ignore list.
   If the domain name is not identified, the Destination IP address can be added to the ignore list.
2. One or more suspect elements have been identified
   Depending on the severity of the suspicious elements identified and the level of `Risk` of the alert, it will be necessary to act and respond according to the escalation procedures.
   Some examples of feasible actions are shown below.

7.5.10.2.3 What answers are needed if the threat is confirmed?

- **Isolate the system**: immediately isolate the contaminated system and ensure it cannot cause further damage
- **Notify**: inform relevant parties of threat detection
- **Collect information**: gather essential information such as IP addresses and domain name
- **Neutralize the threat** by blocking the IP address or domain of the C&C server
- **Analyze logs**: review system and network logs to trace the spread of the threat.

7.5.10.2.4 What if an alert from this engine is identified as a false positive?

If an alert from this engine is identified as a recurring false positive, it is recommended to add the domain or IP to the ignore list.
It is also possible to adjust the engine parameters to reduce its sensitivity.

7.5.11 Analyzing the Yara alerts

7.5.11.1 Introduction

For information, see the following paragraphs:

- *For what types of threats is this engine designed?*
- *How does this particular engine detect threats?*
- *How does the Yara engine work in the GCenter?*

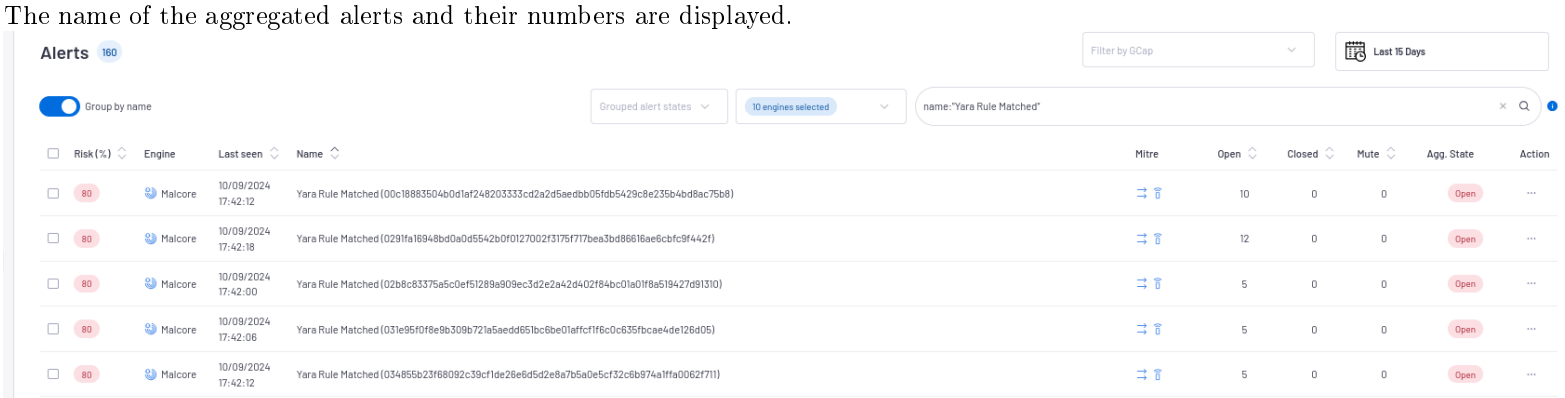
7.5.11.1.1 Management of the Yara engine

For engine informations, see the paragraph *Viewing the engine status*.
For information on engine upgrade, see the paragraph *Engine update*.
For information on engine configuration, see the paragraph *Engine configuration*.

7.5.11.1.2 Events generated by the engine

Events generated by the engine are **alerts** only.
Events generated by the Yara engine are included with the Malcore **alerts**.
These are displayed:

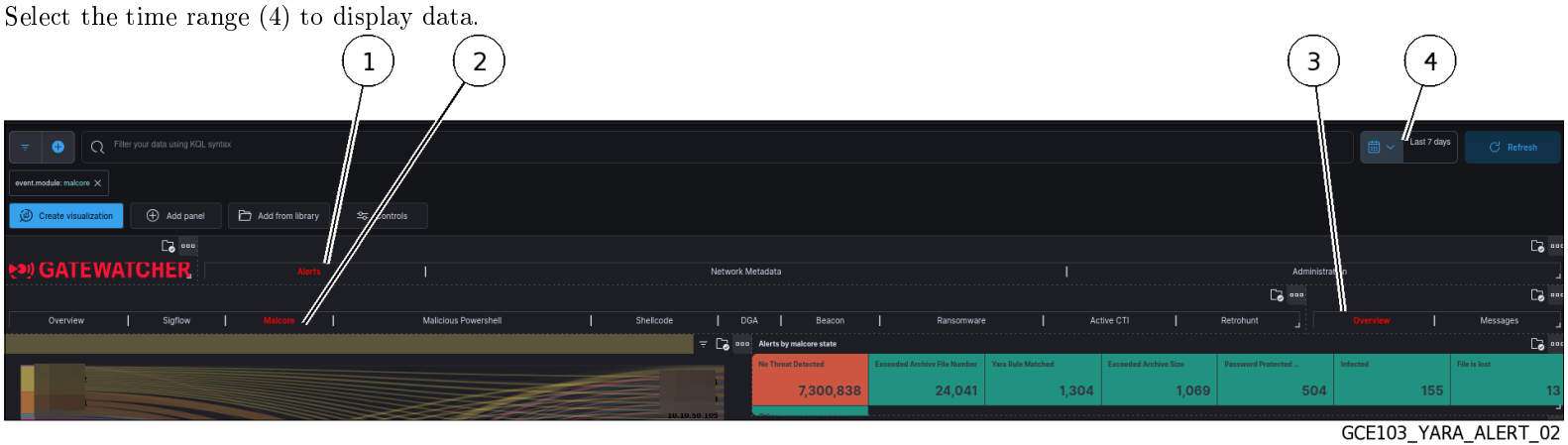
- In the main interface named **WebUI** of the GCenter in the `Alerts` screen:
  The main interface named **WebUI** is described in *Overview of the WEB UI*.
  - To filter the Yara alerts, type `name:"Yara Rule Matched"` in the search field then validate.
  - Use the `Group by name` selector to view the number of different alerts.
    The name of the aggregated alerts and their numbers are displayed.



  - Click on a grouping of alerts to display the list, if needed.
  - Disable the `Group by name` selector.
    Different Source and Destination information is displayed for each alert.
    `Tags` and `Notes` are also visible and editable.
    The various Quick Access `Actions` are available for each alert.
  - Click on an alert.

    The detailed information of this alert is displayed in *Example of an Yara alert in the WebUI*.

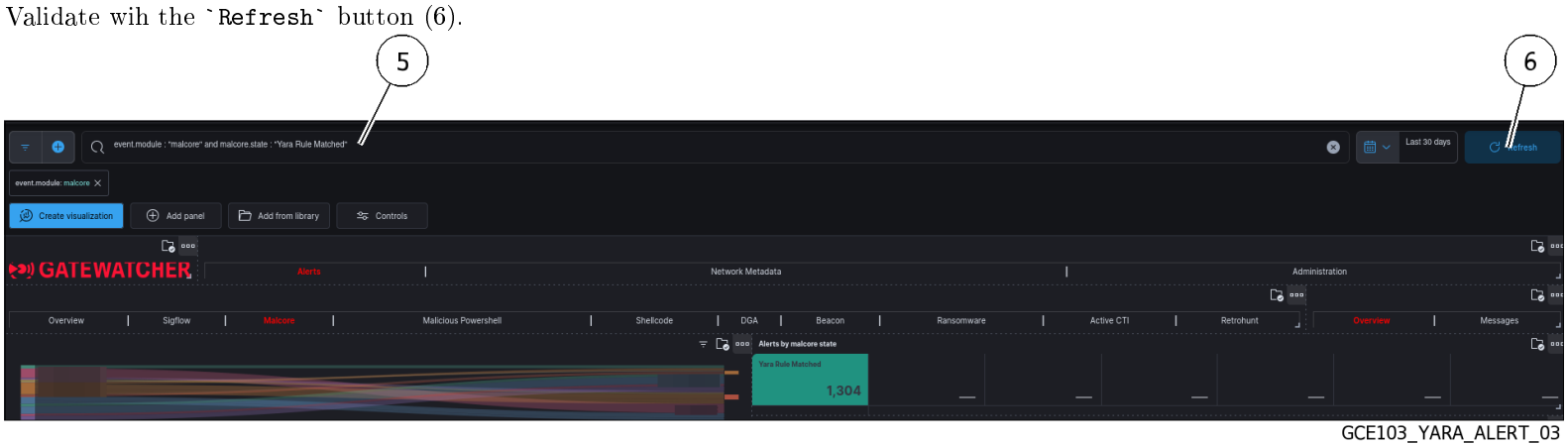
- In the **Kibana UI** interface
  - To view all Yara alerts:
  - In the main interface **WebUI**, click on the `Hunting` icon.
  - Click on the `Malcore` tab (2) of the `Alerts` category (1).
  - Select the `Overview` tab (3).
  - Select the time range (4) to display data.



GCE103_YARA_ALERT_02

See the presentation of the *WebUI `Alerts` screen*.

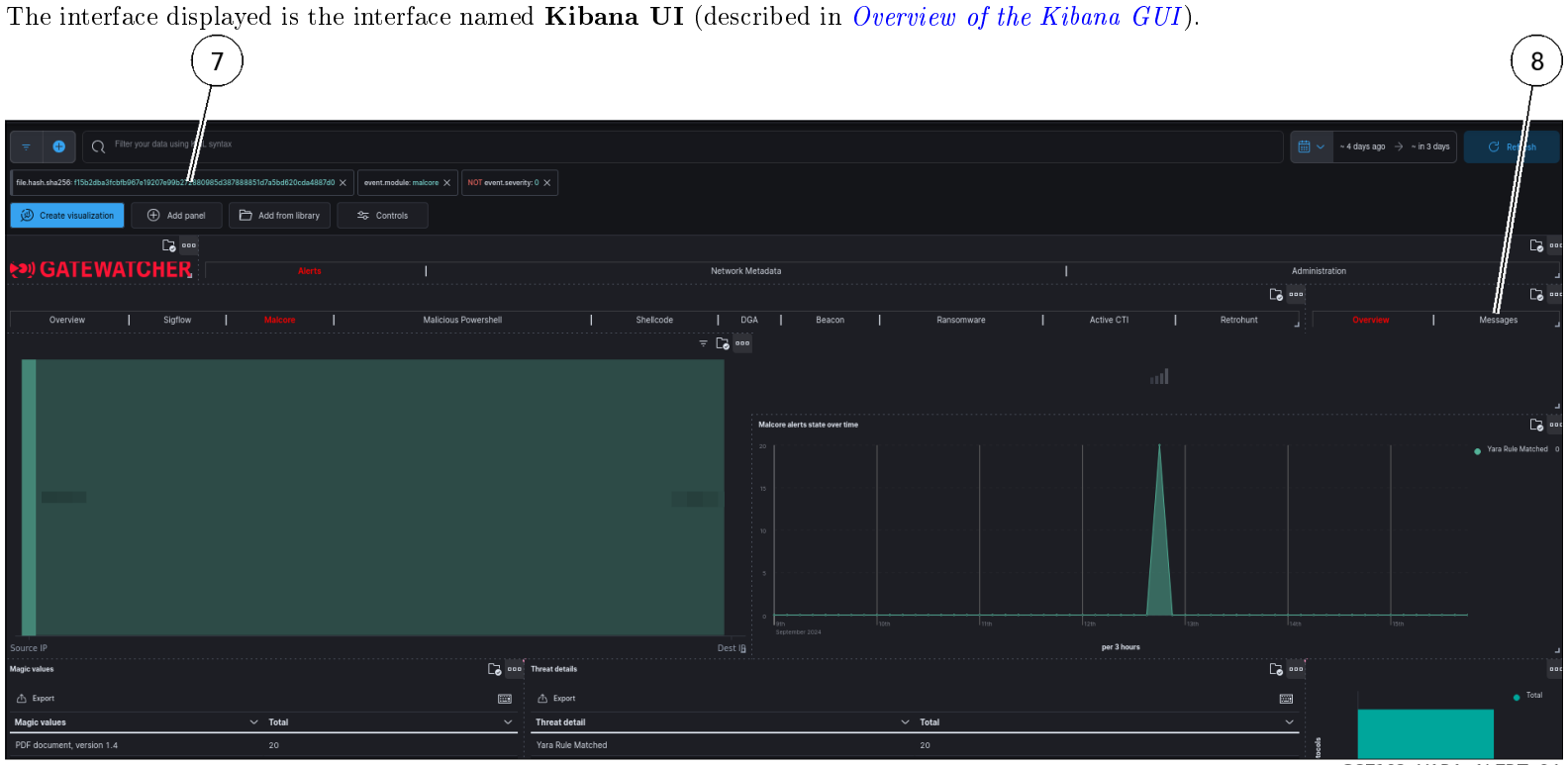
- To filter the Yara alerts on Kibana, enter the following command `event.module : "malcore" and malcore.state : "Yara Rule Matched"` (5) in the search field.
- Validate wih the `Refresh` button (6).



GCE103_YARA_ALERT_03

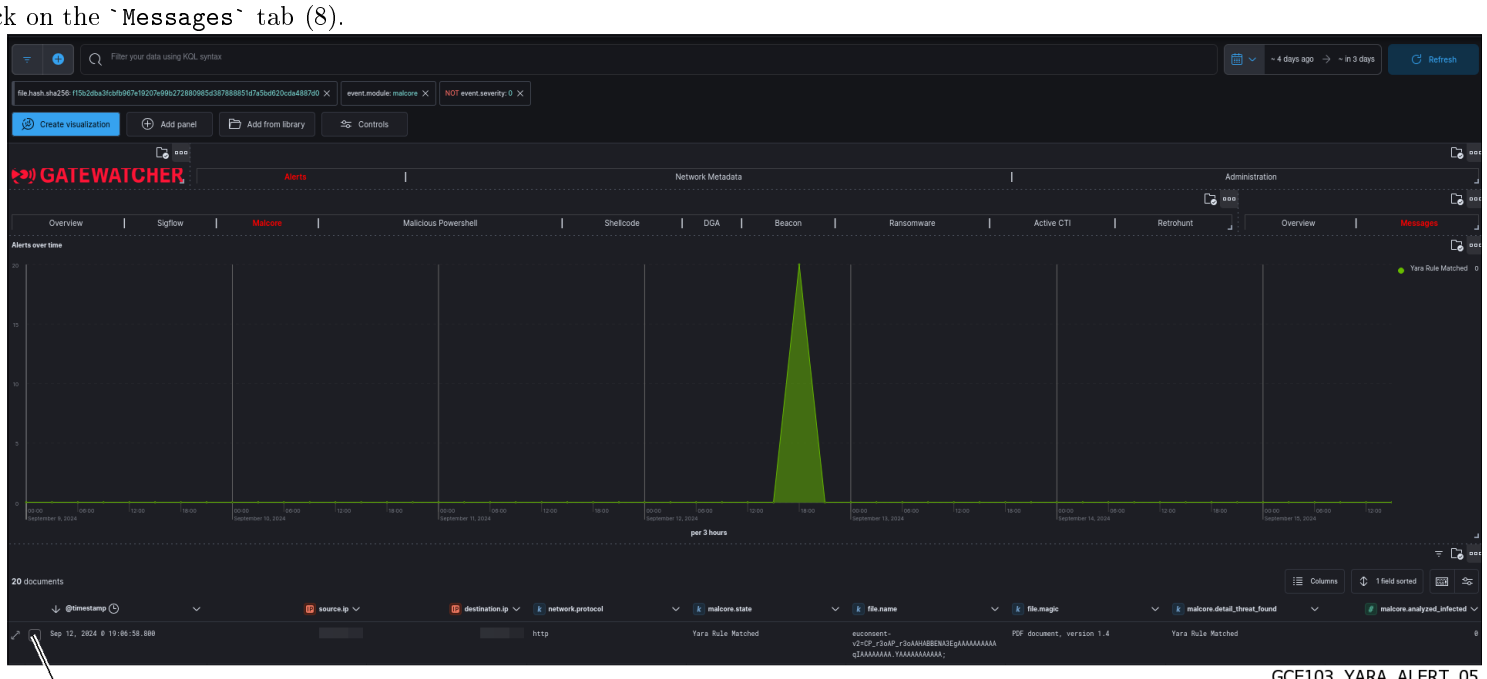
- To consult information about a specific alert:

- After selecting the alert, click on the `Open malcore file transaction` command of the `Actions` menu.
  Kibana is opened on the `Malcore` tab of the `Alerts ` section: in the `Overview` tab, the database is filtered on the `file.hash.sha256` parameter (7).
  The interface displayed is the interface named **Kibana UI** (described in *Overview of the Kibana GUI*).



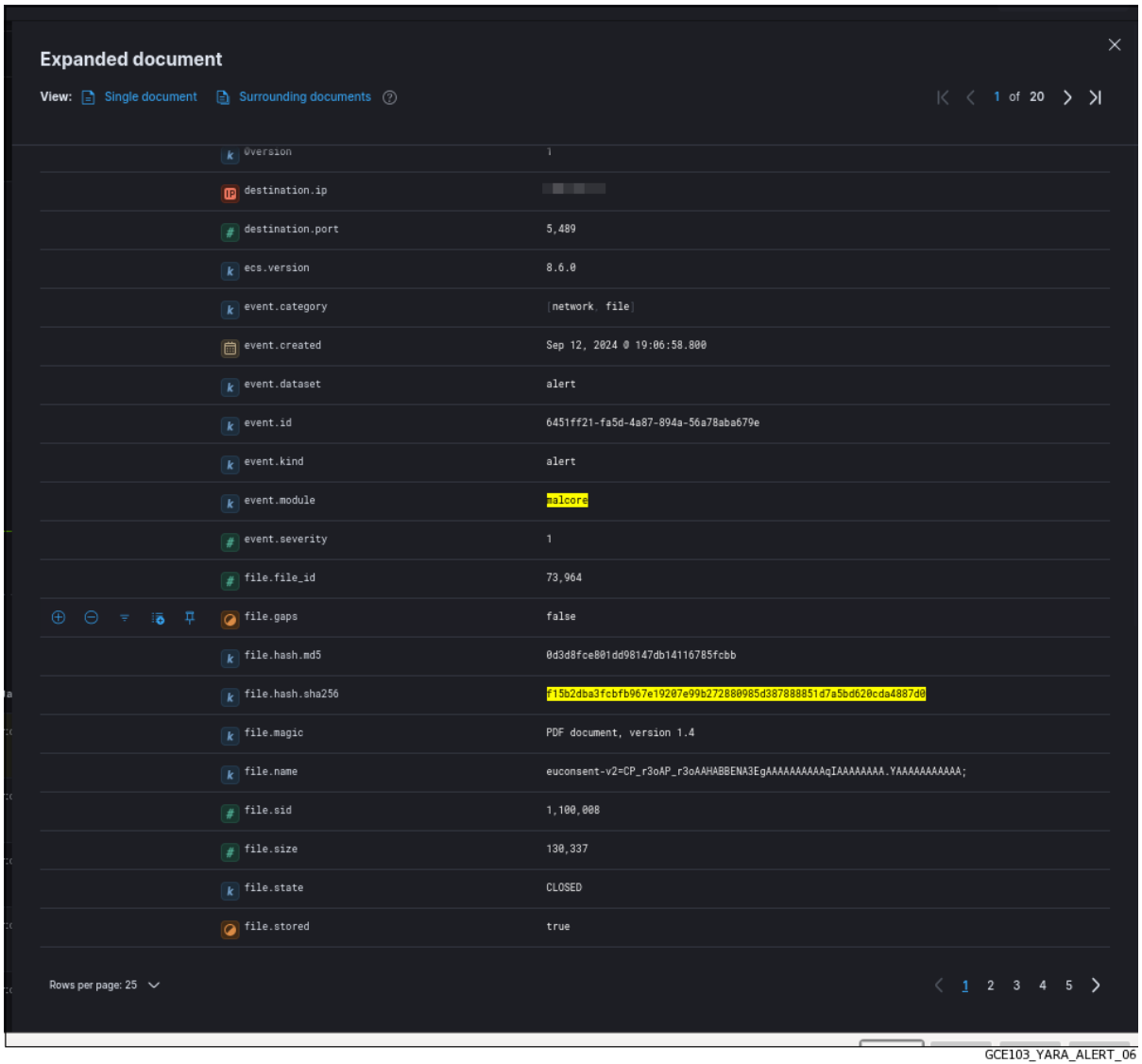
GCE103_YARA_ALERT_04

- Click on the `Messages` tab (8).



GCE103_YARA_ALERT_05

- Click on the toggle icon (9) on the left of the Alert
  The expanded document is displayed.



GCE103_YARA_ALERT_06

The detailed information of this alert can be viewed in table or json format (see the *Yara log data structure*).
The displayed counters are given in the *Engine log data structure* appendix.

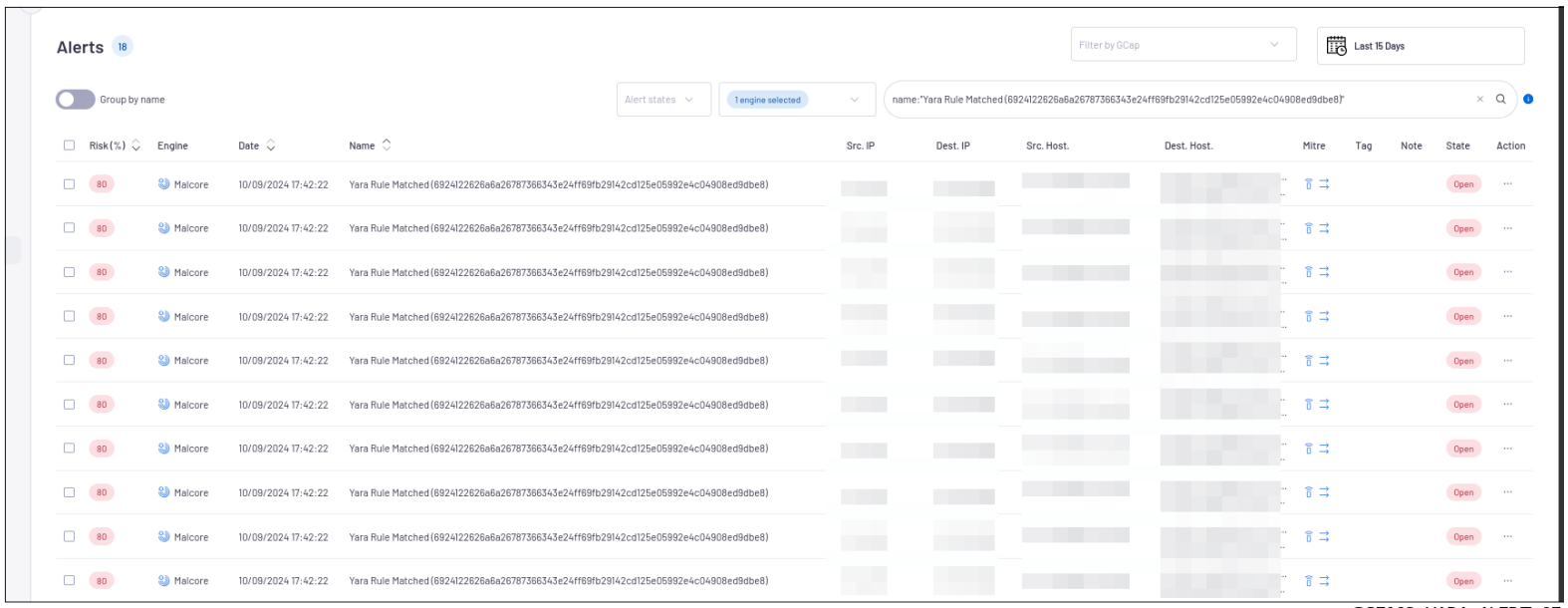
Note:

The **Kibana UI** can also be accessed without any filters via the `Hunting` icon on the left side menu bar in the WebUI.

7.5.11.1.3 Essential information to understand the context of the alert

7.5.11.1.3.1 What are the key fields of an alert and their meaning?

Before undertaking any investigation or qualification of the alert, it is essential to start by observing several elements that will provide essential information to understand the context of the alert.
These elements can be found either in the **WebUI** interface or in the **Kibana UI** interface (for more information, refer to the previous paragraph).



GCE103_YARA_ALERT_07

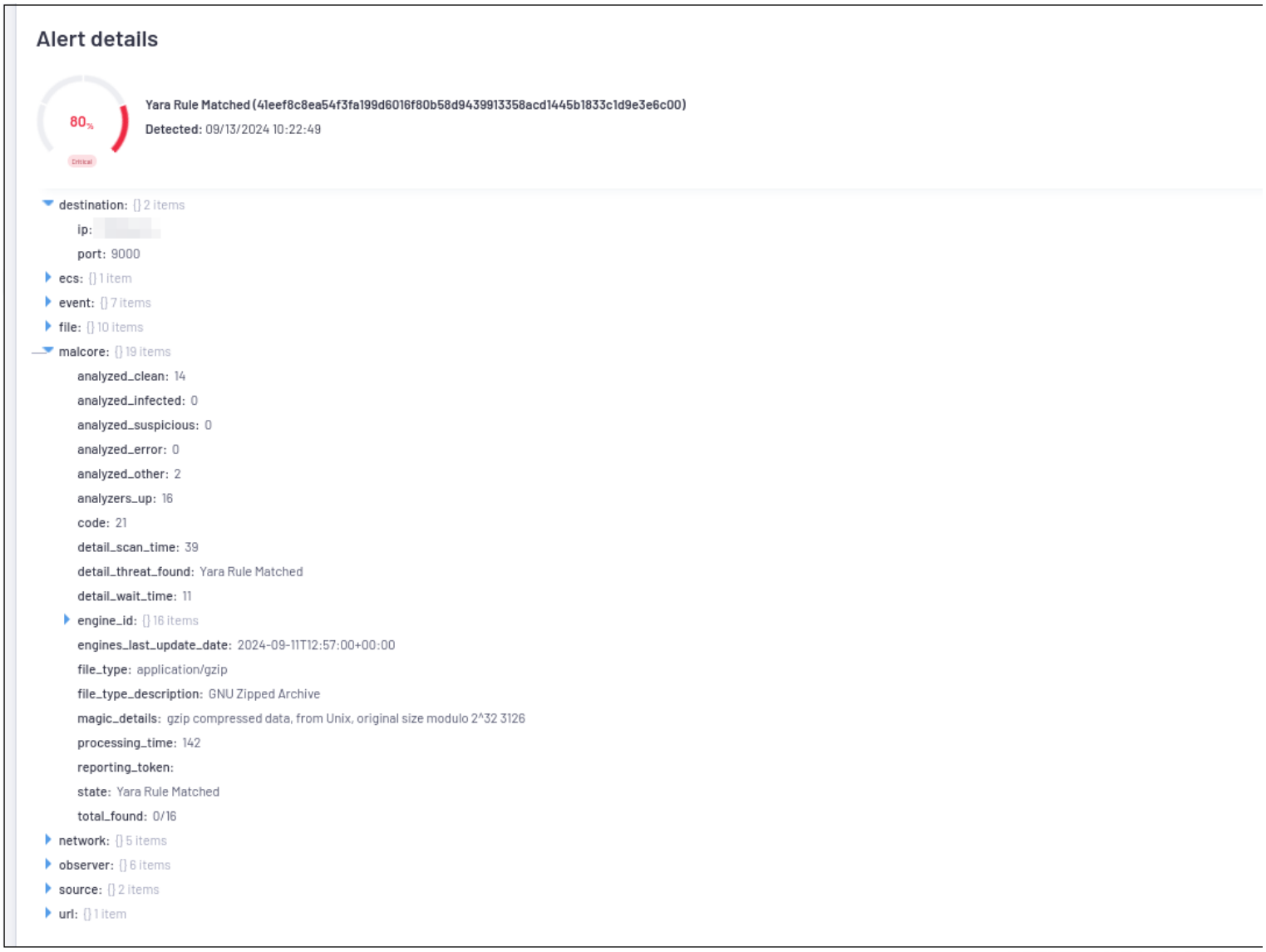
In the information displayed on the WebUI `Alerts` screen, these key elements include:

- `Engine:`
  The alerts related to the Yara engine include the term `Malcore` for the Engine field.
- `Date:`
  The date when the engine rose an alert in the local timezone. The UTC date is accessible in the alert detail under *.event.created*
- `Name:`
  At the beginning of this field is indicated the result of the Yara scan (yara rule matched) associated to the the sha256 of the file.
- `Src. IP` and `Dest. IP`
  The IP addresses associated with the alert, whether source or destination, provide information about the network communication involved in the incident.
- `Src. Host.` and `Dest.Host.`
  The source and destination hosts associated with the alert provide information about the systems involved in the network communication of the incident.

More information is available on the `Alert Details` screen after clicking on an alert in the `Alerts` screen of the **WebUI**.

GCE103_YARA_ALERT_08

- Click on the `Details` tab (1).



GCE103_YARA_ALERT_09

- `detail_threat_found`: this field is always `yara rule matched`
- `protocol`
  This field indicates the protocol through which the file was observed on the network.
  This information can help identify how the file was delivered or offer a way to gather more protocol-specific information.
- `magic details`
  This is the file format detected by Malcore.
  The file format is not detected based on filename or extension but rather by the content of the file.
  This information can help to understand the nature of the malicious file in question, in particular the platforms that are targeted and it sometimes allow to reveal the real nature of a file.
  For example: "PE32 executable (GUI) Intel 80386, for MS Windows".
  In this example, "PE32 executable" indicates that it is an executable file in Portable Executable format, commonly used for Windows programs.
- `file.name`
  This field indicates original filename used during the delivery.
- `file.hash.md5` and `file.hash.sha256`
  These fields indicate the checksum respectively in MD5 and SHA256 of the sample.
  This checksum is a unique value representing the content of a file.

7.5.11.2 Alert handling procedure

7.5.11.2.1 How do you verify the accuracy of an alert and determine if it represents a real threat?

Yara will produce an alert if the file content matches a rule in the Yara ruleset uploaded in Yara setting (see Yara configuration in detection strategy).
As of now, it is not possible to know which Yara rule is the origin of the alert.
To investigate, one must download the file flagged by the Yara engine and analyze it manually.

7.5.11.2.2 What answers are needed if the threat is confirmed?

Note:

This procedure allows to deepen the investigation and assess the extent of the incident after confirmation of a threat generated by the Yara engine

- **Isolate the system**: immediately isolate the contaminated system and ensure it cannot cause further damage
- **Notify**: inform relevant parties of threat detection
- **Dynamic analysis**: if possible, run the file in a secure environment (sandbox) to observe its behavior (a GBox for example)
- **Collect information**: gather essential information such as file hash, file name, source and location
- **Neutralize the threat** by deleting the file, blocking the original IP address, etc.
- **Reverse engineering (if necessary)**: if the threat is particularly complex, reverse engineering can be considered to understand in depth its internal functioning.

  This can help identify exploited vulnerabilities and propagation mechanisms.

  The feature `` `Download Malware` ``, presented previously, enables to recover the file for analysis.
- **Analyze logs**: review system and network logs to trace the spread of the threat.

7.6 Using of NDR dashboards

7.6.1 Introduction

When an attack on an information system is confirmed, analyst teams must be able to quickly understand the origin of the attack, its target, and its overall impact.
The NDR dashboards of the GCenter will facilitate these inquiries by making available a wealth of essential information.
They will enable:

- Analyzing the alerts for each type of engine
- Viewing information and alerts specific to the network's equipment
- Viewing information and alerts specific to the network's users
- Viewing the relationships between the different equipment and users

To	Apply the procedures
Retrieving information related to an alert	*Procedure to retrieve information related to an alert*
Processing equipment	*Procedure to process the equipment*
Processing an user	*Procedure to process the users*
Managing association rules	*Procedure to manage association rules*
Relation between equipment and users	*Procedure to analyze the relationship between equipment and users*

7.6.2 Links associated

See the *Overview of the WEB UI*.

7.6.3 Prerequisites

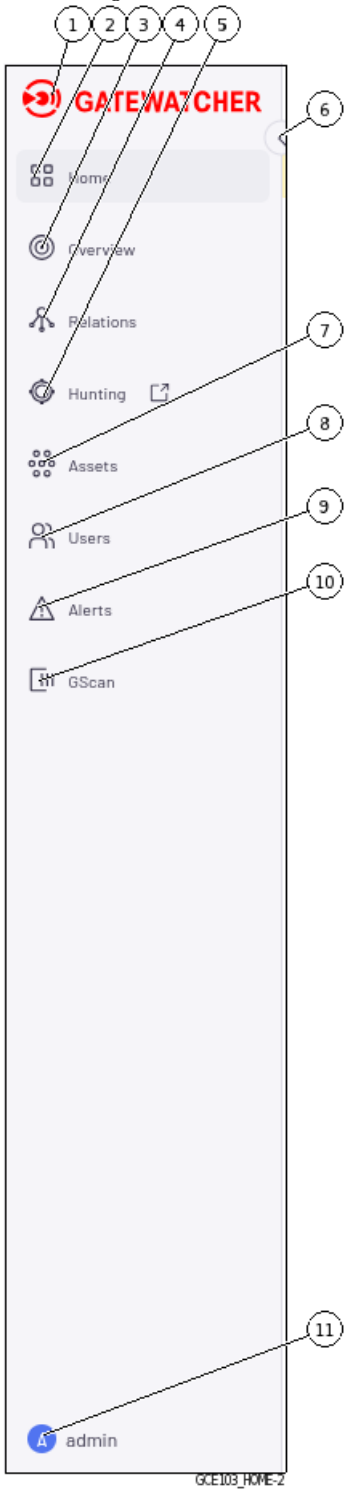
- User: member of **Operator** group

7.6.4 Preliminary operations

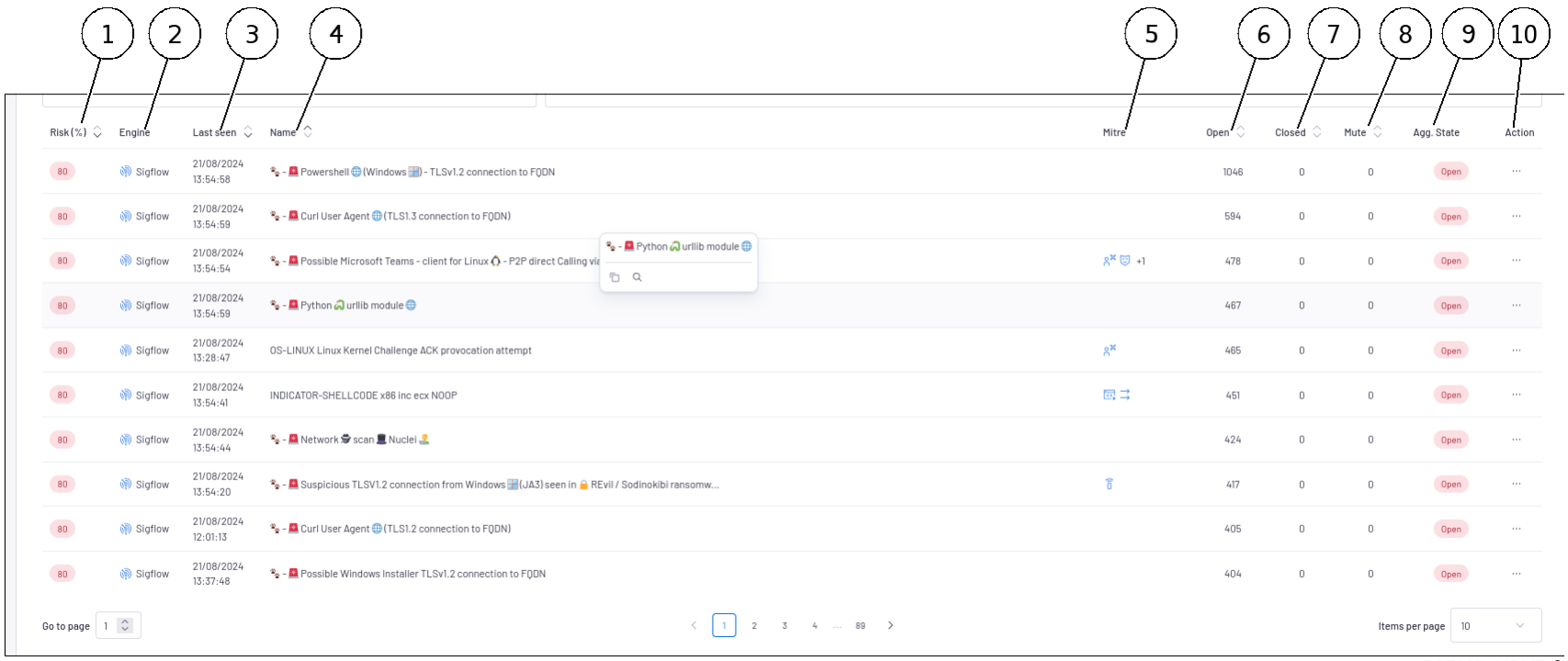
- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

7.6.5 Procedure to retrieve information related to an alert

- From the navigation bar, click on the `Home` button (2).

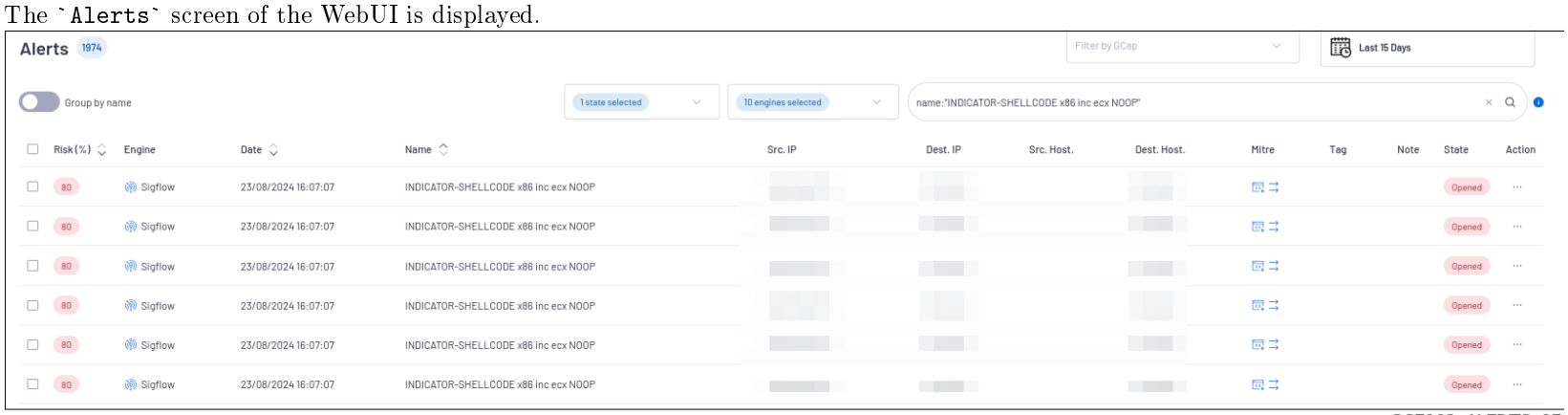


In the Message Area of the `Home` screen, alerts are displayed classified by risk level (item 1).



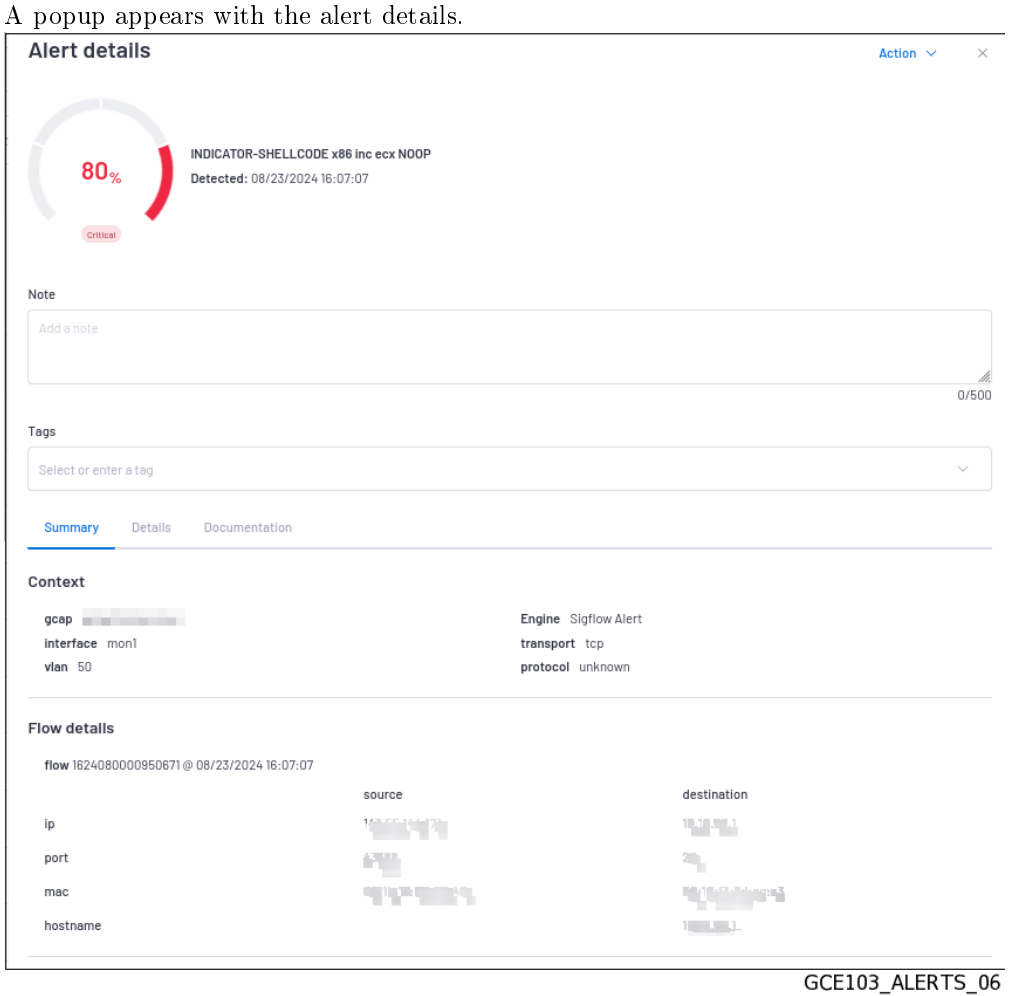
GCE103_HOME-6

- Click on an alert requiring investigation.
  The `Alerts` screen of the WebUI is displayed.



GCE103_ALERTS_05

- If the `Group by name` button is ticked, click again on the alert again in the page that appears.
- Once the alerts are not aggregated, click on the alert requiring investigation.
  A popup appears with the alert details.



GCE103_ALERTS_06

This window displays important information:

- The details of the alert

- The name of the equipment concerned or impacted by this alert
- The IP addresses concerned or impacted by this alert

Note:

This window is detailed in the *`Alert details` window*.

According the engine which has detected the alarm, refer to the specific procedure defined below

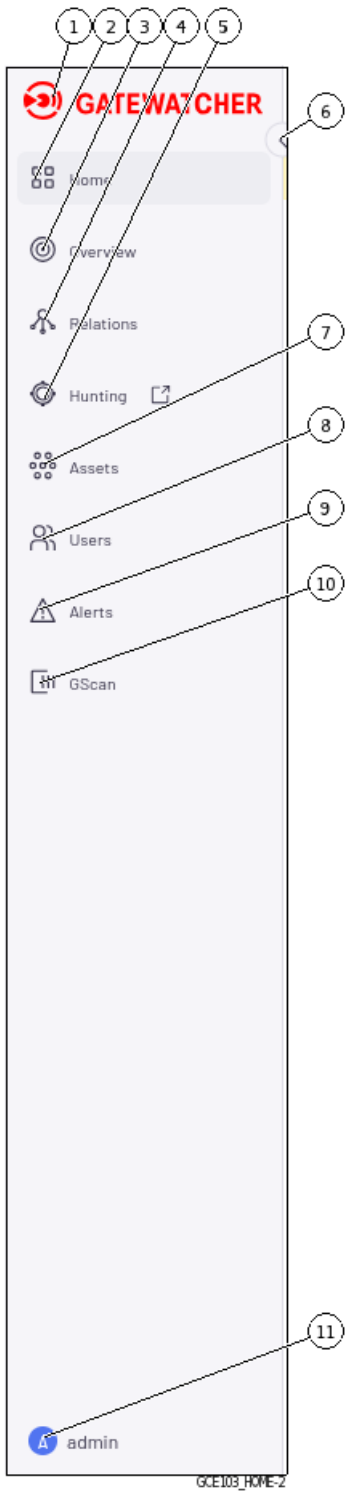
The specific processing of alerts detected by...	is indicated in the procedure...
the Malcore engine	*Analyzing the Malcore alerts*
the Powershell detect engine	*Analyzing the Malicious Powershell detect alerts*
the Shellcode detect engine	*Analyzing the Shellcode detect alerts*
the Sigflow engine	*Analyzing the Sigflow alerts*
the DGA engine	*Analyzing the DGA detect alerts*
the Retroanalyzer engine	*Analyzing the Malcore retroanalyzer alerts*
the CTI engine	*Analyzing the Active CTI alerts*
the Retro hunt engine	*Analyzing the Retrohunt alerts*
the Ransomware detect engine	*Analyzing the Ransomware detect alerts*
the Beacon detect engine	*Analyzing the Beacon detect alerts*
the Yara engine	*Analyzing the Yara alerts*

- From the equipment IP, search on it in the `Users` page (example: IP:192.168.0.1).
- Click on the user to display the user record.

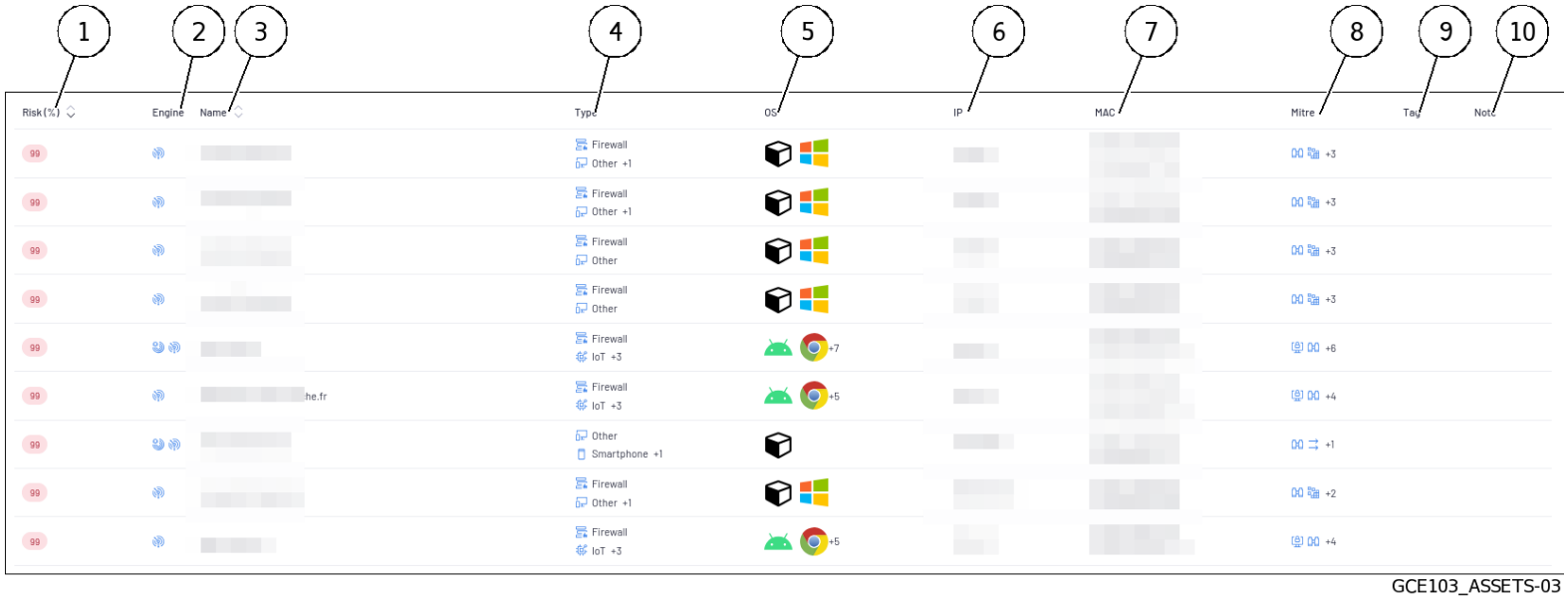
  The following are displayed:
  - Its risk score
  - IP address
  - Its equipment on the network
  - The metadata generated
  - Alerts generated
  - Its relationship with other equipment or network users
- Continue investigations, as above, if other equipment is present in the alert being processed.

7.6.6 Procedure to process the equipment

- From the navigation bar, click on the `Assets` button (7).



The `Assets` window is displayed.



The active equipment management interface provides a list of the different equipment on the network listed by risk score.

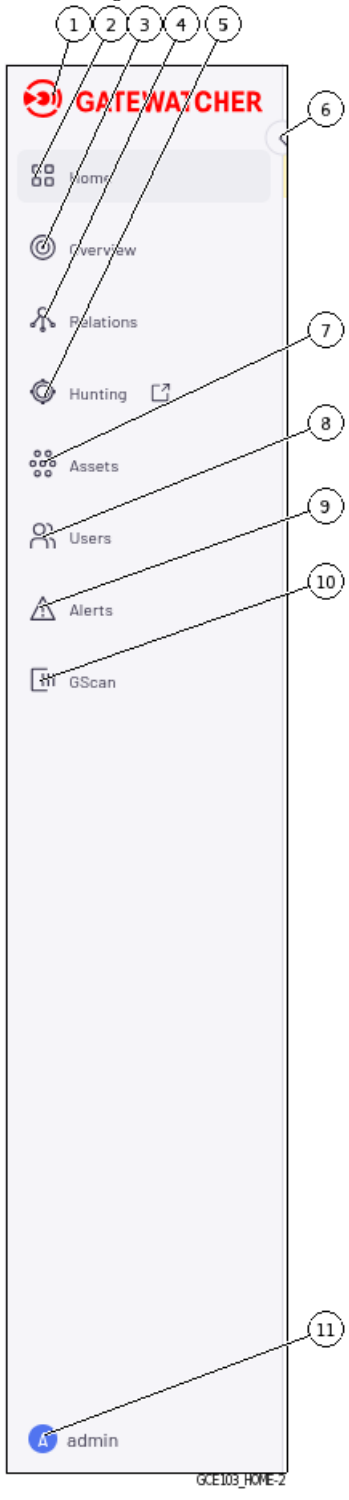
The equipment with the highest risk score are those that have raised the most high criticality alerts. It may therefore be necessary to carry out an in-depth analysis of the equipment in question.

It may therefore be necessary to perform a thorough analysis on the equipment in question.

- Click on the desired equipment.
- Analyze the various alerts (1) noted for this equipment.
- If necessary, add a tag (9) that will give status to the equipment.
- If necessary, add a note (10) to indicate the different analyzes performed.

7.6.7 Procedure to process the users

- From the navigation bar, click on the `Users` button (8).



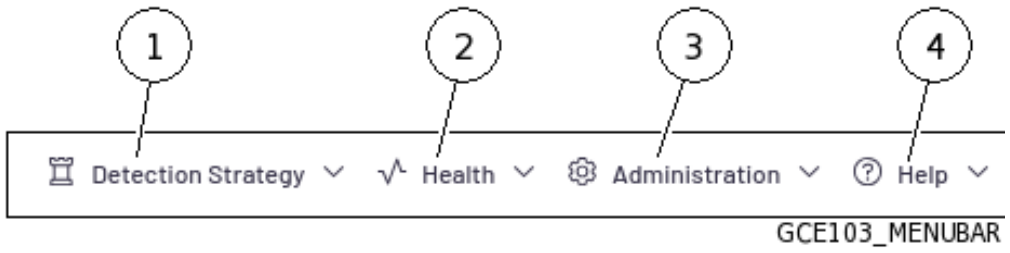
The `Users` window is displayed.

The active user management interface provides a list of the different users on the network listed by risk score (1).
The user with the highest risk score are those that have raised the most high criticality alerts.
It may therefore be necessary to carry out an in-depth analysis of the user in question.

- Click on the desired user.
- Analyze the various alerts noted for this user.
- If necessary, add a tag (7) to give the user a status.
- If necessary, add a note (8) to indicate the different analyzes performed.

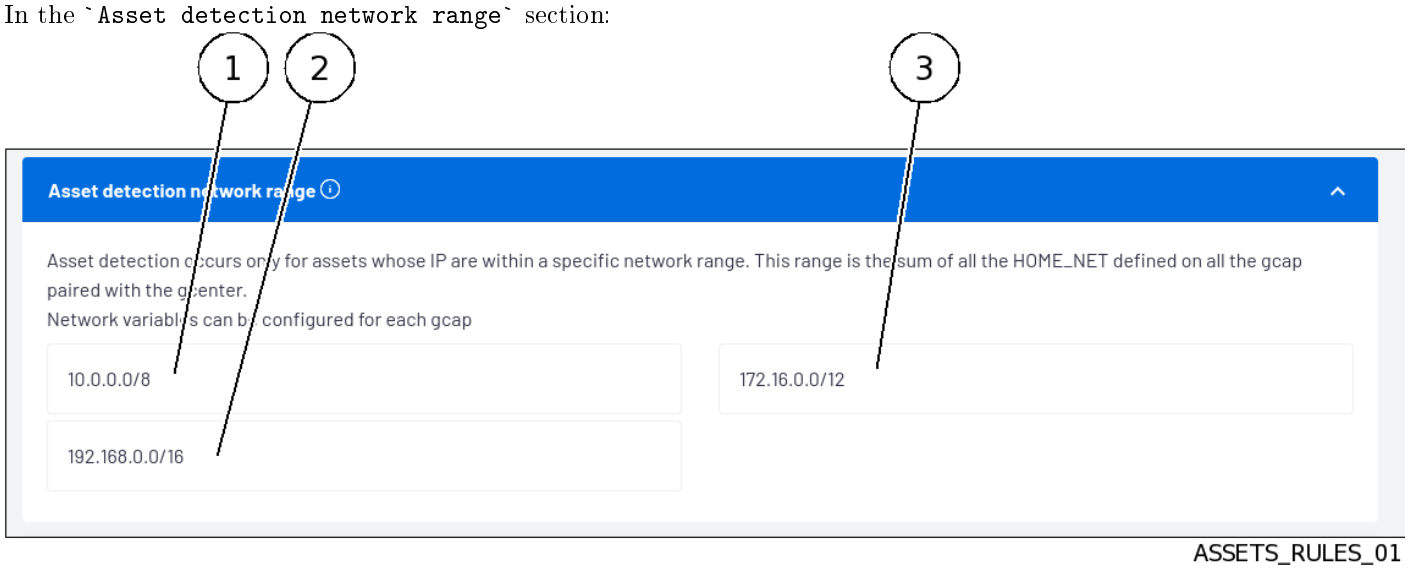
7.6.8 Procedure to manage association rules

- From the navigation bar, click successively on :



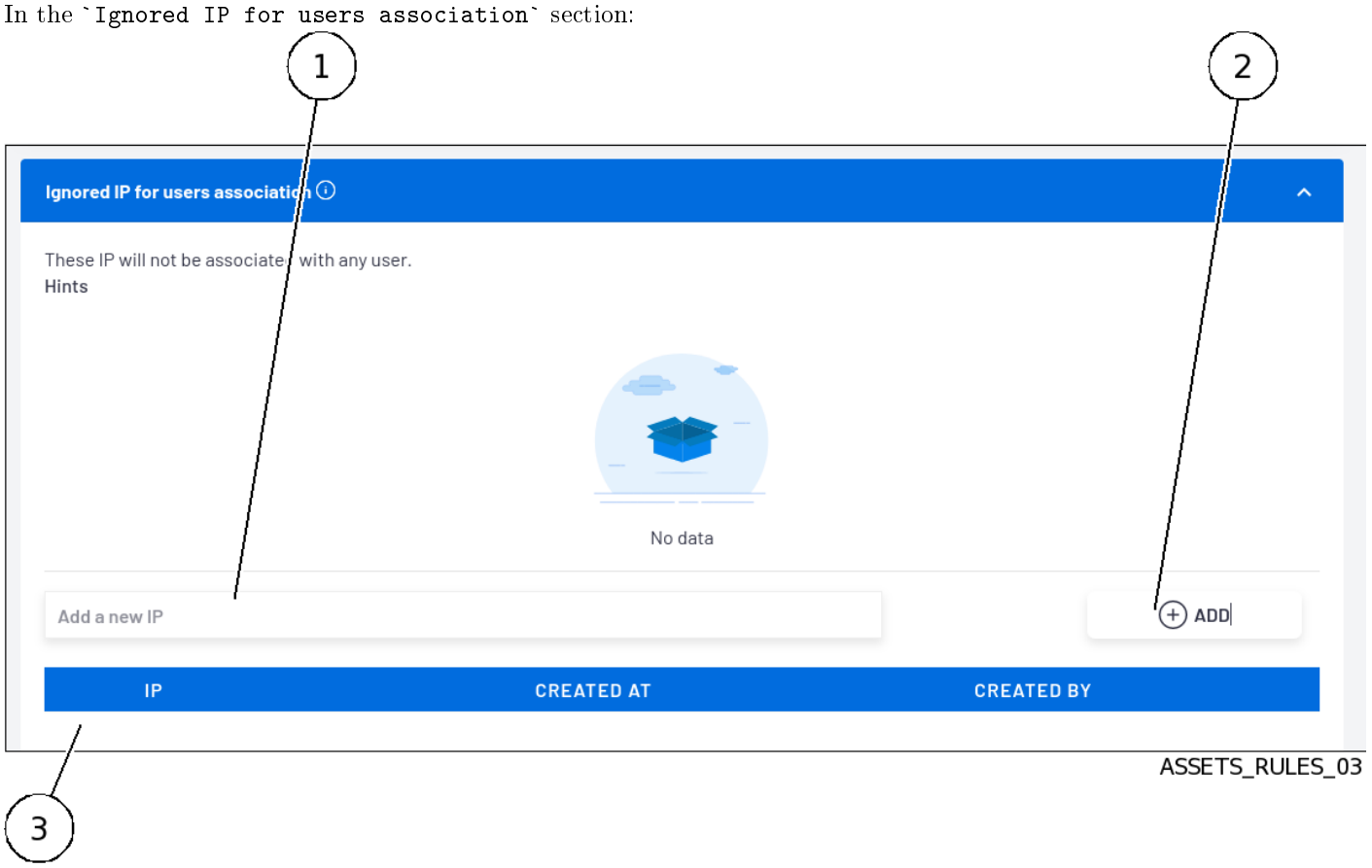
  - The `Detection strategy` button (1)
  - The `Configuration` button on the menu `Assets and users detection`
    The interface for managing association rules `Assets/Users association rule` allows to set up rules concerning equipment and users present on the network.

- In the `Asset detection network range` section:

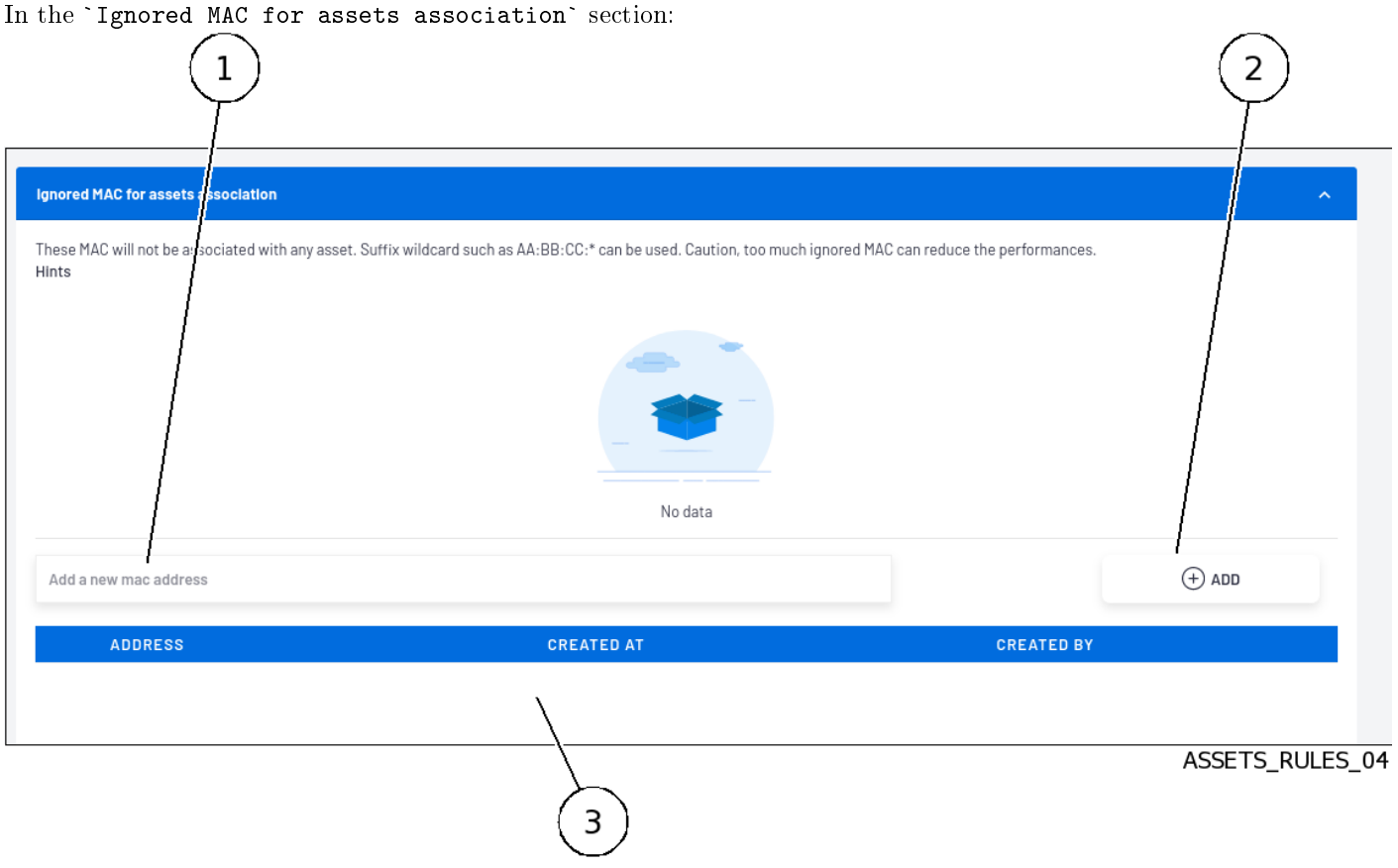


  - Click on the `Network variables can be configured for each GCap` link to add internal networks via the GCap profile customization feature.
    For more information, see the *`Asset detection network range` section of the `Assets/Users Association rules` screen*.

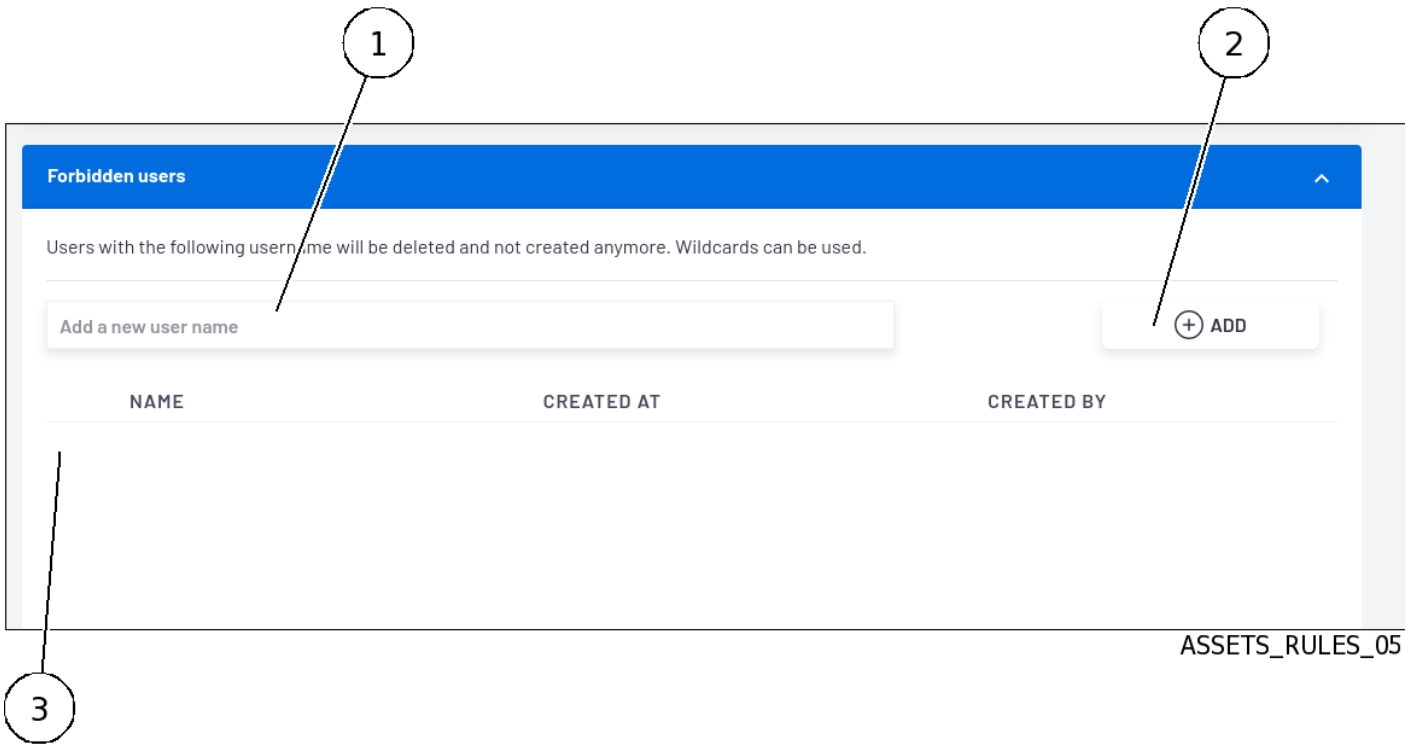
- In the `Ignored IP for users association` section:



  - Declare IP addresses that cannot be associated with a user to avoid wrong associations.
    For more information, see the *`Ignored IP for users association` section of the `Assets/Users Association rules` screen*.
- In the `Ignored MAC for assets association` section:

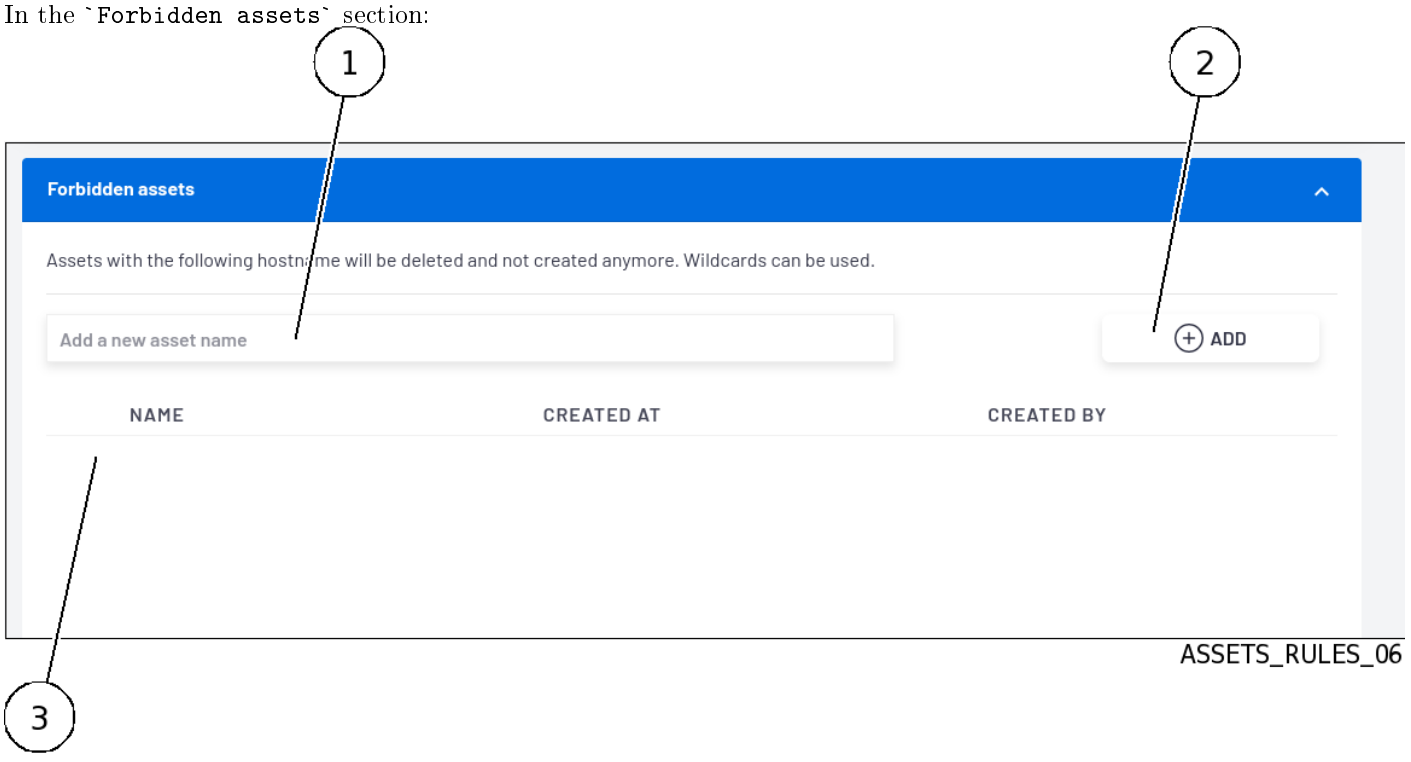


  - Declare MAC addresses that cannot be associated with equipment to avoid wrong associations.
    For more information, see the *`Ignored MAC for assets association` section of the `Assets/Users Association rules` screen*.
- In the `Forbidden users` section:



- Declare users not to appear in NDR dashboards (example: CEO, administrator).
  For more information, see the *`Forbidden users` section on the `Assets/Users Association rules` screen*.

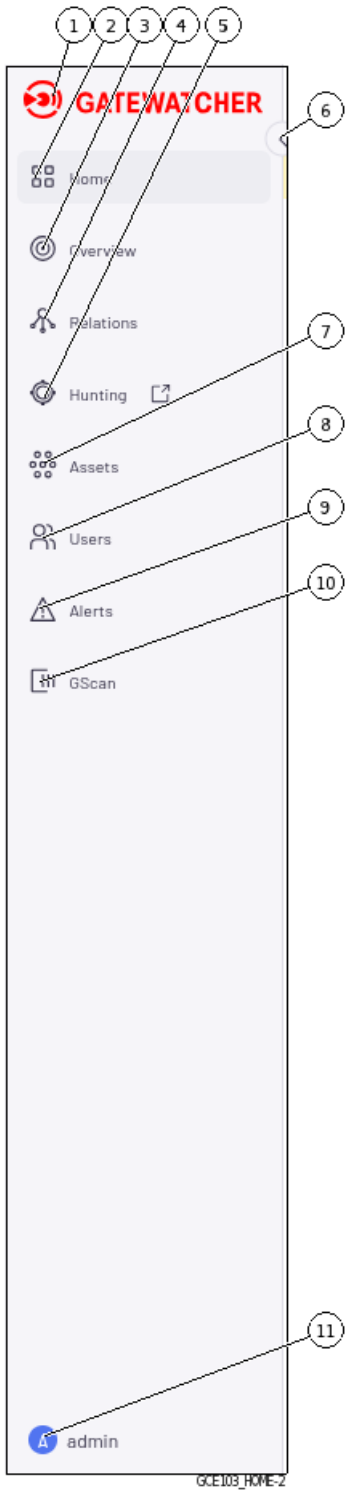
- In the `Forbidden assets` section:



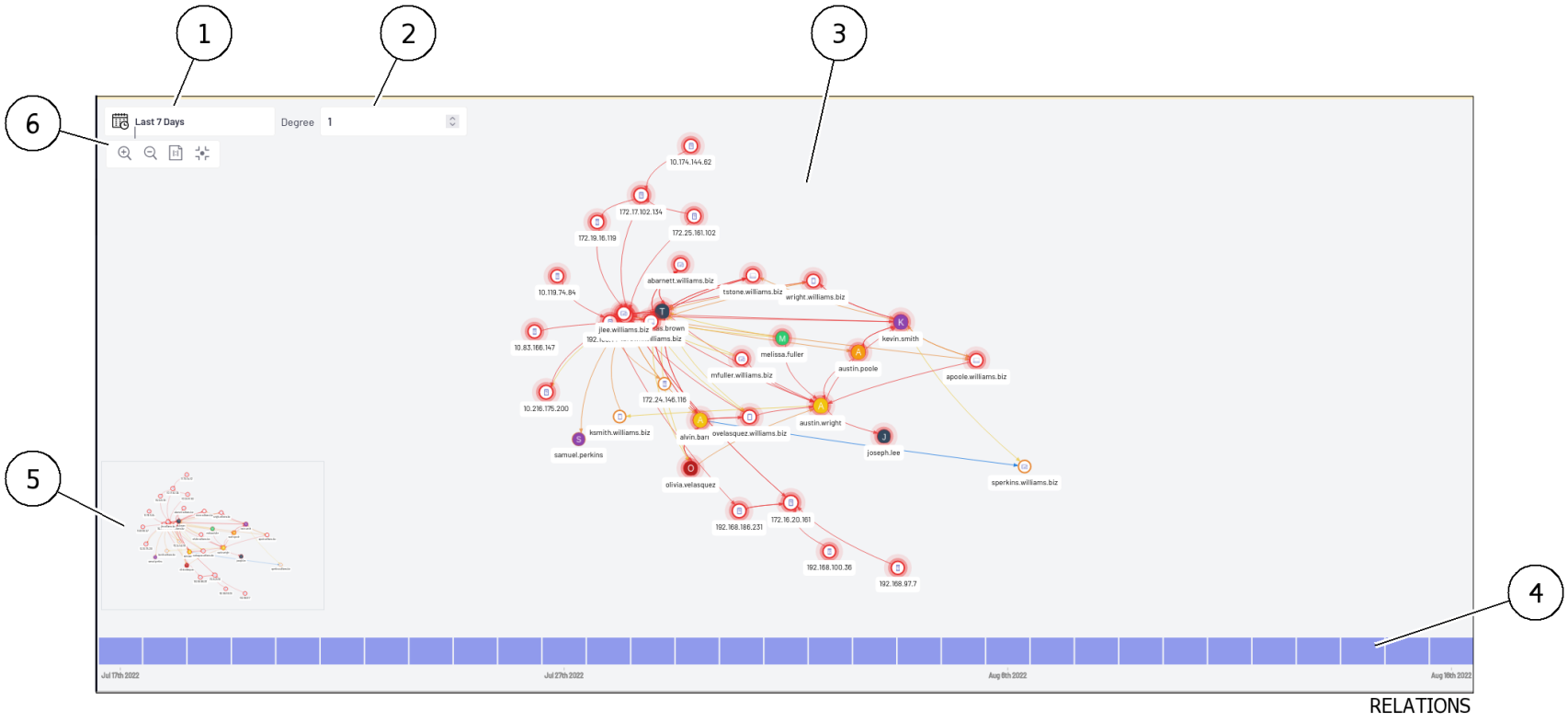
- Declare the equipment not to appear in the NDR dashboards (example: sensitive equipment, irrelevant equipment).
  For more information, see the *`Forbidden assets` section on the `Assets/Users Association rules` screen*.

7.6.9 Procedure to analyze the relationship between equipment and users

- From the navigation bar, click on the `Relations` button (4).



The `Relations` window is displayed.



- Choose the desired period using the timeline at the bottom of the page.

- Locate a user or equipment flashing red (risk score > 75%).
- Click on it, its interactions with other users and equipment are activated and a popup is displayed.
- Move the mouse over the activated links (interactions) to see what they mean.
- In the popup, the elements enabling further investigation are shown:
  - The main information about the item
  - Alerts raised by the item

7.7 Using of the Kibana dashboards

7.7.1 Introduction

The Kibana dashboards enable more in-depth investigation as they provide access to all events in the solution.
It is possible to trace a comprehensive attack by switching from dashboard to dashboard.
The purpose of this procedure is to present the method for tracing a specific attack.

7.7.2 Links associated

See the *Overview of the Kibana GUI*.

7.7.3 Prerequisites

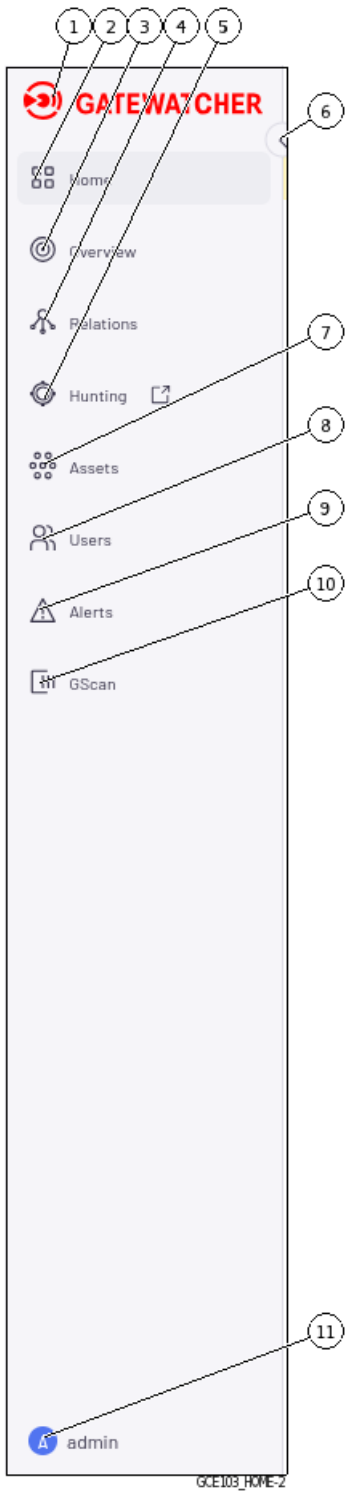
- User: member of **Operator** group

7.7.4 Preliminary operations

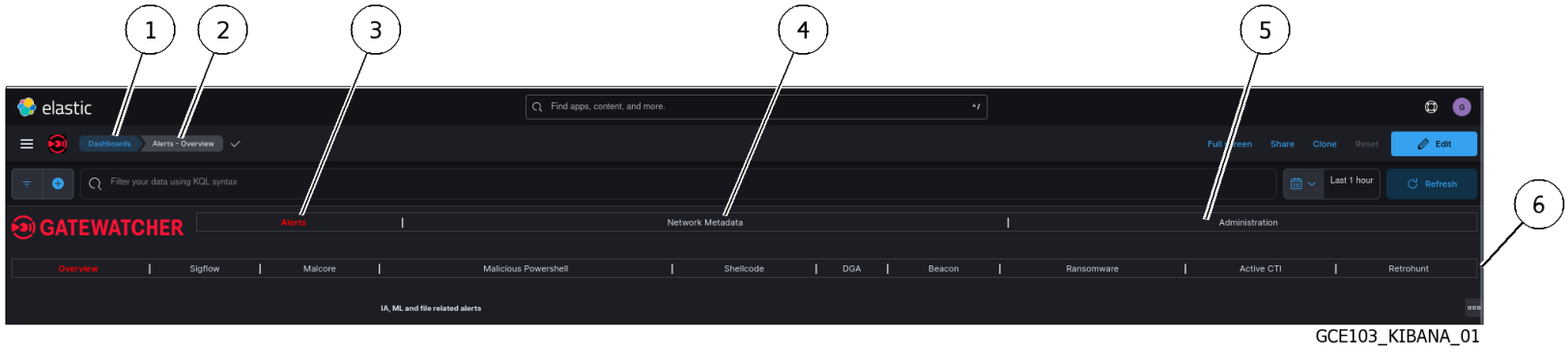
- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

7.7.5 Procedure introducing the Kibana investigation method

- From the navigation bar, click on the `Hunting` button (5).



The `Hunting` window is displayed.



- Go to the `Malcore` tab.
- In the `Message` tab, locate the alert on an infected file requiring investigation.
- Scroll down this alert to display all the fields in the event.
- Find the `flow_id` field and perform a positive filter on it by pressing the +. The filter is displayed under the search bar.
- Click on this filter and then click on `Pin across all apps` to attach the filter and be able to keep it in the other dashboards.
- Browse the different "alert" dashboards to see if other alerts were generated for this flow.
- Browse the metadata dashboard to see which metadata were generated for this flow.

7.8 Detecting with GScan

7.8.1 Introduction

GScan allows you to manually submit files for analysis.
The following options are possible:

- Malware: submit files to the Malcore engine
- Powershell: scans files containing Powershell scripts and detects potential threats that can serve as a gateway to install malware on Windows.
  With regard to malicious powershells, detection is based on a supervised machine learning model, and on the fact that these scripts generally use obfuscation techniques or that are similar to them (base64, concatenation, type conversion, etc.).
- Shellcode: submits files for analysis by the shellcode detect engine

Before starting an analysis, it is necessary to check the type of analysis to be performed, see above.
To start parsing a file, simply drag the file into the `DRAG and DROP or CLICK TO SELECT YOUR FILES` area or click on this area to send the suspicious file.
The result of the analysis is then displayed in a thumbnail with the status of the file for each type of analysis chosen.
The `SCAN HISTORY` page displays the history of the analysis performed.

Note:

Attention the maximum file size should not exceed 30MB by default.
There is no limitation on the number of file scans.

Concerning the compressed files analyzed by Malcore:

- The number of files contained in an archive is:
- limited
- editable (50 is the default)
- The number of times the file is compressed is:
- limited (max recursion level)
- editable (5 is the default)
- If files are password protected, the password must be declared in the global settings.

These settings are only accessible to members of the administrator group.

7.8.2 Links associated

The graphical interface is described in the *WebUI `GScan` screen*.

7.8.3 Prerequisites

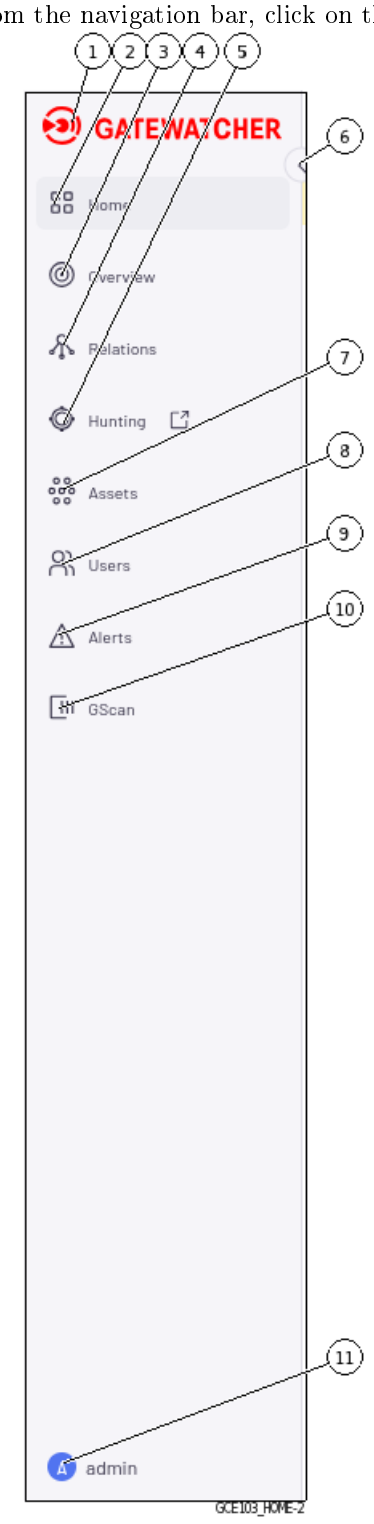
- User: member of **Operator** group

7.8.4 Preliminary operations

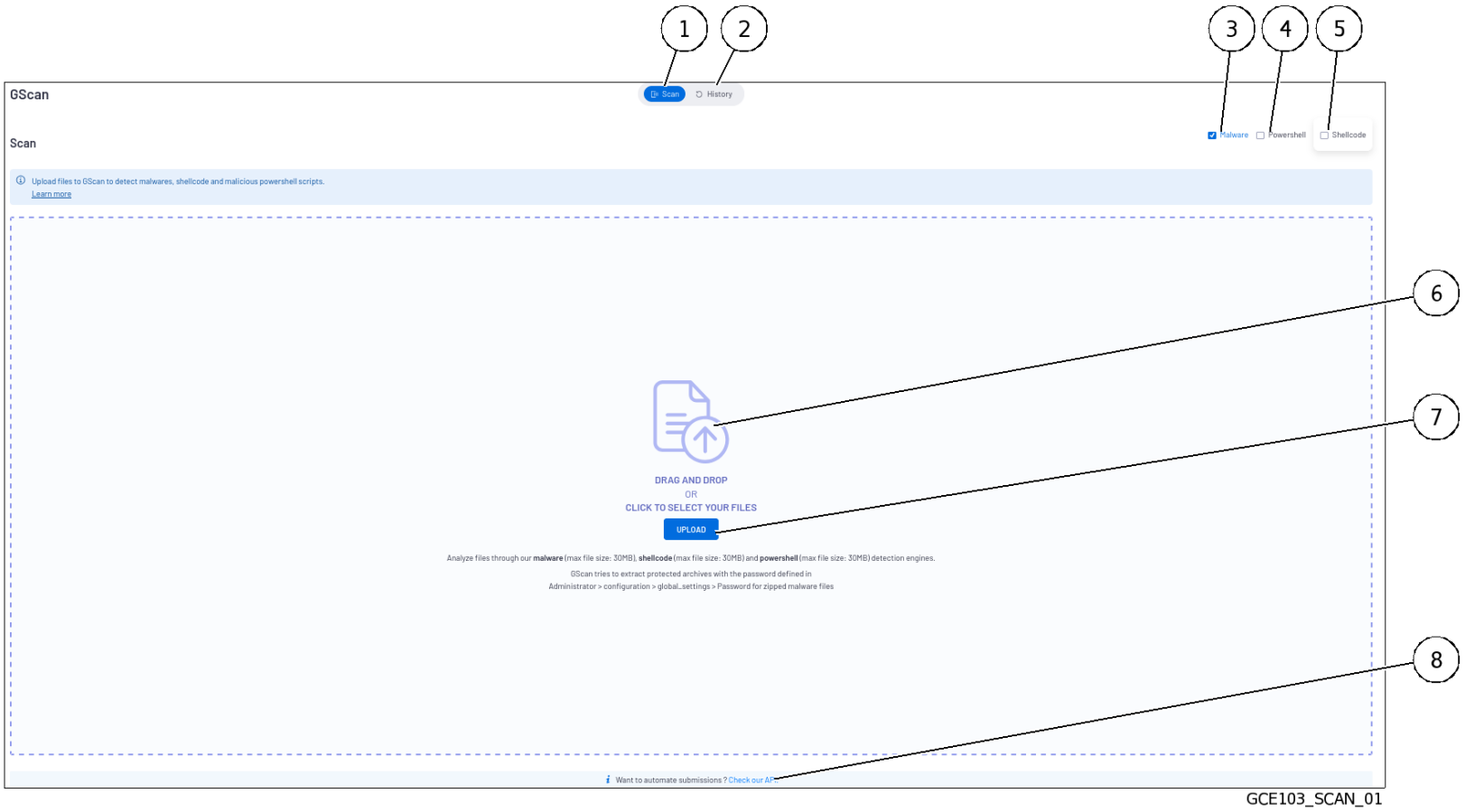
- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

7.8.5 Procedure

- From the navigation bar, click on the `GScan` button (10).



The `GScan` window is displayed.



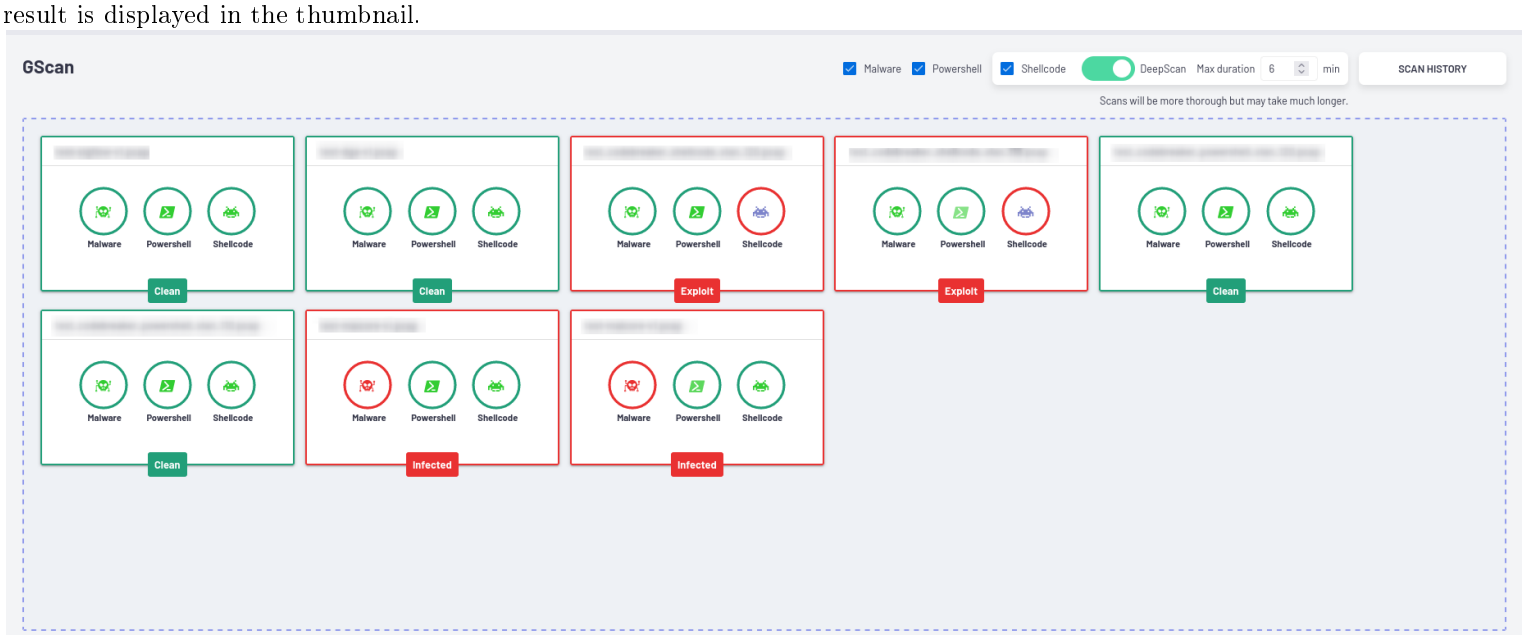
GCE103_SCAN_01

- Tick one or more of the following: `Malware` (3), `Powershell` (4) or `Shellcode` (5).

Note:

The `DeepScan` option, checked by default, allows a thorough analysis of the file.

- As applicable:
- Drop desired file in `DRAG and DROP` box (6)
  or
- click on the `UPLOAD` button (7) then select the load file from the user PC and finally validate the selection
  The result is displayed in the thumbnail.



In the case of a positive result, the thumbnail is displayed in red with the `Infected` information.
In the case of a negative result, the thumbnail is displayed in green with the `clean` information.

Table 4: Malcore engine results. Are valid only for Malcore configuration at the time of analysis

Return code	Result	Description	Action
0	No Threat Detected	File was analyzed and declared healthy	No
1	Infected	File was scanned and declared infected	No
2	Suspicious	The file was analyzed and declared as likely to be infected: some Malcore engines detected this file as malicious...	To be submitted to a GBox

continues on next page

Table 4 – continued from previous page

Return code	Result	Description	Action
3	Failed Scan	An error occurred during the run	In the case of use via GScan or GBox, restart the analysis
7	Skipped - Whitelisted	The file is not analyzed and considered healthy since this file is defined in the Malcore whitelist	None if it is normal that this file is in the Malcore whitelist otherwise modify the list then restart the analysis
8	Skipped – Blacklisted	The file is not scanned and considered infected since this file is defined in the Malcore blacklist	None if it is normal that this file is in the Malcore blacklist otherwise modify the list then restart the analysis
9	Exceeded Archive Depth	The number of times the file is compressed is limited (max recursion level). The message indicates that the defined value has been exceeded.	It is possible to increase this limit and to restart the analysis (attention this can lead to an increase in processing time...)
10	Not scanned	Pb analysis engine	Contact the Gatewatcher support if this happens again
12	Encrypted Archive	The archive is encrypted and therefore not parsable: the password indicated does not work	Enter the correct password and run the analysis again
13	Exceeded Archive Size	The maximum file size should not exceed the defined value (maximum value 10MB). The parsed archive is larger than the defined value.	If the set value is less than 10MB, it is possible to change this limit and restart the analysis, otherwise none
14	Exceeded Archive File Number	The maximum number of files in the archive must not exceed the defined value. The scanned archive contains a number of files greater than the defined value.	It is possible to increase this limit and to restart the analysis (attention this can lead to an increase in processing time...)
15	Password Protected Document	Solution detected inconsistent behavior with password protected document	No action+
16	Exceeded Archive Timeout	The archive scan time has been exceeded, Malcore engines are not responding within the deadline	Restart the analysis if possible
17	Filetype Mismatch	File type mismatch problem: the solution detects the file extension with its contents and compares it with the file extension displayed	No action+
18	Potentially Vulnerable File	The verdict of the result is: Potentially vulnerable files are files associated with identified vulnerable components or applications.	No action+
19	Cancelled	User explicitly canceled this file analysis request	posted for information
21	Yara Rule Matched	The verdict of the result is: a corresponding Yara rule (malware sample identification)	Posted for information
22	Potentially Unwanted	The solution detected potentially unwanted applications.	Posted for information
23	Unsupported File Type	File type not supported by the solution.	No
255	In Progress	Analysis in progress...	Wait for the analysis to complete

Table 5: Shellcode or Powershell engine results. Only valid for configuration at time of analysis

State	description	action
Clean	File was analyzed and declared healthy	No
Exploit	File was scanned and declared infected (Shellcode or Powershell)	No
Suspicious	The file was analyzed and declared susceptible to infection: the engine detected this file as malicious	If possible to submit to a GBox

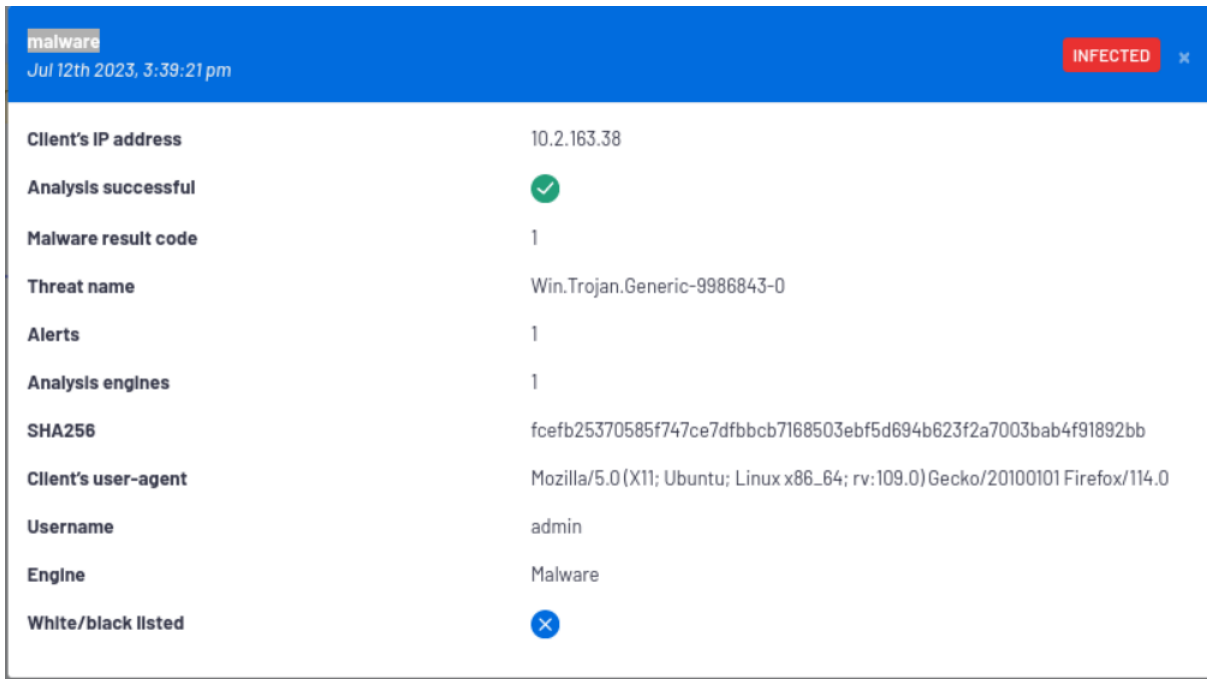
Note:

In the case of an `` `Analysis Error` `` message, leave the mouse over the icon.

If the message `` `GScan is not enabled` `` is displayed, contact a member of the administrator group to activate this option from the configuration menu.

Otherwise check that the motors are up to date. To do this, use the `` `Health check` `` screen. Use Updates to remedy this.

- Click on the thumbnail.
  The detail window is displayed:
  - In the case of a positive result, this window gives detailed information about the detected threat.



- In the case of a negative result, this window gives detailed information about the analysis.

- In all cases, this analysis is now available in the history accessible by the `SCAN HISTORY` button.

Tip:

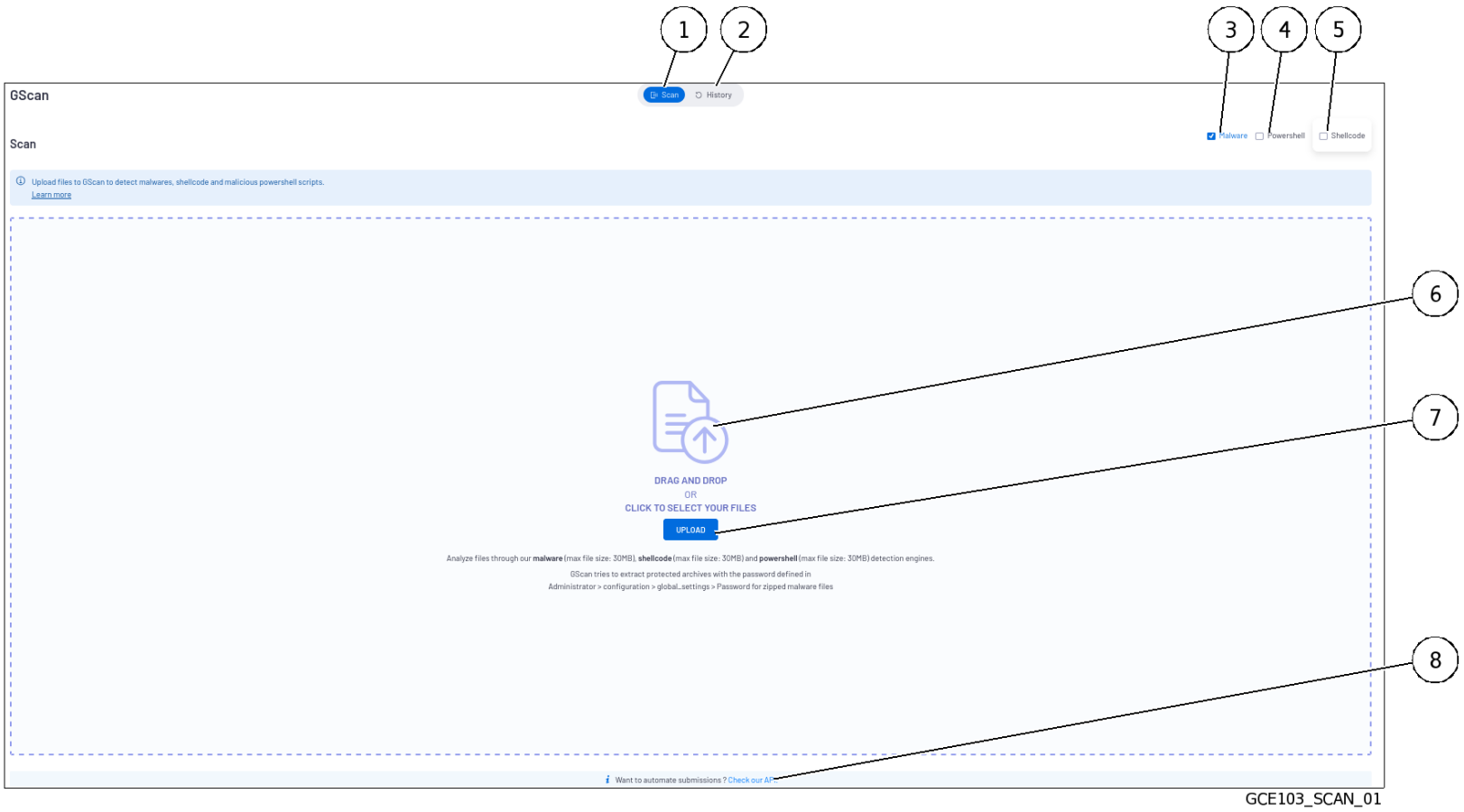
The result is indicative only for the type of analysis selected.
A file is declared clean only for the selected engine.

For the alerts detected by the engine, the details of the counters of the report given in *Engine log data structure* appendix.

7.8.6 Ex post facto search procedure

It is possible to change the type of detection after a first analysis.

- From the navigation bar, click on the `GScan` button.

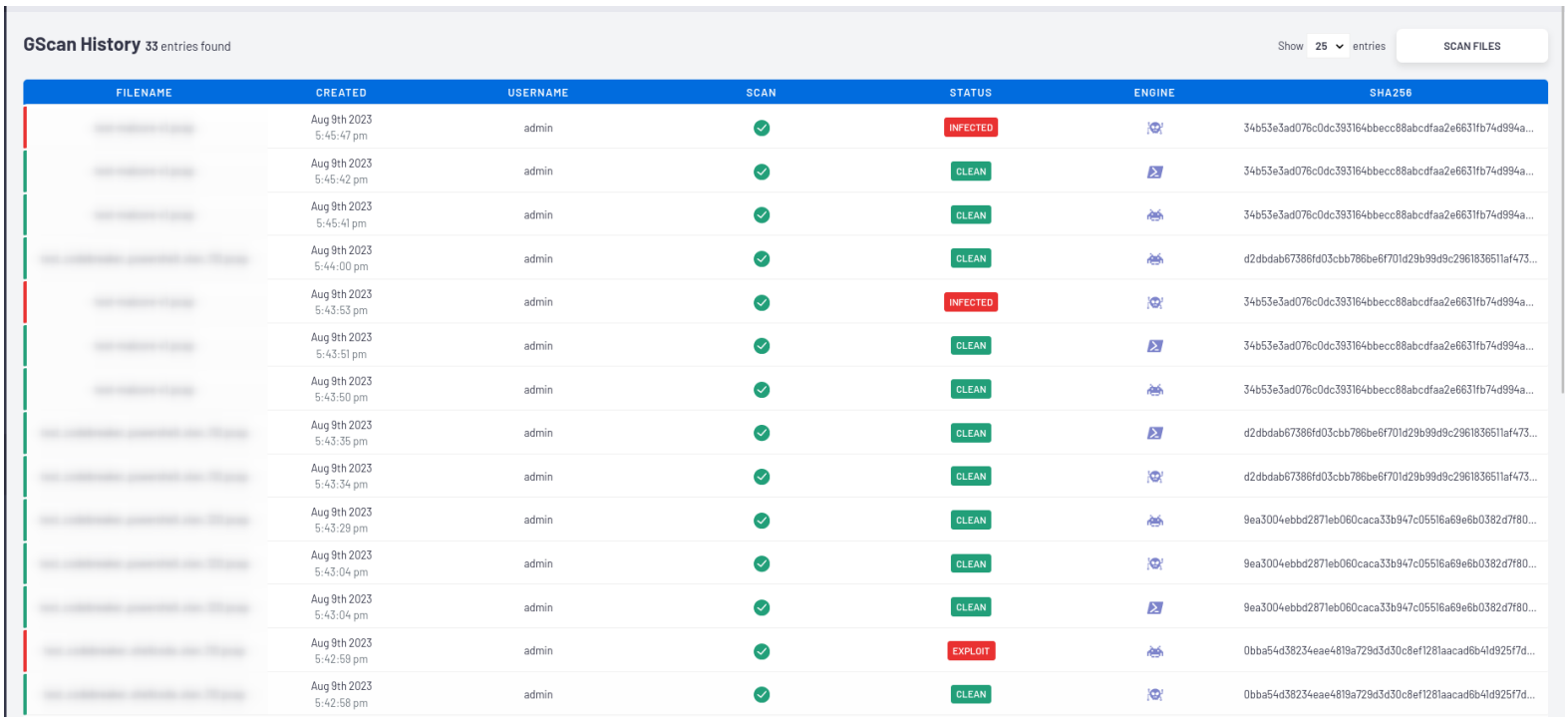


GCE103_SCAN_01

- Tick the `Malware` box for example.
- Place the desired file in the dotted box.
  The result is displayed in the thumbnail.
- Tick the `Shellcode` box.
  The thumbnail shows the result for the Shellcode analysis.

7.8.7 Procedure to view the history

- Click the `SCAN HISTORY` button (2).



- Click on a scanned file to view the details of the analysis done.

7.9 Configuring Metadata Rate Limiters

7.9.1 Introduction

In addition to alerts, GCaps generate metadata events on analyzed network flows.
This information can be useful in surveys, but in a certain context, it can quickly exceed the indexing capabilities of the GCenter.
In order to reduce the amount of metadata while maintaining most information exchanges, it is possible to enable the limiters defined below.

7.9.2 Links associated

The graphical interface is described in the *`Metadata rate limiter` screen*.

7.9.3 Prerequisites

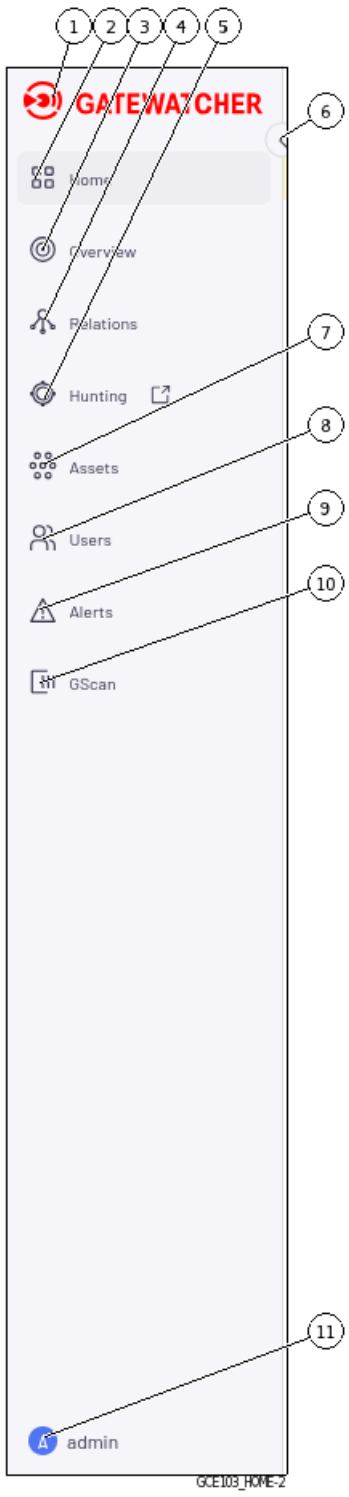
- User: member of **Operator** group

7.9.4 Preliminary operations

- Login to GCenter via a browser (see *Connection to the GCenter web interface via a web browser*)

7.9.5 Procedure to view metadata

- In the navigation bar, click on the `Hunting` button (5).



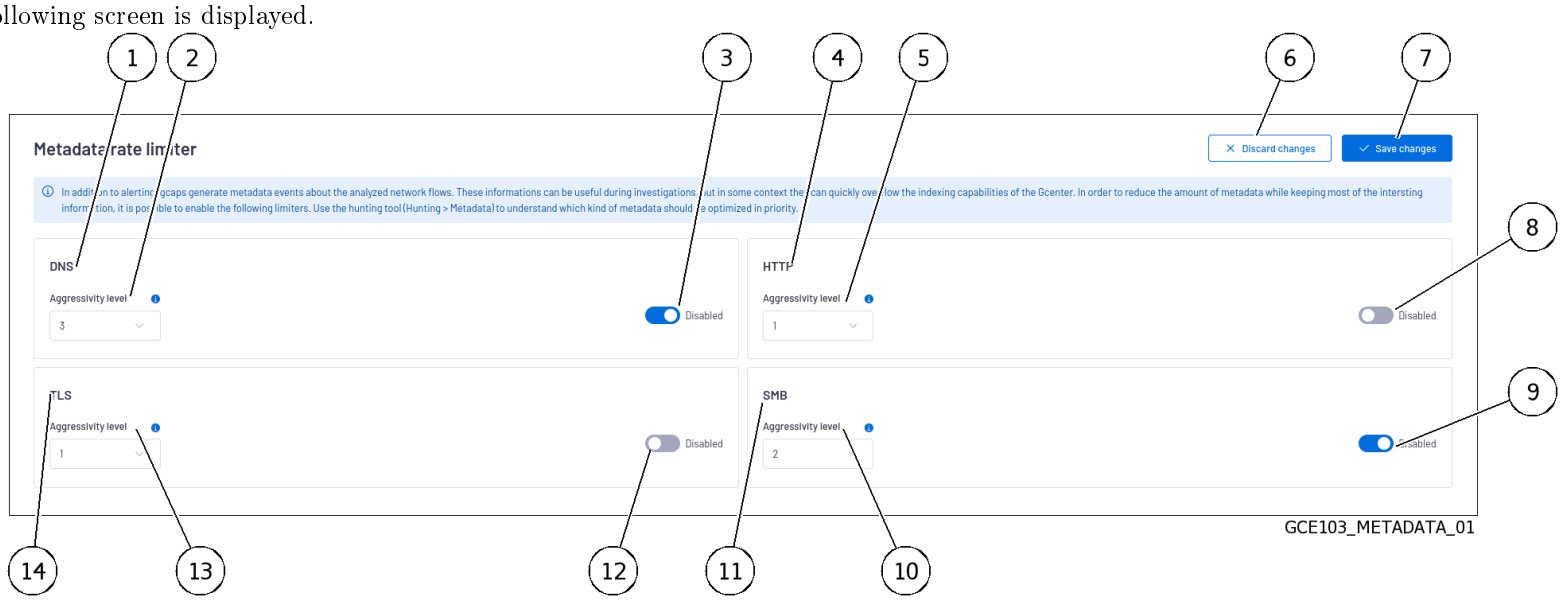
The `Hunting` window is displayed.

This GUI is described in *Main tabs*.

- Use the Kibana tool (hunting > Metadata command) to understand what kind of metadata should be optimized first.

7.9.6 Procedure to setup the limiter then activate

- In the navigation bar, click successively on:
- The `Detection Strategy` menu
- The `Metadata rate limiter` command of the `Detection Strategy` category
  The following screen is displayed.



- If necessary, for the first selected protocol (`DNS`, `HTTP`, `TLS`, `SMB`):
- Select filtration level (`Aggressivity level` field)
- Activate with the selector `Enabled - Disabled`
- Proceed to next protocol
- Validate with the `Save changes` button (7).

7.10 Logging out of the GCenter web interface

7.10.1 Introduction

This procedure describes how to log out of the GCenter web interface.

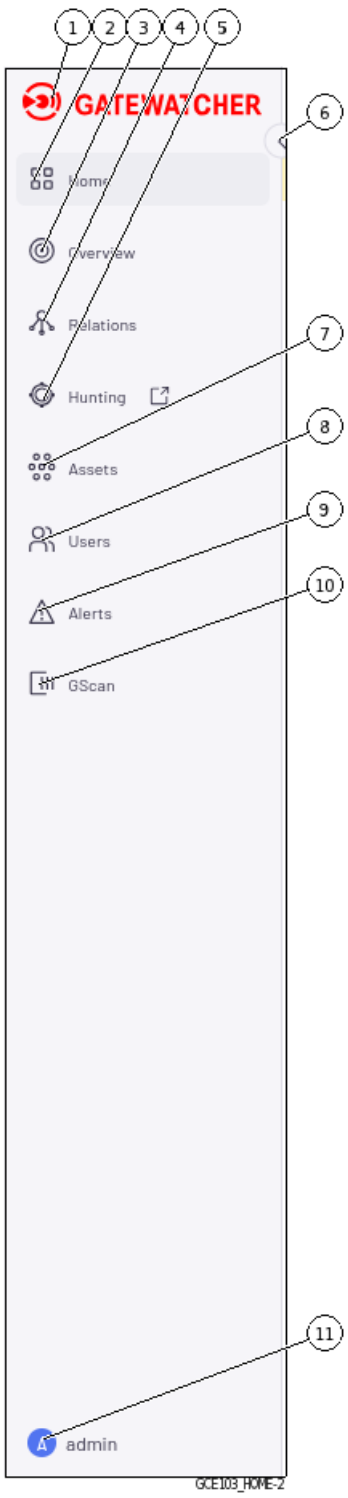
7.10.2 Prerequisites

- User: all users

7.10.3 Preliminary operations

- Accessing GCenter from your workstation (*Connection to the GCenter web interface via a web browser*).

7.10.4 Procedure



- In the GCenter interface, click on the checking account button (11).
- Select the `Logout` command.
  The GCenter interface is closed and the login screen is displayed.

Chapter 8

Use cases of the administrator level

8.1 Connecting to the GCenter web interface via a web browser

8.1.1 Introduction

This procedure describes connecting from a remote computer to the GCenter web interface via a web browser.
This connection is the nominal way to access the web interface of the equipment.

8.1.2 Prerequisites

- User: all users

8.1.3 Preliminary operations

- Know the name of the GCenter or its IP address.
- Access GCenter from your workstation.

8.1.4 Procedure

On the remote PC:

- Open a web browser
- Enter the IP address or FQDN of the GCenter
- Validate.
  The GCenter login window is displayed.
- Enter the login name
- Enter the password
- Validate.
  The GCenter graphical interface is displayed.

Note:

During the first login, it is necessary to change the password.
Passwords must comply with the password policy (see *Password management policy*).

8.2 Configuring the NDR

8.2.1 Introduction

8.2.1.1 The `Assets and users tracking` and `Relationship tracking` functions

The NDR database stores information about:

- the various alerts on the network classified by risk score and type.
- the active equipment management interface presents a list of the various equipment present on the network classified by risk score.
- The different alerts present on the network and displayed in the `Alerts` dashboard classified by risk score (for more information on the dashboard, see *WebUI `Alerts` screen*)
- The different assets present on the network and displayed in the `Assets` dashboard classified by risk score (for more information on the dashboard, see *WebUI `Assets` screen*)
- The different users present on the network and displayed in the `Users` dashboard classified by risk score (for more information on the dashboard, see *WebUI `Users` screen*)

The `Assets and users tracking` and ` Relationship tracking` functions include:

Function	Status	Description	See
`Assets and users tracking`	Activable	Synchronization between the NDR WebUI's `Assets` and `Users` dashboards with the data available in Elasticsearch	See *Procedure to enable the `Assets and users tracking` and `Relationship tracking` functions*.
`Assets and users tracking`	Can disable	The NDR `Assets` and `Users` dashboards are disabled. Data is no longer stored in Elasticsearch.	See *Procedure to disable the `Assets and users tracking` and `Relationship tracking` functions*.
`Relationship tracking`	Activable	synchronization between the NDR `Relations` dashboard in the WebUI and the data available in Elasticsearch	See *Procedure to enable the `Assets and users tracking` and `Relationship tracking` functions*.
`Relationship tracking`	Can disable	The NDR `Relations` dashboard is disabled. Data is no longer stored in Elasticsearch.	See *Procedure to disable the `Assets and users tracking` and `Relationship tracking` functions*.

8.2.1.2 Elasticsearch retention period

The retention time of Elasticsearch depends on the maximum space allocated (in Gb) to store the logs (see the *`Retention policy` screen*).
Therefore, the data retention period in Elasticsearch depends on the amount of logs generated by the GCaps.
The retention period of Elasticsearch can be changed: see the *Procedure to configure the Elasticsearch retention*.

8.2.2 Links associated

See the *`Global settings` screen*.
The configuration interface is described in the *WebUI `Assets` screen*.

8.2.3 Prerequisites

- User: member of **Administrator** group

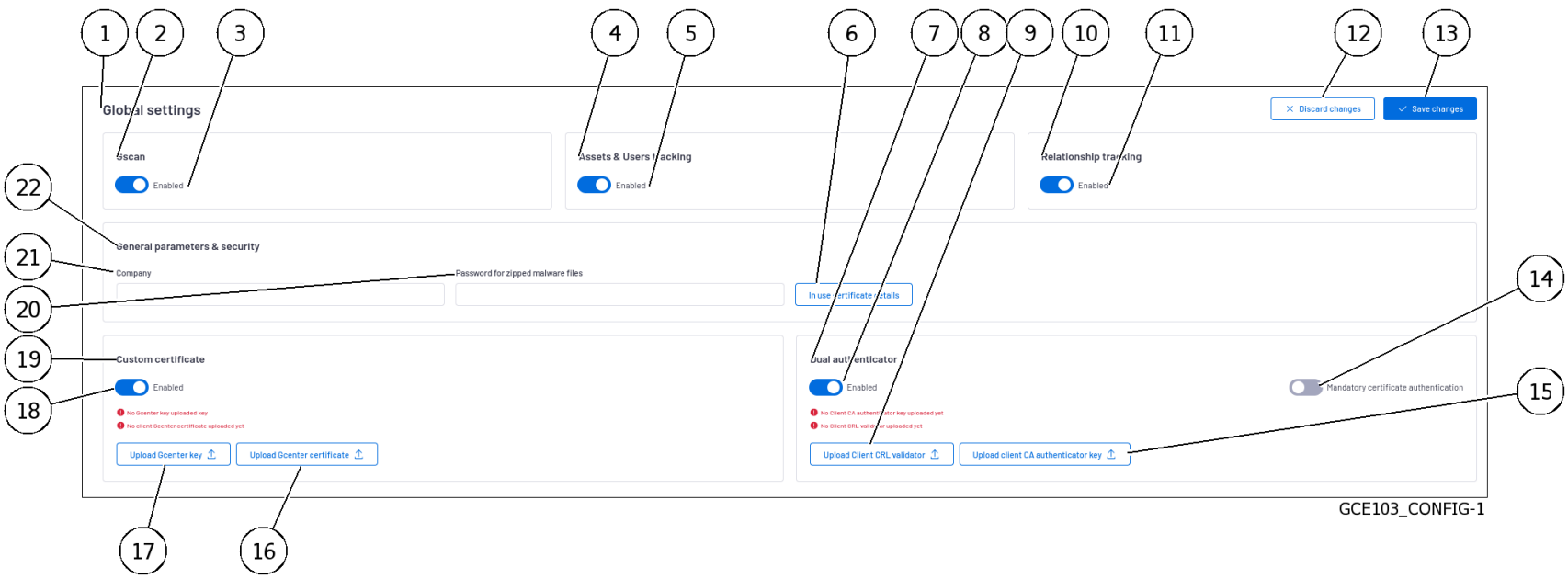
8.2.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.2.5 Procedure to access the `Data Exports` window for an administrator account

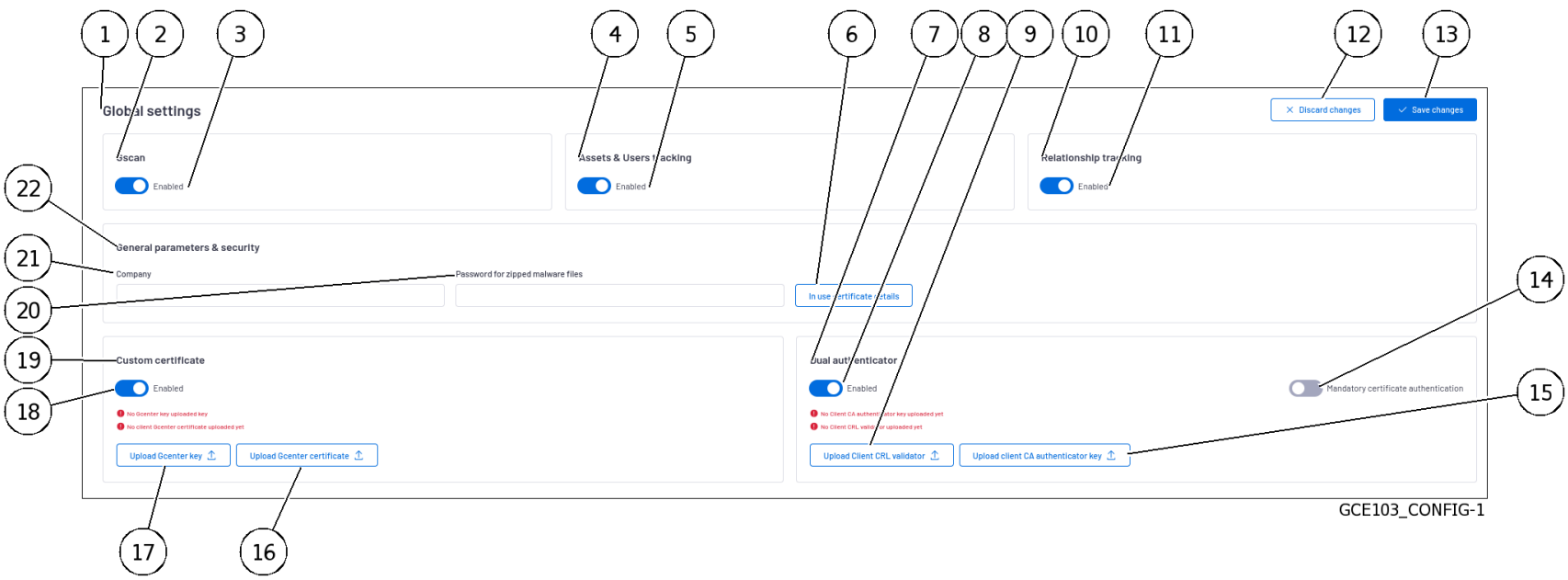
- In the navigation bar, successively click on:
- The `Administration` menu
- The `Global settings export` command in the `System` category
  The `Global settings` screen is displayed.

8.2.6 Procedure to enable the `Assets and users tracking` and `Relationship tracking` functions



- Use the `Assets and users tracking` selector (4) to enable tracking of active assets (`Assets`) and users (`users`).
  The functions visible by pressing the `Assets` and `users` buttons in the WebUI are now accessible if the license enables it.
- Use the `Relationship tracking` selector (10) to enable tracking relations between active devices and view these relations.
  The functions visible by pressing the `Relations` button are now accessible if the license enables it.
- Click on the `Save changes` button (13).

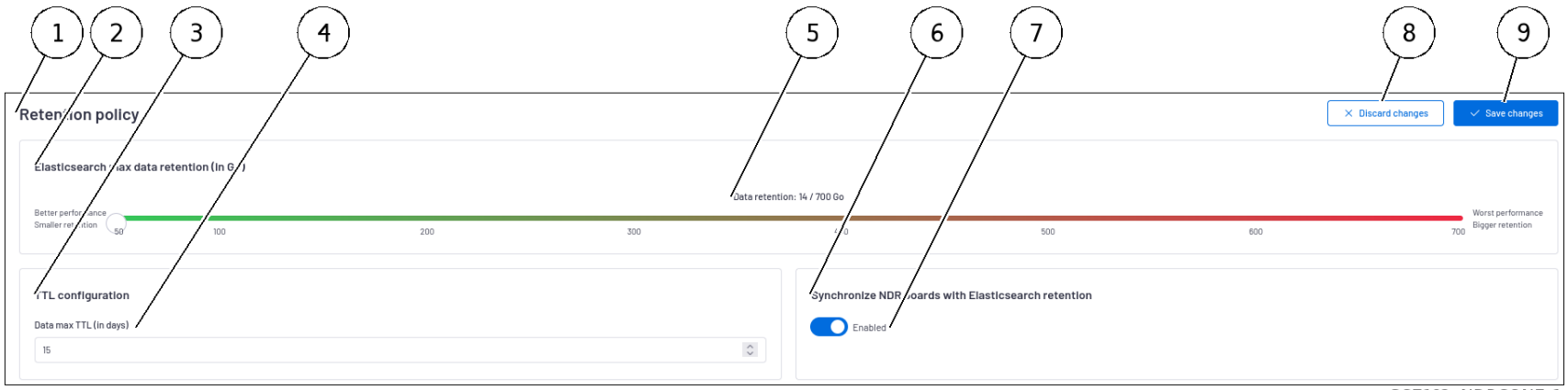
8.2.7 Procedure to disable the `Assets and users tracking` and `Relationship tracking` functions



- To disable the tracking of relations only, use the `Relationships tracking` selector (10).
  The functions visible by pressing the `Relations` button are now inaccessible.
- To disable all the functions of the `Assets and users tracking` (4) and `Relationship tracking` (10), use the `Assets and users tracking` selector (1).
  The functions visible by pressing the `Assets` and `users` buttons in the WebUI are now inaccessible.
- Click on the `Save changes` button (13).

8.2.8 Procedure to configure the Elasticsearch retention

- In the navigation bar, successively click on:
- The `Administration` menu
- The `Retention policy` command in the `Data` category
  The `Retention policy` window is displayed.



GCE103_NDRCONF-1

- Configure the Elasticsearch retention with `Data retention` cursor (5) of the `Elasticsearch max data retention (in Go)` zone (2).
- Use the selector (7) of the `Synchronize NDR boards with elasticsearch retention` zone (6) to enable synchronizing NDR dashboards with data in Elasticsearch.
- Click on the `Save changes` button (9).

8.3 Administrating a GCap

8.3.1 Pairing a GCap with the GCenter

8.3.1.1 Introduction

The GCap probe must be associated to the GCenter in order to receive the network flow.
This procedure complements the procedure "Pairing a GCap with a GCenter" found in the GCap documentation.
This procedure describes the pairing between a GCap and a GCenter.
Pairing enables configuring the IPSec tunnel between the GCap and the GCenter.
The following operations must be performed:

- The *Preliminary operations*
- The *Procedure to set the GCenter IP on the GCap*
- The *Procedure to access the `GCaps pairing` window for an administrator account*
- The *Procedure to set the compatibility mode on the GCap*
- The *Procedure to pair a new GCap in the GCenter*
- The *Procedure to pair the GCap and the GCenter*

8.3.1.2 Links associated

See *`GCaps Pairing` screen*.

8.3.1.3 Prerequisites

- User: member of **Administrator** group

8.3.1.4 Preliminary operations

- Know the **Fully Qualified Domain Name FQDN** (FQDN) of the GCap and its IP address (for example: 'gcapname.domain.com')
- Know the FQDN of the GCenter and its IP address.
- Check whether the date and time of the GCenter and the GCap match.
- On the GCap, obtain the FQDN (hostname.domain) of the GCap via the `show status` command, `Gcap FQDN` line.

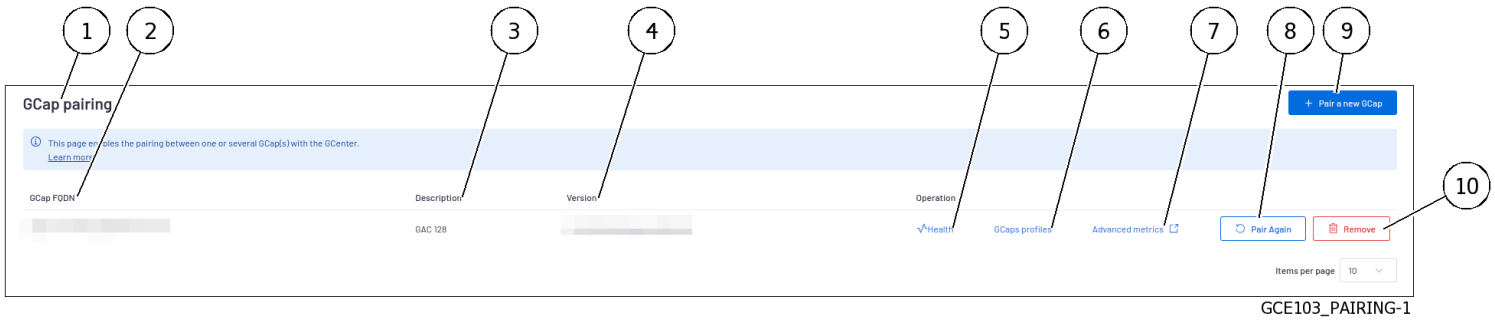
8.3.1.5 Procedure to set the GCenter IP on the GCap

- Apply the "Procedure for setting up the GCenter IP on the GCap" in the "Pairing a GCap with a GCenter" section of the GCAP documentation.

8.3.1.6 Procedure to access the `GCaps pairing` window for an administrator account

- Connect to GCenter via a browser (refer to *Connecting to the GCenter web interface via a web browser*).
- In the navigation bar, successively click on:
  - The `Administration` button
  - The `GCap Pairing` command of the `GCap setup` category

  The `GCap pairing` window is displayed.



GCE103_PAIRING-1

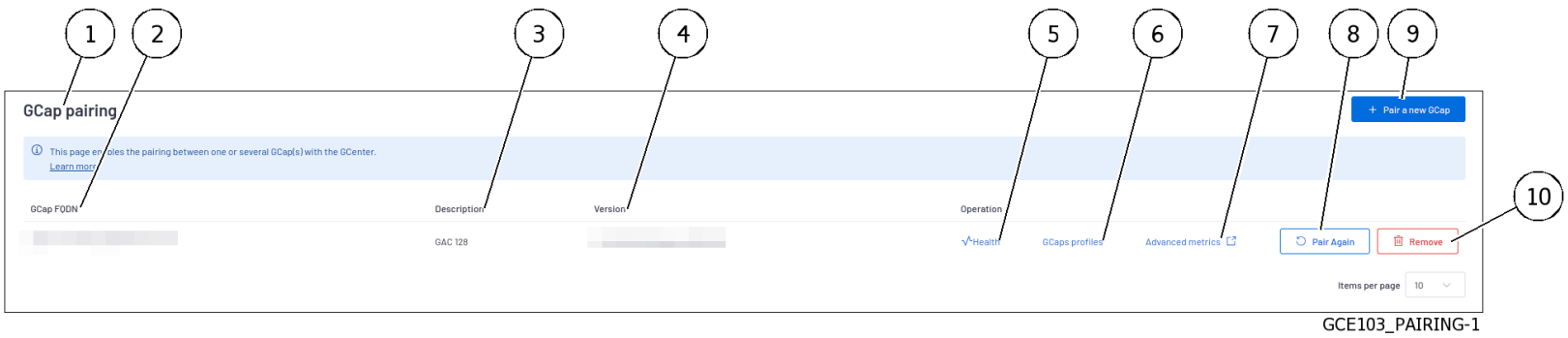
8.3.1.7 Procedure to set the compatibility mode on the GCap

- To view the software version of the GCenter:
- Log into the GCenter and view the GCenter version number
- View the GCenter version in the `Help` menu

  The information is located at the bottom in the `Current GCenter version is` field (Example: GCenter v2.5.3.103).
- To set the compatibility mode, apply the `Procedure for setting the compatibility mode` on the GCap in the GCAP documentation.

8.3.1.8 Procedure to pair a new GCap in the GCenter

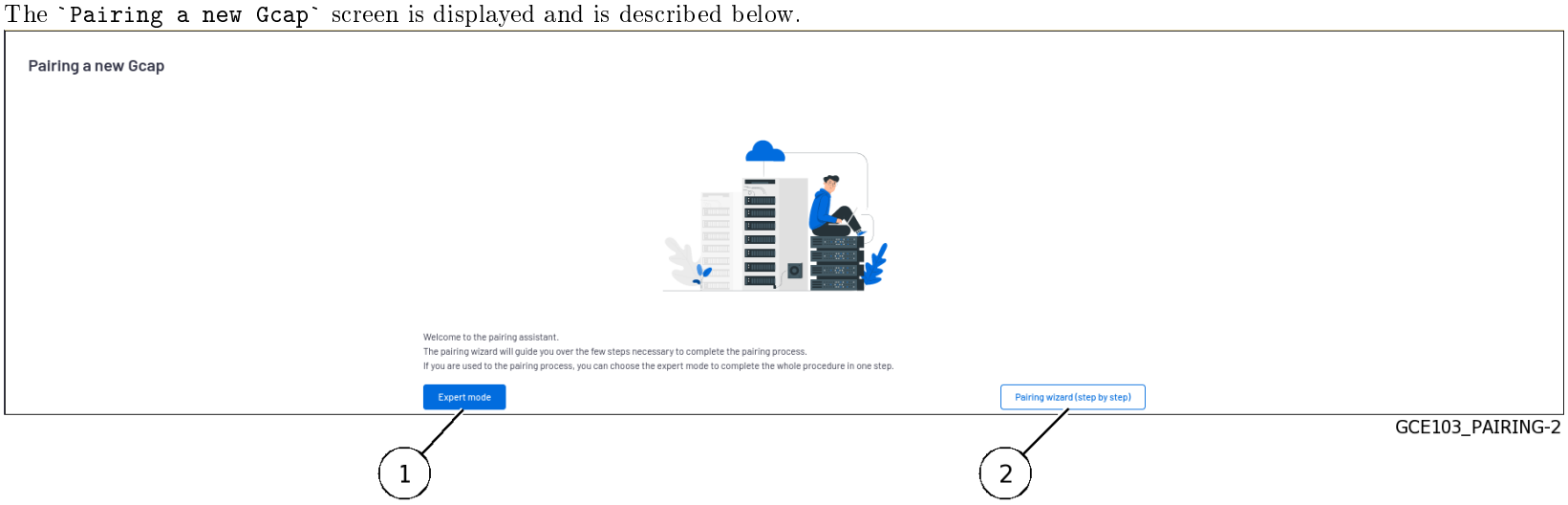
The `GCap pairing` window (1) is displayed.



GCE103_PAIRING-1

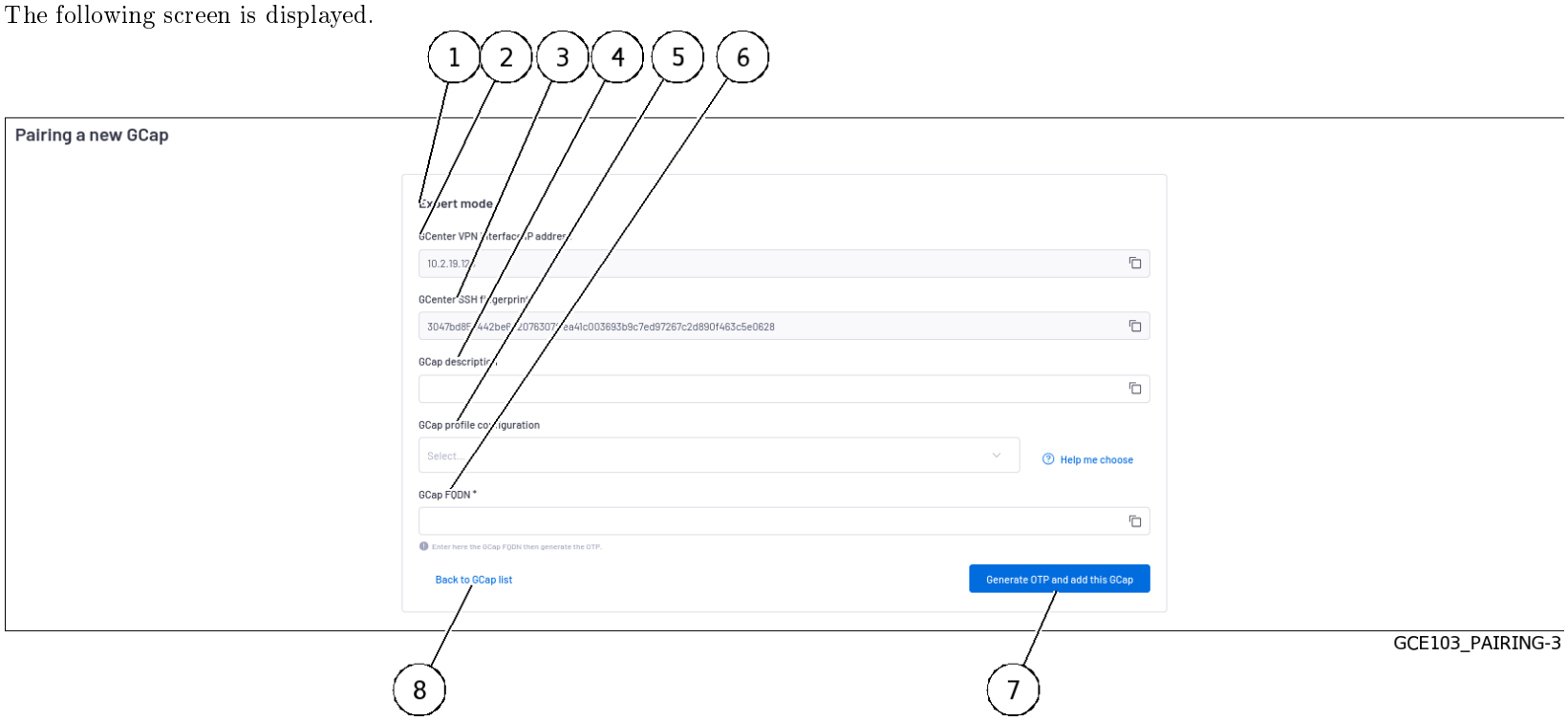
- Click on the `Pair a new GCap` button (9).

The `Pairing a new Gcap` screen is displayed and is described below.



GCE103_PAIRING-2

- Click on the `Expert mode` button (1).
  The following screen is displayed.



GCE103_PAIRING-3

- On the GCenter:
- Enter the IP address of the GCenter VPN interface (2)
  The screen displays the GCenter SSH fingerprint in the field (3).
- Enter a description if necessary in the field (4)
- Select the profile to be applied to the GCap (5)
- Enter the GCap FQDN in the field (6)
- Click on the `Generate OTP and add this GCAP` button (7)

The `SUCCESS` window is displayed showing the OTP (One Time Password).
For example: pcmqsnf7iyo34ianzzi7gbgrr

- Copy the OTP.
- Click on the `OK` button.

8.3.1.9 Procedure to pair the GCap and the GCenter

- On the GCap: perform the operations defined in the `Procedure for Pairing the GCap and GCenter` found in the GCAP documentation.
  After entered the `pairing otp` command with the OPT copied on the gcenter interface, the message is displayed:

```
Resetting any previous GCenter pairing...
Generating IPSec certificates for the GCenter pairing...
Probing for GCenter SSH fingerprint...

Fingerprint for GCenter x is
e655bc02553e2291a486a32bdce3943a315f830de70b2c627c39884e80
1f08b2. Is it correct? (Y/N)
```

- On the GCenter, compare the GCenter fingerprint retrieved by the GCap in the CLI with the one present in the section `GCaps pairing..` under the text `Gcenter SSH fingerprint` in the GCenter web interface on the web browser.

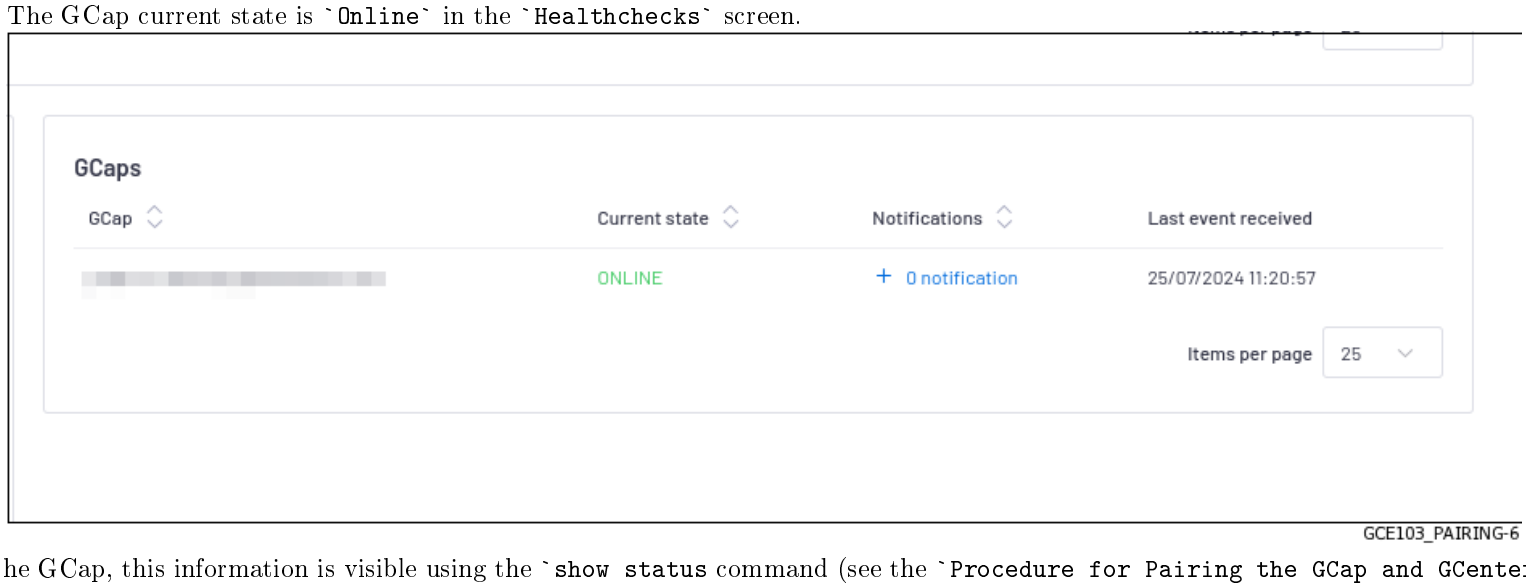
- If the fingerprints are not identical:
- Check the GCenter IP address and the value entered in the GCap
- Check the GCap FQDN and the name entered in the GCenter
- If they are identical, answer **Y** on the GCap and validate.
  After the message is displayed:

```
Pairing successful
```

- On the GCenter WebUI:
  - The `GCap pairing` screen displays the new GCap paired:

GCE103_PAIRING-5

  - The GCap current state is `Online` in the `Healthchecks` screen.



GCE103_PAIRING-6

- On the GCap, this information is visible using the `show status` command (see the `Procedure for Pairing the GCap and GCenter` in the GCAP documentation.

Tip:

The `Paired on GCenter` field takes:
- The value `Not paired` when the GCap is not paired
- The IP value of the GCenter when the GCap is paired

8.3.2 Pairing again a GCap

8.3.2.1 Introduction

This procedure describes the pairing again between a GCap and a GCenter.

Warning:

When pairing again, the VPN tunnel between the GCap and the GCenter is momentarily interrupted.
This means that during this process, data is no longer sent from the GCap to the GCenter, however, the GCap retains the data in order to send it back once the tunnel is re-established.

8.3.2.2 Links associated

See the *`GCaps Pairing` screen*.

8.3.2.3 Prerequisites

- User: member of **Administrator** group

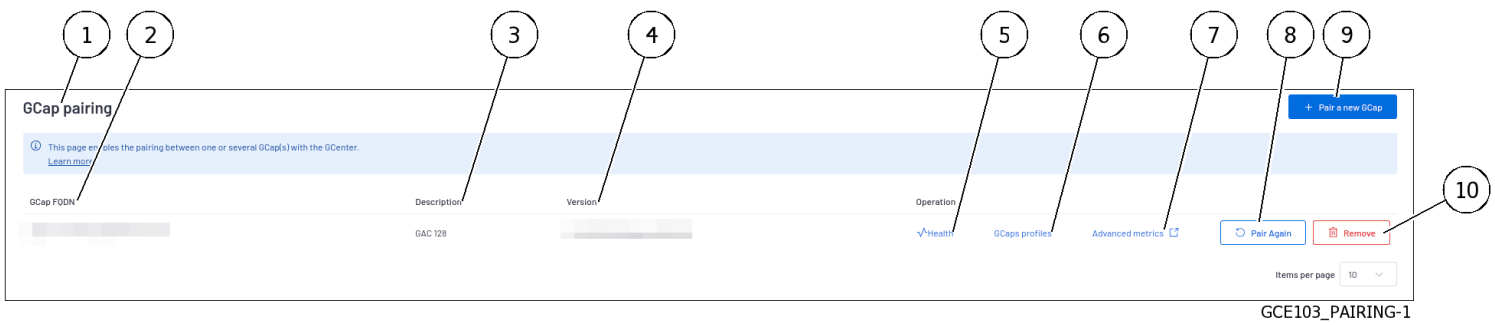
8.3.2.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.3.2.5 Procedure to access the `GCaps pairing` window for an administrator account

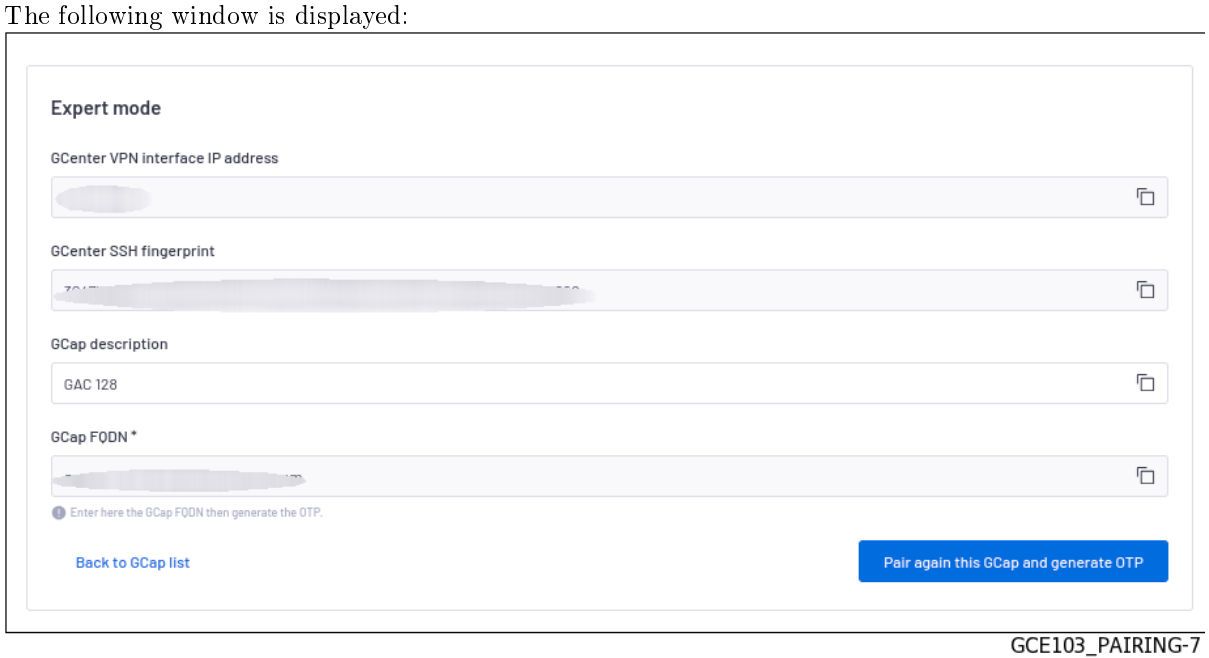
- In the navigation bar, successively click on:
- The `Administration` button
- The `GCap Pairing` command of the `GCap setup` category
  The `GCap pairing` window (1) is displayed.

8.3.2.6 Procedure



GCE103_PAIRING-1

- Click on the `Pair again` button (8).
  The following window is displayed:

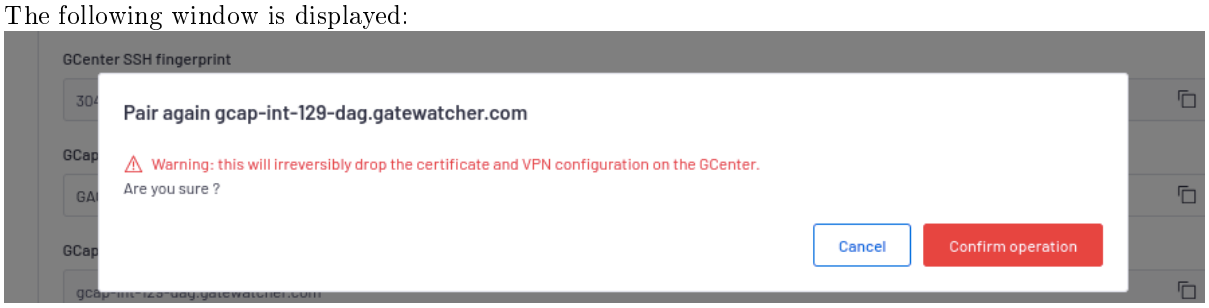


GCE103_PAIRING-7

  The parameters of the current GCap are displayed.

- Click on the `Pair again this GCap and generate OTP` button.

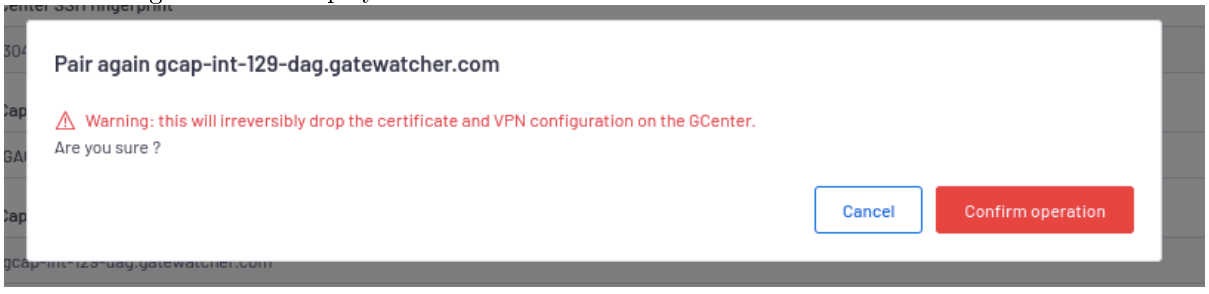
The following window is displayed:



- Click on the `Confirm operation` button.
  The following window is displayed:

GCE103_PAIRING-9

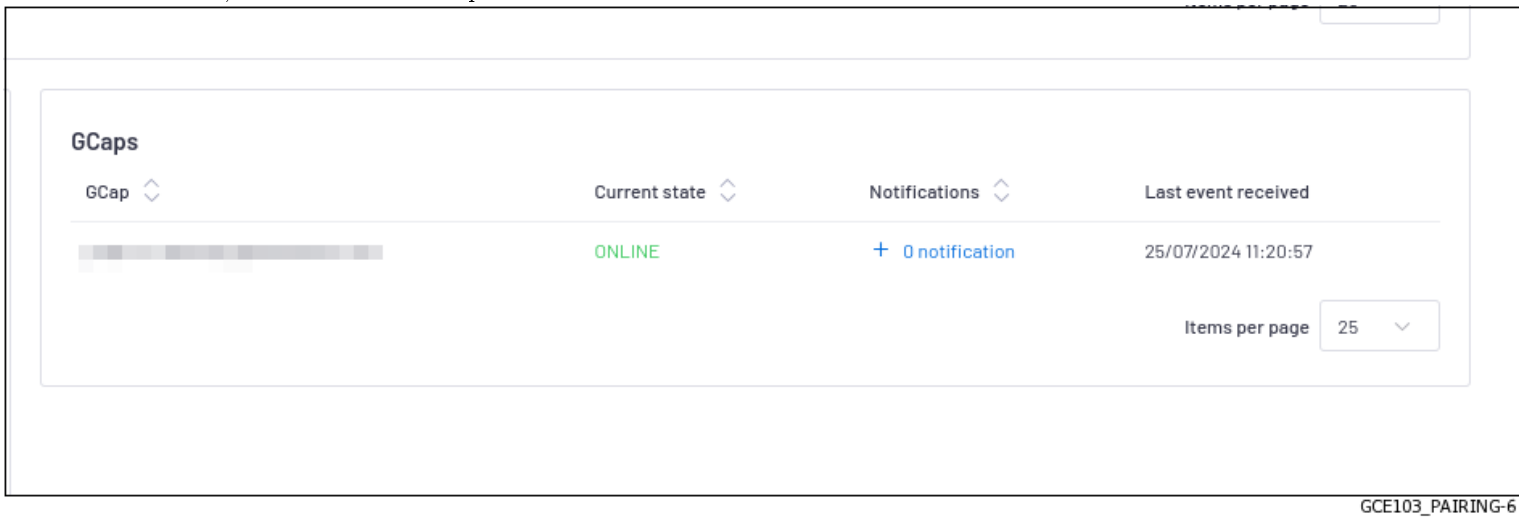
- Click on the `Pair again this GCap and generate OTP` button.
  The following window is displayed:



- Click on the `Confirm operation` button.
- On the GCap, enter the `pairing` command with the OPT copied on the GCenter interface, the message is displayed:
- On the GCenter, compare the GCenter fingerprint retrieved by the GCap in the CLI with the one present in the section `GCaps pairing..` under the text `Gcenter SSH fingerprint` in the GCenter web interface.
- If they are identical, answer **Y** on the GCap and validate.
- On the GCenter, copy the OTP.
- On the GCap, paste the OTP then validate.
  After the message is displayed:

```
Pairing successful
```

- On the GCenter WebUI, check that the GCap current state is `Online` in the `Healthchecks` screen.



GCE103_PAIRING-6

The procedure is finished.

8.4 Managing the GCenter backup and restoration

8.4.1 Setting the backup

8.4.1.1 Introduction

The `Backup/Restore` section of the GCenter enables saving and restoring the data and configuration of the GCenter.
It is possible to:

- Schedule these backups
- Quantify the number of local backups on the GCenter
- Choose the storage location for the backups by selecting one of the three choices

This procedure describes how to configure the GCenter backup process.

To	Apply the procedures
To enable the backup scheduling	1 - Apply the *Procedure to access the `Backup Configuration` screen* 2 - Apply the *Procedure to enable backup scheduling*
To setup the backup	1 - Apply the *Procedure to access the `Backup Configuration` screen* 2 - Apply the *Procedure to setup the backup*

8.4.1.2 Links associated

For more information, see the *Overview of the backup and restoration*.
The graphical interface managing the **configuration** is described in the *`Configuration` screen*.
The graphical interface managing **usage** is described in the *`Backup operations` screen*.

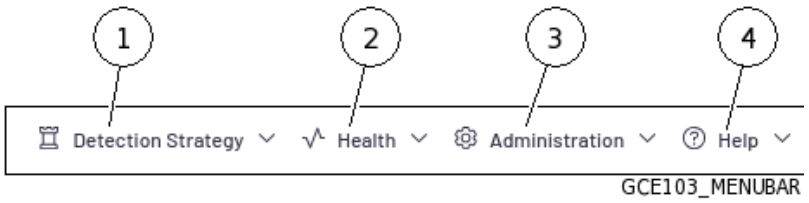
8.4.1.3 Prerequisites

- User: member of **Administrator** group

8.4.1.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.4.1.5 Procedure to access the `Backup Configuration` screen



- Click on the `Administration` menu (3).
- Click on the `Configuration` command from the `Backup and restore` submenu.
  The following screen is displayed.

Backup configuration
General settings
he maximum number of backups saved locally
3
Enable scheduled backup
Daily
Weekly
Monthly
15
Time of day
0:0
14
Scheduled backup progression
No backup operation was recently made
Remote settings
4
Target
Ftp
5
IP Address/Hostname
url
Port
22
Remote backup path
~/
Output interface
mgmt0 - 10.2.19.128
6
Username
Password
password
Password confirmation
password
7
Test configuration
8
Save
BACKUP_CONF-01
13
12
11
10
9

- Use the `Enable scheduled backup` selector (2).
  The backup scheduler area becomes visible (items 3, 14 and 15 are shown).
- Click on one of the buttons (3) defining the frequency (`Daily`, `Weekly`, `Monthly`).
- Click on the `Time of day` field (15).
  A clock is displayed to indicate the hour.

- Select the hour.

  A new clock is displayed to show the minutes.
- Select the minute.

- In the `Weekly` frequency is selected, choose the day of the week.
- In the `Monthly` frequency is selected, choose the day of the month.
- Continue the setup according to the following procedure.

8.4.1.7 Procedure to setup the backup

- Choose the storage location of the backups (4) by selecting one of the following three choices:
  - The `Local` choice: for a local only backup
  - The `SCP` choice: for a backup on a remote SCP server and for a local backup
  - The `FTP` choice: for a backup on a remote FTP server and for a local backup
- Enter the different parameters.

  For more details on these parameters, see the *`Configuration` screen*.
- Check the configuration using the `Test Configuration` button (7).
- Check the remote server to make sure the test file is present.
- Save the configuration using the `Save` button (8).

Important:

Note that it is necessary to change the passive port range of the FTP server to the following settings: [59000:59100]; so that the backup can be loaded correctly.

8.4.2 Operating the backup

8.4.2.1 Introduction

Launching the backup can be:

- Automatic - managed by the scheduler
- Manual

This procedure describes how manual backup works.

8.4.2.2 Links associated

For more information, see the *Overview of the backup and restoration*.
The graphical interface managing the **configuration** is described in the *`Configuration` screen*.
The graphical interface managing **usage** is described in the *`Backup operations` screen*.

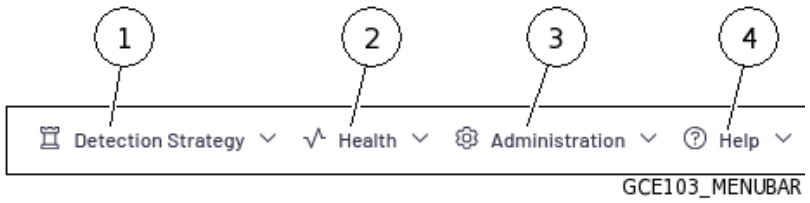
8.4.2.3 Prerequisites

- User: member of **Administrator** group
- Update all engines with the full.gwp package

8.4.2.4 Preliminary operations

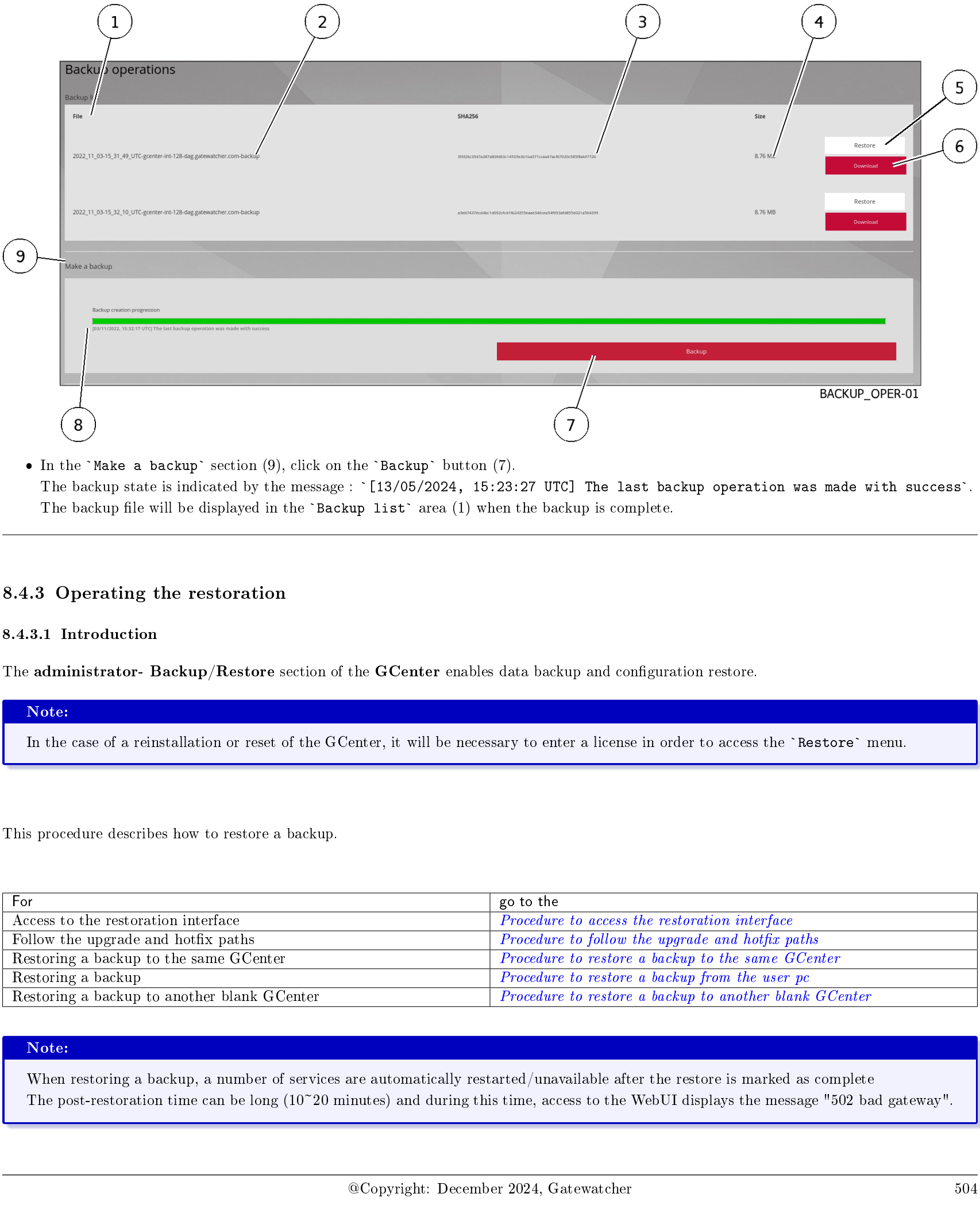
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*) with the prerequisite rights.
- Configure the backup (see the *Setting the backup* procedure).

8.4.2.5 Procedure to operate a manual backup



GCE103_MENUBAR

- Click on the `Administration` menu (3).
- Click on the `Operations` command from the `Backup and restore` submenu.
  The following screen is displayed.



BACKUP_OPER-01

- In the `Make a backup` section (9), click on the `Backup` button (7).
  The backup state is indicated by the message : `[13/05/2024, 15:23:27 UTC] The last backup operation was made with success`.
  The backup file will be displayed in the `Backup list` area (1) when the backup is complete.

8.4.3 Operating the restoration

8.4.3.1 Introduction

The **administrator- Backup/Restore** section of the **GCenter** enables data backup and configuration restore.

Note:

In the case of a reinstallation or reset of the GCenter, it will be necessary to enter a license in order to access the `Restore` menu.

This procedure describes how to restore a backup.

For	go to the
Access to the restoration interface	*Procedure to access the restoration interface*
Follow the upgrade and hotfix paths	*Procedure to follow the upgrade and hotfix paths*
Restoring a backup to the same GCenter	*Procedure to restore a backup to the same GCenter*
Restoring a backup	*Procedure to restore a backup from the user pc*
Restoring a backup to another blank GCenter	*Procedure to restore a backup to another blank GCenter*

Note:

When restoring a backup, a number of services are automatically restarted/unavailable after the restore is marked as complete
The post-restoration time can be long (10~20 minutes) and during this time, access to the WebUI displays the message "502 bad gateway".

Important:

It is possible to restore a backup on a GCenter with a different IP configuration.
Before performing this operation, all network interfaces present on the source GCenter must be active and configured on the target GCenter.
Example:

- The source GCenter has two active interfaces (MGMT0 and VPN0).
- Both interfaces must be enabled and configured at the IP level on the target GCenter before performing the restore.

8.4.3.2 Links associated

For more information, see the *Overview of the backup and restoration*.
The graphical interface managing the **configuration** is described in the *`Configuration` screen*.
The graphical interface managing **usage** is described in the *`Backup operations` screen*.

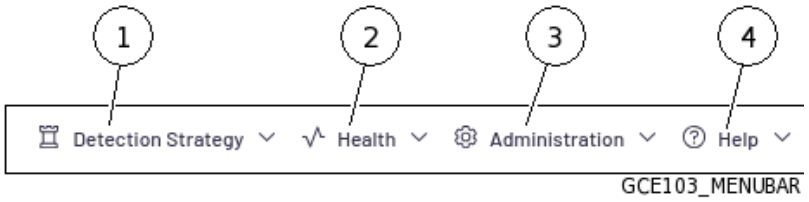
8.4.3.3 Prerequisites

- User: member of **Administrator** group

8.4.3.4 Preliminary operations

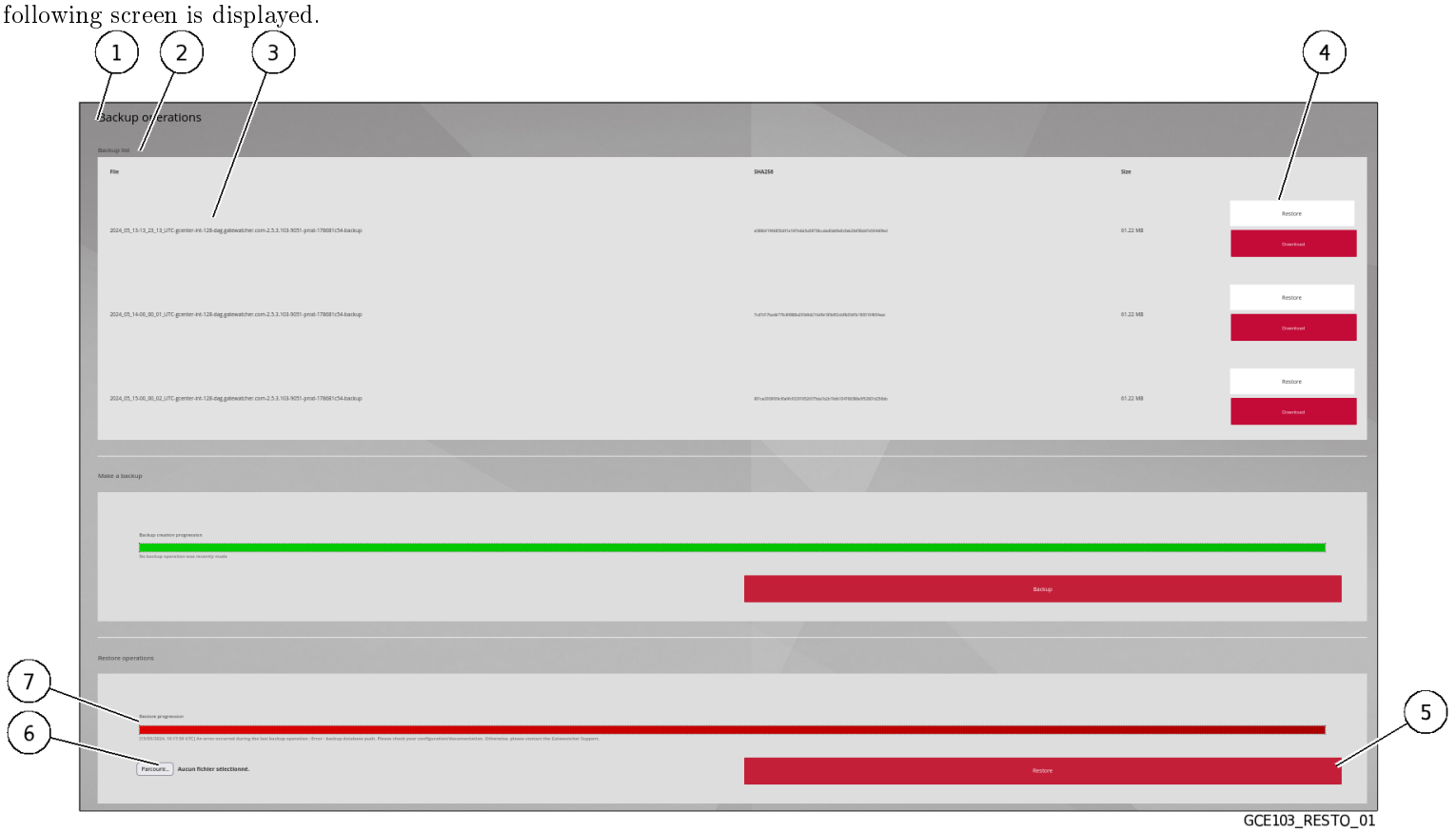
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.4.3.5 Procedure to access the restoration interface



GCE103_MENUBAR

- Click on the `Administration` menu (3).
- Click on the `Operations` command from the `Backup and restore` submenu.
  The following screen is displayed.



GCE103_RESTO_01

8.4.3.6 Procedure to follow the upgrade and hotfix paths

Tip:

Since the upgrade and hotfix path is not specified in the backup name, it is imperative to set up a tracking of these paths.

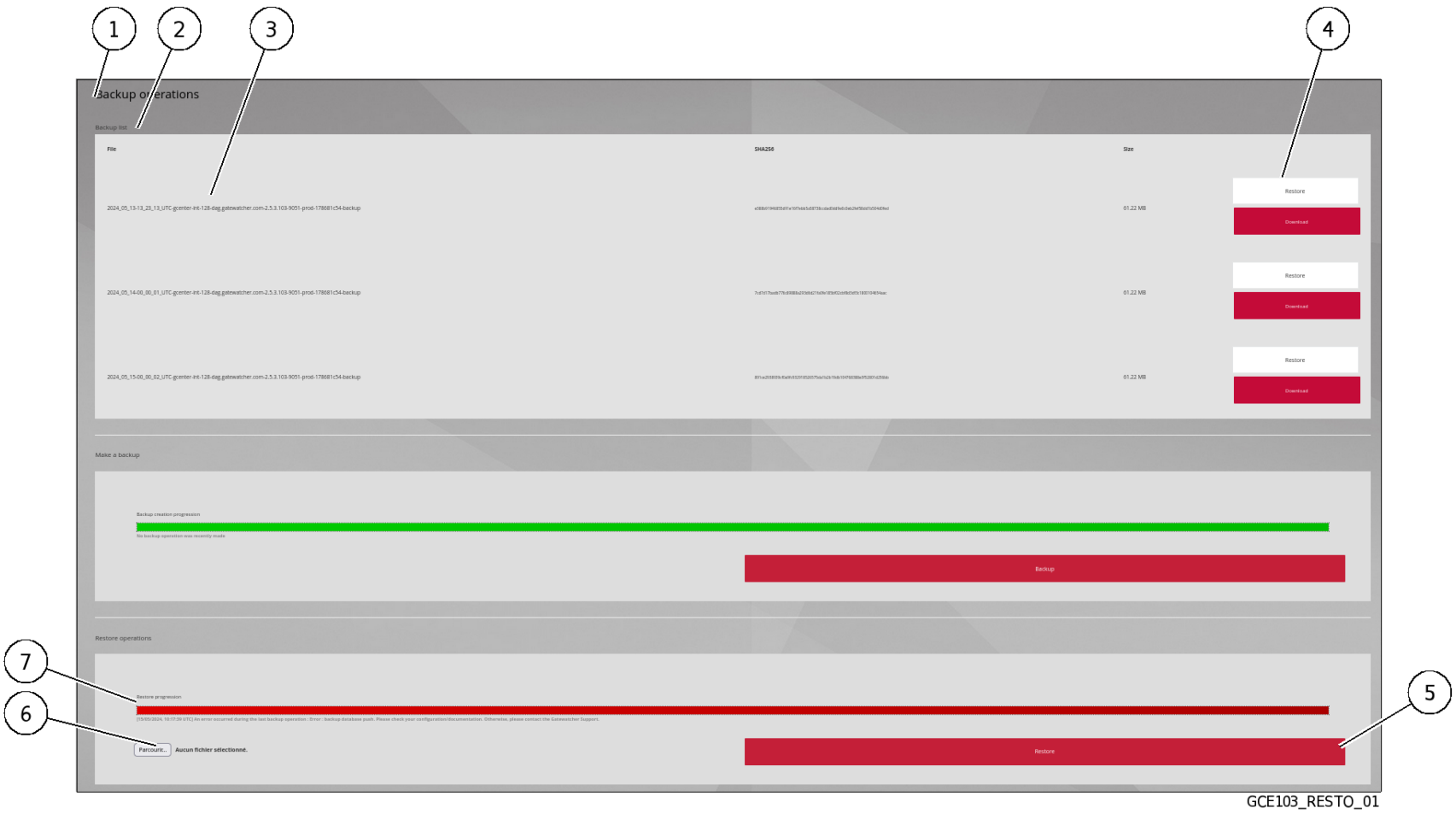
To do this, when downloading or exporting the SCP or FTP of the backup:

- Create a tree structure indicating the current version of the GCenter (example: 2.5.3.102-XXXX-HFX)
- Store the downloaded or exported backup in this folder
- Modify the tree structure each time a version is upgraded or a hotfix is applied
- Use the backup in the directory of the GCenter version to be restored

---

8.4.3.6.1 Procedure to restore a backup to the same GCenter

The `Backup operations` screen (1) is displayed.



- Choose the backup to be restored (3) in the `Backup list` area (2)
- Click the `Restore` button (4) of the backup to be restored.
  The restoration operates immediately.
  The status is given in the `Restore progression` field (7).
  After restarting the GCenter, the backup will be restored.

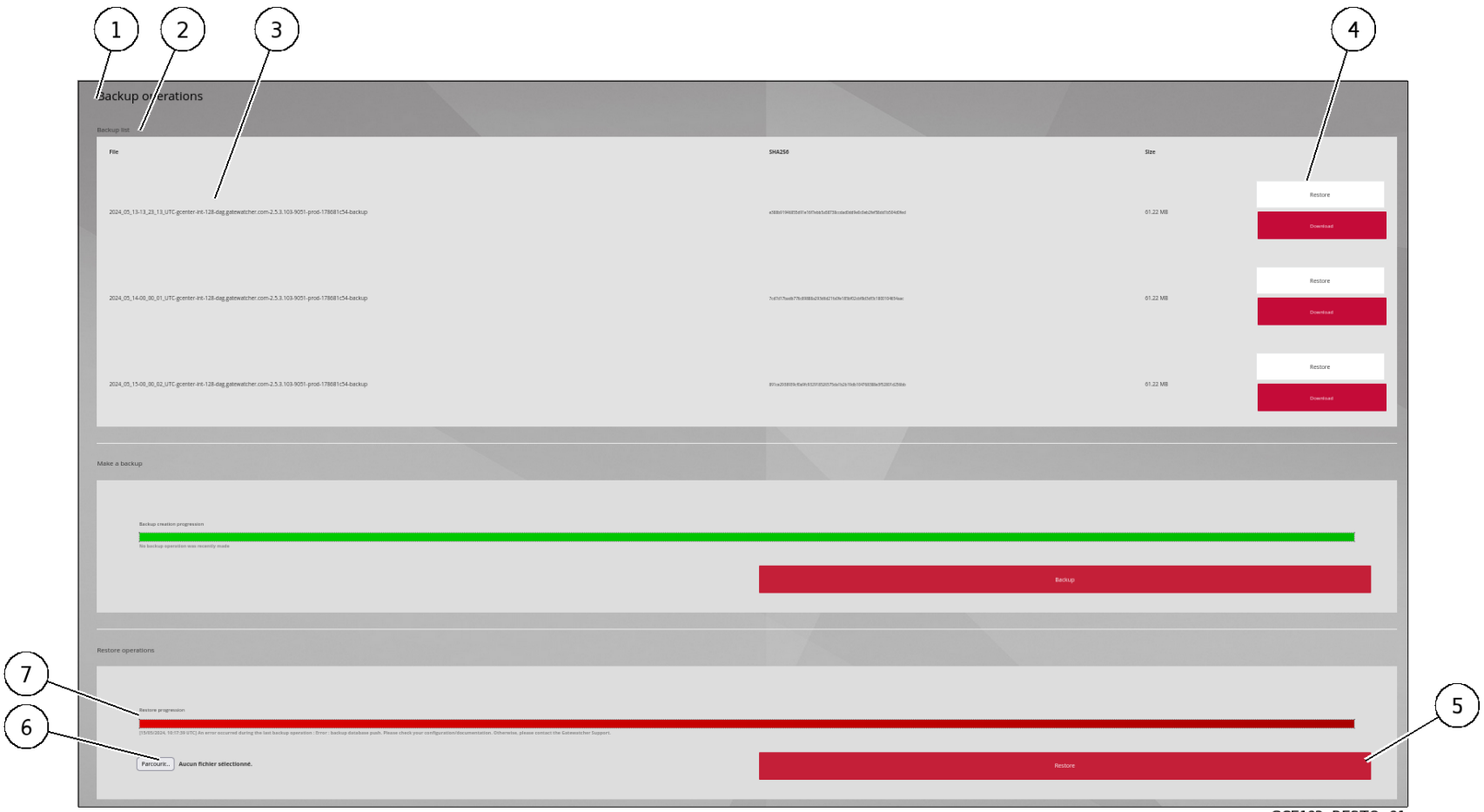
Note:

It is essential that the upgrade path be respected, as indicated in the *Procedure to follow the upgrade and hotfix paths*.

8.4.3.6.2 Procedure to restore a backup from the user pc

Note:

The backup to restore has to be located onto a directory of the user pc. If this backup is located on a backup server, move this backup file to the local directory.



- Click on the `Browse` button (6).
- Select the backup to restore from the local directory and validate.
- Click on the `Restore` button (5).

  The status is given in the `Restore progression` field (7).

  After restarting the GCenter, the backup will be restored.

Note:

It is essential that the upgrade path be respected, as indicated in the *Procedure to follow the upgrade and hotfix paths*.

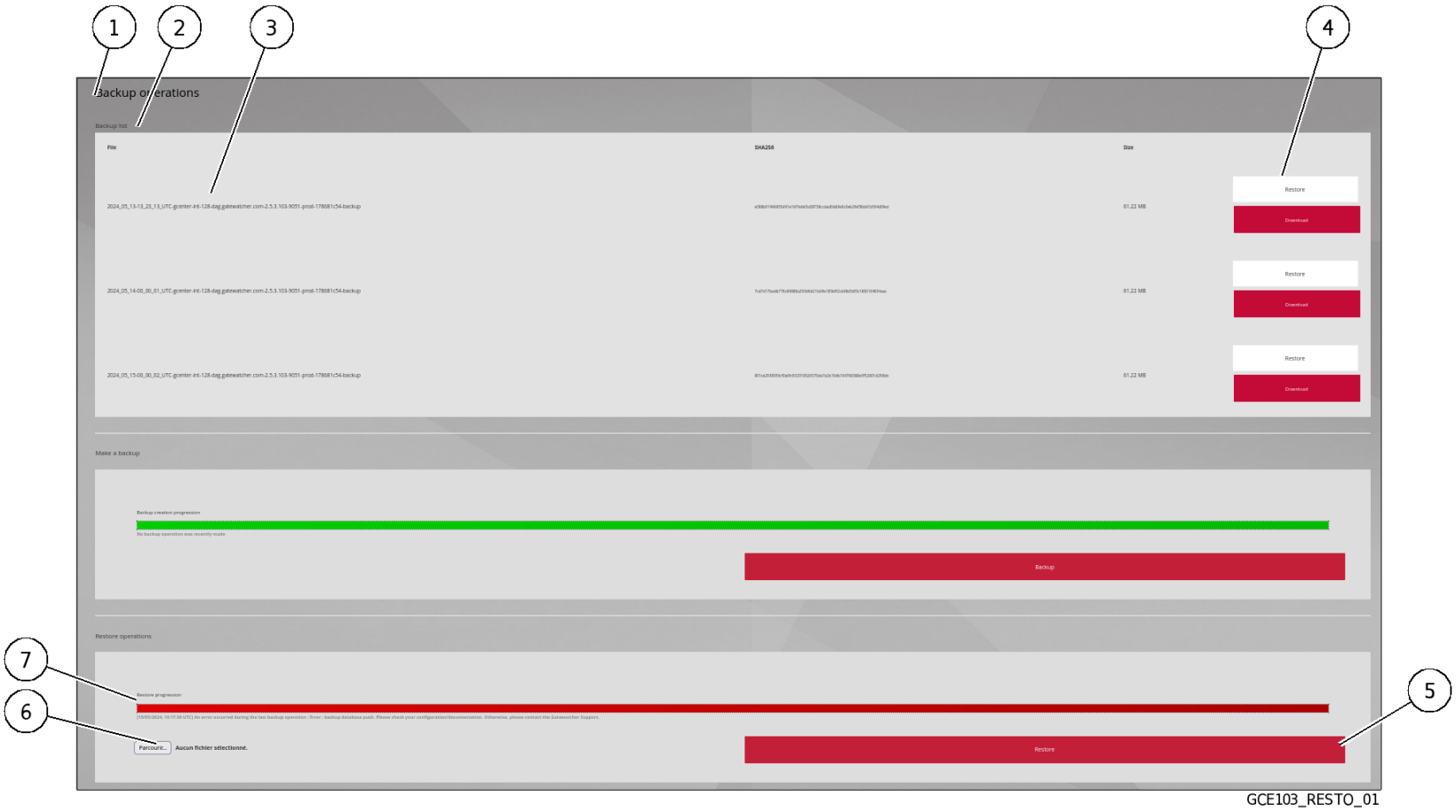
8.4.3.6.3 Procedure to restore a backup to another blank GCenter

In the event of a GCenter replacement, it is mandatory to respect these criteria before restoring the backup:

- Reinstall the new GCenter along the same upgrade and hotfix path as the old GCenter
- Name the new GCenter in the same way as the old GCenter (same FQDN)
- Configure the network section of the new GCenter, allowing access to the WebUI
- Apply the license to the new GCenter in order to access all the configurations. Until a license is entered, the WebUI is blocked on the license page.

Once the above steps are completed:

- Access the restoration page as described in the previous procedures



GCE103_RESTO_01

- Click on the `Browse` button (6)
- Select the backup to restore from the local directory and validate
- Click on the `Restore` button (5)

  The status is given in the `Restore progression` field (7)

  After restarting the GCenter, the backup is restored

8.5 Managing of the GCenter software

8.5.1 Configuring automatic update of signatures and/or anti-viral engines

8.5.1.1 Introduction

Threat DB updates module manages the updates.
This procedure describes how to configure automatic update from:

- A server on the local network (choice `local`)
- A server on the Internet (choice `online`)

Note:

To maximize the effectiveness of updates, it is advisable to download these updates as soon as they appear on https://update.gatewatcher.com
To do this, connect to the site to view the time of creation of these updates and schedule the daily frequency and the time that follows that of the creation of packages.

8.5.1.2 Links associated

See the *Update presentation*.
The update packages are available in the https://update.gatewatcher.com/update/.
The automatic configuration screen is described in the *`Threat DB update` screen*.

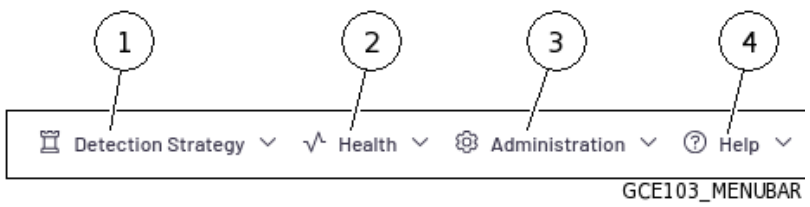
8.5.1.3 Prerequisites

- User: member of **Administrator** group

8.5.1.4 Preliminary operations

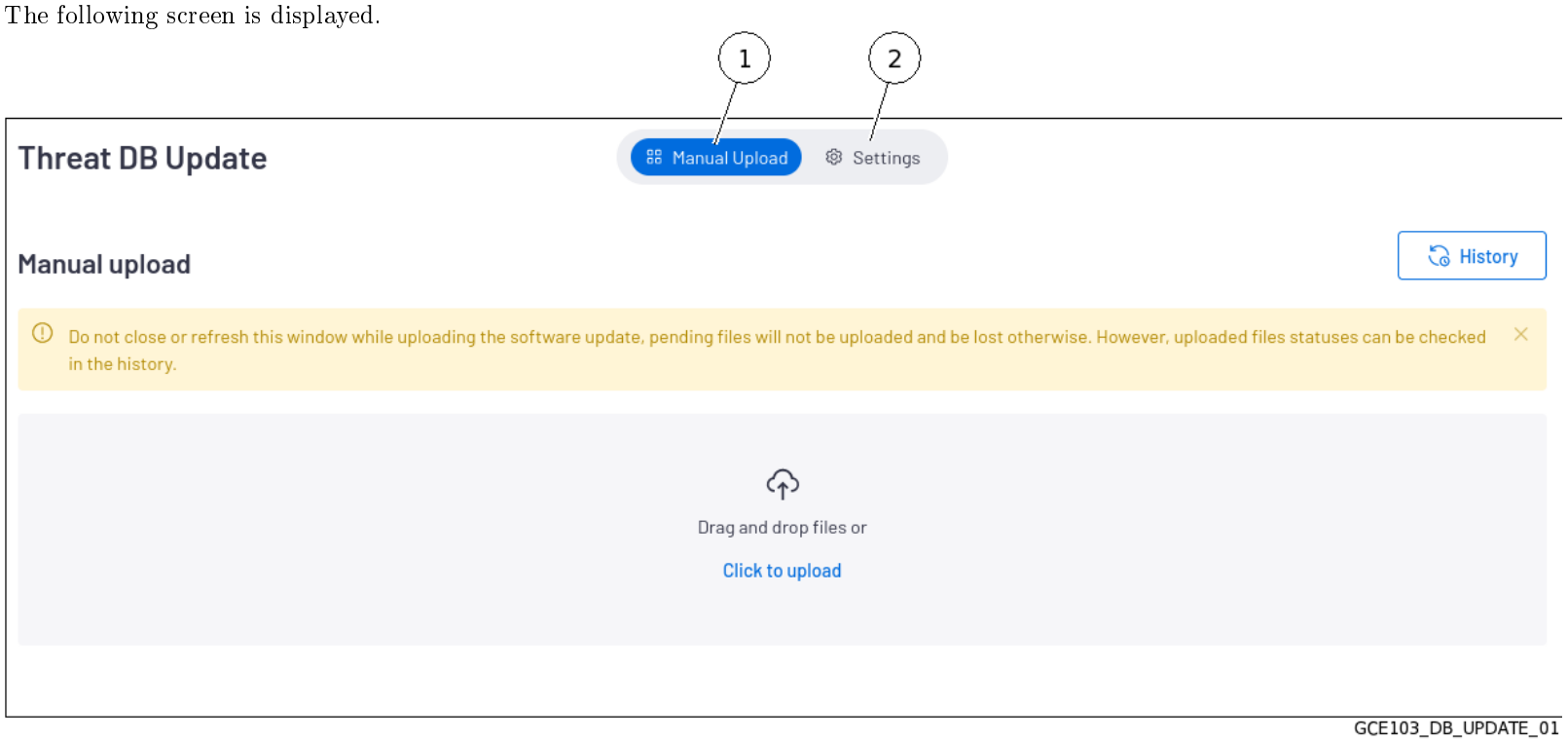
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*) with the prerequisite rights.

8.5.1.5 Procedure to access the `Settings` screen



GCE103_MENUBAR

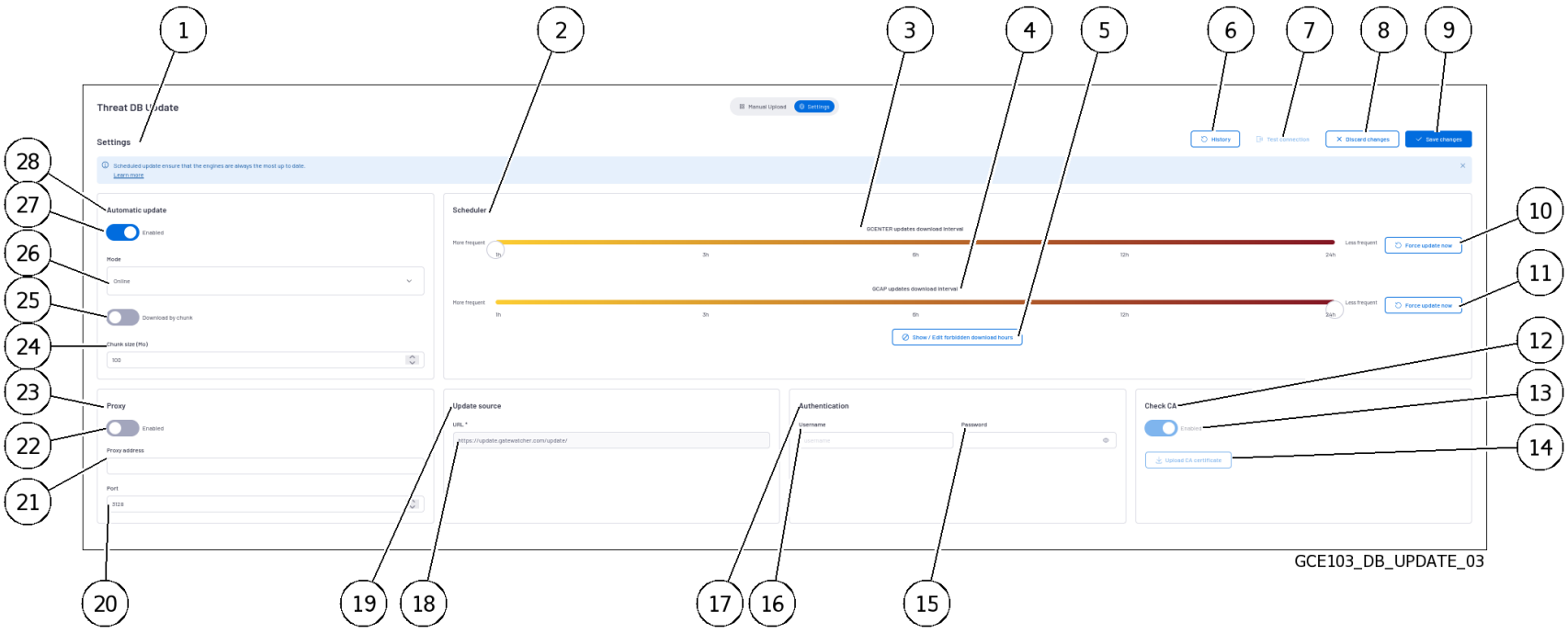
- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Threat DB update` command from the `Updates` submenu.
  The following screen is displayed.



GCE103_DB_UPDATE_01

- Click on the `Settings` button (2).
  The `Settings` window is displayed.
- Perform the *Procedure to setup the Online Mode*
  or
  Perform the *Procedure to setup the Local mode*

8.5.1.6 Procedure to setup the Online Mode



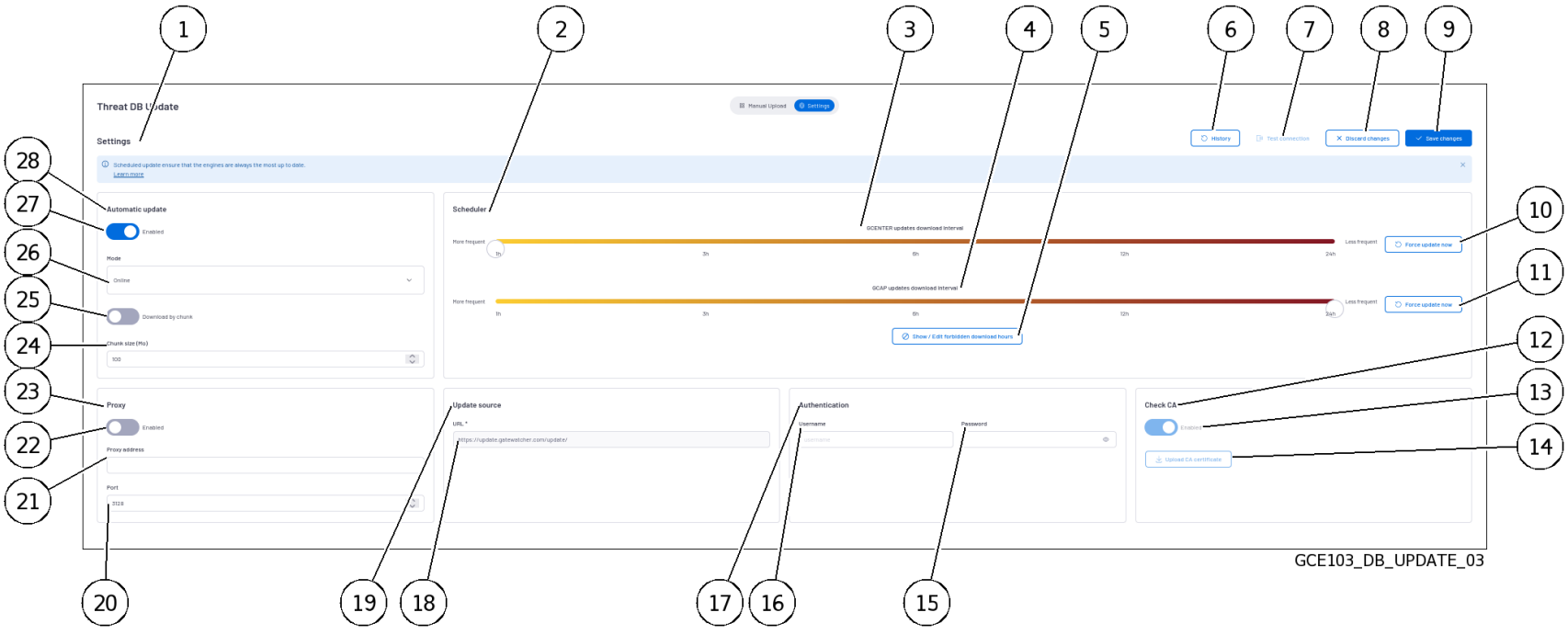
- Configure the update parameters in the `Automatic update` area (28):
  - Click on the `Enabled` selector (27) to activate the function.
  - Select the **Online** choice in the `Mode` zone (26).
    The URL (18) field is automatically filled.
  - If needed, configure the `Download by chunk` function:
    - Click on the `Download by chunk` selector (25) to activate the function
    - Choose the `Chunk size` (24)
- Configure the proxy (23) if needed to connect to the update.gatewatcher.com site:
  - Use the `Enabled` selector (22) to activate the function
  - Enter the proxy server address as an IP address or FQDN in the `Proxy address` field (21)
  - Enter the Proxy Listening Port (1-65535) (20)
- Configure frequency of updates in the `Scheduler` area (2):
  - Use the `GCENTER updates download interval` cursor (3) to the desired value
  - Use the `GCAP updates download interval` cursor (4) to the desired value
  - Click on the `Show / Edit forbidden download hours` button (5) to display or change the schedule of prohibited hours:
    - Define the forbidden download hours then validate with the `Save` button (9).
- Configure the `Authentication` feature (17) to connect to the update.gatewatcher.com site:
  - `Username`: field (16)
  - `Password`: field (15)

Note:

The `Update source` field (19) is automatically entered.
The `Check CA` field (12) is not used on Online mode.

- Click the `Save changes` button (9).
- To test the connection with the current parameters, use the `Test connection` (7) button.
  If the test is ok, the following message is displayed: Update settings are valid.
- To download immediately updates, use:
  - `Force update now` button (10) for the GCenter
  - `Force update now` button (11) for the GCap

8.5.1.7 Procedure to setup the Local mode



Prerequisites:

- In the case of local mode, perform the local repository configuration prerequisites:

- The server must be reachable in HTTP on port 80
- Create the following tree structure: "2.5.3.10X/GCenter" according to the GCenter version (2.5.3.100 or 2.5.3.101)
- Retrieve the necessary gwp files (full.gwp for example) on https://update.gatewatcher.com/update/
- In "2.5.3.10X/gcenter", put the previously retrieved gwp file
- In "2.5.3.10X/gcenter", put a sha256s file that contains an entry "sha256sum NomDuFichier"

Note:

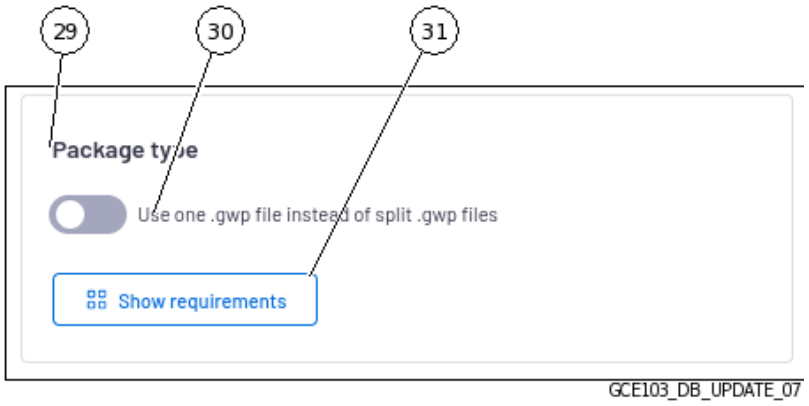
The 2.5.3.10X folder must be at the root of the HTTP server that was previously launched for the local mode to work.

Note:

To maximize the effectiveness of updates, it is advisable to download these updates as soon as they appear on https://update.gatewatcher.com (python script for example)
To do this, connect to the site to view the time of creation of these updates.
Consider the existing infrastructure to upload these files (+5GB) to the local repository.
Schedule the daily frequency and time following that of making available on the local depot.

- Configure the update parameters in the `Automatic update` area (28):
  - Click on the `Enabled` selector (27) to activate the function
  - Select the **Local** choice in the `Mode` zone (26)
    The URL (18) fields are automatically filled.
  - If needed, configure the `Download by chunk` function:
    - Click on the `Download by chunk` selector (25) to activate the function
    - Choose the `Chunk size` (24)
- Configure the `Proxy` (23) if needed to connect to the local repository:
  - Use the `Enabled` selector (22) to activate the function
  - Enter the proxy server address as an IP address or FQDN in the `Proxy address` field (21)
  - Enter the Proxy Listening Port (1-65535) (20)
- Configure frequency of updates in the `Scheduler` area (2):
  - Use the `GCENTER updates download interval` cursor (3) to the desired value
  - Use the `GCAP updates download interval` cursor (4) to the desired value
  - Click on the `Show / Edit forbidden download hours` button (5) to display or change the schedule of prohibited hours:
    - Define the forbidden download hours then validate with the `Save` button.
- If needed, configure the `Authentication` (17) feature to connect to the local repository:
  - `Username`: field (16)
  - `Password`: field (15)
- If needed, configure the certificate int in the `Check CA` area (12):
  - Use the `Enabled` selector (13) to activate the feature
  - Use the `Upload CA file` button (14) to download the certificate file

At the bottom of the screen, there is the following category:



- Choose the engine .gwp file(s) to be downloaded:
  - Use the `Use one .gwp file instead of split .gwp files` button (30):
    - If enabled, the file downloaded is the full.gwp file

      If disabled, the files downloaded are the engine .gwp files (one file per detection engine and one per Malcore engine)
  - To have information to the current choice, the list of file to be downloaded , click the `Show requirements` button.
- Click the `Save changes` button (9).
- To test the connection with the current parameters, use the `Test connection` button (7).

  If the test is ok, the following message is displayed: Update settings are valid.
- To download immediately updates, use:
  - `Force update now` button (10) for the GCenter
  - `Force update now` button (11) for the GCap

8.5.2 Installing an update manually

8.5.2.1 Introduction

This procedure describes the various options for updating the signature files of the solution's detection engines.
To know the engine which needs to be updated, see the *`Health checks` screen*.

8.5.2.2 Links associated

See the *Update presentation*.
The update packages are available here (https://update.gatewatcher.com/update/).
The graphical interface is described in the *`Threat DB update` screen*.
Updates can be done automatically: for this, see the *Configuring automatic update of signatures and/or anti-viral engines* procedure.

8.5.2.3 Prerequisites

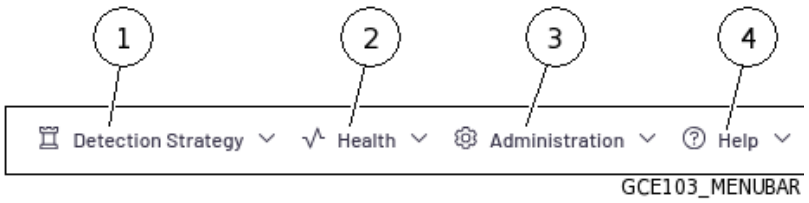
- User: member of **Administrator** group

8.5.2.4 Preliminary operations

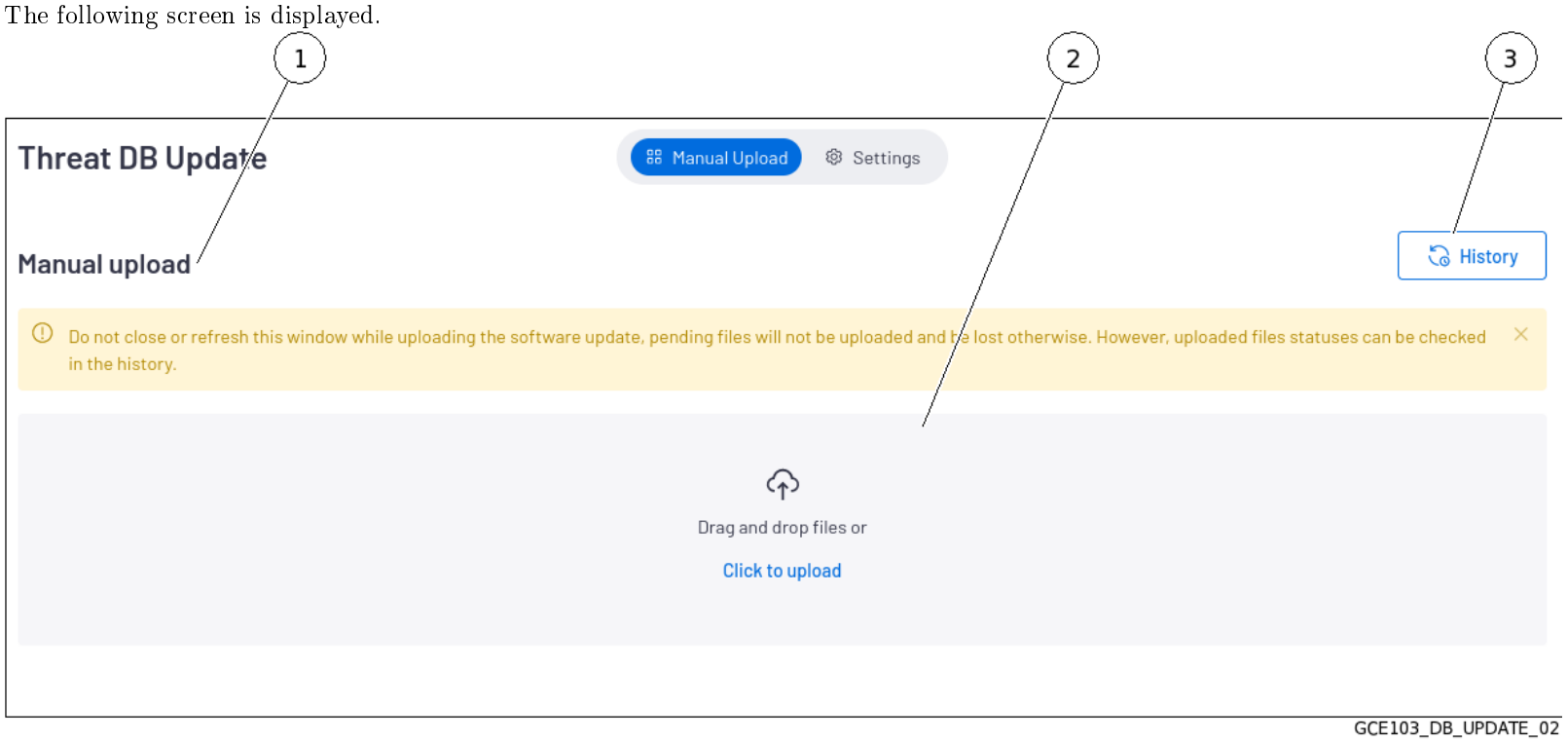
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*) with the prerequisite rights.
- Check the engine which has to be updated (see *`Health checks` screen*).
- Download the package from https://update.gatewatcher.com/update/.

To update the engine	Use the file
Beacon detect engine	beacon.gwp
Active CTI engine	cti.gwp
DGA detect engine	dga.gwp
Malcore (all motors)	malcore.gwp
One or several malcore engines	engine hash.gwp + common_utilities.gwp
Sigflow	sigflow.gwp
All engines	full.gwp

8.5.2.5 Procedure



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Threat DB update` command from the `Updates` submenu.
  The following screen is displayed.



- Click on the area (2).
  A window is displayed to select the package to download.
- Select the previously downloaded package.

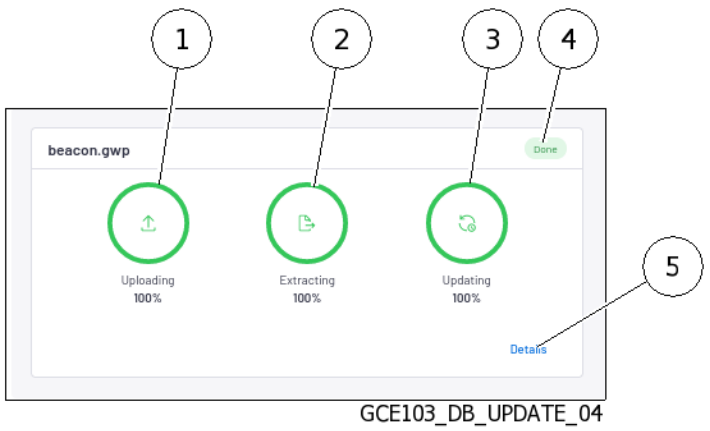
Note:

If the selected file is not an update file but an upgrade file then a message is displayed as the following example.

```
An error occurred during the last gum operation : Error : Gwp file decryption error, are you sure it is a␣
↪TypeGwp.THREAT_DB_UPDATE ?
Please check your configuration/documentation. Otherwise, please contact the Gatewatcher Support.
```

- Validate.
  The update begins and is made in the following steps:
  - The uploading (1)
  - The extracting (2)
  - The updating (3)

  The status of each step is displayed:



  The progress of each step is given by a percentage.
  The state (4) of the installation is given: state ", uploading", "in progress" or "done"
  More information is given by clicking in the `Details` link (5).

- See the *`Health checks` screen* to check the engine update is successful.

8.5.3 Installing a hotfix

8.5.3.1 Introduction

A hotfix enables a given correction or modification to be applied without having to upgrade the entire solution.
This procedure describes how to apply a hotfix.

8.5.3.2 Links associated

See the *Hotfix presentation*.
The engine hotfix packages are available here (https://update.gatewatcher.com/hotfix/).
The graphical interface is described in the *`Software update` screen*.

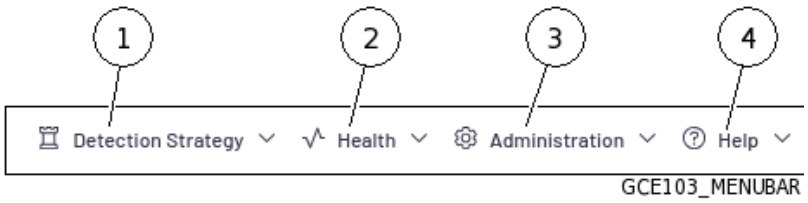
8.5.3.3 Prerequisites

- User: member of **Administrator** group

8.5.3.4 Preliminary operations

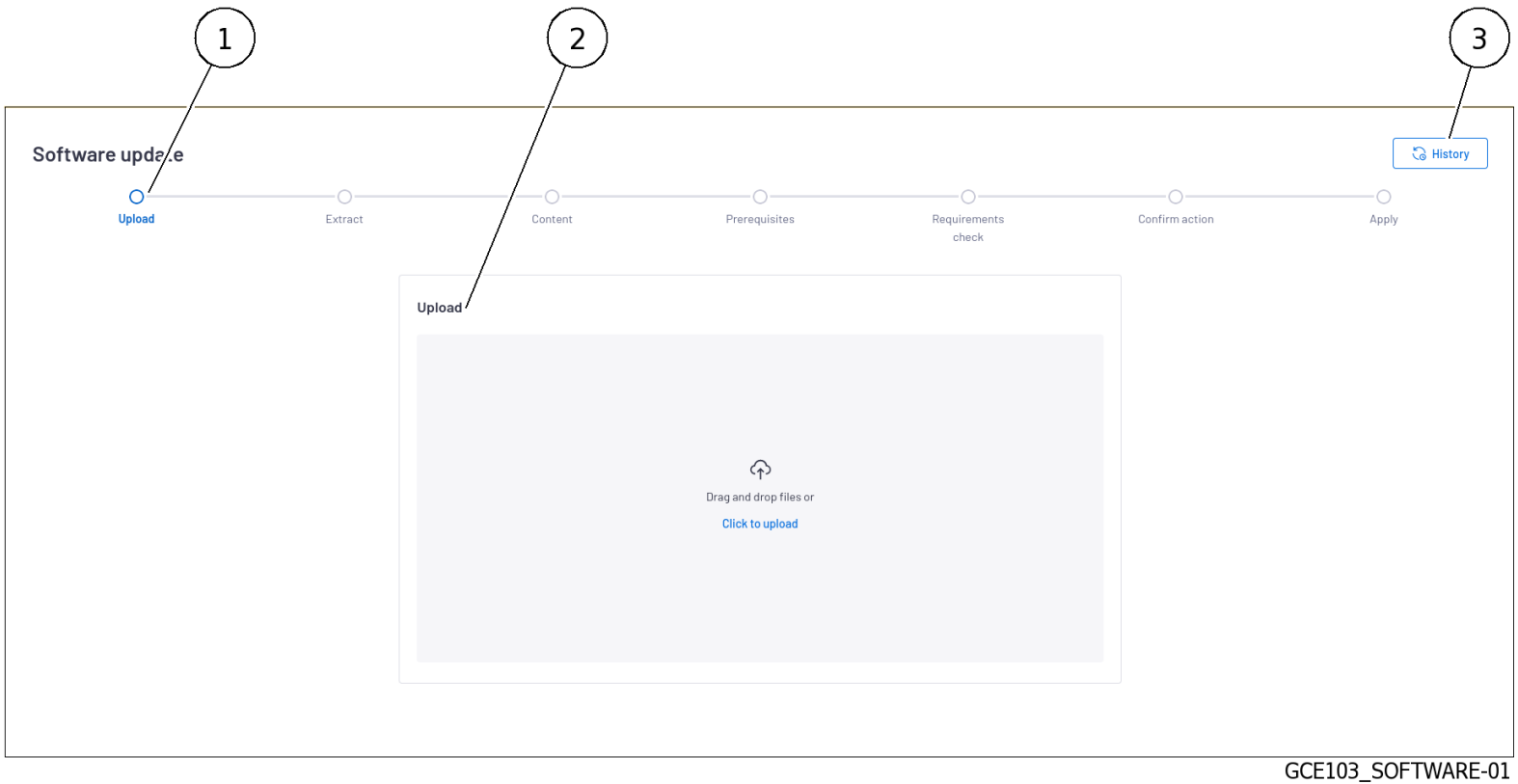
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*) with the prerequisite rights.
- Read the release note of the desired version to see whether any other prerequisites are required.
- Download the hotfix package from the site indicated in the introduction.

8.5.3.5 Procedure



GCE103_MENUBAR

- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Software update` command from the `Updates` submenu, the following screen is displayed.



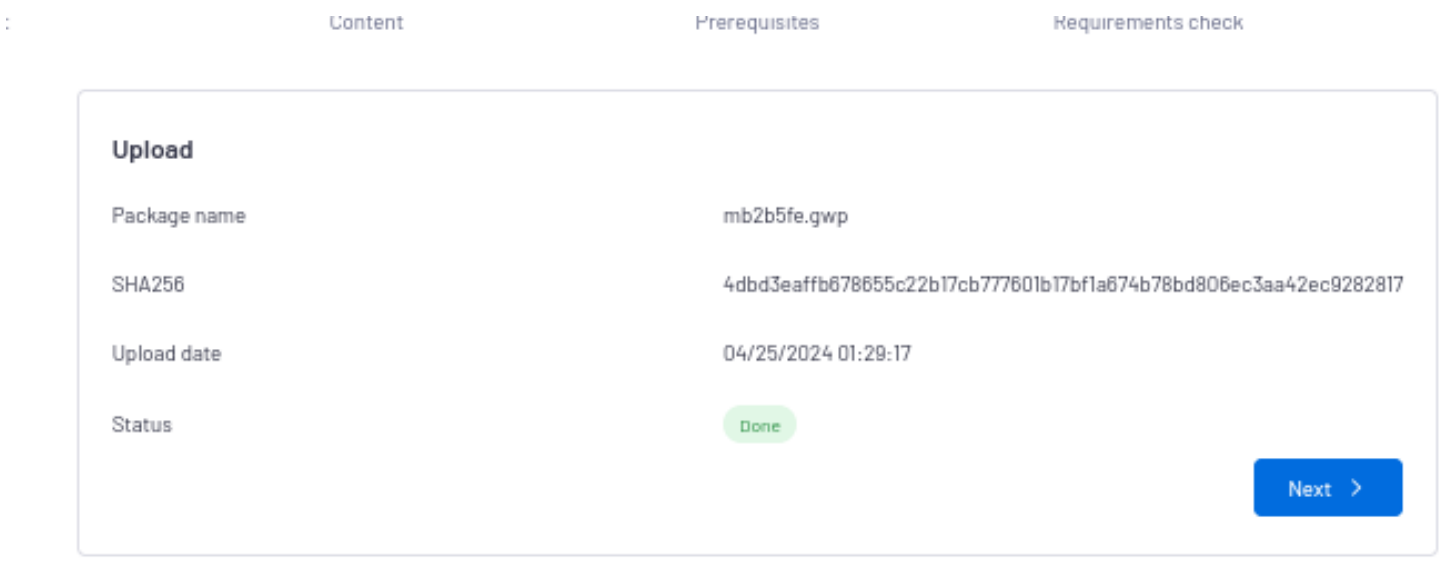
GCE103_SOFTWARE-01

- Click on the `Upload` area (2).
  A window is displayed to select the package to download.
- Select the previously downloaded package.
- Validate.

Note:

If the selected file is not an update file, the error message is displayed : `Wrong file type, .gwp only`.

The first step `Upload` begins...
The file is uploaded and the status is displayed.



- Click on the `Next` button.
  The second step `Èxtract` begins..

Note:

If the selected file is not an hotfix file, but a engine update file, the following error message is displayed : `The file is a gcenter threat db update, but a software update is expected.`.

The `Èxtract` window is displayed with messages.

```
Extract

 Starting
 Unwrapping the gwp file
 Moving the gwp content to the target folder
 Extraction done. Waiting for launching the requirement check
```

- Click on the `Next` button.
  The step `Content` begins..
  The `Content` window is displayed with messages.

```
Content

 Change the ....
```

- Click on the `Next` button.
  The step `Prerequisites` begins...
  The Prerequisites window is displayed with messages.

```
Prerequisites

 The patcher requirement check
```

- Click on the `Next` button.
  The step `Requirements check` begins...
  The Requirements check window is displayed with messages.

```
Requirements check
```

(continues on next page)

(continued from previous page)

```
Starting
Starting the requirements check
Un tar the requirements check file.
Execute the requirement script.
The requirements check were made with success. Your are free to continue.
```

- Click on the `Next` button.
  The step `Confirm action` begins...
  The `Confirm action` window is displayed with messages.

```
Please confirm this sensitive action

Do you want to change ...
```

- Click on the `Next` button.
  The step `Apply` begins...
  The `Apply` window is displayed with messages.

```
Apply

Starting
Starting the patching process.
Starting the patcher operation
Un tar the patcher file.
Patch done.
```

- Click on the `Next` button.
  The hotfix was applied and the corrections are made on the GCenter.

Note:

In some cases, applying a hotfix may cause the web server to restart.
This will make the web interface unavailable for a few minutes as specified in the release note.

8.5.4 Installing of an upgrade

8.5.4.1 Introduction

An upgrade enables a major version enhancement to be performed.
This involves a reboot of the device concerned.
This procedure describes how to apply an upgrade.

For	go to
Applying a GCenter upgrade	*Procedure to apply a GCenter upgrade*
Applying a GCap upgrade	*Procedure to apply a GCap upgrade*

8.5.4.2 Links associated

See the *Upgrade presentation*.
All upgrade packages are available https://update.gatewatcher.com/upgrade.
The graphical interface is described in the *`Software update` screen*.

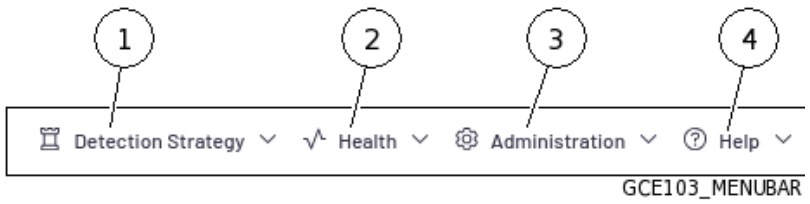
8.5.4.3 Prerequisites

- User: member of **Administrator** group

8.5.4.4 Preliminary operations

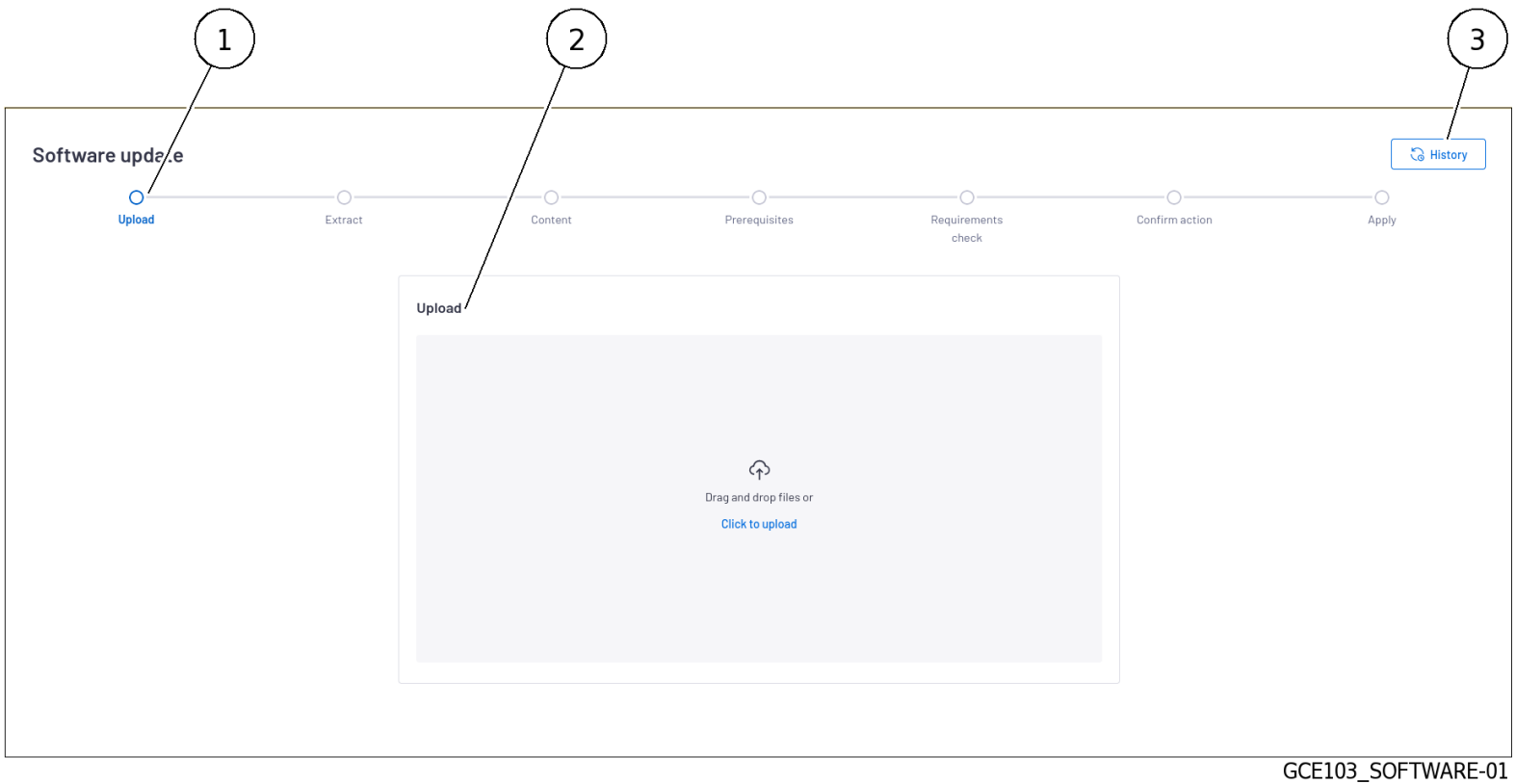
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)
- Log in to the GCap CLI.
- Read the release note of the desired version to see whether any other prerequisites are required.
- Download the upgrade package for the desired version from the site (https://update.gatewatcher.com/upgrade).

8.5.4.5 Procedure to apply a GCenter upgrade



GCE103_MENUBAR

- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Software update` command from the `Updates` submenu.
  The following screen is displayed.



GCE103_SOFTWARE-01

- Click on the `Upload` area (2).
  A window is displayed to select the package to download.
- Select the previously downloaded package.
- Validate.

> **Note:**
>
> If the selected file is not an update file, the error message is displayed : `Wrong file type, .gwp only`.

The first step `Upload` begins...
The file is uploaded and the status is displayed.
The `Upload` window is displayed with messages.

```
Upload

 Package name    xxxxxx
 SHA256          xxxxxx
 Upload date     xxxxxx
 Status          Done
```

- Click on the `Next` button.
  The second step `Extract` begins..
  The `Extract` window is displayed with messages.
- Click on the `Next` button.
  The step `Content` begins..
  The `Content` window is displayed with messages.
- Click on the `Next` button.
  The step `Prerequisites` begins...
  The `Prerequisites` window is displayed with messages.
- Click on the `Next` button.
  The step `Requirements check` begins...
  The Requirements check window is displayed with messages.
- Click on the `Next` button.
  The step `Confirm action` begins...
  The Confirm action window is displayed with messages.
- Click on the `Next` button.
  The step `Apply` begins...
  The Apply window is displayed with messages.
- Click on the `Next` button.
- Restart the GCenter (see the procedure *`Restart` command*)
  After restarting, the GCenter loaded the desired version.

8.5.4.6 Procedure to apply a GCap upgrade

- On the GCenter:
  - Select the previously downloaded package.
  - Validate.

> **Note:**
> If the selected file is not an update file, the error message is displayed : `Wrong file type, .gwp only`.

  The first step `Upload` begins...
  The file is uploaded and the status is displayed.
  The Upload window is displayed with messages.

```
Upload

 Package name    xxxxxx
 SHA256          xxxxxx
 Upload date     xxxxxx
 Status          Done
```

  - Click on the `Next` button.
    The second step `Extract` begins..
    The Extract window is displayed with messages.
  - Click on the `Next` button.
    The step `Content` begins..
    The Content window is displayed with messages.
  - Click on the `Next` button.
    The step `Prerequisites` begins...
    The Prerequisites window is displayed with messages.
  - Click on the `Next` button.
    The step `Requirements check` begins...
    The Requirements check window is displayed with messages.
  - Click on the `Next` button.
    The step `Confirm action` begins...
    The Confirm action window is displayed with messages.
  - Click on the `Next` button.
    The step `Apply` begins...
    The Apply window is displayed with messages.
- Log on to the GCap CLI:
- Run the `system upgrade list` command to retrieve the package name

- Run the command `system upgrade apply packagename` to start the upgrade.
  After restarting, the GCap loaded the desired version.

8.6 Administrating the GCenter

8.6.1 Configuring the export data to a SIEM via the syslog protocol

8.6.1.1 Introduction

This procedure describes how to configure the 2 connections to the SIEM via the syslog protocol.
The two available connections are named :

- Data export #1
- Data export #2

8.6.1.2 Links associated

See the *Connection to Syslog servers* presentation.
See the presentation of the exported data described in the *Data use* paragraph.
The graphical interface of the data export function is described in *`Data export` screen*.

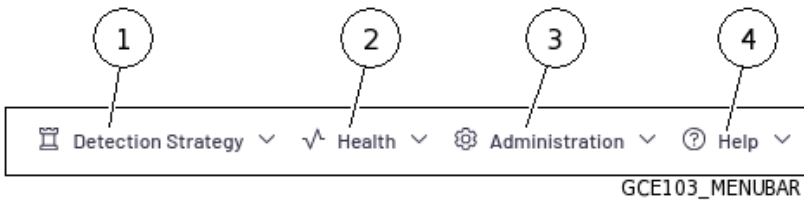
8.6.1.3 Prerequisites

- User: member of **Administrator** group

8.6.1.4 Preliminary operations

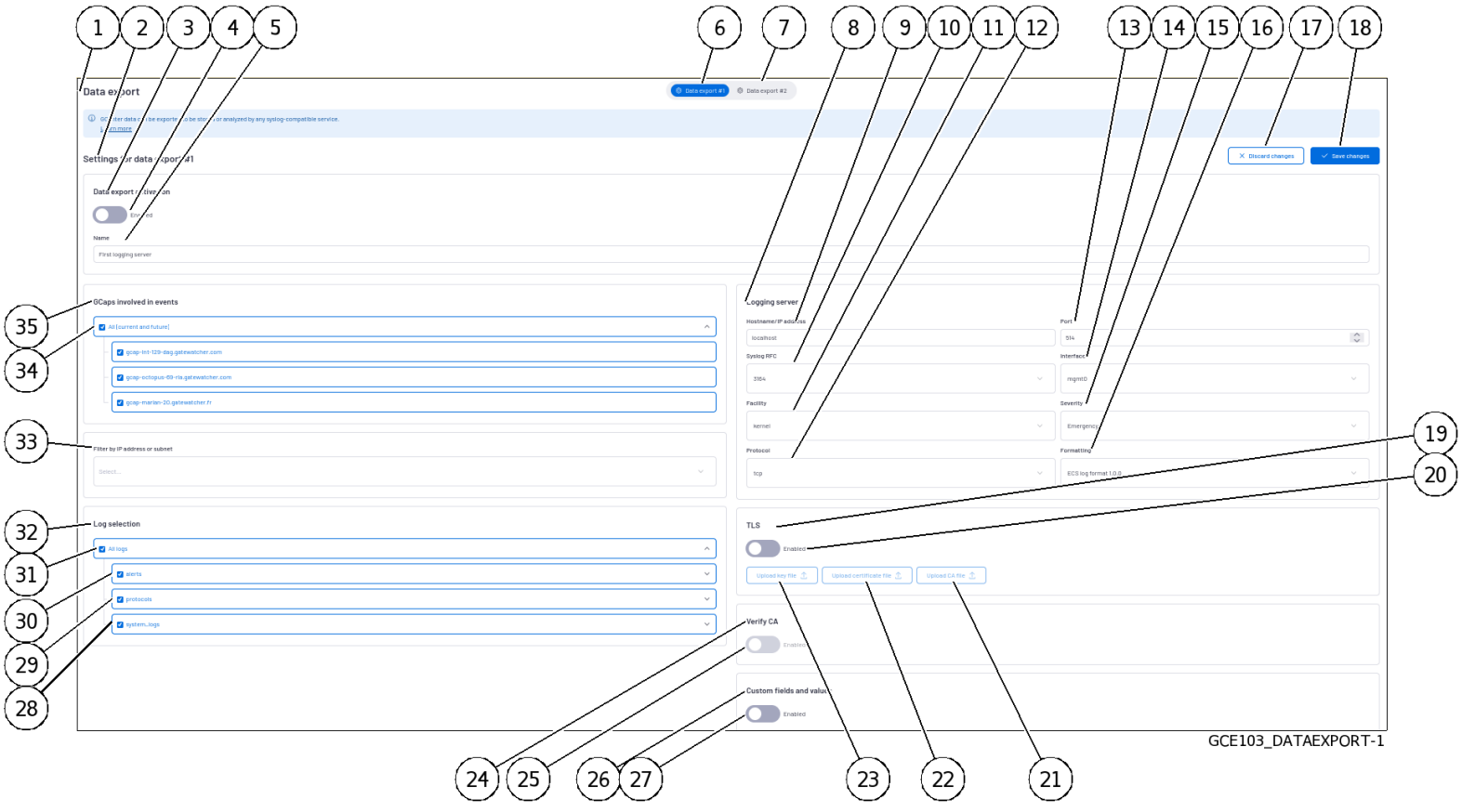
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.6.1.5 Procedure to access the `Data export` window



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Log export` command from the `Data` submenu.
  The `Data export` window is displayed.

8.6.1.6 Procédure to set the `Data export #1` settings



- Click the `Data export #1` button (6).
  The `Settings for data export #1` area (2) is displayed.
- Enter the necessary parameters.
  The list of items is detailed in *`Data export` screen*.
- Validate using the `Save changes` button (9).
- If necessary, set up the other connection (7).

8.6.1.7 Procedure to activate the export

- Use the `Enabled` selector (4) to activate the export.
- Validate using the `Save changes` button (18).

8.6.2 Configuring the export data to ETL Logstash via the syslog protocol

8.6.2.1 Introduction

This procedure describes how to configure the connection to Logstash.
A pipeline developed by Gatewatcher makes it possible to retrieve the JSON content of the exported logs so that it can then be manipulated as desired with the Logstash filters.
Configuring the connection between the GCenter and the Logstash ETL requires the following steps:

- On the GCenter, configure data export, see *Procedure to set the data export #1 settings*
- On the Logstash server, configure the flow receiving pipeline from the GCenter (see *Procedure to be performed on the server*)

Note:

See the presentation of *Connection to Syslog servers*.
See the presentation of the exported data described in *Data use*.
The graphical interface of the data export function is described in *`Data export` screen*.

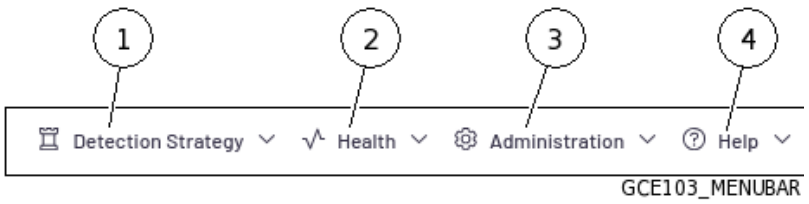
8.6.2.2 Prerequisites

- User: member of **Administrator** group

8.6.2.3 Preliminary operations

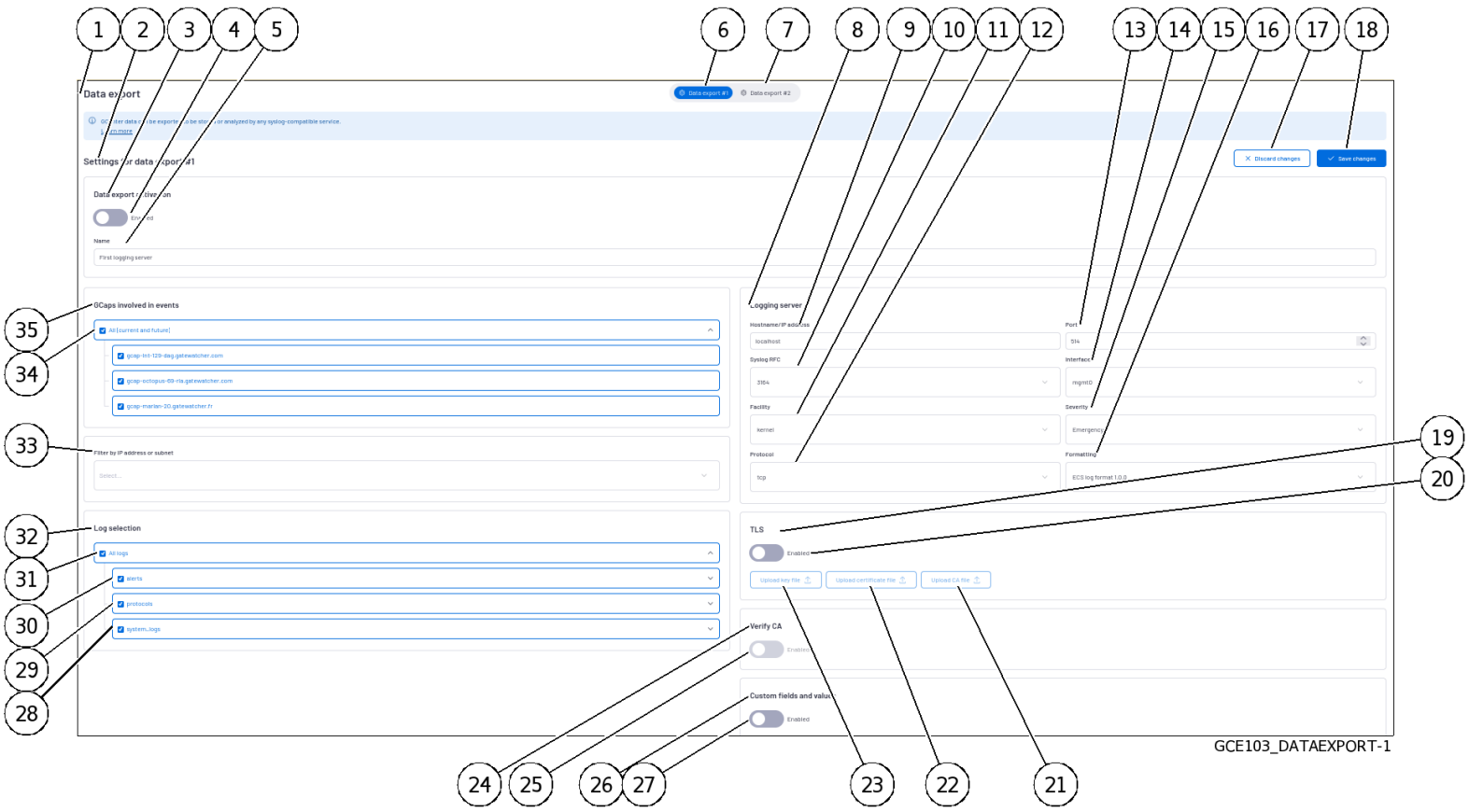
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.6.2.4 Procedure to access the `Data export` window



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Log export` command from the `Data` submenu.
  The `Data export` window is displayed.

8.6.2.5 Procedure to set the data export #1 settings



- Click the `Data export #1` button (6).
  The `Settings for data export #1` area (2) is displayed.
- Enter the necessary parameters.
  The list of items is detailed in *`Data export` screen*.

Item	Name	Value to enter
4	• `Enabled` selector	• Activated
5	• `Name`	• $SYSLOG_NAME
9	• `Hostname/IP address`	• $LOGSTASH_IP

continues on next page

Table 1 – continued from previous page

Item	Name	Value to enter
10	• `Syslog RFC`	• 3164
11	• `Facility`	Syslog header `facility` default kernel; header will be removed by the reception pipeline
12	• `Protocol`	• $PROTOCOL
13	• `Port`	• $LOGSTASH_PORT
14	• `Interface`	Choose the GCenter interface used for Syslog export $GCENTER_IFACE
15	• `Severity`	Value of `severity` in the Syslog header emergency by default; the header will be deleted by the reception pipeline
16	• `Formatting`	• Choice between the log formatting: - ECS log format 1.0.0. for the Elastic Common Schema (ECS) format - Legacy retro-compatibility 2.5.3.102 for standard syslog export
26	`Custom fields and values`	Zone to Custom fields and values This zone contents:
27	• `Enabled` selector	• Activates the feature. Disabled by default.
32	`Log selection`	Zone to select the log to be exported. This zone contents:
31	• `All logs`	• Check box to select all logs The list of the log types is displayed. The log types are `alerts` (30), `protocols` (29), `system_logs` (28) The alerts types are detailed in the note below. The protocols types are detailed in the note below: these protocols are the Sigflow protocols. The system_logs has only one choice: notification.
33	`Filter by IP address or subnet`	Allows to select the events source with its IP address or subnet. By default, all data is sent to the remote server if the field is empty.
35	`Gcap involved in events`	Zone to select data to sent: all data from the GCap paired and selected to the GCenter is sent to the remote server This zone contents:
34	• `All (current and futures)`	• Check box to select all known GCaps The list of the GCaps is displayed. Each GCap can be selected independently.
17	`Ip addresses`	Filter by **IP** or **networks**. By default, all data is sent to the remote server if the field is empty

Note:

`Select All` selects all the protocols listed: a protocol that is not selected will not be exported.
If the GCap is newer than the GCenter, some protocols may be missing.
To export everything, disable this filter with `Deselect all`.

Note:

The `TLS` zone and `Verify CA` enables the encryption of the flow generated by the GCenter.
Logstash's "syslog" input is not compatible with data encryption.
This feature cannot be used.

- Validate using the `Save changes` button (18).
  The following message indicates that the update has been completed: `Updated with success`.

8.6.2.6 Procedure to be performed on the server

- Configure the flow receiving pipeline from the GCenter.

8.6.2.6.1 Pipeline Logstash

The input used is Syslog.
In order to be compatible with any Syslog header, a grok pattern is specified.
The JSON content of the log is in the syslog_message field.

```
yaml
input {
  syslog {
    port => $LOGSTASH_PORT
    type => syslog
    grok_pattern => '^<%{NUMBER:syslog_priority}>(?:1 |)(?:%{SYSLOGTIMESTAMP:syslog_timestamp}|%{TIMESTAMP_
↪ISO8601:syslog_timestamp}) %{SYSLOGHOST:syslog_hostname} (?:gatewatcher\[-\]:|gatewatcher - - \[-\]) %
↪{GREEDYDATA:syslog_message}\n$'
  }
}
```

Only the syslog_message field is preserved and is converted to JSON.
The original field (syslog_message) and the field specific to elasticsearch (@version) are then removed.

```
yaml
filter {
  prune {
    whitelist_names => [ "syslog_message" ]
  }

  json {
    source => "syslog_message"
  }

  mutate {
    remove_field => [ "@version","syslog_message" ]
  }
}
```

Any output can then be used.
In this example, the logs are described directly on the disk as files:

```
yaml
output {
  file {
    path => '/usr/share/logstash/data/output/%{[type]}-%{+YYYY.MM.dd}.log'
    codec => json_lines
  }
}
```

8.6.3 Creating a POC Logstash

8.6.3.1 Introduction

This procedure describes how to quickly create a Logstash Proof Of Concept.

8.6.3.2 Prerequisites

- User: member of **Administrator** group

8.6.3.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.6.3.4 Procedure

A POC with a Logstash docker can be done in minutes.
The following commands, given as an indication, should facilitate this task.

Important:

The controls are given as an indication to mount a demonstrator quickly. It does not follow the best practices necessary for the development of a production component.

- On a Linux machine with docker, run the following commands to retrieve the default Logstash configuration files: (procedure tested with Logstash version 8.17.3).

```
mkdir logstash_docker
cd logstash_docker
sudo docker run --name="logstash_tmp" --rm -d -it docker.elastic.co/logstash/logstash:8.17.3
sudo docker cp logstash_tmp:/usr/share/logstash/config config
sudo docker cp logstash_tmp:/usr/share/logstash/pipeline pipeline
sudo docker rm -f logstash_tmp
```

A *logstash_ docker* folder has been created with two subfolders: *config* and *pipeline*.
In *config*, parameters can be kept by default, except for the *xpack.monitoring.elasticsearch.hosts* parameter which must be commented in *logstash.yaml*.

- In the *pipeline* folder, replace the default pipeline with the pipeline described in the *Pipeline Logstash* section (in the `logstash.conf` file).
  A docker using these configuration files and this pipeline can then be started:

```
sudo docker run --name="logstash_export" --rm -it -p $LOGSTASH_PORT:$LOGSTASH_PORT/$PROTOCOL -v $(pwd)/config/:/
↪usr/share/logstash/config/ -v $(pwd)/pipeline:/usr/share/logstash/pipeline/ -v $(pwd)/output:/usr/share/
↪logstash/data/output/ --user $(id -u):$(id -g) docker.elastic.co/logstash/logstash:8.17.3
```

If an error message is displayed, the file rights are probably wrong. Change "--user $(id -u):$(id -g)" by "--user $root:root"
After modification, to run this command in background, use the following command:

```
sudo docker run --name="logstash_export" --rm -d -it -p $LOGSTASH_PORT:$LOGSTASH_PORT/$PROTOCOL -v $(pwd)/
↪config/:/usr/share/logstash/config/ -v $(pwd)/pipeline:/usr/share/logstash/pipeline/ -v $(pwd)/output:/usr/
↪share/logstash/data/output/ --user $(id -u):$(id -g) docker.elastic.co/logstash/logstash:8.17.3
```

Logstash will then create an *output* directory in which the received logs will be written, with one JSON per line.

8.6.4 Configuring the connection to the MISP

8.6.4.1 Introduction

This procedure describes the connection configuration with a MISP server present in the infrastructure.

The MISP connector allows you to bring IOC directly from a MISP to the GCenter in the form of rules.
From the GCenter, these rules can be included in a ruleset and therefore sent to the GCap.
This connector allows to add a source of threat intelligence of quality while respecting the instructions of the ANSSI on the qualification of signatures.
The MISP configuration is added to the Sigflow menu in a new menu `MISP`.

8.6.4.2 Links associated

For more information, see the *Interconnection with external systems*.
The graphical interface is described in *`MISP settings` screen*.

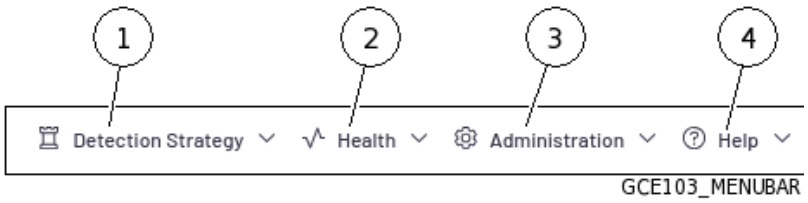
8.6.4.3 Prerequisites

- User: member of **Administrator** group

8.6.4.4 Preliminary operations

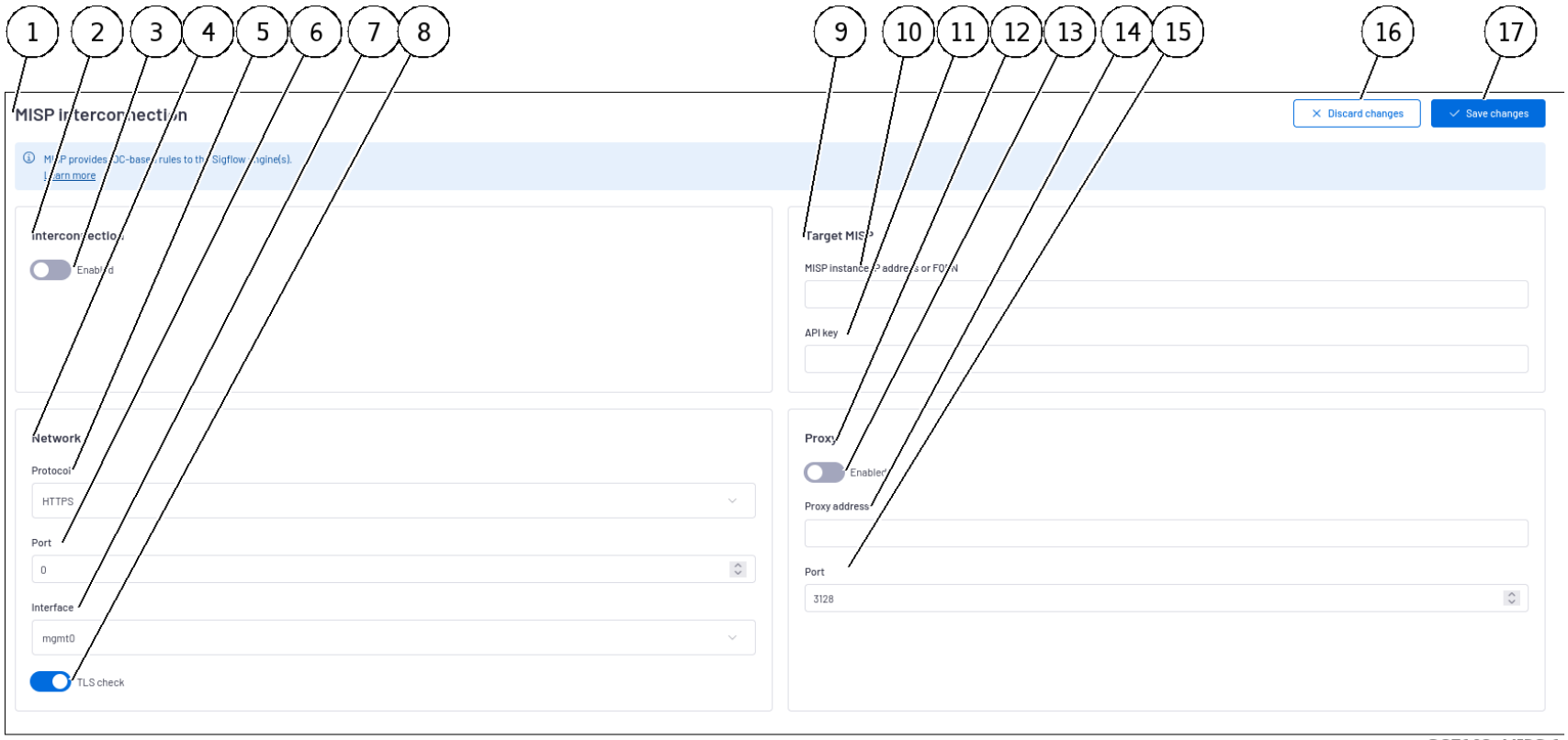
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.6.4.5 Procedure to access the `MISP settings`



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `MISP` command from the `Third party` submenu.
  The `MISP` window is displayed.

8.6.4.6 Procedure to configure the connection



GCE103_MIPS-1

- Use the `Enabled` selector (3) to activate the interconnection (2).
- If necessary, use the `TLS check` selector (8).
- Enter the parameters of the `Network` area (4):
  - Select the communication protocol (5) to use to contact the MISP instance: two options are possible ('https' and 'http')
  - Enter the listening port (6)
  - Select the GCenter network interface (7) to connect to
- Enter the Target MISP parameters (9):
  - Enter the FQDN or IP address (10) of the MISP instance
  - Enter the API key (11) of the MISP instance
- If needed, enter the Proxy parameters (12):
  - use the `Enabled` selector (13)
  - Enter the Proxy address (14).
  - Enter the listening port (15).
- Click on the `Save changes` button (17).

  The sub-menu `MISP` of the menu `Sigflow` is now available to members of the `operator` group.

  It is therefore possible to choose a manual or automatic update.

8.6.5 Deleting data (log files)

8.6.5.1 Introduction

This procedure enables clearing the information tables of the analysis engines, syslog exchanges, and NDR information over a given period of time. This deletion period is selected by the administrator, however, it cannot exceed the total retention time of the data already pre-configured in the solution.

Important:

Data not yet processed will also be deleted.

Note:

After a full or incremental save by the backup functionality, the old logs are automatically deleted, depending on the data retention time, thus freeing up disk space.

8.6.5.2 Links associated

See the log files and their management presentation in the paragraph *Data use*.
The graphical interface is described in *`Diagnostics` screen*.

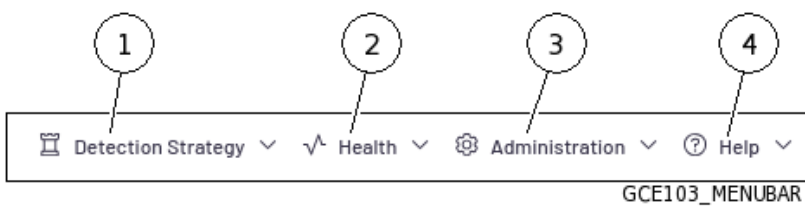
8.6.5.3 Prerequisites

- User: member of **Administrator** group

8.6.5.4 Preliminary operations

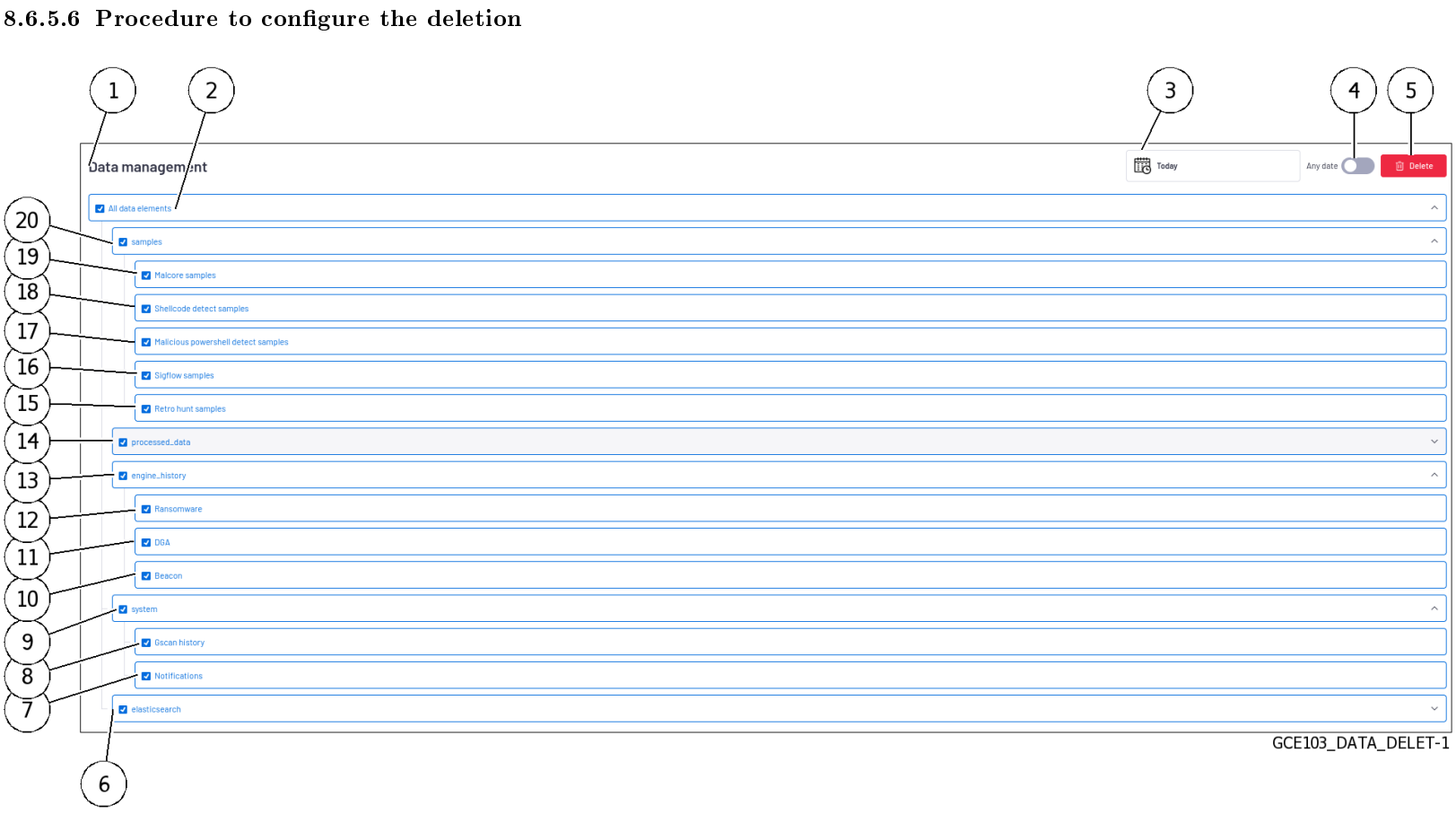
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.6.5.5 Procedure to access to the `Data deletion` window



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Data Management` command from the `Data` submenu.
  The `Data Management` window is displayed.

8.6.5.6 Procedure to configure the deletion



- Choosing the time interval (3) in which the deletion is to be carried out or select the `Any date` cursor.
  A window opens.
  - Use the calendar to enter the start date.
  - Use the calendar to enter the end date.
  - Validate using the `Apply` button.
- Select the information to be deleted:
  - Select `Any data elements` (2) to delete all
  - Or select one of the categories (6 to 19)
- Validate using the `Delete` button (3).

8.6.6 Generating and loading files for diagnosis

8.6.6.1 Introduction

This procedure enables generating and loading:

- Log files, information tables, analysis engines, syslog exchanges, and NDR information for a given period.
- The Tech support file

Important:

Indeed, this archive can only be extracted by an advanced administrator having knowledge of the data extraction password.

8.6.6.2 Links associated

See the presentation of the data for the diagnosis in the *Data use* paragraph.
The graphical interface is described in the *`Diagnostics` screen*.

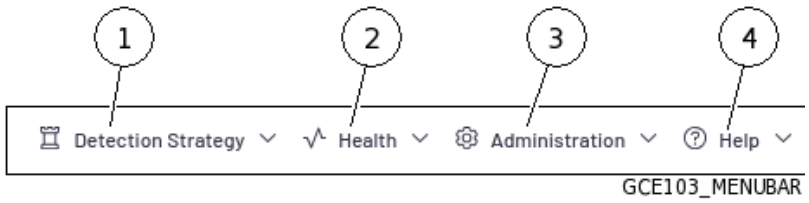
8.6.6.3 Prerequisites

- User: member of **Administrator** group

8.6.6.4 Preliminary operations

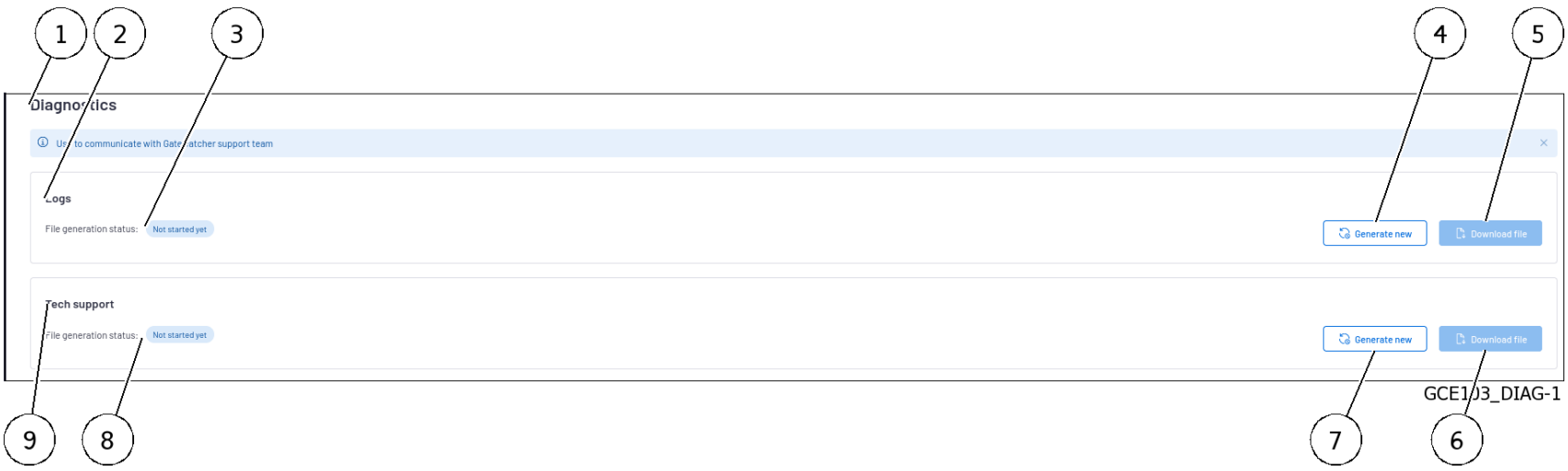
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.6.6.5 Procedure to access the `Diagnostics` window



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Diagnostics` command from the `Maintenance` submenu.
  The `Diagnostics` window is displayed.

8.6.6.6 Procedure to generate and load the logs



- Press the `Generate new` button (4) in the `Logs` area (2)

A message is displayed to indicate the result of the generation: example `Success : Logs generation started`
A status is displayed as following :

```
File generation status:     File generated
Filename: gcenter.domain.local-2025_03_20-10_04_59_UTC-logs.gwl
Generated at: 20/03/2025 11:05
```

- Click on the `Download file` button (4).

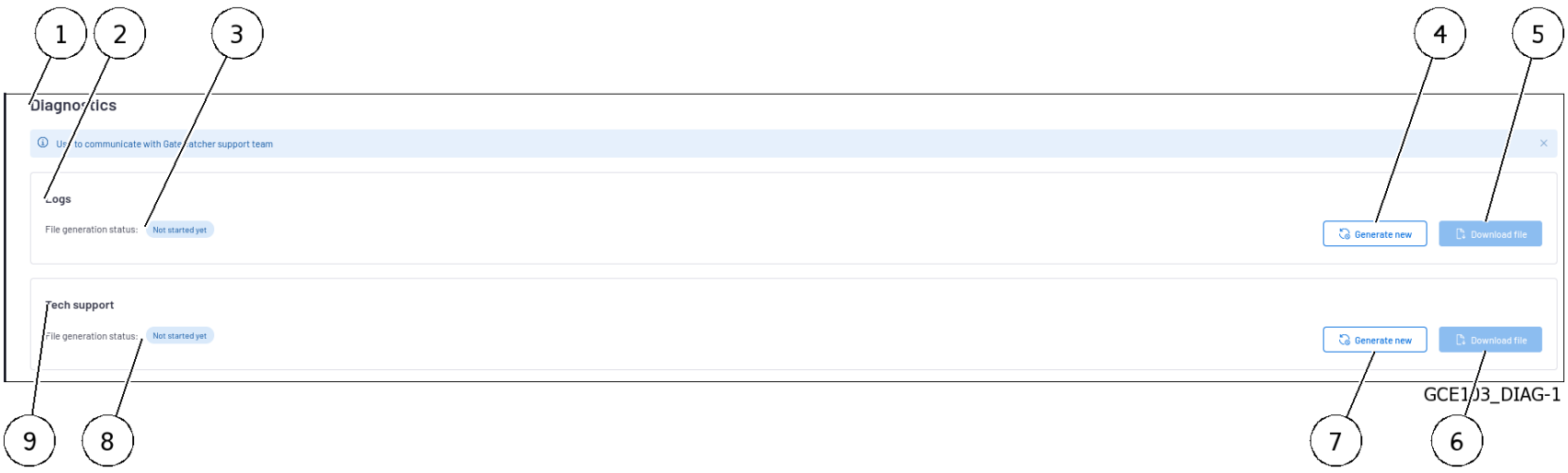
  A message is displayed as following:

```
Success
Downloading logs file: gcenter.domain.local-2025_03_20-10_04_59_UTC-logs.gwl
```

  The file is therefore present in the computer's local directory.
  The file uploaded for a log file is named **hostname-time-logs.gwl**. This file is encrypted. It is only visible to the GATEWATCHER support team.

- Send these files to the GATEWATCHER support team for analysis.

8.6.6.7 Procedure to generate and load the Tech support files



- Press the `Generate new` button (7) in the `Tech support` area (9).
  A message is displayed to indicate the result of the generation: example `Success : Tech support generation started`
  A status is displayed as following :

```
File generation status:
File generated
Filename: tech-support.txtGenerated at: 20/03/2025 11:09
```

- Press the `Download` button (7).
  A message is displayed as following:

```
Success
Downloading tech support file: tech-support.txt
```

  The file is therefore present in the computer's local directory.
  The file downloaded for a Tech support is named **tech-support.txt**. This file is a text file and can be opened.

- Send these files to the GATEWATCHER support team for analysis.

8.6.7 Using an endpoint API

8.6.7.1 Introduction

This procedure shows how:

- Run an endpoint locally
- Retrieve the answer
- Have the corresponding .json
- Know the model of the response and have an example of it

By clicking on the `Try it out` button, it is possible to test the selected query and the tool generates the query to use with curl.
The *Procedure to run an endpoint* specifies how to use the swagger GUI to select an API, execute the request, retrieve the response and curl of the request.
However, this request inherits the rights (and therefore the token) of the request creator.
To make a request with different rights, refer to *Procedure to modify the token associated with the request*.

8.6.7.2 Links associated

See the presentation in the *API* paragraph.
The graphical interface is described in the *Overview of the API interface*

8.6.7.3 Prerequisites

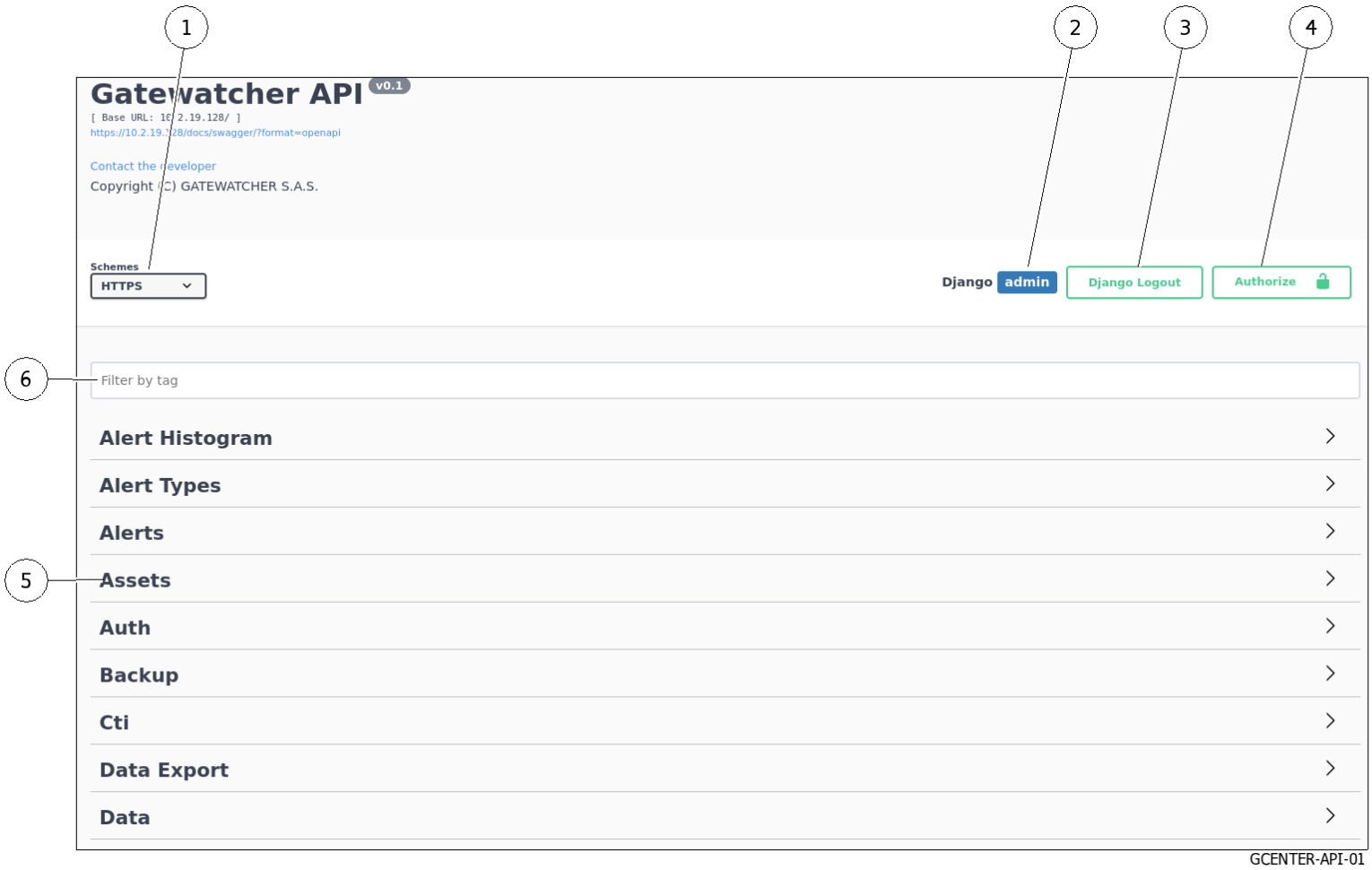
User: member of **Administrator** group

8.6.7.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.6.7.5 Procedure to access to API

After pressing the `API reference` command of the `Documentation` menu, the `Gatewatcher API` screen is displayed.



8.6.7.6 Procedure to run an endpoint

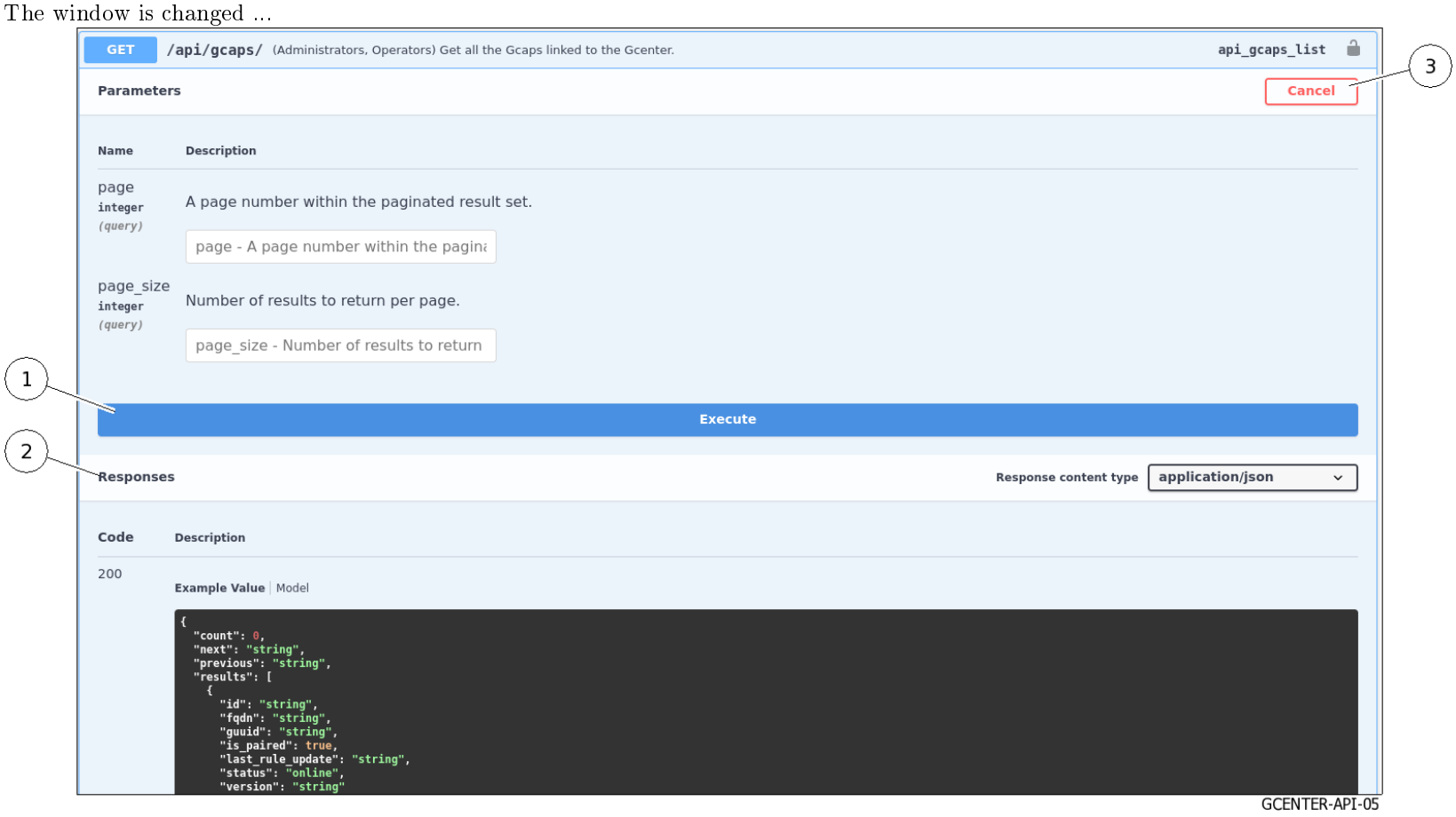
To illustrate this example, the API chosen is the one that lists the GCaps connected to the GCenter.

- Select the `Gcaps` theme from the list of existing themes (5).
- Click on the API `GET/api/gcap/ (Administrators, Operator) Get all the GCaps linked to the GCenter`.
  The window below is displayed.

Tip:

For some endpoints, it is mandatory to enter parameters before running it.

- Click on the button (2) `Try it out`.
  The window is changed ...



GCENTER-API-05

- Click on the button (1) `Execute`.
  The request is launched and the next window is displayed.

GCENTER-API-06

This window has several zones:

- The display zone (2) `Curl` for the Curl query
- Display zone (3) `URL` for URL request
- Zone (4) `Server response`:
  - The Return `Code` (5):

- If the code is set to `200` then the execution has been completed correctly.
- If the message `code 400 Undocumented Error Bad Request` is displayed, verify that the required parameters are entered.

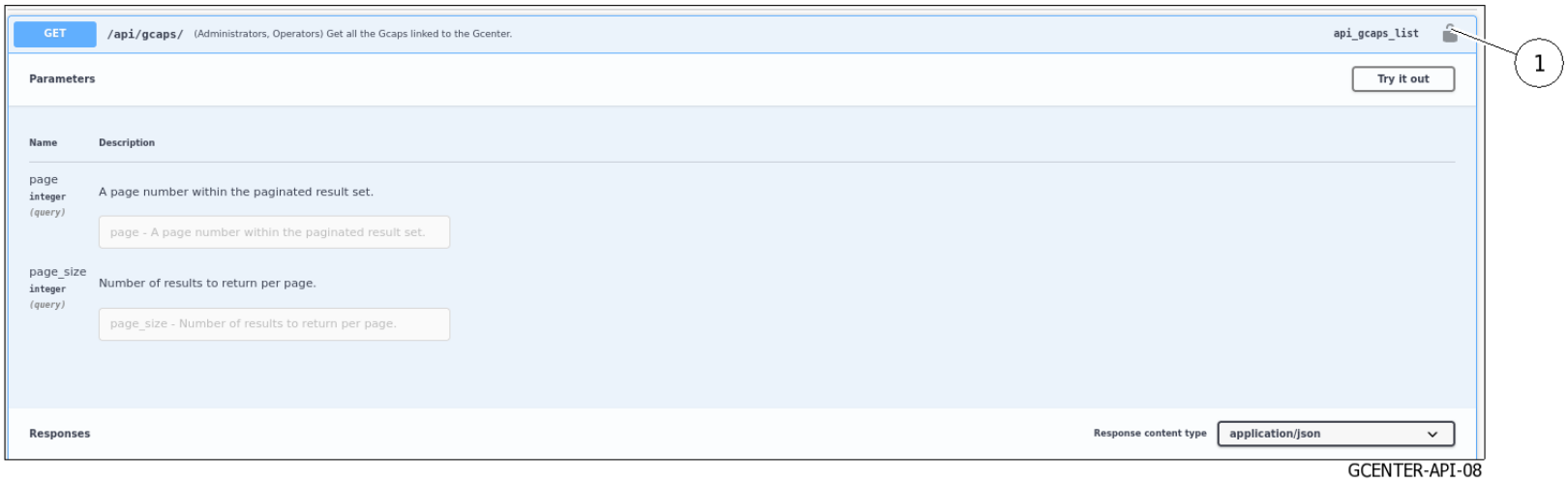
- The body of the answer (6): refer to *Overview of the API interface*
- The field detailing the answer header (7)
- The value in ms of the query duration (8)
- The `Download` button to download the corresponding .json file

- The `Responses` zone

  This zone displays different information depending on the use of the link `Model` or `Example Value`.
- Or the output model (`Model`): refer to *Overview of the API interface*
- An example of the answer in the expected field with values for example (`Example Value`): refer to *Overview of the API interface*

  The values are:
  - For integer type (value 0)
  - For type string (value = string)
  - For boolean type (value = true)

8.6.7.7 Procedure to modify the token associated with the request



GCENTER-API-08

- Click the button (1).

  The `Available authorizations` window is displayed:

  There are two options:
  - Or the use of an apikey (token previously created)
  - Or the use of an authorization by name and password of an account previously created
- To use an apikey (token previously created):
  - Paste the token in the `value` field
  - Validate by clicking on the `Authorize` field
  - Close window with the `Close` field

  Note:

  The token can have a limited life: see *Procedure to add a new API key*.

- To use an authorization:

- Click in the `Username field
  The list of existing accounts is displayed.
- Enter the account password
- Validate by clicking on the `Authorize` field
- Close window with the `Close` field

8.6.8 Managing the license

8.6.8.1 Introduction

This procedure describes viewing the current license information and changing it if necessary.
This is necessary if the following message is displayed: `No valid license found. New alerts and network events will not be received anymore. See license configuration here.`

Note:

Click on the `here` link which opens the `License` window.

To	Apply the procedures
Enter a new license	1 - Apply the *Procedure to access to the `License` screen* 2 - Apply the *Procedure to enter a new license*
Enter a new CTI license	1 - Apply the *Procedure to access to the `License` screen* 2 - Apply the *Procedure to enter a new CTI license*

8.6.8.2 Links associated

The graphical interface is described in the *`License` screen*.

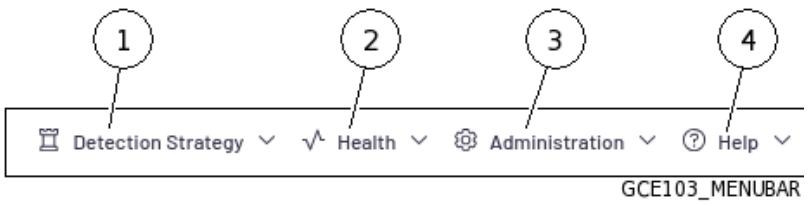
8.6.8.3 Prerequisites

- User: member of **Administrator** group

8.6.8.4 Preliminary operations

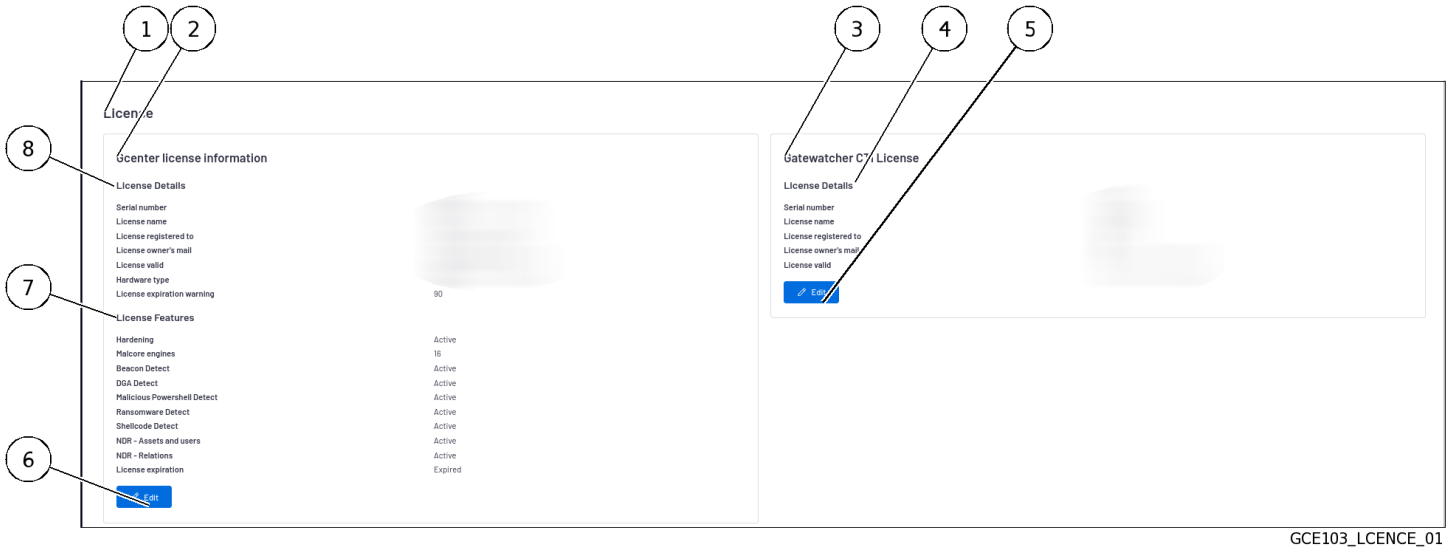
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.6.8.5 Procedure to access to the `License` screen



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `License` command from the `System` submenu.
  The `License` window is displayed.

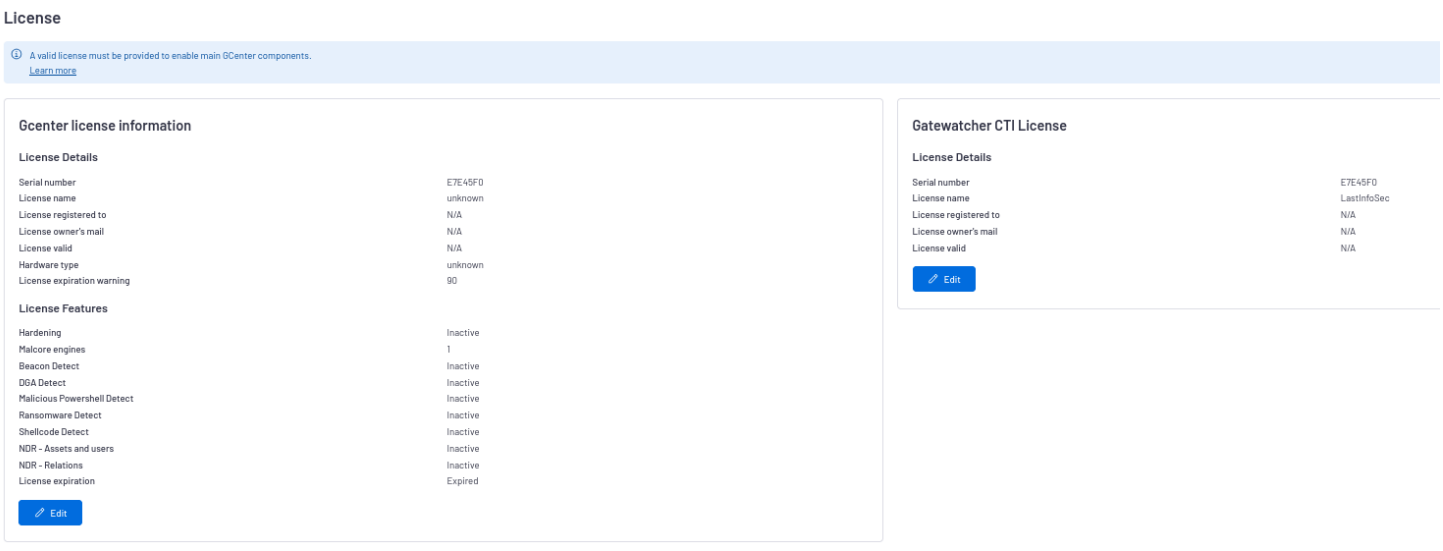
Case of a valid license



GCE103_LCENCE_01

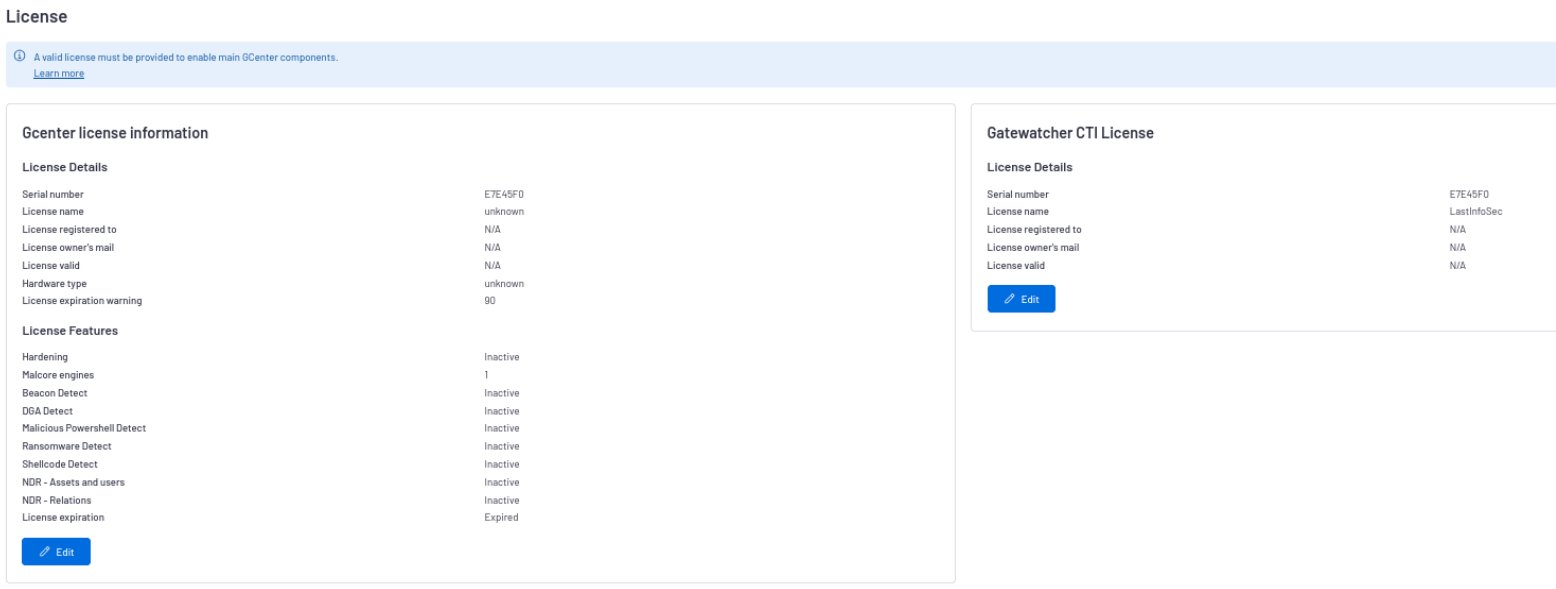
The engines are active.

Case of a missing license



The engines are inactive.

8.6.8.6 Procedure to enter a new license



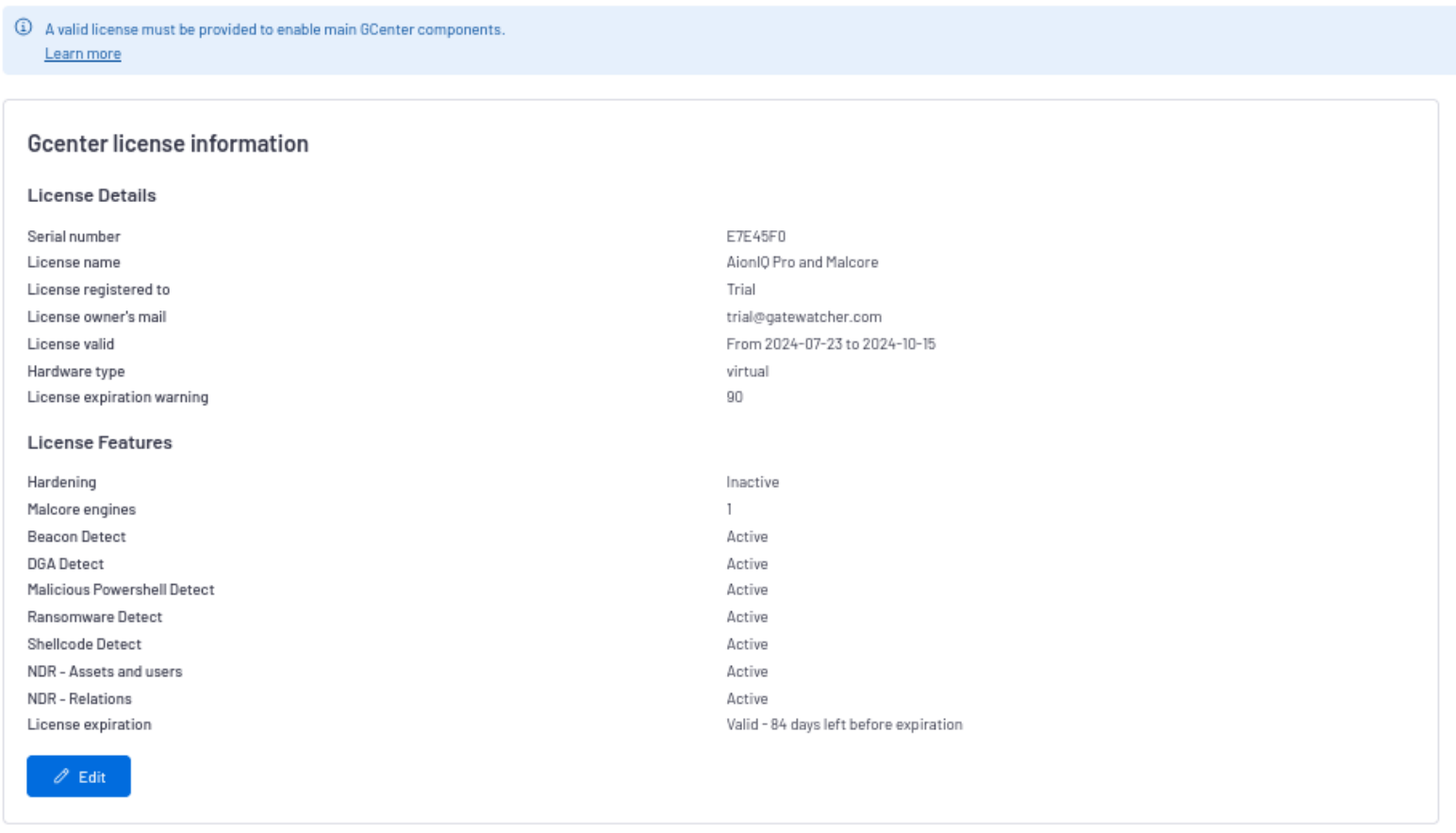
- Click on the `Edit` button (6).
  The `Edit a license` screen (1) is displayed.

- Enter the license key in the `License key` field (2).
- Enter the number of days of the license expiry alarm message in the `License expiry warning (in days)` field (3).
- Tick the choice `I accept the General Terms of Use` (7).

Note:

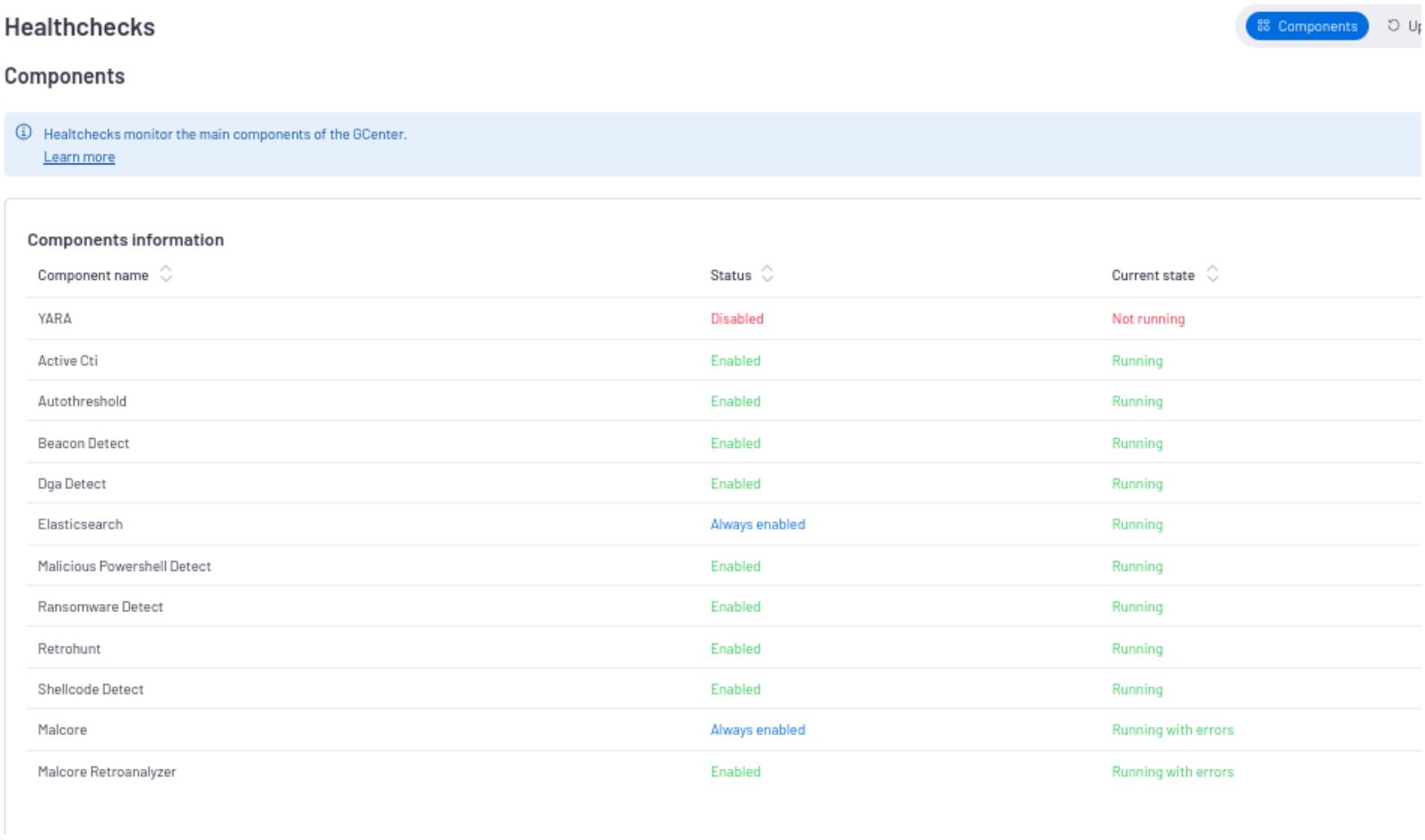
PLEASE, READ THE GENERAL TERMS AND CONDITIONS OF PRODUCTS AND SERVICES by using the link (4).

- Click on the `Submit` button (5) to save current settings and update the GCenter.
  Once the license, validated and activated the content of the page updates and displays the details of the content of the license.
  In case of missing or expired license, the interface will automatically redirect to this page in order to resolve the situation.

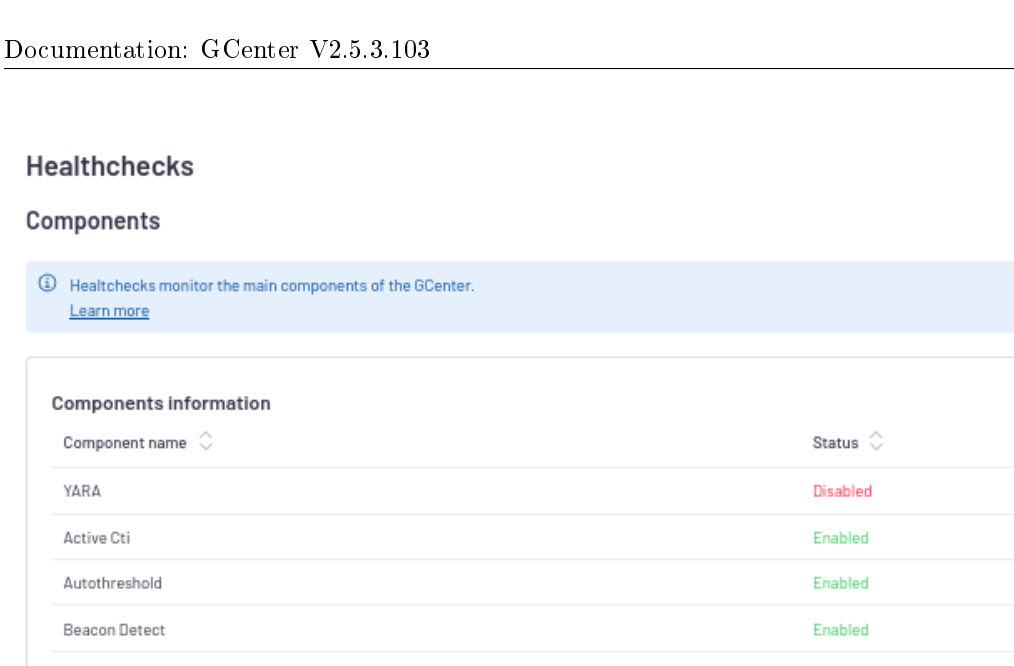


The engine state becomes `Active`, but it is necessary to update the engines.
To do so, refer to the procedure:

- Either *Installing an update manually*
- Either *Configuring automatic update of signatures and/or anti-viral engines* and use the `Force update now` button



8.6.8.7 Procedure to enter a new CTI license



- Enter the license key in field `License key` (2).
- Tick the choice `I accept the General Terms of Use` (6).

> **Note:**
> PLEASE, READ THE GENERAL TERMS AND CONDITIONS OF PRODUCTS AND SERVICES by using the link (3.

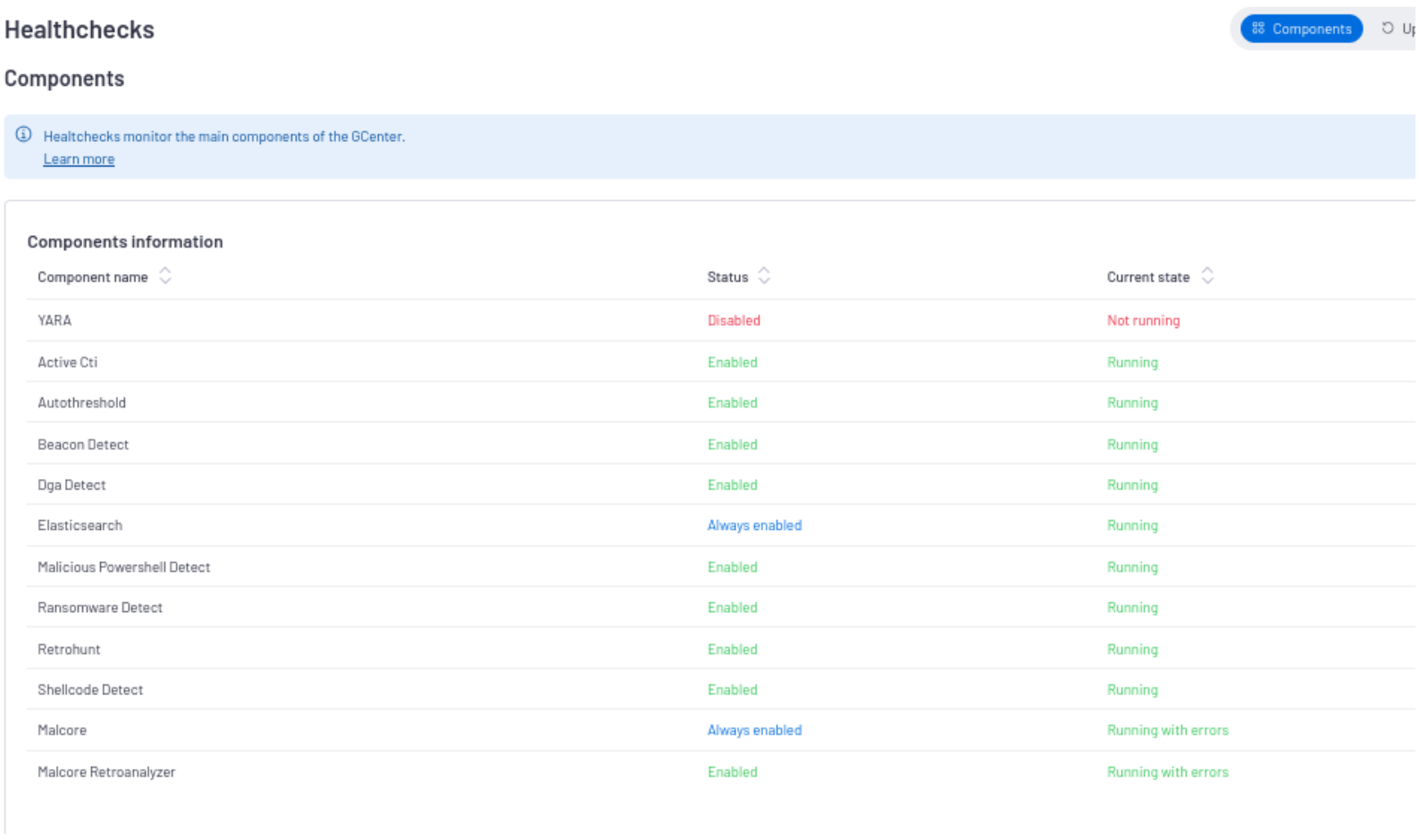
- Click on the `Submit` button (4) to save current settings and update the GCenter.
  The following message is displayed if it is ok.

```
Success

 License updated
```

Once the license, validated and activated the content of the page updates and displays the details of the content of the license.
The `Healthchecks` screen shows the activation of the Active CTI and Retro hunt motors.

The license is accepted but it is necessary to update the engines.
To do so, refer to the procedure:

- Either *Installing an update manually*
- Either *Configuring automatic update of signatures and/or anti-viral engines* and use the `Force update now` button



8.6.9 Configuring the GCenter

8.6.9.1 Introduction

This procedure describes the overall configuration of GCenter.

8.6.9.2 Links associated

The graphical interface is described in *`Global settings` screen*.

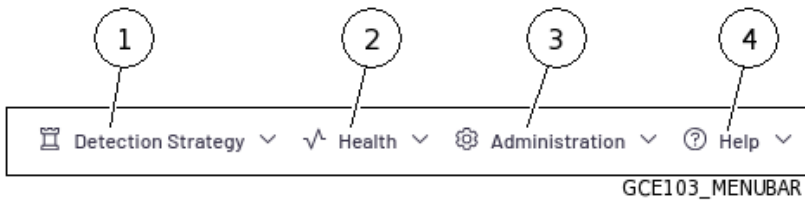
8.6.9.3 Prerequisites

- User: member of **Administrator** group

8.6.9.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

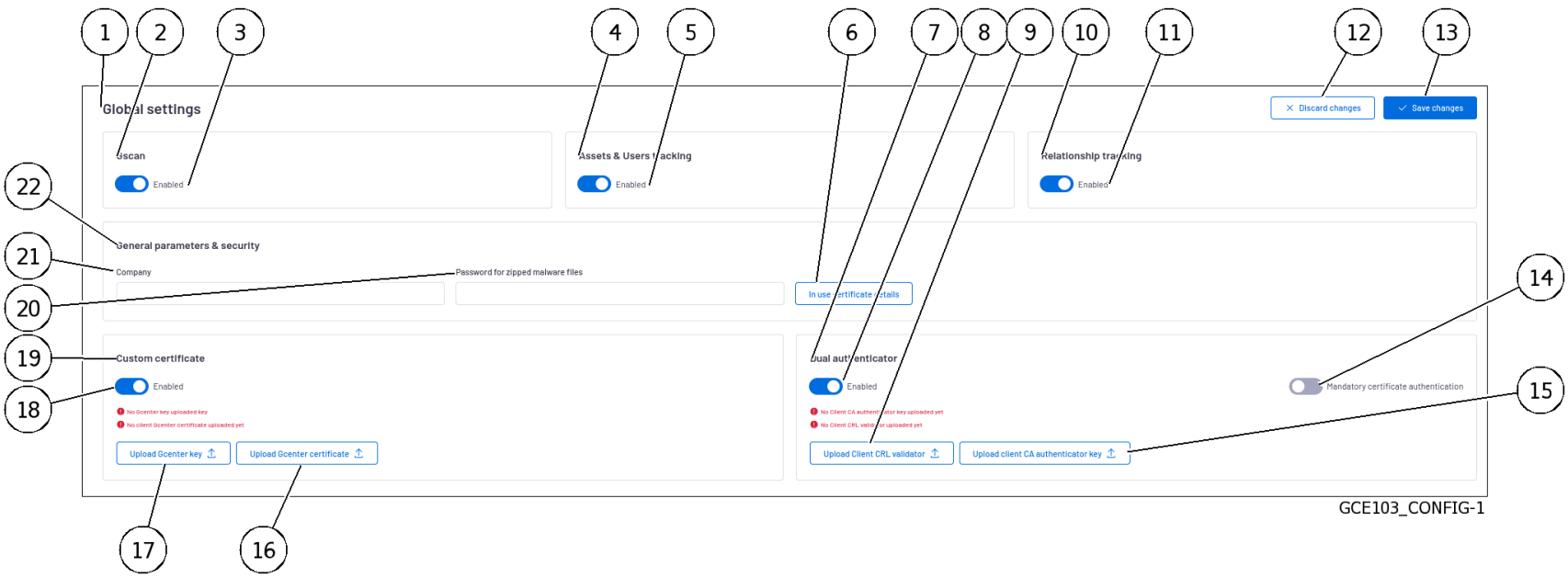
8.6.9.5 Procedure to access the `Global settings` screen



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Global settings` command from the `System` submenu.
  The `Global settings` window is displayed.

8.6.9.6 Procedure

The following screen is displayed:



- Use the `Enabled` selector (3) of the `GScan` zone (2) to allow real-time local analysis of suspicious malware or executables.
  The default is: enabled.

  Note:

  As part of the Military Programming Law, the GScan feature is disabled by default in this management interface.

- Enter the parameters of the `General parameters & security` zone (22):
- Enter the company name in `Company` field (21).
  This field adds the company name on the detection analysis reports.
  These reports can be downloaded after making an association between the GCenter and the Intelligence platform.
  The default is: empty.
- Enter the password that protects the archive when downloading malware in `Password for zipped malware files` field (20).
  The default is: empty.
  This password protects the archive when downloading malware and decompresses it to avoid an unfortunate click.
  This password is the same for downloading shellcodes.
  This feature is described in more detail in the Malcore parts.
- If needed, use the `In use certificate details` button (6).
  Opens a screen to display information on the certificate currently on the following zones:

  * the `In use certificate details KEY` zone
  * the `In use certificate details PEM` zone
  * the `CA certificate information` zone

- If needed, use the `Custom certificate` function (19):

- Use the `Enabled` selector (18)
- Use the `Upload Gcenter Key` button (17) to select a GCenter key file
- Use the `Upload Gcenter certificate` button (16) to select a GCenter certificate

- If needed, use the `Dual authenticator` function (7):

- Use the `Enabled` selector (8))
- Use the `Upload Client CRL validator` button (9) to select a file from the list of revoked certificates
- Use the `Upload Client CA authenticator key` button (15) to select a certificate file issued by the certification authority in PEM format
- Use the `Mandatory certificate authentication` selector to make it mandatory for users to hold a certificate issued by the certification authority

- Press the `Save changes` button (13) to save current settings and update the GCenter.

Important:

If the equipment **GCenter** and **GCap** is in an environment that is part of the LPM framework (Military Programming Law) the GSCAN service is automatically disabled and cannot be activated.
For more information, refer to the LPM section of this document.

8.7 Managing user accounts

8.7.1 Creating local user

8.7.1.1 Introduction

This procedure describes how to create a new GCenter user.
To do this, enter the following:

- Mandatory information - username and password
- Optional information - email address, first and last name
- Select membership of existing groups - Operator, Administrator
- Enable or disable this new user

8.7.1.2 Links associated

See the presentation of the *Web interface accounts and their management*.
This graphical interface is described in the *`Users management` screen*.

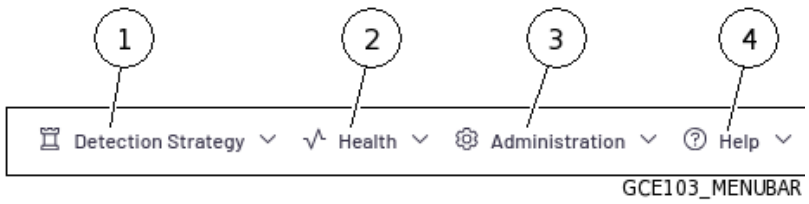
8.7.1.3 Prerequisites

- User: member of **Administrator** group

8.7.1.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

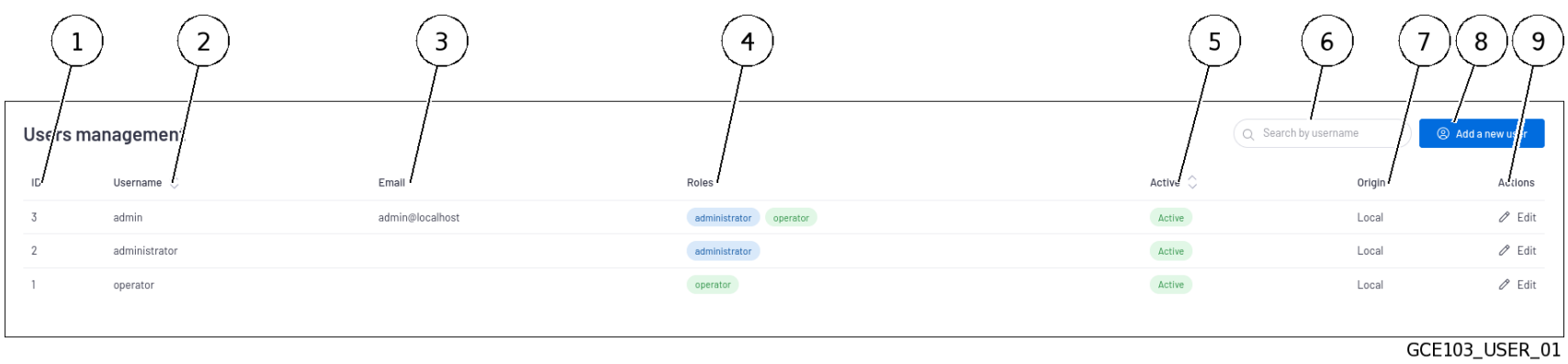
8.7.1.5 Procedure to access the `Users management` screen



GCE103_MENUBAR

- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Users management` command from the `Authentication` submenu.
  The `Users Management` window is displayed.

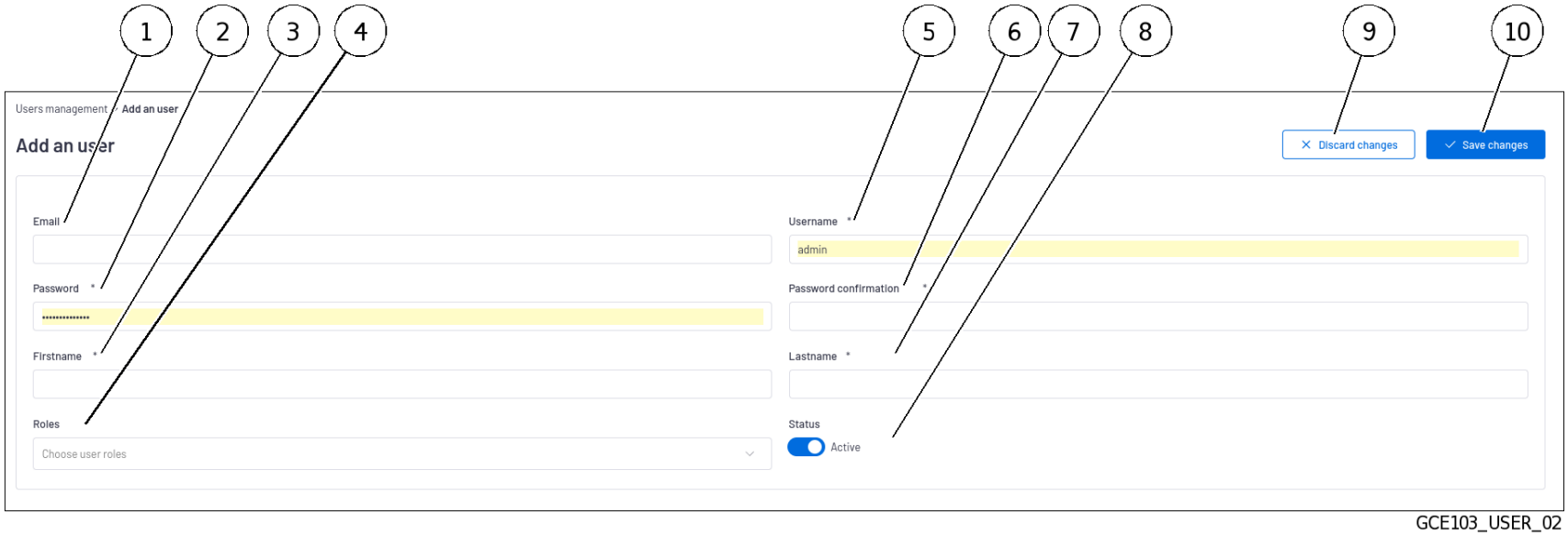
8.7.1.6 Procedure to create a new user



GCE103_USER_01

The window shows account information such as ID, username, creation date, last login, and admin group membership.

- Click on the `Add a new user` button (8).
  The `Add a new user` window is displayed.



GCE103_USER_02

- Enter the email address in the field `Email` (1) : optional field.
- Enter the password. To do this:

- Enter it in the `Password` field (2)
- Enter it again in the `Password confirmation` field (6)
  The password entered must match the *Password management policy*.
  The system checks the password against the verification policy.
  If the password does not meet the verification policy, one of the following messages will be displayed:
  - `Password must contain 12 characters or more`: indicates a password that is too short
  - `Password must contain a capital letter`: indicates the lack of a capital
  - `Password must contain a lowercase letter`: indicates the lack of a small letter
  - `Password must contains a special character`: indicates the lack of a special character
  - `Password must contains a number`: indicates the lack of a number

  If the two passwords do not match, the following message is displayed: `The two password fields do not match.`

- Enter the user's first name in the `First name` field (3).
- Select the role(s) (4): optional field
  - `Operator`
  - `Administrator`

- Enter the full name of the new user in the `Username` field (5).
  It may contain only letters, numbers, and [@/./+/-/-/_.] characters.
- Enter the user's last name in the field `Last name` (7): optional field.
- Activate the account with the `Status` selector (8).
- Validate the entry with the `Save changes` button (10).

8.7.2 Changing some of a local user's information

8.7.2.1 Introduction

This procedure describes how to modify local users:

- Email address
- First name
- Last name
- Membership of the `Operator` or / and `Administrator` groups
- Account enabling

8.7.2.2 Links associated

See the presentation of the *Web interface accounts and their management*.
This graphical interface is described in the *`Edit` screen*.

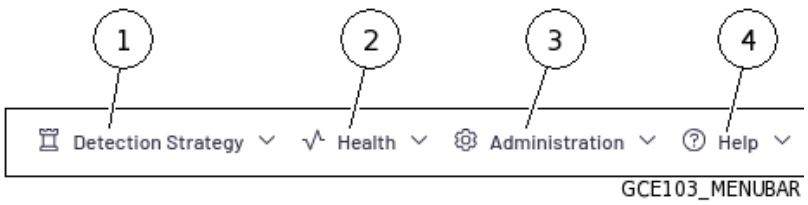
8.7.2.3 Prerequisites

- User: member of **Administrator** group

8.7.2.4 Preliminary operations

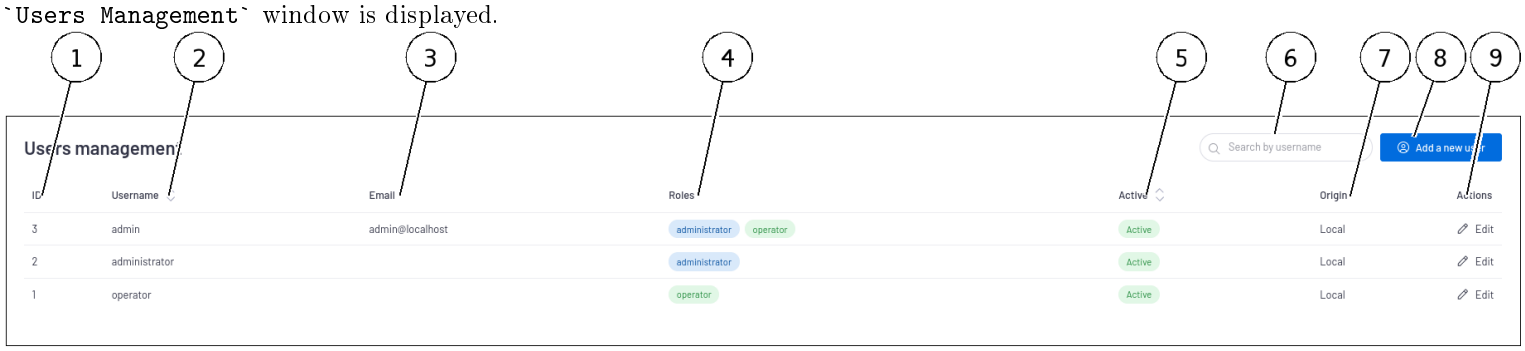
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*) with the prerequisite rights.

8.7.2.5 Procedure to access to the `Users management` window



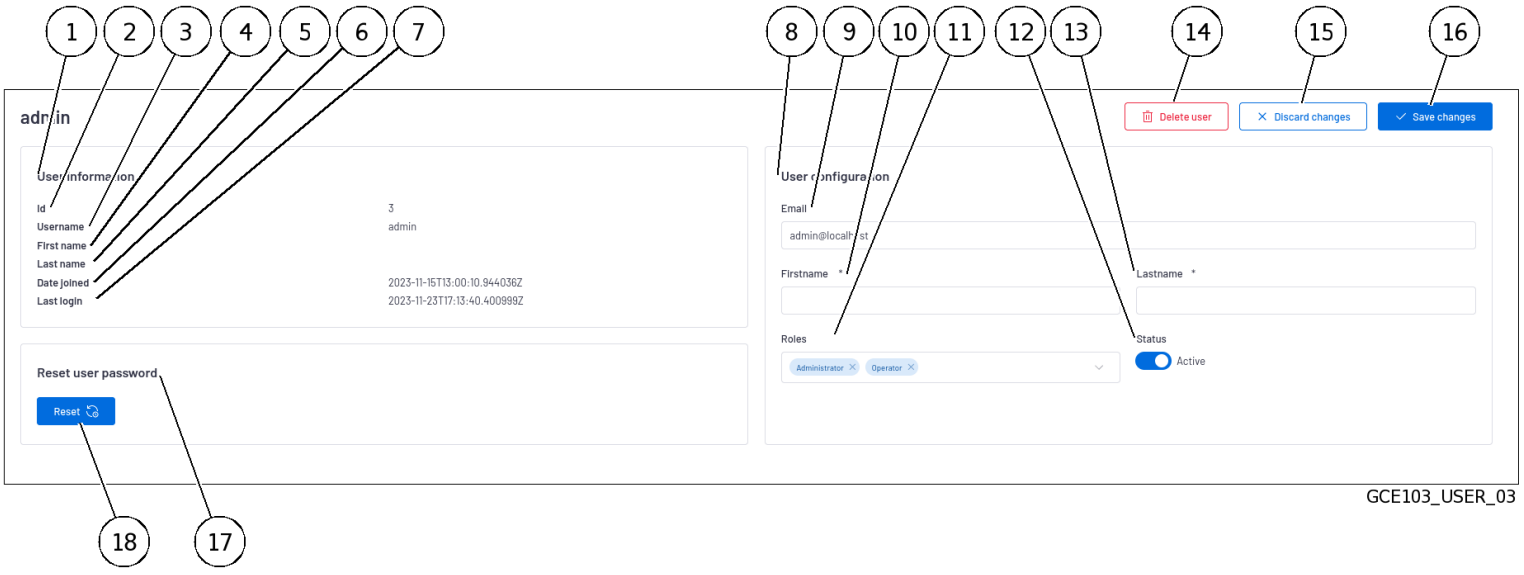
GCE103_MENUBAR

- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Users management` command from the `Authentication` submenu.
  The `Users Management` window is displayed.



GCE103_USER_01

- Click on the `Edit` button of the column (9) of the user whose settings have to be changed.
  The `Edit` window is displayed.



The window shows account information such as ID, username, creation date, last login, and admin group membership.

8.7.2.6 Procedure to change certain user information

- In the `User information` area (2), view the current configuration:

- in the `Email address` field (1)
- in the `Id` field (2)
- in the `Username` field (3)
- in the `First name` field (4)
- in the `Last name` field (5)

- In the `User configuration` area (8), enter or modify the data found in:

- in the `First name` field (4)
- in the `Last name` field (5)
- in the `Email` field (9)
- in the `Roles` field (11)
  Defines the roles granted to the account.
  The possible roles are Operator and/or Administrator.
- with the `Status` selector (12)
  The selector activates or deactivates the account.

- Confirm the changes using the `Save changes` button (16).

8.7.3 Resetting a local user's password

8.7.3.1 Introduction

This procedure describes how to reset the current user's password.

Note:

This procedure enables the password associated with the user account to be regenerated if it is lost or forgotten.
The system will propose a new password.

Danger:

It is possible to select your own account!
If this is voluntary, carefully note the password displayed.

8.7.3.2 Links associated

See the presentation of the *Web interface accounts and their management*.
This graphical interface is described in the *`Edit` screen*.

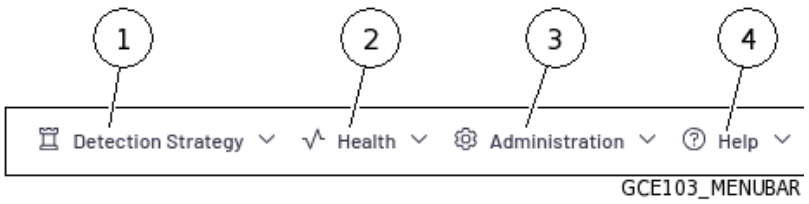
8.7.3.3 Prerequisites

- User: member of **Administrator** group

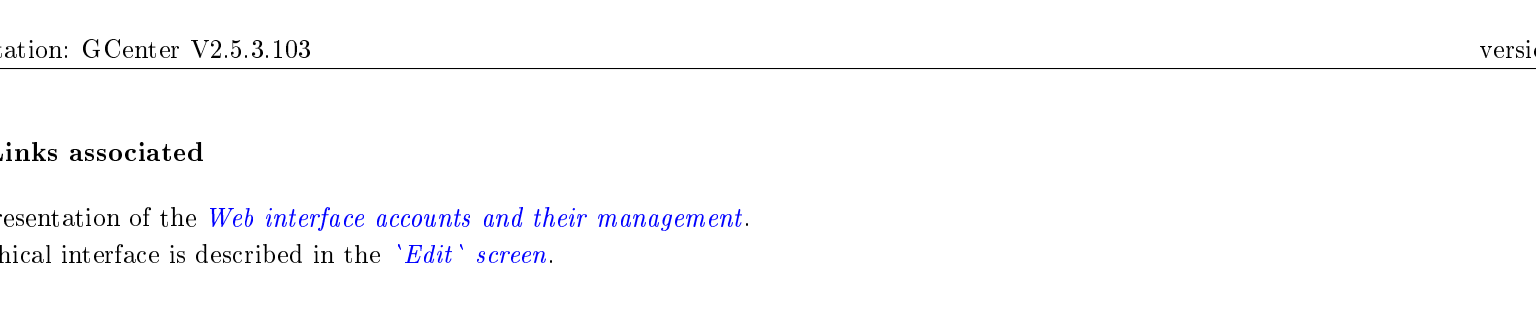
8.7.3.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

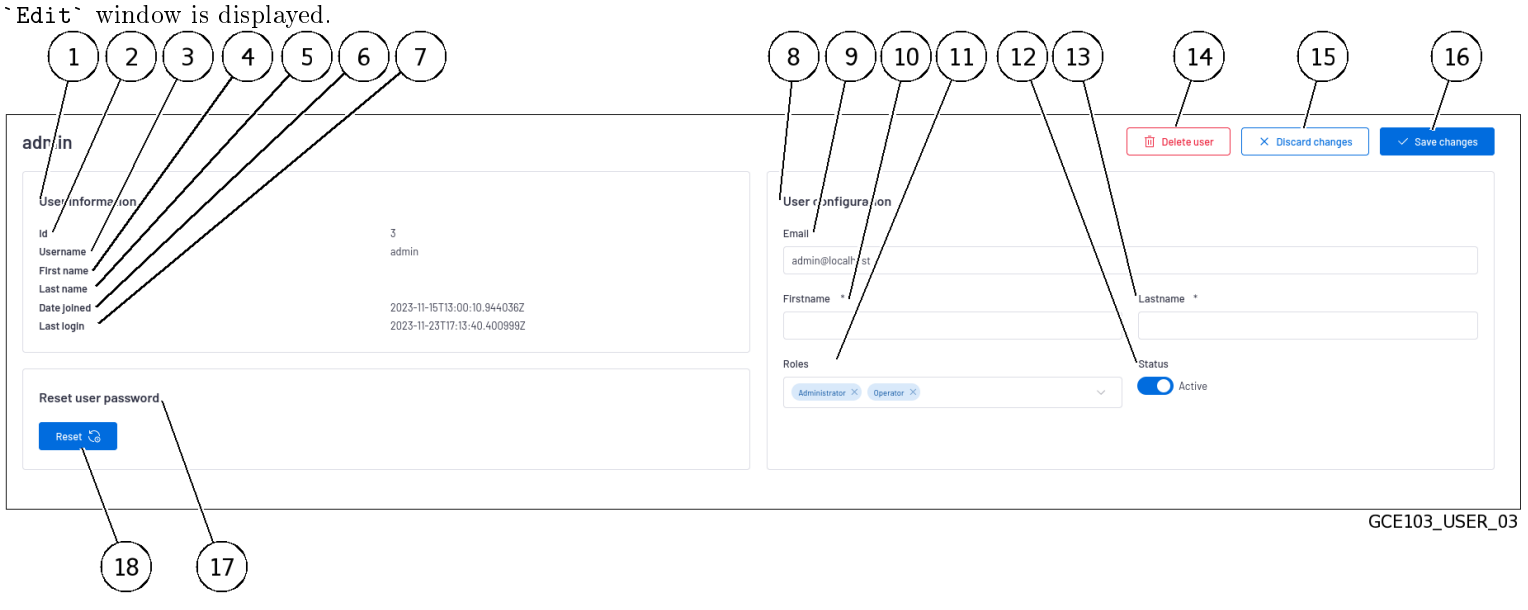
8.7.3.5 Procedure to access to the `Users management` window



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Users management` command from the `Authentication` submenu.
  The `Users Management` window is displayed.



- Click on the `Edit` button of the column (9) of the user whose password has to be changed.
  The `Edit` window is displayed.



8.7.3.6 Procedure to reset a user's password

Note:

This procedure enables the password associated with the user account to be regenerated if it is lost or forgotten.
The system will propose a new password.

- Select the user's account.
- Click the `Reset` button (18) in the `Reset user's password` area (17).
  The following message is displayed: `Password changed to xxxxxx. Please, ask your user to change it to a new one at the next login (safety first)!`.
- Click on the New temporary password link to copy the new password.
- Contact the user and inform it of its new password (paste this new password in the sent email).
  Please ask your user to change it to a new one at the next login.
- Inform the user to refer to the *Changing the checking account password* procedure.

8.7.4 Deleting a local user

8.7.4.1 Introduction

This procedure describes how to delete a local user.

8.7.4.2 Links associated

See the presentation of the in *Web interface accounts and their management*.
This graphical interface is described in the *`Edit` screen*.

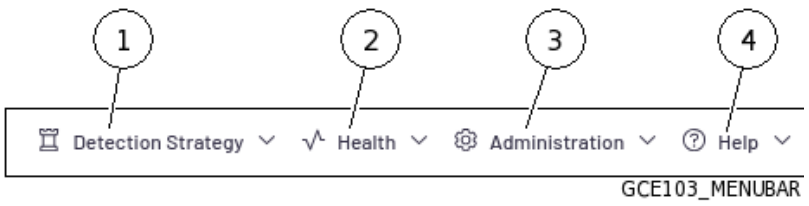
8.7.4.3 Prerequisites

- User: member of **Administrator** group

8.7.4.4 Preliminary operations

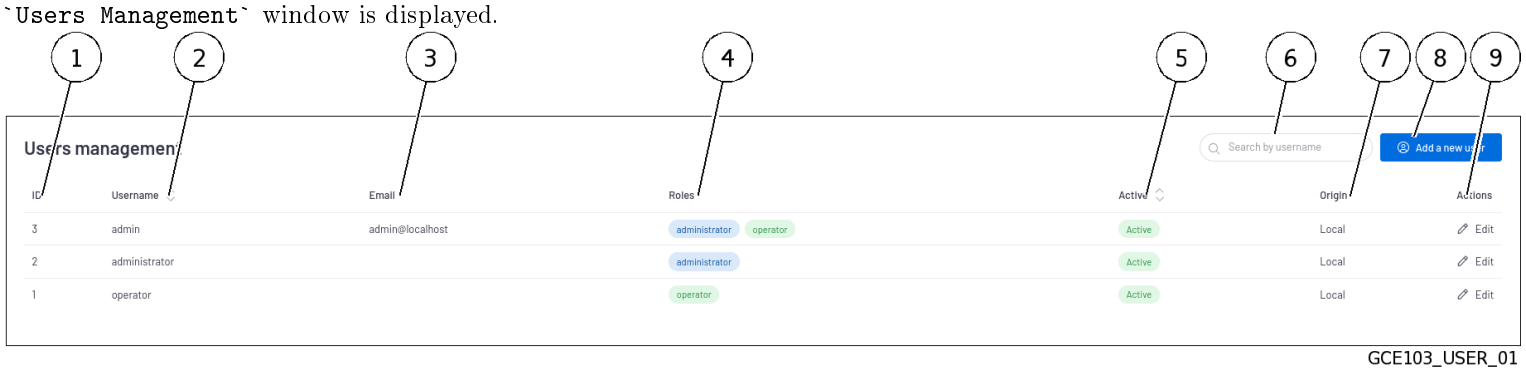
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.7.4.5 Procedure to access to the `Users management` window



GCE103_MENUBAR

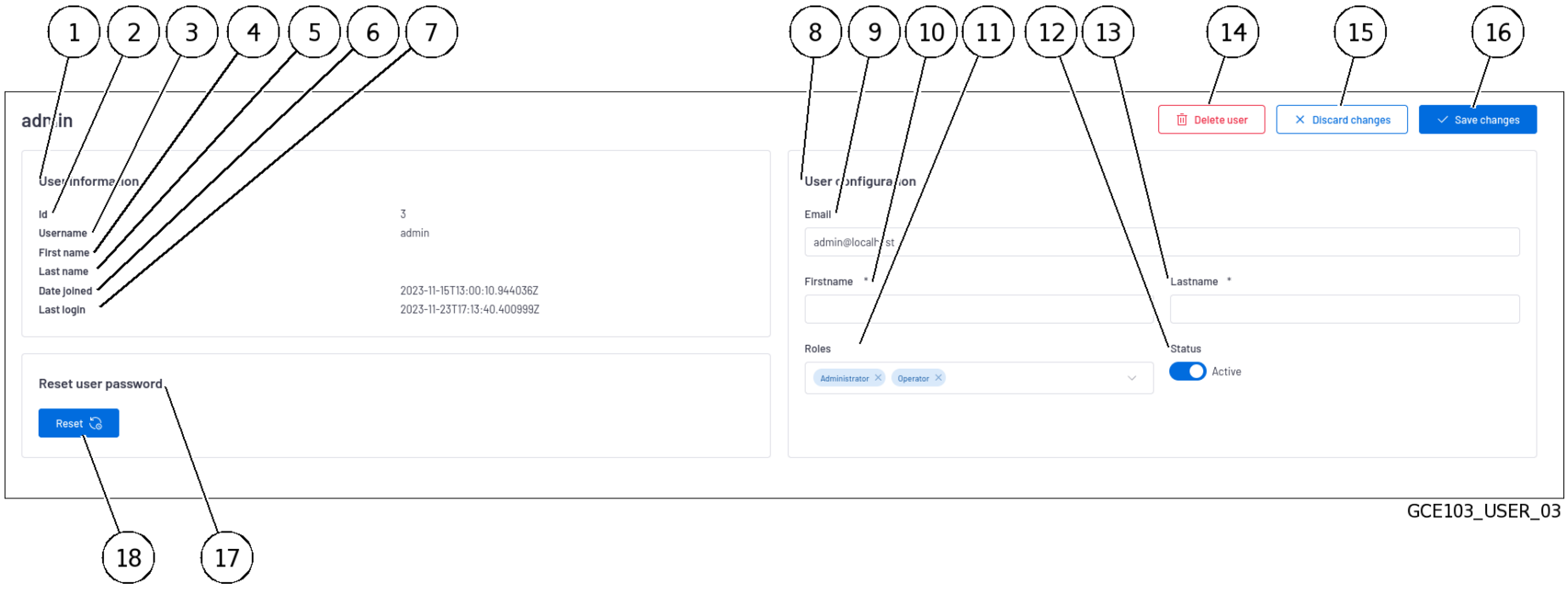
- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Users management` command from the `Authentication` submenu.
  The `Users Management` window is displayed.



GCE103_USER_01

- Click on the `Edit` button of the column (9) of the user to delete.
  The `Edit` window is displayed.

8.7.4.6 Procedure to delete local user



GCE103_USER_03

Danger:

It is possible to select your own account! If this is voluntary, carefully note the password displayed.

- Select the user account.
- Click the `Delete user` button (14).
  The `Delete user` window is displayed to confirm the deletion.
- Click on the `Delete` button.
  The list of accounts is updated.

8.7.5 Displaying of the connection status between the GCenter and the LDAP server

8.7.5.1 Introduction

This procedure enables displaying the connection status between the GCenter and the LDAP / ActiveDirectory server.

8.7.5.2 Links associated

This graphical interface is described in the *`LDAP binding` screen*.

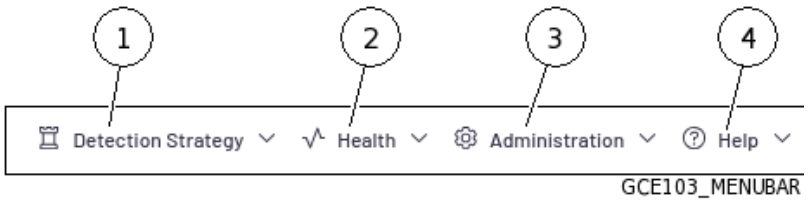
8.7.5.3 Prerequisites

- User: member of **Administrator** group

8.7.5.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.7.5.5 Procedure to access to the `LDAP configuration` window



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `LDAP binding` command from the `Authentication` submenu.
  The `LDAP Configuration` window is displayed.

8.7.5.6 Procedure to test the connection

- Click on the `Test connection` link.
  If the connection is not ok, an error message is displayed like this:

```
Error
Cannot connect to LDAP with current settings: {'result': -1, 'desc': "Can't contact LDAP server", 'errno': 11,
↪'ctrls': [], 'info': 'Resource temporarily unavailable'}
```

8.7.6 Enabling the connection between the GCenter and the LDAP server

8.7.6.1 Introduction

This procedure enables the connection and thus the authentication by the LDAP/ActiveDirectory server.

8.7.6.2 Links associated

This graphical interface is described in the *`LDAP binding` screen*.

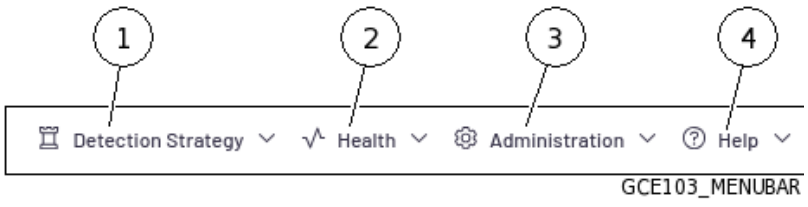
8.7.6.3 Prerequisites

- User: member of **Administrator** group

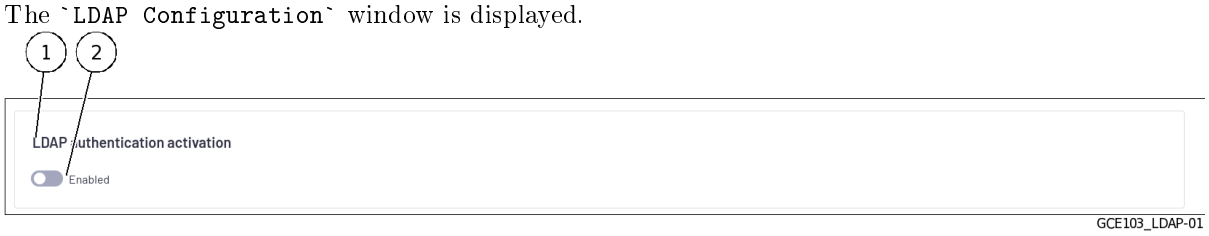
8.7.6.4 Preliminary operations

- Configure the LDAP server settings (see the *Configuring the connection between the GCenter and the LDAP server*).
- Set up users and groups (see the *Configuring the users and groups defined on LDAP / ActiveDirectory*).

8.7.6.5 Procedure to enable the LDAP functionality



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `LDAP binding` command from the `Authentication` submenu.
  The `LDAP Configuration` window is displayed.



In the `LDAP authentication settings` area (1):

- Use the `Enabled` selector (2).
- Click on the `Save changes` button.
  A Warning window is displayed with the message `Saving and applying the new LDAP settings will restart the application and disconnect all users!`
- Click on the `Confirm` button.

Note:

The current session is disconnected when the LDAP configuration is applied.

8.7.7 Configuring the connection between the GCenter and the LDAP server

8.7.7.1 Introduction

This procedure enables setting up the LDAP server using:

- The `LDAP server binding settings` area
- The `LDAP advanced settings` area

This screen enables entering the connection information to a remote authentication server.

8.7.7.2 Links associated

This graphical interface is described in the *`LDAP binding` screen*.

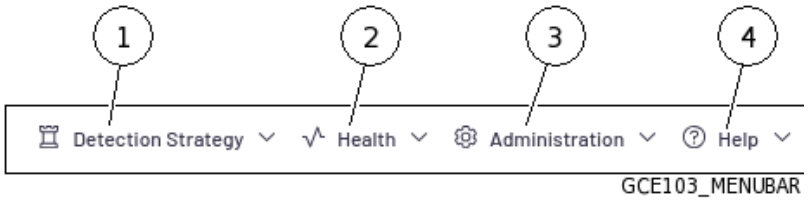
8.7.7.3 Prerequisites

- User: member of **Administrator** group

8.7.7.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

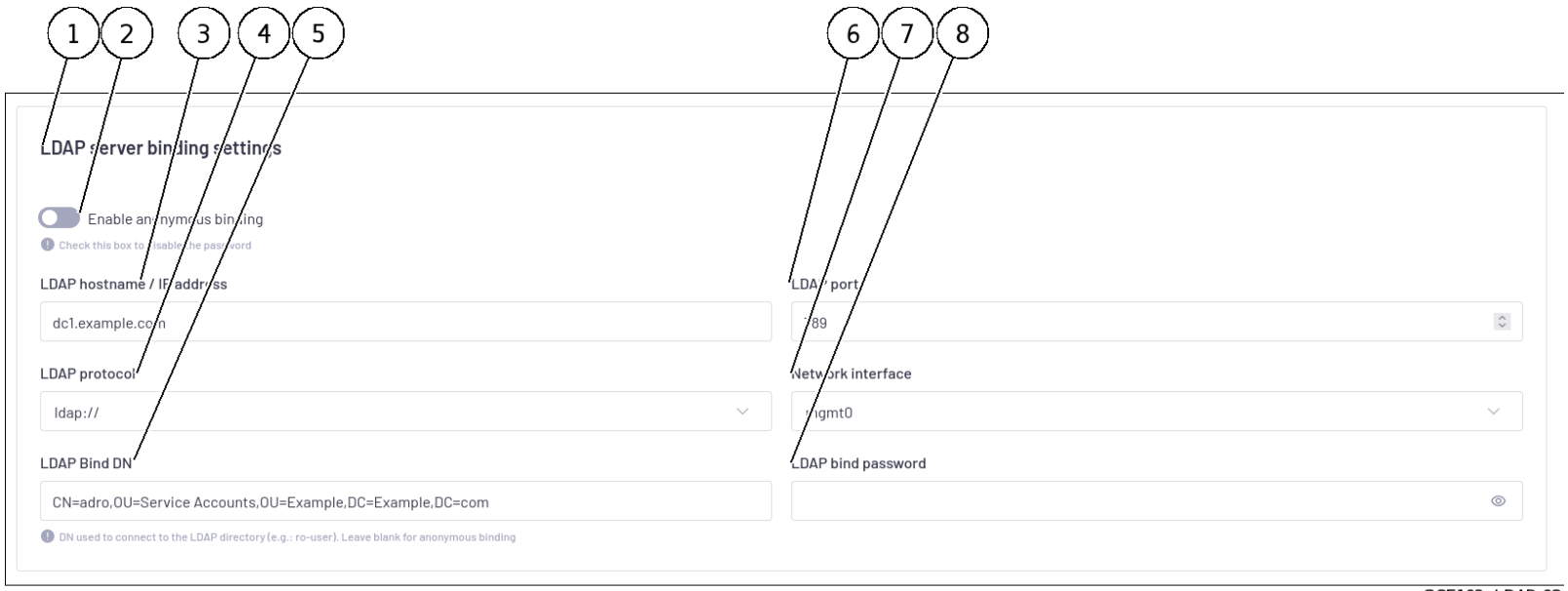
8.7.7.5 Procedure to access to the `LDAP configuration` area



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `LDAP binding` command from the `Authentication` submenu.
  The `LDAP Configuration` window is displayed.

8.7.7.6 Procedure to enter the settings of the `LDAP server binding settings` area

This area enables the input of login information to a remote authentication server.



GCE103_LDAP-02

- Expand the window to access the parameters using the arrows.
- Enter the following parameters:

Item	Name	Function
1	`LDAP server binding settings`	Login information input area
2	`Enable anonymous binding` selector	• Enables not having to enter the login password
3	`LDAP hostname / IP address`	• Specifies the IP address or name of the remote server
4	`LDAP protocol`	• Chooses the protocol used for the connection ldap:// ou ldaps://
5	`LDAP binding DN`	• Specifies the user name for connecting to the remote server DN used to connect to the LDAP directory (e.g.: ro-user). Leave blank for anonymous binding
6	`LDAP port`	• Specifies the port of the remote server 389 for ldap or 636 for ldaps for example
7	`Network interface`	• Chooses the GCenter interface through which to communicate with the remote server mgmt0 by default
8	`LDAP binding password`	• Specifies the user's password for connecting to the remote server

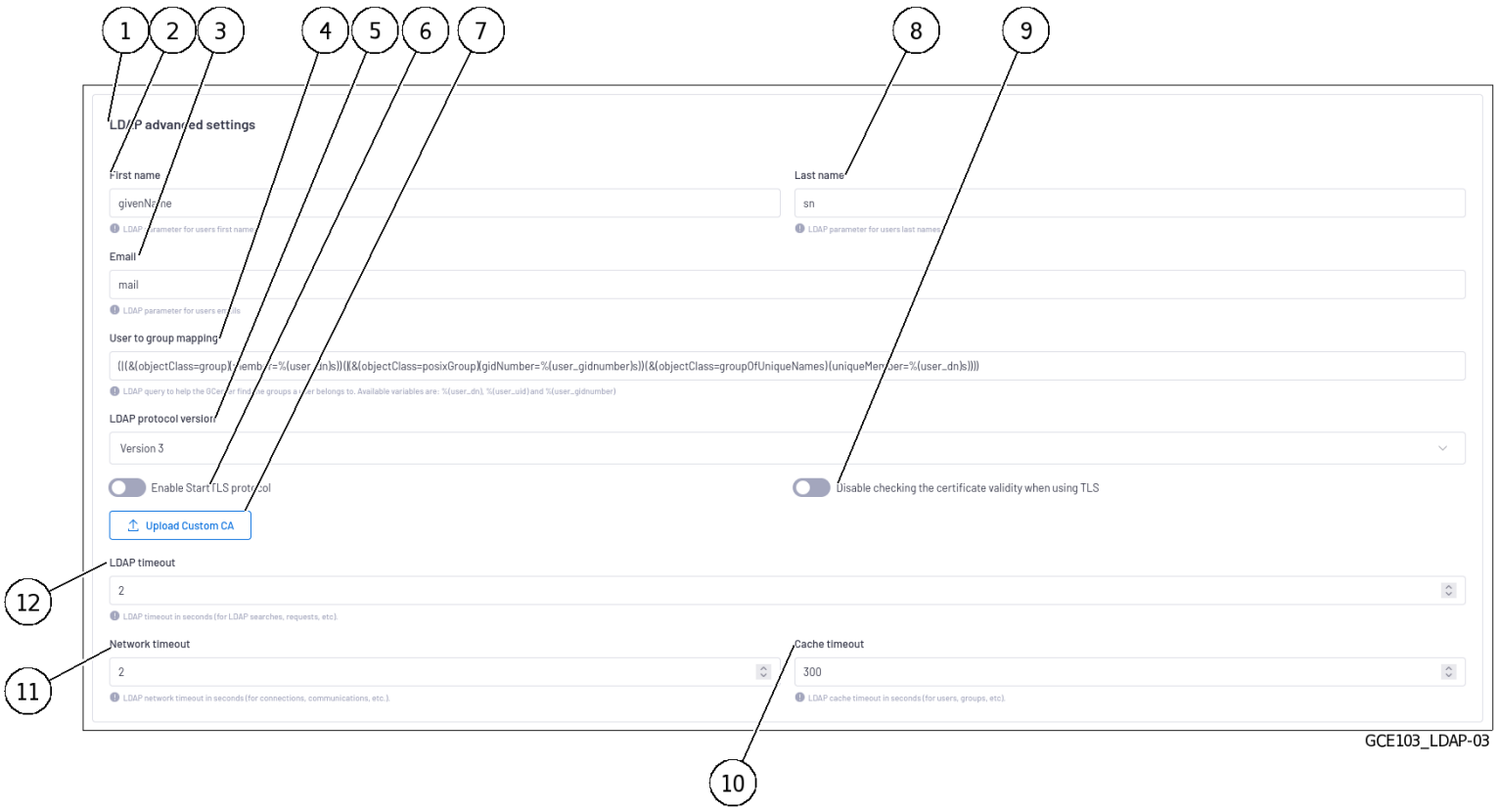
Note:

If the `Enable anonymous binding` option is enabled, it is not necessary to fill in the username and password.

- Save the changes with the `Save changes` button.
  Warning window is displayed with the message `Saving and applying the new LDAP settings will restart the application and disconnect all users!`.
- Click on the `Confirm` button.

8.7.7.7 Procedure to enter the settings of the `LDAP advanced settings` area

This area enables advanced configuration of the connection to a remote authentication server.



- Expand the window to access the parameters using the arrows.
- Enter the following parameters:

Item	Name	Function
1	`LDAP advanced settings`	Area of advanced configuration of the connection to a remote authentication server
2	`First name`	• Specifies the LDAP parameter for the first name of the users
3	`Email`	• Specifies the LDAP setting for the user's email
4	`User to group mapping`	• Enables entering an LDAP query to help the GCenter find the groups a user belongs to
5	`LDAP protocol version`	• Chooses the LDAP version of the remote server
6	`Enable StartTLS protocol` selector	• Enables or disables the StartTLS protocol
7	`Upload Custom CA` button	• Loads a certificate for LDAP use
8	`Last name`	• Specifies the LDAP parameter for the last name of the users
9	`Disable checking the certificate validity when using TLS` selector	• Enables or disables certificate validity checking (LDAPS)
10	`Cache timeout`	• Specifies the waiting time for LDAP users and groups
11	`Network timeout`	• Specifies the waiting time at the LDAP communications network level (by default: 2)
12	`LDAP timeout`	• Specifies the waiting time for LDAP queries (by default: 2)

8.7.7.8 Procedure to finish the settings

- Click on the `Save changes` button.
  Warning window is displayed with the message `Saving and applying the new LDAP settings will restart the application and disconnect all users!`.
- Click on the `Confirm` button.

Note:

To configure the LDAPS:
- Enter in `LDAP server binding settings`:
  - `LDAP protocol`: *ldaps://*
  - `LDAP_port`: *636*
- Enter the certificate of the certification authority in the field `LDAP advanced settings`.

Note:

To configure LDAP over TLS:
- Enter the certificate of the certification authority in the `LDAP advanced settings` field
- Tick the `Enable StartTLSProtocol` box in the `LDAP advanced settings` window

8.7.8 Configuring the users and groups defined on LDAP / ActiveDirectory

8.7.8.1 Introduction

This procedure enables specifying the mapping of users and groups between the GCenter and the remote authentication server.

8.7.8.2 Links associated

This graphical interface is described in the *`LDAP binding` screen*.

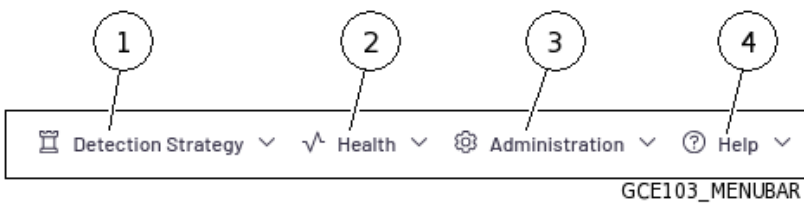
8.7.8.3 Prerequisites

- User: member of **Administrator** group

8.7.8.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

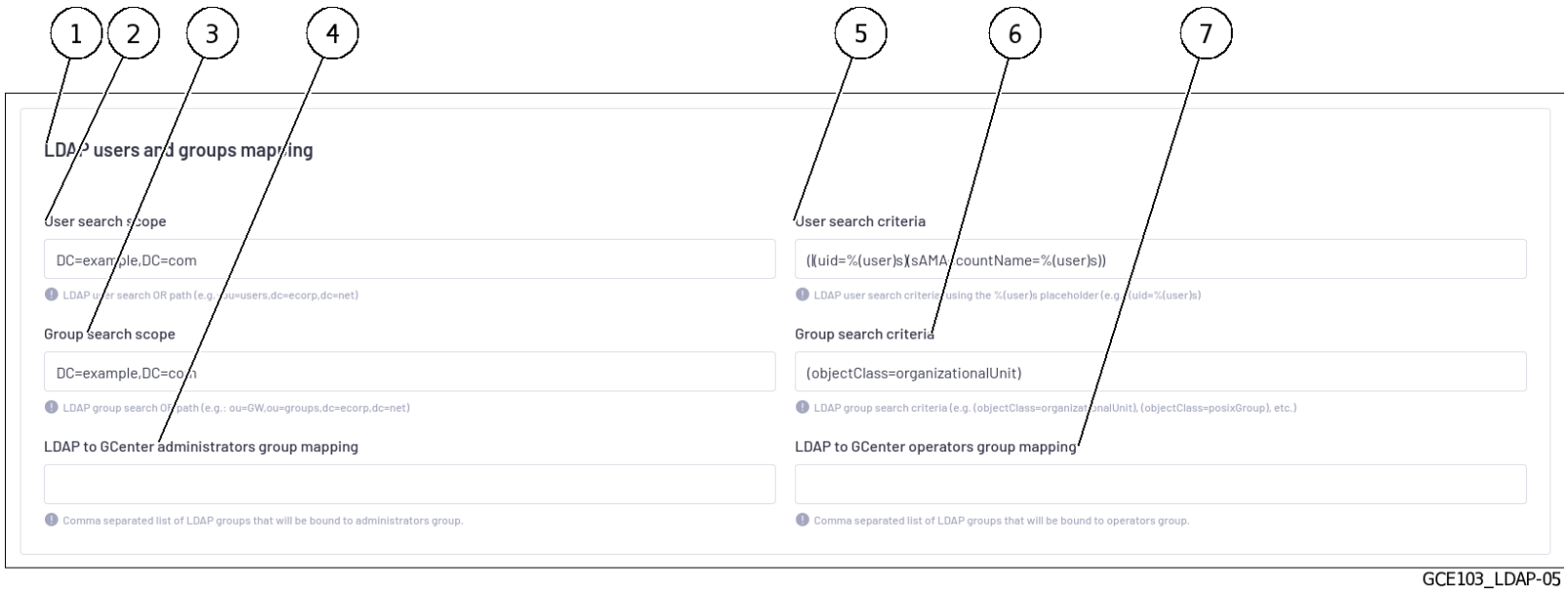
8.7.8.5 Procedure to access to the `LDAP configuration` area



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `LDAP binding` command from the `Authentication` submenu.
  The `LDAP Configuration` window is displayed.

8.7.8.6 Procedure to enter the settings of the `LDAP users and groups mapping` area

This area enables to specify the mapping of users and groups between the GCenter and the remote authentication server.



GCE103_LDAP-05

- Expand the window to access the parameters using the arrows.
- Enter the following parameters:

Item	Name	Function
1	`LDAP users and groups mapping`	Area to specify the mapping of users and groups between the GCenter and the remote authentication server
2	`User search scope`	• Specifies the search for users in the remote directory by default: DC=example, DC=com
3	`Group search scope`	• Specifies the search for groups in the remote directory by default: DC=example, DC=com
4	`LDAP to GCenter administrators group mapping`	• Specifies which groups will have the "administrator" role Groups of administrators for example
5	`User search criteria`	• Specifies the search criteria for users in the remote directory by default: *(|(uid=%(user)s)* *(sAMAccountName=%(user)s))*
6	`Group search criteria`	• [Specifies the search criteria for groups in the remote directory | by default: | (objectClass=organizationalUnit)
7	`LDAP to GCenter operators group mapping`	• Specifies which groups will have the "operator" role groups of analysts for example

Note:

If the `Enable anonymous binding` option is enabled, it is not necessary to fill in the username and password.

Note:

The same group can be present in both the `LDAP to gcenter administrators group mapping` and `LDAP to gcenter operators group mapping` fields.

- Save the changes with the `Save changes` button.
  Warning window is displayed with the message `Saving and applying the new LDAP settings will restart the application and disconnect all users!`.
- Click on the `Confirm` button.
- Click on the `Save changes` button.
  Warning window is displayed with the message `Saving and applying the new LDAP settings will restart the application and disconnect all users!`.
- Click on the `Confirm` button.

8.7.9 Viewing the authentication history

8.7.9.1 Introduction

This procedure enables viewing the history of all authentications on the GCenter.

8.7.9.2 Links associated

This graphical interface is described in *`History` screen*.
Refer to the Kibana interface, see *Overview of the Kibana GUI*.
See the procedure *Configuring the authentication history*.

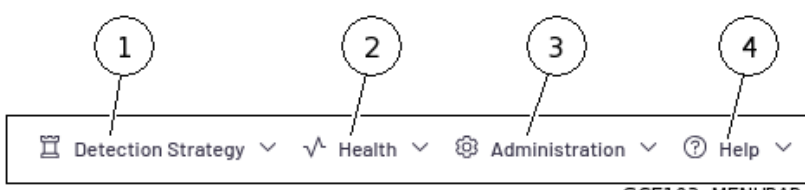
8.7.9.3 Prerequisites

- User: member of **Administrator** group

8.7.9.4 Preliminary operations

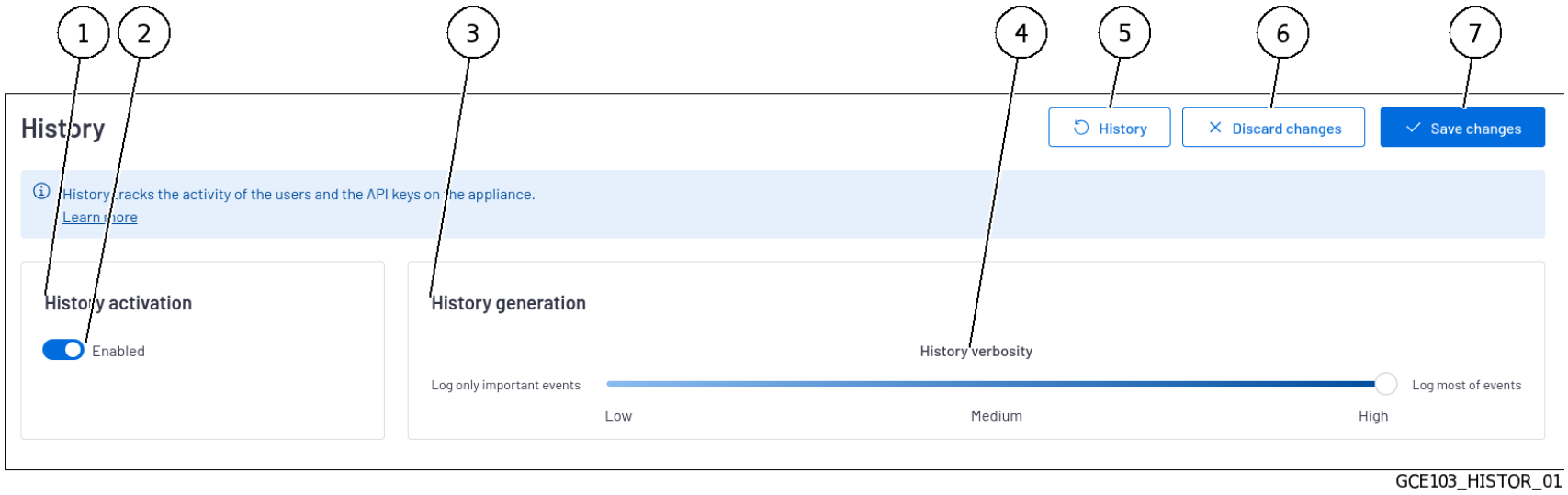
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.7.9.5 Procedure to access to the `History` window



GCE103_MENUBAR

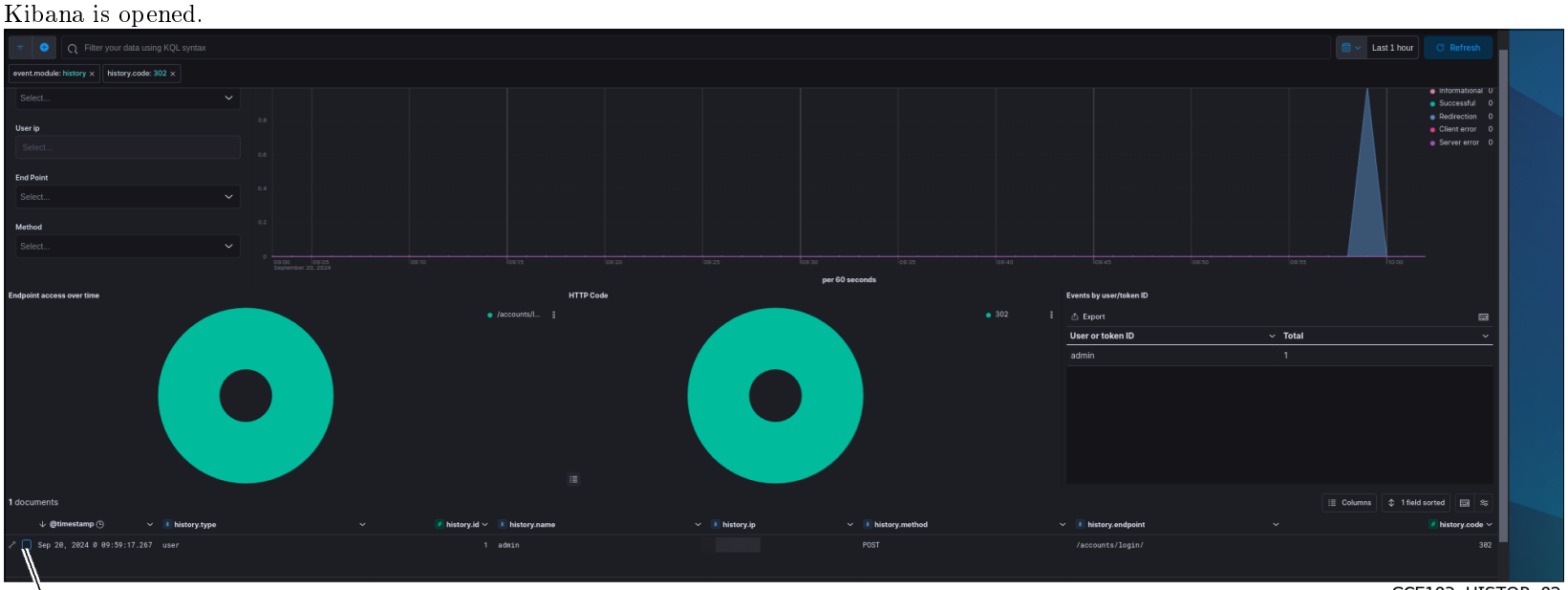
- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `History` command from the `Authentication` submenu.
  The `History` window is displayed.



GCE103_HISTOR_01

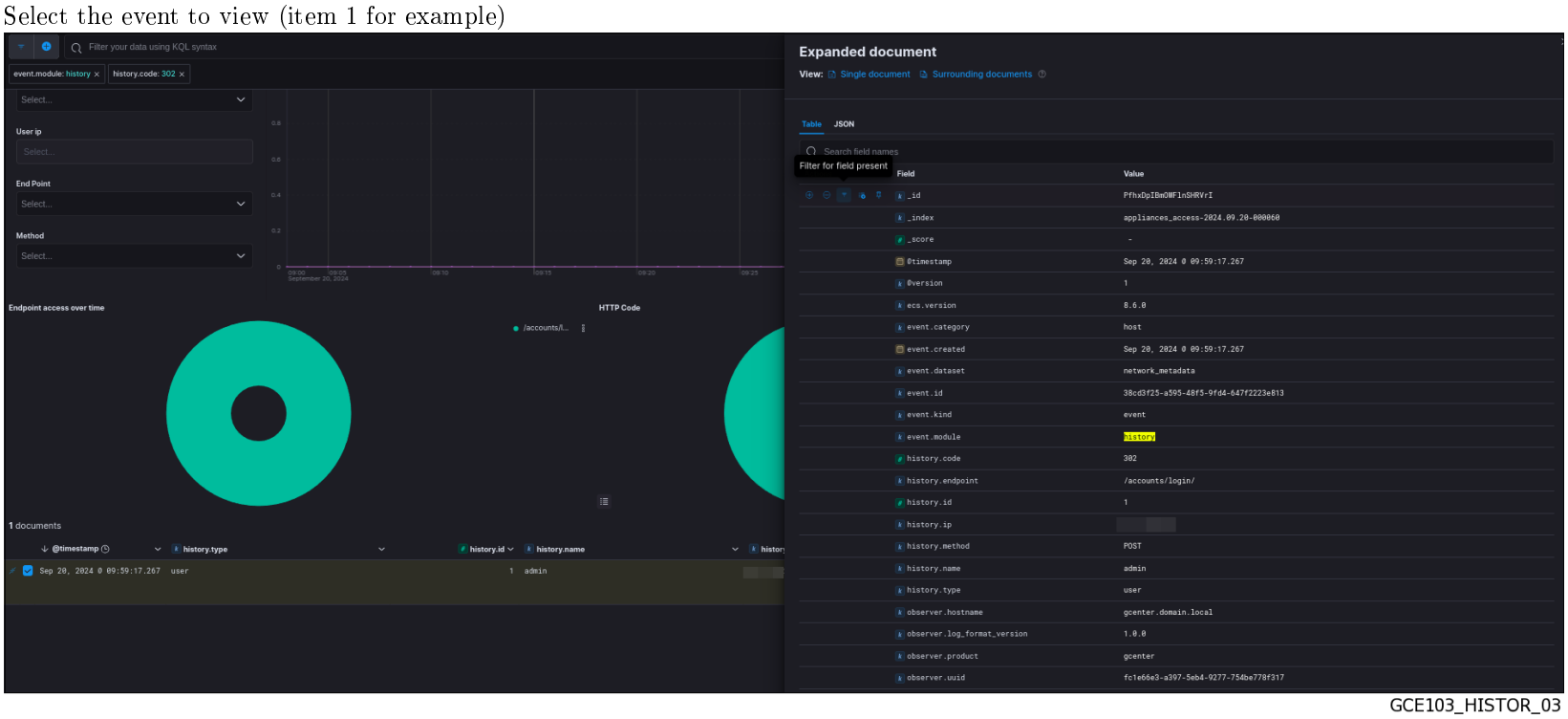
8.7.9.6 Procedure to explore history events in Kibana

- Click on the `History` button (5).
  Kibana is opened.



GCE103_HISTOR_02

- Select the event to view (item 1 for example)



GCE103_HISTOR_03

The detailed information is displayed.

8.7.10 Configuring the authentication history

8.7.10.1 Introduction

This procedure configures the history of all authentications on the GCenter.

8.7.10.2 Links associated

This graphical interface is described in *`History` screen*.
See the procedure de *Viewing the authentication history*.

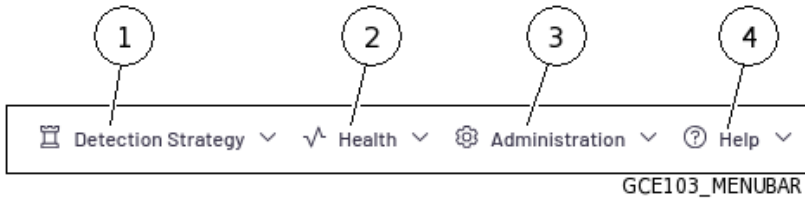
8.7.10.3 Prerequisites

- User: member of **Administrator** group

8.7.10.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.7.10.5 Procedure to access to the `History` window



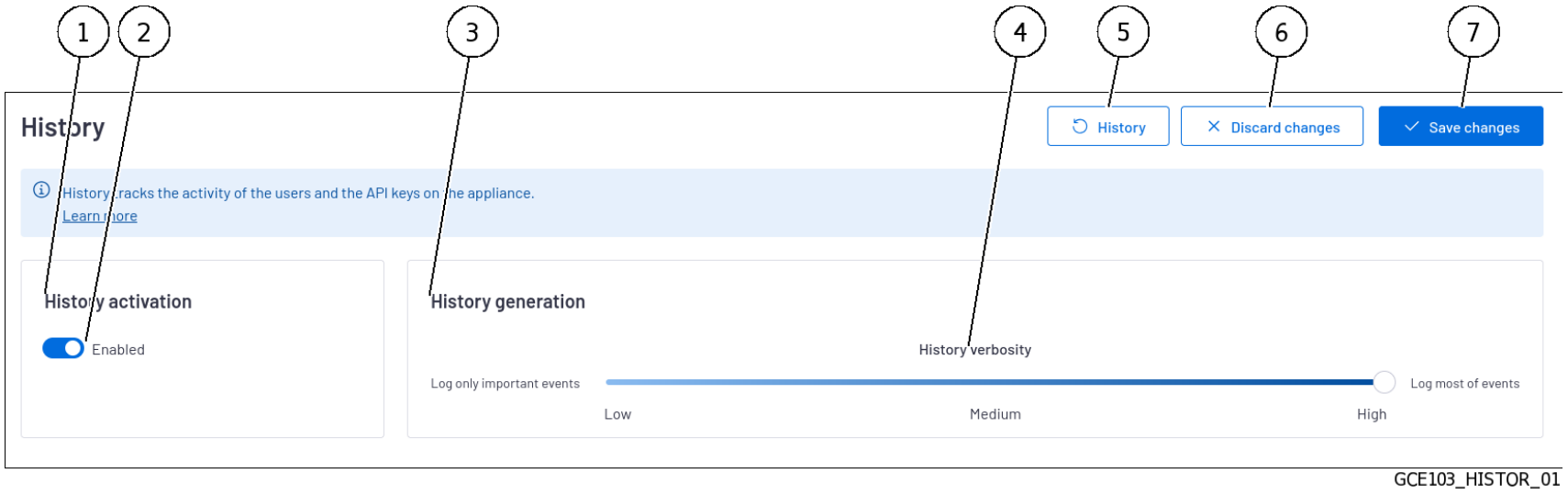
GCE103_MENUBAR

- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `History` command from the `Authentication` submenu.
  The `History` window is displayed.

GCE103_HISTOR_01

8.7.10.6 Procedure to activate the history

- Click on the `Enabled` selector (2) in the `History activation` area (1) onto the enabled position.



GCE103_HISTOR_01

- Click on the `Saves changes` button (7).
  The following message is displayed:

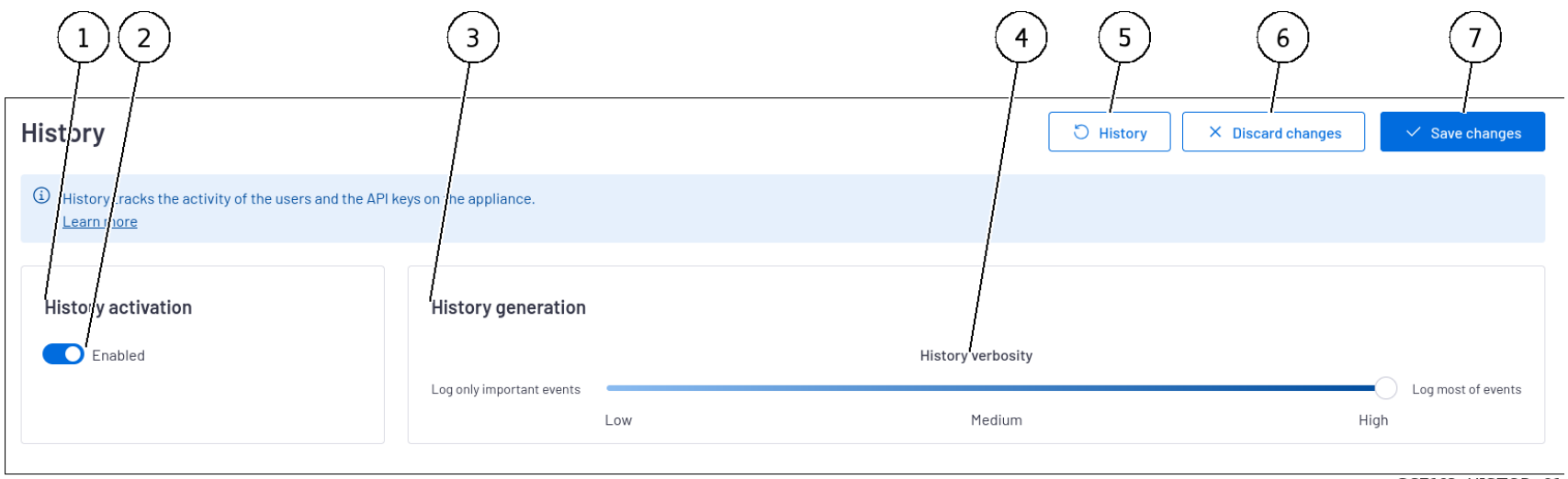
```
Success
Your data has been saved
```

8.7.10.7 Procedure to desactivate the history

- Click on the `Enabled` selector (2) in the `History activation` area (1) onto the disabled position.
- Click on the `Saves changes` button (7).
  The following message is displayed:

```
Success
Your data has been saved
```

8.7.10.8 Procedure to modify the History verbosity



- Use the `History verbosity` slider (4) to modify the event numbers to store.
- Click on the `Saves changes` button (7).
  The following message is displayed:

```
Success
Your data has been saved
```

8.7.11 Managing an API access token

8.7.11.1 Introduction

To	Apply the procedures
View the current API keys	1 - Apply the *Procedure to access to the `API keys` window* 2 - Apply the *Procedure to view the current API keys*
Add an API access token	1 - Apply the *Procedure to access to the `API keys` window* 2 - Apply the *Procedure to add a new API key*
Delete an existing token	1 - Apply the *Procedure to access to the `API keys` window* 2 - Apply the *Procedure to delete a API key*

8.7.11.2 Links associated

This graphical interface is described in the *`API keys` screen*.

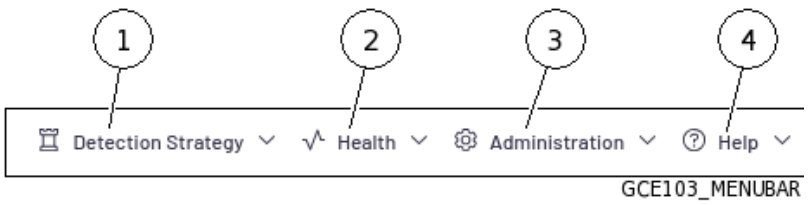
8.7.11.3 Prerequisites

- User: member of **Administrator** group

8.7.11.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

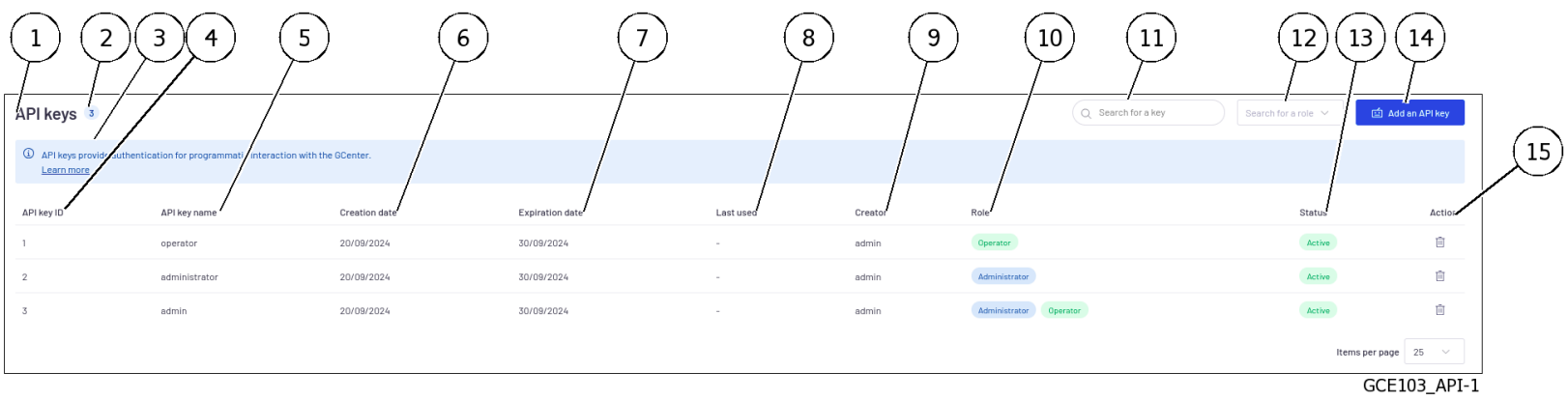
8.7.11.5 Procedure to access to the `API keys` window



GCE103_MENUBAR

- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `API keys` command from the `Authentication` submenu.
  The `API keys` window is displayed.

8.7.11.6 Procedure to view the current API keys



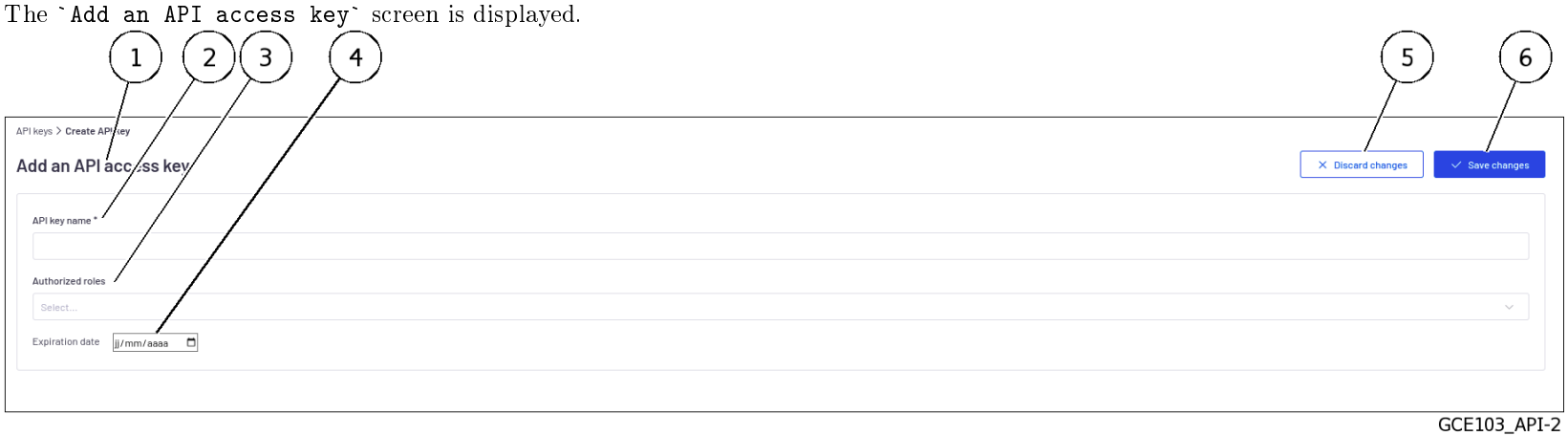
GCE103_API-1

The `API keys` window gives about information about the current API keys.
The information detailed is given in the *`API keys` screen*.

8.7.11.7 Procedure to add a new API key

GCE103_API-1

- Click on the `Add an API key` button (14).
  The `Add an API access key` screen is displayed.



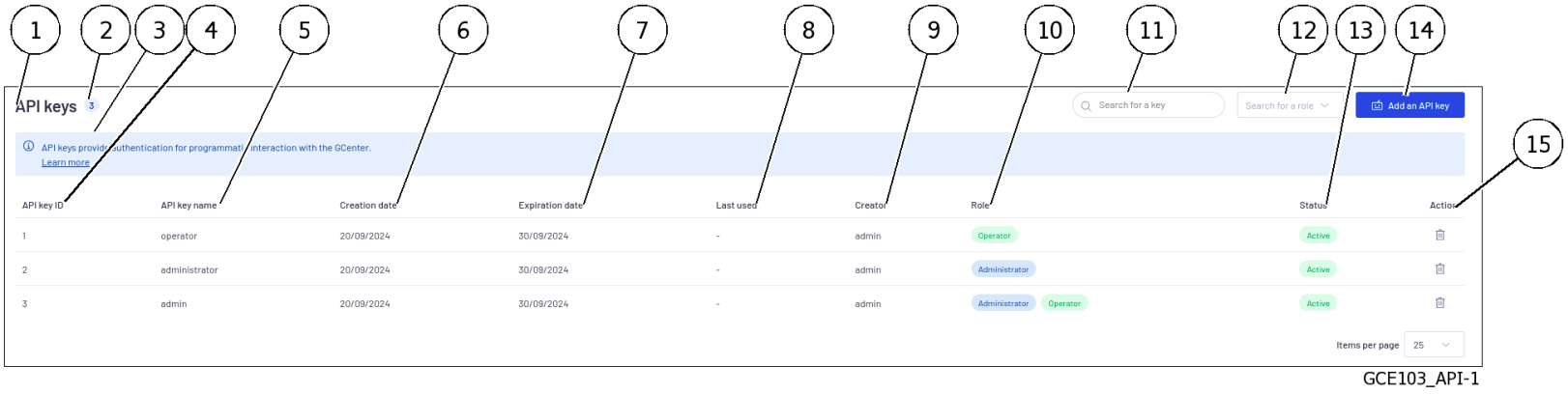
GCE103_API-2

- Enter the name of the API in the `API key name` field (2).
- Select the desired account, hence the rights, using the `Authorized roles` field (3).
- Select the expiration date by clicking on the `Expiration date` field (4): use the calendar displayed.
- Press the `Save changes` button (6).
  After adding:
  - A message that the token was created is displayed
  - The created token is displayed

```
Token generated with success ```LMLqOuFC_bDC1rtHTHCT7aokw3SOMfxxO6KSXTjHXbgl9_IOXVz-I18p34-
↪1i8NY9Grasu_IrpA24JkWhz5UWul12ePiebn_SOaiFhJpjHLD8slMx2aW1hVhiqL92UbDwtJ6uej7wpZ-IM```
 Make sure you save it. You won't be able to access it again.
```

- Use the displayed token.
  The list in `The API Token list` area is updated.

8.7.11.8 Procedure to delete a API key



GCE103_API-1

- If necessary, delete an existing token using the trash button.
  A confirmation window is displayed with the following message.
  `Are you sure you want to delete the key "..." .`
- Press the `Delete` button.

8.7.12 Managing the password policy

8.7.12.1 Introduction

This procedure enables:

- Viewing the current password policy configuration
- Changing the policy

To	Apply the procedures
To enable the password expiration	1 - Apply the *Procedure to access to the `Password policy` window* 2 - Apply the *Procedure to enable the password expiration*
To enable the Password policy	1 - Apply the *Procedure to access to the `Password policy` window* 2 - Apply the *Procedure to enable the Password policy*
To active the Password reuse	1 - Apply the *Procedure to access to the `Password policy` window* 2 - Apply the *Procedure to active the Password reuse*
To active the Anti-bruteforce protection	1 - Apply the *Procedure to access to the `Password policy` window* 2 - Apply the *Procedure to active the Anti-bruteforce protection*

8.7.12.2 Links associated

This graphical interface is described in the *`Password policy` screen*.

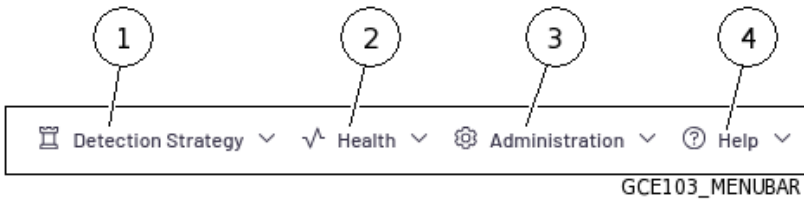
8.7.12.3 Prerequisites

- User: member of **Administrator** group

8.7.12.4 Preliminary operations

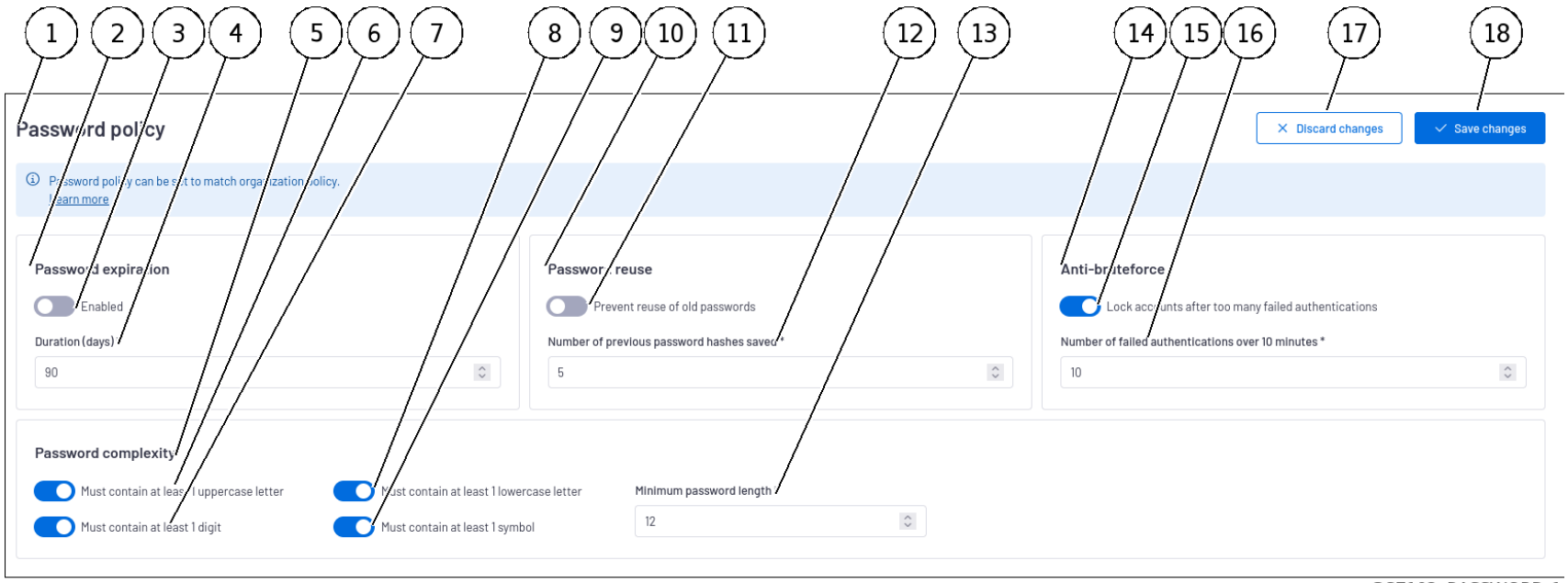
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.7.12.5 Procedure to access to the `Password policy` window



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Password policy` command from the `Authentication` submenu.
  The `Password policy` window is displayed.

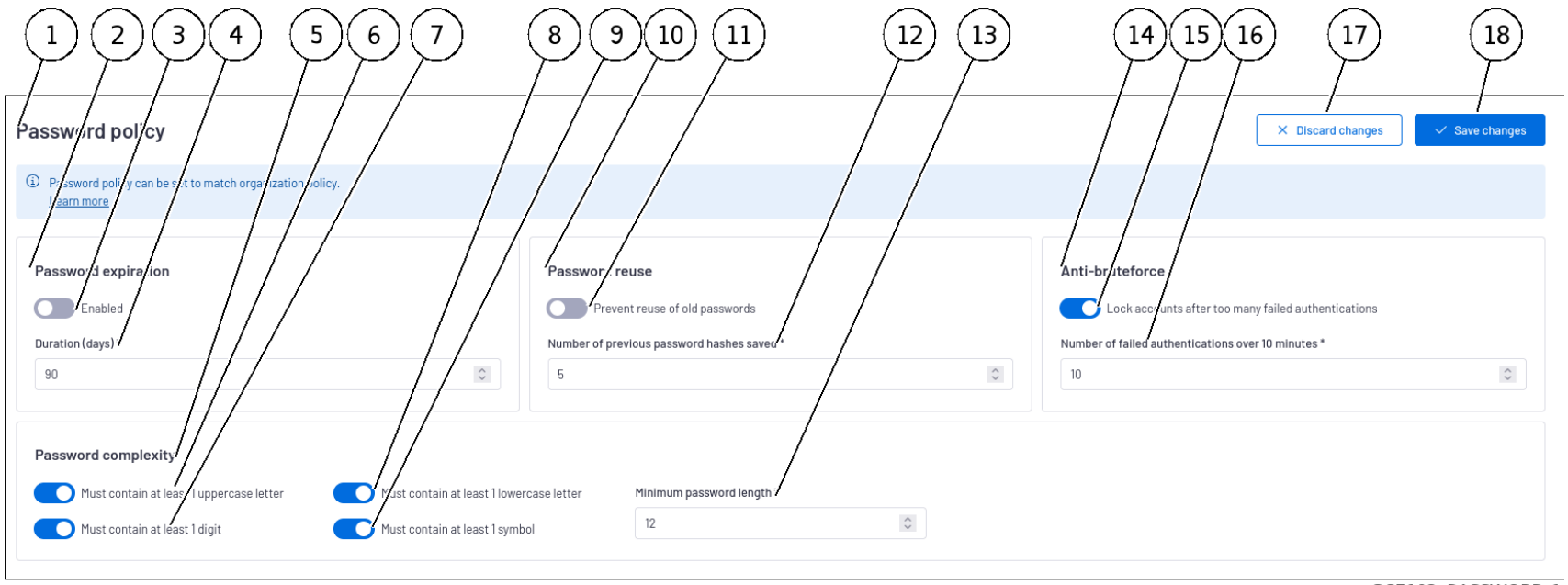
8.7.12.6 Procedure to enable the password expiration



GCE103_PASSWORD-1

- Use the `Enabled` selector (3) of the `Password expiration` zone (2).
- Select the duration of the password validity in the `Duration (days)` field (4).
- Click on the `Save changes` button (18).

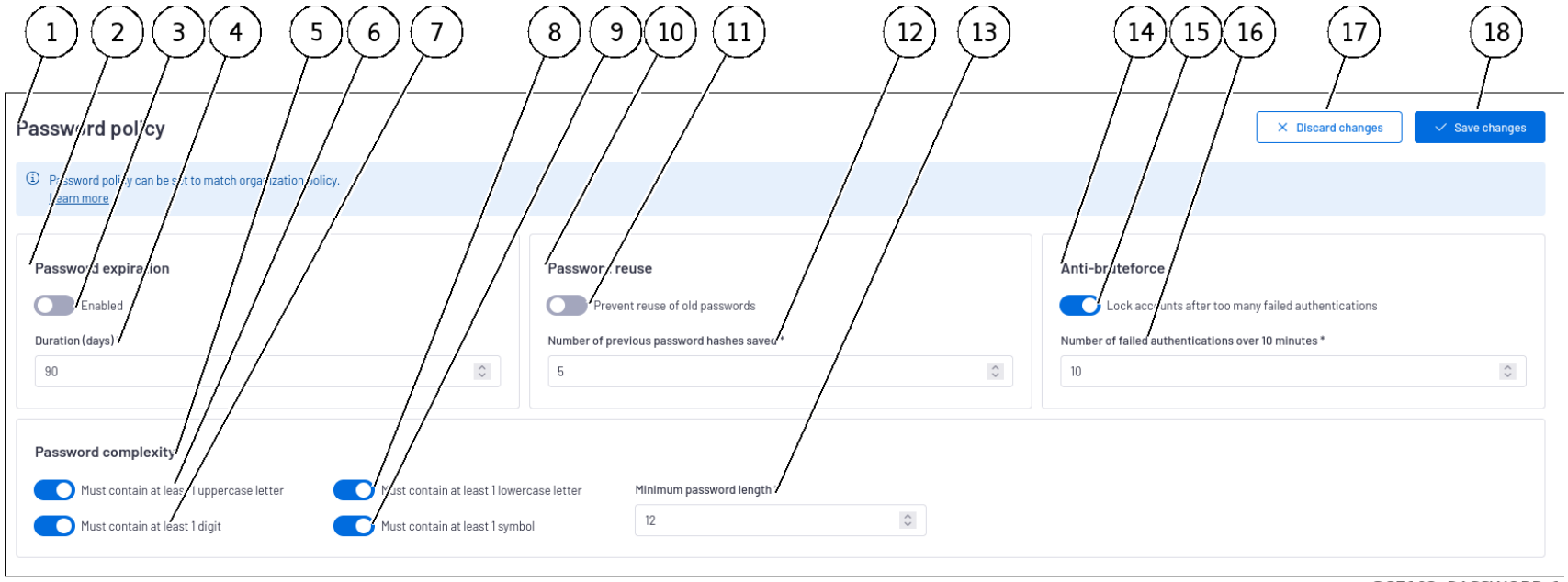
8.7.12.7 Procedure to enable the Password policy



GCE103_PASSWORD-1

- Use the `Require upper case` selector (6) to enable the presence of at least one upper case letter.
- Use the `Require digit` selector (7) to enable the presence of at least one digit (0 to 9).
- Use the `Require lower case` selector (8) to enable the presence of at least one lower case letter.
- Use the `Require symbols` selector (9) to activate the presence of at least one symbol (i.e. neither a number nor a letter).
- Use the `Minimum password length` selector (13) to set the minimum password length.
- Click on the `Save changes` button (18).

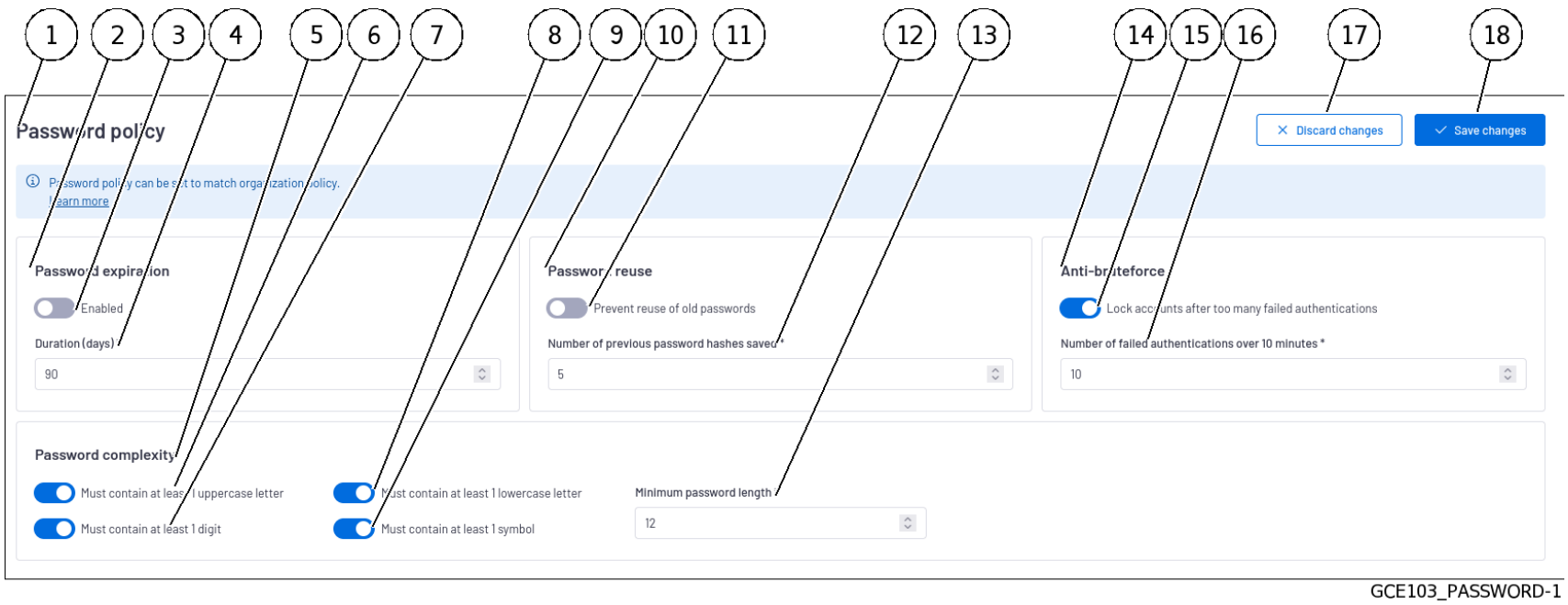
8.7.12.8 Procedure to active the Password reuse



GCE103_PASSWORD-1

- Use the `Prevent reuse of old passwords` selector (11).
- Select the number of previous password hashes saved ie the last passwords cannot be reused in the `Number of previous password hashes saved` field (12).
- Click on the `Save changes` button (18).

8.7.12.9 Procedure to active the Anti-bruteforce protection



GCE103_PASSWORD-1

- Use the `Lock accounts after too many failed authentications` selector (15).
- Select the number of the failed authentications over 10 minutes (after this limit, the account will be locked) in the `Number of failed authentications over 10 minutes` field (16).
- Click on the `Save changes` button (18).

8.8 Configuring the detection engines

8.8.1 Setting up the Malcore engine

8.8.1.1 Introduction

This procedure describes:

- Setting up the analysis expiration delay for an already scanned file
  For this, see the *Procedure to setup the analysis timeout*.
- Setting up the engine
  For this, see *Procedure to change the analysis limits*.

8.8.1.2 Links associated

The engine is described in the *Malcore engine* paragraph.
The graphical interface is described in the *`Malcore` screen*.

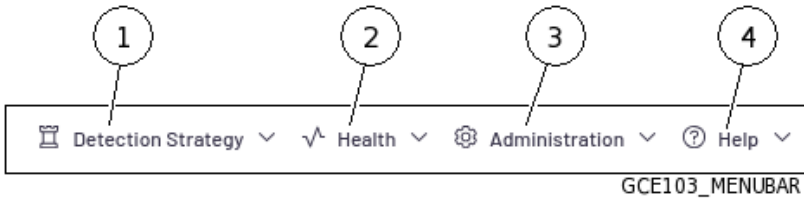
8.8.1.3 Prerequisites

- User: member of **Administrator** group

8.8.1.4 Preliminary operations

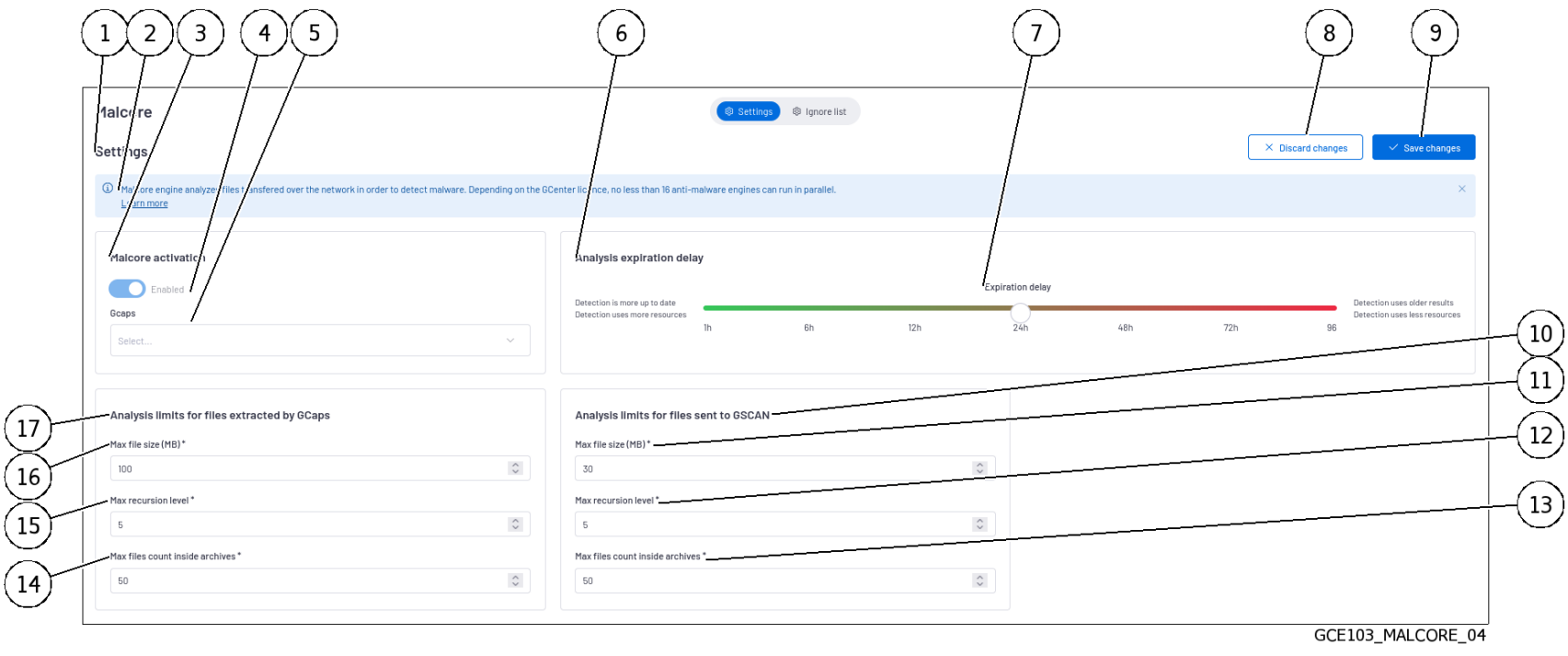
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.8.1.5 Procedure to access the `Malcore` window



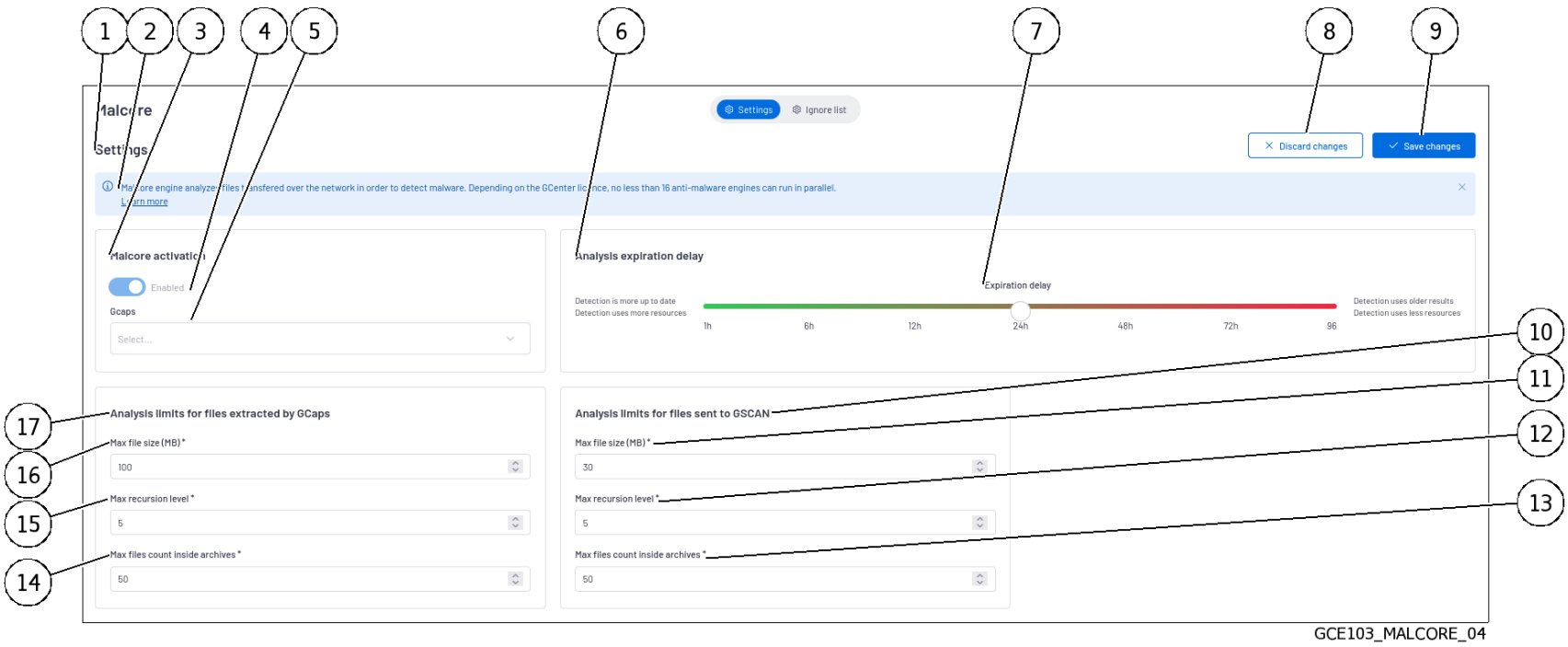
- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `Malcore` command from the `Malware` submenu.
  The `Malcore` window is displayed.
- Click on the `Settings` button to display the `Settings` area.

8.8.1.6 Procedure to setup the analysis timeout



- If necessary, use the cursor `Expiration delay` (7) to set the analysis timeout.
  This parameter sets the time during which Malcore will not re-scan a file already seen on the network.
  If the antivirus engines were updated and the same file reappears, it will be scanned again.
  During the specified time, if a file is seen on the network again, then it is not re-scanned. The result of the first scan is used.
- Confirm the changes using the `Save changes` button (9).
  A confirmation message is displayed: `Updated with success`.

8.8.1.7 Procedure to change the analysis limits



Note:

Increasing the limits can lead to more detection although it has a negative impact on performance.

- Modifying the analysis parameters (17) in terms of flows taken into account by the Malcore engine:
  - If necessary, modify parameter (16): maximum size of files extracted by a GCap (MB)
  - If necessary modify parameter (15): maximum recursion level for archives extracted by GCap
  - If needed, modify parameter (14): maximum number of files for the archives extracted by GCap

Note:

The size of the files extracted by a GCap and the maximum file size taken into account by the Malcore engine may differ.
The maximum file size value on the GCap side must always be smaller than the maximum file size on the Malcore side.

- Modifying the analysis parameters (10) via the GSCan module by the Malcore engine:
- If necessary, modify parameter (11): maximum size of files sent to GScan (MB)
- If necessary, change the parameter (12): maximum recursion level for the archives sent to Gscan
- If necessary, modify the parameter (13): maximum number of archive files sent to Gscan
- Confirm the changes using the `Save changes` button (9).
  A confirmation message is displayed: `Updated with success`.

8.8.2 Managing the Ignore list of the Malcore engine

8.8.2.1 Introduction

The `Ignore list` defines the exception list of files that Malcore must consider healthy.
These files are declared healthy without analysis and defined using:

- Their SHA256 fingerprint (whatever the name)
- The file name

This procedure describes how to populate this list.

To	Apply the procedures
Manage the Ignored files list based on SHA256	1 - Apply the *Procedure to access the `Malcore` window* 2 - Apply the *Procedure to manage the Ignored files list based on SHA256*
Manage the Ignored files list based on filenames	1 - Apply the *Procedure to access the `Malcore` window* 2 - Apply the *Procedure to manage the Ignored files list based on filenames*

8.8.2.2 Links associated

The engine is described in *Malcore engine* paragraph.
The graphical interface is described in the *`Malcore` screen*.

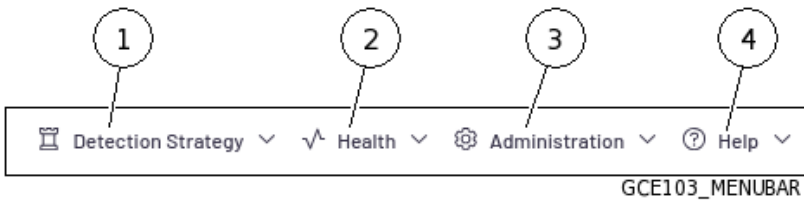
8.8.2.3 Prerequisites

- User: member of **Administrator** group

8.8.2.4 Preliminary operations

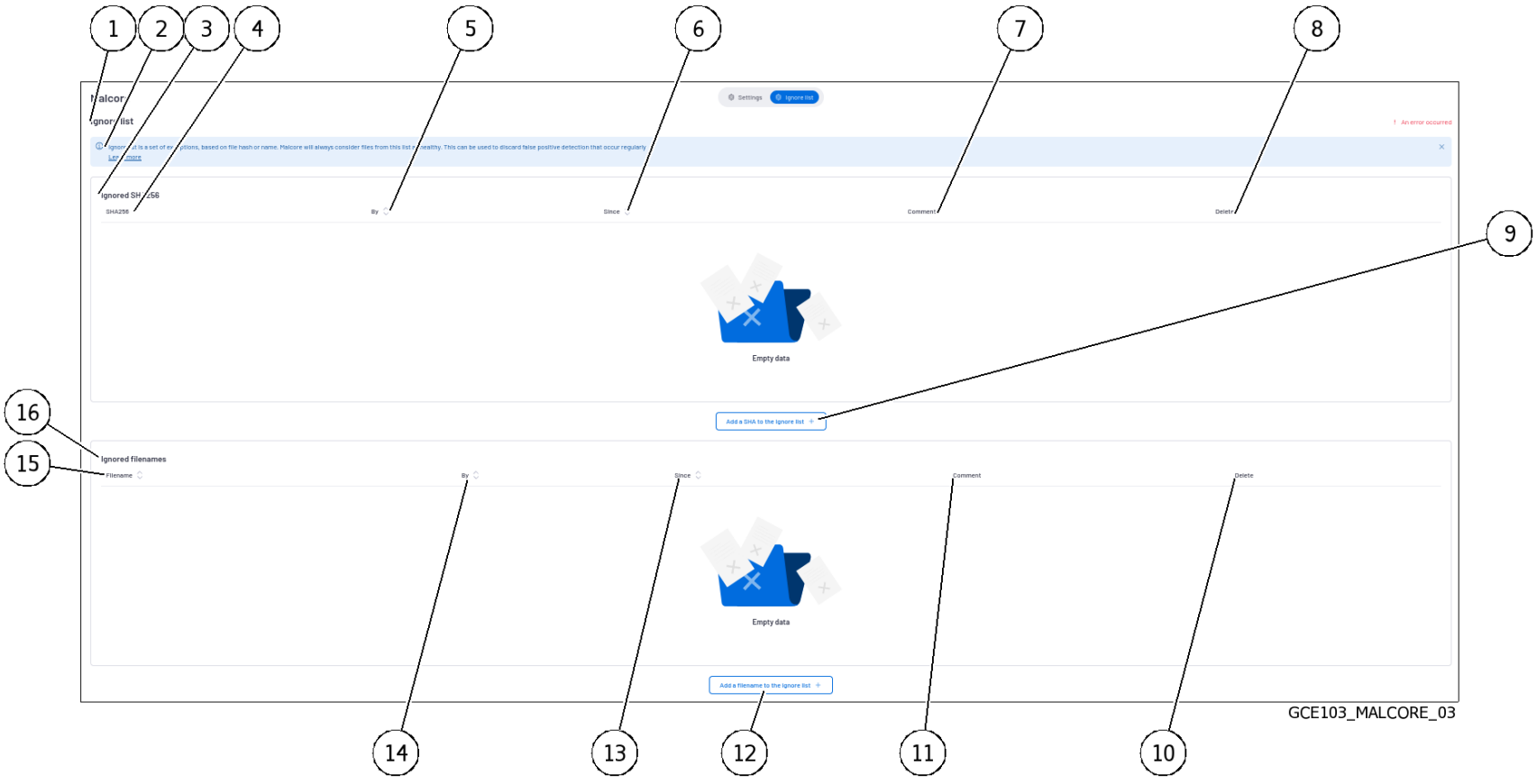
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.8.2.5 Procedure to access the `Malcore` window



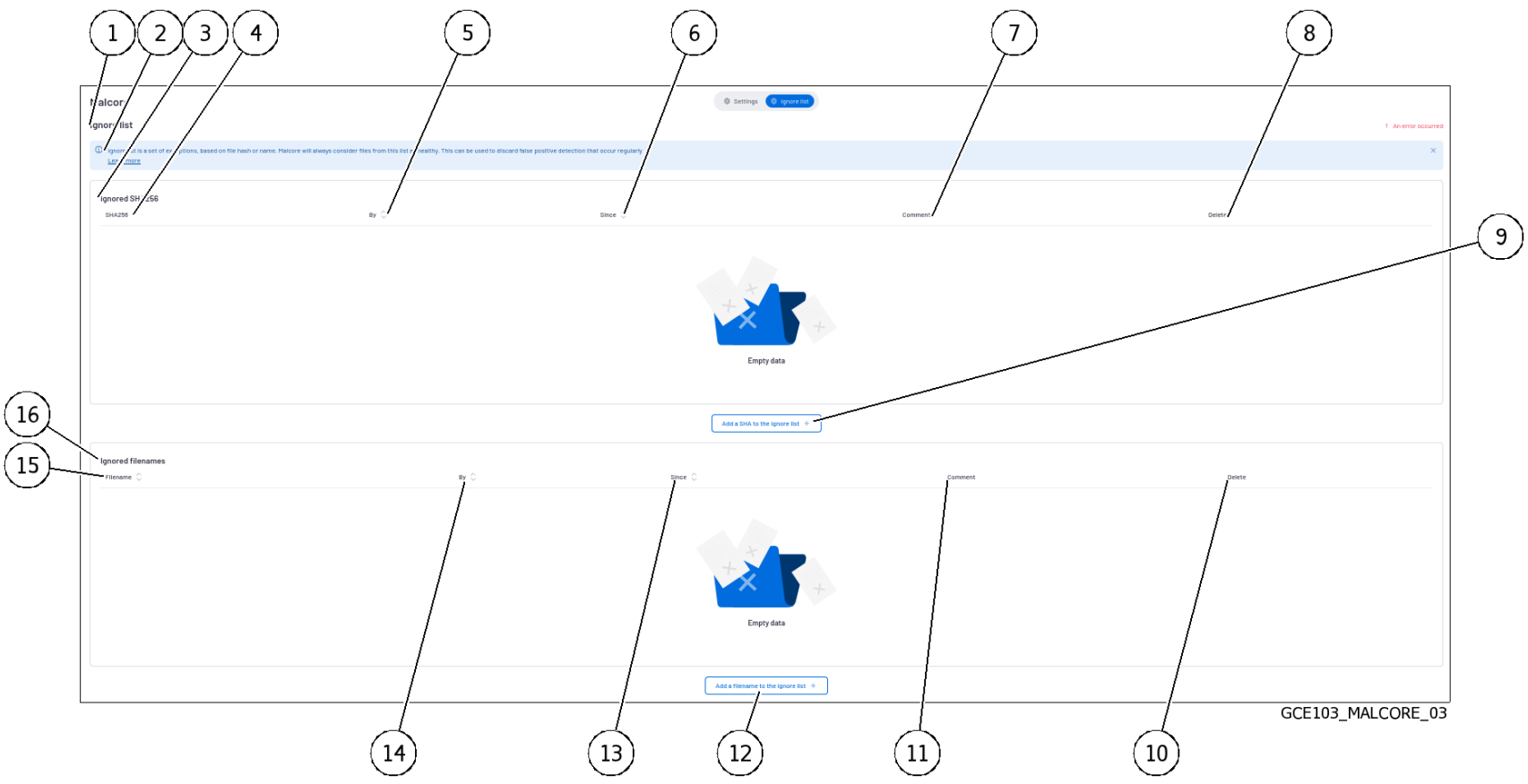
- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `Malcore` command from the `Malware` submenu.
  The `Malcore` window is displayed.
- Click on the `Ignore list` button to display the `Ignored list` area.

8.8.2.6 Procedure to manage the Ignored files list based on SHA256



- To add an item to the `Ignored SHA256` list (3):
- Click on the `Add a SHA to the ignored list` button (9).
  The `Add a SHA to ignore` window is displayed.
- Enter the SHA256 in the `SHA256` field.
- Enter a comment, if any, for further details.
- Click on the `Save` button:
  - If successful, the following message is displayed: `The SHA256 xxxxx was successfully added...`
  - In case of an error, the following message is displayed.
    For example, `The SHA256 was not added to white list. File with SHA256 xxxxx already exists...`

8.8.2.7 Procedure to manage the Ignored files list based on filenames



- To add an item to the `Ignored filenames` list (16):
- Click on the `Add a filename to the ignore list` button (12).

The `Add a filename to ignore` window is displayed.
- Enter the filename.
- Enter a comment, if any, for further details.
- Click on the `Save` button.
  If successful, the following message is displayed: `Your data has been saved..`

8.8.3 Setting up the Malcore retroanalyzer engine

8.8.3.1 Introduction

This procedure describes the enabling / disabling of the engine.

To	Apply the procedures
Enable the engine	1 - Apply the *Procedure to access to the `Malcore retroanalyzer` window* 2 - Apply the *Procedure to enable the engine*
Disable the engine	1 - Apply the *Procedure to access to the `Malcore retroanalyzer` window* 2 - Apply the *Procedure to disable the engine*

8.8.3.2 Links associated

The engine is presented in the *Malcore retroanalyzer engine* paragraph.
The engine activation GUI is described in *`Malcore retroanalyzer` screen*.

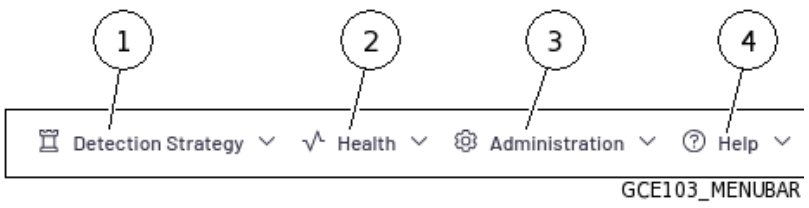
8.8.3.3 Prerequisites

- User: member of **Administrator** group

8.8.3.4 Preliminary operations

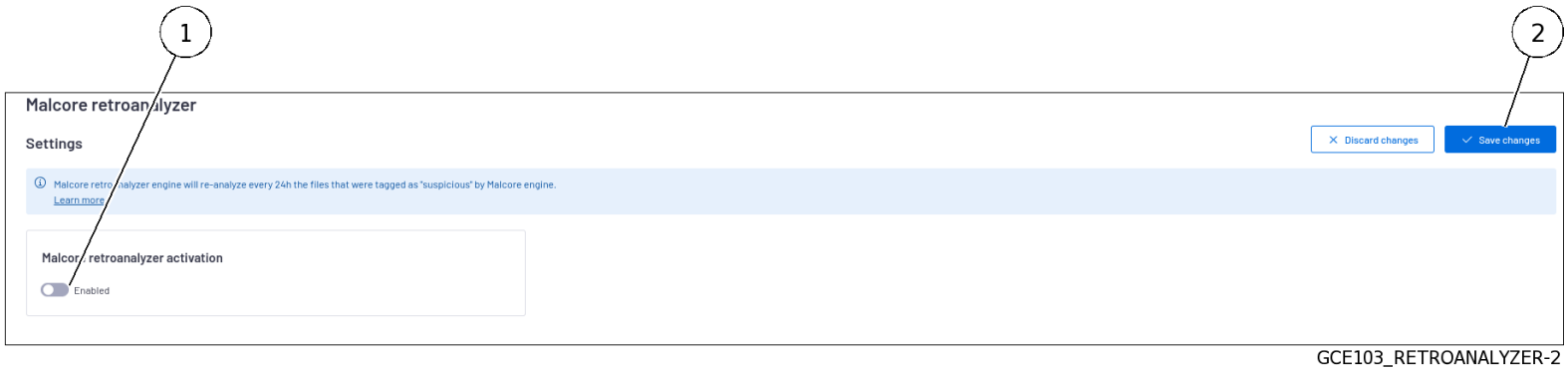
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.8.3.5 Procedure to access to the `Malcore retroanalyzer` window



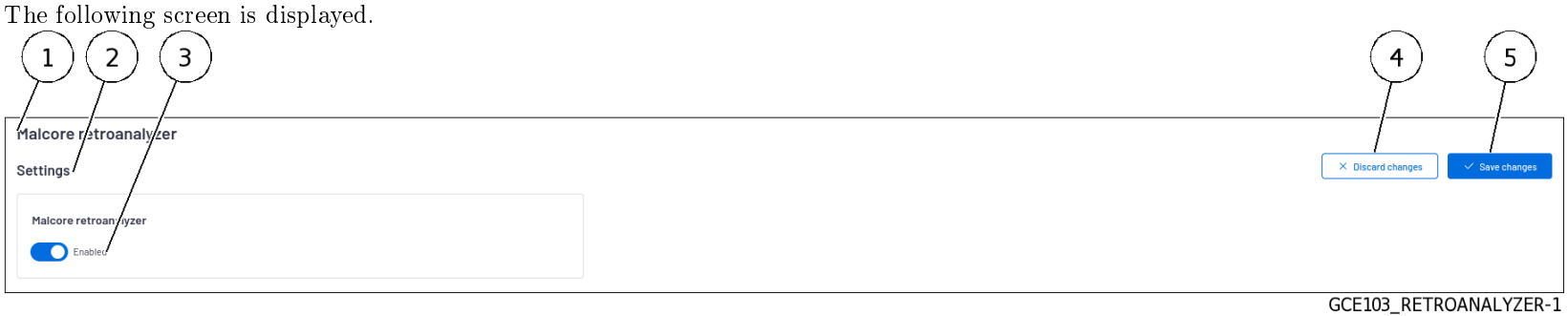
- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `Malcore retroanalyzer` command from the `Malware` submenu.
  The `Malcore retroanalyzer` window is displayed.

8.8.3.6 Procedure to enable the engine



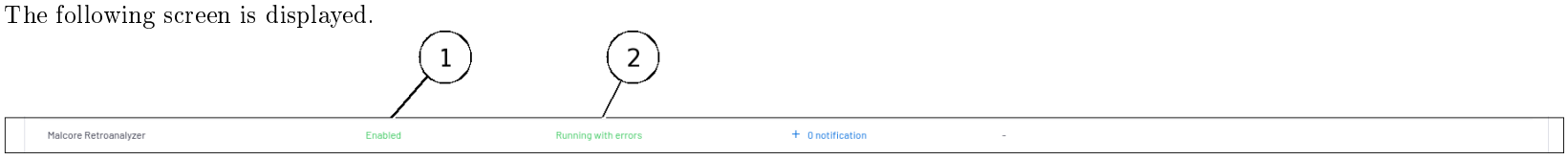
GCE103_RETROANALYZER-2

- Use the `Enabled` selector (1) to enable the engine.
- Click on the `Save changes` button (2).
  The message `Success: Your data has been saved` is displayed.
  The following screen is displayed.



GCE103_RETROANALYZER-1

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.

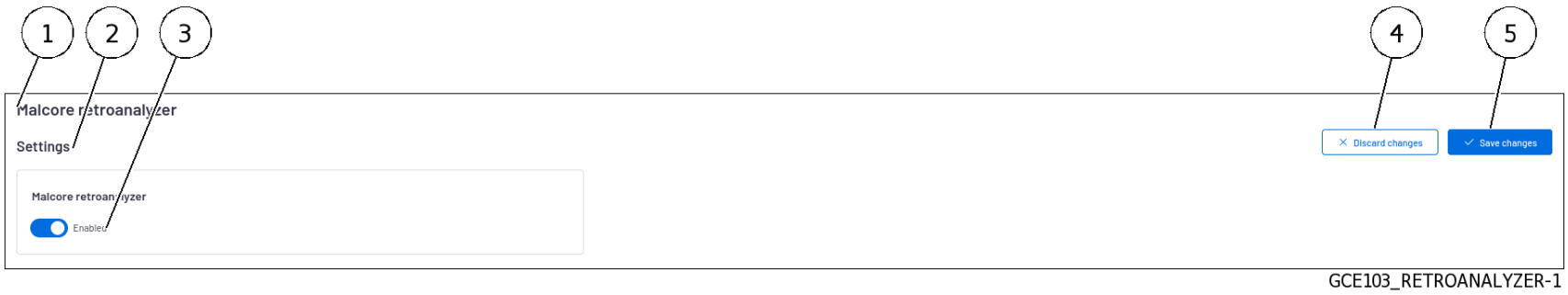


GCE103_RETROANALYZER-3

The screen indicates:

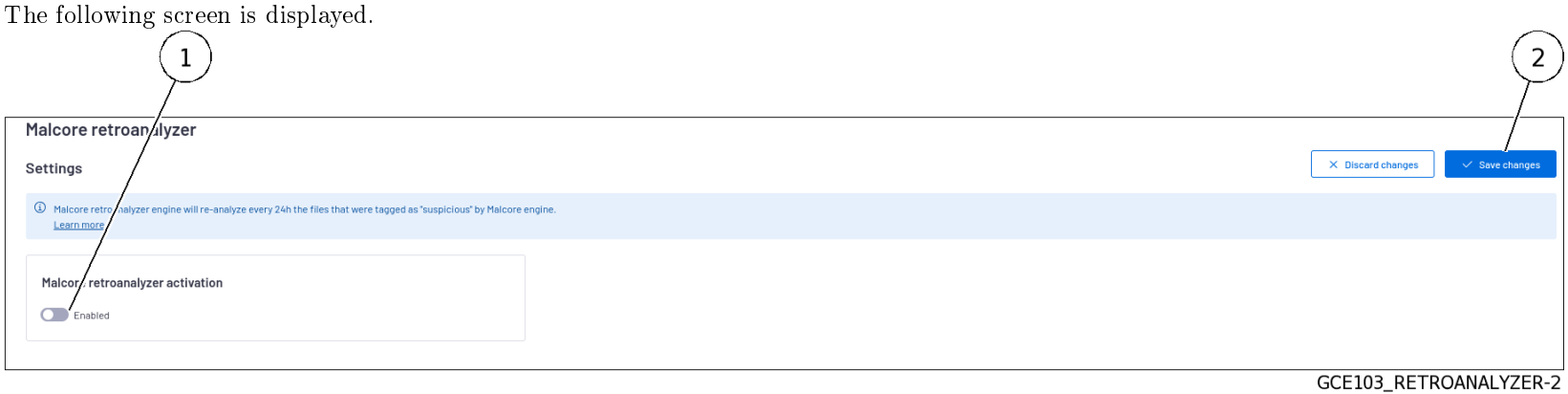
- The status of the engine (1): here `Enabled`
- The state of the engine (2): here `Running`

8.8.3.7 Procedure to disable the engine



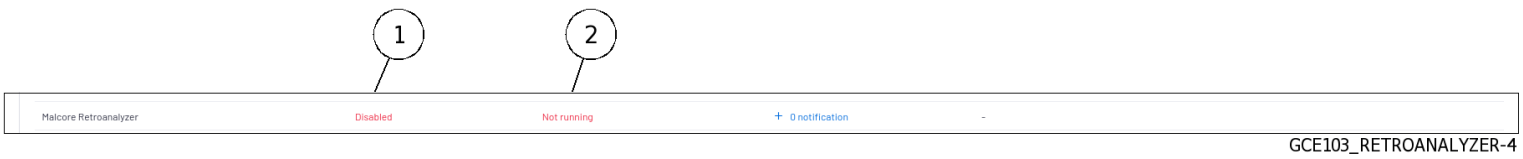
GCE103_RETROANALYZER-1

- Use the `Enabled` selector (3) to disable the engine.
- Click on the `Save changes` button (5).
  The message `Success: Your data has been saved` is displayed.
  The following screen is displayed.



GCE103_RETROANALYZER-2

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.



GCE103_RETROANALYZER-4

The screen indicates:

- The status of the engine (1): `Disabled`
- The state of the engine (2): `Not running`

8.8.4 Setting up the Yara engine

8.8.4.1 Introduction

This procedure describes:

- The enabling / disabling of the engine
- The managing of a ruleset

To	Apply the procedures
Enable the engine	1 - Apply the *Procedure to access the `YARA engine` window* 2 - Apply the *Procedure to enable the engine*
Manage the current ruleset	1 - Apply the *Procedure to access the `YARA engine` window* 2 - Apply the *Procedure to manage the current ruleset*
Disable the engine	1 - Apply the *Procedure to access the `YARA engine` window* 2 - Apply the *Procedure to disable the engine*

8.8.4.2 Links associated

Information about the Yara ruleset:

- it contains the Yara rules
  For further information about the yara rules, see information on https://yara.readthedocs.io/en/stable/writingrules.html
- To validate the rules, it is possible to use the validator (https://yaravalidator.manalyzer.org/)
- The ruleset file has to be named with the extension .yara (example.yara)
- To download an Yara ruleset example, `yara_ruleset_example.yara`

The engine is presented in the *Yara engine* paragraph.
The graphical interface is described in the *`YARA` screen*.

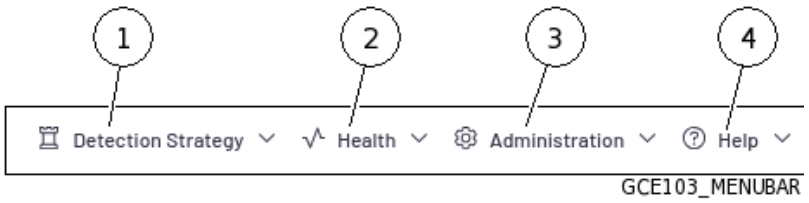
8.8.4.3 Prerequisites

- User: member of **Administrator** group

8.8.4.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

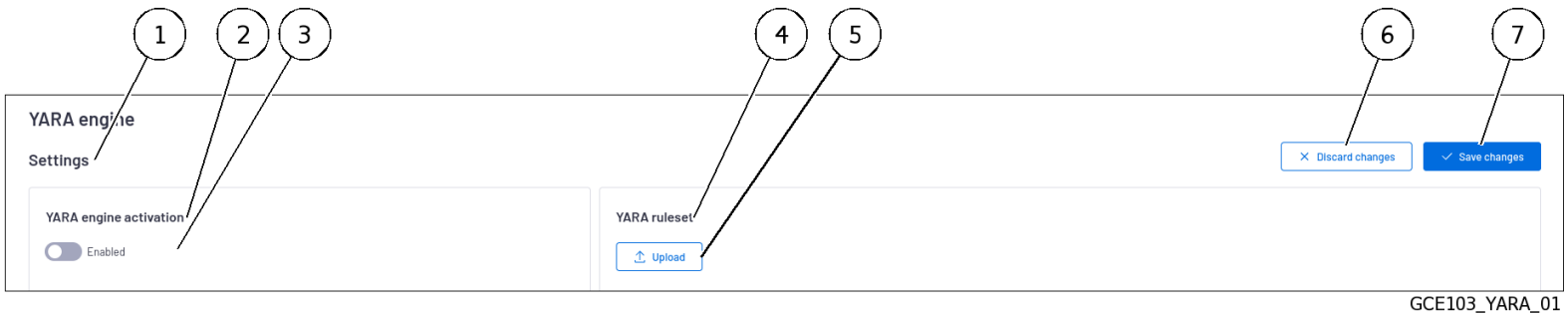
8.8.4.5 Procedure to access the `YARA engine` window



GCE103_MENUBAR

- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `YARA engine` command from the `Malware` submenu.
  The `YARA engine` window is displayed.

8.8.4.6 Procedure to enable the engine



GCE103_YARA_01

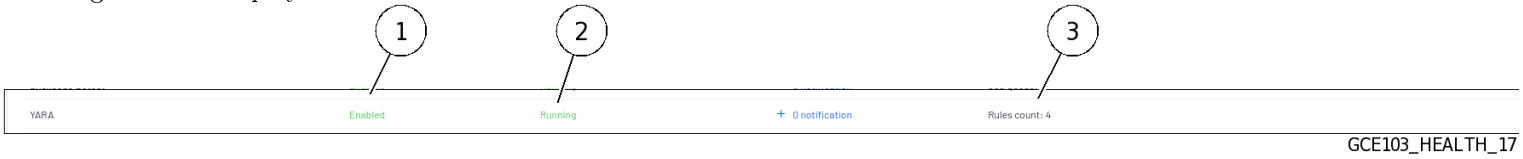
- Use the `Enabled` selector (3) to enable the engine.
- Click on the `Upload` button (5) to upload the ruleset from the local PC.
- From the opened window, select the ruleset.
- Validate.
  The following screen is displayed.

The loaded ruleset is displayed: the file size is displayed.

Important:

Keep a copy of the used yara ruleset file on a secure location.

- Click on the `Save changes` button.
  The message `Success: Your data has been saved` is displayed
  If the message `You must provide a non empty file of rules if Yara engine is enabled` is displayed: no yara file is loaded or this file is empty.
- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.



GCE103_HEALTH_17

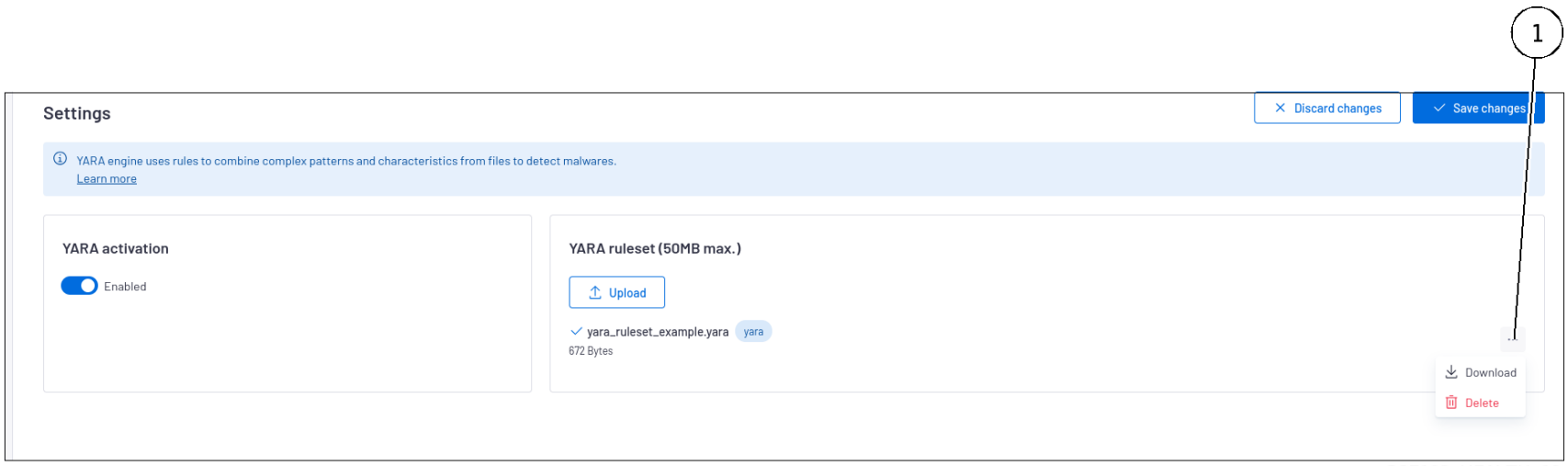
The screen indicates:

- The status of the engine (1): here `Enabled`
- The state of the engine (2): here `Running`

- The Additional information (3): here Rules count 4 indicates the number of rules defined in the ruleset

---

8.8.4.7 Procedure to manage the current ruleset

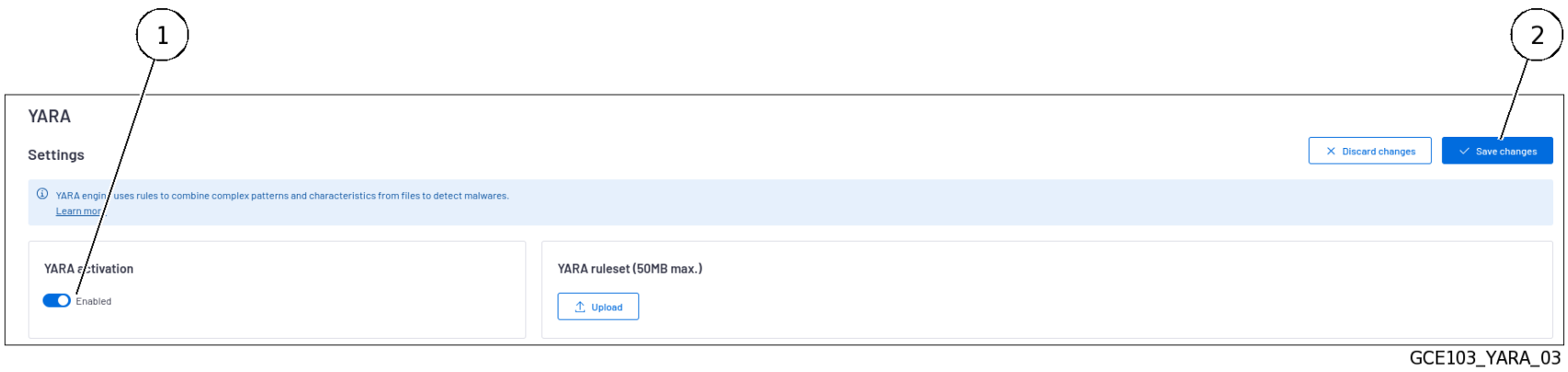


GCE103_HEALTH_18

- Click on the `...` link (1) to display the submenu.
- If needed, use the `Download` command to download the current ruleset from the GCenter to the local PC.
- If needed, use the `Delete` command to delete the current ruleset on the GCenter.

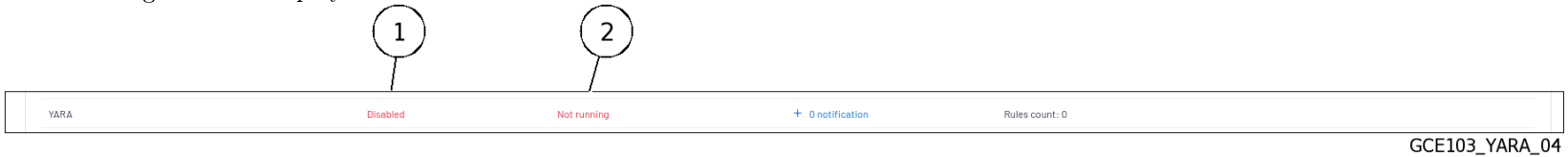
8.8.4.8 Procedure to disable the engine

- Before disable the engine, download the current ruleset (to do so, apply the previous procedure).



GCE103_YARA_03

- Use the `Enabled` selector (1) to disable the engine.
- Click on the `Save changes` button (2).
  The message `Success: Your data has been saved` is displayed.
- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.



GCE103_YARA_04

The screen indicates:

- The status of the engine (1): `Disabled`
- The state of the engine (2): `Not running`
- The Additional information: Rules count: 0 indicates the number of rules defined in the ruleset

---

8.8.5 Setting up the DGA detect engine

8.8.5.1 Introduction

This procedure describes:

- the enabling / disabling of the engine
- the setting of the engine sensitivity

To	Apply the procedures
Enable the engine	1 - Apply the *Procedure to access to the `DGA` window* 2 - Apply the *Procedure to enable the engine*
Set the engine sensitivity	1 - Apply the *Procedure to access to the `DGA` window* 2 - Apply the *Procedure to set the engine sensitivity*
Disable the engine	1 - Apply the *Procedure to access to the `DGA` window* 2 - Apply the *Procedure to disable the engine*

8.8.5.2 Links associated

The engine is presented in the *DGA detect engine* paragraph.
The graphical interface is described in the *`DGA detect` screen (DGA command)*.

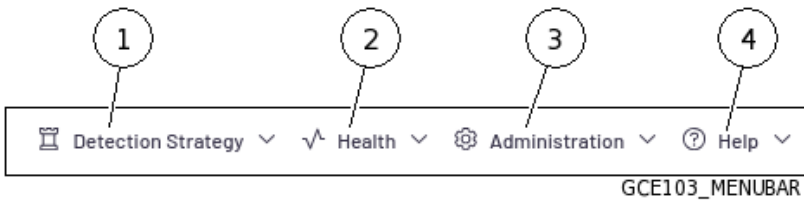
8.8.5.3 Prerequisites

- User: member of **Administrator** group

8.8.5.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

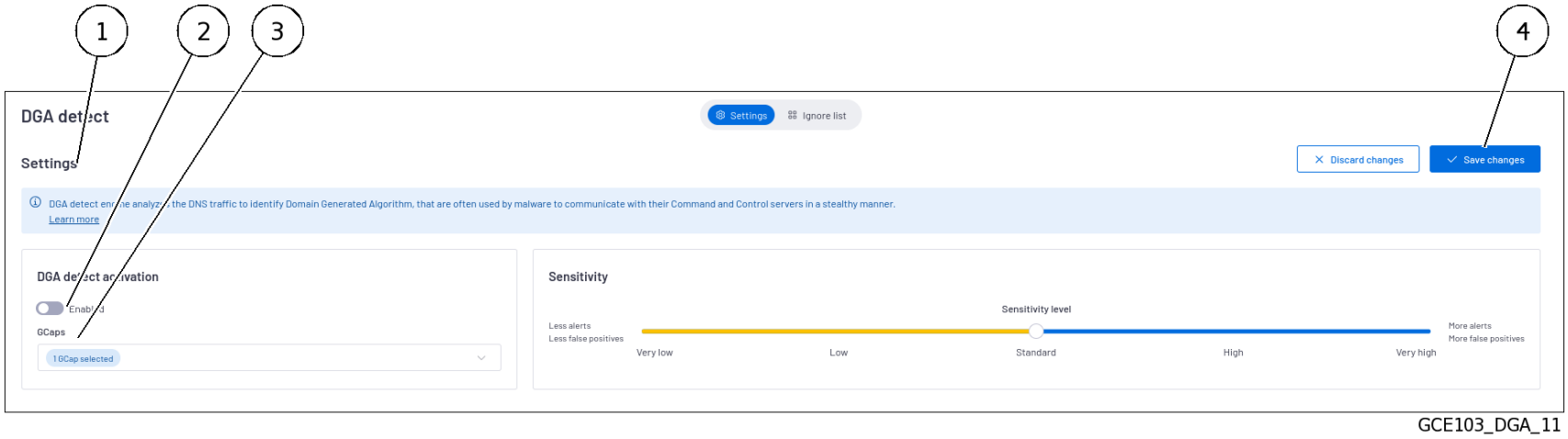
8.8.5.5 Procedure to access to the `DGA` window



- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `DGA` command from the `C&C` submenu.
  The `DGA` window is displayed.

8.8.5.6 Procedure to enable the engine

- Click on the `Settings` section.
  The `Settings` window (1) displays the option to enable/disable the engine.



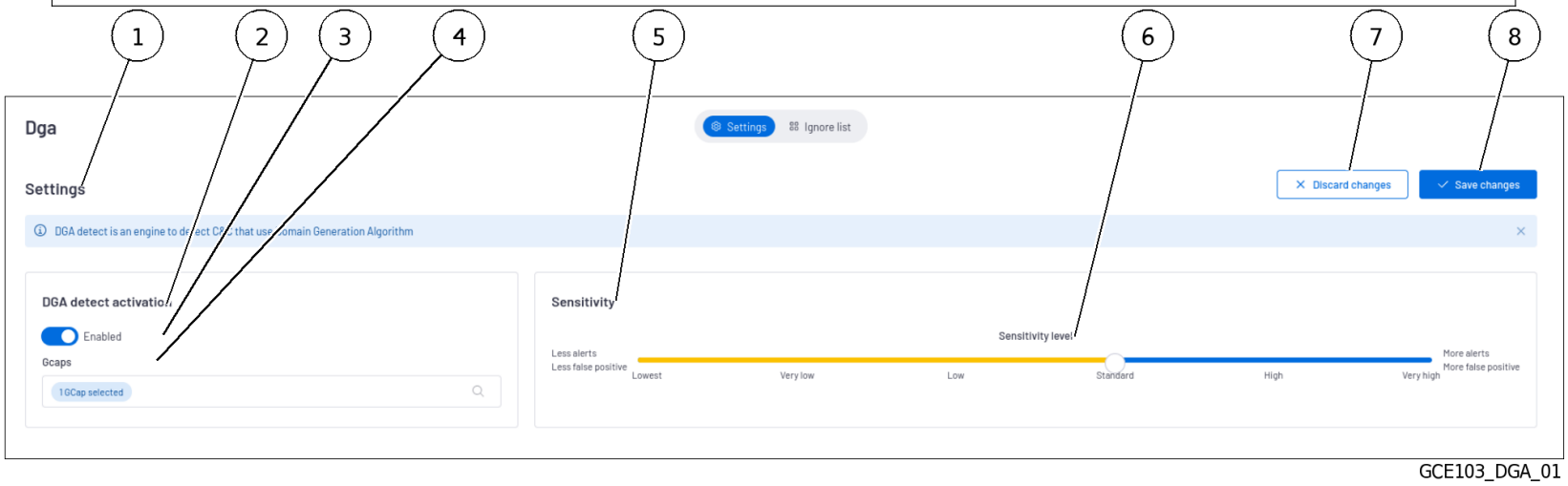
GCE103_DGA_11

- Use the `Enabled` selector (2) to enable the engine.

> **Note:**
> This feature is disabled by default.

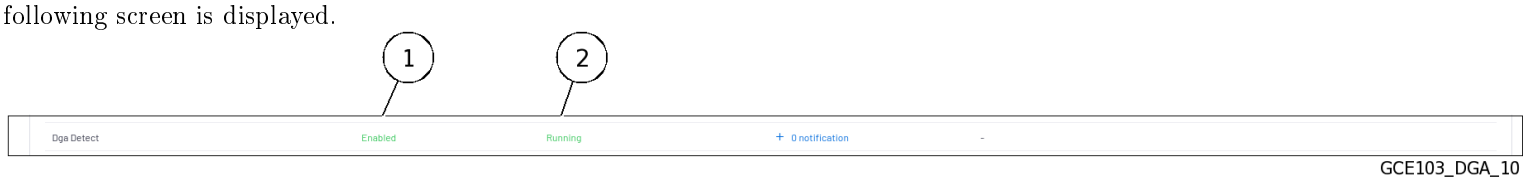
- Click on the `Gcaps` field (3).
  The list of the Gcaps connected to the GCenter is displayed.
- Click on each GCap to select or unselect this GCap.
  The selection is visible using the check mark.
  To enable the engine of a GCap, it must have a check mark on this GCap.
  After each action, the number of GCap selected is displayed (only the engine of the GCap selected is enabled).
- Click on the `Save changes` button (4).
  The following message is displayed.

```
Success
Your settings have been successfully saved.
```



GCE103_DGA_01

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.



GCE103_DGA_10

  The screen indicates:

  - The status of the engine (1): here `Enabled`
  - The state of the engine (2): here `Running`

8.8.5.7 Procedure to set the engine sensitivity

GCE103_DGA_01

- In the `Sensitivity` area (5), move the slider to set the Sensitivity level (6).
  The Sensitivity levels are explained in the *How does this DGA detect engine work in the GCenter?* paragraph.
- Click on the `Save changes` button (8).

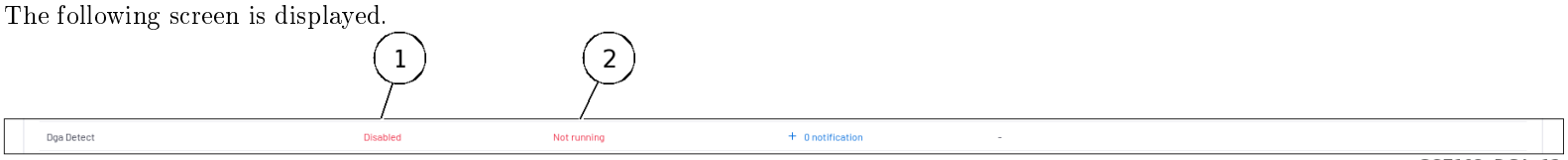
8.8.5.8 Procedure to disable the engine

- Click on the `Settings` section.

GCE103_DGA_01

The `Settings` window (1) displays the option to enable/disable the engine.

- To disable the GDA detect engine of a specific GCap:
  - Click on the `Gcaps` field (4).
    The list of the Gcaps connected to the GCenter is displayed.
  - Click on each GCap to select or unselect this GCap.
    The selection is visible with the checkbox.
    To disable the engine of a GCap, it must not have a check mark on this GCap.
    After each action, the number of GCap selected is displayed (only the engine of the GCap selected is enabled).
  - Click on the `Save changes` button (8).
    The message `Success: Your settings have been successfully saved.` is displayed.
- To disable the GDA detect engine of all GCaps:
  - Use the `Enabled` selector (2) to disable the engine.
  - Click on the `Save changes` button (8).
    The message `Success: Your settings have been successfully saved.` is displayed.
  - Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
    The following screen is displayed.



GCE103_DGA_12

The screen indicates:

- The status of the engine (1): `Disabled`
- The state of the engine (2): `Not running`

8.8.6 Managing the Ignore list of the DGA detect engine

8.8.6.1 Introduction

The `Ignore list` defines the exception list of domain names that DGA detect engine must consider healthy.
This removes alerts related to recurring false positives.
This procedure describes how to populate this list.

To	Apply the procedures
To add an item to the `Ignore list`	1 - Apply the *Procedure to access to the `Domain Name Generation (DGA) Detection Management` window* 2 - Apply the *Procedure to add an item to the `Ignore list`*
To delete an item to the `Ignore list`	1 - Apply the *Procedure to access to the `Domain Name Generation (DGA) Detection Management` window* 2 - Apply the *Procedure to delete an item to the `Ignore list`*

8.8.6.2 Links associated

The engine is presented in the *DGA detect engine* paragraph.
The graphical interface is described in the *`DGA detect` screen (DGA command)*.

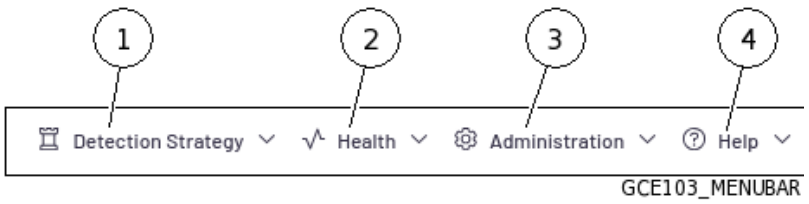
8.8.6.3 Prerequisites

- User: member of **Administrator** group

8.8.6.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.8.6.5 Procedure to access to the `Domain Name Generation (DGA) Detection Management` window

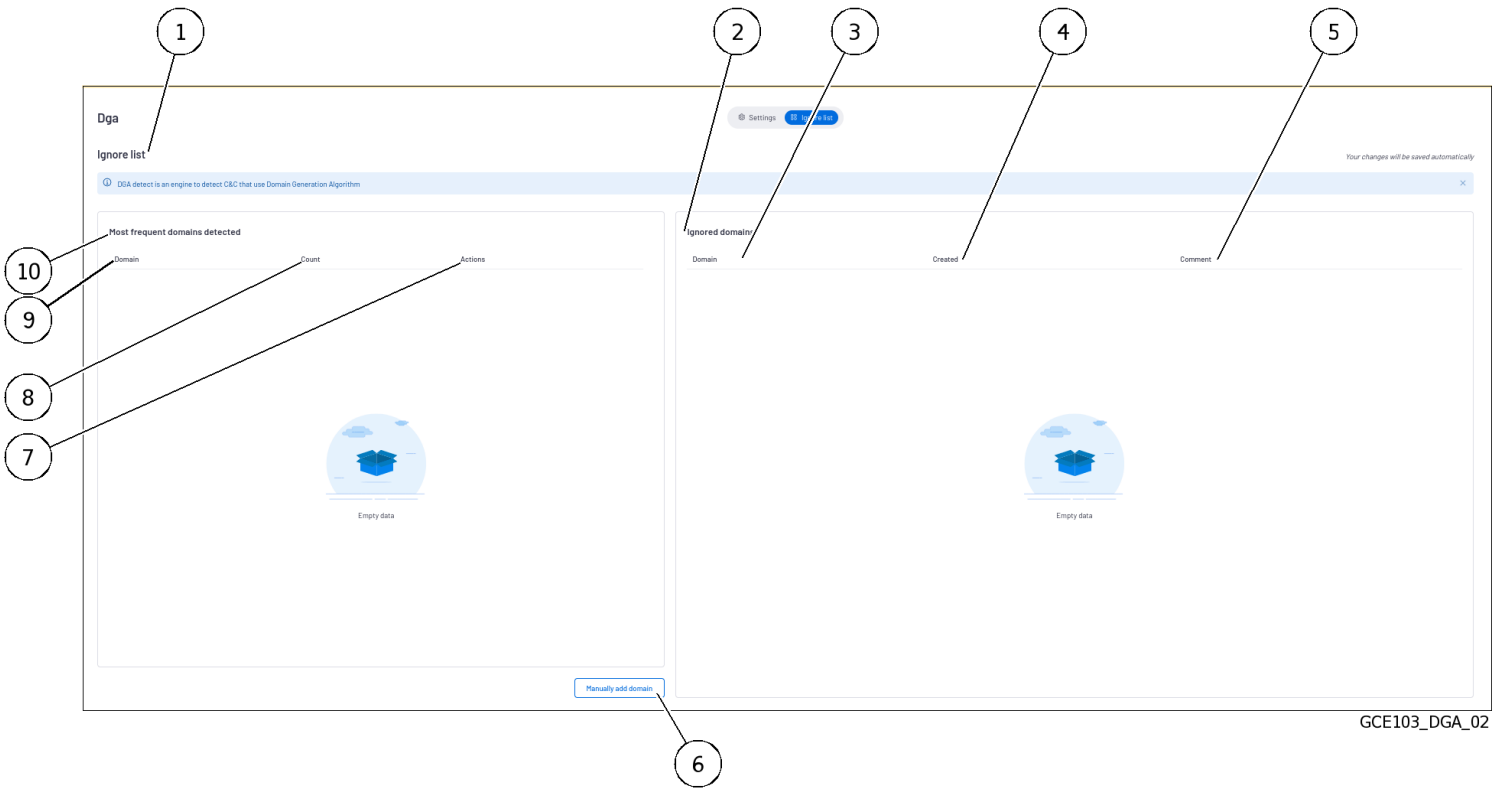


- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `DGA` command from the `C&C` submenu.
  The `DGA` window is displayed.

8.8.6.6 Procedure to add an item to the `Ignore list`

GCE103_DGA_01

- Click on the `Ignore list` section.
  The `Ignore list` window is displayed.



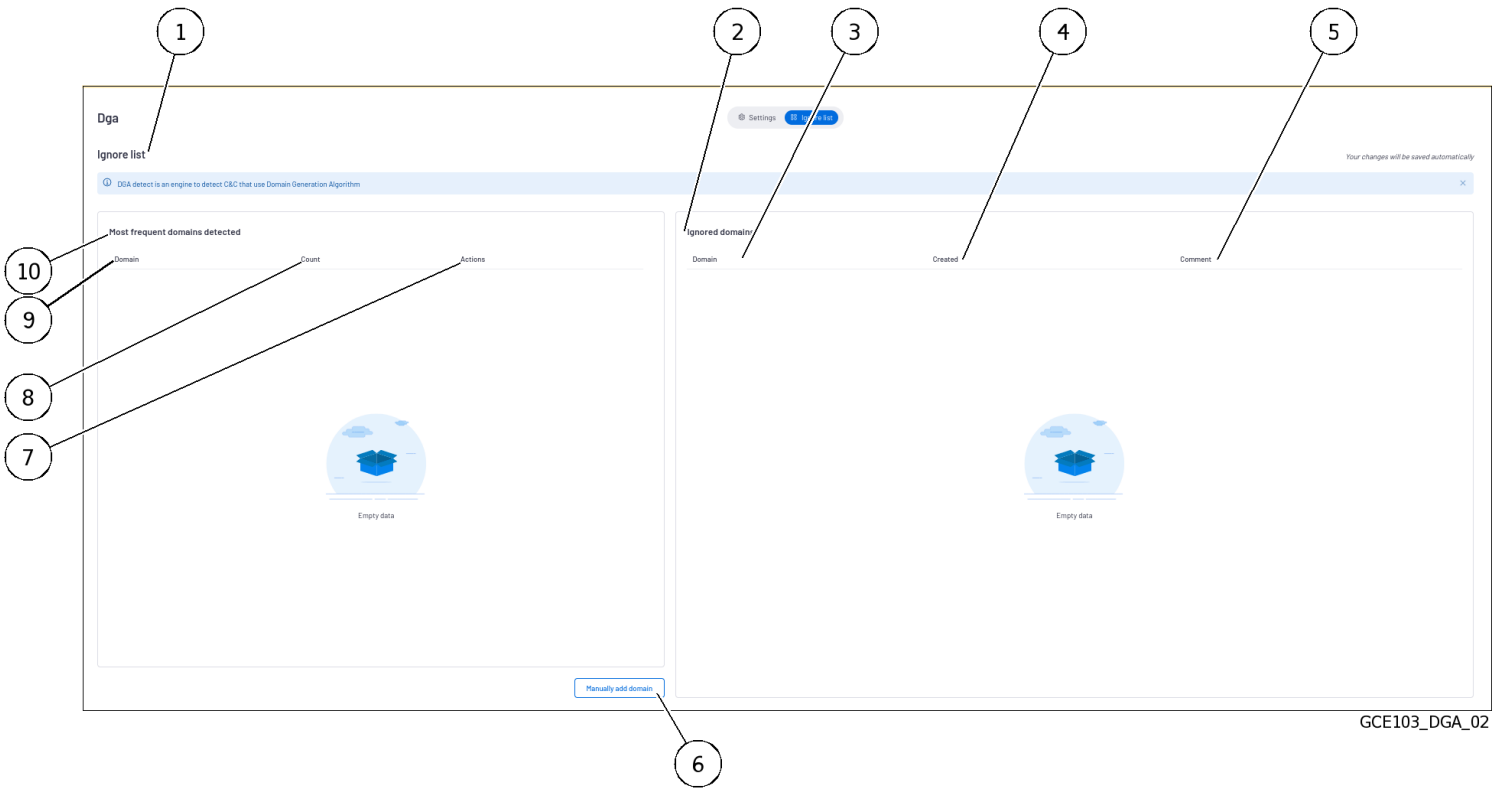
GCE103_DGA_02

- Click on the `Manually add domain` button (6).
  The `Add a domain to ignore` window is displayed.
- Enter the domain name.
- Click on the `Save` button.
  If successful, the following message is displayed: `Your data has been saved`.
  In case of errors, a message is displayed.
  For example, `The domain name was not added to white list. xxx already exists in white list`

8.8.6.7 Procedure to delete an item to the `Ignore list`

GCE103_DGA_01

- Click on the `Ignore list` section.
  The `Ignore list` window is displayed.



GCE103_DGA_02

- Click on the trash of the row to be deleted from the list (2).
  The following message is displayed: `Domain successfully deleted`.

8.8.7 Setting up the Malicious Powershell detect engine

8.8.7.1 Introduction

This procedure describes the enabling / disabling of the engine.

To	Apply the procedures
Enable the engine	1 - Apply the *Procedure to access the `Malicious Powershell detect` window* 2 - Apply the *Procedure to enable the engine*
Disable the engine	1 - Apply the *Procedure to access the `Malicious Powershell detect` window* 2 - Apply the *Procedure to disable the engine*

8.8.7.2 Links associated

The engine is presented in the *Malicious Powershell detect engine* paragraph.
The graphical interface is described in the *`Malicious Powershell detect` screen (Malicious Powershell command)*.

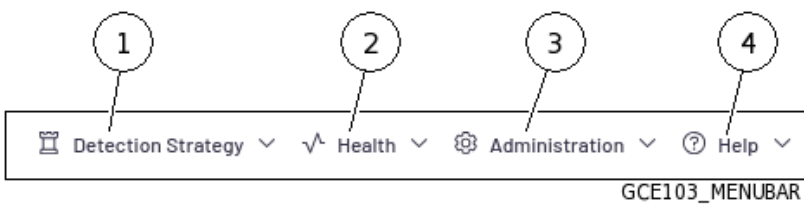
8.8.7.3 Prerequisites

- User: member of **Administrator** group

8.8.7.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

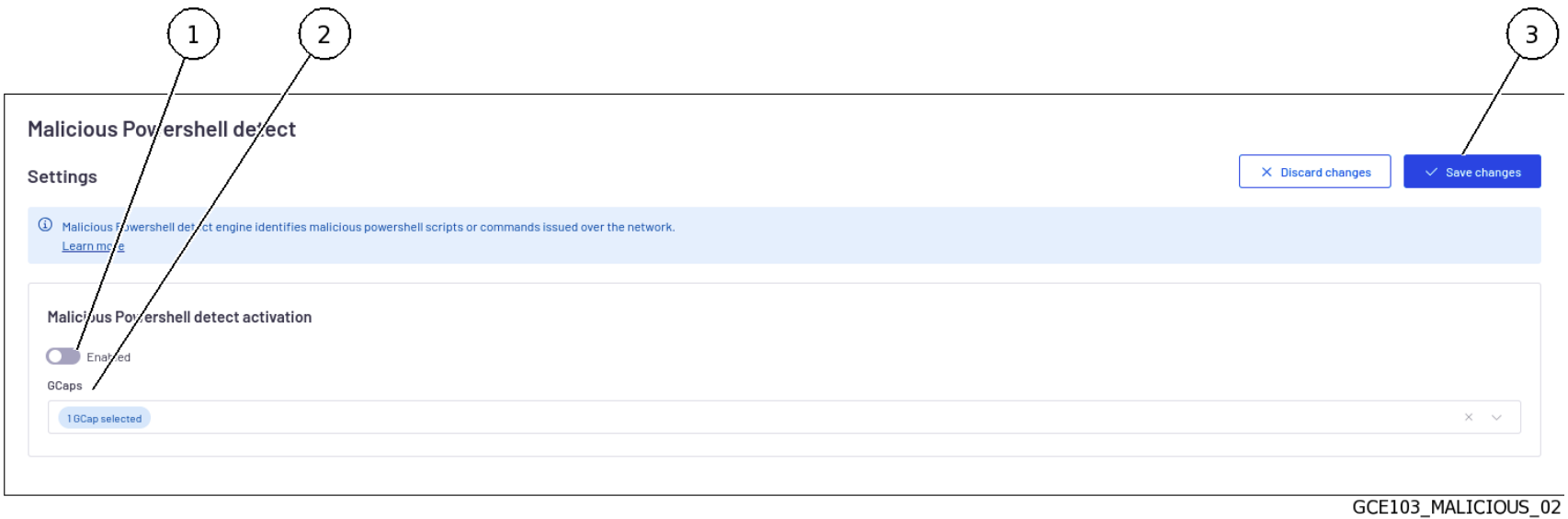
8.8.7.5 Procedure to access the `Malicious Powershell detect` window



GCE103_MENUBAR

- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `Malicious Powershell` command from the `Malware` submenu.
  The `Malicious Powershell detect` window is displayed.

8.8.7.6 Procedure to enable the engine

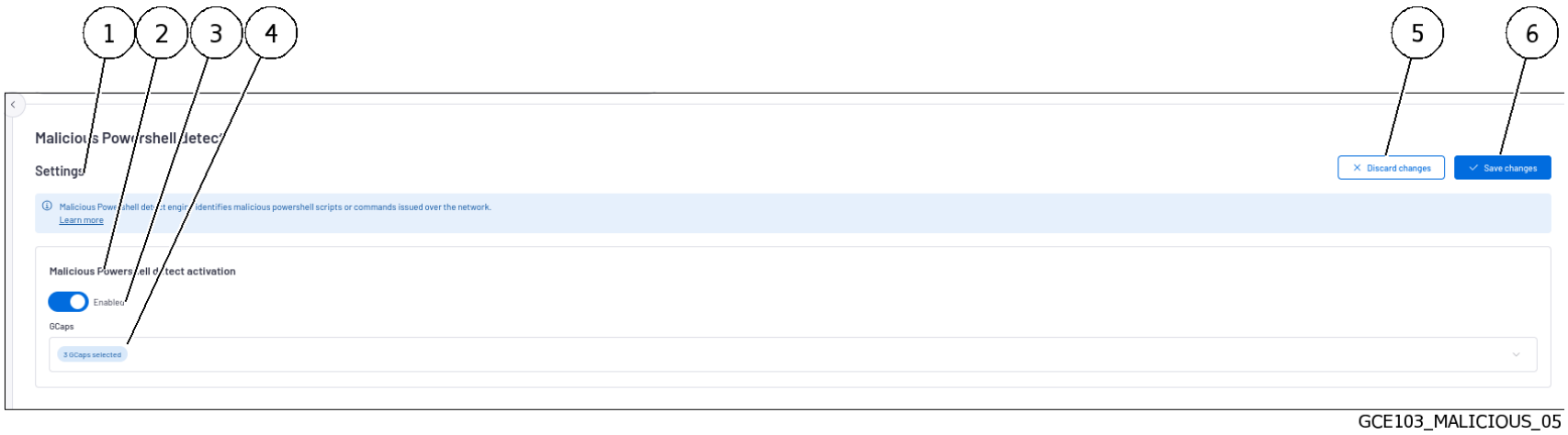


GCE103_MALICIOUS_02

- Use the `Enabled` selector (1) to enable the engine.
- Select the GCap (2) where the engine has to be activated.
- Click on the `Save changes` button (3).
  The following message is displayed.

```
Apply changes

 Enabling or disabling an engine on a GCap will cause it to restart.
 Are you sure you want to apply these configuration changes now?
```

- Click on the `Apply` button.
  The message `Success:  Your data has been saved` is displayed
  The following screen is displayed.



GCE103_MALICIOUS_05

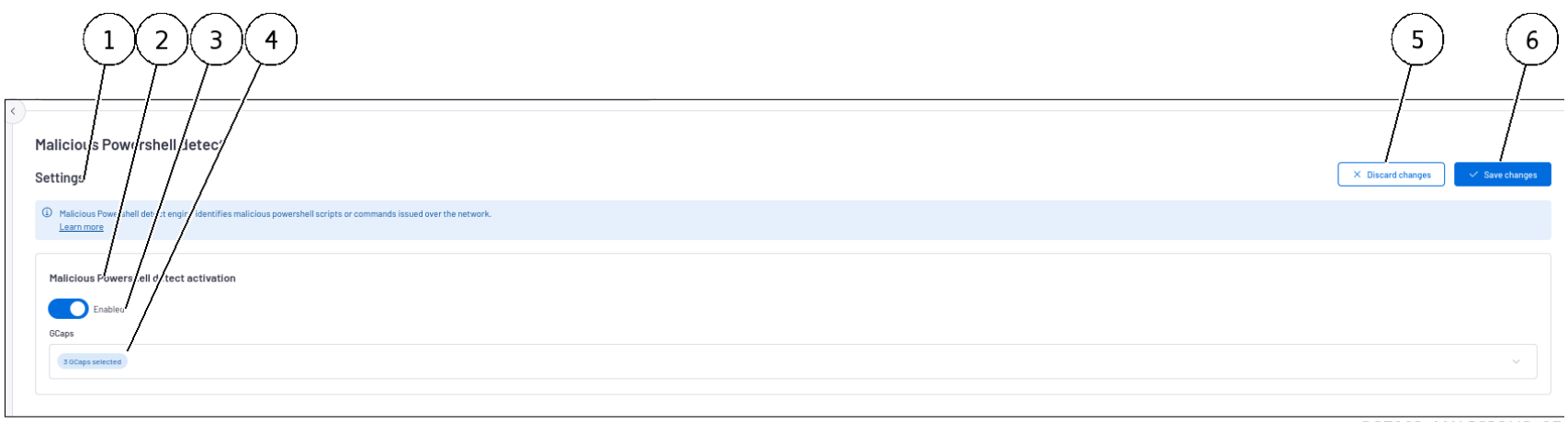
- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.

GCE103_MALICIOUS_03

  The screen indicates:

  - The status of the engine (1): here `Enabled`
  - The state of the engine (2): here `Running`

8.8.7.7 Procedure to disable the engine

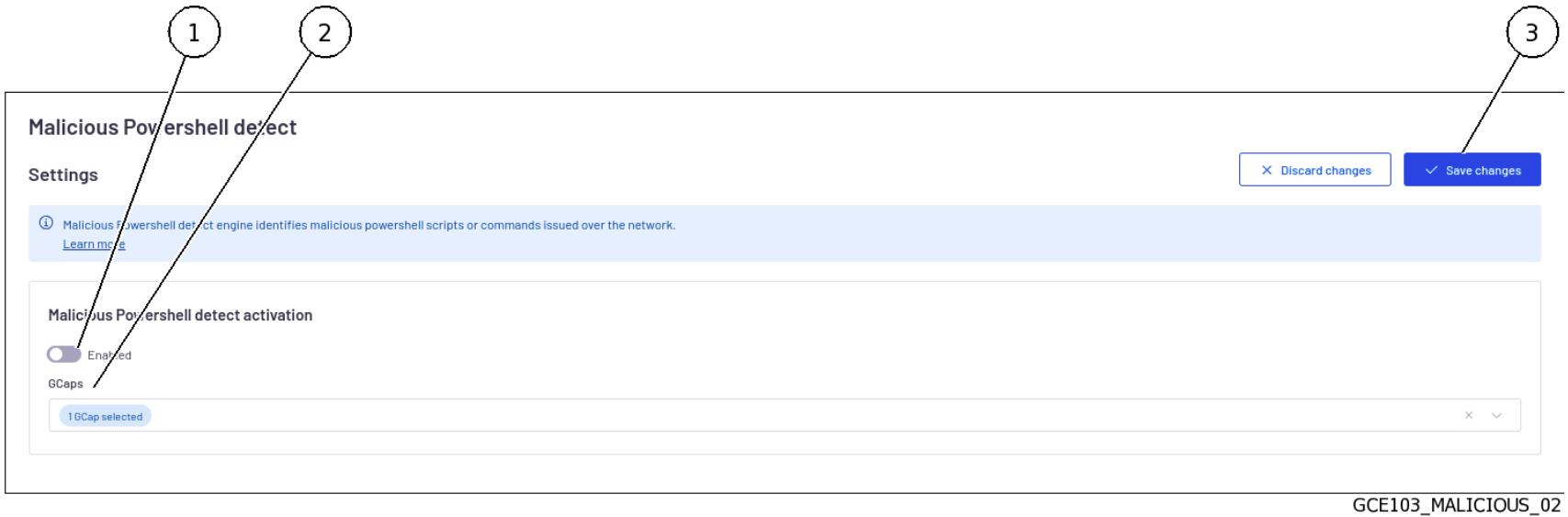


GCE103_MALICIOUS_05

- Use the `Enabled` selector (3) to disable the engine.
- Click on the `Save changes` button (6).
  The following message is displayed.

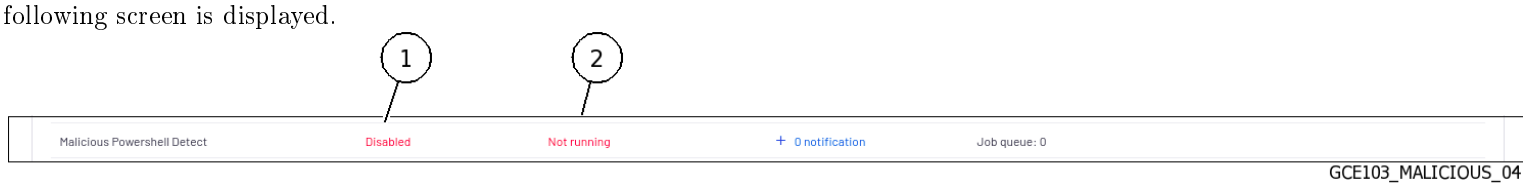
```
Apply changes

Enabling or disabling an engine on a GCap will cause it to restart.
Are you sure you want to apply these configuration changes now?
```

- Click on the `Apply` button.
  The message `Success:  Your data has been saved` is displayed
  The following screen is displayed.



GCE103_MALICIOUS_02

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.



GCE103_MALICIOUS_04

  The screen indicates:

  - The status of the engine (1): `Disabled`
  - The state of the engine (2): `Not running`

8.8.8 Setting up the Shellcode detect engine

8.8.8.1 Introduction

This procedure describes the enabling / disabling of the engine.

To	Apply the procedures
Enable the engine	1 - Apply the *Procedure to access the `Shellcode detect` window* 2 - Apply the *Procedure to enable the engine*
Disable the engine	1 - Apply the *Procedure to access the `Shellcode detect` window* 2 - Apply the *Procedure to disable the engine*

8.8.8.2 Links associated

The engine is presented in the *Shellcode detect engine* paragraph.
The graphical interface is described in *`Shellcode detect` screen (Shellcode command)*.

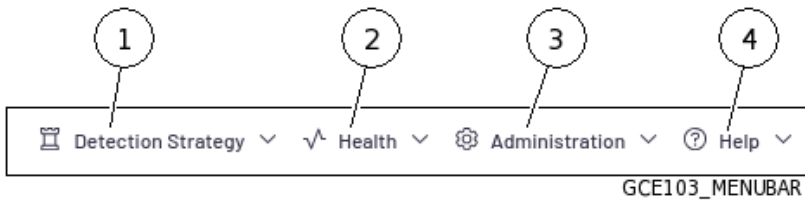
8.8.8.3 Prerequisites

- User: member of **Administrator** group

8.8.8.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

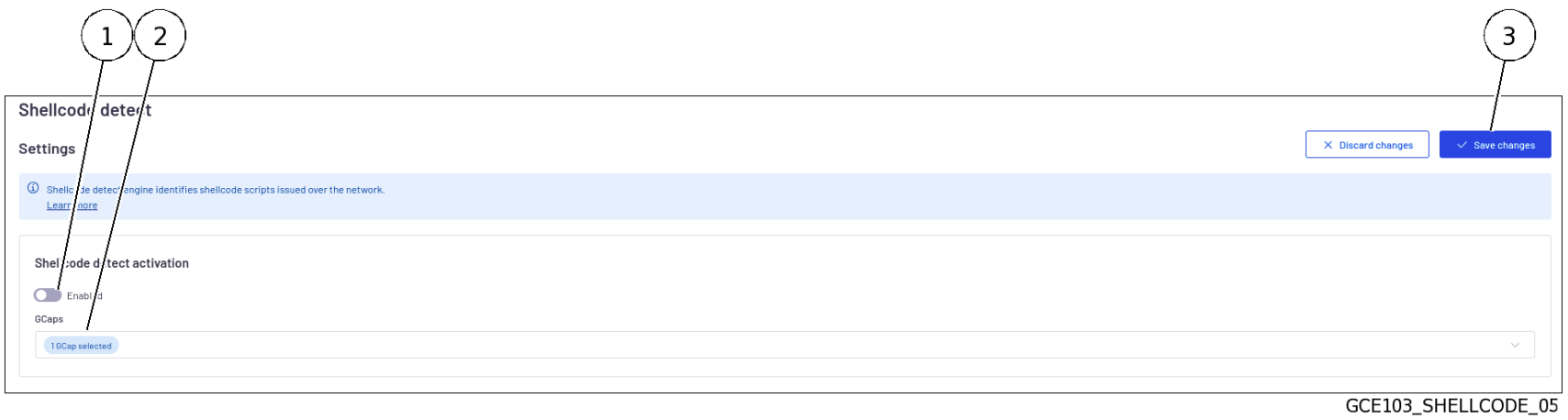
8.8.8.5 Procedure to access the `Shellcode detect` window



GCE103_MENUBAR

- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `Shellcode` command from the `Exploit` submenu.
  The `Shellcode detect` window is displayed.

8.8.8.6 Procedure to enable the engine

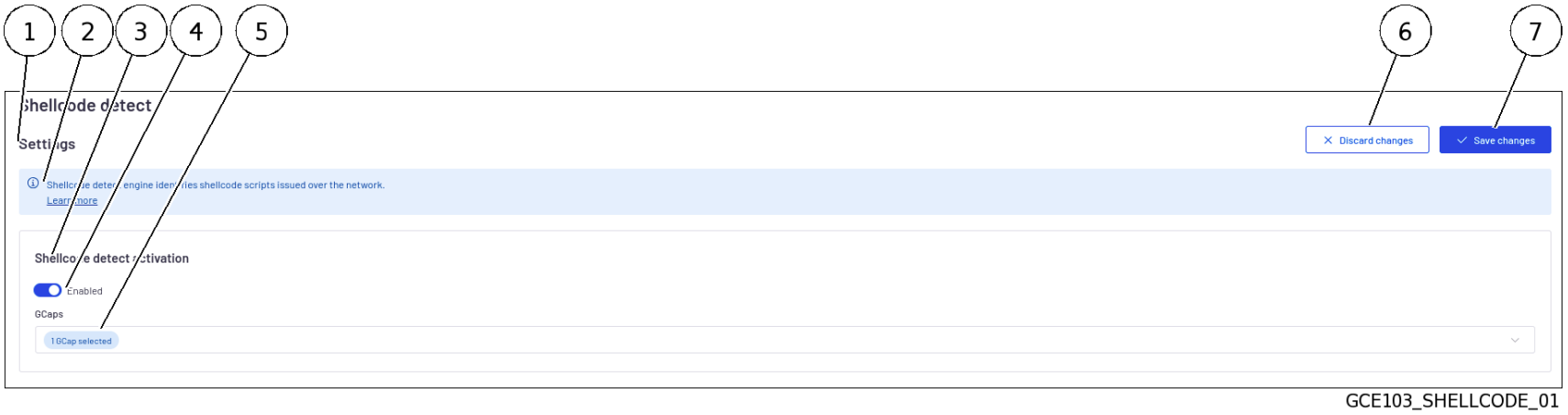


GCE103_SHELLCODE_05

- Use the `Enabled` selector (1) to enable the engine.
- Select the GCap (2) where the engine has to be enabled.
- Click on `Save changes` button (3).
  The following message is displayed.

```
Apply changes

 Enabling or disabling an engine on a GCap will cause it to restart.
 Are you sure you want to apply these configuration changes now?
```

- Click on the `Apply` button.
  The message `Success:  Your data has been saved` is displayed
  The following screen is displayed.



GCE103_SHELLCODE_01

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.

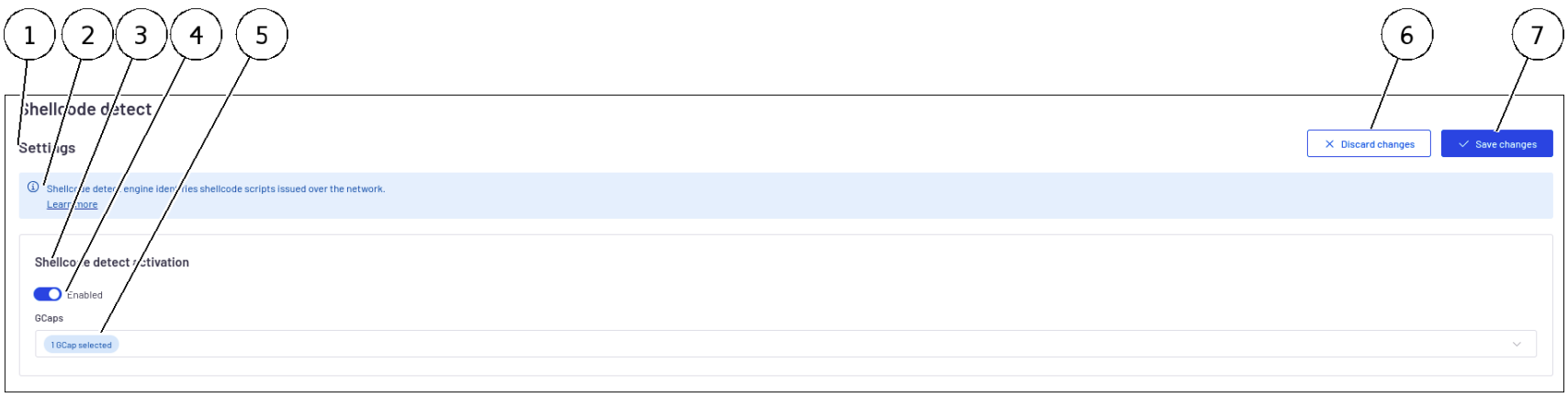
The following screen is displayed.

GCE103_SHELLCODE_06

The screen indicates:

- The status of the engine (1): here `Enabled`
- The state of the engine (2): here `Running`

8.8.8.7 Procedure to disable the engine

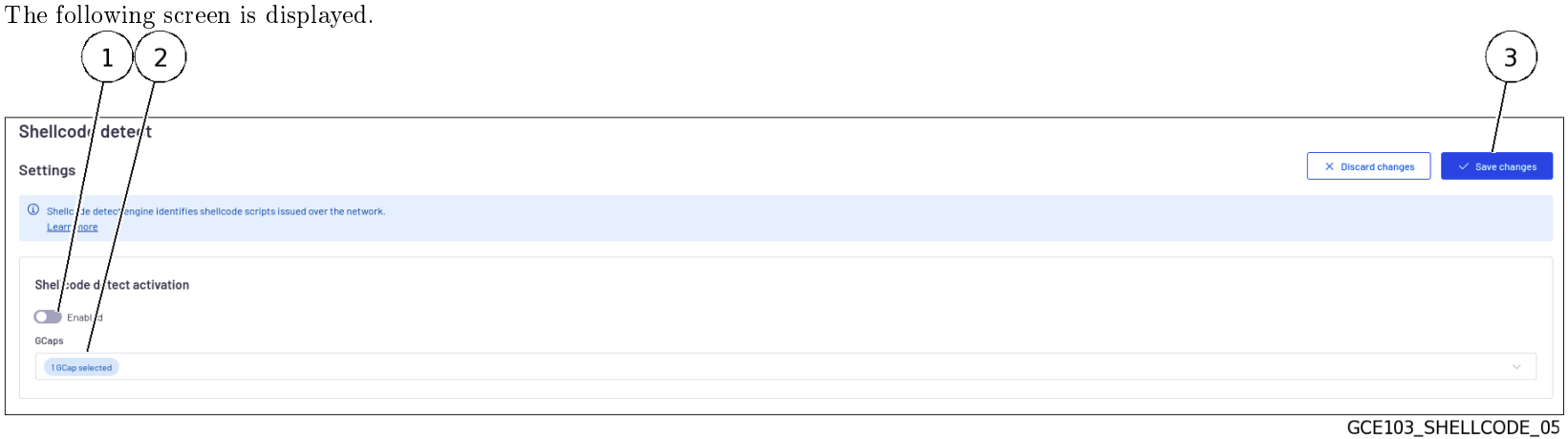


GCE103_SHELLCODE_01

- Use the `Enabled` selector (4) to disable the engine.
- Click on the `Save changes` button (7).
  The following message is displayed.

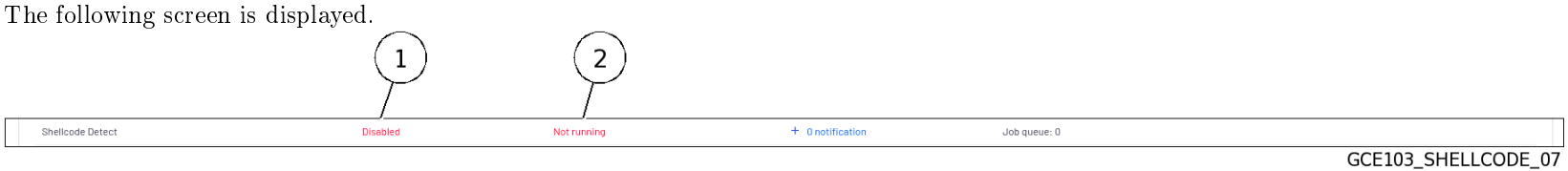
```
Apply changes

Enabling or disabling an engine on a GCap will cause it to restart.
Are you sure you want to apply these configuration changes now?
```

- Click on the `Apply` button.
  The message `Success:  Your data has been saved` is displayed
  The following screen is displayed.



GCE103_SHELLCODE_05

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.



GCE103_SHELLCODE_07

The screen indicates:

- The status of the engine (1): `Disabled`
- The state of the engine (2): `Not running`

8.8.9 Setting up the Active CTI engine

8.8.9.1 Introduction

This procedure describes:

- The enabling / disabling of the engine
- The setting of the retention time of the Compromission Indices

To	Apply the procedures
Enable the engine	1 - Apply the *Procedure to access the `Active CTI` window* 2 - Apply the *Procedure to enable the engine*
Set the retention time of the Compromission Indices	1 - Apply the *Procedure to access the `Active CTI` window* 2 - Apply the *Procedure to setup the IOC retention duration*
Disable the engine	1 - Apply the *Procedure to access the `Active CTI` window* 2 - Apply the *Procedure to disable the engine*

8.8.9.2 Links associated

The engine is described in the *Active CTI engine* paragraph.
The graphical interface is described in *`Active CTI` screen*.

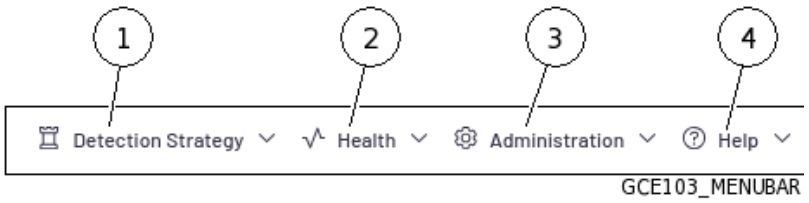
8.8.9.3 Prerequisites

- User: member of **Administrator** group

8.8.9.4 Preliminary operations

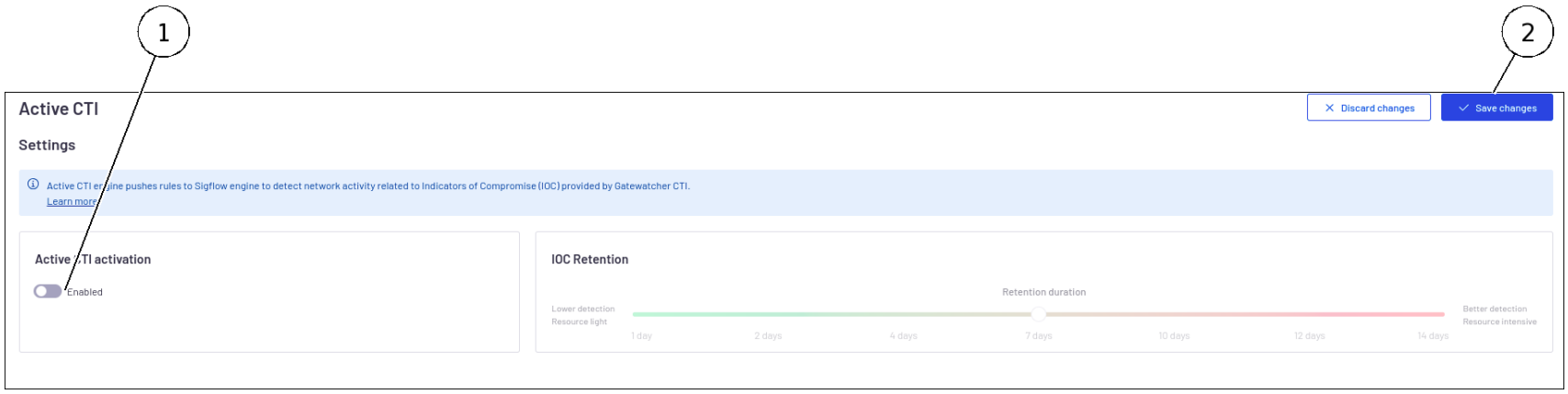
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.8.9.5 Procedure to access the `Active CTI` window



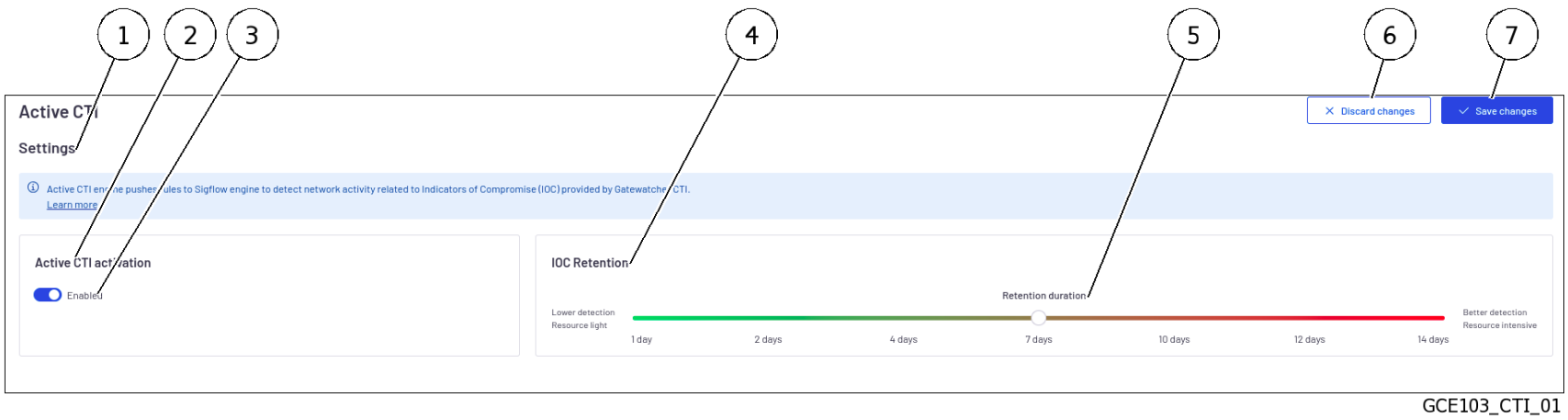
- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `Active CTI` command from the `Threat intel` submenu.
  The `Active CTI` window is displayed.

8.8.9.6 Procedure to enable the engine



GCE103_CTI_02

- Use the `Enabled` selector (1) to enable the engine.
- Click on the `Save changes` button (2).
  The message `Success: Your data has been saved` is displayed
  The following screen is displayed.



GCE103_CTI_01

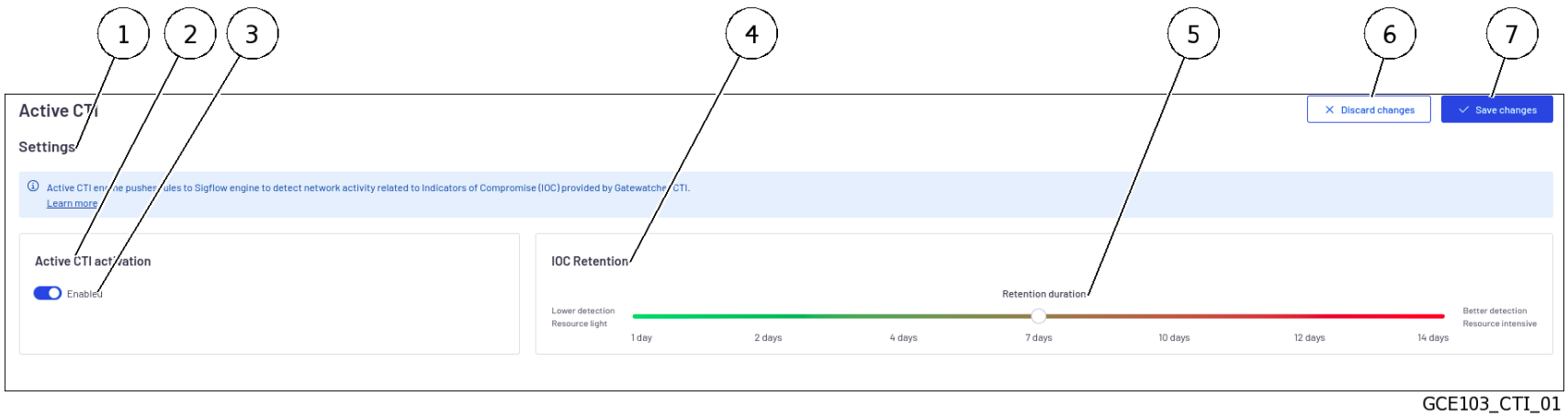
- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.

GCE103_CTI_03

The screen indicates:

- The status of the engine (1): here `Enabled`
- The state of the engine (2): here `Running`

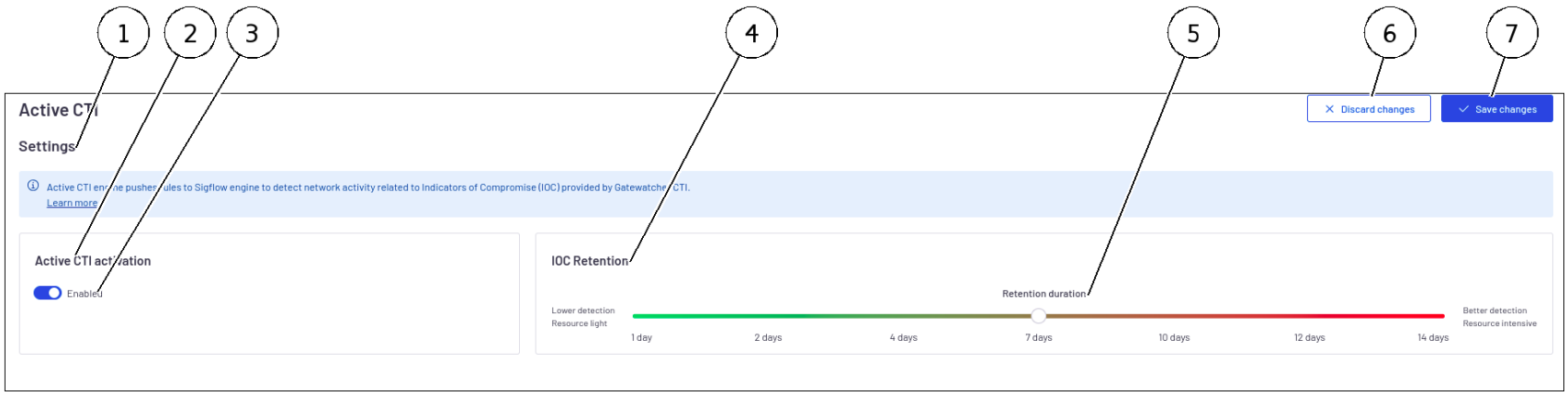
8.8.9.7 Procedure to setup the IOC retention duration



GCE103_CTI_01

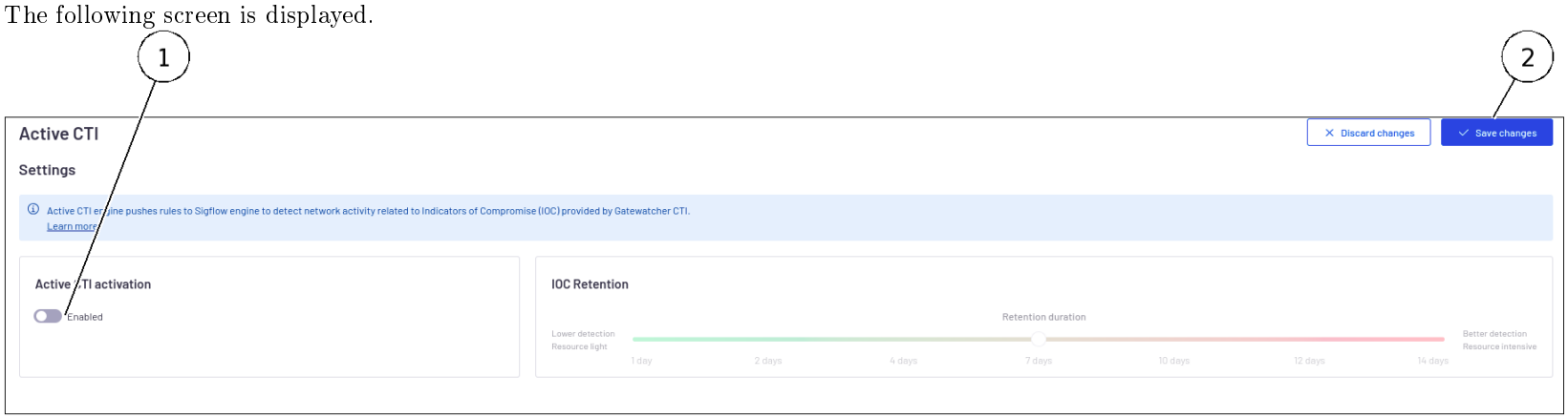
- Use the `Retention duration` selector (5) to define the chosen duration.
  The value by default is 7 days.
  The longer the retention period, the greater the number of IOCs.
  So the search will be longer but the probability of finding a match between the flow coming from the GCap and the IOC is more important (hence a better detection performance).
- Confirm the changes using the `Save changes` button (7).

8.8.9.8 Procedure to disable the engine



GCE103_CTI_01

- Use the `Enabled` selector (3) to disable the engine.
- Click on the `Save changes` button (7).
  The message `Success: Your data has been saved` is displayed
  The following screen is displayed.



GCE103_CTI_02

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.

GCE103_CTI_04

The screen indicates:

- The status of the engine (1): `Disabled`
- The state of the engine (2): `Not running`

8.8.10 Setting up the retro hunt engine

8.8.10.1 Introduction

This procedure describes the enabling / disabling of the engine.

To	Apply the procedures
Enable the engine	1 - Apply the *Procedure to access the `Retro Hunt` window* 2 - Apply the *Procedure to enable the engine*
Disable the engine	1 - Apply the *Procedure to access the `Retro Hunt` window* 2 - Apply the *Procedure to disable the engine*

8.8.10.2 Links associated

The engine is described in the *Retro hunt engine* paragraph.
The graphical interface is described in *`Retro hunt` screen*.

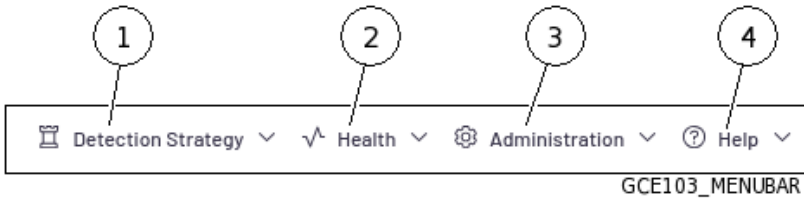
8.8.10.3 Prerequisites

- User: member of **Administrator** group

8.8.10.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

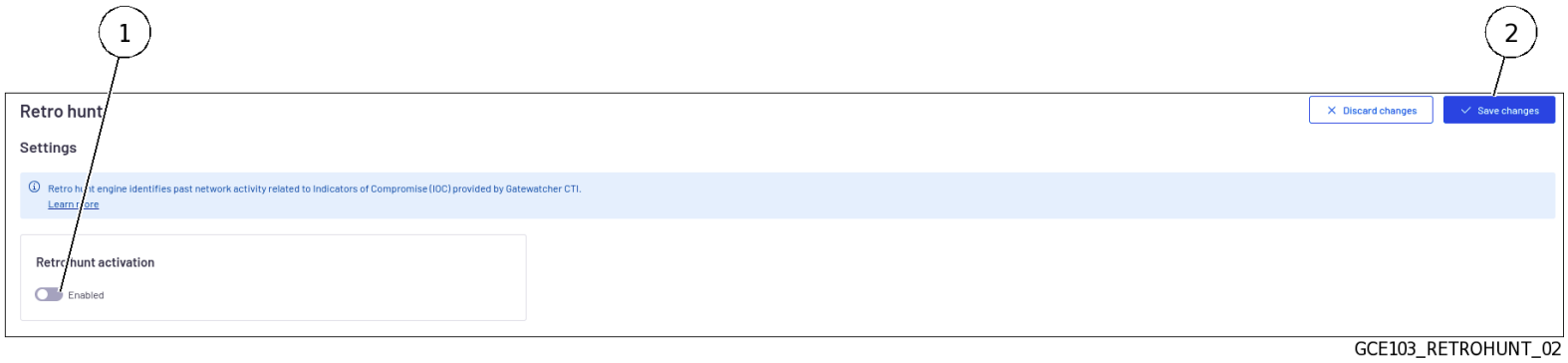
8.8.10.5 Procedure to access the `Retro Hunt` window



GCE103_MENUBAR

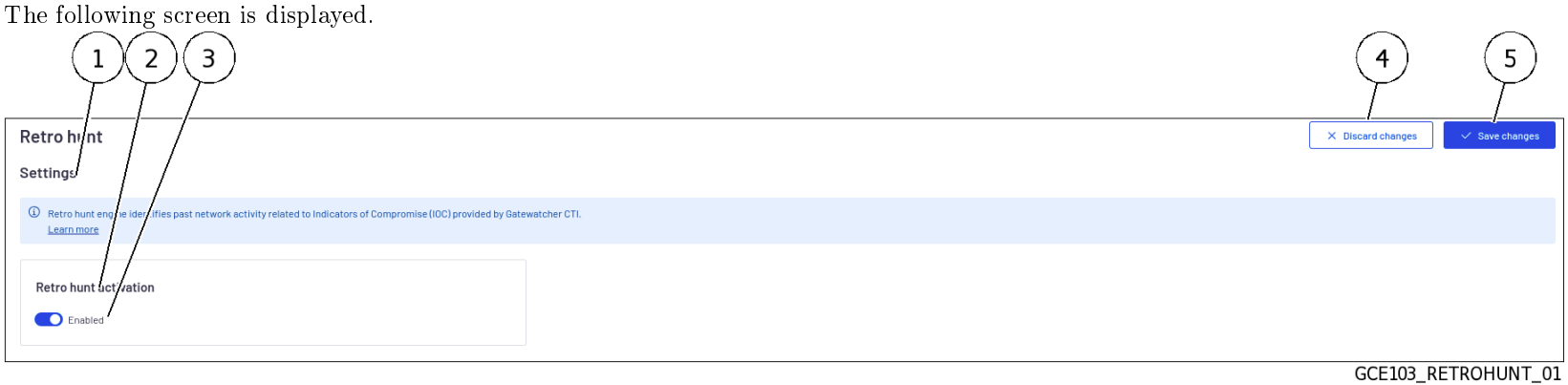
- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `Retro Hunt` command from the `Threat intel` submenu.
  The `Retro Hunt` window is displayed.

8.8.10.6 Procedure to enable the engine



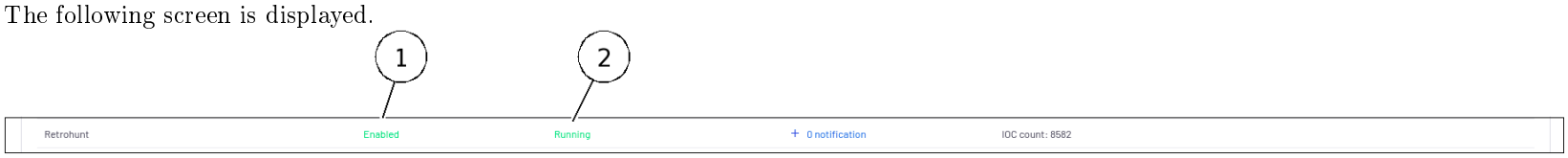
GCE103_RETROHUNT_02

- Use the `Enabled` selector (1) to enable the engine.
- Click on the `Save changes` button (2).
  The message `Success: Your data has been saved` is displayed
  The following screen is displayed.



GCE103_RETROHUNT_01

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.

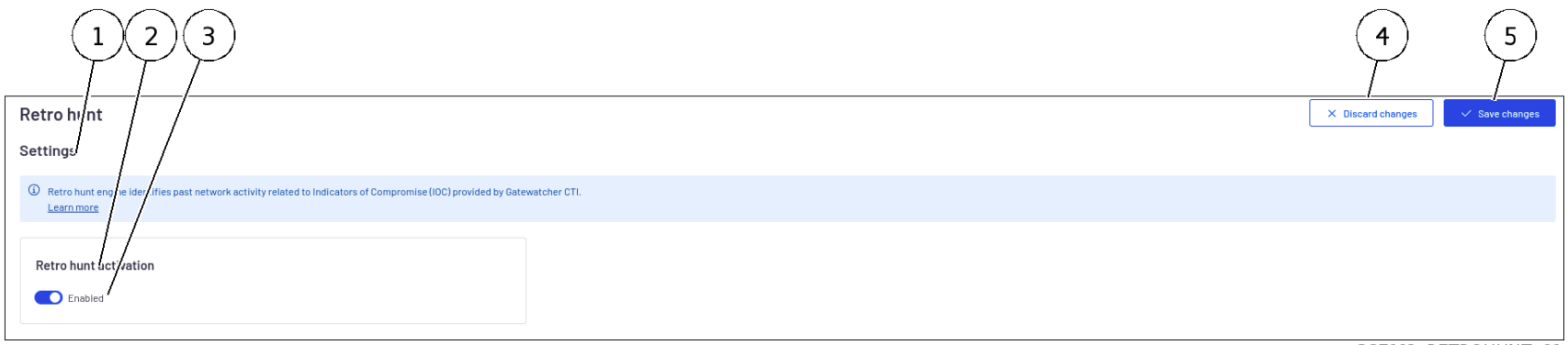


GCE103_RETROHUNT_03

The screen indicates:

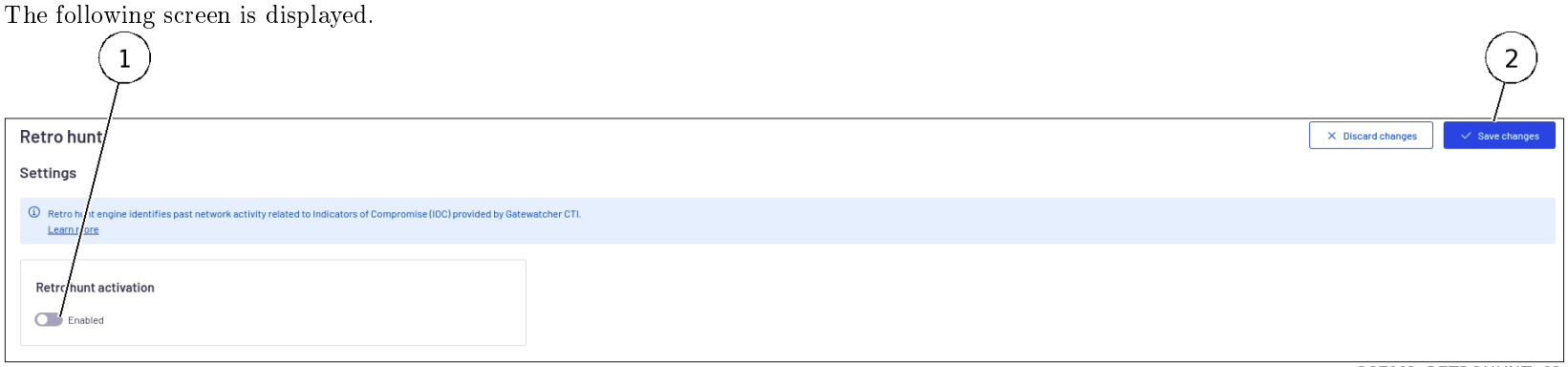
- The status of the engine (1): here `Enabled`
- The state of the engine (2): here `Running`

8.8.10.7 Procedure to disable the engine



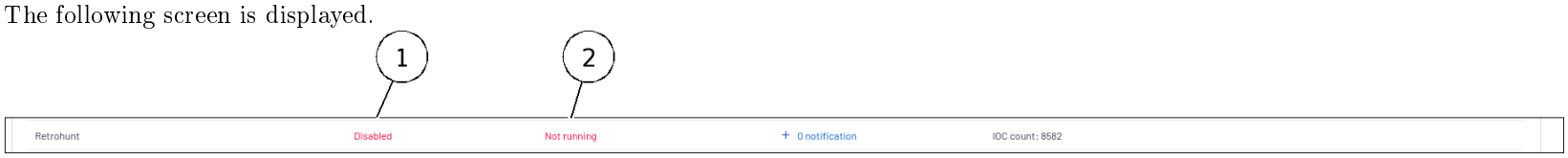
GCE103_RETROHUNT_01

- Use the `Enabled` selector (3) to disable the engine.
- Click on the `Save changes` button (5).
  The message `Success: Your data has been saved` is displayed
  The following screen is displayed.



GCE103_RETROHUNT_02

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.



GCE103_RETROHUNT_04

The screen indicates:

- The status of the engine (1): `Disabled`
- The state of the engine (2): `Not running`

8.8.11 Setting up the Ransomware detect engine

8.8.11.1 Introduction

This procedure describes the enabling / disabling of the engine.

To	Apply the procedures
Enable the engine	1 - Apply the *Procedure to access the `Ransomware detect` window* 2 - Apply the *Procedure to enable the engine*
Disable the engine	1 - Apply the *Procedure to access the `Ransomware detect` window* 2 - Apply the *Procedure to disable the engine*

8.8.11.2 Links associated

The engine is presented in the *Ransomware detect engine* paragraph.
The graphical interface is described in the *`Ransomware detect` screen (Ransomware command)*.

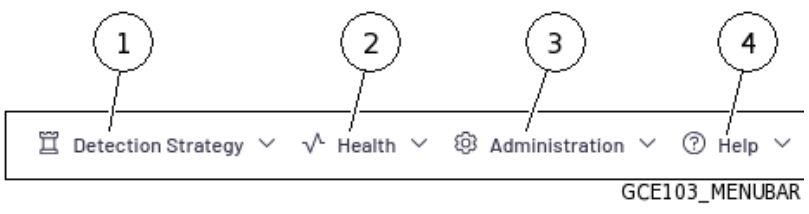
8.8.11.3 Prerequisites

- User: member of **Operator** group

8.8.11.4 Preliminary operations

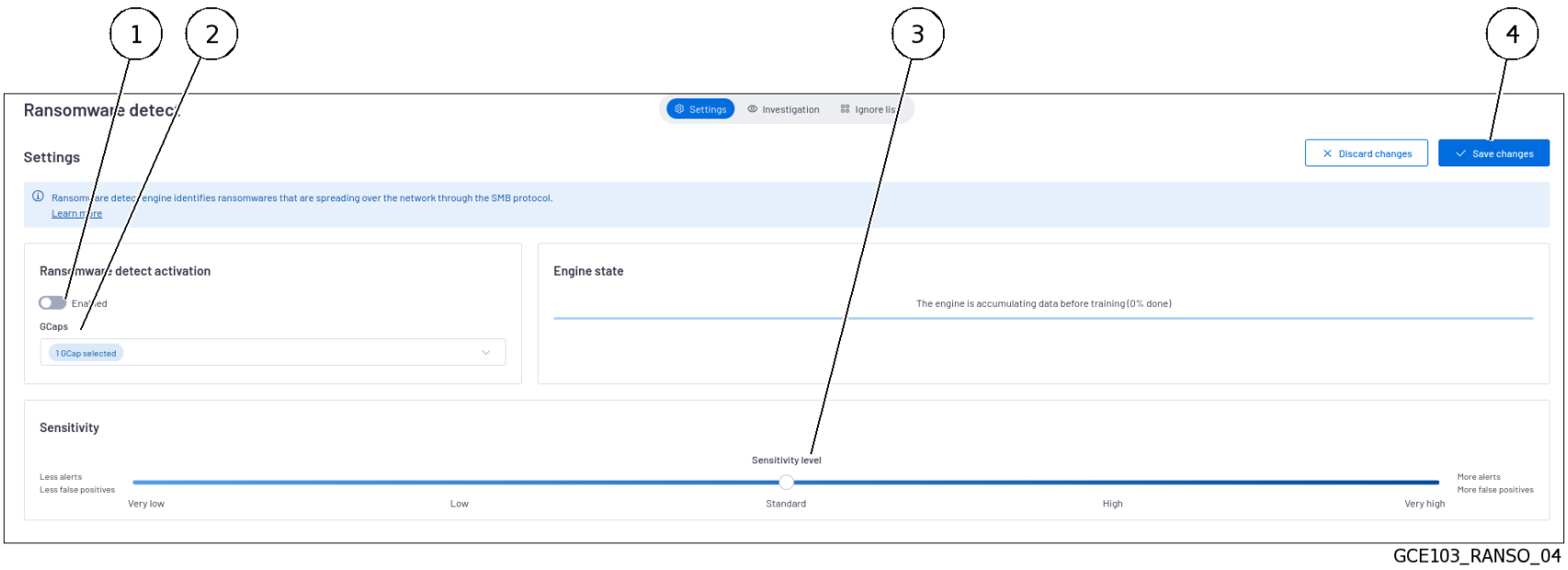
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.8.11.5 Procedure to access the `Ransomware detect` window



- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `Ransomware` command from the `Behaviour analysis` submenu.
  The `Ransomware detect` window is displayed.

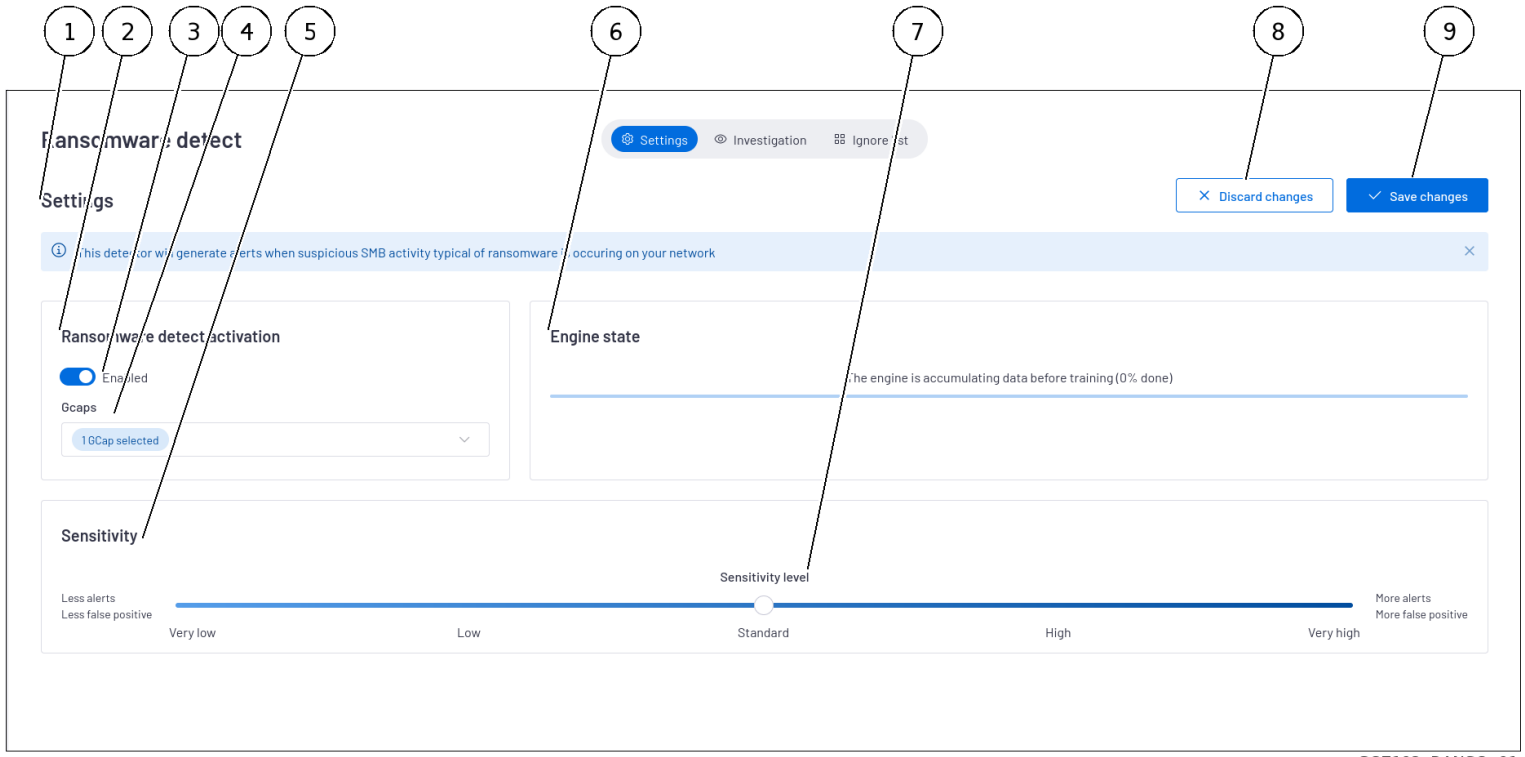
8.8.11.6 Procedure to enable the engine



- Use the `Enabled` selector (1) to enable the engine.
- Select the Gcap (2) where the engine has to be activated.
- Use the `Sensitivity level` (3) to adjust the sensitivity threshold to raise an alert (see *`Ransomware detect` screen (Ransomware command)* for further details)
- Click on `Save changes` button (4).
  The message `Success: Your data has been saved` is displayed.

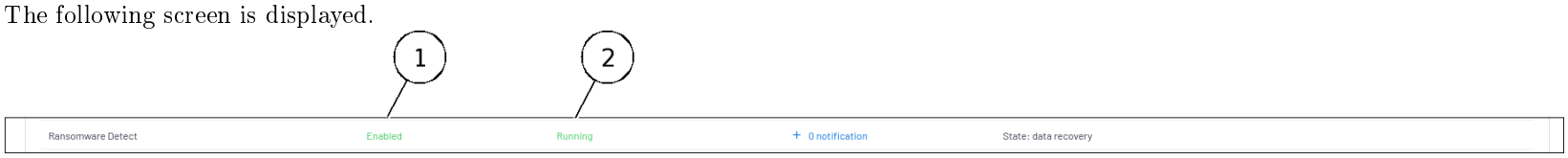
```
Success
Your settings have been successfully saved.
```

  The following screen is displayed.



GCE103_RANSO_01

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.



GCE103_RANSO_05

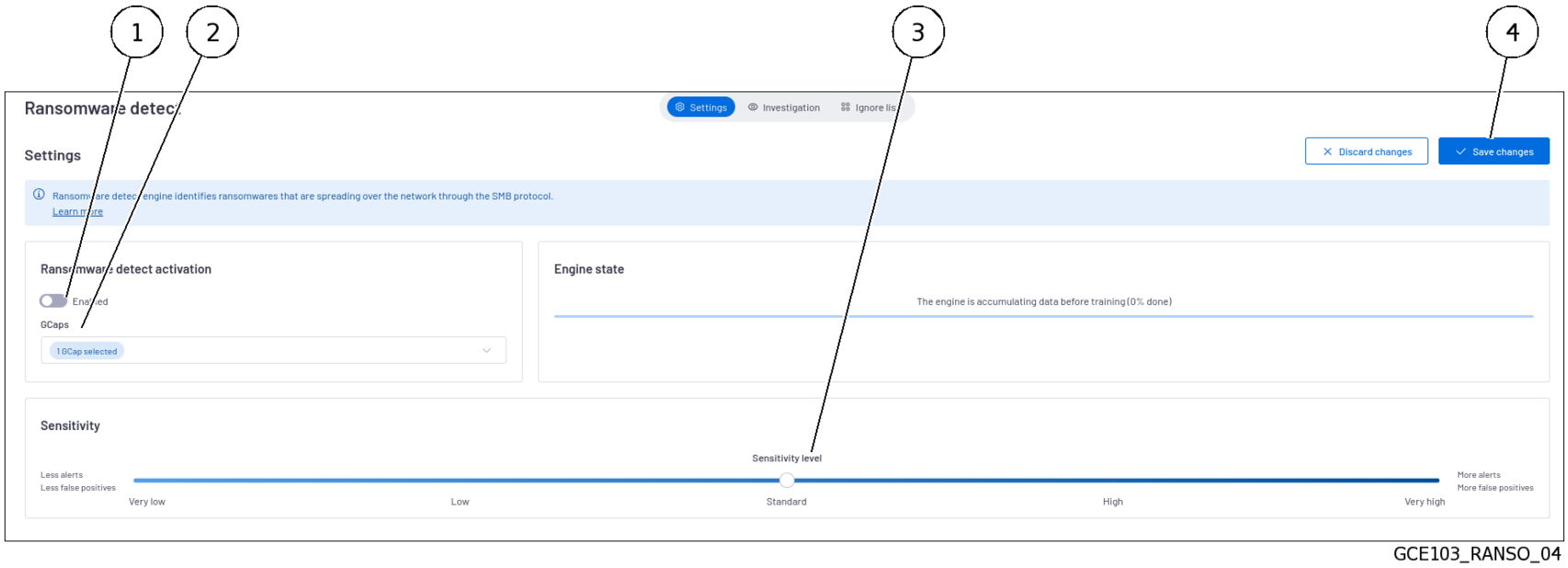
The screen indicates:

- The status of the engine (1): here `Enabled`
- The state of the engine (2): here `Running`

8.8.11.7 Procedure to disable the engine

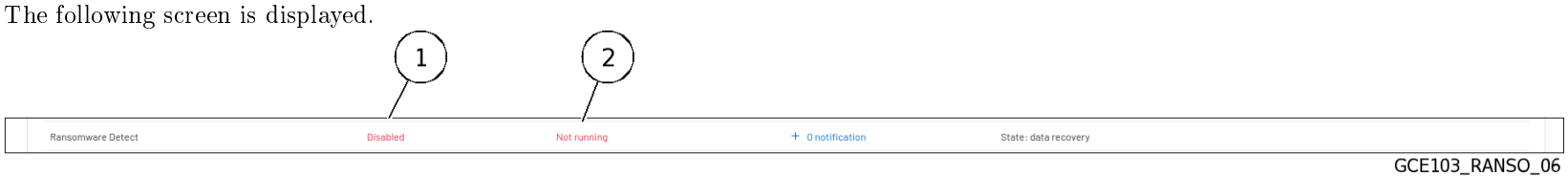
GCE103_RANSO_01

- Use the `Enabled` selector (3) to disable the engine.
- Click on the `Save changes` button (9).
  The message `Success: Your settings have been successfully saved.` is displayed
  The following screen is displayed.



GCE103_RANSO_04

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.



GCE103_RANSO_06

The screen indicates:

- The status of the engine (1): `Disabled`
- The state of the engine (2): `Not running`

8.8.12 Managing the Ignore list of the Ransomware detect

8.8.12.1 Introduction

The `Ignore list` defines the list of IP addresses not to be analyzed and therefore consider them to be healthy.
This removes alerts related to recurring false positives.
This procedure describes how to populate this list.

8.8.12.2 Links associated

The engine is presented in the *Ransomware detect engine* paragraph.
The graphical interface is described in the *`Ransomware detect` screen (Ransomware command)*.

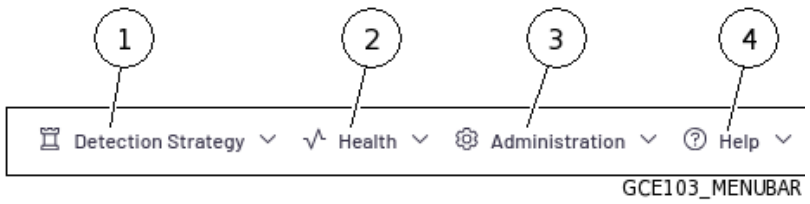
8.8.12.3 Prerequisites

- User: member of **Administrator** group

8.8.12.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.8.12.5 Procedure to access the `Ransomware detect` window



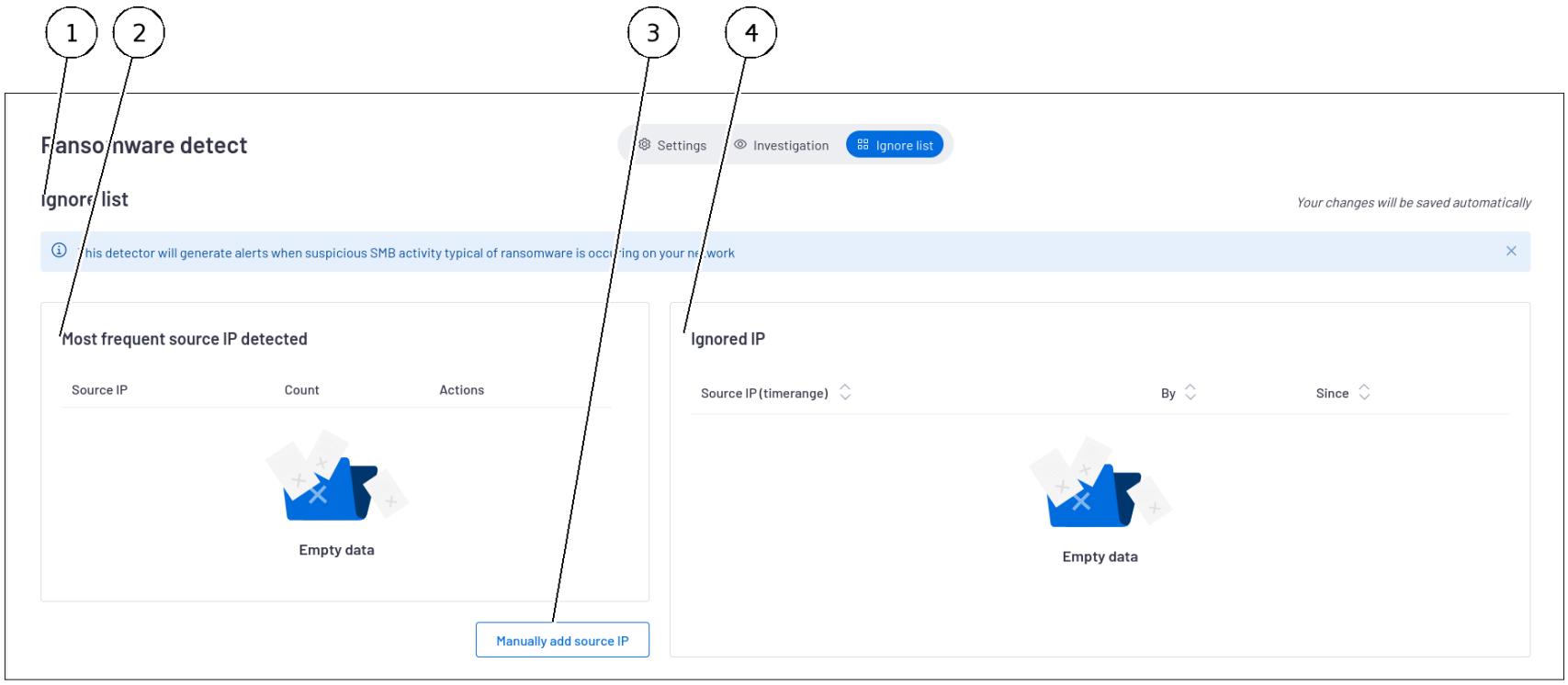
GCE103_MENUBAR

- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `Ransomware` command from the `Behaviour analysis` submenu.
  The `Ransomware detect` window is displayed.

8.8.12.6 Procedure to manage the `Ignore list`

GCE103_RANSO_01

- Click on the `Ignore list` section.



GCE103_RANSO_03

Note:

The area (2) displays the most frequent source IP addresses detected.

- To add an item to the `Ignored IP` list:
- Click on the `Manually add source IP` button (3).
  The `Add a source IP to ignore` window is displayed.
- Enter the source IP in the `Source IP *` field
- Enter the time range in the `Time ranges` field if needed.
  The expected format is 'hh:mm'
- Click on the `Save` button.
  If successful, the following message is displayed: `Your data has been saved`.
  In case of errors, a message is displayed.
  For example, `IP doest not match v4 format` for an invalid IP address or `Only numbers separated by ':'  are expected` for a invalid hour.
- To delete an item from the `Ignored IP` list:
- Click on the trash of the row to be deleted.
  A confirmation window is displayed...
- Validate the deletion by clicking on the `Save` button.
  The following message is displayed: `IP successfully deleted`.

8.8.13 Setting up the beacon detect engine

8.8.13.1 Introduction

This procedure describes the enabling / disabling of the engine.

To	Apply the procedures
Enable the engine	1 - Apply the *Procedure to access the `Beacon detect` window* 2 - Apply the *Procedure to enable the engine*
Disable the engine	1 - Apply the *Procedure to access the `Beacon detect` window* 2 - Apply the *Procedure to disable the engine*

8.8.13.2 Links associated

The engine is presented in the *Beacon detect engine* paragraph.
The graphical interface is described in *`Beacon detect` screen (Beacon command)*.

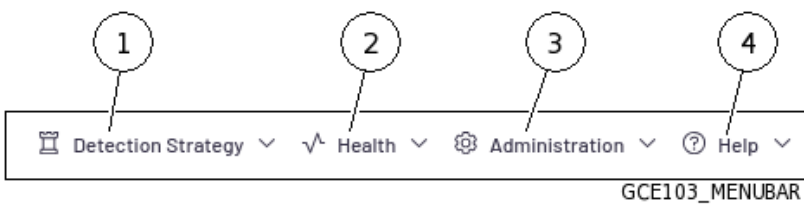
8.8.13.3 Prerequisites

- User: member of **Operator** group

8.8.13.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

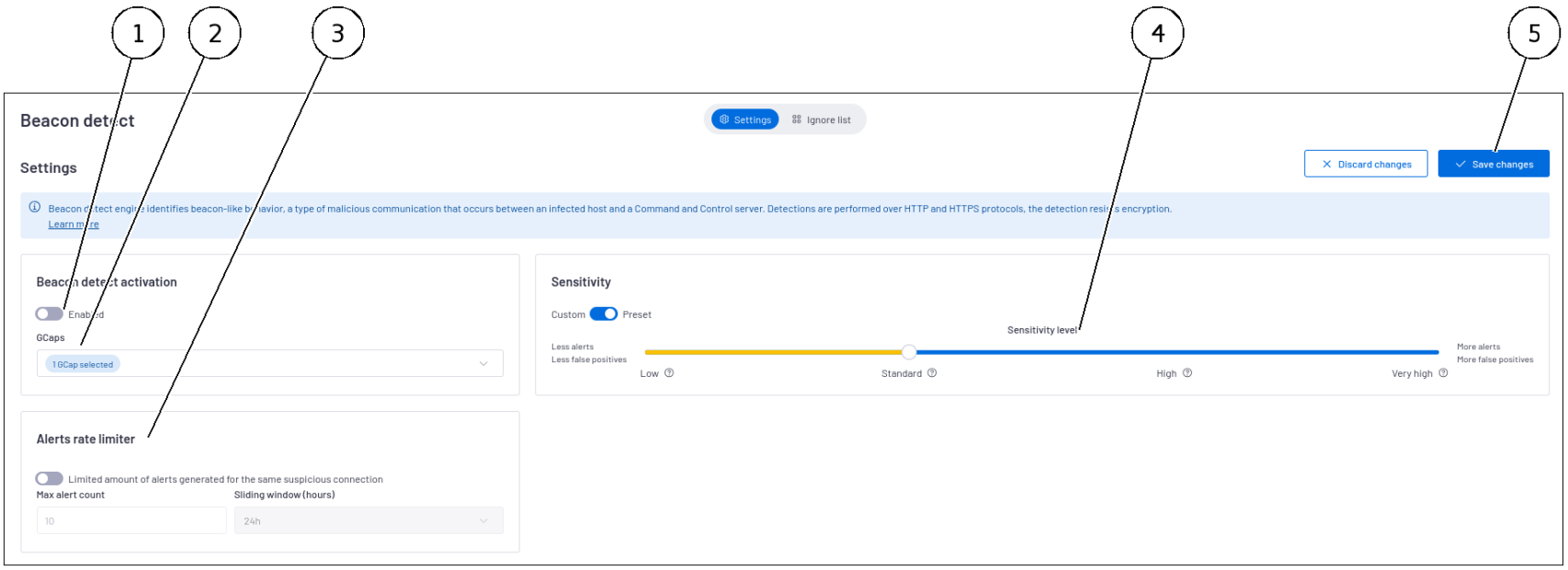
8.8.13.5 Procedure to access the `Beacon detect` window



- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `Beacon` command from the `C&C` submenu.
  The `Beacon detect` window is displayed.

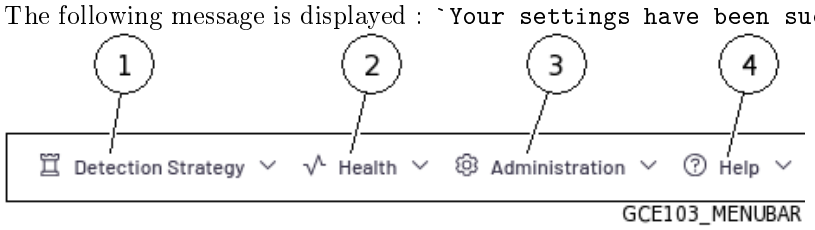
8.8.13.6 Procedure to enable the engine

- Click on the `Settings` section.
  The `Settings` window displays the option to enable/disable the engine.



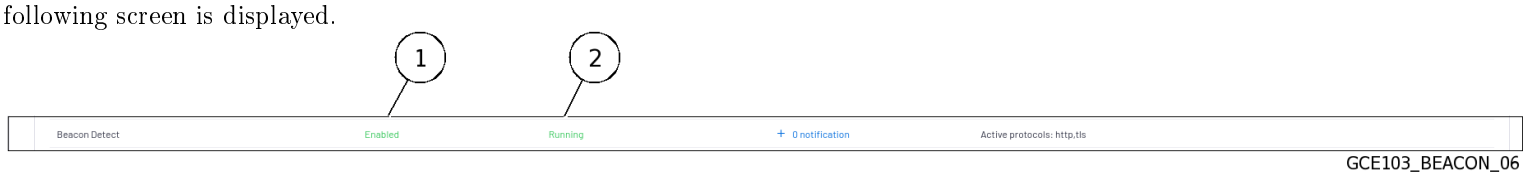
- Use the `Enabled` selector (1) to enable the engine.
  When the engine is turned on again after being off for at least a few minutes, the scan window is reset to the current time.
- Select the Gcap (2) where the engine has to be activated.
- Use the `Sensitivity level` (4) to adjust the sensitivity threshold to raise an alert (see *`Beacon detect` screen (Beacon command)* for further details)
- If needed `Use the Alerts rate limiter` feature (3).
- Click on `Save changes` button (5).

The following message is displayed : `Your settings have been successfully saved.`



GCE103_MENUBAR

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.



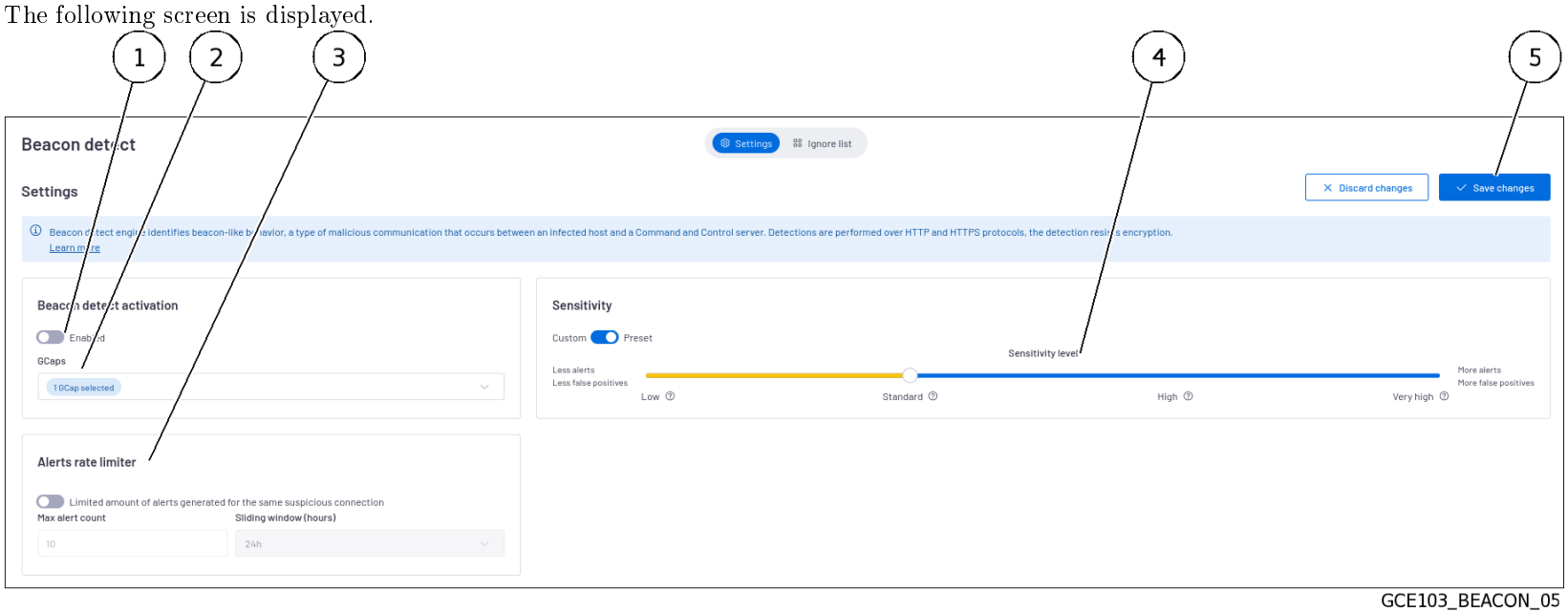
GCE103_BEACON_06

The screen indicates:

- The status of the engine (1): here `Enabled`
- The state of the engine (2): here `Running`

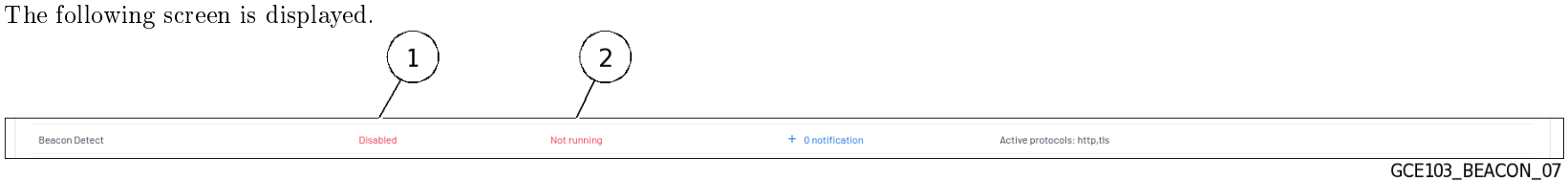
8.8.13.7 Procedure to disable the engine

- Click on the `Settings` section.
  The `Settings` window displays the option to enable/disable the engine.
- Use the `Enabled` selector (1) to disable the engine.
- Click on the `Save changes` button (5).
  The following message is displayed.
  The message `Success:  Your data has been saved` is displayed
  The following screen is displayed.



GCE103_BEACON_05

- Click on the `Main healthchecks` command on the `Health-Monitoring` menu.
  The following screen is displayed.



GCE103_BEACON_07

The screen indicates:

- The status of the engine (1): `Disabled`
- The state of the engine (2): `Not running`

8.8.14 Managing the Ignore list of the Beacon detect

8.8.14.1 Introduction

The `Ignore list` allows a Domain URL or IP address to be declared healthy.
This removes alerts related to recurring false positives.
This procedure describes how to populate this list.

To	Apply the procedures
To add an item to the `Ignore list`	1 - Apply the *Procedure to access the `Beacon detect` window* 2 - Apply the *Procedure to add an item to the `Ignored destinations` list*
To delete an item to the `Ignore list`	1 - Apply the *Procedure to access the `Beacon detect` window* 2 - Apply the *Procedure to delete an item to the `Ignored destinations` list*

8.8.14.2 Links associated

The engine is presented in the *Beacon detect engine* paragraph.
The graphical interface is described in *`Beacon detect` screen (Beacon command)*.

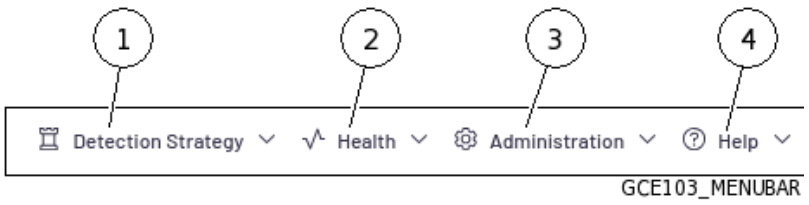
8.8.14.3 Prérequis

- User: member of **Administrator** group

8.8.14.4 Opérations préliminaires

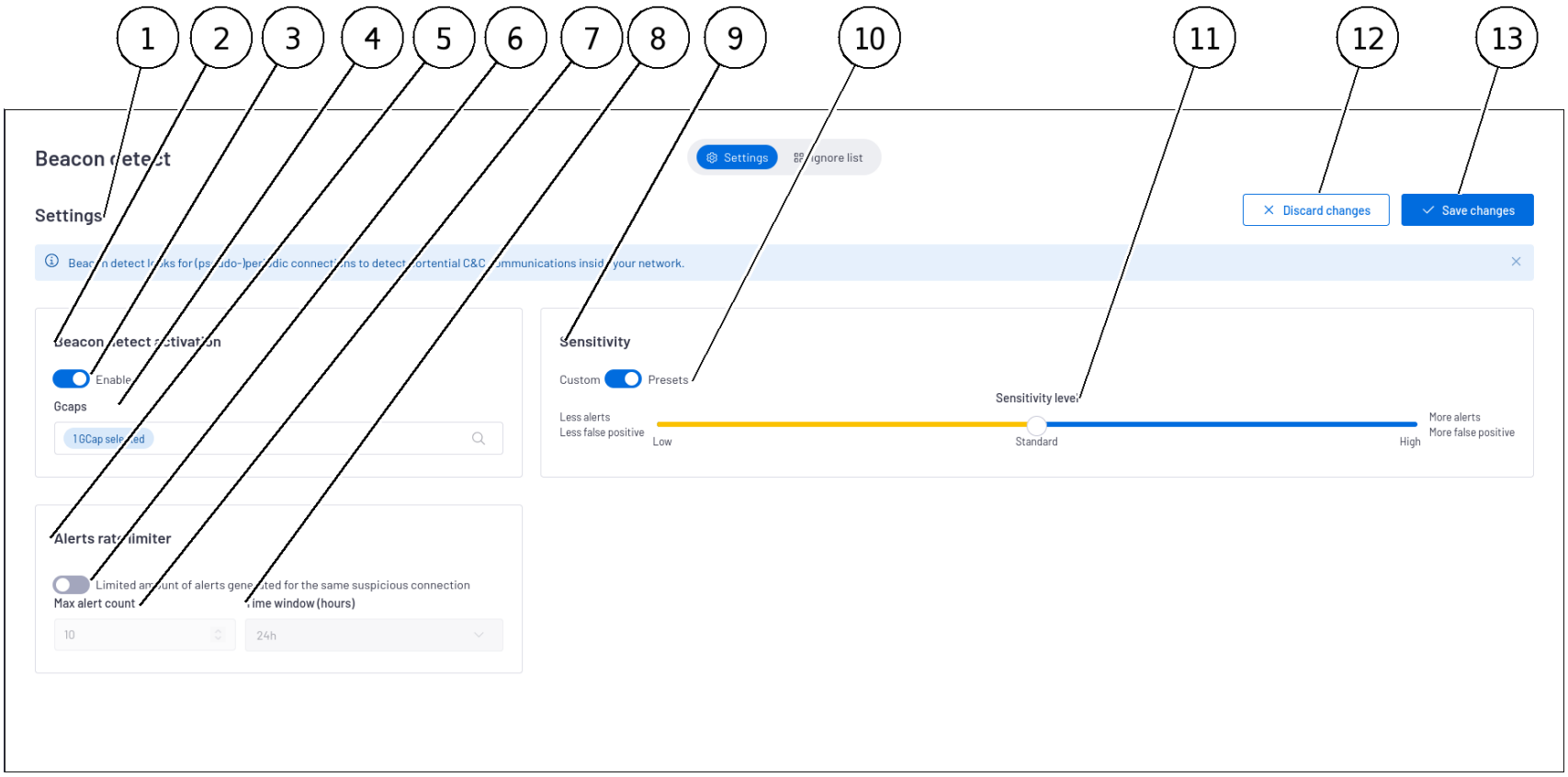
- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.8.14.5 Procedure to access the `Beacon detect` window



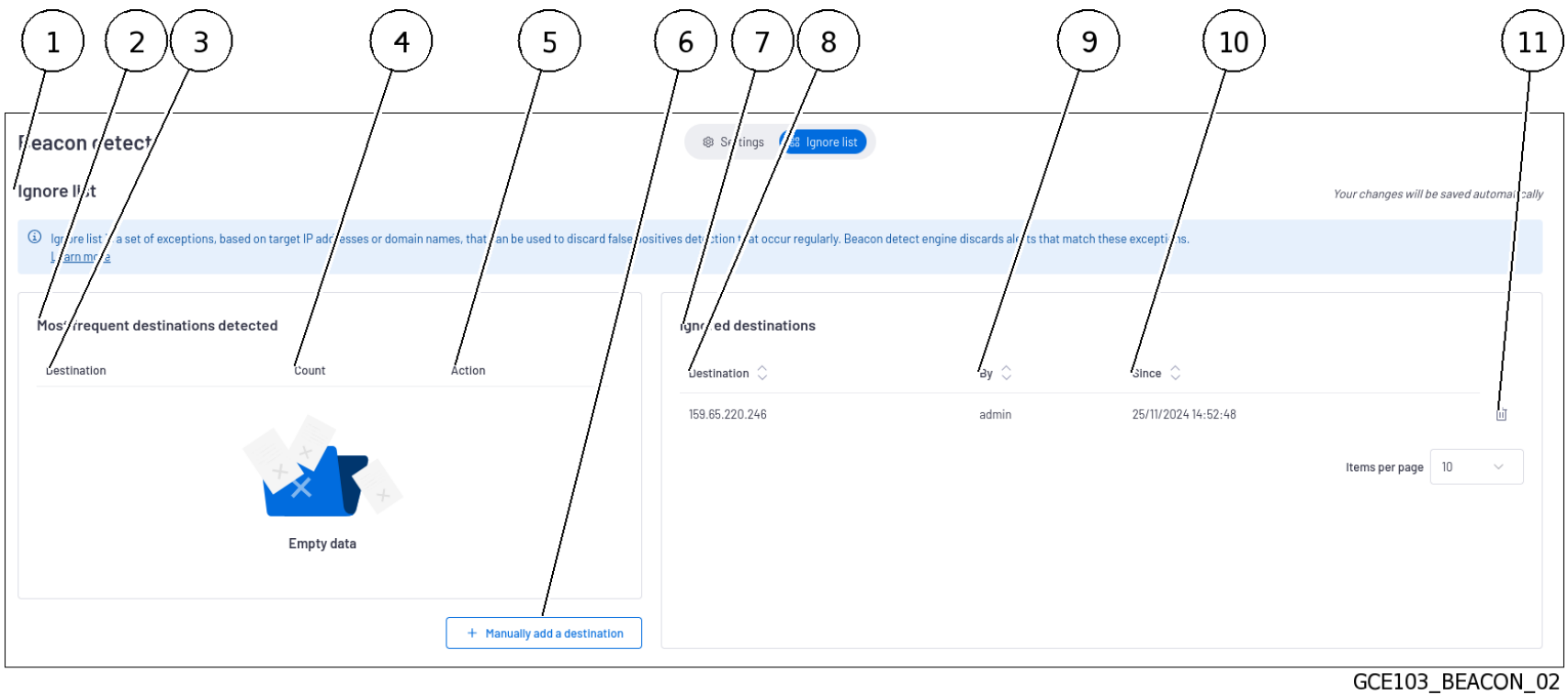
- In the GCenter interface, click on the `Detection Strategy` menu (1).
- Click on the `Beacon` command from the `C&C` submenu.
  The `Beacon detect` window is displayed.

8.8.14.6 Procedure to add an item to the `Ignored destinations` list



GCE103_BEACON_01

- Click on the `Ignore list` section.



GCE103_BEACON_02

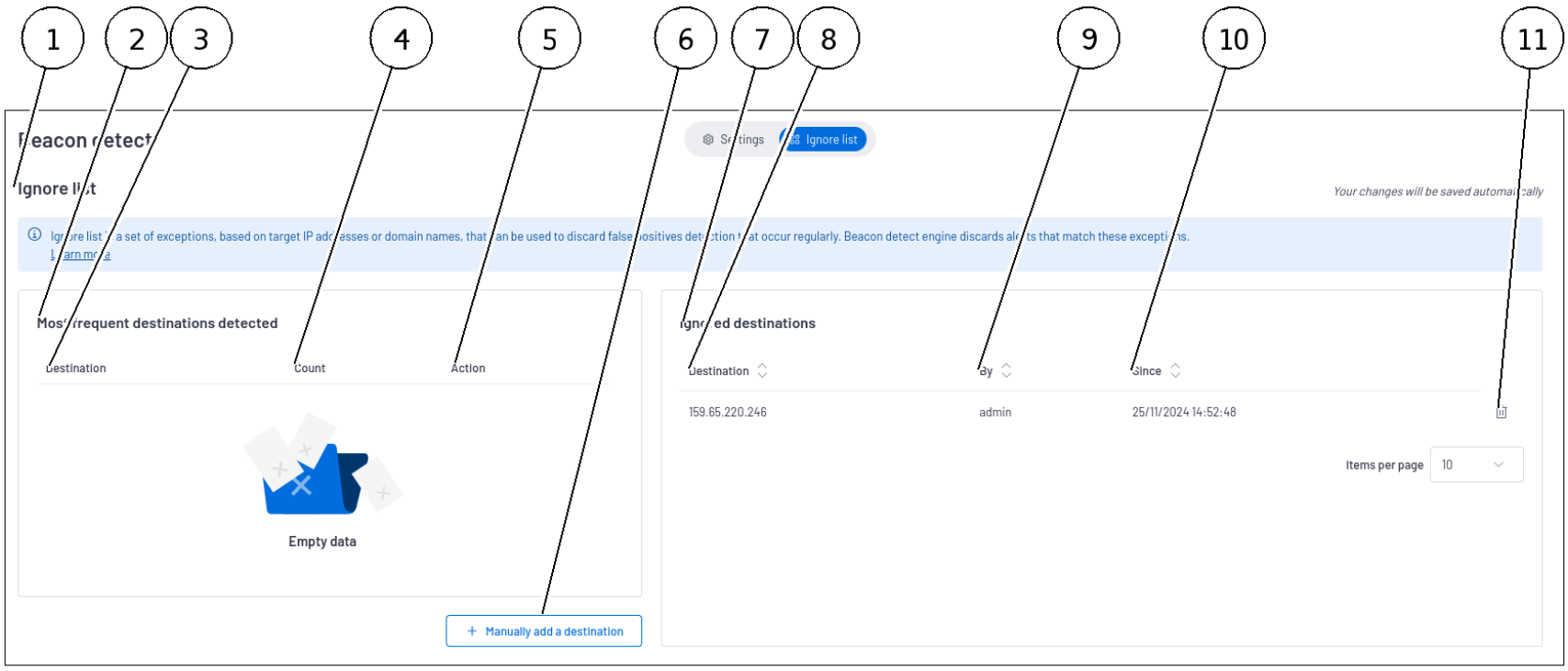
Note:

The area (2) displays the most frequent destinations detected.

- Click on the `Manually add destination` button (6)
  The `Add a destination to ignore` window is displayed
- Enter the url or IP address in the `Destination *` field
- Click on the `Save` button.

8.8.14.7 Procedure to delete an item to the `Ignored destinations` list

- Click on the `Ignore list` section.



GCE103_BEACON_02

- Click on the trash of the row to be deleted from the list.
  The following message is displayed: `Domain successfully deleted`.

8.9 Managing current user

This section describes how to manage the current user on the GCenter.
For more details on the accounts, see *Web interface accounts and their management*.

8.9.1 Changing the checking account password

8.9.1.1 Introduction

This procedure describes how to change the current user's password.
To enter a new password consistent with the policy to be applied, the system proposes six passwords.
A `REGENERATE` button enables six new passwords to be generated.

Danger:

Carefully note down the submitted password, especially if the checking account is the only account in the administrator group.

8.9.1.2 Links associated

For information, see the paragraphe *Web interface accounts and their management*.
For presentation of the screen, see the *`Profile / Edit Password` screen*.

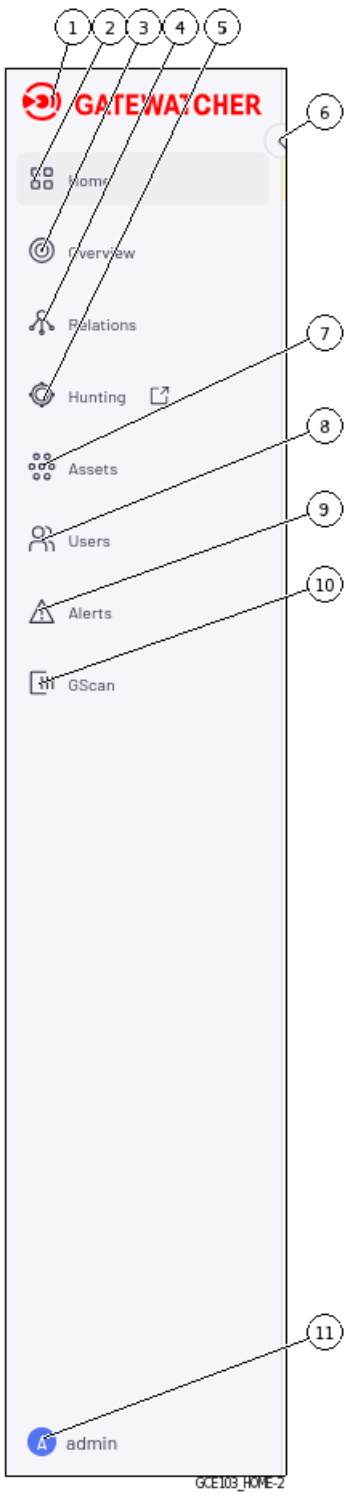
8.9.1.3 Prerequisites

Not Applicable

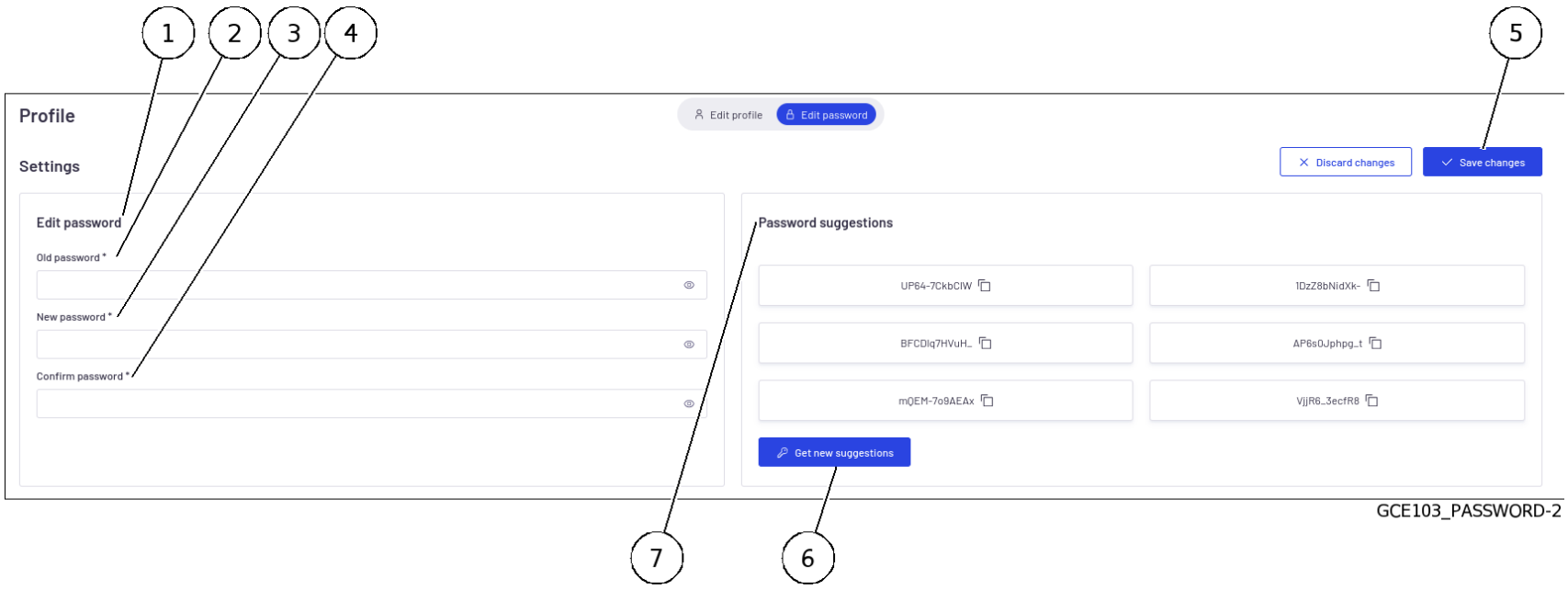
8.9.1.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.9.1.5 Procedure



- In the GCenter interface, click on the checking account button (11).
- Click on the `Edit password` command.



- Enter the previous password in the `Old password` field (2).
- Enter the new password in the `New password` field (3).
- Enter the new password in the `Confirm password` field (4).

  The password entered must match the *Password management policy*.

  The system checks the password against the verification policy.

  If the password does not meet the verification policy, one of the following messages will be displayed:
  - `Minimal length 12`: indicates a password that is too short (12 characters minimum)
  - `Uppercase`: indicates the lack of a capital letter
  - `Lowercase`: indicates the lack of a small letter
  - `Symbol`: indicates the lack of a special character
  - `Digit`: indicates the lack of a digit

Note:

To copy one of the proposed passwords, click on the right side of the password.
A window will appear informing that the password is copied to the clipboard.
To paste the password, right-click and then paste into each of the two fields.
Make sure to note down the password before saving.

- Click on the `Save changes` button (5).

Note:

If the following message is displayed `you used this password recently, please choose a different one.`, enter a password that has not been used before.

8.9.2 Changing some of the current user's information

8.9.2.1 Introduction

This procedure describes how to modify local users:

- Email address
- First name
- Last name

Danger:

Carefully note down the submitted password, especially if the checking account is the only account in the administrator group.

8.9.2.2 Links associated

For information, see the *Web interface accounts and their management*.
For presentation of the screen, see the *`Profile / Edit profile` screen*.

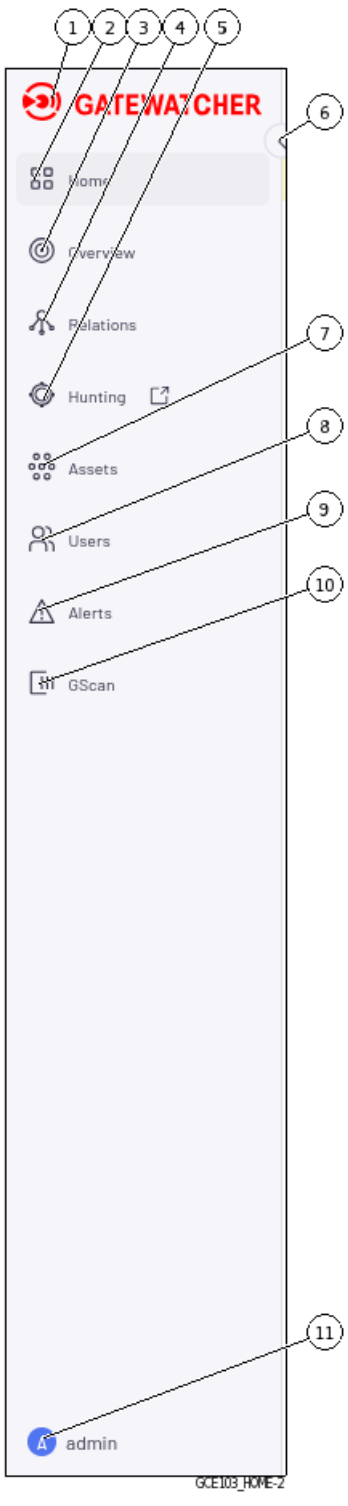
8.9.2.3 Prerequisites

Not Applicable

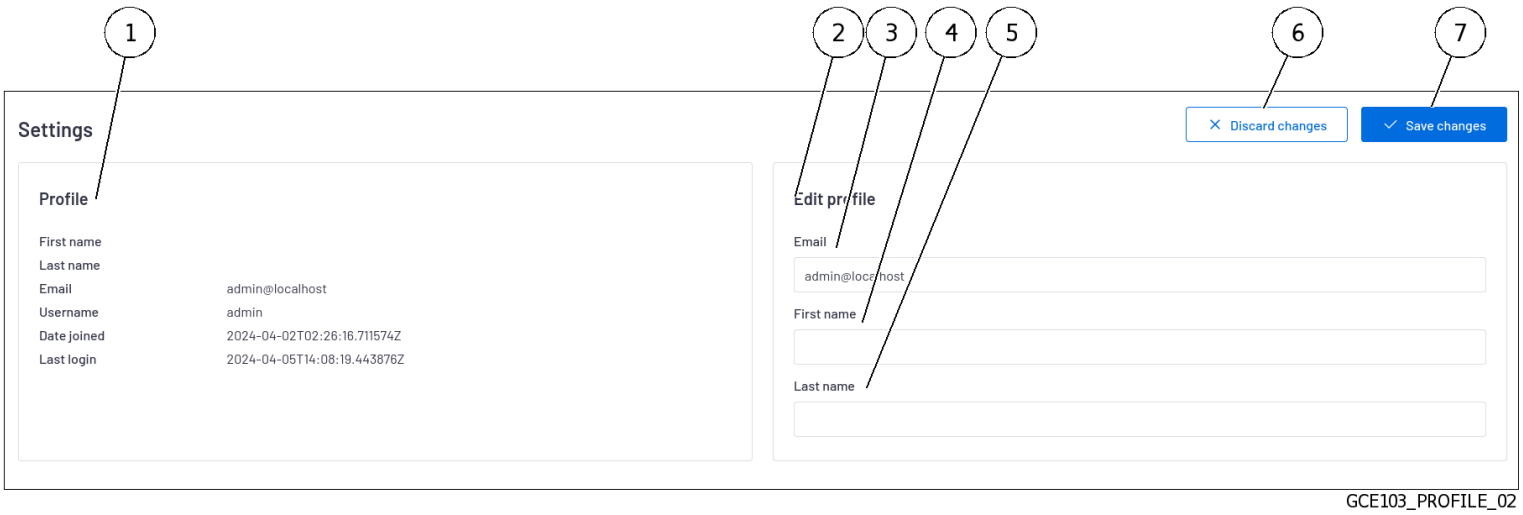
8.9.2.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.9.2.5 Procedure



- In the GCenter interface, click on the checking account button (11).
- Click on the `Edit profile` command.



The `Profile` area (1) shows account information such as username, creation date, and last login.

- Enter or modify the data found in the `Edit Profile` area (2):
- In the `Email ` field (3)
- In the `First name` field (4)
- In the `Last name` field (5)
- Confirm the changes using the `Save changes` button (7).
  A confirmation window displays the message `Profile successfully saved!`.

8.10 Monitoring the netdata

8.10.1 Configuring the Netdata polling interface

8.10.1.1 Introduction

This procedure describes the configuration of the Netdata interface to allow a remote server (for example NAGIOS) to read the selected metrics via the netdata API.

User Authentication:

Authenticated users can search the Netadata API, available on Gstats.
For simple automation, it is possible to allow an unauthenticated user to probe the API.
In this case, the API endpoint is redirected to http on the port specified below http://gcenter_fqdn:redirection_port

List of authorized IP addresses

A restricted access list is the client subnets for which this redirection is available.
Depending on the IP/mask pair, it is therefore possible to allow an IP or a range of IP addresses per line entered.
It is possible to add multiple rows.

List of accessible metrics

For a remote PC defined in the list of allowed IPs, it is possible to view the available metrics.
To do this, you must enter the following URL in a web browser http://IP-gcenter:8001/host/fqdn-gcenter/api/v1/allmetrics

Below, an extract of the metrics is displayed.

```
# chart: net_drops.vnet0 (name: net_drops.vnet0)
NETDATA_NET_DROPS_VNET0_INBOUND="0"       # drops/s
NETDATA_NET_DROPS_VNET0_OUTBOUND="-0"       # drops/s
NETDATA_NET_DROPS_VNET0_VISIBLETOTAL="0"       # drops/s

# chart: net_errors.vnet0 (name: net_errors.vnet0)
NETDATA_NET_ERRORS_VNET0_INBOUND="0"       # errors/s
NETDATA_NET_ERRORS_VNET0_OUTBOUND="-0"       # errors/s
NETDATA_NET_ERRORS_VNET0_VISIBLETOTAL="0"       # errors/s
```

(continues on next page)

(continued from previous page)

```
# chart: net.vnet0 (name: net.vnet0)
NETDATA_NET_VNET0_RECEIVED="8"      # kilobits/s
NETDATA_NET_VNET0_SENT="1"      # kilobits/s
NETDATA_NET_VNET0_VISIBLETOTAL="9"      # kilobits/s

# chart: elasticsearch_gesmaster.cluster_stats_shards_total (name: elasticsearch_gesmaster.cluster_stats_shards_total)
NETDATA_ELASTICSEARCH_GESMASTER_CLUSTER_STATS_SHARDS_TOTAL_SHARDS="114"      # shards
NETDATA_ELASTICSEARCH_GESMASTER_CLUSTER_STATS_SHARDS_TOTAL_VISIBLETOTAL="114"      # shards

# chart: elasticsearch_gesmaster.cluster_stats_indices (name: elasticsearch_gesmaster.cluster_stats_indices)
NETDATA_ELASTICSEARCH_GESMASTER_CLUSTER_STATS_INDICES_INDICES="114"      # indices
NETDATA_ELASTICSEARCH_GESMASTER_CLUSTER_STATS_INDICES_VISIBLETOTAL="114"      # indices
```

8.10.1.2 Links associated

See the presentation of the *Data use*
The graphical interface is described in *`Netdata polling` screen*

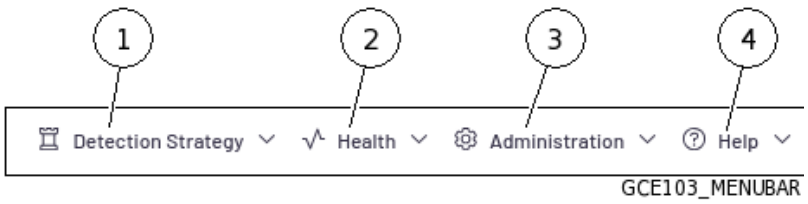
8.10.1.3 Prerequisites

- User: member of **Administrator** group

8.10.1.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

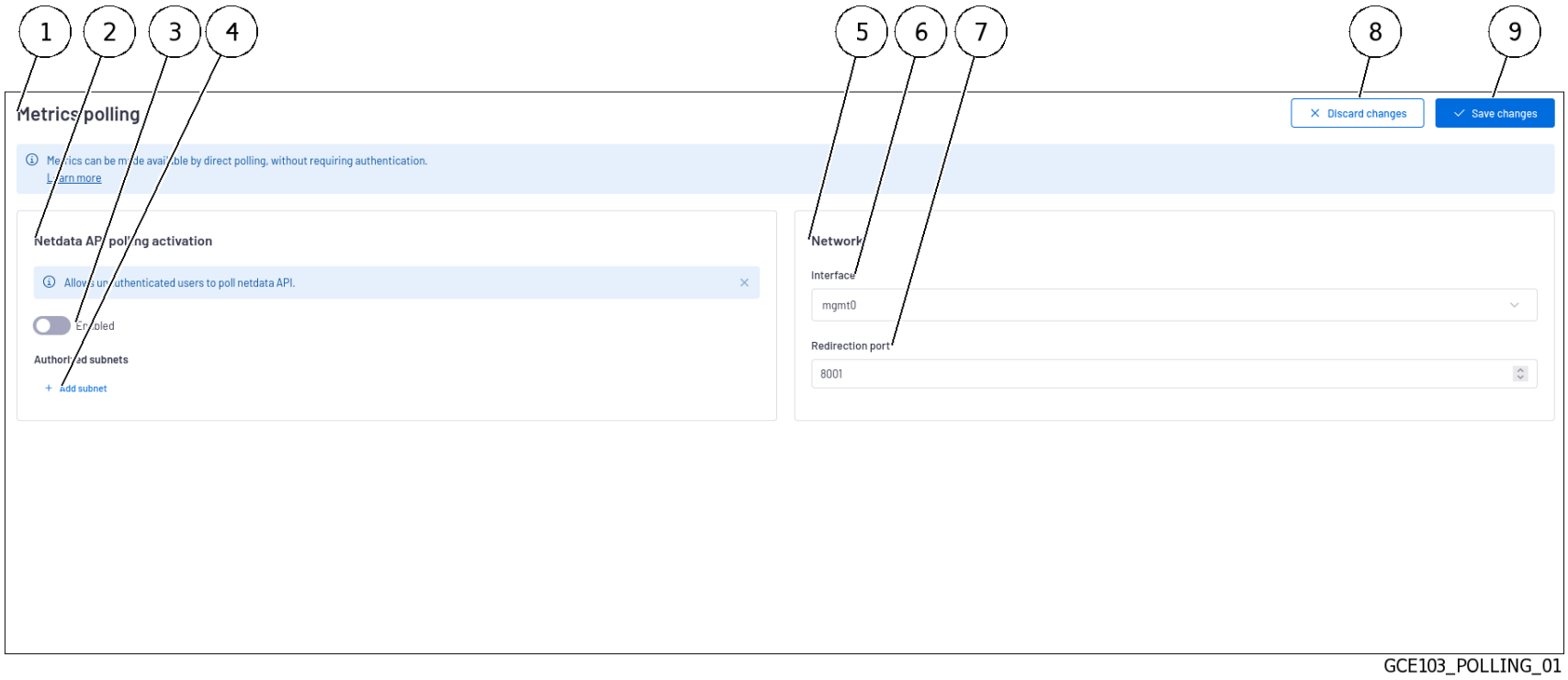
8.10.1.5 Procedure to access to the `Netdata polling` screen



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Metrics polling` command from the `Monitoring` submenu.
  The `Metrics polling` window is displayed.

8.10.1.6 Procedure to configure

The following screen is displayed:



GCE103_POLLING_01

- Use the `Enabled` selector (3) of the `Netdata API polling activation` zone (2).
- To add an IP address or subnet:

- Press on the `Add subnet` link (4)
- In the `ADD IP/MASK` window, enter the IP address then `/` then the mask
- Press on the `ADD` button

  The address entered is displayed in the `Authorized subnets` field.

- Select the GCenter input interface in the `Interface` field (6).
- Select the redirection port (7): default 8001
- Click on the `Save changes` button (9).

  If all is ok then the message `Success : Your data has been saved` is displayed.

8.10.2 Configuring the Netdata export interface

8.10.2.1 Introduction

This procedure describes the configuration of the Netdata interface to export system data to remote servers (Netdata, Nagios...).

8.10.2.2 Links associated

See the presentation of the *Data use*
The graphical interface is described in *`Netdata polling` screen*

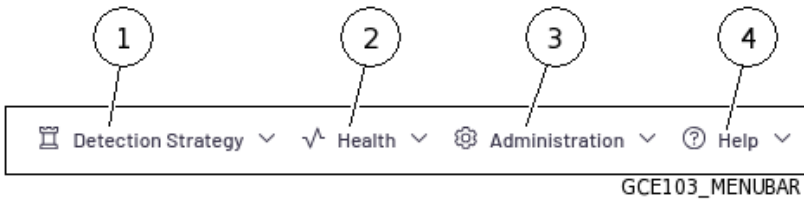
8.10.2.3 Prerequisites

- User: member of **Administrator** group

8.10.2.4 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.10.2.5 Procedure to access to the `Netdata Export Configuration` screen



- In the GCenter interface, click on the `Administration` menu (3).
- Click on the `Metrics Export` command from the `Monitoring` submenu.
  The `Metrics Export` window is displayed.

8.10.2.6 Procedure to configure

- Activate the `Enabled` selector (2) of the `Netdata export activation` zone (1).
- Enter the Netdata server FQDN or IP address in the `IP address or hostname` field (3).
- Enter the Netdata server API key in field (13).
- Select the network interface to use for this connection in the `Interface` (5).
- Select the Netdata server listening port (6).
- If necessary, enable the `Enabled`` selector (11) of the ```SSL` zone (12).
- If necessary, activate the `Verify CA` selector (10).
- If necessary, click on the `Upload CA file` button (9) to load the certificate file.
- Press on the `Save` button (8).

8.10.3 Setting up a Netdata server

8.10.3.1 Introduction

This procedure describes the installation of a Netdata monitoring server and its interconnection to a GCenter for monitoring purposes.

Note:

The Netdata version compatible with the GCenter and the GCap is 1.19

The configuration consists of:

- *Procedure to install via docker*
- *Procedure to configure stream.conf and GCenter*
- *Procedure to create alerts for Netdata*

8.10.3.2 Prerequisites

- User: member of **Administrator** group

8.10.3.3 Preliminary operations

- Login to GCenter via a browser (see *Connecting to the GCenter web interface via a web browser*)

8.10.3.4 Procedure to install via docker

- Enter the following command to install the Netdata docker.

```
docker pull netdata/netdata:v1.19.0
```

- Enter the following command to be able to edit the Netdata configuration from the host machine, you must launch a temporary container to retrieve the configuration files.

```
mkdir netdataconfig
docker run -d --name netdata_tmp netdata/netdata
docker cp netdata_tmp:/usr/lib/netdata netdataconfig/
docker rm -f netdata_tmp
```

- Enter the following command to launch the final container

```
docker run -d --name=netdata \
  -p 19999:19999 \
  -v $(pwd)/netdataconfig/netdata:/usr/lib/netdata:rw \
  -v netdatalib:/var/lib/netdata \
  -v netdatacache:/var/cache/netdata \
  -v /etc/passwd:/host/etc/passwd:ro \
  -v /etc/group:/host/etc/group:ro \
  -v /proc:/host/proc:ro \
  -v /sys:/host/sys:ro \
  -v /etc/os-release:/host/etc/os-release:ro \
  --restart unless-stopped \
  --cap-add SYS_PTRACE \
  --security-opt apparmor=unconfined \
  netdata/netdata
```

8.10.3.5 Procedure to configure stream.conf and GCenter

- Enter the following command to generate the uuid.

```
sudo docker exec -it netdata uuidgen
```

- Enter the following commands to configure stream with the uuid generated previously.
  Netdata recommends to use edit-config

```
sudo docker exec -it netdata /etc/netdata/edit-config stream.conf
```

```
[dd236090-a42d-43e2-b0ba-ff8eaa6216a2] << Remplacer l'uuid ici
    enabled = yes
    default history = 36000
    default memory mode = ram
    health enabled by default = auto
    allow from = *
    default postpone alarms on connect seconds = 60
```

- Enter the following commands to configure netdata.conf

```
sudo docker exec -it netdata /etc/netdata/edit-config netdata.conf
```

```
[global]
      ...
      hostname = netdata-docker.gatewatcher.com
      ...
      timezone = Europe/Paris
```

- Enter the following commands to configure the Netdata export in the GCenter.

> **Note:**
>
> Read the Netdata configuration parameters in the Netdata part visible in the *`Netdata Export Configuration` screen*.
> For Netdata to send notifications, configure the *health_alarm_notify.conf*

```
sudo docker exec -it netdata /etc/netdata/edit-config health_alarm_notify.conf
```

- See also the reference documentation : Alarm Configuration

8.10.3.6 Procedure to create alerts for Netdata

- Enter the following commands to create alerts in the container folder:

```
/usr/lib/netdata/conf.d/health.d
```

> **Note:**
>
> In order for the new alerts to be taken into account, it is necessary to restart the docker container.

- Enter the following commands to create your own alerts
  To clarify the management of alerts, it is advisable to create a *`*.conf`* file by alert category.
  Here are some examples:

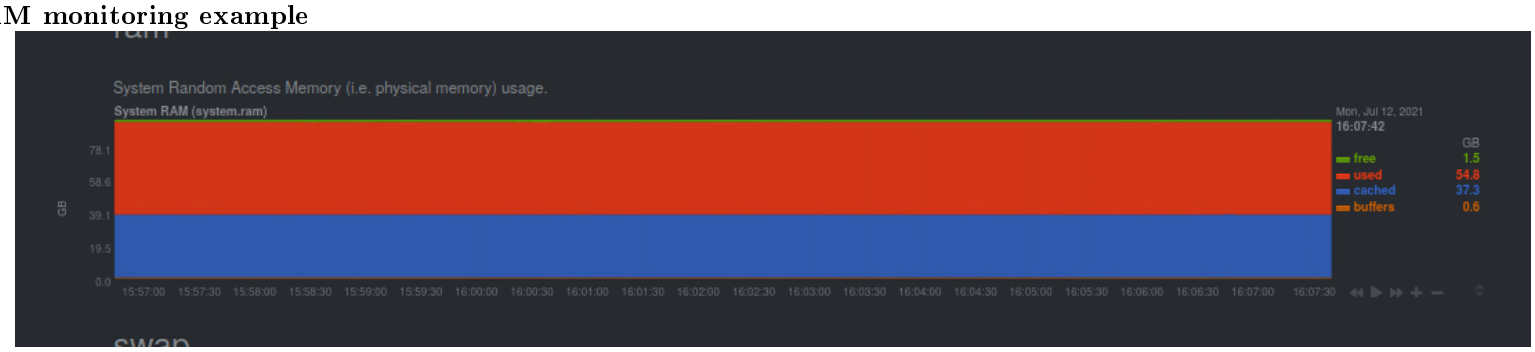
Description	Link
Alert in case of absence/traffic overload	`traffic.conf`
Alert in case of deactivation of the GCap analysis services	`suricata_status.conf`
Alert if a restart of Gcap/GCenter has occurred	`reboot.conf`
RAM overload alert	`ram.conf`
Alert in case of "dropped" network packets on the Gcap	`drop.conf`
Alert in case of disk filling (here the/data partition of the Gcap)	`disk.conf`
CPU overload alert	`cpu.conf`

The creation of alerts is based on the metrics that Netdata collects.

- To know these metrics, connect to the GCenter Netdata interface.

```
https:// IP ou FQDN du GCenter /gstats
```

RAM monitoring example



The name of the Graph is *system.ram*, and the curve to watch is *used*.
The alert in the *ram.conf* file will be written as follows:

- The alarm is named as follows:

```
1>>  alarm: ram_usage
```

- The alarm is named as follows:

```
2>> on: system.ram
```

- The 10 min average of the used curve is calculated as follows:

```
3>> lookup: average -10m percentage of used
```

- The unit is specified as follows:

```
4>> units: %
```

- The time interval between each calculation is specified as follows:

```
5>> every: 1m
```

- Alert and critical thresholds are specified as follows:

```
6>> warn: $this > 70
7>> crit: $this > 90
```

- The delay to clear the alarm after triggering is specified as follows:

```
8>> delay: down 15m multiplier 1.5 max 1h
```

- The alarm description is specified as follows:

```
9>> info: average RAM utilization over the last 10 minutes
```

- The definition that will be alerted (see health_alarm_notify.conf) is defined as follows:

```
10>> to: sysadmin
```

8.10.4 Using a Netdata server

8.10.4.1 Introduction

This procedure gives as an indication the steps necessary to set up a Netdata monitoring server, and its interconnection to a GCenter to ensure monitoring.

Note:

The Netdata version compatible with the GCenter and the GCap is 1.19

8.10.4.2 Prerequisites

- User: member of **Administrator** group

8.10.4.3 Procedure to install via docker

- Install the Netdata docker.

```
docker pull netdata/netdata:v1.19.0
```

- To be able to edit the Netdata configuration from the host machine, a temporary container must be launched to retrieve the configuration files.

```
mkdir netdataconfig
docker run -d --name netdata_tmp netdata/netdata
docker cp netdata_tmp:/usr/lib/netdata netdataconfig/
docker rm -f netdata_tmp
```

- Launch the final container.

```
docker run -d --name=netdata \
 -p 19999:19999 \
 -v $(pwd)/netdataconfig/netdata:/usr/lib/netdata:rw \
 -v netdatalib:/var/lib/netdata \
 -v netdatacache:/var/cache/netdata \
 -v /etc/passwd:/host/etc/passwd:ro \
 -v /etc/group:/host/etc/group:ro \
 -v /proc:/host/proc:ro \
 -v /sys:/host/sys:ro \
 -v /etc/os-release:/host/etc/os-release:ro \
 --restart unless-stopped \
 --cap-add SYS_PTRACE \
 --security-opt apparmor=unconfined \
 netdata/netdata
```

8.10.4.4 Procedure to configure the stream.conf file and GCenter

- Generate the uuid.

```
sudo docker exec -it netdata uuidgen
```

- Configure stream with the uuid generated previously.

  Netdata recommends using edit-config

```
sudo docker exec -it netdata /etc/netdata/edit-config stream.conf
```

```
[dd236090-a42d-43e2-b0ba-ff8eaa6216a2] << Remplacer l'uuid ici
    enabled = yes
    default history = 36000
    default memory mode = ram
    health enabled by default = auto
    allow from = *
    default postpone alarms on connect seconds = 60
```

8.10.4.5 Procedure to configure the netdata.conf file

```
sudo docker exec -it netdata /etc/netdata/edit-config netdata.conf
```

```
[global]
       ...
       hostname = netdata-docker.gatewatcher.com
       ...
       timezone = Europe/Paris
```

8.10.4.6 Procedure to configure the Netdata export in the GCenter

Note:

Read the *Setting up a Netdata server*.

- For Netdata to send notifications, the *health_alarm_notify.conf* ` file must be configured.

```
sudo docker exec -it netdata /etc/netdata/edit-config health_alarm_notify.conf
```

  Reference : Alarm Configuration

8.10.4.7 Procédure to create alerts for Netdata

- Create alerts in the container folder.

```
/usr/lib/netdata/conf.d/health.d
```

- In order for the new alerts to be taken into account, it is necessary to restart the docker container.
- To clarify the management of your alerts, it is advisable to create a *. conf* ` file by alert category.

  Examples include:

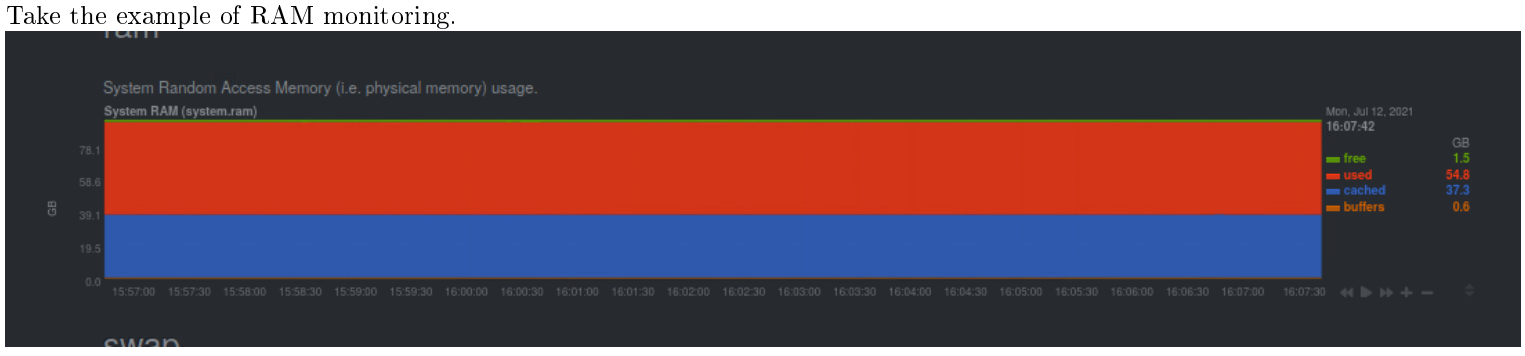
Description	Link
Alert in case of absence/traffic overload	`traffic.conf`
Alert in case of deactivation of the GCap analysis services	`suricata_status.conf`
Alert if a restart of the GCap/GCenter has occurred	`reboot.conf`
RAM overload alert	`ram.conf`
Alert in case of "dropped" network packets on the Gcap	`drop.conf`
Alert in case of disk filling (here the/data partition of the GCap)	`disk.conf`
CPU overload alert	`cpu.conf`

- Create your own alerts.

  The creation of alerts is based on the metrics that netdata collects.
  - To know these metrics, connect to the Netdata interface of the GCenter.

```
https:// IP or FQDN Gcenter /gstats
```

Take the example of RAM monitoring.



The Graph name is *system.ram* ` and the curve to watch is *used*.

- The alert in the *ram.conf* ` file will be written as follows:
  - The alarm is called

```
1>>  alarm: ram_usage
```

  - The chart is named in Netdata:

```
2>> on: system.ram
```

  - Indicates that the 10 min average of the *used* curve

```
3>> lookup: average -10m percentage of used
```

  - The unit is specified

```
4>> units: %
```

  - The time interval between each calculation is specified

```
5>> every: 1m
```

  - Alert and critical thresholds are defined

```
6>> warn: $this > 70
7>> crit: $this > 90
```

  - Set time to clear alarm after tripping

```
8>> delay: down 15m multiplier 1.5 max 1h
```

  - Description de l'alarme

```
9>> info: average RAM utilization over the last 10 minutes
```

  - Define who will be alerted (see health_alarm_notify.conf)

```
10>> to: sysadmin
```

8.11 Logging out of the GCenter web interface

8.11.1 Introduction

This procedure describes how to log out of the GCenter web interface.

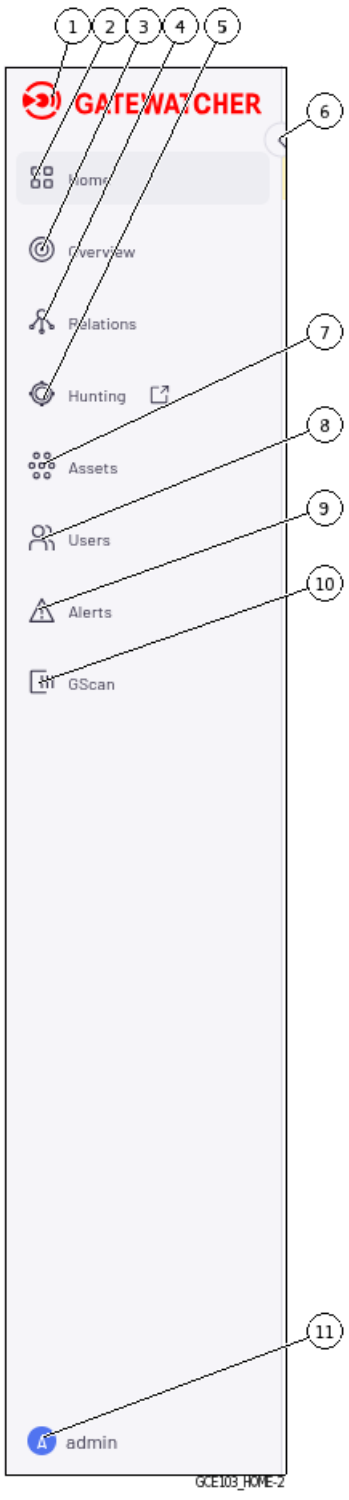
8.11.2 Prerequisites

- User: all users

8.11.3 Preliminary operations

- Accessing GCenter from your workstation (*Connecting to the GCenter web interface via a web browser*).

8.11.4 Procedure



- In the GCenter interface, click on the checking account button (11).
- Select the `Logout` command.
  The GCenter interface is closed and the login screen is displayed.

Chapter 9

Appendices

9.1 Military Programming Law (MPL)

9.1.1 Regulatory reminders

Some reminders of the main principles of the french Military Programming Law (MPL):

- Fench Military Programming Law (Act no. 2013-1168 of 18 December 2013)
- Article 22: implementation supervised by the ANSSI for the OIVs
  - Impose security measures,
  - Impose controls on the most critical information systems
  - Make it compulsory to report incidents observed by OIVs on their information systems
- Article L.1332-6-1 of the Defense Code amended by Act no. 2015-917 of 28 July 2015 - Art. 27
  - Establish organizational and technical measures
  - Define procedures for identifying and reporting security incidents affecting vital information systems (SIIV)

9.1.2 Goal Reminders

The objectives are :

- To protect national critical infrastructures against cyber attacks
- Reduce exposure to risks and
- Optimise the quality of services provided by organisations

9.1.3 Reminders of requirements

Requirements for OIVs and security incident detection service provider (PDIS) actors are to be taken into account on equipment:

- Implement an information systems security policy
- Carry out a security certification
- Communicate the elements on the IVIS set up by the operator to the ANSSI
- Observe and react to security alerts
- Limit access
- Partition the networks
- Select the qualified technologies

9.1.4 MPL applied to the GCenter

Note:

Whatever the mode, the AIONIQ solution integrates GRSECURITY improvements, including PaX, thus reducing the attack surface including at the kernel level.

The specific configuration points that allow the solution to comply with the Military Programming Law are presented here.
Although a number of actions are performed automatically when entering MPL mode, the administrator will have to customise and modify some of the parameters manually:

- AD/LDAP **manual action required**
- USB port **automatic action**
- Update in "Offline" mode **manual action required**
- Interface separation **manual action required**
- Certificate integration **manual action required**
- iDRAC Disabled **manual action required**
- The groups **manual action required**

9.1.4.1 Automatic actions

9.1.4.1.1 USB Port

Access via USB ports can involve risks.
When the AIONIQ solution is in MPL mode, the USB ports are automatically disabled

USB ports are automatically deactivated after switching to LPM mode from the **SETUP** profile settings configuration menu.
If a USB device is already plugged in, the port used will not deactivate until after disconnecting the present media.
In order for it to be supported again, you will need to restart the GCenter by reconnecting the device before booting.

Note:

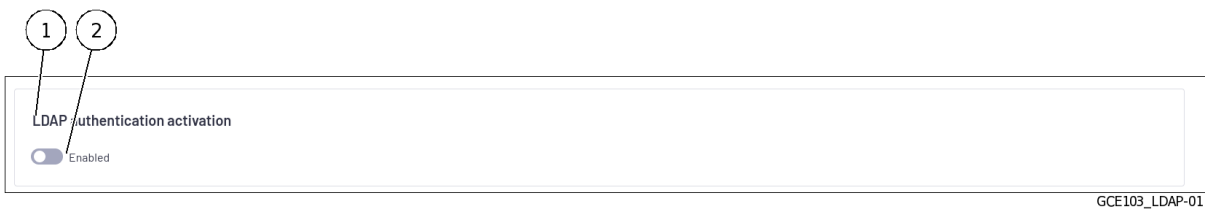
This limits access to the device's TTY.

9.1.4.2 Manual actions

The following list of actions should only be performed by an administrator of the AIONIQ solution.

9.1.4.2.1 No connection between GCenter and an LDAP

In the context of an IS subject to the MPL, there are certain constraints, in particular the fact that the GCenter is not connected to an Active Directory or LDAP.
It is necessary to check whether this is the case.
To do this, go to the ADMINISTRATORS section of the GCenter and click on Accounts and LDAP configuration.



GCE103_LDAP-01

In the `LDAP authentication settings` (2) area:

- Use the `Enable` selector (2) to deactivate the function.
- Click on the `Save changes` button.

This change will cause the application to restart, resulting in a disconnection from the user page.
Once the administrator clicks the `Confirm` button, it will be necessary to reconnect to the interface.

9.1.4.2.2 Deactivation of remote control console interface

The remote control console interface is made via a specific network connection.
This connection interface is called iDRAC at Dell (or TSM at Lenovo).

According to ANSSI, it is recommended to disable this interface for security reasons.
Under certain conditions, it can nevertheless be reactivated by the administrator to facilitate maintenance.

9.1.4.2.3 Network interface separation

As part of an IS subject to the LPM, the GCenter must have a special configuration of its network interfaces.
Indeed, in order to guarantee this compliance and a good level of security, the management flow and that of the interconnection with the GCap must be on two different interfaces respectively [MGMT0] and [VPN0].
This change is not effective automatically after LPM mode is enabled, even if the network cables are correctly connected.
It is precisely from the **SETUP** interface that the administrator can modify and manually add a new IP address for the [VPN0] interface.
Only the [MGMT0] and [VPN0] interfaces are impacted. Refer to the setup configuration document to make the change.
Details of flows in this mode are described in section *Interconnection between devices*.
For even more security, sending logs to a SIEM in an operating area can therefore be done through a dedicated interface by separating the management interface (administrator) from the log export interface (operator).

9.1.4.2.4 Update in "Offline" mode

In order for the AIONIQ solution to comply with the Military Programming Law, signature updates must be done in Manual or Local mode.
Therefore, there are two possibilities:

- Either from the **GCenter** web interface (see section *Local update*). This is a *manual* update.
- Or via a location on the network, disconnected from the internet, (see section *Manual Update*). This corresponds to an *Local* update.

9.1.4.2.4.1 Certificate integration

In order to comply with the specific requirements concerning the use of cryptographic mechanisms, GATEWATCHER advises referring to the documents written by the national authority on information system security and defense.
The Military Programming Law imposes rules and recommendations concerning the management of the keys used, authentication mechanisms, and the choice and sizing of cryptographic mechanisms.
All these prerequisites are available in the RGS General Security Reference (RGS B1, RGS B2, and RGS B3) of the ANSSI.

9.1.5 Groups

In order to respect the separation of roles on the GCenter, default groups are already created to facilitate user management:

- The operators group
- The administrators group

A user is therefore a member of one or both groups.
Profiles are managed from *`Users management` screen*.

9.1.5.1 Mission of a member of the operator group

A member of the operator group has as mission :

- Viewing of synthetic dashboards via the WebUI interface showing information about the monitored system
- Main dashboard (Home) to synthetically display alarms classified by level of risk
- Dashboard to display the network map. It shows the relationships between the elements present on the network
- Dashboards to display alarms classified by criteria (Users, Assets, Alerts) or by type of risk (Overview)
- Consultation of detailed dashboards via the Kibana interface showing the data information present in the detection event dashboards.
- Own account management
- Changing the checking account password
- Modification of certain information of the current user
- Sigflow engine configuration
- Management of SIGFLOW engine rule sources
- Creation of a ruleset of the SIGFLOW engine
- Modification of SIGFLOW engine rules
- Generation of SIGFLOW engine rulesets
- GCap configuration from the GCenter with GCaps Profiles
- Détection ruleset
- Base variables
- Net variables
- File rule management
- Packet filters

9.1.5.2 Mission of a member of the administrator group

A member of the administrator group is responsible for:

- NDR configuration, for example:
- Alerts displayed in the Alerts dashboard
- The equipment displayed in the Assets dashboard
- Users displayed in the Users dashboard
- Administrating a GCap, for example:
- Pairing a GCap with the GCenter
- Re-pairing a GCap
- Managing the GCenter backup and restoration, for example:
- Setting the backup
- Operating the backup
- Operating the restoration
- Managing of the GCenter software, for example:
- Configuring automatic update of signatures and/or anti-viral engines
- Installing an update manually
- Installing a hotfix
- Installing of an upgrade
- Administrating the GCenter
- Configuring the export data to a SIEM via the syslog protocol
- Configuring the export data to ETL Logstash via the syslog protocol
- Creating a POC Logstash
- Configuring the connection to the MISP
- Deleting data (log files)
- Generating and loading files for diagnosis
- Using an endpoint API
- Managing the license
- Configuring the GCenter
- Managing user accounts
- Creating local users
- Changing some of a local user's information
- Resetting a local user's password
- Deleting a local user
- Displaying of the connection status between the GCenter and the LDAP server
- Enabling the connection between the GCenter and the LDAP server
- Configuring the connection between the GCenter and the LDAP server
- Configuring the users and groups defined on LDAP / ActiveDirectory
- Viewing the authentication history
- Configuring the authentication history

- Managing an API access token
- Managing the password policy
- Configuring the detection engine
- Setting up the Malcore engine
- Managing the *Ignore list* of the Malcore engine
- Setting up the Malcore retroanalyzer engine
- Setting up the Yara engine
- Setting up the DGA detect engine
- Managing the *Ignore list* of the DGA detect engine
- Setting up the Malicious Powershell detect engine
- Setting up the Shellcode detect engine
- Setting up the Active CTI engine
- Setting up the retro hunt engine
- Setting up the Ransomware detect engine
- Managing the *Ignore list* of the Ransomware detect
- Setting up the beacon detect engine
- Managing the *Ignore list* of the Beacon detect
- Managing current user
- Changing the checking account password
- Changing some of the current user's information
- Monitoring the netdata
- Configuring the Netdata polling interface
- Configuring the Netdata export interface
- Setting up a Netdata server
- Using a Netdata server

9.2 Engine log data structure

The logs are composed of different parts:

- The header part
- The source part defined by "_source"
- The field part defined by "_fields"

9.2.1 Counters of the header part of logs

Table 1: Table header part of Malcore logs

Fields	Required	Description	Values or example
_index	Yes	Internal index	engines_alerts-2024.11.26-000022
_type	Yes	default type	_doc
_id	Yes	internal identifier	q5zQZ5MBe7GX5B2fx7DG
_version	Yes	internal version	1
_score	Yes	relevance of the response to the request	0

9.2.2 Counters of the source part of logs

9.2.2.1 beacon category

Level 1	Level 2	Data type	Description	Value or example
beacon	active	boolean	Beacon is active	true
beacon	hostname_resolution	string	Hostname resolution status	"not_analyzed"
beacon	id	string	unique identifier for the beaconing activity or signal	"c4c886b4ad"
beacon	mean_time_interval	numeric	Mean time interval between beacons	1
beacon	possible_cnc	string	Possible CNC	"not_recognized"
beacon	session_count	numeric	Session count	260
beacon	type	string	Type of beacon. unique identifier for the beaconing activity or signal	The type of connection. Can be user, token or nothing

---

9.2.2.2 DCERPC category

Level 1	Level 2	Level 3	Data type	Description	Value or example
dcerpc	call_id		numeric	unique identifier for RPC call	27
dcerpc	interfacesx[x]	ack_result		acknowledgment result of RPC interface call	
dcerpc	interfaces[x]	uuid		universally unique identifier for the RPC interface	
dcerpc	interfaces[x]	version		version of the RPC interface	
dcerpc	req	frag_cnt	numeric	number of fragments in the RPC request	1
dcerpc	req	opnum	numeric	operation number for the RPC request	4
dcerpc	req	stub_data_size	numeric	size of the stub data in the request	24
dcerpc	request	raw data of the RPC request	string		REQUEST
dcerpc	res	frag_cnt	numeric	number of fragments in the RPC response	1
dcerpc	res	stub_data_size	numeric	size of the stub data in the response	68
dcerpc	response	raw data of the RPC response	string		RESPONSE
dcerpc	rpc_version		string	version of the RPC protocol used	5.0

9.2.2.3 destination category

Level 1	Level 2	Data type	Description	Value or example
destination	ip	string	IP address of the destination	x.x.x.x
destination	mac	string	MAC address of the destination	90:e2:ba:a6:a4:91
destination	port	numeric	Port of the destination	19609

9.2.2.4 dga category

Level 1	Level 2	Data type	Description	Value or example
dga	dga_count	numeric	Number of DGAs	29
dga	dga_ratio	numeric	Ratio of DGAs (dga_count/nx_domain_count)	1
dga	malware_behavior_confidence	numeric	Malware behavior confidence in percent	50
dga	nx_domain_count	numeric	Number of NX domains analyzed	29
dga	top_DGA	string	Top DGAs based on score	tjzjyiheo.com", "nvtcvimt.com", "vmfyaxnse.com", "htjykhvta.com", "csmanuivsrlx.com", "sbxsgfddr.com", "oyttwuyshcgxxaenbit.com", "seklusaprnkwhvybzc.com", "xxcnirvbqivbucfsbliu.com", "jgjvgfetpammdrxwn.com"

9.2.2.5 DHCP category

Level 1	Level 2	Data type	Description	Value or example
dhcp	assigned_ip	string	IP address assigned by the DHCP server	192.168.1.2
dhcp	client_ip	string	Client IP address	x.y.z.a
dhcp	client_mac	string	Client MAC address	00:e0:ed:01:6e:bd
dhcp	dhcp_type	string	Type of dhcp message	
dhcp	dns_servers	string	List of DNS servers provided by DHCP	192.168.1.1
dhcp	hostname	string	Hostname of the client	d002465
dhcp	id	numeric	Id of the dhcp message	107809848
dhcp	lease_time	numeric	duration for which the DHCP lease is valid	3600
dhcp	params	numeric	Parameters of dhcp message	
dhcp	next_server_ip	string	IP address of the next DHCP server to contact	0.0.0.0
dhcp	relay_ip	string	IP address of the DHCP relay agent	0.0.0.0
dhcp	routers	string	list of routers/gateway addresses provided by DHCP	192.168.1.1
dhcp	subnet_mask	string	subnet mask assigned by the DHCP server	255.255.255.0
dhcp	type	string	Type of the dhcp message	Type of DHCP message (e.g. request, offer)

9.2.2.6 DNP3 category

Level 1	Level 2	Level 3	Level 4	Data type	Description	Value or example
dnp3	application	control	con	boolean		false
dnp3	application	control	fin	boolean		true
dnp3	application	control	fir	boolean		true
dnp3	application	control	sequence	numeric		7
dnp3	application	control	uns	boolean		false
dnp3	application	complete		boolean		true
dnp3	application	function_code		numeric		129
dnp3	application	objects	count	numeric		6
dnp3	application	objects	group	numeric		1
dnp3	application	objects	points. sub : - comm_lost - index - local_forced - online - prefix - remote_forced - reserved0 - reserved1 - restart - state	numeric		values: - 0 - 0 - 0 - 1 - 0 - 0 - 0 - 0 - 0 - 1
dnp3	application	objects	prefix_code	numeric		0
dnp3	application	objects	qualifier	numeric		0
dnp3	application	objects	range_code	numeric		0
dnp3	application	objects	start	numeric		0
dnp3	application	objects	stop	numeric		5
dnp3	application	objects	variation	numeric		1
dnp3	control	dir		boolean		false
dnp3	control	fcb		boolean		false
dnp3	control	fcv		boolean		false
dnp3	control	function_code		numeric		
dnp3	control	pri		boolean		true
dnp3	dst			numeric		3
dnp3	iin	indicators		array		[]
dnp3	src			numeric		4
dnp3	type			string		response

@Copyright: December 2024, Gatewatcher

9.2.2.7 DNS category

Level 1	Level 2	Level 3	Level 4	Data type	Description	Values or example
dns	answers	name		string	The domain name to which this resource record pertains.	ztqnmsruernxksa0l.com
dns	answers	data[0]	rdata	string	Resource Data (ex: IP that domain name resolves to)	
dns	answers	data[0]	rrname	string	Resource Record Name (ex: a domain name)	
dns	answers	data[0]	rrtype	string	Resource Record Type (ex: A, AAAA, NS, PTR)	
dns	answers	data[0]	tttl	string	Time-To-Live for this resource record	
dns	answers	type		string	The type of data contained in this resource record.	A
dns	authorities	rrname		string	name of the resource record in the authority section	com
dns	authorities	rrtype		string	type of the resource record in the authority section	SOA
dns	authorities	soa	expire	numeric	expiration time for the SOA (Start of Authority) record	604800
dns	authorities	soa	minimum	numeric	minimum TTL (Time to Live) for the SOA record	86400
dns	authorities	soa	mname	string	primary master name server in the SOA record	nstld.verisign-grs.com
dns	authorities	soa	refresh	numeric	refresh interval for the SOA record	1800
dns	authorities	soa	retry	numeric	retry interval for the SOA record	900
dns	authorities	soa	rname	string	responsible person's email address in the SOA record	a.gtld-servers.net
dns	authorities	soa	serial	numeric	serial number for the SOA record	1410273997
dns	authorities	ttl		numeric	Time to Live (TTL) for the authority section	5
dns	flags			string	Indicating DNS answer flag, in hexadecimal	8183
dns	grouped	A[0]		string	A record	
dns	id			numeric	The DNS packet identifier assigned by the program that generated the query. The identifier is copied to the response.	26738
dns	query	rrname		string		
dns	query	rrtype		string		A
dns	query	tx_id		numeric		193630
dns	query	opcode		numeric		0
dns	query	type		string		query
dns	query	id		numeric	The DNS packet identifier assigned by the program that generated the query. The identifier is copied to the response.	57318
dns	qr			boolean	Indicating in case of DNS answer flag, Query/Response flag (ex: true if set)	true
dns	ra			boolean	Indicating in case of DNS answer flag, Recursion Available flag (ex: true if set)	true
dns	rd			boolean	Indicating in case of DNS answer flag, Recursion Desired flag (ex: true if set)	true
dns	response_code		The DNS response code.	string	The DNS response code.	NXDOMAIN
dns	type			string	Indicating DNS message type, can be "answer" or "query"	answer
dns	version			numeric	Indicating DNS logging version in use	2

9.2.2.8 ecs category

Level 1	Level 2	Data type	Description	Value or example
ecs	version	numeric	ECS version this event conforms to	8.6.0

9.2.2.9 email category

Level 1	Level 2	Data type	Description	Value or example
email	attachments[0]	string	List of objects describing the attachments.	
email	body_md5		MD5 hash of the email body	
email	message_id		unique identifier for the email message	
email	status		Status of the email	
email	subject		The subject of the email message.	
email	subject_md5		MD5 hash of the email subject	
email	to.address[0]		Email address of recipient	

9.2.2.10 event category

Level 1	Level 2	Data type	Description	Value or example
event	category	string	file category network category intrusion_detection	file network intrusion_detection
event	created	date	Time when the event was first read by an agent or by your pipeline	2024-12-17T11:01:15.955324+00:00
event	dataset	string	Name of the dataset	alert
event	end	date		2024-12-17T11:00:05.717000+00:00
event	id	string	Unique ID to describe the event	28e92cac-b1de-4b20-ab71-5eeb325f64ed
event	kind	string	The kind of the event. The highest categorization field in the hierarchy	alert
event	module	string	Name of the module this data is coming from	Malcore or malcore_retroanalyzer, active_cti or ...
event	severity	numeric	Analysis result code	Between 0 and 3 0=clean 1=infected 2=suspicious 3=Other
event	severity_human	string	Analysis result	Suspicious
event	start	date		

9.2.2.11 ether category

Level 1	Level 2	Data type	Description	Value or example
ether	src_macs		source MAC address of the Ethernet frame	52:54:10:f5:71:63
ether	dest_macs		destination MAC address of the Ethernet frame	fa:2a:73:90:d5:3d

9.2.2.12 file category

Level 1	Level 2	Level 3	Data type	Description	Value or example
file	file_id		numeric	The file id	646
file	gaps		boolean	Monitoring inconsistency in file size	false
file	hash	md5	string	MD5 hash of the analyzed file	c279be702893....
file	hash	sha1	string	SHA1 of the analyzed file	
file	hash	sha256	string	SHA256sum of the analyzed file	4679e7f2018c19...
file	magic		string	File format identifier (Magic signature): detected by Sigflow using a reduced database.	Zip archive data, at least v2.0 to extract
file	name		string	Name of the file including the extension, without the directory	smtptest-2021-02-24T17-30-01Z.zip
file	sid		string	Alert ID. Must be unique.	1100043
file	size		numeric	File size in bytes	77068
file	state		string	Completeness of the analyzed file (CLOSED) otherwise TRUNCATED. The Sigflow file-store.stream-depth variable defines the size of the reconstructed files. The file is TRUNCATED if its size is > File-store stream depth (10 MB) by default.	CLOSED
file	stored		boolean	Still at "true", the file was stored on disk for further analysis	true
file	tx_id		numeric	transaction identification (query/response pair)	1

9.2.2.13 flow category

Level 1	Level 2	Data type	Description	Value or example
flow	bytes_toclient	numeric	Size of flow to customer	15280
flow	bytes_toserver	numeric	Size of flow to server	128
flow	pkts_toclient	numeric	Number of packets to client	12
flow	pkts_toserver	numeric	Number of packets to server	4
flow	start	date	Date and time of first package seen by Sigflow	2024-11-26T09:16:56.277148+0000

9.2.2.14 FTP category

Level 1	Level 2	Data type	Description	Value or example
ftp	command	string	FTP command issued by the client	EPSV
ftp	completion_code	string	FTP response code indicating the result of a command	229
ftp	dynamic_port	numeric	port used by FTP for dynamic data transfer (PASV mode)	1024
ftp	reply	string	FTP server's reply message to the client	"Extended Passive Mode OK (|||1024|)"
ftp	reply_received	string	timestamp when the FTP reply was received	yes
ftp	reply_truncated	boolean	indicates if the FTP reply was truncated	false

9.2.2.15 FTP data category

Level 1	Level 2	Data type	Description	Value or example
ftp_data	filename	string	name fo the file involved in FTP data transfer	README.txt
ftp_data	command	string	FTP command related to the data transfer (e.g. RETR, STOR)	RETR

9.2.2.16 HTTP category

Level 1	Level 2	Level 3	Level 4	Data type	Description	Value or example
http	accept			string	Accept header of the request	
http	accept_encoding			string	Accept encoding header of the request	"accept-encoding"
http	date			date	Date header of the request	"gzip, deflate"
http	hostname			string	The hostname this HTTP event is attributed to	tsevid-synonymi.justdanceatsea.com
http	http_port		port used for the HTTP connection	numeric	Port HTTP	8080
http	http_refer			string		"http://tsevid-synonymi.justdanceatsea.com:8080/ndf4xx22ci.php",
http	http_user_agent		referrer URL in the HTTP request	string	User agent of the request	
http	http2	request	priority	numeric	priority of the HTTP/2 request	15
http	http2	stream_id	stream ID in an HTTP/2 request/response	numeric		13
http	http2	response	HTTP/2 response sent by the server	numeric		{}
http	last_modified			string		
http	request	method		string	HTTP request method	"GET"
http	request	mime_type		string	Mime type of the body of the request.	
http	request_headers	name=	accept	string	acceptable content types in the HTTP request	"accept"
http	request_headers	value		string	value of the specific HTTP header ("/FireInstaller4.exe","GET","http", "nghttp2/1.43.0"..)	"/"
http	request_headers	name=	accept-encoding	string	encoding methods accepted by the client	
http	request_headers	name=	:authority	string	authority (host and port) in the HTTP/2 request	":authority"
http	request_headers	name=	:method	string	HTTP method (e.g., GET, POST)	:method
http	request_headers	name=	:path	string	path of the resource in the HTTP requests	":path"
http	request_headers	name=	:scheme	string	URI scheme (e.g. HTTP, HTTPS)	":scheme"
http	request_headers	name=	user-agent	string	client's user agent information	"user-agent"
http	response	bytes		numeric	Total size in bytes of the response (body and headers)	77068
http	response	mime_type	HTTP response status code	string	Mime type of the body of the response	application/x-shockwave-flash

continues on next page

Table 17 – continued from previous page

Level 1	Level 2	Level 3	Level 4	Data type	Description	Value or example
http	response	status		numeric	HTTP response code 1xx informational response – the request was received, continuing process 2xx successful – the request was successfully received, understood, and accepted 3xx redirection – further action needs to be taken in order to complete the request 4xx client error – the request contains bad syntax or cannot be fulfilled 5xx server error – the server failed to fulfil an apparently valid request	200
http	response_headers	name=	accept-ranges	string	indicates if the server supports range requests	
http	response_headers	name=	content-length	string	length of the response body	
http	response_headers	name=	content-type	string	type of the content returned in the response	
http	response_headers	name=	date	string	date and time the response was sent	
http	response_headers	name=	etag	string	entity tag for caching validation	
http	response_headers	last_modified	etag	string	entity tag for the last modified version of the resource	
http	response_headers	last_modified	server	string	server providing the last modified resource	
http	response_headers	last_modified	status	string	status of the HTTP response	
http	response_headers	value		string		
http	server	value		string	Server header of the request	
http	url			string	URL of the request	
http	version			string	HTTP version	HTTP/1.1

9.2.2.17 HTTP2 category

Level 1	Level 2	Level 3	Level 4	Data type	Value or example
http2	http_method			string	GET
http2	http_user_agent			string	nghttp2/1.43.0
http2	http2	request	priority	numeric	15
http2	http2	stream_id		numeric	13
http2	http2	response		string	{}
http2	http2	length		numeric	3663
http2	request_headers	name=	accept	string	
http2	request_headers	value		string	/
http2	request_headers	name=	accept-encoding	string	
http2	request_headers	value		string	gzip, deflate
http2	request_headers	name=	:authority	string	
http2	request_headers	value		string	10.2.10.205
http2	request_headers	name=	:method	string	
http2	request_headers	value		string	GET
http2	request_headers	name=	:path	string	
http2	request_headers	value		string	/3k.zip
http2	request_headers	name=	:scheme	string	
http2	request_headers	value		string	http
http2	request_headers	name=	user-agent	string	
http2	request_headers	value		string	15
http2	response_headers	name=	accept-ranges	string	
http2	response_headers	value		string	bytes
http2	response_headers	name=	content-length	string	

continues on next page

Table 18 – continued from previous page

Level 1	Level 2	Level 3	Level 4	Data type	Value or example
http2	response_headers	value		string	3663
http2	response_headers	name=	content-type	string	
http2	response_headers	value		string	text/plain
http2	response_headers	name=	date	string	
http2	response_headers	value		string	Mon, 08 Jan 2024 15:28:50 GMT
http2	response_headers	name=	etag	string	
http2	response_headers	value		string	"659c131d-e4f"
http2	response_headers	last_modified	etag	string	
http2	response_headers	value		string	Mon, 08 Jan 2024 15:22:05 GMT
http2	response_headers	last_modified	server	string	
http2	response_headers	value		string	nginx/1.25.2
http2	response_headers	last_modified	:status	string	
http2	response_headers	value		string	200
http2	status			numeric	200
http2	url			string	/3k.zip
http2	version			string	2

9.2.2.18 IKEV2 category

Level 1	Level 2	Data type	Description	Value or example
ikev2	alg_auth	numeric	Authentication algorithm	"AUTH_HMAC_SHA1_96"
ikev2	alg_dh	string	Diffie-Hellman group	"2048-bit MODP Group"
ikev2	alg_enc	string	Encryption algorithm	"ENCR_AES_CBC"
ikev2	alg_esn	string	Extended Sequence Numbers	"NoESN"
ikev2	alg_perf	string	Pseudo-Random Function	"PRF_HMAC_SHA1"
ikev2	errors	numeric	Number of errors	0
ikev2	exchange_type	numeric	IKEv2 exchange type	34
ikev2	init_spi	string	Initiator's SPI	"605830378bec4174"
ikev2	message_id	boolean	Message ID	0
ikev2	notify	string	Notify message	["NAT_DETECTION_SOURCE_IP", "NAT_DETECTION_DESTINATION_IP", "IKEV2_FRAGMENTATION_SUPPORTED", "MULTIPLE_AUTH_SUPPORTED"]
ikev2	payload	string	Payload type	["SecurityAssociation", "KeyExchange", "Nonce", "Notify", "Notify", "Notify", "Notify", "NoNextPayload"]
ikev2	resp_spi	string	Responder's SPI	"5afa8990956d8af0"
ikev2	role	string	Role of the participant	"responder"
ikev2	version_major	numeric	Major version	2
ikev2	version_minor	numeric	Minor version	0

9.2.2.19 ioc category

Level 1	Level 2	Level 3	Data type	Description	Value or example
ioc	id		numeric		
ioc	campaigns		string	The campaigns of the IOC	
ioc	case_id		string	The case id of the IOC	aa8d51ed-0883-4b12-8b43
ioc	categories		string	The categories of the IOC	trojan malware
ioc	creation_date		date	The creation date of the IOC	2025-01-28T08:02:50+00:00
ioc	description		string	The description of the IOC	eb4db30601b1f4babefa4...' is a Suspicious SHA256.nThis SHA256 is linked to a trojan attack.nWe advised to use this IoC in detection mode.
ioc	external_links	source_name	string	The external links of the IOC	
ioc	external_links	url	string		"url": "https://info.gatewatcher.com/fr/speed-meeting-lastinfosec", "source_name": "IOCAnalysisCollector"
ioc	families		string	The families of the IOC	
ioc	id		string		e9a6f382-d06b-490f-9b6e
ioc	kill_chain_phases		string	The kill chain phases of the IOC	
ioc	meta_data	cwe	string		
ioc	meta_data	descriptions	string		
ioc	meta_data	usageMode	string		"descriptions": [], "usageMode": "detection", "cwe": []
ioc	package_date		date	The package date of the IOC	025-01-28T08:50:04.124404+00:00
ioc	relations		string	The uuid related to the IOC	"0e3cc27b-7999-48ce-8484", "5556c4ab-3e5e-4d56-8410"
ioc	signature		string	The signature of the IOC	SHA256 - trojan/malware - Unknown family - Unknown threat actor - e9a6f3
ioc	tags		string	The tags of the IOC	"trojan.generickd.66527077", "troj/drodzp-cf", "trojan.generickd.66527077 (b)", "trojan/generickd!vemnohoo"
ioc	targeted_countries		string	The targeted countries of the IOC	
ioc	targeted_organizations		string	The targeted organizations of the IOC	
ioc	targeted_platforms		string	The targeted platforms of the IOC	
ioc	targeted_sectors		string	The targeted sectors of the IOC	Services - Autres
ioc	threat_actor		string	The threat actor of the IOC	
ioc	tlp		string	The color based level of the IOC	green
ioc	ttp		string	The tactics, techniques, and procedures of the IOC	
ioc	type		string	The type of the IOC	SHA256
ioc	updated_date		date	The updated date of the IOC	2025-01-28T08:04:31+00:00
ioc	usage_mode		string	The usage mode of the IOC	detection
ioc	value		string	The value of the IOC	eb4db357dc6f2dd8facf132ecafd...
ioc	vulnerabilities		string	The vulnerabilities of the IOC	

@Copyright: December 2024, Gatewatcher

9.2.2.20 krb5 category

Level 1	Level 2	Data type	Description	Value or example
krb5		string		cli-krb5
krb5	encryption	string	encryption	aes256-cts-hmac-sha1-96
krb5	msg_type	string	msg_type	KRB_AS_REP
krb5	realm	string	the Kerberos Realm	GATEWATCHER.COM
krb5	sname	string	sname	krbtgt/GATEWATCHER.COM
krb5	weak_encryption	boolean	weak_encryption	false

9.2.2.21 malcore category

Level 1	Level 2	Level 3	Level 4	Data type	Description	Value or example
malcore	analyzed_clean			numeric	GEYEGO: Number of engines with result CLEAN	0
malcore	analyzed_error			numeric	GEYEGO: Number of engines with result in FAILED, CLEANED_OR_DELETED, SCAN_SKIPPED_WHITELIST, SCAN_SKIPPED_BLACKLIST, NOT_SCANNED, CANCELED, UNSUPPORTED_FILE_TYPE, IN_PROGRESS	0
malcore	analyzed_infected			numeric	GEYEGO: Number of engines with result INFECTED	9
malcore	analyzed_other			numeric	GEYEGO: Number of engines with result other results than the one described above	7
malcore	analyzed_suspicious			numeric	GEYEGO: Number of engines with result SUSPICIOUS	0
malcore	analyzers_up		MALCORE: Total number of engines used for this analysis	numeric	Total number of engines used for analysis	16
malcore	code			numeric	Usually. Can be forced to SCAN_SKIPPED_BLACKLIST(8) or SCAN_SKIPPED_WHITELIST(7) if filtered or NOT_SCANNED(10) if file is lost. See the table Malcore engine results (*Malcore engine results*)	1
malcore	detail_scan_time			numeric	File analysis time (ms) by malcore engines	245
malcore	detail_threat_found			string	Comma separated list of detected threat names	"Infected: EICAR-Test-File (not a virus) (B)....
malcore	detail_wait_time			numeric	Time elapsed between sending the file to the node and receiving the engine result in milliseconds	1096
malcore	engine_id	0-15		numeric	unique identifier for a Malcore engine (0 to 15)	4
malcore	engine_id	0-15	id	string	engine id	b557a5r
malcore	engine_id	0-15	scan_result	string	analysis result (INFECTED, UNSUPPORTED_FILE_TYPE, NOT_SCANNED or CLEAN)	INFECTED
malcore	engine_id	0-15		string	threat_details	EICAR-Test-File (not a virus) (B)
malcore	engines_last_update_date			date	GEYEGO: median last update time of all analyzers used.	2023-07-11T11:32:00Z

continues on next page

Table 22 – continued from previous page

Level 1	Level 2	Level 3	Level 4	Data type	Description	Value or example
malcore	file_type			string	MALCORE: file type.	application/zip
malcore	file_type_description			string	MALCORE: file type, but longer.	ZIP Archive
malcore	magic_details			string	GEYEGO: Lib magic result	Zip archive data, at least v2.0 to extract
malcore	processing_time			numeric		1341
malcore	reporting_token			string	GEYEGO: GBOX analysis token, if available	GBOX#
malcore	state			string	Result is "Infected" as soon as the result of an engine is "Infected"	Infected
malcore	total_found			string	GEYEGO: string presenting <infected>/<total number>	XX/YY with YY between 0 and 16 and XX between 0 and YY; example 9/16

9.2.2.22 malcore_retroanalyzer category

Level 1	Level 2	Level 3	Level 4	Data type	Description	Value or example
malcore_retroanalyzer	analyzed_clean			numeric	GEYEGO: Number of engines with result CLEAN	0
malcore_retroanalyzer	analyzed_error			numeric	GEYEGO: Number of engines with result in FAILED, CLEANED_OR_DELETED, SCAN_SKIPPED_WHITELIST, SCAN_SKIPPED_BLACKLIST, NOT_SCANNED, CANCELED, UNSUPPORTED_FILE_TYPE, IN_PROGRESS	0
malcore_retroanalyzer	analyzed_infected			numeric	GEYEGO: Number of engines with INFECTED result	9
malcore_retroanalyzer	analyzed_other			numeric	GEYEGO: Number of engines with result other results than the one described above	7
malcore_retroanalyzer	analyzed_suspicious			numeric	GEYEGO: Number of engines with result SUSPICIOUS	0
malcore_retroanalyzer	analyzers_up			numeric	MALCORE: Total number of engines used for this analysis	16
malcore_retroanalyzer	code			numeric	Can be forced to SCAN_SKIPPED_BLACKLIST(8) or SCAN_SKIPPED_WHITELIST(7) if filtered or NOT_SCANNED(10) if file is lost. See the table Malcore engine results (*Malcore engine results*)	1
malcore_retroanalyzer	detail_scan_time			numeric	Analysis time of the files (ms) by the malcore engines	245
malcore_retroanalyzer	detail_threat_found			string	List of detected threat names, separated by commas	"Infected: EICAR-Test-File (not a virus) (B)....
malcore_retroanalyzer	detail_wait_time			numeric	MALCORE: process_info.processing_time_details.others_time_process_info_	1096
malcore_retroanalyzer	engine_id			numeric	malcore engine number (0 to 15)	4
malcore_retroanalyzer	engine_id	0-15	id	string	engine id	b557a5r
malcore_retroanalyzer	engine_id	0-15	scan_result	string	analysis result (INFECTED or CLEAN)	INFECTED
malcore_retroanalyzer	engine_id	0-15	threat_details	string	treat details of the result for this engine	EICAR-Test-File (not a virus) (B)
malcore_retroanalyzer	engines_last_update_date			date	GEYEGO: median last update time of all analyzers used.	2023-07-11T11:32:00Z

continues on next page

Table 23 – continued from previous page

Level 1	Level 2	Level 3	Level 4	Data type	Description	Value or example
malcore_retroanalyzer	file_type			string	MALCORE: file type.	application/zip
malcore_retroanalyzer	file_type_description			string	MALCORE: file type, but longer.	ZIP Archive
malcore_retroanalyzer	magic_details			string	GEYEGO: Lib magic result	Zip archive data, at least v2.0 to extract
malcore_retroanalyzer	processing_time			numeric		1341
malcore_retroanalyzer	reporting_token			string	GEYEGO: GBOX analysis token, if available	GBOX#
malcore_retroanalyzer	state			string	The result is "Infected" as soon as the result of a motor is "Infected"	Infected
malcore_retroanalyzer	total_found			string	GEYEGO: string presenting <infected>/<total number>	XX/YY with YY between 0 and 16 and XX between 0 and YY; example 9/16

9.2.2.23 malicious_powershell category

Level 1	Level 2	Level 3	Data type	Description	Value or example
malicious_powershell	id		string	MD5 of the file	b5c38e2159f80a5a3076a353360cb5f1
malicious_powershell	proba_obfuscated		numeric	probability of obfuscation	0.6
malicious_powershell	sample_id (id)		string	file id	12-04-2024T14:12:40_03afe38854c8443db03-gatewatcher.com",
malicious_powershell	score		numeric	score of the PowerShell script	332
malicious_powershell	score_details	AddContent	numeric	Adds content to a file/folder	0
malicious_powershell	score_details	Base64	numeric	Score represented by an integer of a/patterns base64 detected	188
malicious_powershell	score_details	CharInt	numeric	Score represented by an integer of one/of the detected charitable patterns	6
malicious_powershell	score_details	FmtStr	numeric	Score represented by an integer of a/of detected fmtstr patterns	8
malicious_powershell	score_details	GetContent	numeric	Get-Content applet to read file data	0
malicious_powershell	score_details	InvokeExpression	numeric	InvokeExpression Applet	100
malicious_powershell	score_details	InvokeRestMethod	numeric		0
malicious_powershell	score_details	InvokeWebRequest	numeric	Invoke-WebRequest applet sends HTTP and HTTPS requests to a webpage	0
malicious_powershell	score_details	SetContent	numeric	Applet SetContent writes new content or replaces existing content in a file	0
malicious_powershell	score_details	StartBitsTransfer	numeric	Start-BitsTransfer Order	0
malicious_powershell	score_details	StrCat	numeric	Function that concatenates strings	4
malicious_powershell	score_details	StreamReader	numeric	Object to read and display each directory name	0
malicious_powershell	score_details	StreamWriter	numeric	Write a file that lists directories	0
malicious_powershell	score_details	StrJoin	numeric	Score represented by an integer of a/strjoin patterns detected	6
malicious_powershell	score_details	StrReplace	numeric	Score represented by an integer of a/strreplace patterns detected	0
malicious_powershell	score_details	SystemIOFile	numeric	Manipulation of a file (creation, opening, copy, etc.)	0
malicious_powershell	score_details	WebClientInvokation	numeric	Score represented by an integer of one/of detected webclientinvokation patterns	20

9.2.2.24 matched_event category

Level 1	Level 2	Data type	Description	Value or example
matched_event	id	numeric	The ID of the matched event	
matched_event	content	string	Content all categories of the matched event	

9.2.2.25 metadata category

Level 1	Level 2	Data type	Description	Value or example
metadata	flowbits	string		min.gethttp

9.2.2.26 MQTT category

Level 1	Level 2	Level 3	Data type	Description	Value or example
mqtt	connack	dup	boolean		false
mqtt	connack	qos	numeric		0
mqtt	connack	retain	boolean		false
mqtt	connack	return_code	numeric		0
mqtt	connack	session_present	boolean		false

9.2.2.27 nba category

Level 1	Level 2	Level 3	Data type	Description	Value or example
nba	action		string		
nba	category		string		
nba	gid		numeric		
nba	metadata	performance_impact	string		
nba	metadata	signature_severity	string		
nba	packet		string		
nba	payload		string		
nba	payload_printable		string		
nba	rev		numeric		
nba	signature		string		
nba	signature_id		numeric		
nba	stream		numeric		

9.2.2.28 netflow category

Level 1	Level 2	Data type	Description	Value or example
netflow	pkts	numeric	Packets of the flow	1
netflow	age	numeric	Age of the flow	0
netflow	end	date	End time of the flow	2024-09-12T15:00:07.959357+0000
netflow	min_ttl	numeric	Minimum TTL of the flow	255
netflow	bytes	numeric	Bytes of the flow	62
netflow	start	date	Start time of the flow	2024-09-12T15:00:07.959357+0000
netflow	max_ttl	numeric	Maximum TTL of the flow	255

9.2.2.29 network category

Level 1	Level 2	Data type	Description	Value or example
network	community_id	string	hash of source and destination IPs and ports, as well as the protocol used in a communication	1:r6LvcE7ltny4a6Y9xt1Vr...
network	flow_id	numeric	Flow identifier	363747525458479
network	protocol	string	Application Layer protocol. For example, http, dns, or ssh	http
network	timestamp	date	Date and time of alert generation by Sigflow	2024-11-26T09:17:00.775521+0000
network	transport	string	name of the transport layer (udp, tcp, ipv6-icmp, etc.)	tcp
network	tx_id	numeric	transaction identification (query/response pair)	0

9.2.2.30 NFS category

Level 1	Level 2	Data type	Description	Value or example
nfs	filename	string		""
nfs	file_tx	boolean		true
nfs	hhash	string	Hash of the file	87b5a66e
nfs	id	numeric	ID of the NFS event	1
nfs	procedure	string	NFS procedure	WRITE
nfs	status	string	Status of the NFS event	OK
nfs	type	string	Type of the NFS event	response
nfs	version	numeric	NFS version	4

9.2.2.31 observer category

Level 1	Level 2	Level 3	Level 4	Data type	Description	Value or example
observer	gcap	hostname		string	The hostname of the gcap	gcap-xxx.domain.local
observer	gcap	ingress	interface/name	string	GCap input interface used for capture (monx or monvirt)	monvirt
observer	gcap	version		string	The version of the gcap	"2.5.4"
observer	hostname			string	Hostname of the observer	"gcenter.domain",
observer	log_format_version			string	The log format version	"1.0.0"
observer	product			string	The product name of the observer	gcenter
observer	uuid			string	Unique identifier of the alert	f639c844-3f6f-40fa-86c4-47ff603880e2
observer	vendor			string	Vendor name of the observer	gatewatcher
observer	version			string	Observer version	"2.5.x."

9.2.2.32 ransomware events

Level 1	Level 2	Data type	Description	Value or example
ransomware	alert_threshold	numeric	The alert threshold	930
ransomware	malicious_behavior_confidence	numeric	Malicious behavior confidence in percent	80
ransomware	session_score	numeric	The session score	35

9.2.2.33 RDP category

Level 1	Level 2	Level 3	Data type	Description	Value or example
rdp	channels		string	The optional channel field is a list of requested data channel names	["rdpdr", "cliprdr", "rdpsnd"]
rdp	client	build	string		"Windows XP"
rdp	client	capabilities	string	features and capabilities supported by the RDP client	["support_errinfo_pdf"]
rdp	client	client_name	string	name of the RDP client	"ISD2-KM84178"
rdp	client	color_depth	numeric	color depth supported by the RDP client	15
rdp	client	desktop_height	numeric	height of the desktop displayed by the RDP client	
rdp	client	desktop_width	numeric	width of the desktop displayed by the RDP client	864
rdp	client	function_keys	numeric	function keys supported or configured by the RDP client	12
rdp	client	id	string	unique identifier for the RDP client session	"55274-OEM-0011903-00107"
rdp	client	keyboard_layout	string	keyboard layout used by the RDP client	"en-US"
rdp	client	keyboard_type	string	type of keyboard supported by the RDP client	"enhanced"
rdp	client	product_id	numeric	product ID for the RDP client software	1
rdp	client	version	string	version number of the RDP client	"v5"
rdp	event_type		string	The event_type field indicates an RDP event subtype. Possible values: initial_request,initial_response,connect_request,connect_response,tls_handshake	"connect_request"
rdp	protocol			The protocol field is the selected protocol. Possible values: rdp, ssl, hybrid, rds_tls, hybrid_ex	
rdp	server_supports[0]			The optional server_supports field is a list of server capabilities	
rdp	tx_id		numeric	Each RDP record contains a per-flow incrementing tx_id field	2

9.2.2.34 RFB category

Level 1	Level 2	Level 3	Level 4	Data type	Description	Value or example
rfb	authentication	security_type		numeric	type of security method used during RFB (Remote Framebuffer) authentication	2
rfb	authentication	vnc	challenge	string	challenge sent by the VNC server during authentication	"435414a03f719e3bab73fd2de5"
rfb	authentication	vnc	response	string	response sent by the VNC client to the authentication challend	"50e93126e93f23a52"
rfb	client_protocol_version	major		string	major version of the protocol used by the RFB client	"003"
rfb	client_protocol_version	minor		string	minor version of the protocol used by the RFB client	"008"
rfb	server_protocol_version	major		string	major version of the protocol used by the RFB server	"003"
rfb	server_protocol_version	minor		string	minor version of the protocol used by the RFB server	"008"
rfb	server_security_failure_reason			string	reason for security failure during RFB server authentication	"Authentication failed from 192.168.0.1"

9.2.2.35 rpc category

Level 1	Level 2	Level 3	Data type	Description	Value or example
rpc	creds	gid		group ID associated with the RPC credentials	
rpc	creds	machine_name		name of the machine that initiated the RPC request	
rpc	creds	uid	numeric	user ID associated with the RPC credentials	35
rpc	status		string	status of the RPC call	ACCEPTED
rpc	xid		numeric	transaction ID for the RPC request, used for matching requests and responses	1299444754

9.2.2.36 Shellcode category

Level 1	Level 2	Level 3	Data type	Description	Value or example
Shellcode	analysis	args	string	The args of the call	"{'pathname': '//etc/passwd', 'flags': 'O_WRONLY|O_APPEND', 'mode': 'None'}",
Shellcode	analysis	call	string	The call	sys_open
Shellcode	analysis	info	string	More info	"Stop : End of Shellcode (Exit)"
Shellcode	analysis	ret	string	The retention	0
Shellcode	analysis	_id	numeric	The id of the analysis	-1
Shellcode	analysis	stop	numeric	The stop	End of Shellcode (output)
Shellcode	encodings	count	numeric	The count of the encoding	1
Shellcode	encodings	name	string	The name of the encoding	"Shikata_ga_nai",
Shellcode	encodings	options	string	available encoding options used to encode shellcode	
Shellcode	id		string	The id of the Shellcode	8ae5f9d35f3878cace4c311d"
Shellcode	sample_id		string	The sample id of the Shellcode	12-04-2024T14:17:25_925...c1c7_gcap-int-xxx.gatewatcher.com
Shellcode	sub_type		string	The sub type of the Shellcode	"Linux_x86_32",

9.2.2.37 sigflow category

Level 1	Level 2	Level 3	Data type	Description	Value or example
sigflow	action		string	The action of the signature flow	alert, drop, reject, pass "action": "allowed"
sigflow	category		string	The category of the signature flow	Potentially Bad Traffic" Active CTI
sigflow	gid		numeric	The gid of the signature flow	1
sigflow	metadata	affected_product	string		
sigflow	metadata	attack_target	string		
sigflow	metadata	confidence	string		
sigflow	metadata	created_at	string	Created at YEAR_MONTH_DAY	2014_11_15
sigflow	metadata	deployment	string		
sigflow	metadata	ioc	string		fffc7e75-cb75-4210-..
sigflow	metadata	malware_family	string		
sigflow	metadata	performance_impact	string	Performance impact	Significant
sigflow	metadata	reviewed_at	string		
sigflow	metadata	risk	string		highly suspicious
sigflow	metadata	signature_severity	string	Signature severity	2
sigflow	metadata	updated_at	string	Updated at YEAR_MONTH_DAY	2024_04_22
sigflow	packet		string	The packet of the signature flow	kOK6pqSQkOK...
sigflow	packet_info	linktype	numeric	Type of link-layer header	1
sigflow	payload		string	The payload of the signature flow	Potentially Bad Traffic
sigflow	payload_printable		string	The printable payload of the signature flow	GET /emd.exe HTTP/1.1rnHost: opred.netrnConnection: Keep-Alivernrn
sigflow	rev		numeric	The revision of the signature flow	11

continues on next page

Table 38 – continued from previous page

Level 1	Level 2	Level 3	Data type	Description	Value or example
sigflow	signature		string	The signature of the signature flow	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile",
sigflow	signature_id		numeric	The signature id of the signature flow	2019714
sigflow	stream		numeric	The stream of the signature flow	0

9.2.2.38 SIP category

Level 1	Level 2	Data type	Description	Value or example
sip	code	string		"183"
sip	reason	string		"In band info available"
sip	response_line	string		"SIP/2.0 183 In band info available"
sip	version	string		"SIP/2.0"

9.2.2.39 SMB category

Level 1	Level 2	Data type	Description	Value or example
smb	client_dialects[0]	string		
smb	client_guid	string		
smb	command	string	command name	"SMB2_COMMAND_SESSION_LOGOFF"
smb	dialect	string	The negotiated protocol dialect, or “unknown” if missing	3.11
smb	filename	string	filename for CREATE and other commands.	
smb	fuid	string	SMB2+ file GUID. SMB1 FID as hex.	
smb	id	numeric	internal transaction id	12
smb	max_read_size	numeric		
smb	max_write_size	numeric		
smb	session_id	numeric	SMB2+ session_id. SMB1 user id	593737889611
smb	server_guid	string		
smb	share	string		
smb	status	string	status string. Can be both NT_STATUS or DOS_ERR and other variants	STATUS_SUCCESS
smb	status_code	string	status code as hex string	0x0
smb	tree_id	numeric	Tree ID	0

9.2.2.40 SMTP category

Level 1	Level 2	Data type	Description	Value or example
smtp	helo	string	the HELO command sent by the SMTP client to initiate communication	qal-internet.internet
smtp	mail_from	string	the sender’s email address in the MAIL FROM command	
smtp	rcpt_to	string	the recipient’s email address in the RCPT TO command	

9.2.2.41 SNMP category

Level 1	Level 2	Data type	Description	Value or example
snmp	community	string		""
snmp	pdu_type	string		"set_request"
snmp	vars	string		["1.3.6.1.2.1.1.5.0"]
snmp	version	numeric		1

9.2.2.42 source category

Level 1	Level 2	Data type	Description	Value or example
source	ip	string	Source IP address detected by Sigflow	x.y.z.A"
source	mac	string	MAC address of the source network card	xx....
source	port	numeric	Source port detected by Sigflow	8080

9.2.2.43 SSH category

Level 1	Level 2	Level 3	Level 4	Data type	Description	Value or example
ssh	client	hassh		string		
ssh	client	proto_version		string		2.0
ssh	client	software_version		string		OpenSSH_7.4p1
ssh	server	hassh	hash	string		b12d1a1189eff264cf533361ee
ssh	server	hassh		string		curve25519-sha256, ... umac-64@openssh.com,umac-128@oppenssh.com
ssh	server	proto_version		string		2.0
ssh	server	software_version		string		abbix_agent

9.2.2.44 tcp category

Level 1	Level 2	Data type	Description	Value or example
tcp	ack	boolean		
tcp	fin	boolean		
tcp	psh	boolean		
tcp	rst	boolean		
tcp	syn	boolean		
tcp	tcp_flags	string		

9.2.2.45 TFTP category

Level 1	Level 2	Data type	Description	Value or example
tftp	file	string		rfc1350.txt
tftp	mode	string		"octet"
tftp	packet	string		"read"

9.2.2.46 TLS category

Level 1	Level 2	Level 3	Level 4	Data type	Value or example
tls	client	server_name		string	qacrcgtyzm.com
tls	ja3	hash		string	
tls	ja3	string		string	
tls	ja3s	hash		string	
tls	ja3s	string		string	
tls	serial			string	
tls	server	certificate	chain	string	MIIDjBCVBAYv2NFV7jMvdyoO...
tls	server	hash	md5	string	
tls	server	hash	sha1	string	29:d8:c7:2d:fa:30:26:5f:92:e8:2c:e6:62:e2:40
tls	server	hash	sha256	string	
tls	server	issuer		string	C=US, ST=USA, L=NY, O=Company Ltd, OU=office, CN=web
tls	server	not_after		date	2024-08-30T15:56:58
tls	server	not_before		date	2014-09-02T15:56:58
tls	server	subject		string	C=US, ST=USA, L=NY, O=Company Ltd, OU=office, CN=web
tls	sni			string	
tls	version			string	TLSv1

9.2.2.47 url category

Level 1	Level 2	Data type	Description	Value or example
url	domain	string	The domain of the URL	"tsevid-synonymi.justdanceatsea.com"
url	full	string	The full URL	
url	path	string	The path of the URL	/6SuCHKKkf8Sf1aFXJPqD0R6r3oEDCrbwHFm23E...

9.2.2.48 user_agent category

Level 1	Level 2	Data type	Description	Value or example
user_agent	original	string	The user agent of the software used	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; ...)

9.2.2.49 @timestamp category

Level 1	Level 2	Data type	Description	Value or example
@timestamp		string	Date/time when the event was generated by the source.	2023-10-09T08:31:04.503Z
@timestamp	dest_macs	string		

9.2.2.50 @version

Level 1	Data type	Description	Value or example
@version	numeric		1

9.3 Comparison of the counters between V02 and V103

9.3.1 Beacon detect engine

This engine appeared in version 103 so this section is not applicable

---

9.3.2 Malcore engine

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
analyzed_clean	malcore.analyzed_clean	modified
analyzed_error	malcore.analyzed_error	modified
analyzed_infected	malcore.analyzed_infected	modified
analyzed_other	malcore.analyzed_other	modified
analyzed_suspicious	malcore.analyzed_suspicious	modified
analyzers_up	malcore.analyzers_up	modified
app_proto	network.protocol	modified
code	malcore.code	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
detail_scan_time	malcore.detail_scan_time	modified
detail_threat_found	malcore.detail_threat_found	modified
detail_wait_time	malcore.detail_wait_time	modified
engine_id.0.id	malcore.engine_id.0.id	modified
engine_id.0.scan_result	malcore.engine_id.0.scan_result	modified
engine_id.0.threat_details	malcore.engine_id.0.threat_details	modified
engine_id.1.id	malcore.engine_id.1.id	modified
engine_id.1.scan_result	malcore.engine_id.1.scan_result	modified
engine_id.1.threat_details	malcore.engine_id.1.threat_details	modified
engine_id.10.id	malcore.engine_id.10.id	modified
engine_id.10.scan_result	malcore.engine_id.10.scan_result	modified
engine_id.10.threat_details	malcore.engine_id.10.threat_details	modified
engine_id.11.id	malcore.engine_id.11.id	modified
engine_id.11.scan_result	malcore.engine_id.11.scan_result	modified
engine_id.11.threat_details	malcore.engine_id.11.threat_details	modified
engine_id.12.id	malcore.engine_id.12.id	modified
engine_id.12.scan_result	malcore.engine_id.12.scan_result	modified
engine_id.12.threat_details	malcore.engine_id.12.threat_details	modified
engine_id.13.id	malcore.engine_id.13.id	modified
engine_id.13.scan_result	malcore.engine_id.13.scan_result	modified
engine_id.13.threat_details	malcore.engine_id.13.threat_details	modified
engine_id.14.id	malcore.engine_id.14.id	modified
engine_id.14.scan_result	malcore.engine_id.14.scan_result	modified
engine_id.14.threat_details	malcore.engine_id.14.threat_details	modified
engine_id.15.id	malcore.engine_id.15.id	modified
engine_id.15.scan_result	malcore.engine_id.15.scan_result	modified
engine_id.15.threat_details	malcore.engine_id.15.threat_details	modified
engine_id.2.id	malcore.engine_id.2.id	modified
engine_id.2.scan_result	malcore.engine_id.2.scan_result	modified
engine_id.2.threat_details	malcore.engine_id.2.threat_details	modified
engine_id.3.id	malcore.engine_id.3.id	modified
engine_id.3.scan_result	malcore.engine_id.3.scan_result	modified
engine_id.3.threat_details	malcore.engine_id.3.threat_details	modified
engine_id.4.id	malcore.engine_id.4.id	modified
engine_id.4.scan_result	malcore.engine_id.4.scan_result	modified
engine_id.4.threat_details	malcore.engine_id.4.threat_details	modified
engine_id.5.id	malcore.engine_id.5.id	modified
engine_id.5.scan_result	malcore.engine_id.5.scan_result	modified
engine_id.5.threat_details	malcore.engine_id.5.threat_details	modified
engine_id.6.id	malcore.engine_id.6.id	modified
engine_id.6.scan_result	malcore.engine_id.6.scan_result	modified
engine_id.6.threat_details	malcore.engine_id.6.threat_details	modified
engine_id.7.id	malcore.engine_id.7.id	modified
engine_id.7.scan_result	malcore.engine_id.7.scan_result	modified
engine_id.7.threat_details	malcore.engine_id.7.threat_details	modified
engine_id.8.id	malcore.engine_id.8.id	modified
engine_id.8.scan_result	malcore.engine_id.8.scan_result	modified

continues on next page

Table 52 – continued from previous page

2.5.3.102	2.5.3.103	state
engine_id.8.threat_details	malcore.engine_id.8.threat_details	modified
engine_id.9.id	malcore.engine_id.9.id	modified
engine_id.9.scan_result	malcore.engine_id.9.scan_result	modified
engine_id.9.threat_details	malcore.engine_id.9.threat_details	modified
engines_last_update_date	malcore.last_update_date	modified
event_type		hardly_modified
file_type	malcore.file_type	modified
file_type_description	malcore.file_type_description	modified
fileinfo.file_id	file.file_id	modified
fileinfo.filename	file.name	modified
fileinfo.gaps	file.gaps	modified
fileinfo.magic	file.magic	modified
fileinfo.md5	file.hash.md5	modified
fileinfo.sha1	file.sha1	modified
fileinfo.sha256	file.hash.sha256	modified
fileinfo.sid[0]	file.sid[0]	modified
fileinfo.size	file.size	modified
fileinfo.state	file.state	modified
fileinfo.stored	file.stored	modified
fileinfo.tx_id	file.tx_id	modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
http.accept	http.accept	same
http.accept_encoding	http.accept_encoding	same
http.content_type	http.response.mime_type	modified
http.date	http.date	same
http.hostname	http.hostname	same
http.http_content_type	http.request.mime_type	modified
http.http_method	http.request.method	
http.http_user_agent	user_agent.original	modified
http.server	http.server	same
http.status	http.response.status	modified
http.url	url.path	modified
in_iface	observer.gcap.ingress.interface.name	modified
magic_details	malcore.magic_details	modified
processing_time	malcore.processing_time	modified
proto	network.transport	modified
reporting_token	malcore.reporting_token	modified
severity	event.severity	modified
SHA256		removed
src_ip	source.ip	modified
src_port	source.port	modified
state	malcore.state	modified
timestamp		hardly_modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
total_found	malcore.total_found	modified
type		removed
uuid	observer.uuid	modified
	url.domain	added
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.category[1]	added
	event.id	added
	event.kind	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.3 DGA engine

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
type		removed
event_type		hardly_modified
uuid	observer.uuid	modified
matched_event	event.id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
dest_port	destination.port	modified
src_port		hardly_modified
src_ip	source.ip	modified
dest_ip	destination.ip	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
flow_id	network.flow_id	modified
severity	event.severity	modified
probability	dga.dga_ratio	modified
domain_name		hardly_modified
	ecs.version	added
	event.dataset	added
	event.end	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.category[1]	added
	event.start	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	network.transport	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added
	dga.nx_domain_count	added
	dga.top_DGA[0]	added
	dga.top_DGA[1]	added
	dga.top_DGA[2]	added
	dga.top_DGA[3]	added
	dga.top_DGA[4]	added
	dga.top_DGA[5]	added
	dga.top_DGA[6]	added
	dga.top_DGA[7]	added
	dga.top_DGA[8]	added
	dga.top_DGA[9]	added
	dga.dga_count	added
	dga.malware_behavior_confidence	added

9.3.4 Malicious powershell engine

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
dest_ip	destination.ip	modified
dest_port	destination.port	modified
event_type		hardly_modified
file_id	malicious_powershell.sample_id	modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
MD5	malicious_powershell.id	modified
scores.analysis	malicious_powershell.score	modified
scores.analysis_detailed.AddContent	malicious_powershell.score_details.AddContent	modified

continues on next page

Table 54 – continued from previous page

2.5.3.102	2.5.3.103	state
scores.analysis_detailed.Base64	malicious_powershell.score_details.Base64	modified
scores.analysis_detailed.CharInt	malicious_powershell.score_details.CharInt	modified
scores.analysis_detailed.FmtStr	malicious_powershell.score_details.FmtStr	modified
scores.analysis_detailed.GetContent	malicious_powershell.score_details.GetContent	modified
scores.analysis_detailed.InvokeExpression	malicious_powershell.score_details.InvokeExpression	modified
scores.analysis_detailed.InvokeRestMethod	malicious_powershell.score_details.InvokeRestMethod	modified
scores.analysis_detailed.InvokeWebRequest	malicious_powershell.score_details.InvokeWebRequest	modified
scores.analysis_detailed.SetContent	malicious_powershell.score_details.SetContent	modified
scores.analysis_detailed.StartBitsTransfer	malicious_powershell.score_details.StartBitsTransfer	modified
scores.analysis_detailed.StrCat	malicious_powershell.score_details.StrCat	modified
scores.analysis_detailed.StreamReader	malicious_powershell.score_details.StreamReader	modified
scores.analysis_detailed.StreamWriter	malicious_powershell.score_details.StreamWriter	modified
scores.analysis_detailed.StrJoin	malicious_powershell.score_details.StrJoin	modified
scores.analysis_detailed.StrReplace	malicious_powershell.score_details.StrReplace	modified
scores.analysis_detailed.SystemIOFile	malicious_powershell.score_details.SystemIOFile	modified
scores.analysis_detailed.WebClientInvokation	malicious_powershell.score_details.WebClientInvokation	modified
scores.proba_obfuscated	malicious_powershell.proba_obfuscated	modified
severity	event.severity	modified
SHA256		removed
src_ip	source.ip	modified
src_port	source.port	modified
state		removed
sub_type		removed
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.category[1]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	network.transport	added
	observer.gcap.version	added
	observer.gcap.ingress.interface.name	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.5 Shellcode engine

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
calls.0.args	shellcode.analysis[0].args	modified
calls.0.call	shellcode.analysis[0].call	modified
calls.0.ret	shellcode.analysis[0].ret	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
encodings[0].count	shellcode.encodings[0].count	modified
encodings[0].name	shellcode.encodings[0].count	modified
event_type		hardly_modified
file_id	shellcode.sample_id	modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
MD5	shellcode.id	modified
severity	event.severity	modified
SHA256		removed
src_ip	source.ip	modified

continues on next page

Table 55 – continued from previous page

2.5.3.102	2.5.3.103	state
src_port	source.port	modified
state		removed
sub_type	shellcode.sub_type	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.category[1]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	network.transport	added
	observer.gcap.version	added
	observer.gcap.ingress.interface.name	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.6 Ransomware detect engine

This engine appeared in version 103 so this section is not applicable

9.3.7 Sigflow alert

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
type		removed
event_type		hardly_modified
proto	network.transport	modified
uuid	observer.uuid	modified
src_port	source.port	modified
dest_port	destination.port	modified
src_ip	source.ip	modified
dest_ip	destination.ip	modified
ether.src_mac	source.mac	modified
ether.dest_mac	destination.mac	modified
community_id	network.community_id	modified
in_iface	observer.gcap.ingress.interface.name	modified
gcap	observer.gcap.hostname	modified
host		removed
gcenter	observer.hostname	modified
flow_id	network.flow_id	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
flow.pkts_toclient	flow.pkts_toclient	same
flow.bytes_toclient	flow.bytes_toclient	same
flow.pkts_toserver	flow.pkts_toserver	same
flow.bytes_toserver	flow.bytes_toserver	same
flow.start	flow.start	same
http.http_user_agent	user_agent.original	modified
http.protocol	http.version	modified
http.length	http.response.bytes	modified
http.http_content_type	http.response.mime_type	modified
http.http_method	http.request.method	modified
http.hostname	http.hostname	same
http.url	url.path	modified

continues on next page

Table 56 – continued from previous page

2.5.3.102	2.5.3.103	state
http.status	http.response.status	modified
	url.domain	added
payload	sigflow.payload	modified
payload_printable	sigflow.payload_printable	modified
alert.signature	sigflow.signature	modified
alert.rev	sigflow.rev	modified
alert.gid	sigflow.gid	modified
alert.severity		removed
alert.action	sigflow.action	modified
alert.category	sigflow.category	modified
alert.signature_id	sigflow.signature_id	modified
alert.metadata.created_at[0]	sigflow.metadata.created_at[0]	modified
alert.metadata.updated_at[0]	sigflow.metadata.updated_at[0]	modified
stream	sigflow.stream	modified
severity	event.severity	modified
tx_id	network.tx_id	modified
packet_info.linktype	sigflow.packet_info.linktype	modified
packet	sigflow.packet	modified
app_proto	network.protocol	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.category[1]	added
	event.id	added
	event.kind	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.8 Sigflow dcerpc

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
dcerpc.call_id	dcerpc.call_id	same
dcerpc.interfaces[0].ack_result	dcerpc.interfaces[0].ack_result	same
dcerpc.interfaces[0].uuid	dcerpc.interfaces[0].uuid	same
dcerpc.interfaces[0].version	dcerpc.interfaces[0].version	same
dcerpc.interfaces[1].ack_result	dcerpc.interfaces[1].ack_result	same
dcerpc.interfaces[1].uuid	dcerpc.interfaces[1].uuid	same
dcerpc.interfaces[1].version	dcerpc.interfaces[1].version	same
dcerpc.request	dcerpc.request	same
dcerpc.response	dcerpc.response	same
dcerpc.rpc_version	dcerpc.rpc_version	same
dest_ip	destination.ip	modified
dest_port	destination.port	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added

continues on next page

Table 57 – continued from previous page

2.5.3.102	2.5.3.103	state
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.9 Sigflow DGA

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
dest_ip	destination.ip	modified
dest_port	destination.port	modified
domain_name		hardly_modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
matched_event	event.id	modified
probability	dga.dga_ratio	modified
severity	event.severity	modified
src_ip	source.ip	modified
src_port		hardly_modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.end	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.category[1]	added
	event.start	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	network.transport	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added
	dga.nx_domain_count	added
	dga.top_DGA[0]	added
	dga.top_DGA[1]	added
	dga.top_DGA[2]	added
	dga.top_DGA[3]	added
	dga.top_DGA[4]	added
	dga.top_DGA[5]	added
	dga.top_DGA[6]	added
	dga.top_DGA[7]	added
	dga.top_DGA[8]	added
	dga.top_DGA[9]	added
	dga.dga_count	added
	dga.malware_behavior_confidence	added

@Copyright: December 2024, Gatewatcher

9.3.10 Sigflow dhcp

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
dhcp.assigned_ip	dhcp.assigned_ip	same
dhcp.client_ip	dhcp.client_ip	same
dhcp.client_mac	dhcp.client_mac	same
dhcp.dhcp_type	dhcp.dhcp_type	same
dhcp.hostname	dhcp.hostname	same
dhcp.id	dhcp.id	same
dhcp.params[0]	dhcp.params[0]	same
dhcp.params[1]	dhcp.params[1]	same
dhcp.params[2]	dhcp.params[2]	same
dhcp.params[3]	dhcp.params[3]	same
dhcp.params[4]	dhcp.params[4]	same
dhcp.type	dhcp.type	same
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.11 Sigflow dnp3

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
dnp3.application.complete	dnp3.application.complete	same
dnp3.application.control.con	dnp3.application.control.con	same
dnp3.application.control.fin	dnp3.application.control.fin	same
dnp3.application.control.fir	dnp3.application.control.fir	same
dnp3.application.control.sequence	dnp3.application.control.sequence	same
dnp3.application.control.uns	dnp3.application.control.uns	same
dnp3.application.function_code	dnp3.application.function_code	same
dnp3.control.dir	dnp3.control.dir	same
dnp3.control.fcb	dnp3.control.fcb	same

continues on next page

Table 60 – continued from previous page

2.5.3.102	2.5.3.103	state
dnp3.control.fcv	dnp3.control.fcv	same
dnp3.control.function_code	dnp3.control.function_code	same
dnp3.control.pri	dnp3.control.pri	same
dnp3.dst	dnp3.dst	same
dnp3.iin.indicators[0]	dnp3.iin.indicators[0]	same
dnp3.src	dnp3.src	same
dnp3.type	dnp3.type	same
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.12 Sigflow dns

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
dns.answers[0].rdata	dns.answers.data[0].rdata	modified
dns.answers[0].rrname	dns.answers.data[0].rrname	modified
dns.answers[0].rrtype	dns.answers.data[0].rrtype	modified
dns.answers[0].ttl	dns.answers.data[0].ttl	modified
dns.flags	dns.flags	same
dns.grouped.A[0]	dns.grouped.A[0]	same
dns.id	dns.id	same
dns.qr	dns.qr	same
dns.ra	dns.ra	same
dns.rcode	dns.response_code	modified
dns.rd	dns.rd	same
dns.type	dns.type	same
dns.version	dns.version	same
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified

continues on next page

Table 61 – continued from previous page

2.5.3.102	2.5.3.103	state
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.13 Sigflow file

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
app_proto	network.protocol	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
event_type		hardly_modified
fileinfo.file_id	file.file_id	modified
fileinfo.filename	file.name	modified
fileinfo.gaps	file.gaps	modified
fileinfo.magic	file.magic	modified
fileinfo.md5	file.hash.md5	modified
fileinfo.sha1	file.sha1	modified
fileinfo.sha256	file.hash.sha256	modified
fileinfo.sid[0]	file.sid[0]	modified
fileinfo.size	file.size	modified
fileinfo.state	file.state	modified
fileinfo.stored	file.stored	modified
fileinfo.tx_id	file.tx_id	modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
http.hostname	http.hostname	same
http.http_content_type	http.response.mime_type	modified
http.http_method	http.request.method	modified
http.http_user_agent	user_agent.original	modified
http.length	http.response.bytes	modified
http.protocol	http.version	modified
http.status	http.response.status	modified
http.url	url.path	modified
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	url.domain	added
	ecs.version	added
	event.dataset	added

continues on next page

Table 62 – continued from previous page

2.5.3.102	2.5.3.103	state
	event.module	added
	event.created	added
	event.category[0]	added
	event.category[1]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.14 Sigflow ftp

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
ftp.completion_code[0]	ftp.completion_code[0]	same
ftp.reply_received	ftp.reply_received	same
ftp.reply_truncated	ftp.reply_truncated	same
ftp.reply[0]	ftp.reply[0]	same
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
tx_id	network.tx_id	modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.15 Sigflow ftp data

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
ftp_data.command	ftp_data.command	same
ftp_data.filename	ftp_data.filename	same
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
parent_id	parent_id	same
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
tx_id	network.tx_id	modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.16 Sigflow http

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
http.accept	http.accept	same
http.accept_encoding	http.accept_encoding	same
http.content_type	http.response.mime_type	modified
http.date	http.date	same
http.hostname	http.hostname	same
http.http_content_type	http.request.mime_type	modified
http.http_method	http.request.method	
http.http_parsed_user_agent.device	user_agent.device.name	modified
http.http_parsed_user_agent.name	user_agent.name	modified
http.http_parsed_user_agent.os	user_agent.os.family	modified

continues on next page

Table 65 – continued from previous page

2.5.3.102	2.5.3.103	state
http.http_parsed_user_agent.os_full	user_agent.os.full	modified
http.http_parsed_user_agent.os_name	user_agent.os.name	modified
http.http_user_agent	user_agent.original	modified
http.last_modified	http.last_modified	modified
http.length	http.response.bytes	modified
http.protocol	http.version	modified
http.server	http.server	same
http.status	http.response.status	modified
http.url	url.path	modified
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
tx_id	network.tx_id	modified
type		removed
uuid	observer.uuid	modified
	url.domain	added
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.17 Sigflow http2

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
http.http_method	http.request.method	
http.http_parsed_user_agent.device	user_agent.device.name	modified
http.http_parsed_user_agent.name	user_agent.name	modified
http.http_parsed_user_agent.os	user_agent.os.family	modified
http.http_parsed_user_agent.os_full	user_agent.os.full	modified
http.http_parsed_user_agent.os_name	user_agent.os.name	modified
http.http_user_agent	user_agent.original	modified
http.http2.request.priority	http.http2.request.priority	same
http.http2.stream_id	http.http2.stream_id	same
http.length	http.response.bytes	modified
http.request_headers[0].name	http.request_headers[0].name	same
http.request_headers[0].value	http.request_headers[0].value	same
http.request_headers[1].name	http.request_headers[1].name	same
http.request_headers[1].value	http.request_headers[1].value	same
http.response_headers[0].name	http.response_headers[0].name	same
http.response_headers[0].value	http.response_headers[0].value	same
http.response_headers[1].name	http.response_headers[1].name	same

continues on next page

Table 66 – continued from previous page

2.5.3.102	2.5.3.103	state
http.response_headers[1].value	http.response_headers[1].value	same
http.status	http.response.status	modified
http.url	url.path	modified
http.version	http.version	same
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
tx_id	network.tx_id	modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.18 Sigflow ikev2

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
ikev2.errors	ikev2.errors	same
ikev2.exchange_type	ikev2.exchange_type	same
ikev2.init_spi	ikev2.init_spi	same
ikev2.message_id	ikev2.message_id	same
ikev2.notify[0]	ikev2.notify[0]	same
ikev2.notify[1]	ikev2.notify[1]	same
ikev2.payload[0]	ikev2.payload[0]	same
ikev2.payload[1]	ikev2.payload[1]	same
ikev2.payload[10]	ikev2.payload[10]	same
ikev2.payload[2]	ikev2.payload[2]	same
ikev2.payload[3]	ikev2.payload[3]	same
ikev2.payload[4]	ikev2.payload[4]	same
ikev2.payload[5]	ikev2.payload[5]	same
ikev2.payload[6]	ikev2.payload[6]	same
ikev2.payload[7]	ikev2.payload[7]	same
ikev2.payload[8]	ikev2.payload[8]	same
ikev2.payload[9]	ikev2.payload[9]	same
ikev2.resp_spi	ikev2.resp_spi	same
ikev2.role	ikev2.role	same
ikev2.version_major	ikev2.version_major	same
ikev2.version_minor	ikev2.version_minor	same
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified

continues on next page

Table 67 – continued from previous page

2.5.3.102	2.5.3.103	state
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.19 Sigflow krb5

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
type		removed
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
krb5.cname	krb5.cname	same
krb5.encryption	krb5.encryption	same
krb5.msg_type	krb5.msg_type	same
krb5.realm	krb5.realm	same
krb5.sname	krb5.sname	same
krb5.weak_encryption	krb5.weak_encryption	same
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.20 Sigflow mqtt

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
dest_ip	destination.ip	modified
dest_port	destination.port	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
mqtt.connack.dup	mqtt.connack.dup	same
mqtt.connack.qos	mqtt.connack.qos	same
mqtt.connack.retain	mqtt.connack.retain	same
mqtt.connack.return_code	mqtt.connack.return_code	same
mqtt.connack.session_present	mqtt.connack.session_present	same
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.21 Sigflow netflow

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
app_proto	network.protocol	modified
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	ether.dest_macs[0]	modified
ether.src_mac	ether.src_macs[0]	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
netflow.age	netflow.age	same
netflow.bytes	netflow.bytes	same
netflow.end	netflow.end	same
netflow.max_ttl	netflow.max_ttl	same
netflow.min_ttl	netflow.min_ttl	same
netflow.pkts	netflow.pkts	same
netflow.start	netflow.start	same
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified

continues on next page

Table 70 – continued from previous page

2.5.3.102	2.5.3.103	state
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added
	tcp.ack	added
	tcp.syn	added
	tcp.tcp_flags	added
	tcp.psh	added

9.3.22 Sigflow nfs

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
nfs.file_tx	nfs.file_tx	same
nfs.filename	nfs.filename	same
nfs.hhash	nfs.hhash	same
nfs.id	nfs.id	same
nfs.procedure	nfs.procedure	same
nfs.status	nfs.status	same
nfs.type	nfs.type	same
nfs.version	nfs.version	same
proto	network.transport	modified
rpc.auth_type	rpc.auth_type	same
rpc.creds.gid	rpc.creds.gid	same
rpc.creds.machine_name	rpc.creds.machine_name	same
rpc.creds.uid	rpc.creds.uid	same
rpc.status	rpc.status	same
rpc.xid	rpc.xid	same
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	file.name	added
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added

continues on next page

Table 71 – continued from previous page

2.5.3.102	2.5.3.103	state
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.23 Sigflow rdp

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
metadata.flowbits[0]	metadata.flowbits[0]	same
proto	network.transport	modified
rdp.event_type	rdp.event_type	same
rdp.protocol	rdp.protocol	same
rdp.server_supports[0]	rdp.server_supports[0]	same
rdp.server_supports[1]	rdp.server_supports[1]	same
rdp.server_supports[2]	rdp.server_supports[2]	same
rdp.server_supports[3]	rdp.server_supports[3]	same
rdp.tx_id	rdp.tx_id	same
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.24 Sigflow rfb

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
dest_ip	destination.ip	modified
dest_port	destination.port	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
rfb.authentication.security_type	rfb.authentication.security_type	same
rfb.authentication.vnc.challenge	rfb.authentication.vnc.challenge	same
rfb.authentication.vnc.response	rfb.authentication.vnc.response	same
rfb.client_protocol_version.major	rfb.client_protocol_version.major	same
rfb.client_protocol_version.minor	rfb.client_protocol_version.minor	same
rfb.server_protocol_version.major	rfb.server_protocol_version.major	same
rfb.server_protocol_version.minor	rfb.server_protocol_version.minor	same
rfb.server_security_failure_reason	rfb.server_security_failure_reason	same
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.25 Sigfmow sip

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
sip.method	sip.method	same
sip.request_line	sip.request_line	same
sip.uri	sip.uri	same
sip.version	sip.version	same
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified

continues on next page

Table 74 – continued from previous page

2.5.3.102	2.5.3.103	state
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.26 Sigflow SMB

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
smb.client_dialects[0]	smb.client_dialects[0]	same
smb.client_dialects[1]	smb.client_dialects[1]	same
smb.client_dialects[2]	smb.client_dialects[2]	same
smb.client_dialects[3]	smb.client_dialects[3]	same
smb.client_dialects[4]	smb.client_dialects[4]	same
smb.client_guid	smb.client_guid	same
smb.command	smb.command	same
smb.dialect	smb.dialect	same
smb.id	smb.id	same
smb.max_read_size	smb.max_read_size	same
smb.max_write_size	smb.max_write_size	same
smb.server_guid	smb.server_guid	same
smb.session_id	smb.session_id	same
smb.status	smb.status	same
smb.status_code	smb.status_code	same
smb.tree_id	smb.tree_id	same
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added

continues on next page

Table 75 – continued from previous page

2.5.3.102	2.5.3.103	state
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.27 Sigflow SMTP

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
email.attachments[0]	email.attachments[0]	same
email.body_md5	email.body_md5	same
email.from	email.from.address	modified
email.message_id	email.message_id	same
email.status	email.status	same
email.subject	email.subject	same
email.subject_md5	email.subject_md5	same
email.to[0]	email.to.address[0]	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
smtp.helo	smtp.helo	same
smtp.mail_from	smtp.mail_from	same
smtp.rcpt_to[0]	smtp.rcpt_to[0]	same
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
tx_id	network.tx_id	modified
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.28 Sigflow snmp

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
type		removed
event_type		hardly_modified
proto	network.transport	modified
uuid	observer.uuid	modified
src_port	source.port	modified
dest_port	destination.port	modified
src_ip	source.ip	modified
dest_ip	destination.ip	modified
ether.src_mac	source.mac	modified
ether.dest_mac	destination.mac	modified
community_id	network.community_id	modified
in_iface	observer.gcap.ingress.interface.name	modified
gcap	observer.gcap.hostname	modified
host		removed
gcenter	observer.hostname	modified
flow_id	network.flow_id	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
snmp.vars[0]	snmp.vars[0]	same
snmp.pdu_type	snmp.pdu_type	same
snmp.version	snmp.version	same
snmp.community	snmp.community	same
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.29 Sigflow ssh

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
tftp.file	tftp.file	same
tftp.mode	tftp.mode	same
tftp.packet	tftp.packet	same
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed

continues on next page

Table 78 – continued from previous page

2.5.3.102	2.5.3.103	state
uuid	observer.uuid	modified
	file.name	added
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.30 Sigflow tftp

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
tftp.file	tftp.file	same
tftp.mode	tftp.mode	same
tftp.packet	tftp.packet	same
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
type		removed
uuid	observer.uuid	modified
	file.name	added
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.31 Sigflow tls

2.5.3.102	2.5.3.103	state
@timestamp	@timestamp	same
@version	@version	same
community_id	network.community_id	modified
dest_ip	destination.ip	modified
dest_port	destination.port	modified
ether.dest_mac	destination.mac	modified
ether.src_mac	source.mac	modified
event_type		hardly_modified
flow_id	network.flow_id	modified
gcap	observer.gcap.hostname	modified
gcenter	observer.hostname	modified
host		removed
in_iface	observer.gcap.ingress.interface.name	modified
proto	network.transport	modified
src_ip	source.ip	modified
src_port	source.port	modified
timestamp_analyzed		hardly_modified
timestamp_detected		hardly_modified
tls.chain[0]	tls.server.certificate_chain[0]	modified
tls.fingerprint	tls.server.hash.sha1	modified
tls.notafter	tls.server.not_after	modified
tls.notbefore	tls.server.not_before	modified
tls.subject	tls.server.subject	modified
tls.version	tls.version	same
type		removed
uuid	observer.uuid	modified
	ecs.version	added
	event.dataset	added
	event.module	added
	event.created	added
	event.category[0]	added
	event.id	added
	event.kind	added
	network.protocol	added
	network.timestamp	added
	observer.gcap.version	added
	observer.product	added
	observer.vendor	added
	observer.log_format_version	added
	observer.version	added

9.3.32 Yara engine

This engine appeared in version 103 so this section is not applicable

9.4 Malcore engine results

Table 81: Malcore engine results. are valid only for Malcore configuration at the time of analysis

Return code	Result	Description
0	No Threat Detected	File was analyzed and declared healthy
1	Infected	File was scanned and declared infected
2	Suspicious	The file was analyzed and declared as likely to be infected: some Malcore engines have detected this file as malicious..
3	Failed Scan	An error occurred during the run.
7	Skipped - Whitelisted	The file is not analyzed and considered healthy since this file is defined in the Malcore whitelist
8	Skipped – Blacklisted	The file is not scanned and considered infected since this file is defined in the Malcore blacklist

continues on next page

Table 81 – continued from previous page

Return code	Result	Description
9	Exceeded Archive Depth	The number of times the file is compressed is limited (max recursion level). The message indicates that the defined value has been exceeded.
10	Not scanned	Engine not available at time of run
12	Encrypted Archive	The archive is encrypted and therefore not parsable: the password indicated does not work
13	Exceeded Archive Size	The maximum file size should not exceed the defined value (maximum value 10MB). The analyzed archive is larger than the value set
14	Exceeded Archive File Number	The maximum number of files in the archive must not exceed the defined value. The analyzed archive contains a number of files greater than the defined value
15	Password Protected Document	Solution detected inconsistent behaviour with password protected document
16	Exceeded Archive Timeout	The archive scan time has been exceeded, Malcore engines are not responding within the deadline
17	Filetype Mismatch	File type mismatch problem: the solution detects the file extension with its contents and compares it with the file extension displayed
18	Potentially Vulnerable File	Potentially vulnerable files are files associated with identified vulnerable components or applications
19	Cancelled	User explicitly canceled this file analysis request
21	Yara Rule Matched	The verdict of the result is: a Yara rule matches (malware sample identification)
22	Potentially Unwanted	Solution detected potentially unwanted applications
23	Unsupported File Type	File type not supported by the solution
255	In Progress	Analysis in progress..

Chapter 10

Glossary

Alerting
Enables detection of Sigflow signatures for a given protocol. If the latter is enabled for a protocol then the flow that is identified by a signature will raise an alert on the GCenter sid

ANSSI
The National Authority for Security and Defence of Information Systems is a French Service with national competence responsible for IT security.

CLI
The CLI (Command Line Interface) is the means used to administer and configure the GCap. It is the set of commands in text mode.

Critical risk

Low Risk Definition: highly suspicious activity was detected. Hazardous activity was detected. There is a high probability that your organization is facing a serious threat and countermeasures should be taken immediately.
For example, a user downloaded malware or an active element from the network contacted a known control and control domain.
Color definition used for this type of alarms in WebUI : red
Level of risk in this category: 75-100%

Engine hash
Name of 16 MALCORE antivirus engines

GCap
GCap is the detection probe for the Trackwatch/Aioniq solution. It retrieves the network flow from the TAP and reconstructs the files it sends to the GCenter.

GCenter
The GCenter is the component that administers the GCap and performs the analysis of files sent by the GCap.

High risk

High Risk Definition: very suspicious activity has been detected. This type of event should be investigated promptly as it could be a sign of significant compromise.
It is possible that this event is a false positive or related to a bad figuration in your network.
Color definition used for this type of alarms in WebUI : orange
Level of risk in this category: 50-74%

LDAP
LDAP is a protocol for querying and modifying directory services (Active Directory for example)

Logging
Enables metadata generation for a given protocol. Indeed, if the latter is enabled for a protocol then each observed session will generate metadata for that protocol on the GCenter side.

Low risk

Low risk definition: unusual activity detected. This could mean that you have unusual policies or network uses.
These types of events should be mentioned last as they are not a direct sign of significant compromises.
They can be used as good indicators to improve network policies and detect configuration errors.
Color definition used for this type of alarms in WebUI : blue
Level of risk in this category: 0-24%

Malcore
Detection engine for malware detection and analysis

Medium risk

Medium Risk Definition: an activity that could be linked to a threat has been identified. Risk has been set at low values, because the potential threat does not appear critical or because the likelihood of forgery is high.
Color definition used for this type of alarms in WebUI : yellow
Level of risk in this category: 25-49%

Mitre
Knowledge base and behaviour model of cyber-adversaries, reflecting the phases of an adversary's attack life cycle and the platforms it targets.

MTU
The MTU (Maximum Transfer Unit) is the maximum size of a packet that can be transmitted at once (without fragmentation) over a network interface.

OIV
Operators of Vital Importance

OTP

The One Time Password (OTP) is a one-time password defined on the GCenter.

RAID1

RAID 1 is the use of n redundant disks. Each disk in the cluster containing exactly the same data at any time, hence the use of the word «mirror» (mirroring).

RAID5

The RAID 5 uses several hard drives (minimum 3) grouped in a cluster to form a single logical unit. The data is duplicated and distributed on 2 different disks among the present disks.

setup

Account name for a system administrator to access the configuration menu

SIEM

SIEM (Security Information and Event Management) is a centralized system of security events that provides total visibility on the activity of a network and thus allows to react to threats in real time.

Sigflow

The detection engine (also called Sigflow) is responsible for reconstituting files and also one of the engines for analyzing all network traffic and can, according to **rules**, generate alerts, metadata or content.

TAP

The TAP (Test Access Point) is a passive device that duplicates a network flow.

Threat DB update

Threat DB update is the service for the management of detection database updates, hotfix application

`PDF documentation`

@Copyright: December 2024, Gatewatcher

Index

Symbols

```API keys``` screen, 270
```Active CTI``` screen, 224
```Alerts``` screen, 147
```Assets``` screen, 158
```Association rules``` screen, 230
```Auto-threshold``` screen, 220
```Backup operations``` screen, 289
```Beacon detect``` screen, 239
```Configuration``` screen, 287
```DGA detect``` screen, 236
```Data Management``` screen, 294
```Data export``` screen, 295
```Diagnostics``` screen, 286
```GCaps Pairing``` screen, 276
```GCaps profiles``` screen, 167
```GScan``` screen, 161
```Gatewatcher API``` screen, 302
```Gatewatcher Customer Portal``` screen, 309
```Gatewatcher support``` Screen, 310
```Global settings``` screen, 283
```Health checks``` screen, 245
```History``` screen, 262
```Home``` screen, 134
```Hunting``` screen, 155
```LDAP binding``` screen, 266
```License``` screen, 279
```MISP settings``` screen, 274
```Malcore retroanalyzer``` screen, 212
```Malcore``` screen, 209
```Malicious Powershell detect``` screen, 214
```Metadata rate limiter``` screen, 207
```Netdata Export Configuration``` screen, 299
```Netdata polling``` screen, 300
```Network settings``` screen, 282
```Online documentation``` screen, 308
```Overview``` screen, 141
```Password policy``` screen, 273
```Ransomware detect``` screen, 226
```Relations``` screen, 146
```Retention policy``` screen, 292
```Retro Hunt``` screen, 225
```Shellcode detect``` screen, 214
```Software update``` screen, 261
```Sources``` screen, 215, 217
```System Overview``` screen of the Gstats GUI, 251
```System notifications``` command, 252
```Threat DB update``` screen, 256
```Top Relations``` screen, 140
```Top risk``` screen, 138
```Users management``` screen, 263
```Users``` screen, 156
```YARA``` screen, 213
```update.gatewatcher.com``` screen, 310
```

A

Active CTI
    Alert Analysis, 77
    CTI module overview, 71
    Events generated, 72
    Introduction, 71
    Management of the engine, 76
    Management of the engine; CTI update, 76
    Management of the engine; Viewing the engine status, 76
    Setting up the Active CTI engine, 581
Active CTI, Events generated
    Active CTI log data structure, 74
Administrator
    NDR; Configuring the NDR, 492
    Setting up a Netdata server, 603
Administrator, Account management
    Changing some of a local user's information, 542
    Changing some of the current user's information, 598
    Changing the checking account password, 596
    Configuring the authentication history, 554
    Configuring the connection between the GCenter and the LDAP server, 548
    Configuring the users and groups defined on LDAP / ActiveDirectory, 551
    Creating local user, 540
    Deleting a local user, 545
    Displaying of the connection status between the GCenter and the LDAP server, 546
    Enabling the connection between the GCenter and the LDAP server, 547
    Managing an API access token, 556
    Managing the password policy, 558
    Resetting a local user's password, 543
    Viewing the authentication history, 552
Administrator, Active CTI
    Setting up the Active CTI engine, 581
Administrator, Backup restore function
    Operating the backup, 503
    Operating the restoration, 504
    Setting the backup, 501
Administrator, Detection engine
    Managing the Ignore list of the Beacon detect, 593
    Managing the Ignore list of the DGA detect engine, 573
    Managing the Ignore list of the Malcore engine, 563
    Managing the Ignore list of the Ransomware detect, 589
    Setting of the retro hunt engine, 584
    Setting up the beacon detect engine, 591
    Setting up the DGA detect engine, 570
    Setting up the Malcore engine, 561
    Setting up the Malcore retroanalyzer engine, 566
    Setting up the Malicious Powershell detect engine, 576
    Setting up the Ransomware detect engine, 586
    Setting up the Yara engine, 568
Administrator, GCap administration
    Change the default profile or customise the existing profile, 389
    Pairing a GCap with the GCenter, 495
    Pairing again a GCap, 498
Administrator, GCenter administration
    Configuring the connection to the MISP, 524
    Deleting data (*log files*), 526
    Export data to a SIEM via the syslog protocol, 519
    Export data to the ETL Logstash via syslog protocol, 520
    Generating and loading files for diagnosis, 527
    Quick creation of a POC Logstash, 523
    Using an endpoint API, 529
Administrator, GCenter software

Configuring automatic update via Threat DB update, 508
Installing a hotfix, 514
Installing an update manually, 512
Installing of an upgrade, 516
Administrator, Global configuration
Configuring the Netdata export interface, 602
Configuring the Netdata polling interface, 600
Connection to the GCenter web interface via a web browser, 492
GCenter global configuration, 538
Logging out of the GCenter web interface, 608
Managing the license, 534
Using a Netdata server, 606
Administrator, Setting up the Shellcode detect engine, 579
Alerting, **659**
ANSSI, **659**
API, 113
Endpoints list, 115, 317
Overview of the API interface, 311
Presentation of the tittle bar, 126
Using an endpoint API, 529
Audit trail
Configuring the authentication history, 554
Viewing the authentication history, 552

B

Beacon detect
Alert Analysis, 95
Beacon detect engine, 89
Beacon detect log data structure, 93
Configuration of the engine and management of the ignored destination list, 94
Engine update, 94
Events generated, 90
Introduction, 89
Management of the engine, 94
Managing the Ignore list, 593
Viewing the engine status, 94
beacon detect engine
Setting up the beacon detect engine, 591
Beacon detect, Events generated
Events generated by the engine, 458, 460

C

Characteristics
Electrical characteristics, 116
Functional characteristics, 116
Mechanical characteristics, 116
CLI, **659**
Configuration menu
```About``` Command, 331
```Arp Manager``` command, 339
```DateTime``` command, 335
```Diagnose``` command, 341
```Elasticsearch storage mode``` command, 345
```Exit``` command, 349
```GCenter Services Management``` command, 342
```Keyboard``` command, 333
```LPM Mode``` command, 346
```Network``` command, 336
```Password``` command, 333
```Reset``` command, 348
```Restart``` command, 347
```Shutdown``` command, 347
```Tech Support``` command, 332
Overview, 124
Critical risk, **659**
CTI
Active CTI engine, 71
Retro hunt engine, 77
CTI, Events generated
Example of a Active CTI alert in the WebUI, 73
CTI, Events generated by the Retro hunt engine
Example of Retro hunt alert in the WebUI, 79
current account
```Change Password``` screen, 165
```Edit profile``` screen, 164
Overview of the account management menu, 163

D

Data use, 107
DGA detect, 64
Alert Analysis, 70
Analyzing the DGA detect alerts, 444
Configure the DGA detect engine and manage the list of ignored files, 70
DGA detect log data structure, 67
Engine update, 69
Events generated, 65
Introduction, 64
Management of the engine, 69
Viewing the engine status, 69
DGA detect, Events generated
Events generated by the engine, 445
Example of alert in WebUI, 67

E

Engine hash, **659**
External integration
Introduction, 111
MISP Server, 111

G

GApps management, 111
GCap, **659**
Presentation of the GCap, 9
GCap configuration
Configuring filters on targeted parts of the analyzed traffic via the GCap profile, 412
Configuring the Base variables parameters via the GCap profile, 397
Configuring the detection rulesets via the GCap profile, 391
Configuring the file reconstruction rules via the GCap profile, 408
Configuring the flow timeouts via the GCap profile, 407
Configuring the network variables parameters via the GCap profile, 402
GCenter, **659**
GCenter Global Configuration, 538
Managing the license, 534
Presentation of the GCenter, 9
GCenter software
Dedicated modules for managing updates Threat DB update and Software update, 102
Hotfix presentation, 105
Overview of the backup and restoration, 106
Release note, 105
Update presentation, 103
Upgrade presentation, 102
GCenter, Presentation of the GCenter
Different server models, 10
List of the GCenter inputs / outputs, 10
GScan
Detecting with GScan, 481
Gscan
Introduction of the GScan detection, 101
Gstats
```System Overview``` screen of the Gstats GUI, 251
Presentation of the tittle bar, 126

H

High risk, **659**
Hotfix
overview, 102

I

Interconnection
Interconnection between devices, 13

K

Kibana
    ```System logs``` screen, 286
Kibana GUI, 127
    Configuration of the Kibana GUI, 127
    Data exploitation, 131
    Main tabs, 128
    Native dashboards of the ```Administration``` tab, 130
    Native dashboards of the ```Alerts``` tab, 128
    Native dashboards of the ```Network Metadata``` tab, 129
    overview, 127

L

LDAP, **659**
LDAP user
    Configuring the connection between the GCenter and the LDAP server, 548
    Configuring the users and groups defined on LDAP / ActiveDirectory, 551
    Displaying of the connection status between the GCenter and the LDAP server, 546
    Enabling the connection between the GCenter and the LDAP server, 547
Legacy web UI, 131
    Description of the legacy WebUI, 132
    Navigation bar, 132
    Overview, 131
Legacy WebUI
    ```Backup operations``` screen, 289
    ```Configuration``` screen, 287
    ```MISP settings``` screen, 274
List of accounts, 117
Local user
    Changing some of a local user's information, 542
    Creating local user, 540
    Deleting a local user, 545
    Resetting a local user's password, 543
Logging, **659**
Logstash
    Export data to the ETL Logstash via syslog protocol, 520
    Quick creation of a POC Logstash, 523
Low risk, **659**

M

Machine Learning
    Managing the Ignore list of the DGA detect engine, 573
    Setting up the DGA detect engine, 570
Malcore, **659**
    Alert Analysis, 29
    Analyzing the Beacon detect alerts, 460
    Analyzing the Malcore alerts, 415
    Events generated, 21
    Introduction, 21
    Malcore engine, 20, 21
    Management of the engine, 29
    Management of the engine; Engine update, 29
    Management of the engine; Malcore configuration and management of the ignored list feature, 29
    Management of the engine; Viewing the engine status, 29
    Managing the Ignore list, 563
    Setting up the Malcore engine, 561
Malcore retroanalyzer
    Alert Analysis, 71
    Analyzing the Malcore retroanalyzer alerts, 450
    Configuration of the engine and management of the ignored files list, 71
    Engine update, 71
    Events generated, 70
    Management of the engine, 71
    Presentation, 70
    Setting up the Malcore retroanalyzer engine, 566
    Viewing the engine status, 71
Malcore retroanalyzer, Malcore retroanalyzer engine, 70
Malcore, Events generated
    Malcore log data structure, 25
Malicious Powershell Detect
    Analyzing the Malicious Powershell Detect alerts, 427
    Analyzing the Yara alerts, 464
Malicious Powershell detect, 35
    Alert Analysis, 41
    Engine configuration, 41
    Engine update, 41
    Introduction, 35
    Management of the engine, 41
    Setting up the Malicious Powershell detect engine, 576
    Viewing the engine status, 41
Malicious Powershell detect, Events generated, 36
    Example of a Powershell alert in the WebUI, 38
Medium risk, **659**
Metadata rate limiter
    ```Metadata rate limiter``` screen, 207
MISP
    Configuring the connection to the MISP, 524
Mitre, **659**
MTU, **659**

N

Netdata
    Configuring the Netdata export interface, 602
    Configuring the Netdata polling interface, 600
    Overview of the Netdata User Interface, 133
    Setting up a Netdata server, 603
    Using a Netdata server, 606
Netdata Gstats
    ```System Overview``` screen of the Gstats GUI, 251

O

OIV, **659**
Operator
    Analyzing the Active CTI alerts, 450
    Analyzing the Beacon detect alerts, 460
    Analyzing the DGA detect alerts, 444
    Analyzing the Malcore alerts, 415
    Analyzing the Malcore retroanalyzer alerts, 450
    Analyzing the Malicious Powershell Detect alerts, 427
    Analyzing the Ransomware detect alerts, 457
    Analyzing the Retrohunt alerts, 454
    Analyzing the Shellcode detect alerts, 422
    Analyzing the Sigflow alerts, 434
    Analyzing the Yara alerts, 464
    Configuring Metadata Rate Limiters, 487
    Session management;Connection to the GCenter web interface via a web browser, 353
    Session management;Logging out of the GCenter web interface, 490
Operator, Account management
    Changing some of the current user's information, 356
    Changing the checking account password, 354
Operator, GCap configuration
    Configuring filters on targeted parts of the analyzed traffic via the GCap profile, 412
    Configuring the Base variables parameters via the GCap profile, 397
    Configuring the detection rulesets via the GCap profile, 391
    Configuring the file reconstruction rules via the GCap profile, 408
    Configuring the flow timeouts via the GCap profile, 407
    Configuring the network variables parameters via the GCap profile, 402
Operator, GScan
    Detecting with GScan, 481
Operator, Kibana dashboards
    Using of the Kibana dashboards, 480
Operator, NDR dashboards
    Using of NDR dashboards, 470
Operator, Sigflow management
    Creating a Sigflow engine ruleset, 365
    Creation of automatic alarm limits, 385
    Modifying Sigflow engine rules, 379

Sigflow engine rule sources, 358
Updating rules sources, 377
OTP, **659**
Overview of the ```Detection strategy``` menu, 166

R

RAID1, **660**
RAID5, **660**
Ransomware detect
Alert Analysis, 89
Analyzing the Ransomware detect alerts, 457
Configuration of the engine and management of the ignored files list, 89
Engine management; Update, 88
Engine management; Viewing the engine status, 88
Events generated, 85
Introduction, 84
Management of the engine, 88
Managing the Ignore list`` of the Ransomware detect, 589
Ransomware detect engine, 84
Setting up the Ransomware detect engine, 586
Ransomware detect, Events generated
Logs data structure, 87
Reflex
Presentation of Reflex, 12
Retro hunt
Alert Analysis, 84
Analyzing the Retrohunt alerts, 454
CTI module overview, 77
Engine management; Update, 83
Engine management; Viewing the engine status, 83
Events generated, 78
Management of the engine, 83
Retro hunt, events generated
Retro hunt log data structure, 79
retrohunt
Setting of the retro hunt engine, 584

S

setup, **660**
```About``` Command, 331
```Arp Manager``` command, 339
```DateTime``` command, 335
```Diagnose``` command, 341
```Elasticsearch storage mode``` command, 345
```Exit``` command, 349
```GCenter Services Management``` command, 342
```Keyboard``` command, 333
```LPM Mode``` command, 346
```Network``` command, 336
```Password``` command, 333
```Reset``` command, 348
```Restart``` command, 347
```Shutdown``` command, 347
```Tech Support``` command, 332
Direct connection to the GCenter configuration menu in HTTP via iDRAC (*DELL server*), 328
Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode, 329
Direct connection to the GCenter configuration menu via SSH, 330
Direct connection to the GCenter configuration menu with keyboard and monitor, 327
Setup account, 117
Functions allowed in the setup account, 118
Related principles, 117
Shellcode detect
Alert Analysis, 35
Analyzing the Shellcode detect alerts, 422
Engine configuration, 35
Engine update, 35
Events generated, 31
Events generated; Example of a Shellcode log, 32
Events generated; Shellcode log data structure, 32
Introduction, 30
Management of the engine, 34
Viewing the engine status, 35
Shellcode detect engine, 30
Setting up the Shellcode detect engine, 579
Shellcode detect, Events generated
Events generated by the engine, 423
SIEM, **660**
Export data to a SIEM via the syslog protocol, 519
Sigflow, **660**
Alert Analysis, 64
Analyzing the Active CTI alerts, 450
Analyzing the Sigflow alerts, 434
Data structure of the Events of type "alert", 54
Data structure of the events of type "fileinfo", 58
Data structure of the events of type "meta-data", 61
Detailed operation of the rules, 42
Engine update, 63
GCAP Profiles; GCAP Profiles, 47
Introduction, 42
Management of the engine, 63
Organizing the rules, 43
Sigflow engine, 41
Sigflow engine signature sources, 43
Sigflow Setup, 64
View the status of Sigflow, 63
Sigflow Rulesets
Changing signatures, 44
Definition of signatures, 44
Generating rulesets, 47
Optimization of rulesets, 44
Removing or limiting the number of alerts, 46
Rulesets, 43
Sigflow, Events generated, 51
Events generated by the engine, 435
Events of type "alert", 51
Events of type "fileinfo", 56
Events of type "meta-data", 60
List of protocols in the Events of type "alert", 53
Sigflow, GCap configuration
Configuring filters on targeted parts of the analyzed traffic via the GCap profile, 412
Configuring the Base variables parameters via the GCap profile, 397
Configuring the detection rulesets via the GCap profile, 391
Configuring the file reconstruction rules via the GCap profile, 408
Configuring the flow timeouts via the GCap profile, 407
Configuring the network variables parameters via the GCap profile, 402
Sigflow, GCAP Profiles
Alerting et logging, 49
Base variables, 48
Community ID, 49
Detection Rulesets, 47
File rule management, 50
Flow timeouts, 50
HTTP Proxy, 49
Multi-tenant by interface, 48
Multi-tenant by VLAN, 48
Net variables, 50
Packet filtering, 50
Payload, 49
Single-tenant, 48
Stream analysis and file extraction, 49
Sigflow, Sigflow management
Creating a Sigflow engine ruleset, 365
Creation of automatic alarm limits, 385
Modifying Sigflow engine rules, 379
Sigflow engine rule sources, 358
Updating rules sources, 377
Syslog servers
Introduction, 112
Logstash, 113
```

SIEM, 112
SIEM Splunk, 113

T

TAP, **660**
Overview of the TAP, 9
Threat DB update, **660**
Configuring automatic update via Threat DB update, 508
Installing a hotfix, 514
Installing an update manually, 512
Installing of an upgrade, 516
Threat DB update and Software update
overview, 102
Token
Managing an API access token, 556
Managing the password policy, 558

U

Update
overview, 102
Update automatic, 104
Update manual, 104
Upgrade
overview, 102
Use case, Analyzing the Active CTI alerts, 450
Use case, Analyzing the Sigflow alerts, 434
Use case, Member of Administrator group
NDR; Configuring the NDR, 492
Use case, Member of Administrator group, Account management
Changing some of a local user's information, 542
Configuring the authentication history, 554
Configuring the connection between the GCenter and the LDAP server, 548
Configuring the users and groups defined on LDAP / ActiveDirectory, 551
Creating local user, 540
Deleting a local user, 545
Displaying of the connection status between the GCenter and the LDAP server, 546
Enabling the connection between the GCenter and the LDAP server, 547
Managing an API access token, 556
Managing the password policy, 558
Resetting a local user's password, 543
Viewing the authentication history, 552
Use case, Member of Administrator group, Active CTI
Setting up the Active CTI engine, 581
Use case, Member of Administrator group, Backup restore function
Operating the backup, 503
Operating the restoration, 504
Setting the backup, 501
Use case, Member of Administrator group, Detection engine
Managing the Ignore list of the Beacon detect, 593
Managing the Ignore list of the DGA detect engine, 573
Managing the Ignore list of the Malcore engine, 563
Managing the Ignore list of the Ransomware detect, 589
Setting of the retro hunt engine, 584
Setting up the beacon detect engine, 591
Setting up the DGA detect engine, 570
Setting up the Malcore engine, 561
Setting up the Malcore retroanalyzer engine, 566
Setting up the Malicious Powershell detect engine, 576
Setting up the Ransomware detect engine, 586
Setting up the Shellcode detect engine, 579
Setting up the Yara engine, 568
Use case, Member of Administrator group, GCap administration
Pairing a GCap with the GCenter, 495
Pairing again a GCap, 498
Use case, member of Administrator group, GCap administration
Change the default profile or customise the existing profile, 389
Use case, Member of Administrator group, GCenter administration
Configuring the connection to the MISP, 524
Deleting data (*log files*), 526
Export data to a SIEM via the syslog protocol, 519
Generating and loading files for diagnosis, 527
Quick creation of a POC Logstash, 523
Using an endpoint API, 529
Use case, Member of Administrator group, GCenter administration Export data to the ETL Logstash via syslog protocol, 520
Use case, Member of Administrator group, GCenter software
Configuring automatic update via Threat DB update, 508
Installing a hotfix, 514
Installing an update manually, 512
Installing of an upgrade, 516
Use case, Member of Administrator group, Global configuration
Configuring the Netdata export interface, 602
Configuring the Netdata polling interface, 600
GCenter global configuration, 538
Managing the license, 534
Setting up a Netdata server, 603
Using a Netdata server, 606
Use case, Member of Administrator group, Session management
Connection to the GCenter web interface via a web browser, 492
Logging out of the GCenter web interface, 608
Use case, Member of Operator group
Analyzing the Beacon detect alerts, 460
Analyzing the DGA detect alerts, 444
Analyzing the Malcore alerts, 415
Analyzing the Malcore retroanalyzer alerts, 450
Analyzing the Malicious Powershell Detect alerts, 427
Analyzing the Ransomware detect alerts, 457
Analyzing the Retrohunt alerts, 454
Analyzing the Shellcode detect alerts, 422
Analyzing the Yara alerts, 464
Configuring Metadata Rate Limiters, 487
Use case, Member of Operator group , GCap configuration
Configuring the file reconstruction rules via the GCap profile, 408
Use case, Member of Operator group , Account management
Changing the checking account password, 354
Use case, Member of Operator group , GCap configuration
Configuring the detection rulesets via the GCap profile, 391
Use case, Member of Operator group , NDR dashboards
Using of NDR dashboards, 470
Use case, Member of Operator group , Session management
Connection to the GCenter web interface via a web browser, 353
Logging out of the GCenter web interface, 490
Use case, Member of Operator group ,Configuring the network variables parameters via the GCap profile, 402
Use case, Member of Operator group, Account management
Changing some of the current user's information, 356, 598
Changing the checking account password, 596
Use case, Member of Operator group, Configuring the flow timeouts via the GCap profile, 407
Use case, Member of Operator group, GCap configuration
Configuring filters on targeted parts of the analyzed traffic via the GCap profile, 412
Configuring the Base variables parameters via the GCap profile, 397
Use case, Member of Operator group, GScan
Detecting with GScan, 481
Use case, Member of Operator group, Kibana dashboards
Using of the Kibana dashboards, 480
Use case, Member of Operator group, membre groupe operator, gestion Sigflow
Creation of automatic alarm limits, 385
Use case, Member of Operator group, Sigflow management
Creating a Sigflow engine ruleset, 365
Modifying Sigflow engine rules, 379

Sigflow engine rule sources, 358
Use case, Member of Operator group, SIigflow management
Updating rules sources, 377
Use case, Setup account
Direct connection to the GCenter configuration menu in HTTP via iDRAC (*DELL server*), 328
Direct connection to the GCenter configuration menu SSH via the iDRAC interface in serial port forwarding mode, 329
Direct connection to the GCenter configuration menu via SSH, 330
Direct connection to the GCenter configuration menu with keyboard and monitor, 327

W

Web interface accounts and their management
Web Interface Accounts, 118
Web interface interface accounts, 118
WebUI
```API keys``` screen, 270
```Active CTI``` screen, 224
```Alerts``` screen, 147
```Assets``` screen, 158
```Auto-threshold``` screen, 220
```Beacon detect``` screen, 239
```DGA detect``` screen, 236
```Data Management``` screen, 294
```Data export``` screen, 295
```Diagnostics``` screen, 286
```GCaps Pairing``` screen, 276
```GScan``` screen, 161
```Gatewatcher API``` screen, 302
```Gatewatcher Customer Portal``` screen, 309
```Gatewatcher support``` Screen, 310
```Global settings``` screen, 283
```Health checks``` screen, 245
```History``` screen, 262
```Home``` screen, 134
```Hunting``` screen, 155
```LDAP binding``` screen, 266
```License``` screen, 279
```Malcore retroanalyzer``` screen, 212
```Malcore``` screen, 209
```Malicious Powershell detect``` screen, 214
```Netdata Export Configuration``` screen, 299
```Netdata polling``` screen, 300
```Network settings``` screen, 282
```Online documentation``` screen, 308
```Overview``` screen, 141
```Password policy``` screen, 273
```Ransomware detect``` screen, 226
```Relations``` screen, 146
```Retention policy``` screen, 292
```Retro Hunt``` screen, 225
```Rulesets``` screen, 217
```Shellcode detect``` screen, 214
```Software update``` screen, 261
```Sources``` screen, 215
```Threat DB update``` screen, 256
```Top Relations``` screen, 140
```Top risk``` screen, 138
```Users management``` screen, 263
```Users``` screen, 156
```Yara engine``` screen, 213
```update.gatewatcher.com``` screen, 310
Central screen, 127
Navigation bar, 125
Overview of the WEB UI, 124
Presentation of the tittle bar, 126
WebUI, Account management
Changing some of the current user's information, 356, 598
Changing the checking account password, 354, 596
WebUI, Member of Administrator group, Session management
Connection to the GCenter web interface via a web browser, 492
Logging out of the GCenter web interface, 608
WebUI, Session management
Connection to the GCenter web interface via a web browser, 353
Logging out of the GCenter web interface, 490

Y

Yara
Alert Analysis, 101
Configuration of the engine, 101
Events generated, 96
Introduction, 95
Management of the engine, 101
Setting up the Yara engine, 568
Update, 101
Viewing the engine status, 101
Yara engine, 95
Yara, Events generated
Yara log data structure, 99