GCenter documentation 2.5.3.101

Gatewatcher

Created on : December, 2020

Last updated : October, 2024

Table of contents

Chapter 1

Upgrade Path

The general rule for upgrade paths is that **it is necessary to be on the latest hotfix** before installing a major upgrade.

The same applies to the **application of hotfixes that must be done in order** for example v100 -> v100-hf1 -> v100-hf2 -> ...

Where this is not the case, it will be notified in the release note for the relevant version.

Chapter 2

Release Notes

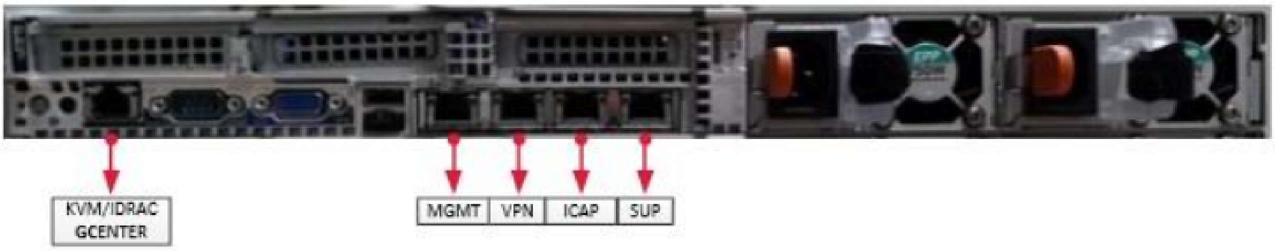
Release notes are referenced in the following table. These release notes (or *Release Note*) contain the list of changes made by the given release, the list of known issues, and also important notes related to the upgrade process.

Chapter 3

Presentation of the equipment

3.1 GCenter

GCENTER is the centralised management equipment of the TRACKWATCH solution. It enables receiving and analysing alerts from the **GCAP** probes and configuring the TRACKWATCH solution in an intuitive way.



CGCENTER thus has five interfaces performing the following roles:

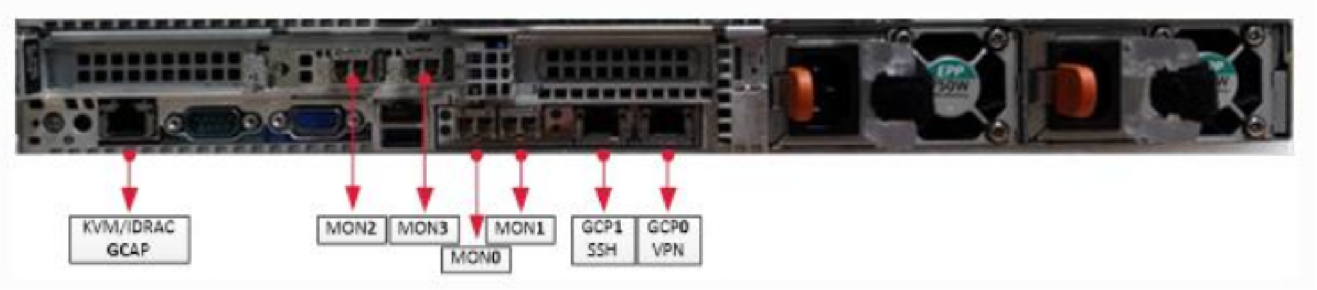
- **KVM/IDRAC**: Remote administration interface
- **SUP0**: Interaction with Nagios
- **ICAP0**: Interaction with the Proxy
- **VPN0**: Dedicated VPN interface with **GCAP** (optional)
- **MGMT0**: Management interface

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.

3.2 GCAP

The **GCAP** probes enable analysing the received flow in order to detect, capture, reconstruct, sort, and transmit files, malicious code, and events to **GCENTER**.



In addition to the three management interfaces, **GCAP** probes have a variable number of capture interfaces:

- **KVM/IDRAC**: Remote administration interface
- **GCP0**: VPN interface and optional management interface
- **GCP1**: Dedicated management interface (optional)
- **mon0-monX**: Capture interface

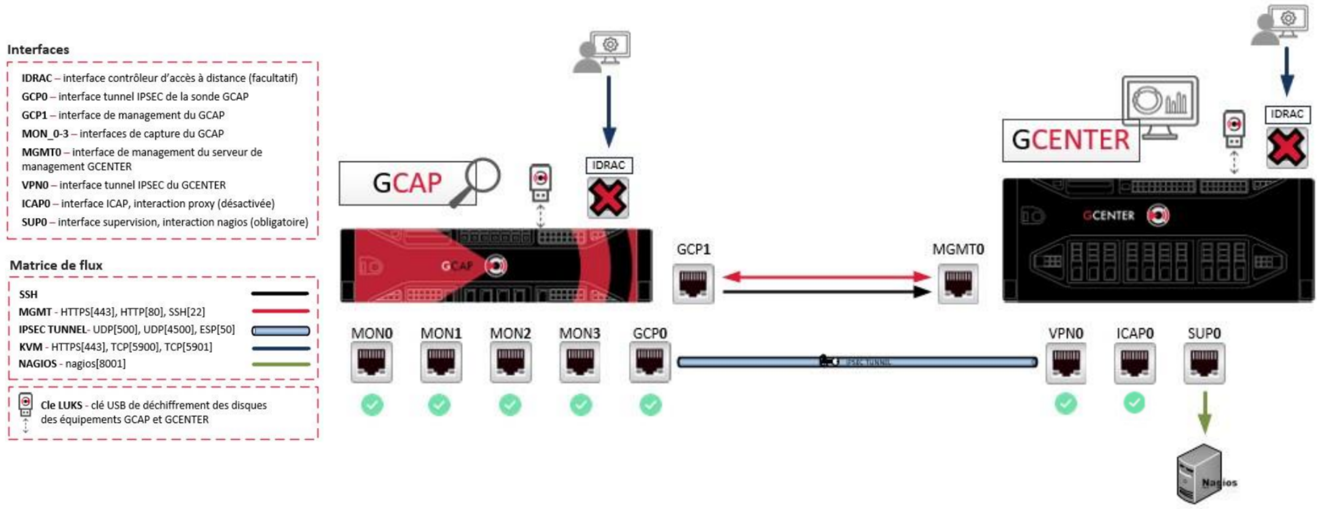
The use of the **GCP1** interface to separate the management flow from the VPN's IPSec traffic may be mandatory for sensitive environments. Otherwise, it is possible to only use the **GCP0** interface for management and VPN flows.

Chapter 4

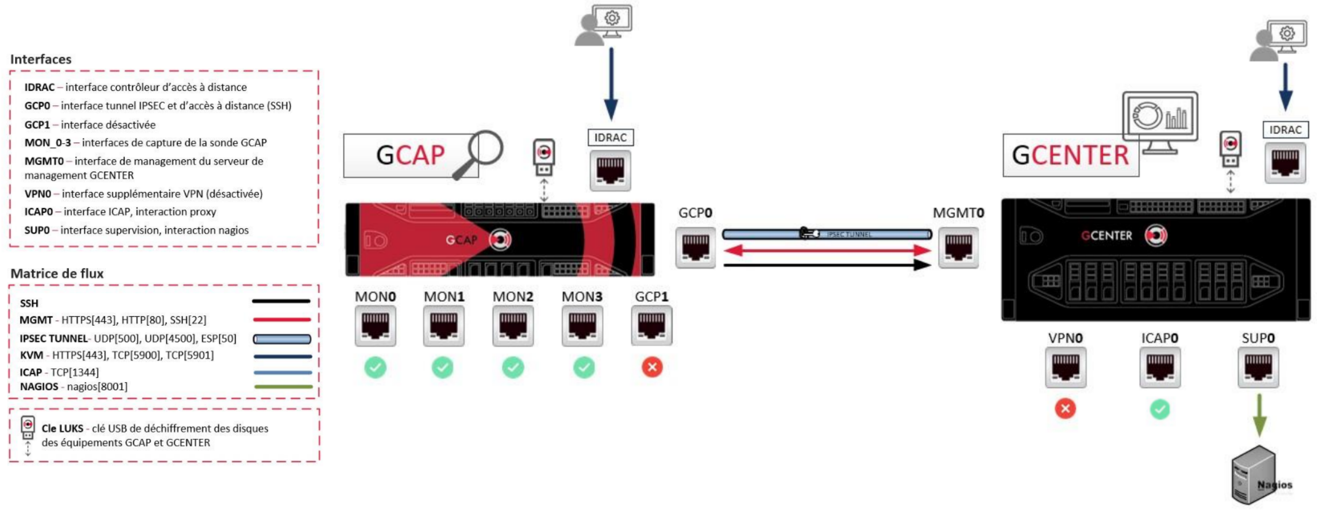
Flow Matrix

As previously explained, two communication modes are possible for communicating between the **GCAP** and the **GCENTER**.

The first mode, which is the mandatory mode in the case of a sensitive environment, is the following:


Interfaces
IDRAC – interface contrôleur d'accès à distance (facultatif)
GCP0 – interface tunnel IPSEC de la sonde GCAP
GCP1 – interface de management du GCAP
MON_0-3 – interfaces de capture du GCAP
MGMT0 – interface de management du serveur de management GCENTER
VPN0 – interface tunnel IPSEC du GCENTER
ICAP0 – interface ICAP, interaction proxy (désactivée)
SUP0 – interface supervision, interaction nagios (obligatoire)
Matrice de flux
SSH
MGMT - HTTPS[443], HTTP[80], SSH[22]
IPSEC TUNNEL- UDP[500], UDP[4500], ESP[50]
KVM - HTTPS[443], TCP[5900], TCP[5901]
NAGIOS - nagios[8001]
Cle LUKS - clé USB de déchiffrement des disques des équipements GCAP et GCENTER
GCAP
IDRAC
GCENTER
IDRAC
GCP1
MGMT0
MON0
MON1
MON2
MON3
GCP0
IPSEC TUNNEL
VPN0
ICAP0
SUP0
Nagios

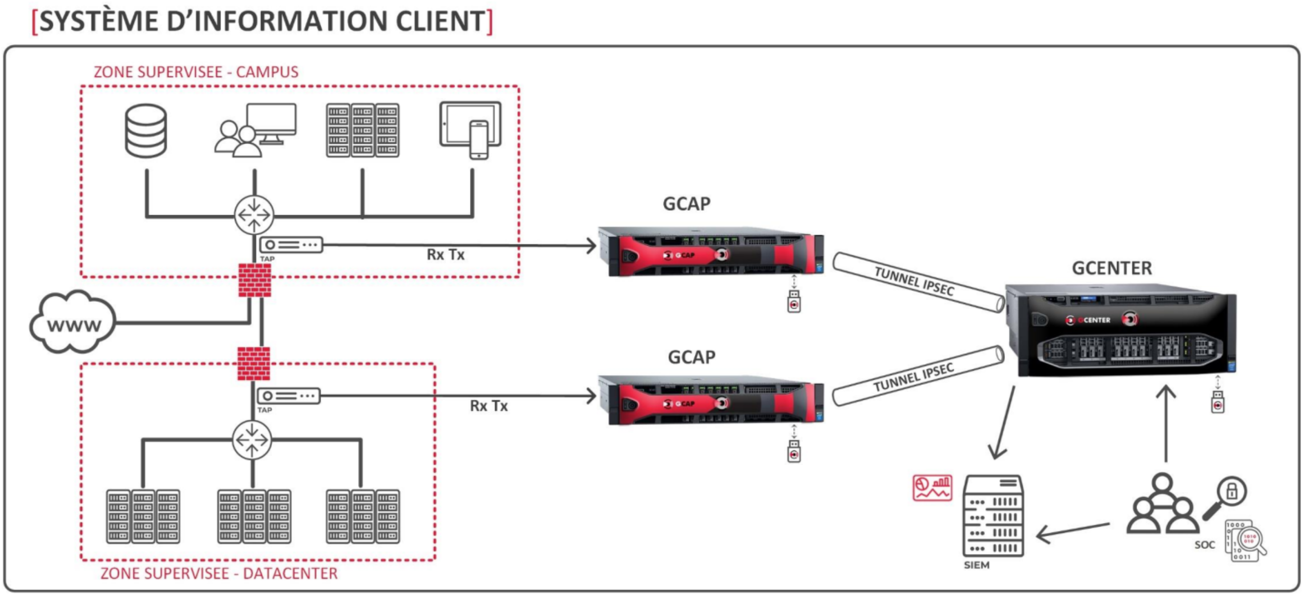
As for the second mode, it enables pooling an interface for transiting the management and VPN flows.

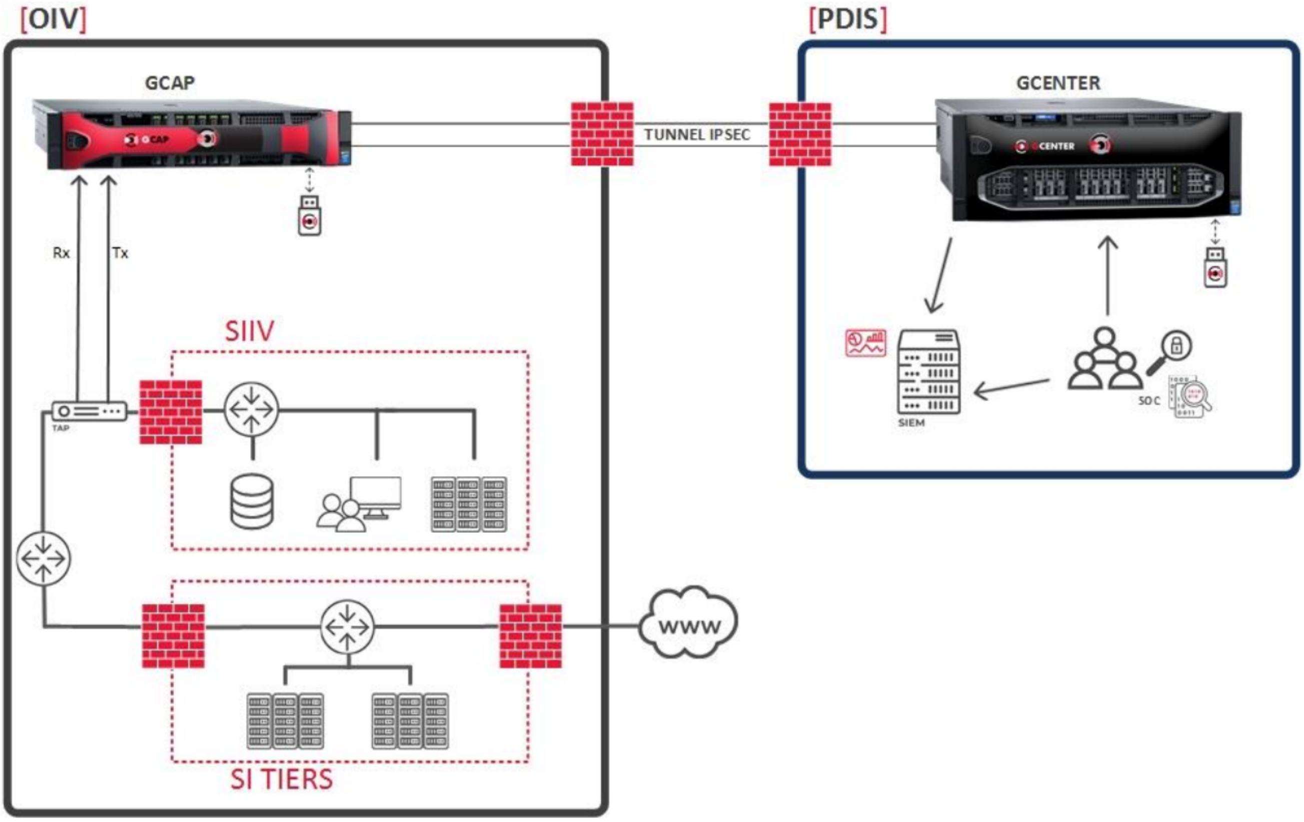

Interfaces
IDRAC – interface contrôleur d'accès à distance
GCP0 – interface tunnel IPSEC et d'accès à distance (SSH)
GCP1 – interface désactivée
MON_0-3 – interfaces de capture de la sonde GCAP
MGMT0 – interface de management du serveur de management GCENTER
VPN0 – interface supplémentaire VPN (désactivée)
ICAP0 – interface ICAP, interaction proxy
SUP0 – interface supervision, interaction nagios
Matrice de flux
SSH
MGMT - HTTPS[443], HTTP[80], SSH[22]
IPSEC TUNNEL- UDP[500], UDP[4500], ESP[50]
KVM - HTTPS[443], TCP[5900], TCP[5901]
ICAP - TCP[1344]
NAGIOS - nagios[8001]
Cle LUKS - clé USB de déchiffrement des disques des équipements GCAP et GCENTER
GCAP
IDRAC
GCENTER
IDRAC
GCP0
IPSEC TUNNEL
MGMT0
MON0
MON1
MON2
MON3
GCP1
VPN0
ICAP0
SUP0
Nagios

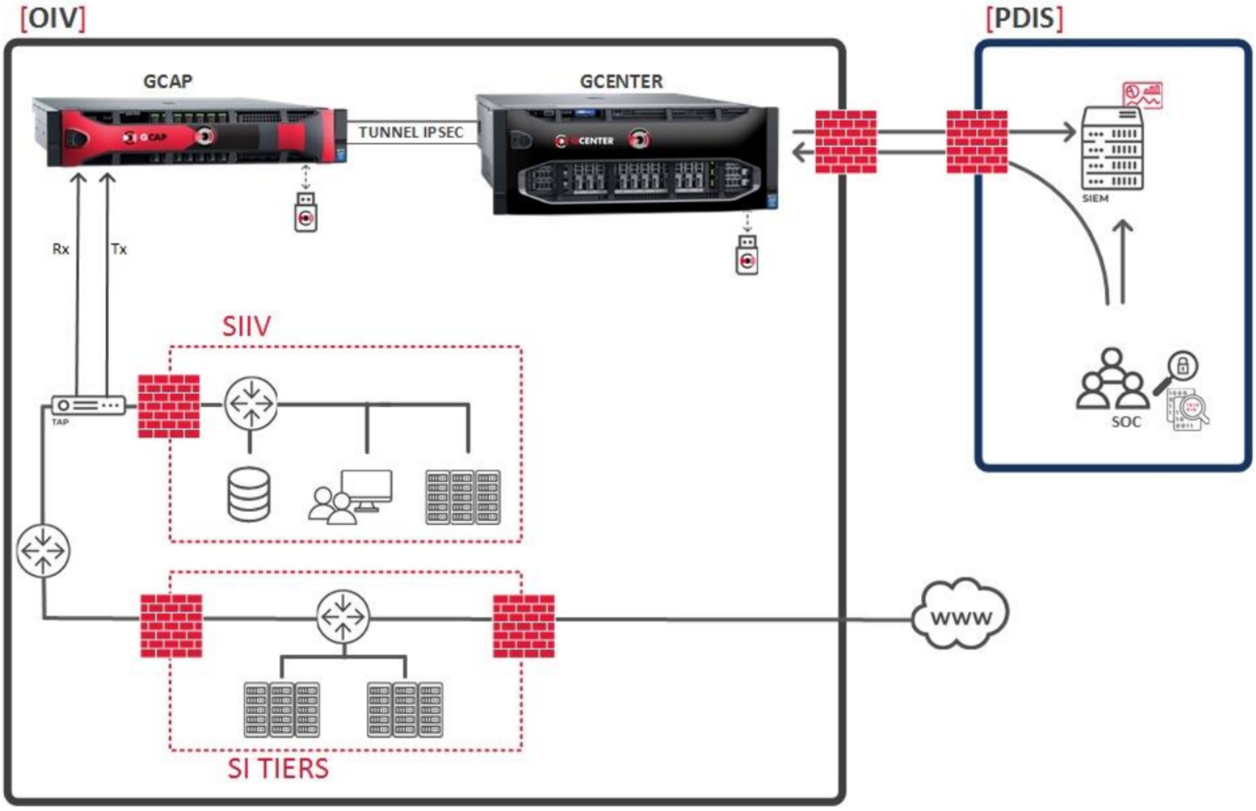
Chapter 5

Example of architectures

Although implementing the TRACKWATCH solution is dependent on the architecture of the IS, here are three examples of typical implementations.







In the case of sensitive information systems, subject to the MPL for example, of the examples provided only the last two are possible.

Chapter 6

Configuration

6.1 Initial configuration

Note:

Installing and configuring the **GCAP** probes is covered in the GCAP documentation available at https://docs.gatewatcher.com/gcap.html.

Although much of the solution is already configured by the Gatewatcher teams, it will be necessary to complete, at a minimum, the network configuration of the GCenter in order to access the interface.

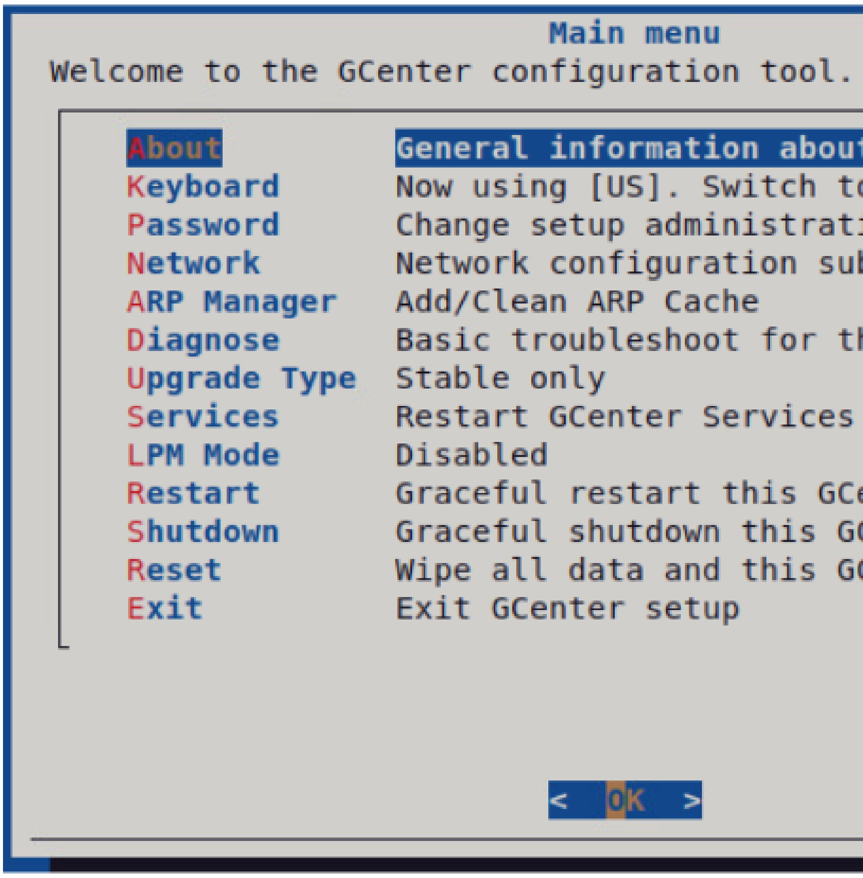
When connecting for the first time, it will be necessary to access the **GCENTER** via the iDRAC interface or a terminal in order to perform the network configuration.

The user to use is the **setup** user, by default the password for this user is: **default**.

Important:

It is essential to change this password as soon as possible.

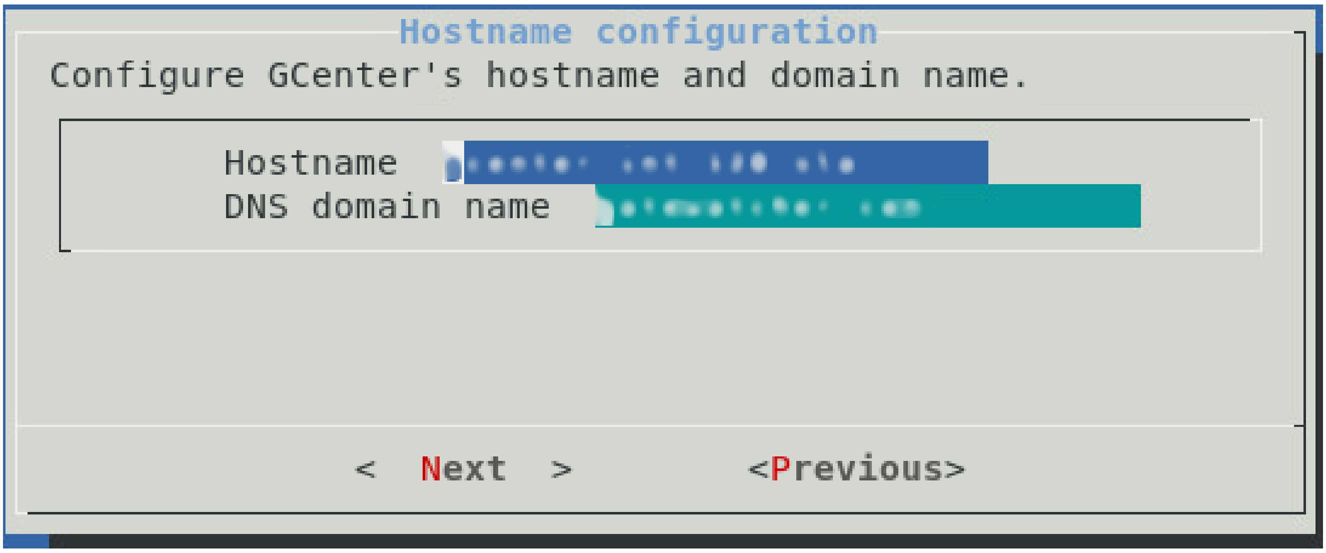
Once logged in, the configuration menu will appear:



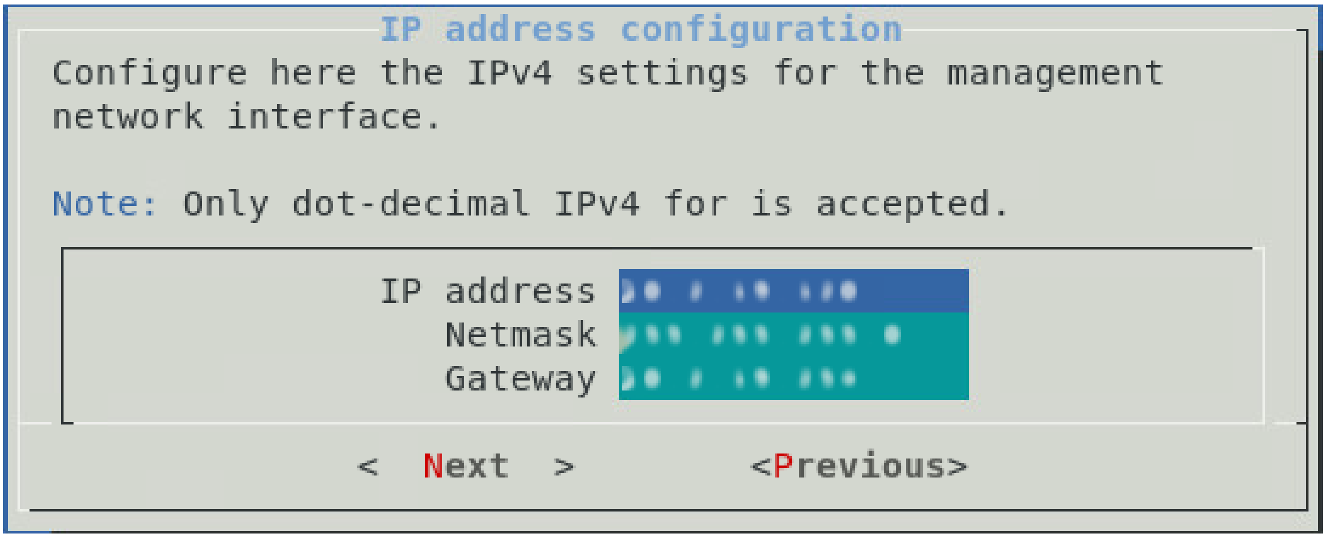
```
                         Main menu
  Welcome to the GCenter configuration tool.

      About           General information about
      Keyboard        Now using [US]. Switch to
      Password        Change setup administrati
      Network         Network configuration sub
      ARP Manager     Add/Clean ARP Cache
      Diagnose        Basic troubleshoot for th
      Upgrade Type    Stable only
      Services        Restart GCenter Services
      LPM Mode        Disabled
      Restart         Graceful restart this GCe
      Shutdown        Graceful shutdown this GC
      Reset           Wipe all data and this GC
      Exit            Exit GCenter setup

                         <  OK  >
```

If necessary, select the *Keyboard* entry to enable an azerty configuration.

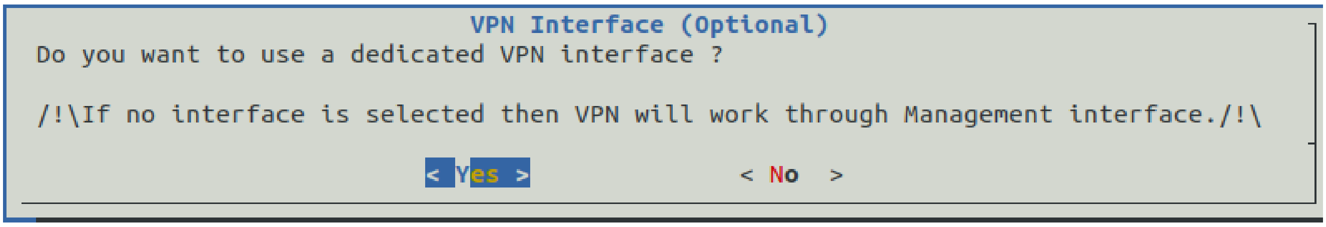
Then by selecting the *Network* entry, simply answer the various questions. Here is an example of the questions asked during the initial configuration.



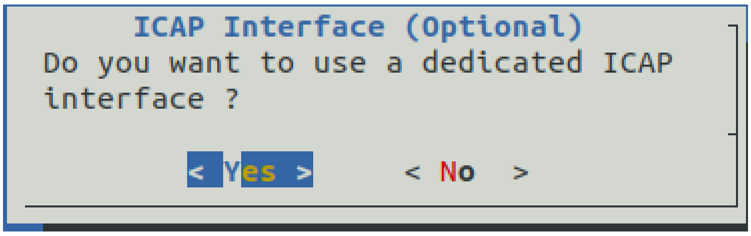
```
              Hostname configuration
 Configure GCenter's hostname and domain name.

        Hostname          [redacted]
        DNS domain name   [redacted]

            <  Next  >        <Previous>
```



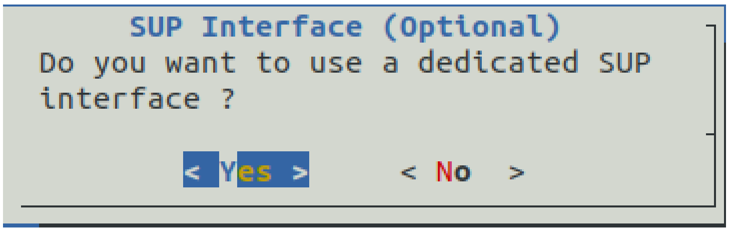
```
IP address configuration
Configure here the IPv4 settings for the management
network interface.

Note: Only dot-decimal IPv4 for is accepted.

      IP address [redacted]
         Netmask [redacted]
         Gateway [redacted]
```



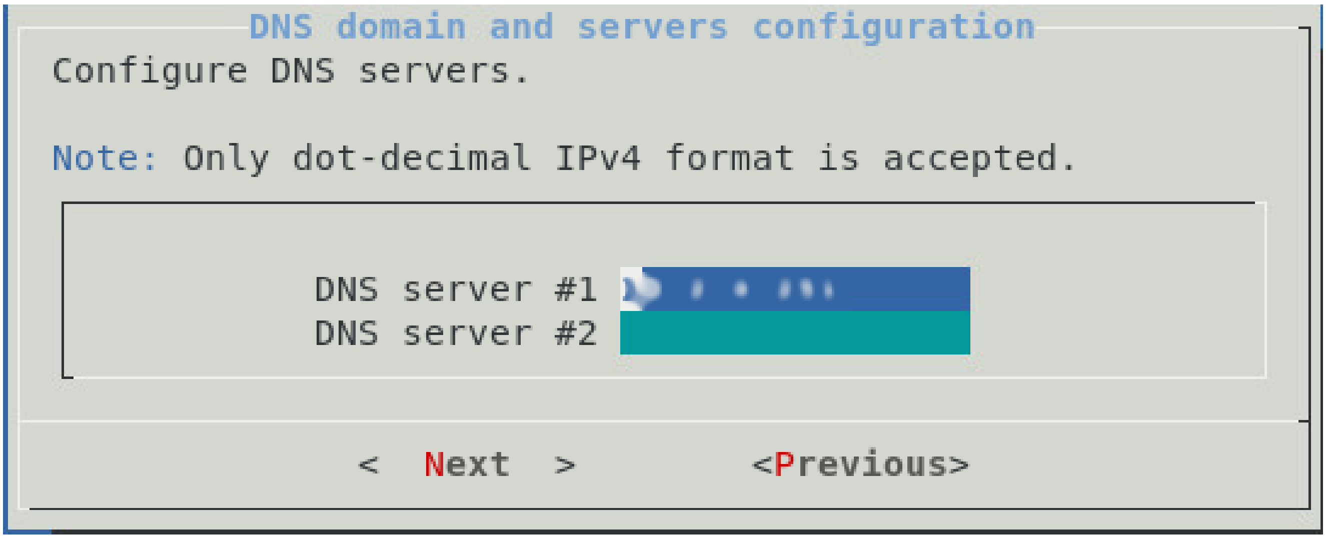
```
VPN Interface (Optional)
Do you want to use a dedicated VPN interface ?

/!\If no interface is selected then VPN will work through Management interface./!\
```



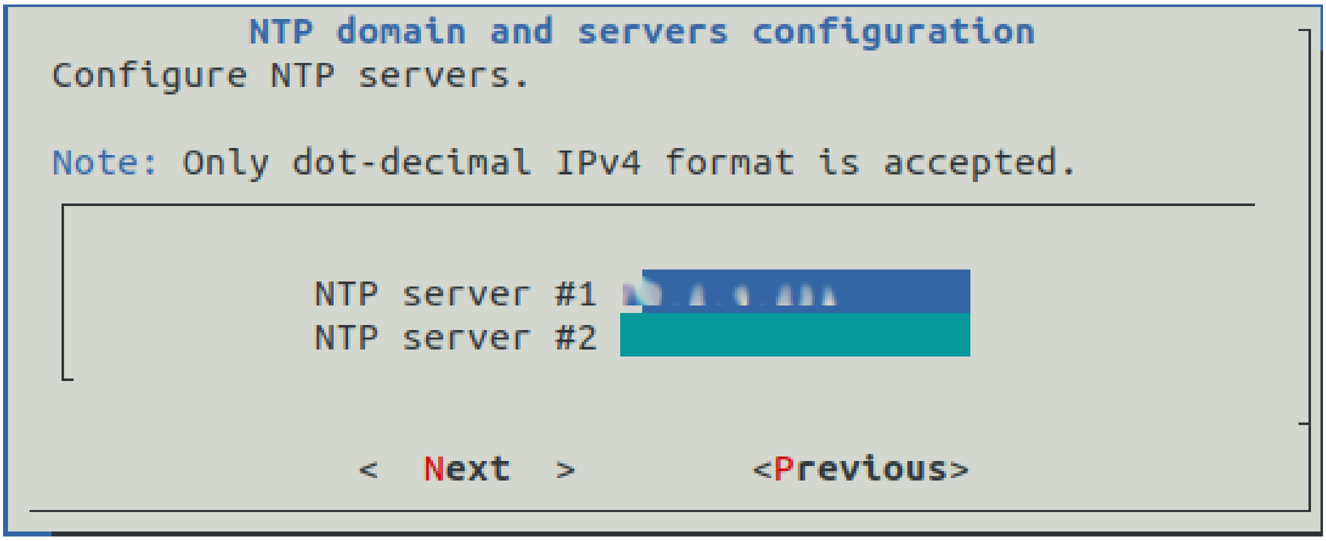
```
ICAP Interface (Optional)
Do you want to use a dedicated ICAP
interface ?
```



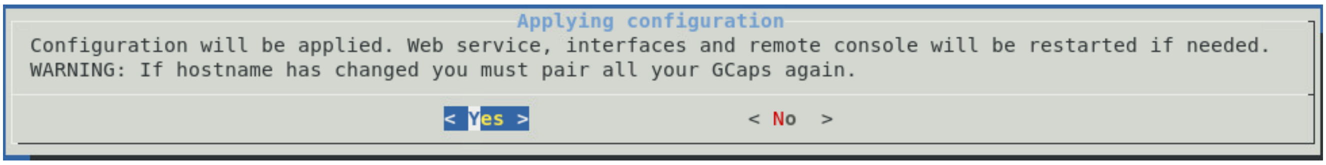
```
SUP Interface (Optional)
Do you want to use a dedicated SUP
interface ?
```



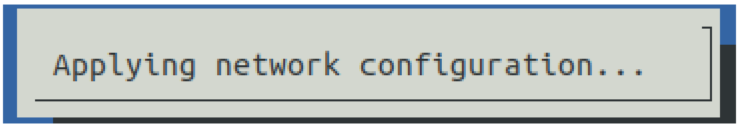
```
DNS domain and servers configuration
Configure DNS servers.

Note: Only dot-decimal IPv4 format is accepted.

   DNS server #1 [redacted]
   DNS server #2
```



```
NTP domain and servers configuration
Configure NTP servers.

Note: Only dot-decimal IPv4 format is accepted.

        NTP server #1 [redacted]
        NTP server #2

      <  Next  >          <Previous>
```



```
Applying configuration
Configuration will be applied. Web service, interfaces and remote console will be restarted if needed.
WARNING: If hostname has changed you must pair all your GCaps again.

              < Yes >                  <  No  >
```



```
Applying network configuration...
```

Once this initial configuration is complete, it is possible to connect to the **GCENTER** interface via a web browser in https at the configured address.

6.2 Global configuration

Rôle Administrateur

Once connected to the interface, in the menu on the left are two sections: Operators and Administrators corresponding to the actions that can be performed by the users of these groups.

The *Gcenter - Configuration* component of the **ADMINISTRATORS** section of the **GCENTER** is particularly important. It will enable major changes to be made to equipment, functions, interconnections, and even analysis results.

From this configuration interface, the administrator will be able to customise the parameters of the **GCENTER** management solution via these seven tabs:

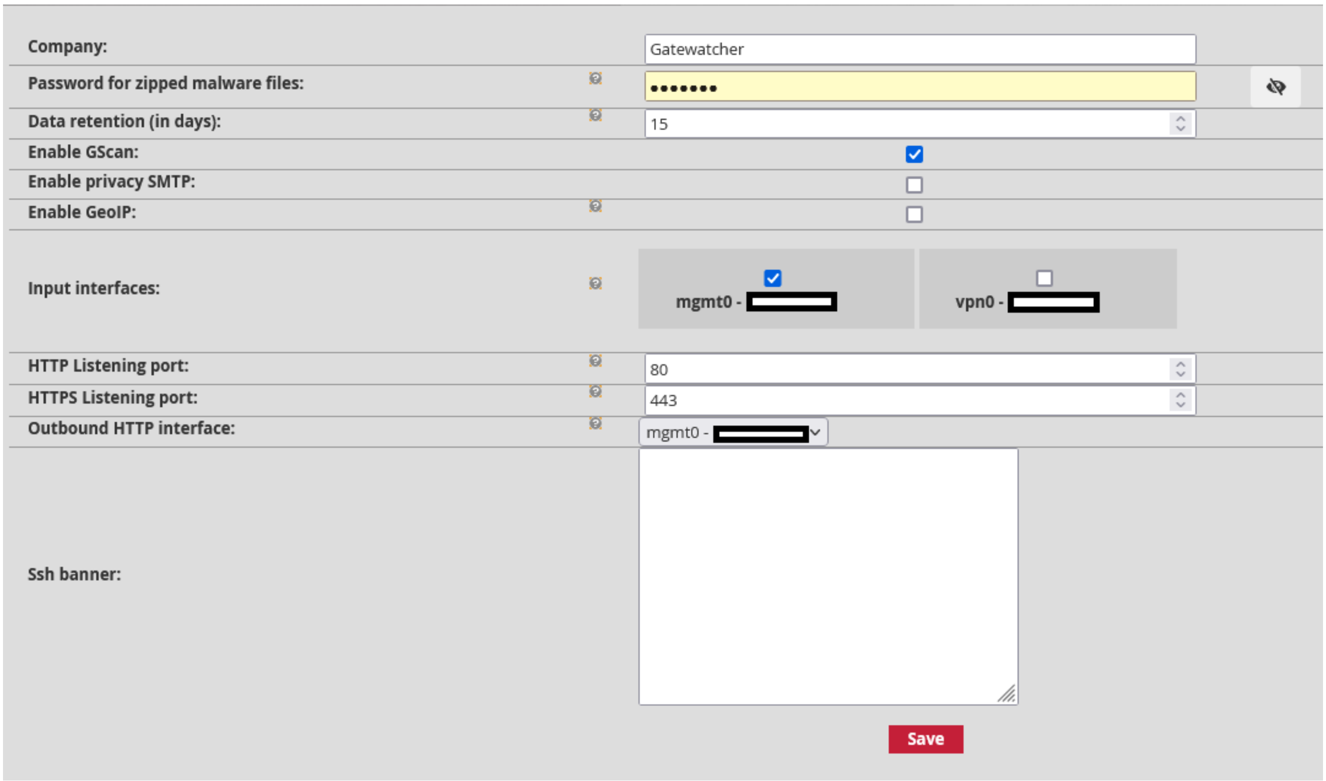
- *Nagios*
- *Global settings*
- *Netdata Export*
- *Proxy settings*
- *SSL settings*
- *Session age settings*
- *Licenses*

6.2.1 Global Settings

Rôle Administrateur

Menu: Administrators > GCenter > Configuration > Global Settings

Each of the menu's sub-options will be detailed for an improved understanding of the product. These options will enable you to refine your criteria as much as possible in order to optimise the general operation.



Company:	Gatewatcher
Password for zipped malware files:	•••••••
Data retention (in days):	15
Enable GScan:	☑
Enable privacy SMTP:	☐
Enable GeoIP:	☐
Input interfaces:	☑ mgmt0 - [redacted] ☐ vpn0 - [redacted]
HTTP Listening port:	80
HTTPS Listening port:	443
Outbound HTTP interface:	mgmt0 - [redacted]
Ssh banner:	

Company (default value: empty): This field enables the company name to be added to the detection analysis reports. These reports can be downloaded after making an association between the TRACKWATCH solution and the Intelligence platform.

Password for zipped malware files (default value: empty): enables you to change the password protecting the archive when downloading malware and unzipping it to avoid an unintentional click. This password will be the same for downloading shellcodes. The details of this Function are described in more depth in *Malcore*

Data retention (in days) (default value: 15): enables choosing the number of days that the TRACKWATCH solution files and index are retained on disk. Note that the configuration is applied in two steps. The first is on the **GCENTER** at this field. The second is on the **GCAP** detection probe in the configuration parameters.

GScan enable (default value: enabled): allows local real-time scanning for malware or suspicious executables. As part of the Military Programming Law, the GScan Function is disabled by default in this management interface.

Privacy SMTP enable (default value: disabled) ensures that privacy rights are respected by hiding the *email.subject* field of SMTP alerts in the GATEWATCHER dashboards for private emails. An email is considered personal if the subject line begins with the words *private*, *personal* or *confidential* (not case sensitive). This option is disabled by default.

GeoIP enable (default value: disabled): allows geolocation of source and destination IP in events. This option must be enabled for the *SmartMap* feature to run. The following fields will be added to events

Input interface: enables/disables the interfaces on which the **GCENTER** will listed on the following ports.

HTTP listening port (default value: 80): the listening port related to the http protocol.

HTTPs listening port (default value: 80): the listening port related to the https protocol.

Outbound HTTP interface: The physical outbound interface for all http flows.

SSH banner (default value: empty): SSH banner presented during pre-authentication on all paired GCaps and the GCenter.

Once the modifications are completed, it will be necessary to record these changes by clicking on the **Save** button.

Important:

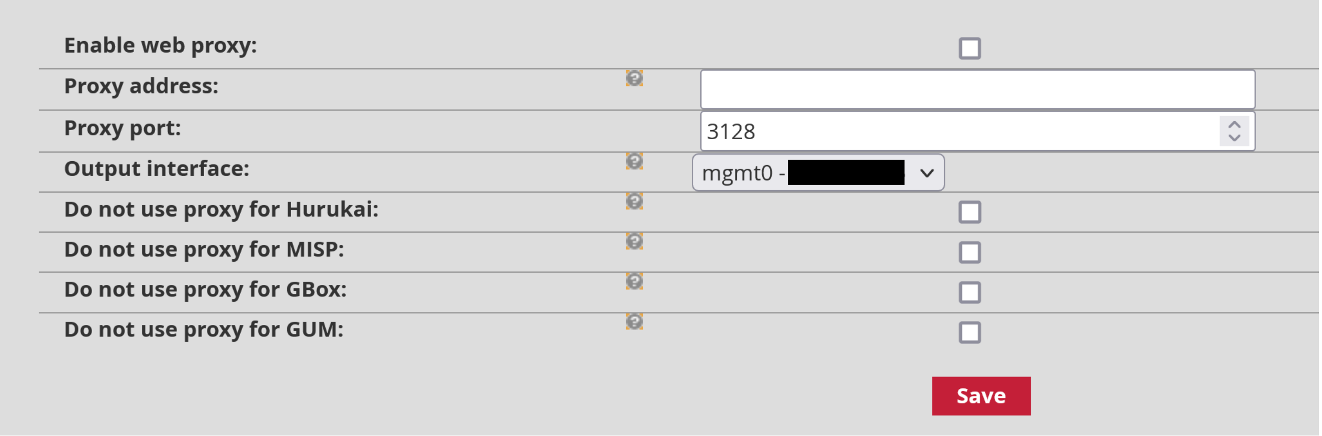
If the **GCENTER** and **GCAP** equipment are in an environment that is part of the Military Planning Law (MPL) framework the GSCAN service is automatically disabled and cannot be activated. For more information, please refer to the MPL section of this document for GScan deactivation.

6.2.2 Proxy Settings

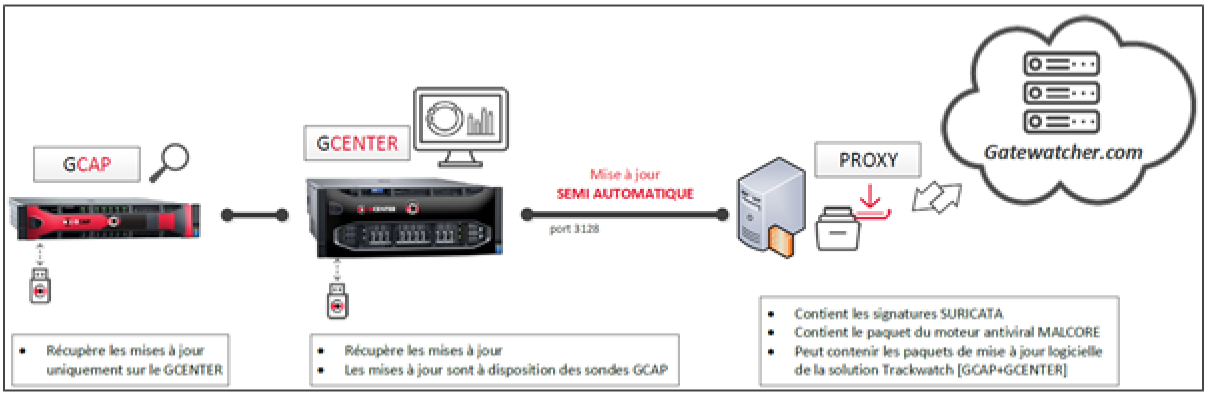
Rôle **Administrateur**

Menu: Administrators > GCenter > Configuration > Proxy Settings

The TRACKWATCH solution includes the possibility of configuring a proxy server (or *proxy*) in order to retrieve updates (signature updates) via the proxy.



Enable web proxy:	□
Proxy address:	
Proxy port:	3128
Output interface:	mgmt0 - [redacted]
Do not use proxy for Hurukai:	□
Do not use proxy for MISP:	□
Do not use proxy for GBox:	□
Do not use proxy for GUM:	□



- Récupère les mises à jour uniquement sur le GCENTER

- Récupère les mises à jour
- Les mises à jour sont à disposition des sondes GCAP

- Contient les signatures SURICATA
- Contient le paquet du moteur antiviral MALCORE
- Peut contenir les paquets de mise à jour logicielle de la solution Trackwatch [GCAP+GCENTER]

Enable Web Proxy: Enables/Disables the use of the proxy

Proxy address: Proxy address as IP address or fully qualified domain name (FQDN)

Proxy port: Proxy listening port (1-65535)

Output interface: the **GCENTER** interface to use to reach the proxy.

Do not use proxy for Hurukai/MISP/GBOX/GUM: Enables the administrator to decide whether to use the proxy settings for integration with [Hurukai](itg-ext. html#hurukai-by-harfanglab)/*MISP* or for access to a *GBOX* or *GUM*.

Once the modifications are completed, it will be necessary to record these changes by clicking on the **Save** button.

This update mode is part of the compliance with the Military Programming Law (MPL). As such, the entity concerned will make its updates on a dedicated update server. For more information, please refer to the *annex concerning MPL related details* of this document and the [update] section (update.html#update-signatures-update).

6.2.3 SSL Settings

Rôle Administrateur

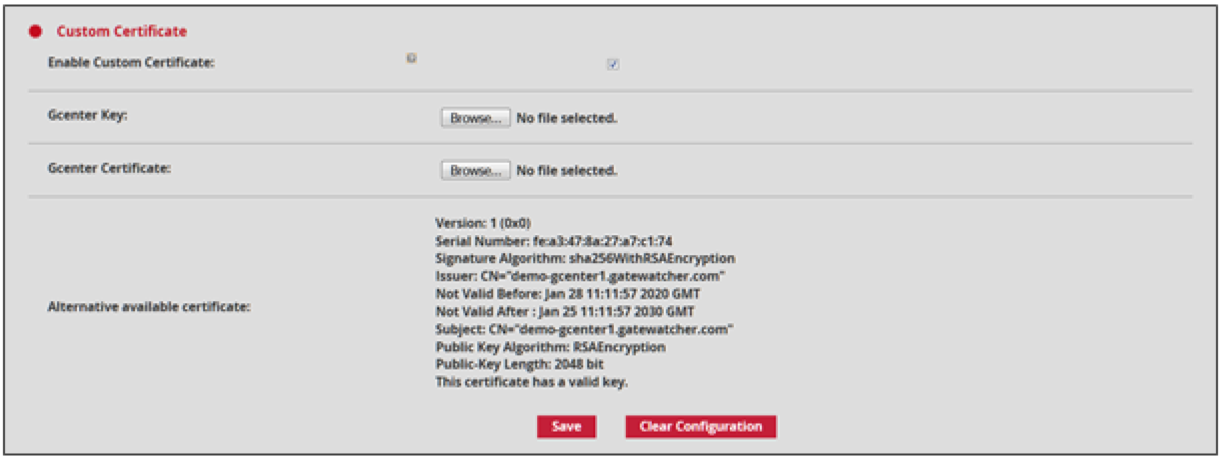
Menu: Administrators > GCenter > Configuration > SSL Settings

This interface enables configuring the Secure Socket Layer (SSL) certificate of the **GCENTER**. The generated certificate will attest to the GCENTER's identity and enable encrypting the exchanged data. From this page it is also possible to configure mutual authentication (mTLS).

The *Security details* section enables obtaining information on the certificate currently in use by the **GCENTER**.

In use certificate details: Displays certificate information such as the date of issue and expiry, and the issuer of the certificate, etc. **CA certificate information**: Displays the information the server holds regarding the certificate authority enabling the correspondents' identity to be determined in the *Dual Authentication* section.

CRL information: lists identifiers that were revoked, invalidated, or are no longer trustworthy.



● Custom Certificate

Enable Custom Certificate: ☑

Gcenter Key: Browse... No file selected.

Gcenter Certificate: Browse... No file selected.

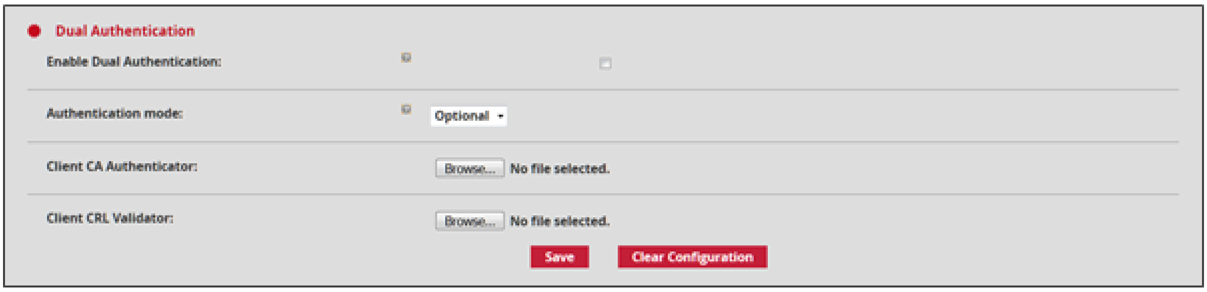
Alternative available certificate:

Version: 1 (0x0)
Serial Number: fe:a3:47:8a:27:a7:c1:74
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN="demo-gcenter1.gatewatcher.com"
Not Valid Before: Jan 28 11:11:57 2020 GMT
Not Valid After : Jan 25 11:11:57 2030 GMT
Subject: CN="demo-gcenter1.gatewatcher.com"
Public Key Algorithm: RSAEncryption
Public-Key Length: 2048 bit
This certificate has a valid key.

The **Custom Certificate** section enables using a specific certificate.

To do so, simply specify the private key in the **GCenter Key** field and the certificate in PEM format in the **GCENTER certificate** field and also activate this certificate by ticking the **Enable Custom Certificate** box.

Finally, the *Dual Authentication* section 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.



● Dual Authentication

Enable Dual Authentication: □

Authentication mode: Optional

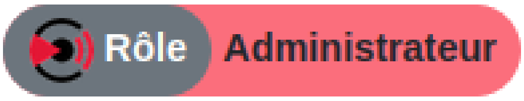
Client CA Authenticator: Browse... No file selected.

Client CRL Validator: Browse... No file selected.

In order to validate this option, it is necessary to add the authority certificate issuing the user certificates in PEM format in the **Client CA Authentication** field, as well as the list of revoked certificates in the **Client CRL Validation** field. Then select the type of authentication *Forced* making it mandatory for users to enter a certificate issued by the certification authority, or *Optional* which only checks if a certificate is present, from 'Authentication mode' after enabling the **Enable Dual Authentication** option.

Once the modifications are completed, it will be necessary to record these changes by clicking on the **Save** button for each modified section.

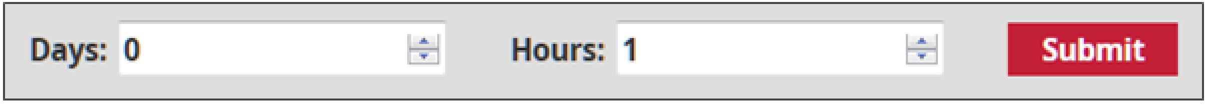
6.2.4 Session age settings



Menu: Administrators > GCenter > Configuration > Session age settings

This section enables configuring the maximum total duration of a session on the GCenter web interface.

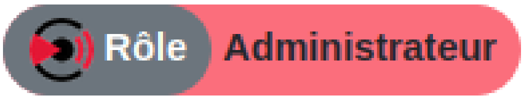
Simply enter the maximum duration of a session in the **Days** and **Hours** fields, then validate.



Days: 0

Hours: 1

6.2.5 Licenses



Menu: Administrators > GCenter > Configuration > License

The License section enables obtaining information on the current license, and to check its validity and available functions.

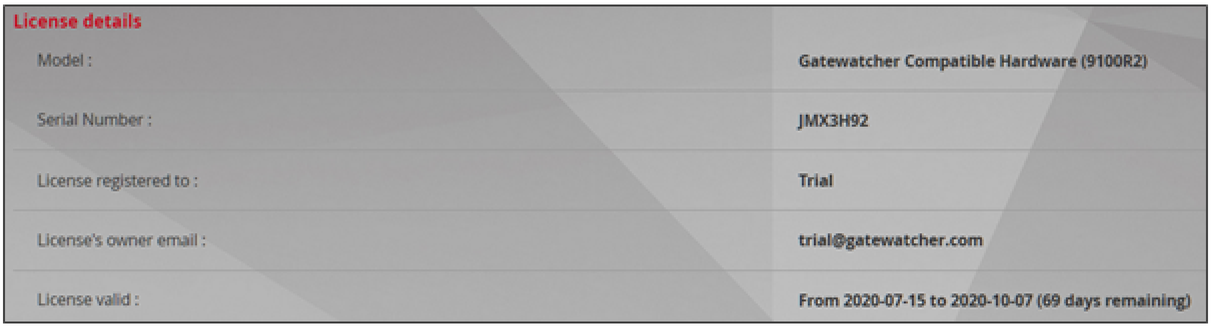
The *Licence details* section enables obtaining information on the material for which this licence was issued via its model and serial number, together with the period of validity of the licence, the associated contact address, and type of licence.

Then, in the *Licence features* section, it is possible to determine the availability of the various modules that will be explained in the rest of this documentation.

Finally, it is possible at the bottom of the page to enter a new licence, and also to set the notification in the interface of a near expiry date by entering the number of days before the expiration.

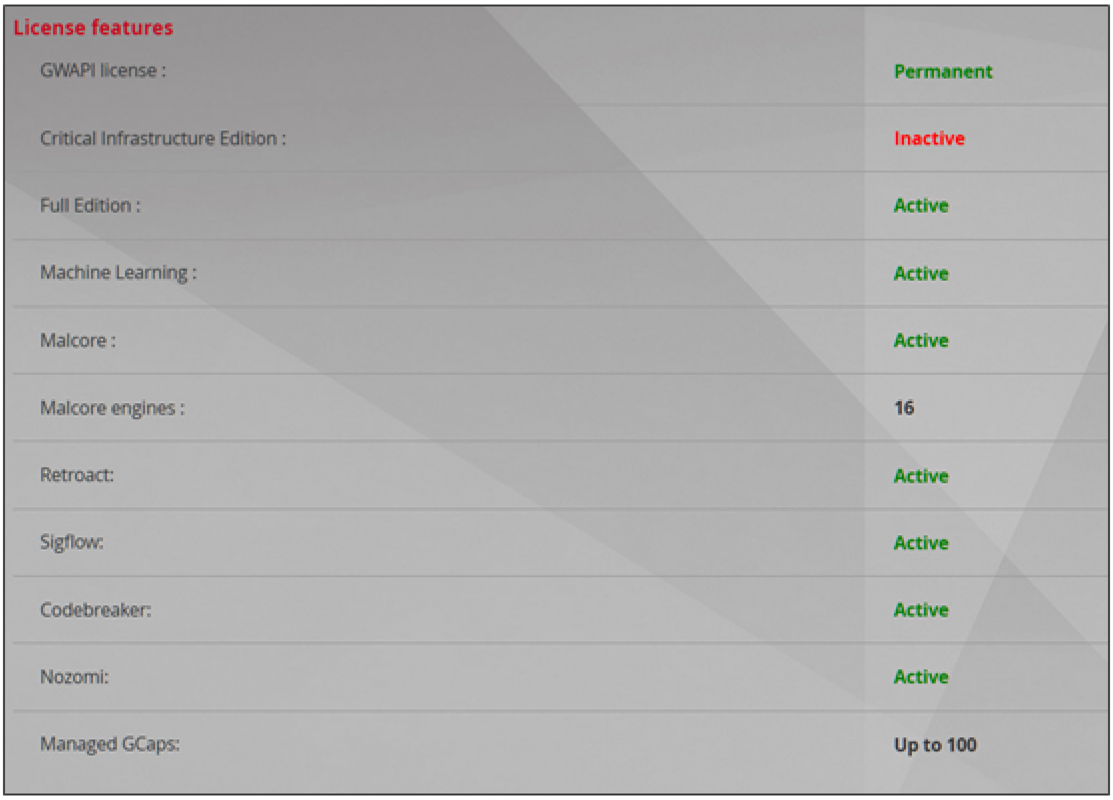
To obtain a **GCENTER** licence, please contact your GATEWATCHER business engineer or contact them at commerciaux@GATEWATCHER.com .

Once the license is validated and activated, the content of the page updates and displays the details of the license.



License details

Model :	Gatewatcher Compatible Hardware (9100R2)
Serial Number :	JMX3H92
License registered to :	Trial
License's owner email :	trial@gatewatcher.com
License valid :	From 2020-07-15 to 2020-10-07 (69 days remaining)



License features

GWAPI license :	Permanent
Critical Infrastructure Edition :	Inactive
Full Edition :	Active
Machine Learning :	Active
Malcore :	Active
Malcore engines :	16
Retroact:	Active
Sigflow:	Active
Codebreaker:	Active
Nozomi:	Active
Managed GCaps:	Up to 100

In the event of a missing or expired licence, the interface will automatically redirect to this page to resolve the issue.

Chapter 7

Presentation

GCAP is the probe enabling the capturing of network flows. It enables generating alerts, providing metadata on the various protocols, and reconstructing the captured files. This data is then transmitted to the **GCenter** in order to continue the analysis of the elements, and to enrich and make available the information generated.

More information on **GCAP** is available in its documentation

Chapter 8

Pairing

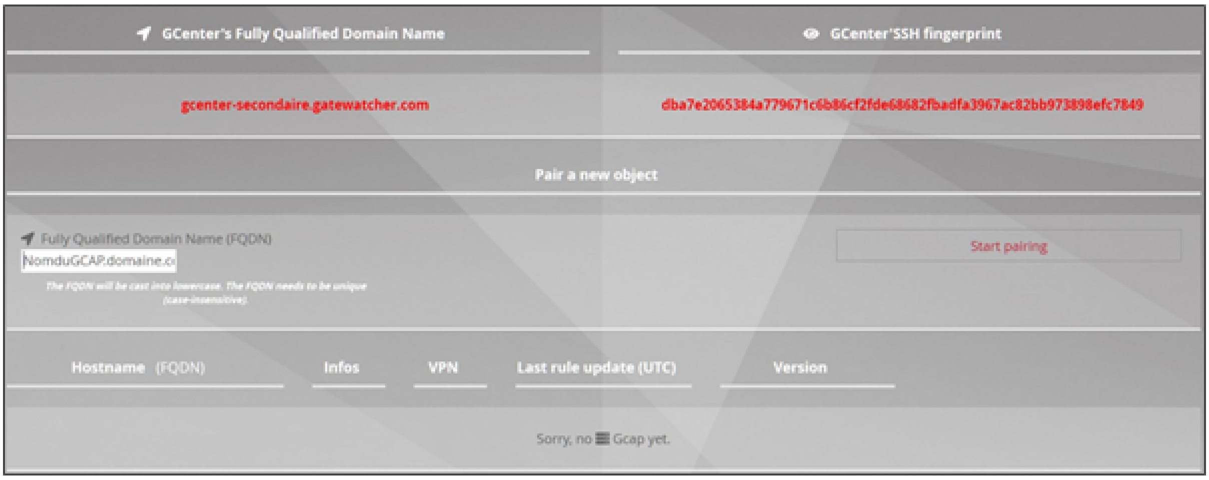
8.1 Add a GCAP

Rôle Administrateur

Menu: Administrators > GCAP Pairing/Status

In order for TRACKWATCH equipment to interact, a **GCAP** probe must first be added.

Pairing enables configuring the IPSec tunnel between the **GCAP** and the **GCENTER**.



GCenter's Fully Qualified Domain Name	GCenter'SSH fingerprint
gcenter-secondaire.gatewatcher.com	dba7e2065384a779671c6b86cf2fde68682fbadfa3967ac82bb973898efc7849

Pair a new object

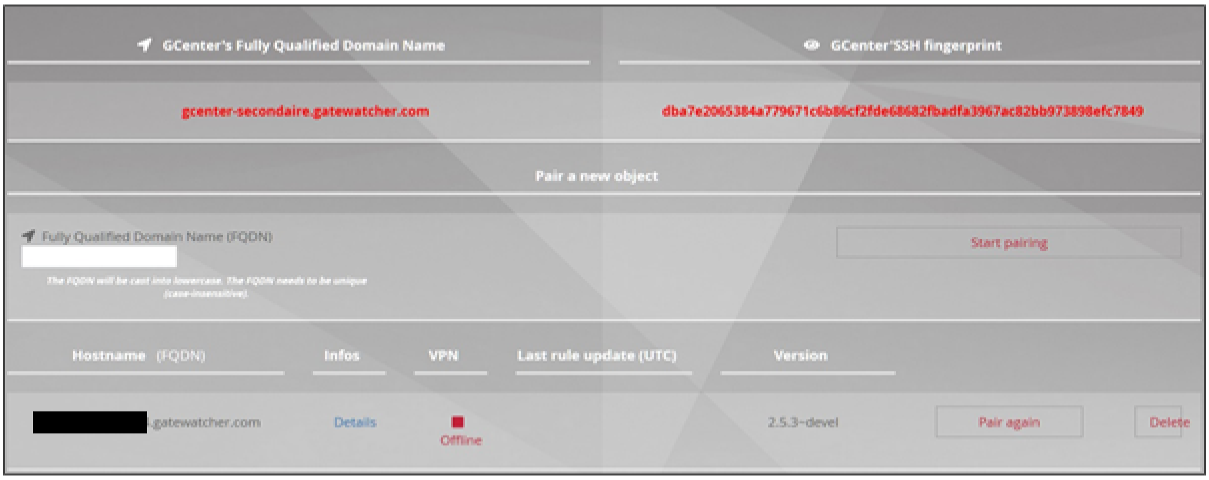
Fully Qualified Domain Name (FQDN): NomduGCAP.domaine.c

The FQDN will be cast into lowercase. The FQDN needs to be unique (case-insensitive).

Hostname (FQDN)	Infos	VPN	Last rule update (UTC)	Version
Sorry, no ☰ Gcap yet.				

It is necessary to fill in the **Fully Qualified Domain Name FQDN** field (Example: '*GCAPname.domain.com*') in the *Pair a new object* section.

After that, you must press the **Start pairing** button to initiate the process.



GCenter's Fully Qualified Domain Name: gcenter-secondaire.gatewatcher.com

GCenter'SSH fingerprint: dba7e2065384a779671c6b86cf2fde68682fbadfa3967ac82bb973898efc7849

Pair a new object

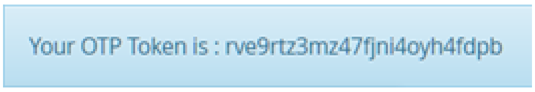
Fully Qualified Domain Name (FQDN)

The FQDN will be cast into lowercase. The FQDN needs to be unique (case-insensitive).

Hostname (FQDN)	Infos	VPN	Last rule update (UTC)	Version		
[redacted].gatewatcher.com	Details	■ Offline		2.5.3-devel	Pair again	Delete

This operation will generate an OTP on the **GCENTER** web interface. This must be filled in on the **GCAP** probe in order to successfully pair the devices.

The **GCENTER's Fully Qualified Domain Name** field is used to verify the tunnel and network connection certificates being established.



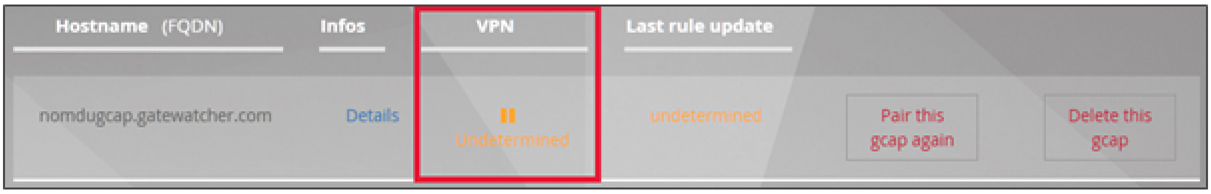
Your OTP Token is : rve9rtz3mz47fjni4oyh4fdpb

The **GCENTER'SSH fingerprint** enables you to ensure that the **GCAP** is communicating with the correct **GCENTER**. This is the **GCENTER** fingerprint. This process is described in more detail in the **GCAP** documentation.

Once the pairing process is complete, it is possible to check via the **GCENTER** interface if the linkage was successful.

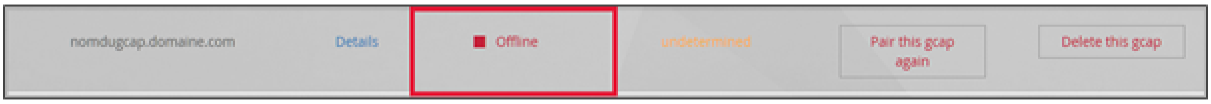
The Online, Undetermined, and Offline statuses identify the status of the VPN link.

The client-side VPN is in an unknown status **GCENTER**:



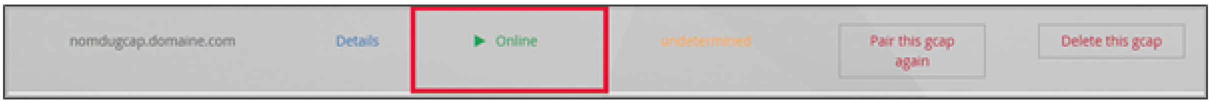
Hostname (FQDN)	Infos	VPN	Last rule update		
nomdugcap.gatewatcher.com	Details	⏸ Undetermined	undetermined	Pair this gcap again	Delete this gcap

The client-side VPN is disconnected from **GCENTER**:



nomdugcap.domaine.com	Details	■ Offline	undetermined	Pair this gcap again	Delete this gcap

The client-side VPN is paired with the **GCENTER**:



nomdugcap.domaine.com	Details	▶ Online	undetermined	Pair this gcap again	Delete this gcap

Diagnostic statuses are available from the 'VPN' tab so that the administrator can quickly verify the correct association.

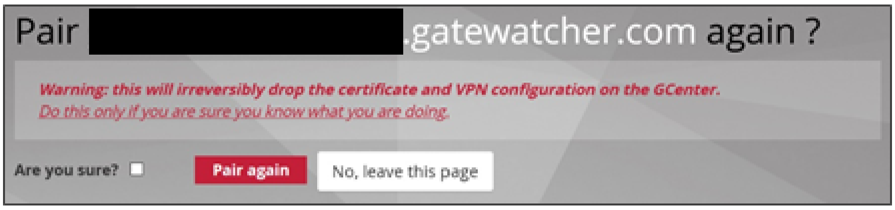
8.2 Re-pairing a GCAP

Rôle Administrateur

Menu: Administrators > GCAP Pairing/Status

If necessary, a **GCAP** can be re-paired to the **GCenter**.

To do this, simply click on **Pair again** and repeat the same process to pair the probe with the **GCENTER**.



Pair [redacted].gatewatcher.com again ?

Warning: this will irreversibly drop the certificate and VPN configuration on the GCenter.
Do this only if you are sure you know what you are doing.

Are you sure? □ Pair again No, leave this page

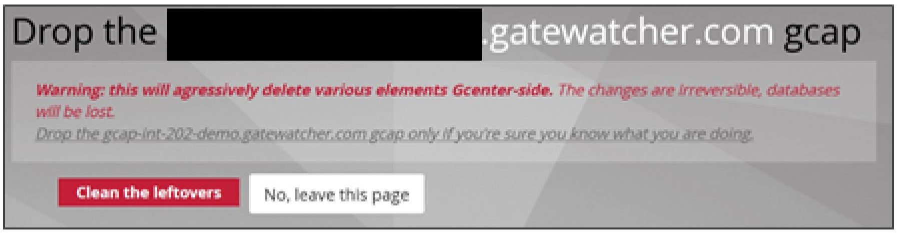
The administrator must tick the 'Are you sure?' box before validating the procedure.

8.3 Delete a GCAP

Rôle Administrateur

Menu: Administrators > GCAP Pairing/Status

It is possible to remove a **GCAP** from the management platform using the **Delete** button.



Drop the [redacted].gatewatcher.com gcap

Warning: this will agressively delete various elements Gcenter-side. The changes are irreversible, databases will be lost.
Drop the gcap-int-202-demo.gatewatcher.com gcap only if you're sure you know what you are doing.

Clean the leftovers No, leave this page

The administrator must tick the 'Are you sure?' box before validating the procedure.

This will remove all data relating to the GCAP pairing such as certificates and configuration. Any logs, metadata or alerts, generated in the past and indexed in elasticsearch will not be modified.

Chapter 9

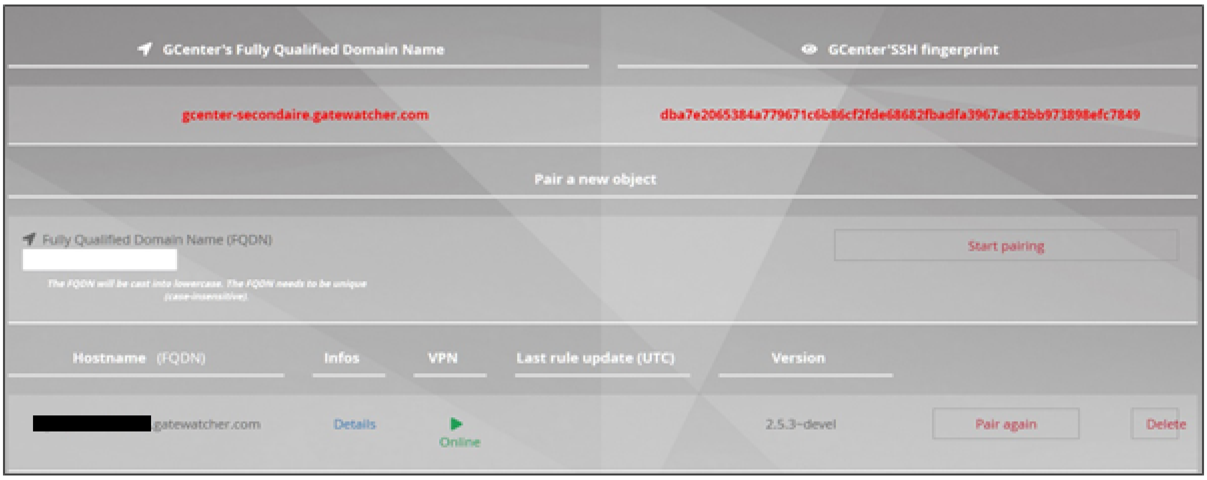
Configuration

9.1 Details of a GCAP

Rôle Administrateur

Menu: Administrators > GCAP Pairing/Status

Once the VPN tunnel is in the *Online* status, it is possible to access information pertaining to the **GCAP** probe.



GCenter's Fully Qualified Domain Name	GCenter'SSH fingerprint
gcenter-secondaire.gatewatcher.com	dba7e2065384a779671c6b86cf2fde68682fbadfa3967ac82bb973898efc7849

Pair a new object

Fully Qualified Domain Name (FQDN)

The FQDN will be cast into lowercase. The FQDN needs to be unique (case-insensitive)

Hostname (FQDN)	Infos	VPN	Last rule update (UTC)	Version		
[redacted]gatewatcher.com	Details	▶ Online		2.5.3-devel	Pair again	Delete

This table enables you to easily view the status of all **GCAP** probes associated with the **GCENTER**.

Hostname (FQDN): The fully qualified name of the probe.

Last rule update (UTC): corresponds to the time stamp of the most recent update in UTC in the format [**year-month-day hh**: **mm**: **ss**] of the Sigflow engine signature rules.

Version': corresponds to the software release (Example: '_2-5-3~_prod') of the **GCAP** detection probe.

The **Info** column provides more information on the **GCAP** probe, thanks to the **Details** button.

Network, system and Sigflow engine acquisition data are sent to the **GCENTER**. The administrator has real-time access to the monitoring of the elements of the **GCAP** capture probe including hard drive throughput, processor, memory, network traffic, and network interfaces, etc.

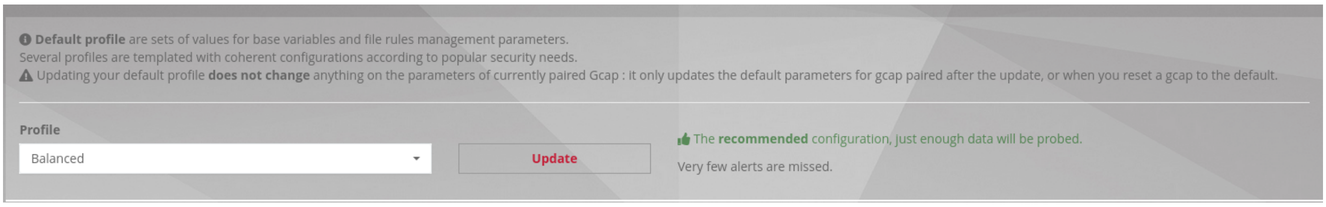
The following metrics are escalated:

9.2 Set a default profile

Rôle Administrateur

Menu: Administrators > GCAP Pairing/Status

The default profiles are sets of values for *Base variables* and *Files rules management*.



Default profile are sets of values for base variables and file rules management parameters.
Several profiles are templated with coherent configurations according to popular security needs.
⚠ Updating your default profile **does not change** anything on the parameters of currently paired Gcap : it only updates the default parameters for gcap paired after the update, or when you reset a gcap to the default.

Profile: Balanced

The **recommended** configuration, just enough data will be probed.
Very few alerts are missed.

Several profiles are available depending on the current security requirements:

- Minimal: the minimal configuration.
- Balanced: the configuration recommended by Gatewatcher.
- MPL: the configuration required in MPL mode.
- Paranoid: all parameters are activated.
- Intuitio: Configuration for the NDR.

Updating your default profile does not change the settings of the currently paired Gcap.

Updates are managed via the **GUM** (**G**atewatcher**U**pdate**M**anager) module.

This module is used to update the solution, and this as well for the update of detection signatures and anti-viral engines (update), as for the application of corrective patches (*Hotfix*) and the GCenter or GCap version upgrades.

Chapter 10

Upgrade

Unlike *updates*, *upgrades* (*hotfix*) cannot be automated. They must be performed by an administrator **after reviewing the *release notes and upgrade notes***.

In the case of a minor upgrade, for example from v2.3.5.101 to 2.3.5.101-hf1, there are two ways to accomplish an upgrade:

- By applying only the *hotfix* HF1 as described in the *next section*
- By performing a full upgrade as described *below* These two solutions are equivalent.

However, in the case of a major upgrade, for example from v2.3.5.100 to 2.3.5.101, only the *upgrade procedure* is applicable.

10.1 Hotfix

Rôle Administrateur Mode LPM non disponible

Menu: Administrators > GUM > Hotfix

> important:: The Hotfix menu is not available if the TRACKWATCH solution is deployed in an MPL environment. It will then be necessary to go through a version upgrade.

More details are available in the section of the documentation dedicated to MPL deployment specifics.

A Hotfix enables a given correction or modification to be applied without having to upgrade the entire solution. In most cases, hotfixes will not require restarting the service.

All hotfix packages can be downloaded via our download platform https://update.gatewatcher.com/hotfix. Patches are listed according to the **GCENTER** version.

From the **GCENTER** web interface, the administrator can apply the previously downloaded hotfix and click **Send hotfix**.

Applying the patch will be taken into account after pressing ** Apply from the ** Saved package list**.

After this manipulation, the equipment will not restart, however the application of these correction packages generates an automatic restart of the WebUI of the **GCENTER**. A manual page refresh may be needed.

The patch packages become cumulative as of version 2.5.3.101.

The description of each corrective package in release notes is available from the website at https://releases.gatewatcher.com.

10.2 Upgrade

Rôle Administrateur

Menu: Administrators > GUM > Upgrade

Important:

All KIBANA objects (dashboards, visualisation, and search, ...) created in version 2.5.3.100 will be deleted upon the first start of version 2.5.3.101. An export/import of the parameters is required to keep the configuration of the objects during the upgrade to 2.5.3.101

This section enables upgrading the TRACKWATCH solution.

All upgrade packages can be accessed via our download platform https://update.GATEWATCHER.com. They can be found in the section according to version **2.5.3.X** then **GCENTER** , **GCAP** or **GBOX**.

In https://update.GATEWATCHER.com/upgrade/2.5.3.101/GCENTER/, the time, the status, the SHA256, and the status of the last patches are respectively filled in. A complete package of the latest fixes to the release is also available under the name GCENTER-2.5.3.101-xxxx_prod-hfx.gwp.

The administrator can then apply the previously downloaded functional update and click **Submit**.

Applying the upgrade package will be taken into account after pressing ** Apply from the ** Saved package lists**.

Once this operation is completed, the equipment will restart.

The description of each corrective package in release notes is available from the website at https://releases.GATEWATCHER.com.

Chapter 11

Updating signatures (Update)

11.1 Update mode

The product can be updated in three different ways depending on the requirements of the information system in which the solution is deployed: *Online* update, *Manual* update, and *Local* update.

11.1.1 Online mode

The online update enables automated updates and reduces administration tasks.

Updates are done automatically from https://update.GATEWATCHER.com and https://gupdate.GATEWATCHER.com.

Note:

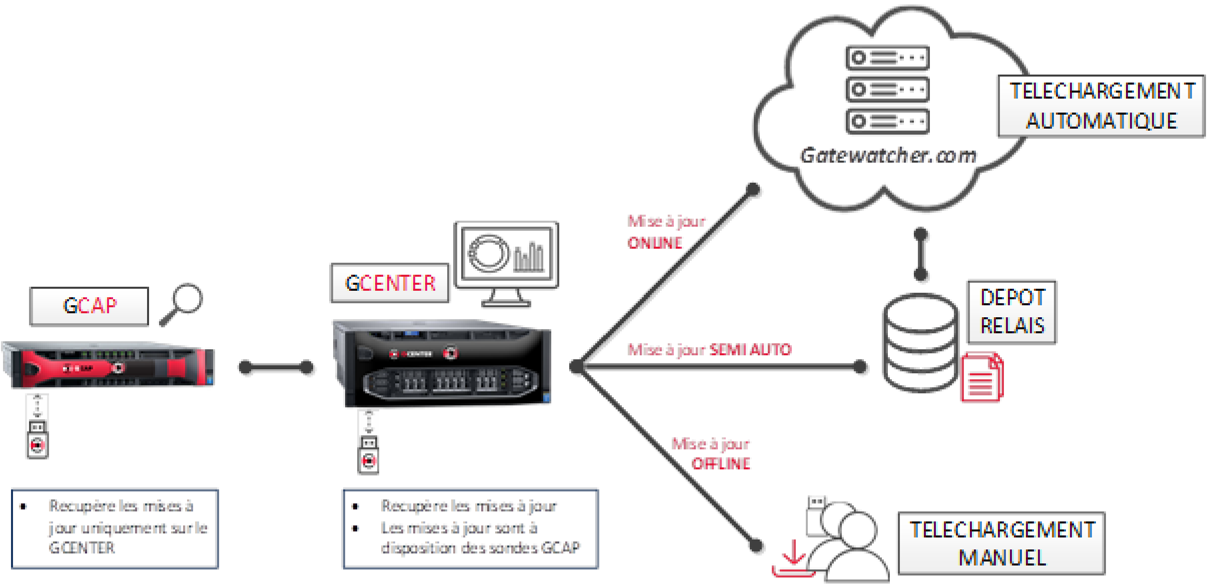
In the case of scheduled *online* mode, scheduling applies only to the **SigFlow** engine. Updates to the **Malcore** engine are performed every 15 minutes.

11.1.2 Manual mode

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 Gcenter via the web interface.

11.1.3 Local mode

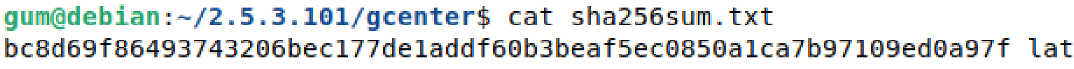
In order to meet specific security constraints, **GCenter** is able to fetch its updates from a local repository.


TELECHARGEMENT AUTOMATIQUE
Gatewatcher.com
Mise à jour ONLINE
GCAP
GCENTER
Mise à jour SEMI AUTO
DEPOT RELAIS
Mise à jour OFFLINE
TELECHARGEMENT MANUEL
Recupère les mises à jour uniquement sur le GCENTER
Recupère les mises à jour
Les mises à jour sont à disposition des sondes GCAP

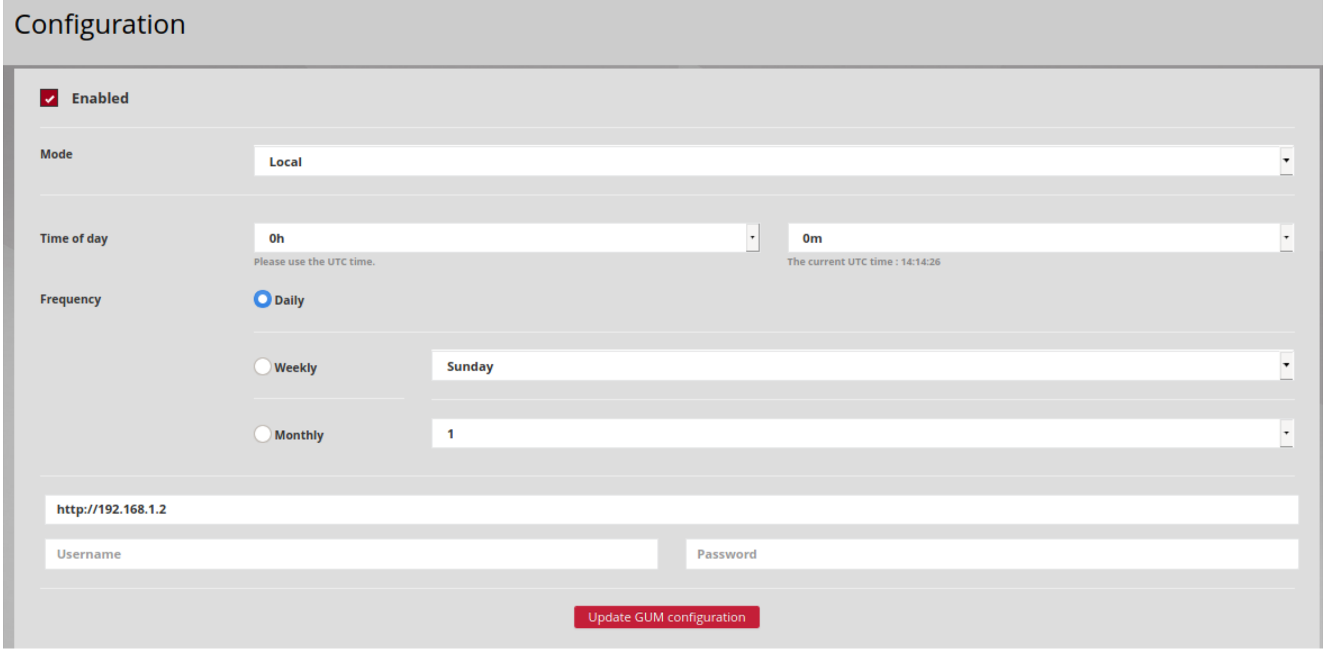
The steps to configure a local repository are as follows:

- Prerequisites: A Web server monitoring on port 80
- Create the following tree structure: "2.5.3.10X/GCenter" depending on the GCenter version (2.5.3.100 or 2.5.3.101). In the following configuration example this tree should be created at the root of the server.
- Retrieve a gwp file (latest_full.gwp for a GCenter V100, latest_full_v3.gwp for a 2.5.3.101) from https://update.gatewatcher.com/update/
- In "2.5.3.10X/GCenter", insert the gwp file retrieved previously.
- In "2.5.3.10X/GCenter", place a sha256sum.txt file that contains a "sha256sum FileName" entry

Example of a `sha256sum.txt` file



```
gum@debian:~/2.5.3.101/gcenter$ cat sha256sum.txt
bc8d69f86493743206bec177de1addf60b3beaf5ec0850a1ca7b97109ed0a97f lat
```



Configuration

☑ Enabled

Mode: Local

Time of day: 0h | 0m

Please use the UTC time.

The current UTC time : 14:14:26

Frequency: ● Daily

○ Weekly: Sunday

○ Monthly: 1

http://192.168.1.2

Username | Password

11.2 Configuration

Rôle Administrateur

Menu: Administrators > GUM > Config

The GUM menu enables entering the necessary parameters for using the online or local mode.

The configuration of the update parameters (signature update) is activated by ticking the **Enabled** box.

The mode can be selected from the list:

- *Local*
- *Online*

Defining when updates are to be made is done via the **Time of day** and **Frequency** fields.

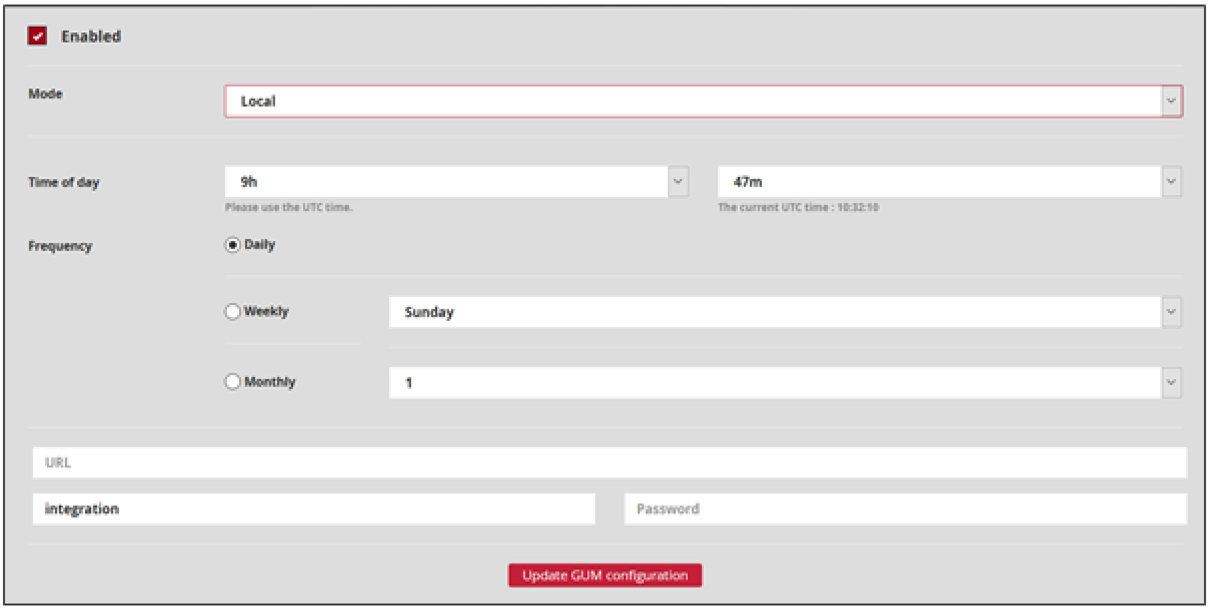
The **URL** field enables specifying the address where **GUM** should check for updates. In the case of an *Online* update,

In the case of online mode, an **intelligence** account will be required for the update package to be downloaded from the site. This user and password combination must be entered in the **Username** and **Password** fields below the address. The **URL** field will be automatically filled in when selecting the **Online** mode. Update packages are retrieved from GateWatcher servers https://update.GATEWATCHER.com/update/.

In the case of local mode, it is necessary to specify the address of the local repository.

The TRACKWATCH solution also provides the possibility to configure a proxy server to reach this repository. This option can be configured in the [Proxy Settings] section (install.html#proxy-settings).

Validation of the form from the 'Update GUM configuration' button is mandatory for the information entered to be taken into account.



☑ Enabled

Mode: Local

Time of day: 9h 47m

Please use the UTC time.

The current UTC time : 10:32:10

Frequency: ● Daily

○ Weekly Sunday

○ Monthly 1

URL

integration

Password

11.3 Manual update of the engines

Rôle Administrateur

Menu: Administrators > GUM > Update

Important:

As of version 2.5.3.101, please use the updates marked with a version 3.

All updates are available through our download platform https://update.GATEWATCHER.com. Once the update package is downloaded, the update of the MALCORE and SIGFLOW engines is done on **GCENTER**.

Three packages can be used to manually perform the updates. The *sigflow* packages to update the detection rules, the *malcore* packages to update the antiviral engines, and *full* to update both engines at the same time.

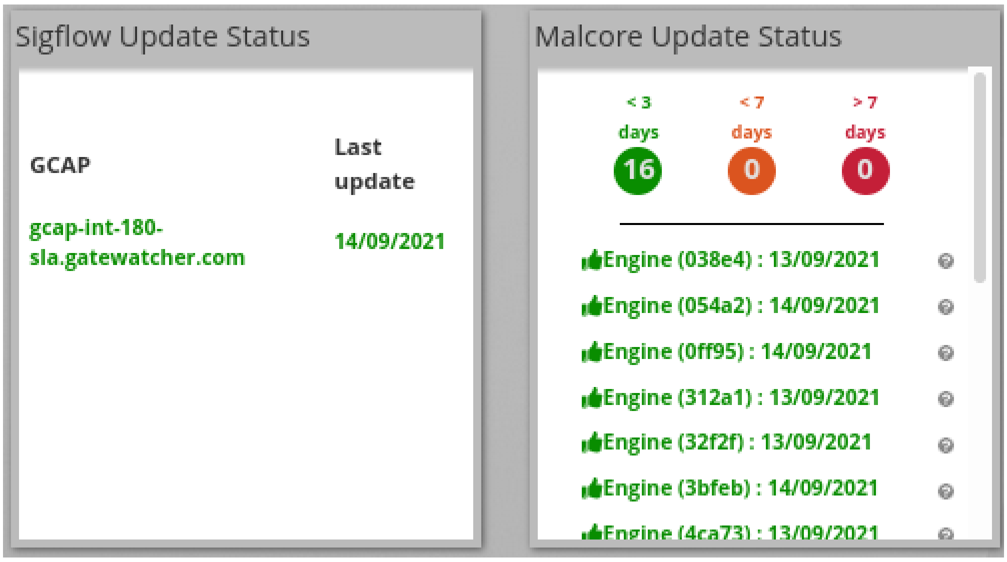
From the **GCENTER** web interface, in the **GUM/Updates** section, the administrator is able to drop the update package and apply it by selecting **Apply**.

11.4 Checking for updates

Rôle Administrateur

Menu: Home Page

The date of the last update of the *Sigflow* and *Malcore* engines is visible directly from the HomePage, accessible by clicking on the **Gatewatcher** logo at the top of the left-hand menu.



Sigflow Update Status

GCAP	Last update
gcap-int-180-sla.gatewatcher.com	14/09/2021

Malcore Update Status

< 3 days	< 7 days	> 7 days
16	0	0

Engine (038e4) : 13/09/2021

Engine (054a2) : 14/09/2021

Engine (0ff95) : 14/09/2021

Engine (312a1) : 13/09/2021

Engine (32f2f) : 13/09/2021

Engine (3bfeb) : 14/09/2021

Engine (4ca73) : 13/09/2021

Chapter 12

Presentation

The MALCORE and RETROACT detection engines enable:

- Detecting malware through a static and heuristic multi-engine analysis of files in real time.
- Analysis via 16 Anti-Virus engines.
- An analysis capacity of more than 6 million files per 24 hours.
- Malware detection by re-analysing potentially harmful files after they pass through with new signatures and heuristic methods.

Chapter 13

Configuration

Rôle Administrateur

Menu: Administrators > GCenter > Malcore Management

The MALCORE management interface enables modifying the **GCENTER** analysis parameters. From this section, the administrator is able to adjust the global detection parameters of the **GCENTER**:

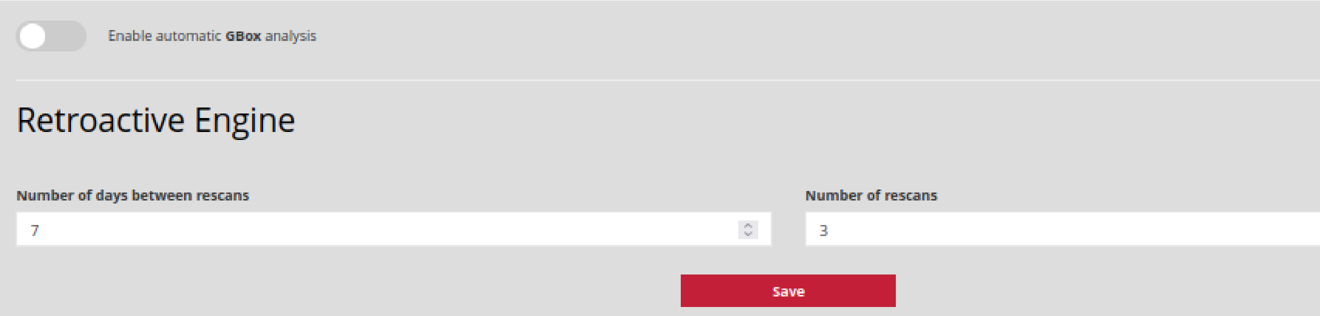
- *Global settings*
- *Profiles*
- *White List*
- *Black List*

13.1 Global settings

Rôle Administrateur

Menu: Administrators > GCenter > Malcore Management > Global Settings

The **RETROACT** analysis engine enables post-compromise detection by reanalysing, a posteriori, files whose malicious potential is suspected by MALCORE's heuristic analysis. These subsequent scans are performed over a configurable period of time, several days/weeks/months after the file has passed, with the new signatures and heuristic methods.



Enable automatic **GBox** analysis

Retroactive Engine

Number of days between rescans: 7

Number of rescans: 3

Number of days between rescans: This is the time period in days between each file rescan.

Number of rescans: corresponds to the amount of rescans to be performed.

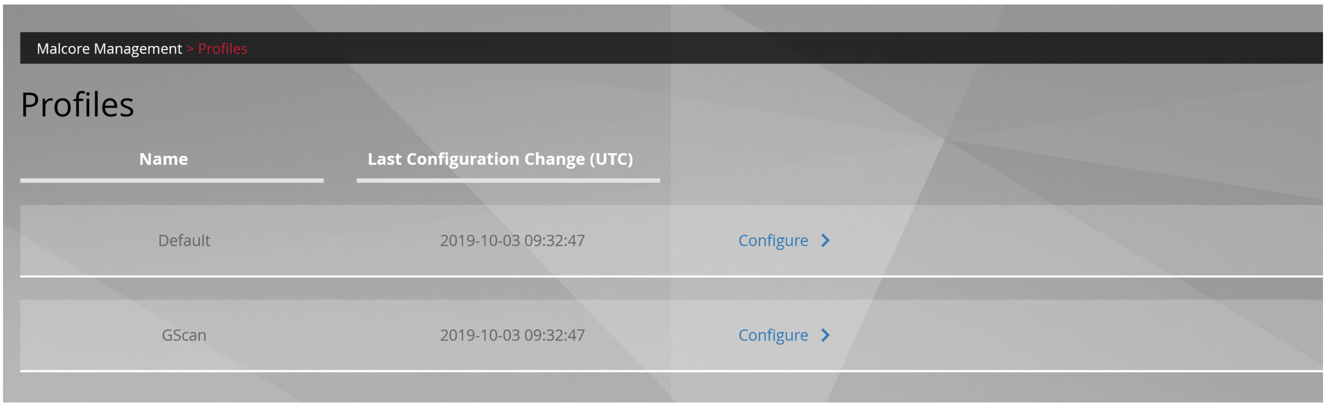
For example, if **Number of days between rescans** is set to 3 and **Number of rescans** is set to 3, the suspicious file will be rescanned on D+3, D+6, and D+9.

Enable automatic GBOX analysis: allows the administrator to activate the automatic sending of all infected or suspicious files to the **GBOX** device if the link is operational.

13.2 Profiles

Rôle Administrateur

Menu: Administrators > GCenter > Malcore Management > Profiles



Malcore Management > Profiles

Profiles

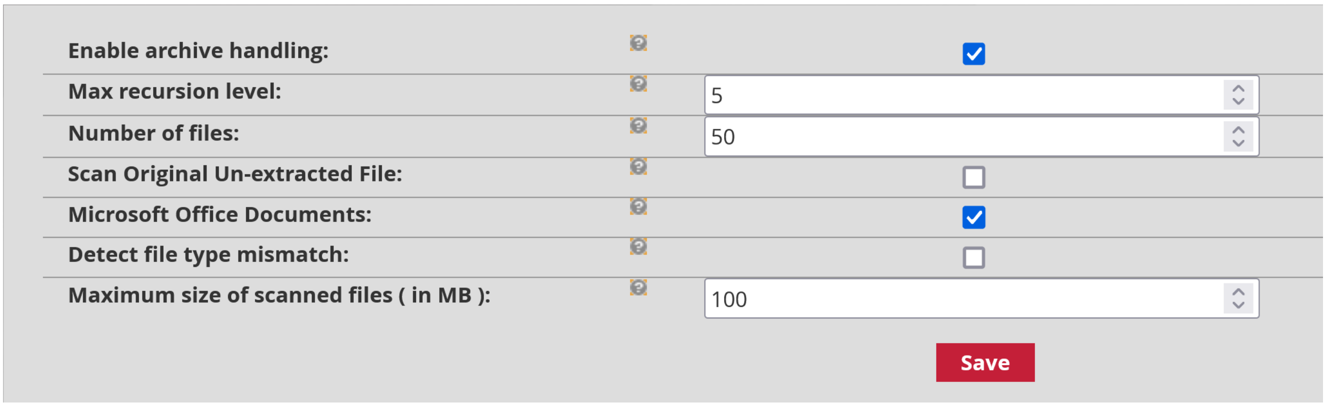
Name	Last Configuration Change (UTC)	
Default	2019-10-03 09:32:47	Configure ›
GScan	2019-10-03 09:32:47	Configure ›

All **MALCORE** profiles are displayed in this view.

However, each profile can be modified as needed via the **Configure** button.

The **Default** profile will be used when processing files sent for analysis by gcaps.

The **Gscan** profile will be used for processing files submitted through the gscan interface.



Enable archive handling:	☑
Max recursion level:	5
Number of files:	50
Scan Original Un-extracted File:	☐
Microsoft Office Documents:	☑
Detect file type mismatch:	☐
Maximum size of scanned files (in MB):	100

Enable archive handling: allows the scanning of all archive types by **MALCORE** (.zip, .rar, .upx).

Max recursion level: indicates the maximum depth level at which **MALCORE** will continue to scan files. For example, a *.zip* contains a folder that contains a folder that contains files. In this case, there are three levels of archive depth. If two is specified in the maximum possible recursion level, then all files in higher levels will not be scanned by **MALCORE**. Setting a limit here enables **MALCORE** to avoid overloading, though it will not scan all file levels. The default value is 5.

Number of files: this is the maximum number of files **MALCORE** can scan per archive. If this number is exceeded, then **MALCORE** will suspect something. The default number is 50 files.

Scan Original Un-extracted File: instructs **MALCORE** to consider the archive itself as a file.

Microsoft Office Documents: tells **MALCORE** to treat Office documents as Office documents (.docx, .xlsx) and not as an archive.

Detect file type mismatch: when ticked, if there is a mismatch between the file type and its extension, the file will appear as *Mismatch* in the dashboards in the **GCENTER** WEB interface.

Maximum size of scanned files (in MB): refers to the maximum size of files that are scanned by **MALCORE**.

Each of these items is taken into account after the administrator records the changes by pressing '**Save**'.

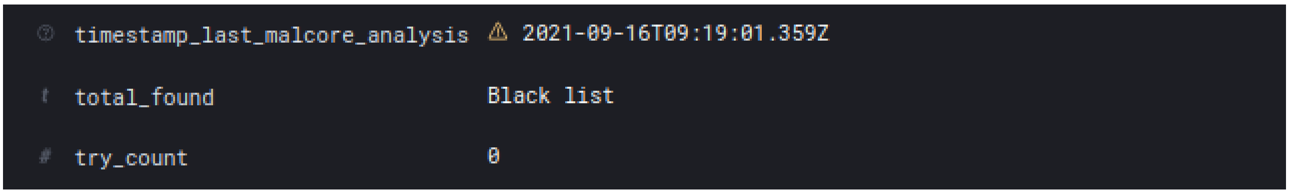
13.3 Exception list

Rôle Administrateur

Menu: Administrators > GCenter > Malcore Management > White list / Black List

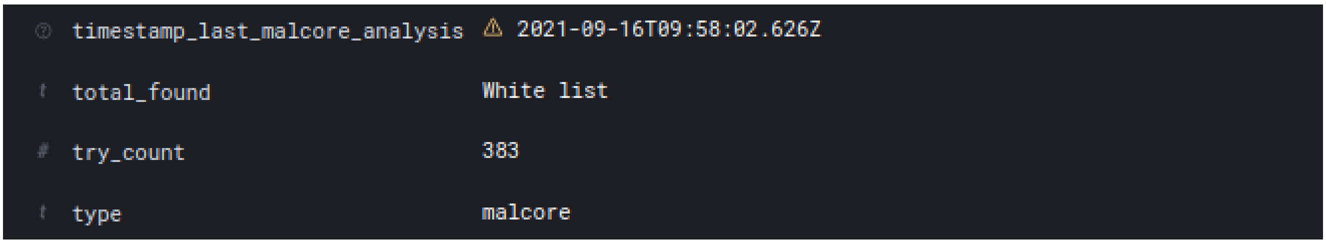
In the **Malcore** settings, it is possible to manage exception lists named Whitelist, for allowed hashes, and Blacklist, for prohibited hashes.

In the event a file to be analysed has a SHA256 hash present in the *Blacklist*, the result of the analysis will appear like this:



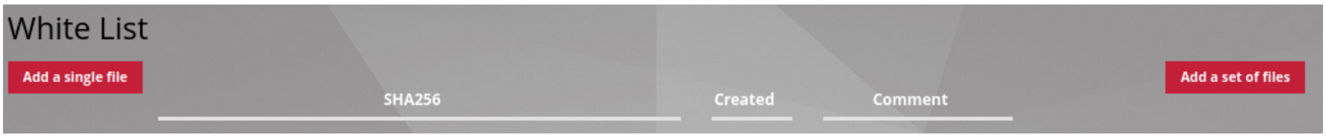
```
timestamp_last_malcore_analysis  ⚠ 2021-09-16T09:19:01.359Z
total_found                      Black list
try_count                        0
```

In the case of a *Whitelist*:



```
timestamp_last_malcore_analysis  ⚠ 2021-09-16T09:58:02.626Z
total_found                      White list
try_count                        383
type                             malcore
```

It is possible to add a hash to these lists either individually via the **GCenter** interface or by batch, by inserting a CSV file.



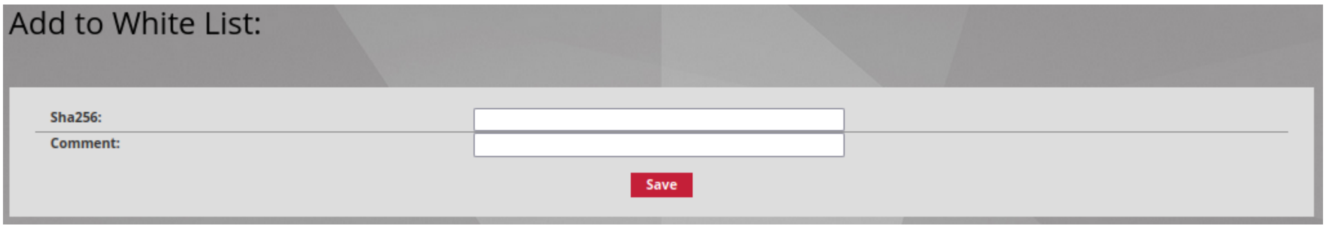
White List

Add a single file

SHA256 Created Comment

Add a set of files

By clicking on **Add a single file**, a single hash can be added by filling in the **Sha256** field and an optional remark for further details in the **Comment** field.



Add to White List:

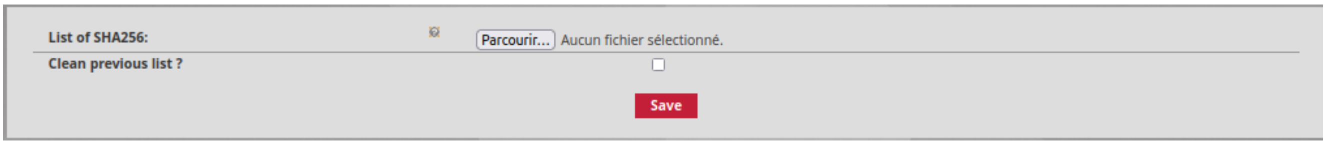
Sha256:

Comment:

Save

All of this information is taken into account after the administrator stores the changes by pressing **Save**.

By clicking on **Add a set of files**, by selecting a file in **csv** on their workstation, the administrator can add a list of hashes by clicking on the button in the **List of SHA256** field. It is necessary to use ';' to separate the various elements of the list.



List of SHA256: Parcourir... Aucun fichier sélectionné.

Clean previous list ? □

The administrator can decide to delete the previous list by ticking the **Clean previous list?** box and record all changes by clicking **Save**.

All additions and changes made from the White List and Black List sections of the MALCORE engine configuration settings will be taken into account in the analysis of the flow as well as for the files scanned via the GScan.

Chapter 14

Detection

14.1 Inspectra

Rôle Opérateur

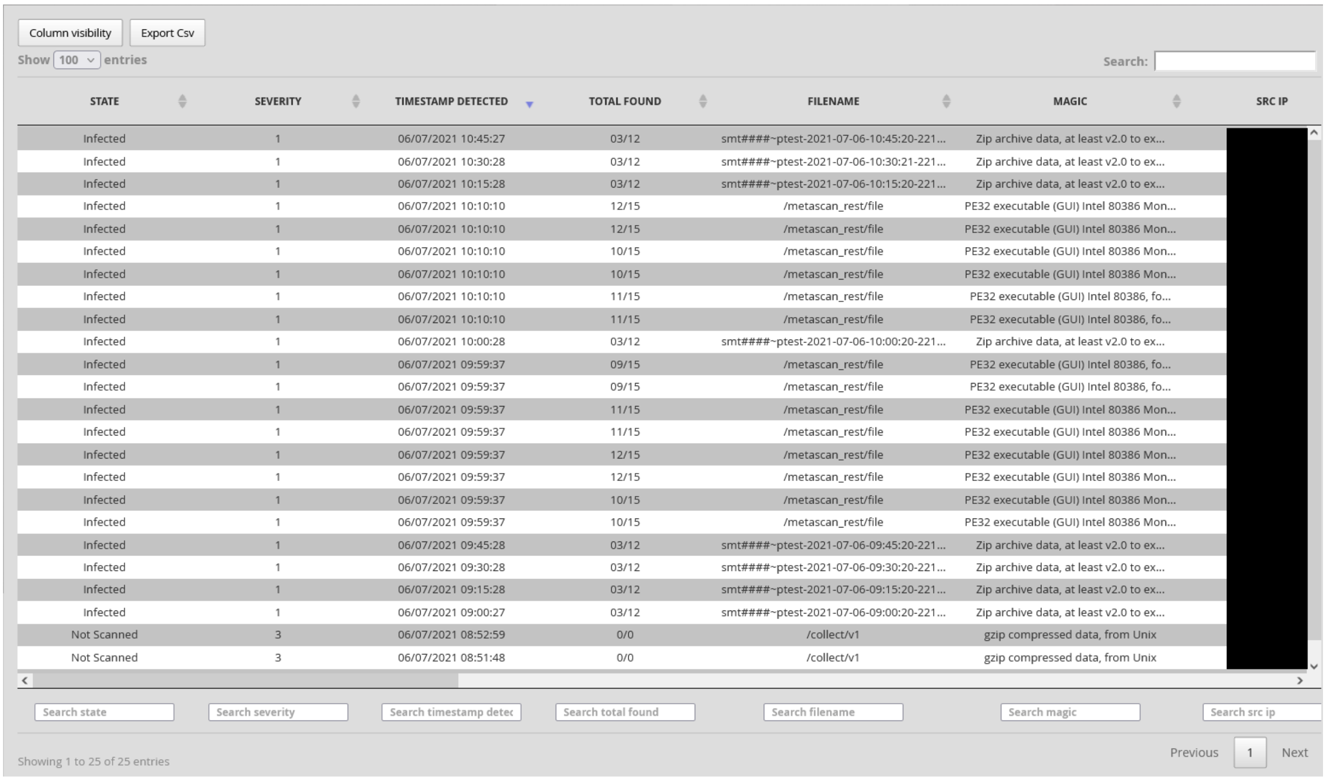
Menu: Operators > Inspectra > Malcore

From the '**OPERATORS - Inspectra - Malcore**' section, the operator accesses a table listing the files seen as suspicious or infected through the **MALCORE** detection engine.

The ***RETROACT*** module will be tasked with highlighting suspicious files, if the feature is enabled.

The suspicious status is generated by the heuristic engines. These engines are able to detect abnormal elements. In the case of suspicious files, they will be reanalysed by **RETROACT**.

Suspicious files are detected by means of various antivirus engines, 1 in the CIE version and 16 in the other versions, operating in parallel. These engines were selected for their complementarity, the relevance of their common detection, their detection technology, and the origin of the security information used.



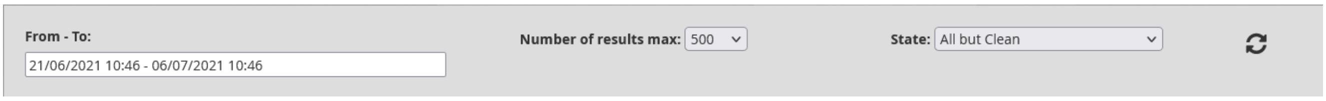
Show 100 entries

Search:

STATE	SEVERITY	TIMESTAMP DETECTED	TOTAL FOUND	FILENAME	MAGIC	SRC IP
Infected	1	06/07/2021 10:45:27	03/12	smt####~ptest-2021-07-06-10:45:20-221...	Zip archive data, at least v2.0 to ex...	[redacted]
Infected	1	06/07/2021 10:30:28	03/12	smt####~ptest-2021-07-06-10:30:21-221...	Zip archive data, at least v2.0 to ex...	[redacted]
Infected	1	06/07/2021 10:15:28	03/12	smt####~ptest-2021-07-06-10:15:20-221...	Zip archive data, at least v2.0 to ex...	[redacted]
Infected	1	06/07/2021 10:10:10	12/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386 Mon...	[redacted]
Infected	1	06/07/2021 10:10:10	12/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386 Mon...	[redacted]
Infected	1	06/07/2021 10:10:10	10/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386 Mon...	[redacted]
Infected	1	06/07/2021 10:10:10	10/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386 Mon...	[redacted]
Infected	1	06/07/2021 10:10:10	11/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386, fo...	[redacted]
Infected	1	06/07/2021 10:10:10	11/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386, fo...	[redacted]
Infected	1	06/07/2021 10:00:28	03/12	smt####~ptest-2021-07-06-10:00:20-221...	Zip archive data, at least v2.0 to ex...	[redacted]
Infected	1	06/07/2021 09:59:37	09/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386, fo...	[redacted]
Infected	1	06/07/2021 09:59:37	09/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386, fo...	[redacted]
Infected	1	06/07/2021 09:59:37	11/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386 Mon...	[redacted]
Infected	1	06/07/2021 09:59:37	11/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386 Mon...	[redacted]
Infected	1	06/07/2021 09:59:37	12/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386 Mon...	[redacted]
Infected	1	06/07/2021 09:59:37	12/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386 Mon...	[redacted]
Infected	1	06/07/2021 09:59:37	10/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386 Mon...	[redacted]
Infected	1	06/07/2021 09:59:37	10/15	/metascan_rest/file	PE32 executable (GUI) Intel 80386 Mon...	[redacted]
Infected	1	06/07/2021 09:45:28	03/12	smt####~ptest-2021-07-06-09:45:20-221...	Zip archive data, at least v2.0 to ex...	[redacted]
Infected	1	06/07/2021 09:30:28	03/12	smt####~ptest-2021-07-06-09:30:20-221...	Zip archive data, at least v2.0 to ex...	[redacted]
Infected	1	06/07/2021 09:15:28	03/12	smt####~ptest-2021-07-06-09:15:20-221...	Zip archive data, at least v2.0 to ex...	[redacted]
Infected	1	06/07/2021 09:00:27	03/12	smt####~ptest-2021-07-06-09:00:20-221...	Zip archive data, at least v2.0 to ex...	[redacted]
Not Scanned	3	06/07/2021 08:52:59	0/0	/collect/v1	gzip compressed data, from Unix	[redacted]
Not Scanned	3	06/07/2021 08:51:48	0/0	/collect/v1	gzip compressed data, from Unix	[redacted]

Showing 1 to 25 of 25 entries

In the window above this table, the operator can click on the ' **From - To**' field to define the time range (in the format *dd/mm/yyyy HH:MM*) of the data being displayed.


From - To: 21/06/2021 10:46 - 06/07/2021 10:46

Number of results max: 500

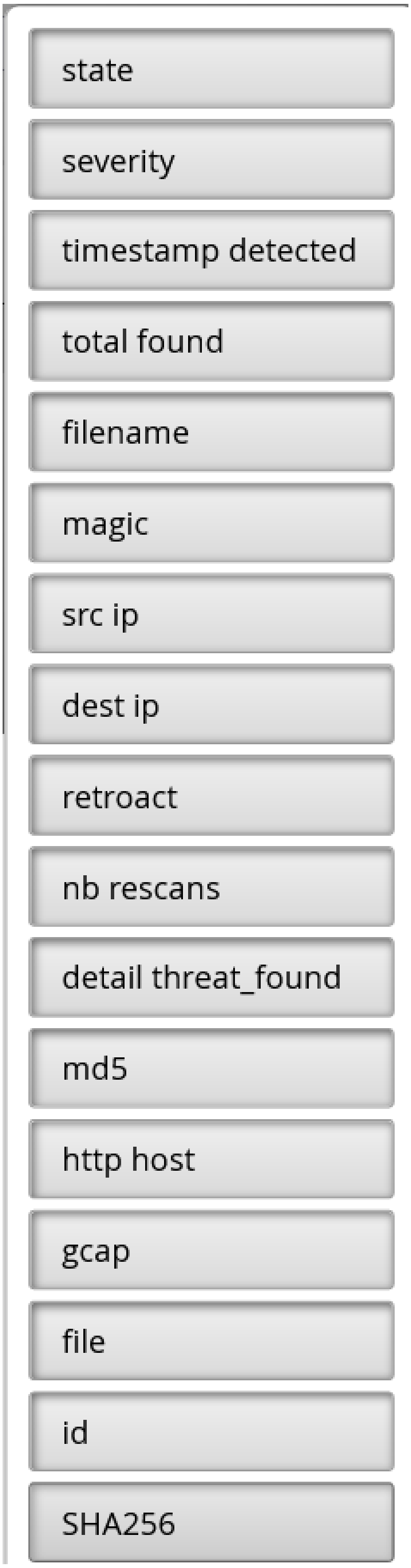
State: All but Clean

'**Number of results max:** is the maximum number of files (lines) displayed in the table.

The '**State**' enables selecting the status of the alerts displayed according to the desired search.

The table's columns are movable and dynamic searches can be made on each of them:

The operator can choose the visibility of the columns in the table by clicking on the **Column visibility** button:


state
severity
timestamp detected
total found
filename
magic
src ip
dest ip
retroact
nb rescans
detail threat_found
md5
http host
gcap
file
id
SHA256

In addition, a vertical view of the alert is displayed via a *right-click* of the mouse.

A quick CSV export of the data based on the selected decision date:

An interactive analysis of the element is possible by means of a *right click* of the mouse. With '**Download malware**' it is possible to retrieve the malware and save it on the computer in a password-protected file in `.zip' format. This password can be changed *here*.

The **TRACKWATCH** is able to provide further analysis of the detected malware through the **Remote analysis**' feature. If the *configuration* is completed beforehand, the operator can decide that the sample should be analysed in the https://intelligence.gatewatcher.com/ platform, i.e. a [**GBOX**] server (itg-ext/intelligence.html#gbox).

The analysis report generated by sending the infected file for further analysis can be downloaded using '**Download analysis report**'.

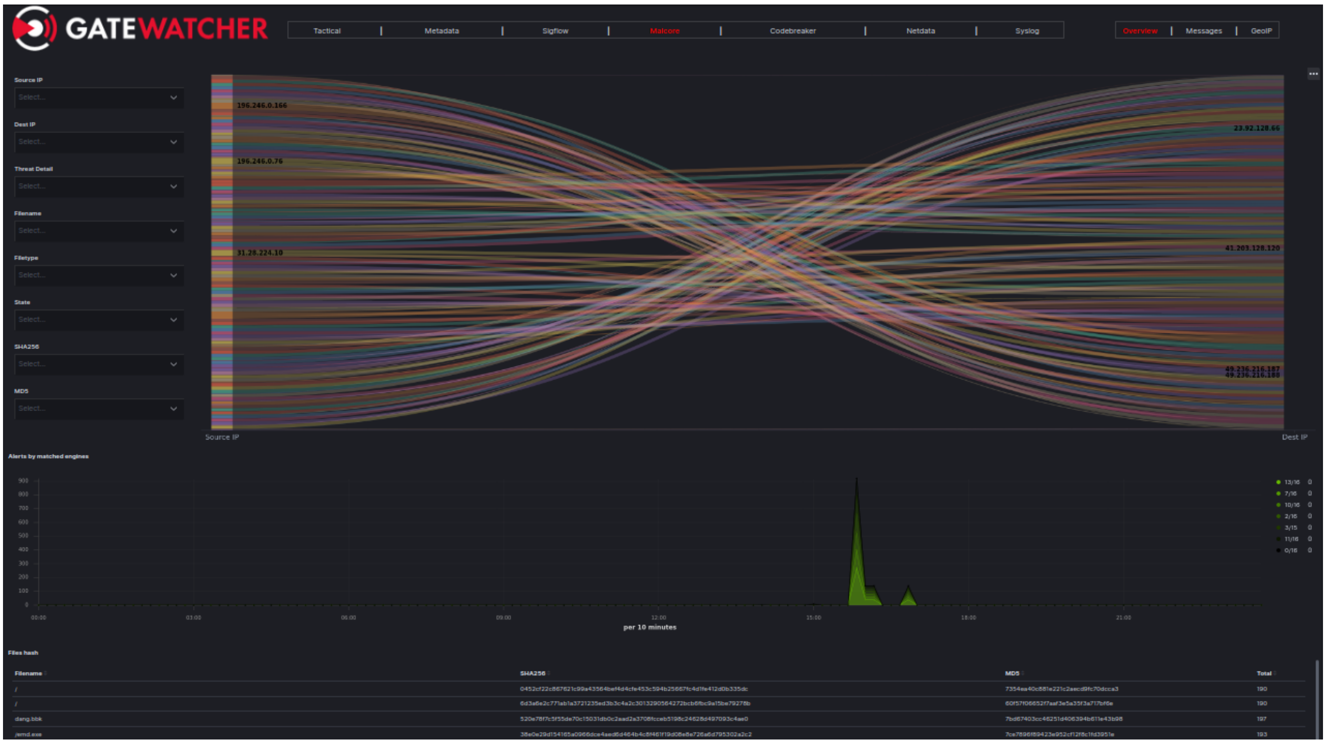
The analysis parameters of the **MALCORE** engine can be changed in the *default profile* settings.

14.2 Dashboards

Menu: Operators > Dashboards > Malcore

In addition to the information already included in the **Inspectra** table, the data collected by Malcore is also provided on the **Malcore** Kibana *dashboard*.

The data will be formatted as follows



Files hash

Filename	SHA256	MD5	Total
/	0452cf22c867621c99a43564bef4d4cfe453c594b25667fc4d1fe412d0b335dc	7354ea40c881e221c2aecd9fc70dcca3	190
/	6d3a6e2c771ab1a3721235ed3b3c4a2c3013290564272bcb6fbc9a15be79278b	60f57f06652f7aaf3e5a35f3a717bf6e	190
dang.bbk	520e78f7c5f55de70c15031db0c2aad2a3708fcceb5198c24628d497093c4ae0	7bd67403cc46251d406394b611e43b98	197
/cmd.exe	38e0e29d154165a0966dce4aed6d464b4c8f461f19d08e8e726a6d795302a2c2	7ce7896f89423e952cf12f8c1fd3951e	193

Chapter 15

Generated events

Attention:

Engine ids are subject to change over time.

15.1 Example of a log

```
json
{
    "engine_id": {
      "714eca0a6475fe7d2bf9a24bcae343f657b230ff68acd544b019574f1392de77": "Trojan.Win32.
↪Vebzenpak.iwgiuz",
      "312a189607571ec2c7544636be405f10889e73d061e0ed77ca0eca97a470838d": "Gen:Variant.
↪Graftor.961641",
      "054a20c51cbe9d2cc7d6a237d6cd4e08ab1a67e170b371e632995766d3ba81af": "Trojan/Win.Generic
↪",
      "0ff95ddb1117d8f36124f6eac406dbbf9f17e3dd89f9bb1bd600f6ad834c25db": "Trojan.Multi",
      "ecc47e2309be9838d6dc2c5157be1a840950e943f5aaca6637afca11516c3eaf": "W32/VBKrypt.AVU.
↪gen!Eldorado",
      "fe665976a02d03734c321007328109ab66823b260a8eea117d2ab49ee9dfd3f1": "Trojan.Win32.
↪Injector",
      "b14014e40c0e672e050ad9c210a68a5303ce7facabae9eb2ee07ddf97dc0da0e": "Trojan.Wacatac",
      "527db072abcf877d4bdcd0e9e4ce12c5d769621aa65dd2f7697a3d67de6cc737": "Trojan.Vebzenpak.
↪Win32.4817",
      "32f2f45e6d9faf46e6954356a710208d412fac5181f6c641e34cb9956a133684": "a variant of Win32/
↪Injector.EPML trojan",
      "038e407ba285f0e01dd30c6e4f77ec19bad5ed3dc866a2904ae6bf46baa14b74": "Trojan.Agent (A)",
      "4ca73ae4b92fd7ddcda418e6b70ced0481ac2d878c48e61b686d0c9573c331dc": "Trojan ( 0057dc101␣
↪)",
      "3bfeb615a695c5ebaac5ade948ffae0c3cfec3787d4625e3abb27fa3c2867f53": "Trojan.Win32.
↪Vebzenpak.afnw",
      "af6868a2b87b3388a816e09d2b282629ccf883b763b3691368a27fbd6f6cd51a": "TR/Injector.vdnis",
      "ad05e0dc742bcd6251af91bd07ef470c699d5aebbb2055520b07021b14d7380c": "TR/Injector.vdnis"
    },
    "@version": "1",
    "detail_scan_time": 289
    "timestamp_detected": "2021-07-05T18:14:45.354Z",
```

(continues on next page)

(continued from previous page)

```
    "SHA256": "9f07b7d90dc159c18619741bbbe05a2eb512a53865ba5101ba9f5668ec01c427",
    "timestamp_last_malcore_analysis": "2021-07-05T18:15:35.546Z",
    "file": "1198",
    "detail_scan_result_i": 1
    "retroact": "None",
    "app_proto": "http",
    "src_port": "80",
    "type": "malcore",
    "detail_wait_time": 88
    "@timestamp": "2021-07-05T18:15:48.857Z",
    "event_type": "malware",
    "filename": "/Im/HBB.exe",
    "total_found": "14/15",
    "scans_history": [
      {
        "code": 1
        "total_found": "14/15",
        "timestamp_analyzed": "2021-07-05T18:15:35.542Z",
        "state": "Infected"
      }
    ],
    "size": "110592",
    "meta": "CLOSED",
    "MD5": "31bbac78b447abc5a1138f5b0f3bb1ae",
    "uuid": "857a9a3f-99e6-4b28-abdd-32a7c28f0295",
    "magic": "PE32 executable (GUI) Intel 80386, for MS Windows",
    "reporting_token": "",
    "severity": 1
    "detail_threat_found": "Infected: Trojan/Win.Generic, TR/Injector.vdnis, Gen:Variant.
↪Graftor.961641, W32/VBKrypt.AVU.gen!Eldorado, a variant of Win32/Injector.EPML trojan,␣
↪Trojan.Agent (A), Trojan.Win32.Injector, Trojan ( 0057dc101 ), Trojan.Win32.Vebzenpak.afnw,␣
↪Trojan.Win32.Vebzenpak.iwgiuz, Trojan.Multi, Trojan.Wacatac, Trojan.Vebzenpak.Win32.4817",
    "detail_def_time": "2021-06-23T00:43:00.000Z",
    "nb_rescans": "Not reanalyzed",
    "dest_ip": "10.7.0.15",
    "replica": false,
    "timestamp_analyzed": "2021-07-05T18:15:48.857Z",
    "code": 1
    "src_ip": "192.185.92.26",
    "gcap": "gcap-int-ppo-164.domain.local",
    "host": "gcap-int-ppo-164.domain.local",
    "state": "Infected",
    "GCenter": "gcenter-int-ppo-237.domain.local",
    "dest_port": "54325",
    "_internal_doc_id": "qPzhd3oBnng1PLWX9yKE",
    "flow_id": 1191592708119283
    "try_count": 0
  }
```

15.2 Summary table of the fields

The syslog export has additional fields:

- smtp.mail_from,
- smtp.rcpt_to,
- email.from, email.to,
- email.cc,
- email.bcc,
- email.in_reply_to,
- http.hostname,
- http.url,
- http.http_refer,
- http.http_user_agent.

Warning:

These fields are affected by a known bug (see release note.)

Warning:

The enrichment at the origin of these fields will be depreciated in v2.5.3.102.

Chapter 16

Detection by gscan

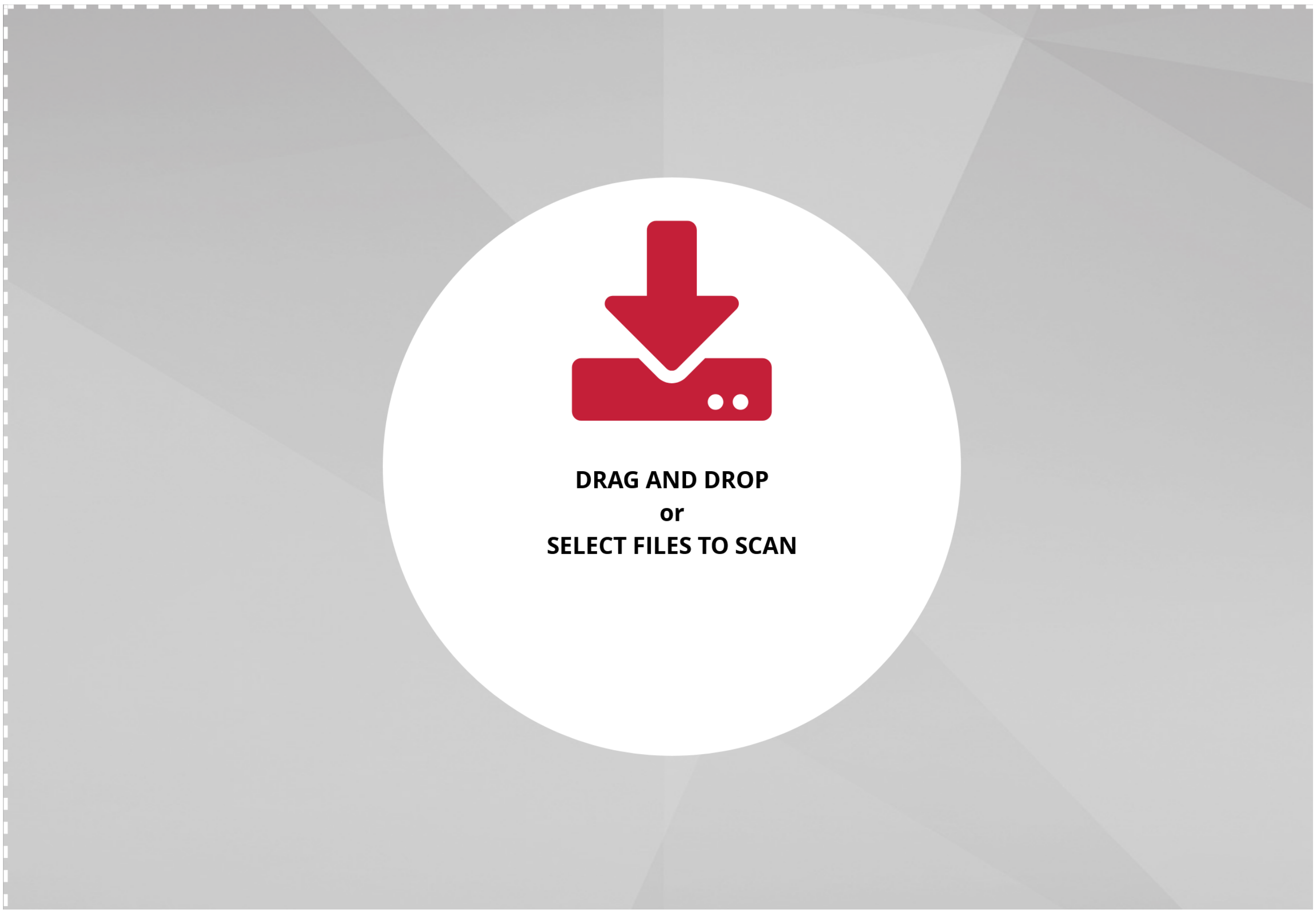
Rôle Opérateur Mode LPM non disponible

Menu: Operators > GScan > Malware Scanning

Note:

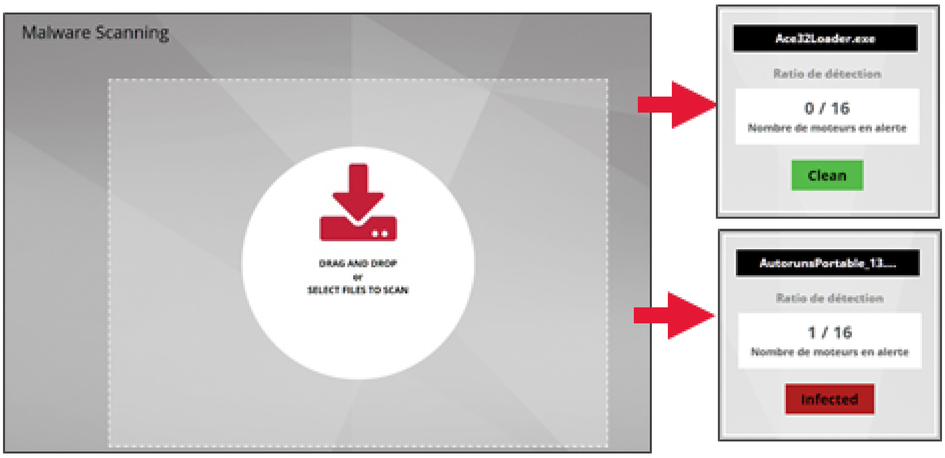
When deployed in an MPL environment, GScan functionality is disabled

Gscan enables an operator to submit a file via the GCenter web interface for malcore analysis



To start analysing a file, simply drag it into the **DRAG and DROP or SELECT FILES TO SCAN** area or click on this area to send your suspicious executables.

Please note that the maximum file size must not exceed 10MB. There is no limit to the number of file scans. The scan result shows almost instantly the status of the sample after analysis. The result can be as follows: Clean or Infected across the 16 engines.



Chapter 17

Presentation

The CODEBREAKER analysis engine enables:

- The detection of exploitative techniques that are offensive, discrete, and sophisticated.
- De-encoding of encrypted payloads.
- Detection of polymorphic shellcodes.

Codebreaker addresses shellcodes for Windows and Linux platforms in 32 and 64 bits.

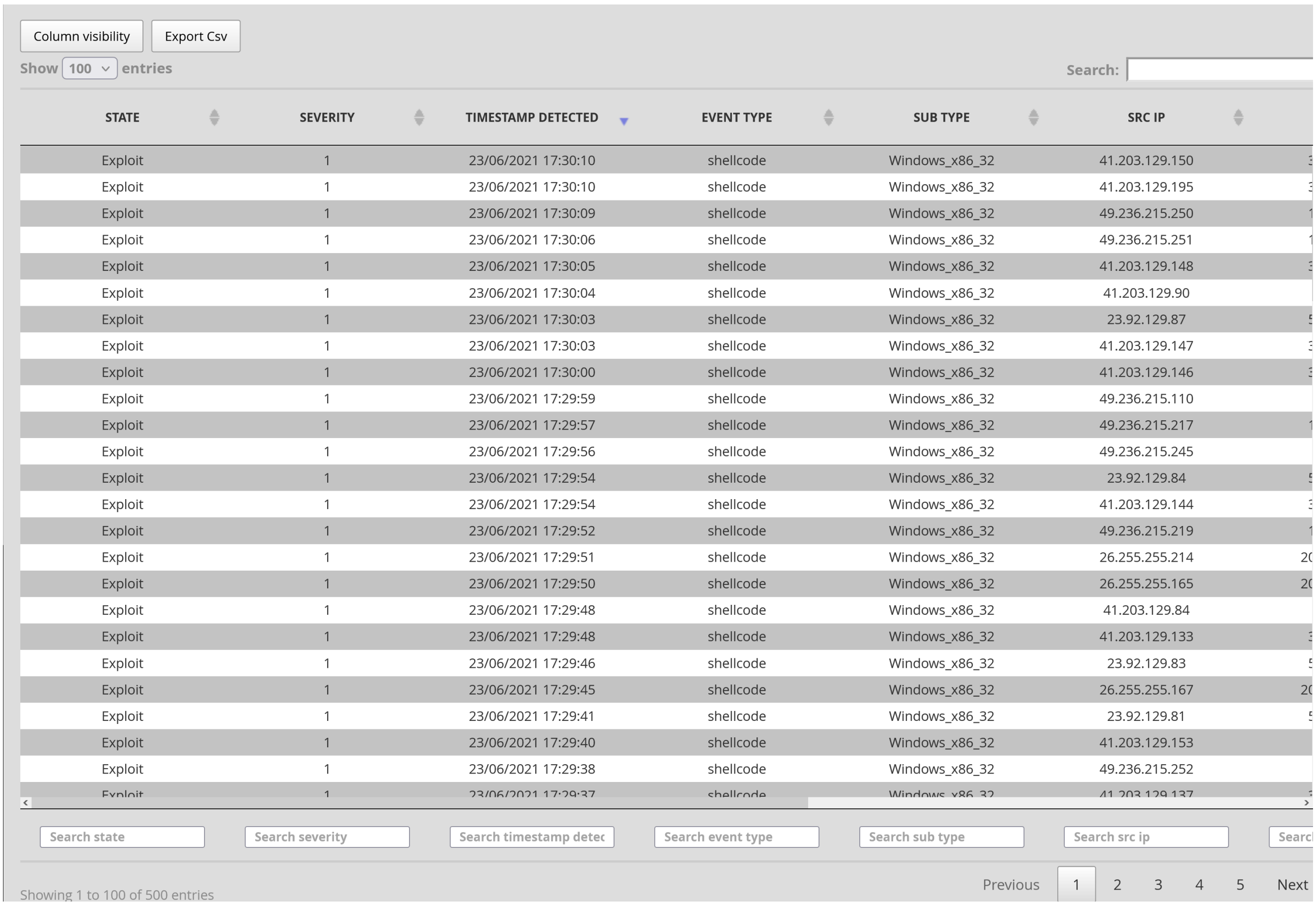
Chapter 18

Detection

Rôle Opérateur

Menu: OPERATORS > Inspectra > Codebreaker

From the '**OPERATORS - Inspectra - Codebreaker**' section, the operator can access a table listing encoded and unencoded shellcodes, polymorphs, and powershells through the **CODEBREAKER** detection engine.



STATE	SEVERITY	TIMESTAMP DETECTED	EVENT TYPE	SUB TYPE	SRC IP
Exploit	1	23/06/2021 17:30:10	shellcode	Windows_x86_32	41.203.129.150
Exploit	1	23/06/2021 17:30:10	shellcode	Windows_x86_32	41.203.129.195
Exploit	1	23/06/2021 17:30:09	shellcode	Windows_x86_32	49.236.215.250
Exploit	1	23/06/2021 17:30:06	shellcode	Windows_x86_32	49.236.215.251
Exploit	1	23/06/2021 17:30:05	shellcode	Windows_x86_32	41.203.129.148
Exploit	1	23/06/2021 17:30:04	shellcode	Windows_x86_32	41.203.129.90
Exploit	1	23/06/2021 17:30:03	shellcode	Windows_x86_32	23.92.129.87
Exploit	1	23/06/2021 17:30:03	shellcode	Windows_x86_32	41.203.129.147
Exploit	1	23/06/2021 17:30:00	shellcode	Windows_x86_32	41.203.129.146
Exploit	1	23/06/2021 17:29:59	shellcode	Windows_x86_32	49.236.215.110
Exploit	1	23/06/2021 17:29:57	shellcode	Windows_x86_32	49.236.215.217
Exploit	1	23/06/2021 17:29:56	shellcode	Windows_x86_32	49.236.215.245
Exploit	1	23/06/2021 17:29:54	shellcode	Windows_x86_32	23.92.129.84
Exploit	1	23/06/2021 17:29:54	shellcode	Windows_x86_32	41.203.129.144
Exploit	1	23/06/2021 17:29:52	shellcode	Windows_x86_32	49.236.215.219
Exploit	1	23/06/2021 17:29:51	shellcode	Windows_x86_32	26.255.255.214
Exploit	1	23/06/2021 17:29:50	shellcode	Windows_x86_32	26.255.255.165
Exploit	1	23/06/2021 17:29:48	shellcode	Windows_x86_32	41.203.129.84
Exploit	1	23/06/2021 17:29:48	shellcode	Windows_x86_32	41.203.129.133
Exploit	1	23/06/2021 17:29:46	shellcode	Windows_x86_32	23.92.129.83
Exploit	1	23/06/2021 17:29:45	shellcode	Windows_x86_32	26.255.255.167
Exploit	1	23/06/2021 17:29:41	shellcode	Windows_x86_32	23.92.129.81
Exploit	1	23/06/2021 17:29:40	shellcode	Windows_x86_32	41.203.129.153
Exploit	1	23/06/2021 17:29:38	shellcode	Windows_x86_32	49.236.215.252
Exploit	1	23/06/2021 17:29:37	shellcode	Windows_x86_32	41.203.129.137

Above this table, the operator can click on the ' **From - To**' field to define the time range (in the format *dd/mm/yyyy HH:MM*) of the data being displayed.

Number of results max: is the maximum number of results displayed in the table.

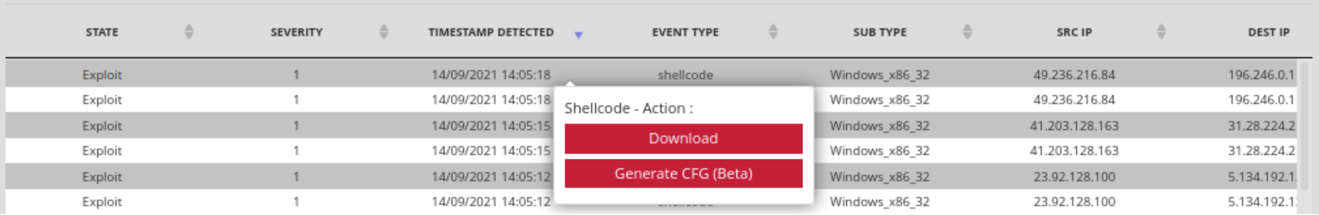
The table's columns are movable and dynamic searches can be made on each of them:

The operator can choose the visibility of the columns in the table by clicking on the *Column visibility* button.

It is also an option to perform a quick CSV export of the data based on the selected decision date:

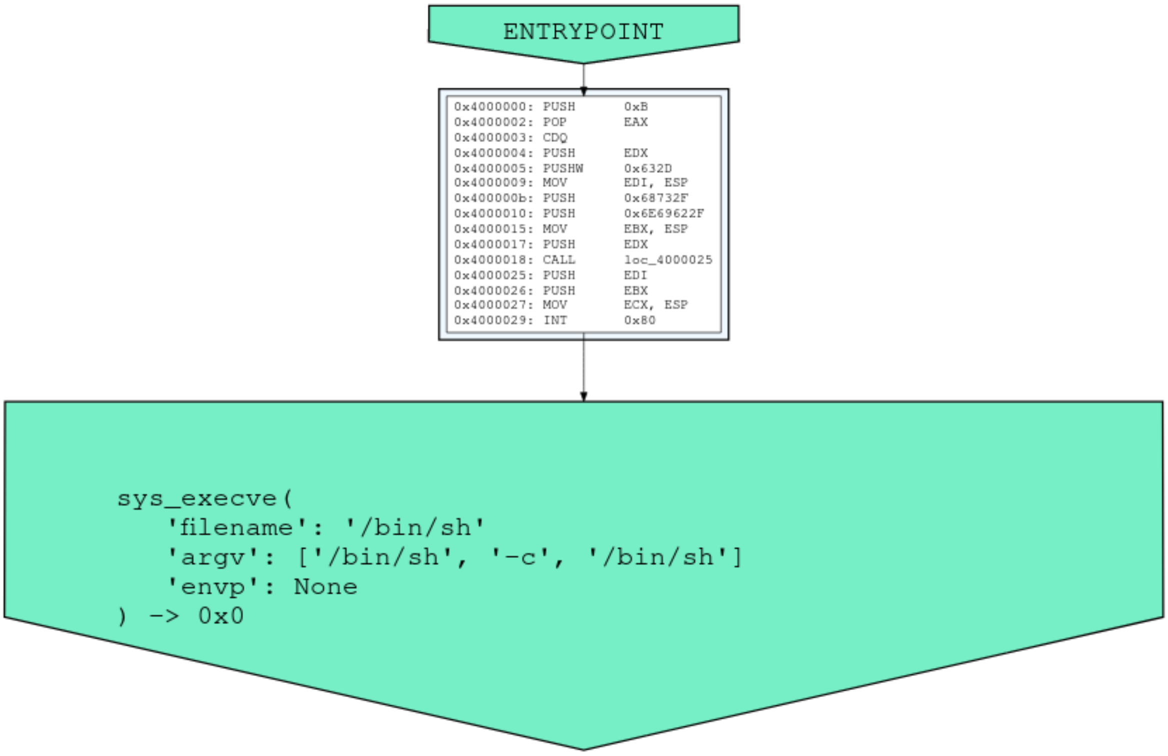
An interactive analysis of the element is possible by means of a ***right click*** of the mouse. With '**Download**' it is possible to retrieve the Shellcode/PowerShell and save it on the computer in a password protected file in `.zip' format. This password can be changed *here*.

The operator can also run the '**Generate CFG**' function to obtain a simplified, graphical version of the detected Shellcode instructions.



STATE	SEVERITY	TIMESTAMP DETECTED	EVENT TYPE	SUB TYPE	SRC IP	DEST IP
Exploit	1	14/09/2021 14:05:18	shellcode	Windows_x86_32	49.236.216.84	196.246.0.1
Exploit	1	14/09/2021 14:05:18		Windows_x86_32	49.236.216.84	196.246.0.1
Exploit	1	14/09/2021 14:05:15		Windows_x86_32	41.203.128.163	31.28.224.2
Exploit	1	14/09/2021 14:05:15		Windows_x86_32	41.203.128.163	31.28.224.2
Exploit	1	14/09/2021 14:05:12		Windows_x86_32	23.92.128.100	5.134.192.1
Exploit	1	14/09/2021 14:05:12		Windows_x86_32	23.92.128.100	5.134.192.1

Below is an example of a CFG generation of a simple shellcode detected by the **CODEBREAKER** analysis engine:



```
0x4000000: PUSH      0xB
0x4000002: POP       EAX
0x4000003: CDQ
0x4000004: PUSH      EDX
0x4000005: PUSHW     0x632D
0x4000009: MOV       EDI, ESP
0x400000b: PUSH      0x68732F
0x4000010: PUSH      0x6E69622F
0x4000015: MOV       EBX, ESP
0x4000017: PUSH      EDX
0x4000018: CALL      loc_4000025
0x4000025: PUSH      EDI
0x4000026: PUSH      EBX
0x4000027: MOV       ECX, ESP
0x4000029: INT       0x80
```

```
sys_execve(
    'filename': '/bin/sh'
    'argv': ['/bin/sh', '-c', '/bin/sh']
    'envp': None
) -> 0x0
```

Finally, as with the rest of the information analysed by the TRACKWATCH solution, the data generated by Codebreaker is available in the dedicated Kibana *dashboard*.

Chapter 19

Generated events

19.1 Codebreaker Shellcode

19.1.1 Example of a Codebreaker Shellcode log

```
json
{
    "flow_id": "1288526885940394",
    "@version": "1",
    "timestamp_detected": "2021-07-01T09:30:57.781Z",
    "SHA256": "1199e5d7281671962afaac9e6f36470f4f217b827ddbefa34026f509c025f76b",
    "src_port": "27114",
    "file_id": "07-01-2021T09:30:57_0431273753_gcap-int-ppo-164.domain.local",
    "type": "codebreaker",
    "@timestamp": "2021-07-01T09:31:03.666Z",
    "event_type": "shellcode",
    "calls": {
      "0": {
        "call": "kernel32_LoadLibraryA",
        "args": "{'lpFileName': 'ws2_32'}",
        "ret": 1880096768
      },
      "1": {
        "call": "ws2_32_WSAStartup",
        "args": "{'wVersionRequested': 400}",
        "ret": 0
      },
      "2": {
        "call": "ws2_32_WSASocketA",
        "args": "{'af': 'AF_INET', 'type': 'SOCK_STREAM', 'protocol': 'IPPROTO_IP', 'g': 0,
↪'dwFlags': 0}",
        "ret": 20
      },
      "3": {
        "call": "ws2_32_connect",
        "args": "{'s': 'Socket_1 (20)', 'name': '10.30.58.183:4444', 'namelen': 16}",
        "ret": 0
      },
      "4": {
```

(continues on next page)

(continued from previous page)

```
        "call": "ws2_32_recv",
        "args": "{'s': 'Socket_1-connected (20)', 'buf': '0x1237e5c', 'len': 4, 'flags': None}
↪",
        "ret": 4
      },
      "5": {
        "call": "kernel32_VirtualAlloc",
        "args": "{'lpAddress': 'Null', 'dwSize': '0xff', 'flAllocationType': 'MEM_COMMIT',
↪'flProtect': 'PAGE_EXECUTE_READWRITE'}",
        "ret": 536870912
      },
      "6": {
        "call": "ws2_32_recv",
        "args": "{'s': 'Socket_1-connected (20)', 'buf': '0x20000000', 'len': 255, 'flags':␣
↪None}",
        "ret": 255
      },
      "stop": "End of shellcode"
    },
    "uuid": "1cfaba49-4f4b-4a25-b32a-1eb2ed8a8366",
    "MD5": "aa9d9b771c61b9e2773f7b6b6d541d18",
    "sub_type": "Windows_x86_32",
    "severity": 1,
    "dest_ip": "31.28.224.101",
    "timestamp_analyzed": "2021-07-01T09:31:03.666Z",
    "encodings": [
      {
        "count": 33,
        "name": "Shikata_ga_nai"
      }
    ],
    "src_ip": "41.203.128.216",
    "gcap": "gcap-int-ppo-164.domain.local",
    "state": "Exploit",
    "GCenter": "gcenter-int-ppo-237.domain.local",
    "dest_port": "82"
  }
```

19.1.2 Table summarising the Codebreaker Shellcode fields

19.2 Codebreaker Powershell

19.2.1 Codebreaker Powershell event modifications

19.2.2 Example of Codebreaker Powershell log

```
json
{
    "flow_id": "2248143006711922",
    "@version": "1",
    "timestamp_detected": "2021-07-06T17:39:29.442Z",
```

(continues on next page)

(continued from previous page)

```
    "MD5": "c2eae0da7d9e27a10ae889cef2d21d0d",
    "SHA256": "04fa65e0e344dfff0396ca9fe3e36ce55f1c2777c698874458b97289383e5de5",
    "uuid": "340fb354-0439-495b-acad-104cb8bf2a31",
    "sub_type": "powershell",
    "severity": 1
    "src_port": "55796",
    "dest_ip": "10.127.0.222",
    "type": "codebreaker",
    "file_id": "07-06-2021T17:39:29_7620562351_gcap-int-ppo-164.domain.local",
    "@timestamp": "2021-07-06T17:39:32.888Z",
    "timestamp_analyzed": "2021-07-06T17:39:32.888Z",
    "src_ip": "10.127.0.111",
    "gcap": "gcap-int-ppo-164.domain.local",
    "event_type": "powershell",
    "state": "Exploit",
    "scores": {
      "proba_obfuscated": 1
      "analysis": 134
      "analysis_detailed": {
        "WebClientInvokation": 0
        "StrReplace": 10
        "Base64": 0
        "CharInt": 16
        "StrCat": 12
        "FmtStr": 96
        "StrJoin": 0
      }
    },
    "dest_port": "4242",
    "gcenter": "gcenter-int-ppo-237.domain.local"
  }
```

19.2.3 Table summarising the Codebreaker Powershell fields

Chapter 20

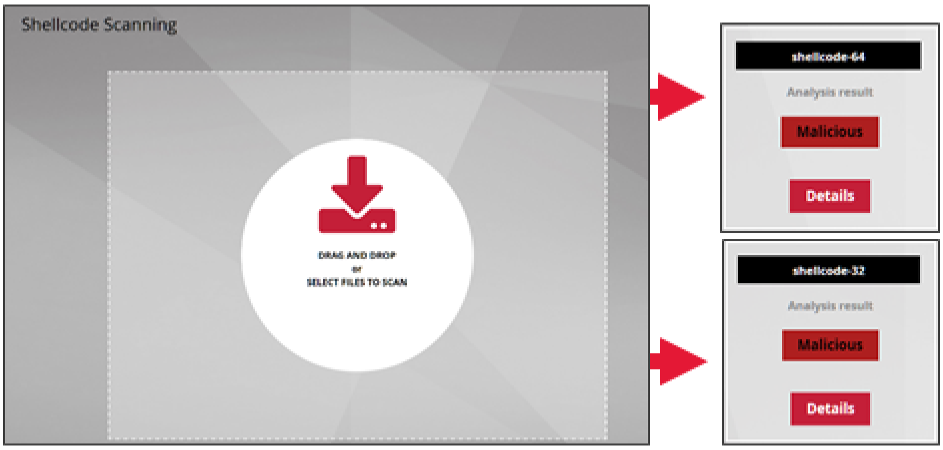
GScan

20.1 Shellcode Scanning

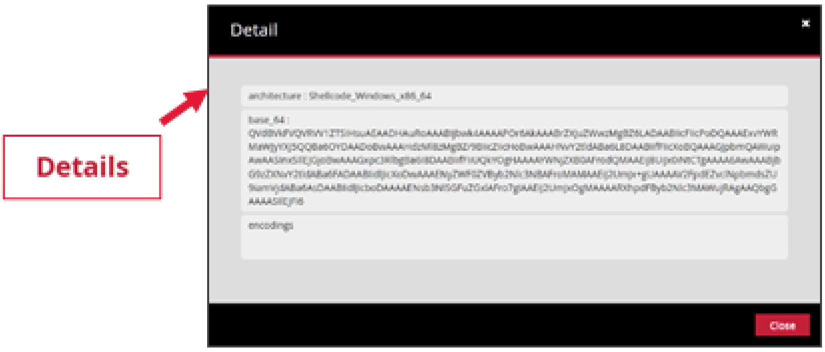
Rôle Opérateur | Mode LPM non disponible

Menu: Operators > GScan > Shellcode Scanning

GScan shellcode enables files to be manually submitted so that they can be analysed by the codebreaker detection engine.



This information is available in the 'Details' section.



architecture : Shellcode_Windows_x86_64

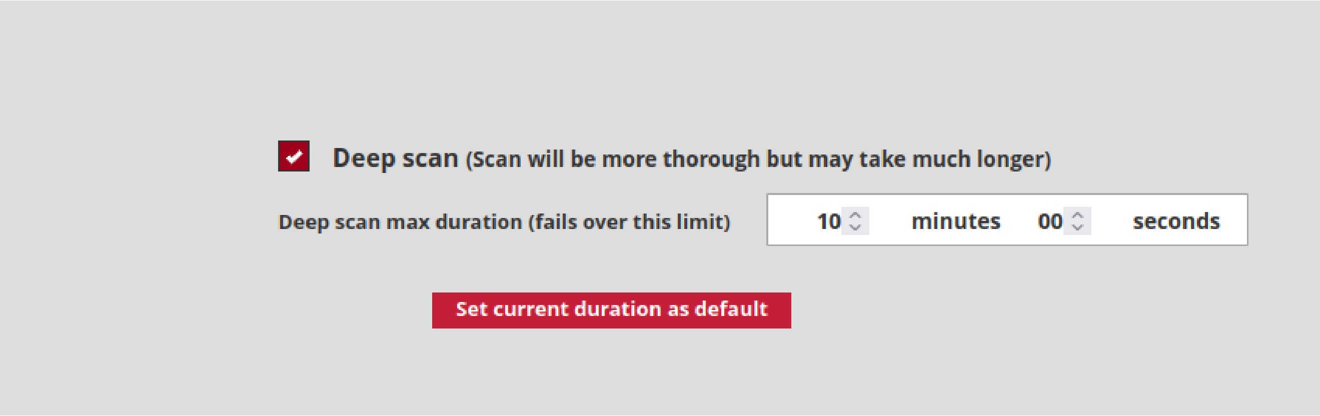
base_64 :

[illegible]

encodings

The **Deep Scan** function enables improved detection of unknown patterns or methods of obfuscation.

It is possible to configure the analysis time and to activate/deactivate the function.



☑ Deep scan (Scan will be more thorough but may take much longer)

Deep scan max duration (fails over this limit) 10 minutes 00 seconds

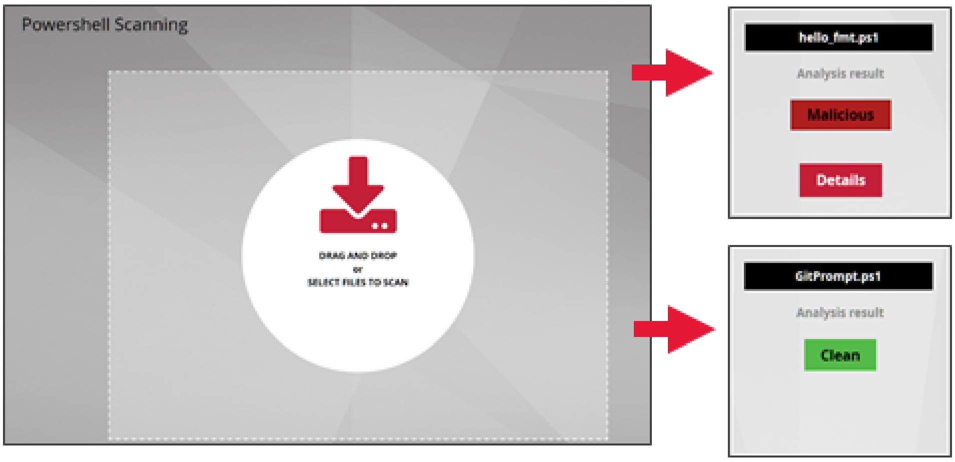
20.2 Powershell Scanning

Rôle Opérateur | Mode LPM non disponible

Menu: Operators > GScan > Powershell Scanning

This interface provides the ability to scan files containing POWERSHELL scripts and detect potential threats that can be used as an entry point to install malware on Windows.

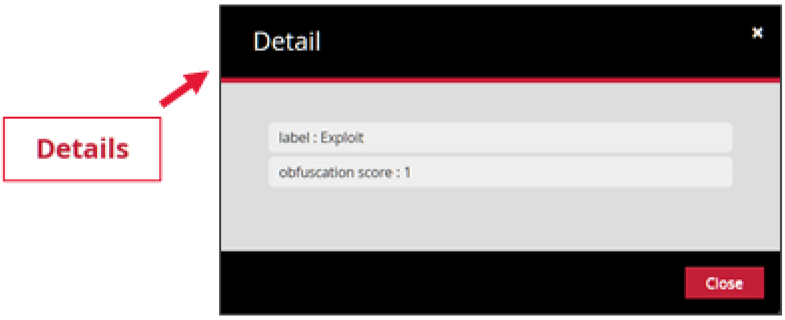
As regards malicious powershells, detection is based on a supervised Machine Learning model, and on the fact that these scripts generally use obfuscation or similar techniques such as base64, concatenation, and type conversion, etc.



hello_fmt.ps1
Analysis result
Malicious

GitPrompt.ps1
Analysis result
Clean

Some additional information is available under the 'Details' tab.



label : Exploit

obfuscation score : 1

The result can be as follows: Clean or Malicious depending on the obfuscation score.

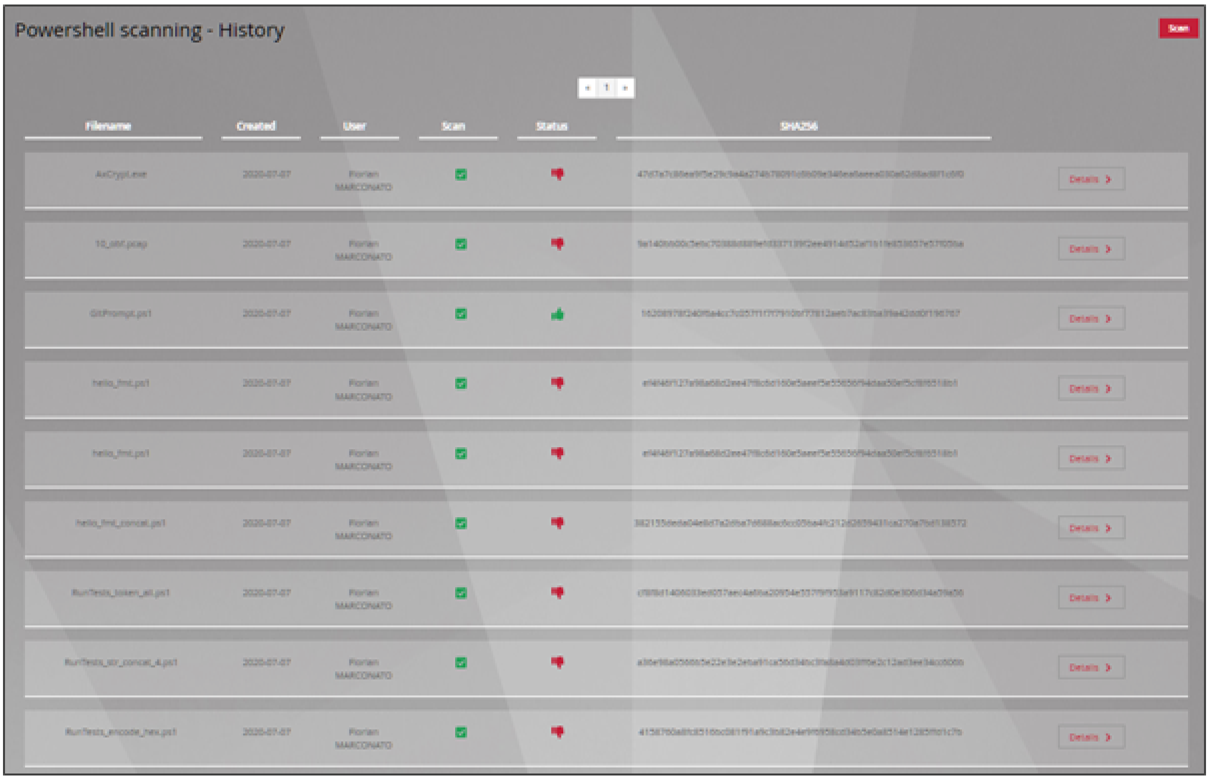
20.3 History

Rôle Opérateur

Menu:

- Operators > GScan > Malware Scanning
- Operators > GScan > Shellcode Scanning
- Operators > GScan > Powershell Scanning

For all MALCORE, CODEBREAKER, and POWERSHELL scans, a history of analysed files per analysis engine is available.

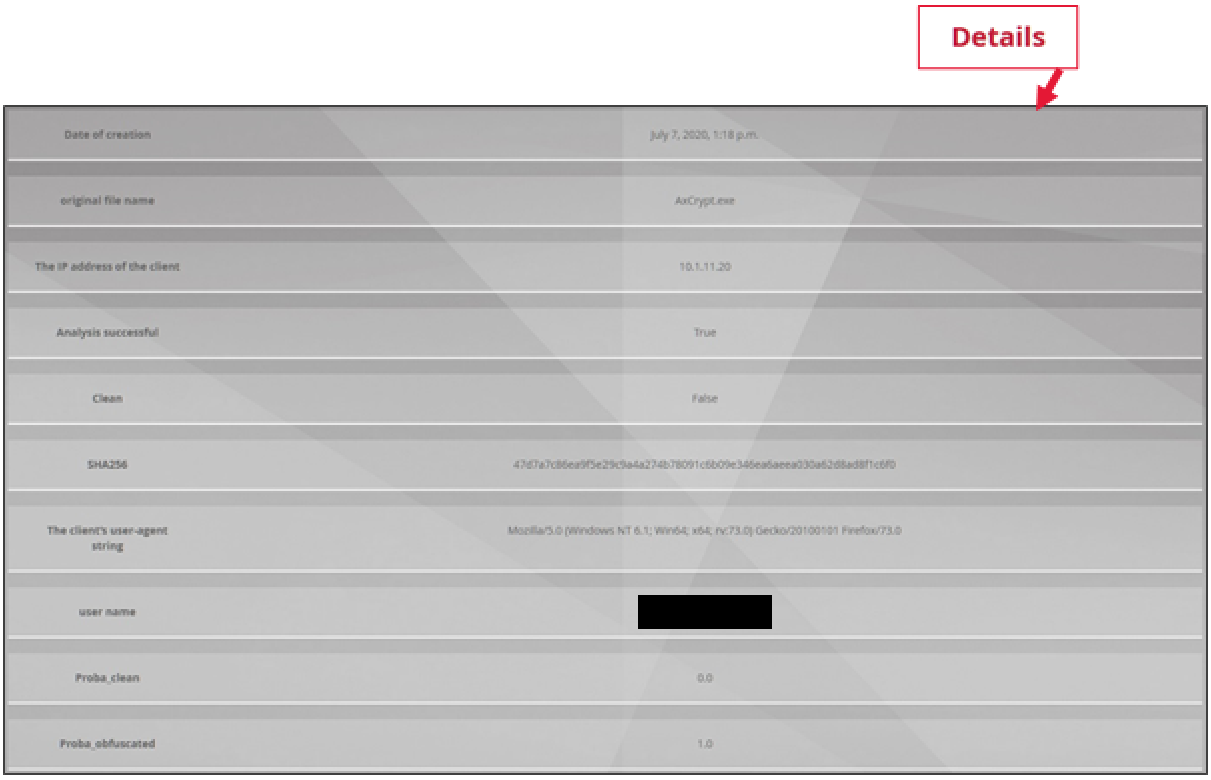


Powershell scanning - History

Filename	Created	User	Scan	Status	SHA256	
AxCrypt.exe	2020-07-07	Florian MARCONATO	☑	👎	[illegible]	Details ›
10_obf.pcap	2020-07-07	Florian MARCONATO	☑	👎	[illegible]	Details ›
GitPrompt.ps1	2020-07-07	Florian MARCONATO	☑	👍	[illegible]	Details ›
hello_fmt.ps1	2020-07-07	Florian MARCONATO	☑	👎	[illegible]	Details ›
hello_fmt.ps1	2020-07-07	Florian MARCONATO	☑	👎	[illegible]	Details ›
hello_fmt_concat.ps1	2020-07-07	Florian MARCONATO	☑	👎	[illegible]	Details ›
RunTests_token_all.ps1	2020-07-07	Florian MARCONATO	☑	👎	[illegible]	Details ›
RunTests_str_concat_4.ps1	2020-07-07	Florian MARCONATO	☑	👎	[illegible]	Details ›
RunTests_encode_hex.ps1	2020-07-07	Florian MARCONATO	☑	👎	[illegible]	Details ›

The list of files that have been analyzes can be seen on the interface.

Further information can be accessed via 'Details'.



Date of creation	July 7, 2020, 1:18 p.m.
original file name	AxCrypt.exe
The IP address of the client	10.1.11.20
Analysis successful	True
Clean	False
SHA256	47d7a7c86ea9f5e29c9a4a274b78091c6b09e346ea6aeea030a62d8ad8f1c6f0
The client's user-agent string	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0
user name	[redacted]
Proba_clean	0.0
Proba_obfuscated	1.0

Chapter 21

Presentation

SIGFLOW analyses all network traffic. It can generate alerts, metadata, and content based on **rules**. Coming from different sources, these rules must describe the characteristics of the attacks to be detected as well as being optimised to reduce false positives. Gatewatcher provides a set of rules that can be downloaded from its update platform. The following paragraphs describe the steps required to provide these rules to the GCAP SIGFLOW module through the GCENTER.

The basic configuration steps are as follows:

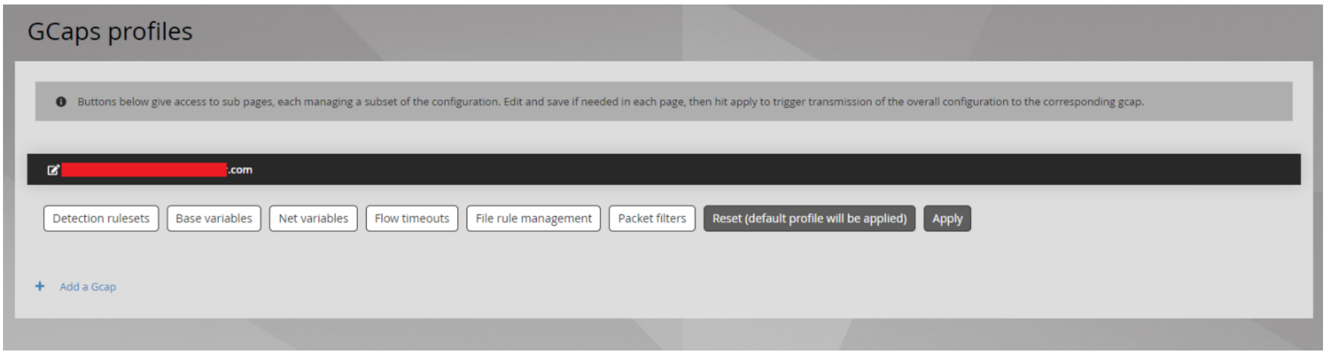
- *Managing the available rule sources*
- *Creating rulesets from sources*
- *Generating rulesets* (important)
- *Applying rulesets on gcap*
- *Advanced configuration of gcap parameters*

Chapter 22

GCAP Profiles

Rôle Opérateur

Menu: Operators > Sigflow > GCap Profiles



GCaps profiles

Buttons below give access to sub pages, each managing a subset of the configuration. Edit and save if needed in each page, then hit apply to trigger transmission of the overall configuration to the corresponding gcap.

[redacted].com

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

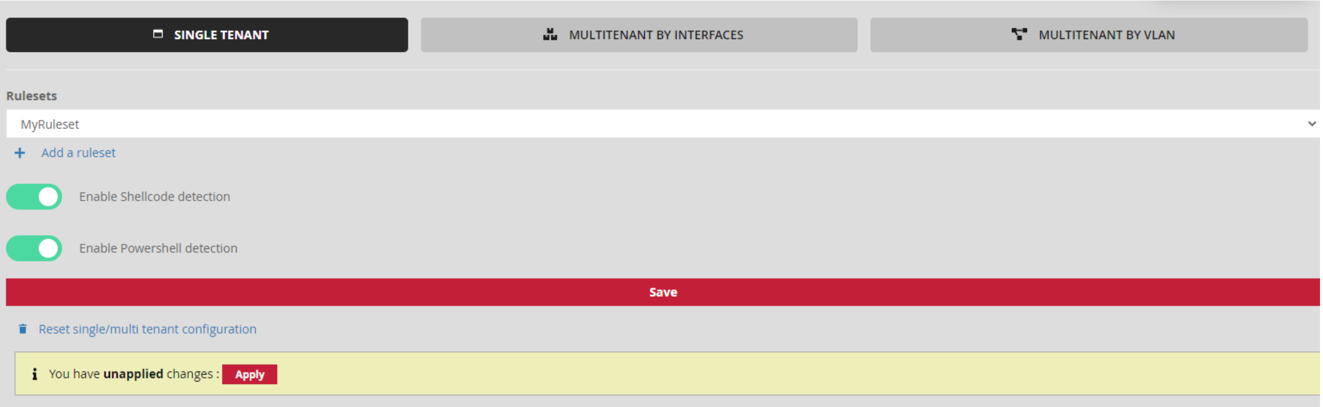
- *Detection Ruleset*
- *Base variables*
- *Net variables*
- *Flow timeouts*
- *Files rules management*
- *BPF filter*

In order to start the detection engine on the GCap probe, the user must first apply a ruleset to it. See section *Sigflow/Rulesets* on creating a ruleset".

22.1 Detection Rulesets

Rôle Opérateur

Menu: Operators > Sigflow > GCAP Profiles



Rulesets

MyRuleset

+ Add a ruleset

Enable Shellcode detection

Enable Powershell detection

Reset single/multi tenant configuration

You have **unapplied** changes :

The **Detection Rulesets** section enables applying previously created SIGFLOW Rulesets to GCAPs paired on the GCENTER. It is also possible to configure the codebreaker module for the GCAP that includes enabling or disabling shellcode and powershell detection separately.

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.

Note:

Codebreaker is not configurable via the **Detection Rulesets** menu with the CIE license.

**The GCAP Detection Rulesets menu enables three configuration options

- **Single tenant:**
  - Assign a ruleset for all GCAP monitoring interfaces;
  - Enable/disable codebreaker for all GCAP monitoring interfaces.
- **The multi-tenant per interface:**
  - Assign a ruleset per GCAP monitoring interface;
  - Enable/disable codebreaker per GCAP monitoring interface.
- **Multi-tenant by vlan:**
  - Assign one ruleset per vlan;
  - Assign a ruleset for the default vlan for those vlans not created via the interface;
  - Enable/disable codebreaker per vlan;
  - Enable/disable codebreaker 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 per vlan configuration at the same time.

22.1.1 Single-tenant

Note:

Changes to this tab require the GCAP configuration to be backed up and implemented via the save and apply button.

Single-tenant configuration:

1. Go to the `Single-tenant` tab;
2. Select a ruleset to apply to all interfaces;
3. Enable or disable shellcode detection for all interfaces;
4. Enable or disable powershell detection for all interfaces;
5. Apply the configuration by clicking the "save" button.

22.1.2 Multi-tenant by interface

The **multi-tenant by interface** enables applying a single-tenant configuration for each of the GCAP interfaces, thus having a different supervision per interface. Indeed, it is possible to apply a different SIGFLOW ruleset, as well as to configure codebreaker for each of the GCAP interfaces.

Note:

It is advisable to optimise the SIGFLOW ruleset in advance before choosing this configuration option. The rules must be adapted to the monitored environment.

Note:

It is necessary to verify whether multiple monitoring interfaces are enabled on the GCAP prior to applying a multi-tenant by interface configuration.

Note:

Changes to this tab require the GCAP configuration to be backed up and implemented via the save and apply button.

Note:

Only activated monitoring interfaces appear in the GCENTER interface.

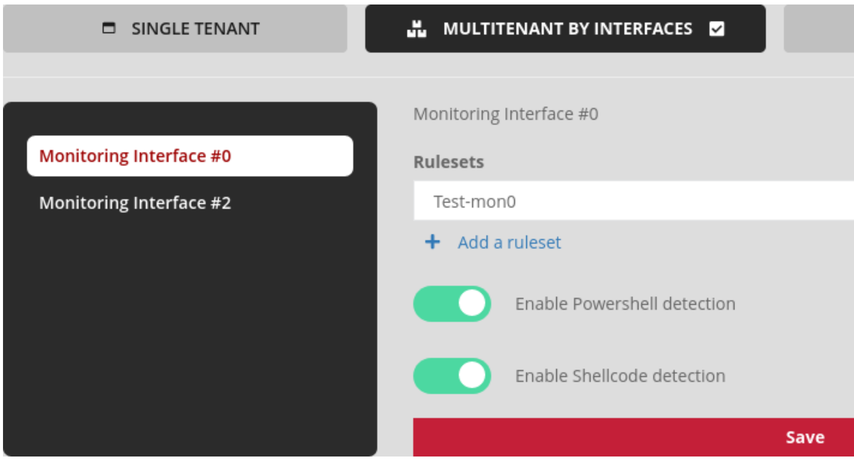
Configuring multi-tenant by interface:

1. Go to the `Multi-tenant by interface` tab;
2. Select a ruleset to apply for each interface;
3. Enable or disable shellcode detection for each interface;
4. Enable or disable powershells detection for each interface;
5. Apply the configuration by clicking the "save" button.

Configuration example:

- **interface mon0:**

  - Ruleset named "Test-mon0",



Monitoring Interface #0

Rulesets

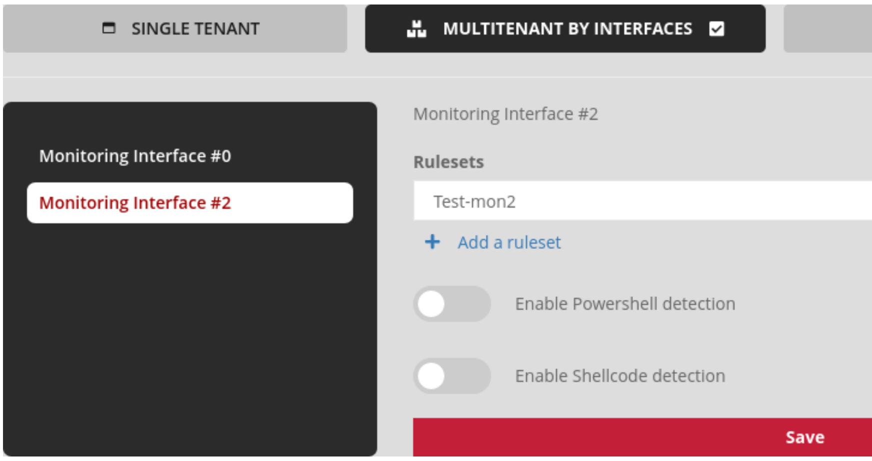
Test-mon0

Enable Powershell detection

Enable Shellcode detection

  - Enabling shellcode/powershell detection.

- **interface mon2:**
  - Ruleset named "Test-mon2",



Monitoring Interface #2

Rulesets

Test-mon2

Enable Powershell detection

Enable Shellcode detection

  - Disable shellcode/powershell detection.

22.1.3 Multi-tenant by vlan

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 SIGFLOW ruleset as well as to configure codebreaker independently for each vlan. A vlan named "default" is created as standard in the interface. It enables a SIGFLOW ruleset to be applied and codebreaker to be configured for all vlans not explicitly specified in the interface.

Note:

It is advisable to optimise the SIGFLOW ruleset in advance before choosing this configuration option. The rules must be adapted to the monitored environment.

Note:

Changes to this tab require the GCAP configuration to be backed up and implemented via the save and apply button.

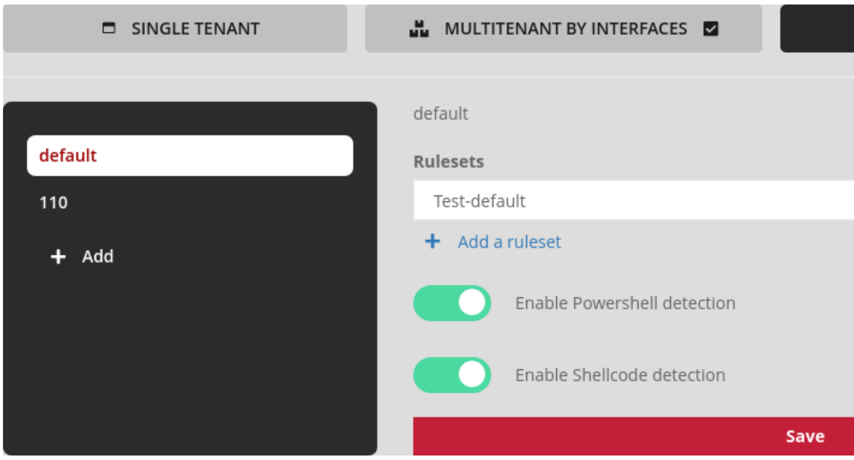
Configuring multi-tenant by vlan:

1. Go to the `Multi-tenant by vlan` tab;
2. Select a ruleset to apply to the default vlan;

3. Enable or disable shellcode detection for the default vlan;
4. Enable or disable powershell detection for vlan "default";
5. Create as many vlans as necessary via the "Add" button;
6. The vlan name must match the vlan number between 0 and 4096;
7. Then select a ruleset to apply to each vlan;
8. Enable or disable shellcode detection for each vlan;
9. Enable or disable powershell detection for each vlan;
10. Apply the configuration by clicking the "save" button.

Configuration example:

- **vlan "default":**
  - Ruleset named "Test-default",



default

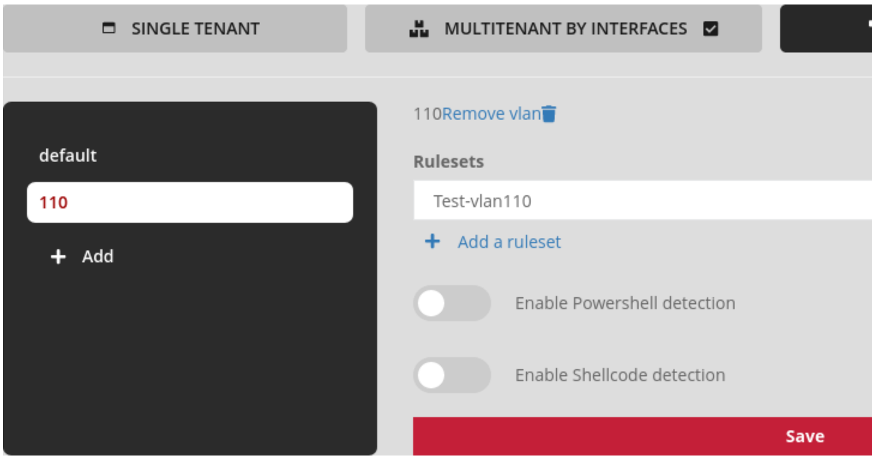
Rulesets

Test-default

● Enable Powershell detection

● Enable Shellcode detection

  - Enabling shellcode/powershell detection.
- **vlan "110":**
  - Ruleset named "Test-vlan110",



110

Rulesets

Test-vlan110

○ Enable Powershell detection

○ Enable Shellcode detection

  - Disable shellcode/powershell detection.

22.2 Base variables

Rôle Opérateur

Menu: Operators > Sigflow > GCAP Profiles

The **Base variables** section enable the operator to adjust the capture parameters of the probe using the advanced Suricata functions configurable from the **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 menu is divided into three sections:

- General
- Stream
- Parsing

22.2.1 Base Variables - General

The **Base Variables - General** tab enables configuring the advanced settings of the GCAP probe (Suricata).

> **Note:**
>
> Changes to this tab require the GCAP configuration to be backed up and implemented via the save and apply button.

The default values for variables on the general tab:

List of variables on the General tab:

- File resend interval (seconds):** time frame in seconds in which, if an identical file is sighted on the network, it will not be resent to the GCENTER by the GCAP. Only the metadata will be sent with the Replica field set to True. After this time interval, if the same file is seen on the network, it will be sent back to the GCENTER.
- **Max pending packets:** Number of simultaneous packets the SURICATA engine can handle. This can range from one packet to tens of thousands of packets. This parameter will have an impact on performance and memory (RAM) usage. A high number of packets being processed enables better performance, more memory to be used, and vice versa. Choosing a low number of packets being processed, while having multiple CPU cores, may result in not using the full capacity of the probe. Example: using a single *core* while having three packets waiting to be processed.
- **Enable XFF:** Enable the HTTP *X-Forwarded-For* header management by adding a new field or by overwriting the source or destination IP address (depending on the direction of the flow) with the IP indicated in this header. The behaviour, either adding a field or overwriting, is handled by the **XFF mode** directive. This directive is helpful when processing flows behind a reverse proxy for example.
- **XFF mode:** Expected behaviour when XFF is activated. Two types of operating modes are available, extra-data or overwrite. Note that in 'overwrite' mode, if the IP address reported in the HTTP X-Forwarded-For header is a different version of the received packet, then it will switch to 'extra-data' mode.
- **XFF deployment:** XFF deployment type. Two types of deployment are available: *reverse* or *forward.* In a *reverse* deployment, the IP address used is the last one, while in a *forward* deployment, the IP address used is the first one.
- **Xff header:** This is the name of the HTTP header in which the actual IP address is present. If more than one IP address is present, the last IP address will be the one used.
- **Payload:** Adds a field containing the base64 encoded payload of a flow triggering an alert.
- **Payload buffer size:** maximum size of the payload buffer to be added to the alert.
- **Payload printable:** Adds a field containing the (*Payload*) in ASCII (so-called 'human') format.
- **Packet:** dump of the captured base64 encoded package.
- **HTTP body:** Adds a field containing the body of base64 encoded HTTP requests. This parameter requires metadata to work.
- **HTTP body printable:** Adds a field containing the body of HTTP requests in ASCII (so-called 'human') format. This parameter requires metadata to work.
- **Flow memcap:** maximum allocation for byte flows.
- **Flow prealloc:** initial flow allocation.
- **FTP memcap (B):** 'maximum allocation for byte flows.
- **SMB Stream Depth (B):** The size of the files that can be restored and saved depends on the value in megabytes. Beyond this value, no reconstruction will be undertaken. If this value is reached, the file may be truncated and not entirely stored. This implies that after this value, the SMB session will no longer be

tracked. Additionally, negative values disable the option. Setting this value to 0 enables any file size to be stored.
- **Files hash:** Enables selecting the hash function for rebuilt files (md5, sha1, and sha256). By default, md5 is selected. The sha256 hash will in all cases be added by the [Malcore] module (malcore.html#presentation).

22.2.2 Base Variables - Stream

Caution:

Changing the settings in this section may cause the TRACKWATCH solution to malfunction. This section is reserved for support staff and advanced users.

Only the "file_store_stream_depth_mb" variable can be modified, never exceeding 100 MB.

The **Base Variables - Stream** tab enables configuring the file reconstruction parameters as well as the **Stream-engine** module of the GCAP probe (Suricata). The **Stream-engine** module of the probe enables monitoring the TCP connections.

Note:

Changes to this tab require the GCAP configuration to be backed up and implemented via the save and apply button.

The engine consists of two parts:

- **Stream-tracking engine:** Enables tracking the TCP connection status;
- **Reassembly-engine:** Reassembles the flow for analysis by Suricata.

The default values for variables on the stream tab:

List of variables on the Stream tab:

- **Enable File-Store stream depth:** Enables control of the stored file size.
- **File-store stream depth (Mb):** Sets the maximum size of files that can be restored and saved in megabytes. If this value is reached, the file may be truncated and not entirely stored. This implies that after this value, the HTTP session will no longer be tracked. A negative value disables the option. A value of 0 enables any file size to be stored. If this option is not enabled, then the value of 'Stream reassembly depth (Mb)' will be taken into account.
- **Stream memcap (B):** This value is the maximum value in bytes allocated to TCP session tracking. In order to avoid a lack of resources, a memcap can be used to restrict the memory used.
- **Stream Prealloc sessions:** This is the amount of sessions the SURICATA engine must hold in memory. This engine works independently of packet processing. It has a management thread that sets this value inside the memcap to allocate memory. The option enables SURICATA to avoid being overloaded by the fast creation of sessions. It instructs it to keep a certain number of sessions ready in memory. It specifies the number of elements to be pre-allocated when the software boots. This reduces the cost of in-running allocations at the expense of the software's initial memory usage.
- **Stream reassembly memcap (B)** The stream reassembly engine must retain segments of data in memory in order to rebuild it. To avoid resource constraints, a memcap is used to limit the memory used. This option is the maximum amount of bytes the flow engine can use to restore a file.
- **Enable the randomizable of chunks size:** The purpose of this setting is to avoid making chunk recovery too predictable. For this purpose, their size will be modified by a random factor that will be added.
- Stream reassembly depth (Mb)** This is the size of the network flow in megabytes. The act of reassembling a data flow is a very important operation that can be controlled using the 'depth' concept. The default value is a parameter that can be overridden by the protocol analysers performing the file extraction. The inspection will be ignored if this value is reached for a particular flow. Setting this value to 0 enables any flow size to be stored.

- **Stream reassembly to server chunk size (B)** The reconstruction of a data stream is carried out in chunks. The size of these chunks is to be set in this field so that the flow is inspected and rebuilt using this value.
- **Stream reassembly to client chunk size (B)** The reconstruction of a data stream is carried out in chunks. The size of these chunks is to be set in this field so that the flow is inspected and rebuilt according to it.

22.2.3 Base Variables - Parsing

The **Base Variables - Parsing** tab enables configuring the **parsing** and **logging** of protocols used by the GCAP probe. Protocols that can be parsed and logged are present in the **GCenter** interface. In the event a **GCAP** probe is one version ahead of the GCenter, it is possible that some protocols have been added.

This is discussed in more detail in the [**GCAP**] documentation (https://docs.gatewatcher.com/gcap.html) in the section `Detection Engine > 3. Selecting the protocols being analysed`.

Terminology for parsing and logging:

- **Parsing** consists of enabling SIGFLOW signature detection for a given protocol. Indeed, if the latter is activated for a protocol, then the flow identified by a signature will raise a SIGFLOW alert in the Kibana dashboard.
- The **logging** consists in enabling the generation of metadata for a given protocol. Indeed, if the latter is activated for a protocol, then each observed session will raise an alert for that protocol in the Kibana dashboard.

Note:

The protocols' default settings vary depending on the GCAP profile used.

Note:

Changes to this tab require the GCAP configuration to be backed up and implemented via the save and apply button.

Here is the list of protocols that can be configured with the parsing option:

- dcerpc
- dnp3
- dns_udp
- dns_tcp
- ftp
- http
- modbus
- smb
- smtp
- ssh
- tls
- dhcp
- ikev2
- krb5
- nfs
- ntp
- tftp

Here is the list of protocols that can be configured with the logging option:

- http
- dns_udp

- dns_tcp
- tls
- smtp
- smb
- ssh
- netflow
- dnp3
- ftp
- dhcp
- ikev2
- krb5
- nfs
- tftp

Here is the default configuration of the parsing option for each protocol according to the profile used:

Here is the default configuration of the logging option for each protocol according to the profile used:

In addition to these protocols, it is also possible to generate NetFlow data.

> **Warning:**
>
> Enabling NetFlow data generation will create a great deal of metadata

22.3 Net variables

Rôle Opérateur

Menu: Operators > Sigflow > GCAP Profiles

The **Net variables** section enables the operator to define the network variables used in the sigflow rules.

note:: Changes to this section require the GCAP configuration to be backed up and implemented via the save and apply button.

In the structure of a SIGFLOW 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;)
```

These flows must go from $HOME_NET to $EXTERNAL_NET.

The first part $HOME_NET is the source, the second $EXTERNAL_NET is the destination. With the source and destination, you specify the origin of the traffic and the location of the traffic, respectively. You can assign IP addresses (IPv4 and IPv6 are supported) and IP ranges. These parameters will be used instead of variables in the detection rules.

This section enables you to define the contents of these variables.

To implement these changes, it is necessary to click on the **Save and Apply** button.

The rule adapts to the needs. It can change depending on the parameter selected in the drop-down menu of each environment. The 'list', 'default (equal to HOME_NET)' and 'exclude (opposite of HOME_NET)' options respectively enable the action of the rule to be defined in relation to a group of addresses, in relation to the addresses specified in the HOME_NET environment, or in relation to all the addresses 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 default configuration used:

22.4 Flow timeouts

Rôle Opérateur

Menu: Operators > Sigflow > GCAP Profiles

Caution:

Changing the settings in this section may cause the TRACKWATCH solution to malfunction. This section is reserved for support staff and advanced users.

The **Flow timeouts** section enables configuring the time in seconds that Suricata retains a flow in memory depending on its status. The udp, tcp, and icmp protocols are configurable.

Note:

Changes to this section require the GCAP configuration to be backed up and implemented via the save and apply button.

The default configuration used depending on the protocol (all values are in seconds):

For each protocol, there are different statuses in which a flow can be found:

- **TCP protocol:**
  - **New:** The period of time during which the connection is established. This field is the time in seconds after the last activity of this flow in this status type.
  - **Established:** The period of time during which the data transfer is taking place. This field is the time in seconds after the last activity of this flow in this status type.
  - **Closed:** The time period during which the connection is terminated. This field is the time in seconds after the last activity of this flow in this status type.
- **UDP and ICMP protocols:**
  - **New:** The status during which packets are sent from a single direction. This field is the time in seconds after the last activity of this flow in this status type.
  - **Established:** The status during which packets are sent in both directions. This field is the time in seconds after the last activity of this flow in this status type.

**Emergency_new', 'Emergency_established' and 'Emergency_closed' are the emergency modes for the three states of TCP, UDP, and ICMP.

22.5 Files rules management

Rôle Opérateur

Menu: Operators > Sigflow > GCAP Profiles

The **Files rules management** section enables configuring the file types that the probe will retrieve for a given protocol. The supported protocols are: HTTP, SMTP, SMB, NFS, and FTP. Files are extracted and then saved to disk with metadata. This includes information such as timestamp, source/destination IP address, protocol, source/destination port, size, and md5sum, etc. File extraction works in parallel with the SIGFLOW signatures defined for these same protocols. Each line in the **Files rules management** 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 probe.

Note:

Changes to this section require the GCAP configuration to be backed up and implemented via the save and apply button.

Here is the list of fields that can be configured for an entry in the Files rules management: section

- **Protocol:** Enables selecting the protocol for which the file will be extracted from among: HTTP, SMTP, SMB, NFS, and FTP.
- **Type:** Enables defining the way suricata recognises the file:
  - extension: Corresponds to the file extension.
  - filemagic: Corresponds to the type of extracted file. The **file** command under linux enables obtaining this information:

```
shell
xxx@debian:~$ file ~/Téléchargements/xxx.exe
/home/xxx/Téléchargements/xxx.exe: PE32 executable (console) Intel 80386, for MS Windows
```

- **Value:** The identifier of the file that will be rebuilt according to the previously configured type:
  - **Type extension:**
    - Fichier javascript: js,
    - Windows executable file: exe.
  - **filemagic type:**
    - Javascript file: Javascript,
    - Windows executable file: PE32 executable.
- Enable** and **Delete** are the tick boxes for activating and removing the file extraction rule respectively.

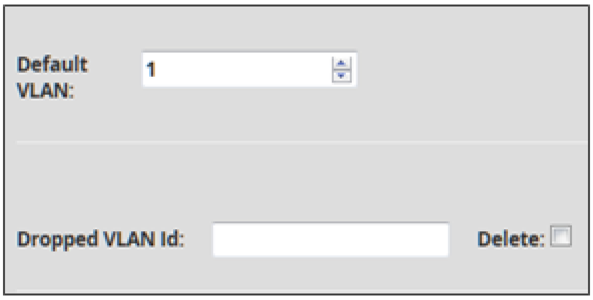
The rules applied depending on the GCAP profile used:

22.6 Packet filtering

Rôle Opérateur

Menu: Operators > Sigflow > GCAP Profiles

Packet filtering enables the operator to adjust the capture parameters of the detection probe using Sigflow's advanced functions.



Default VLAN: 1

Dropped VLAN Id:

Delete: □

The purpose of this feature is to act directly on the TRACKWATCH capture device by modifying the packet acquisition method using Barkeley Packet Filter (BPF). Traffic will therefore be ignored for a given VLAN ID in the 'Dropped VLAN Id' field.

The default VLAN number is set on the **GCENTER** web interface in 'Default VLAN'. By default, this value is 1. Once the VLAN is set, a window appears allowing the operator to add network information about the traffic they want to remove from their notifications.

The operator can remove a filter rule via the **Delete** box. The changes are recorded when the form is validated by clicking on the **Save** button. However, in order to implement them it will be necessary to click on the **Save and Apply** button on the configuration page.

Chapter 23

Rules management

The signatures of the **Sigflow** engine are structured in the following way:

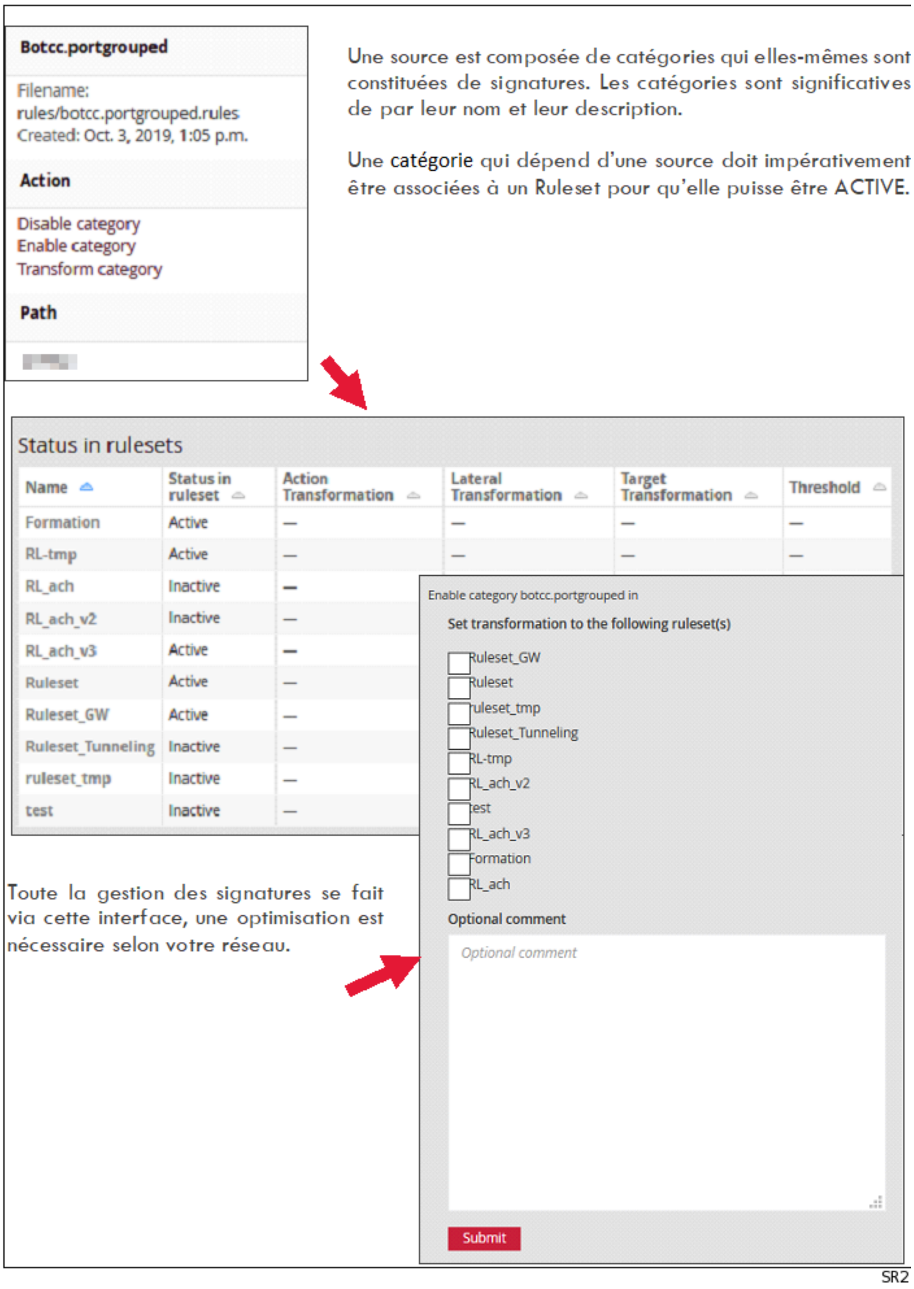
- A list of sources providing signatures
- A list of signatures capable of adapting to the needs of the environment to be monitored
- A list of *Ruleset* enabling signatures to be linked to their sources and a **GCAP**

23.1 Sources

Rôle Opérateur

Menu: Operators > Sigflow > Sources

Sources enable reporting on the locations where signatures are made available.



Une source est composée de catégories qui elles-mêmes sont constituées de signatures. Les catégories sont significatives de par leur nom et leur description.

Une catégorie qui dépend d'une source doit impérativement être associées à un Ruleset pour qu'elle puisse être ACTIVE.

Botcc.portgrouped

Filename: rules/botcc.portgrouped.rules
Created: Oct. 3, 2019, 1:05 p.m.

Action

Disable category
Enable category
Transform category

Path

[redacted]

Status in rulesets

Name	Status in ruleset	Action Transformation	Lateral Transformation	Target Transformation	Threshold
Formation	Active	—	—	—	—
RL-tmp	Active	—	—	—	—
RL_ach	Inactive	—			
RL_ach_v2	Inactive	—			
RL_ach_v3	Active	—			
Ruleset	Active	—			
Ruleset_GW	Active	—			
Ruleset_Tunneling	Inactive	—			
ruleset_tmp	Inactive	—			
test	Inactive	—			

Enable category botcc.portgrouped in

Set transformation to the following ruleset(s)

□ Ruleset_GW
□ Ruleset
□ ruleset_tmp
□ Ruleset_Tunneling
□ RL-tmp
□ RL_ach_v2
□ test
□ RL_ach_v3
□ Formation
□ RL_ach

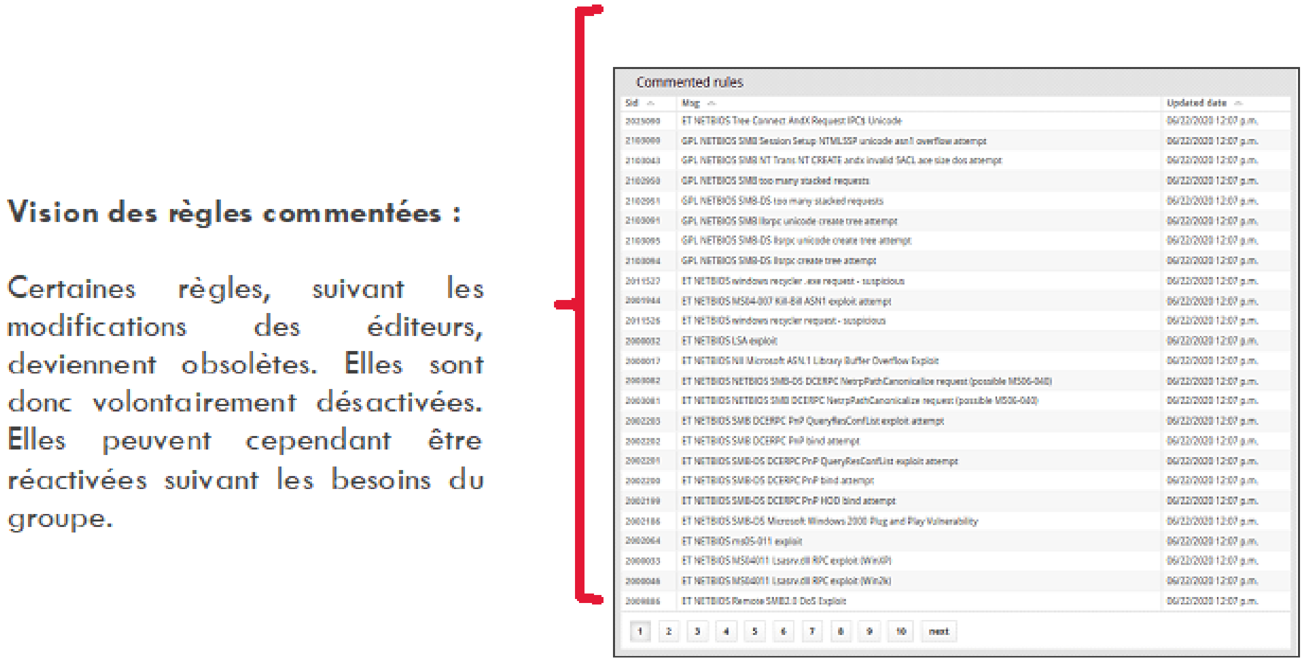
Optional comment

Optional comment

Submit

Toute la gestion des signatures se fait via cette interface, une optimisation est nécessaire selon votre réseau.

SR2



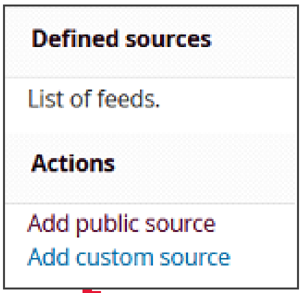
Vision des règles commentées :

Certaines règles, suivant les modifications des éditeurs, deviennent obsolètes. Elles sont donc volontairement désactivées. Elles peuvent cependant être réactivées suivant les besoins du groupe.

Commented rules

Sid	Msg	Updated date
2025090	ET NETBIOS Tree Connect AndX Request IPC$ Unicode	06/22/2020 12:07 p.m.
2103000	GPL NETBIOS SMB Session Setup NTMLSSP unicode asn1 overflow attempt	06/22/2020 12:07 p.m.
2103043	GPL NETBIOS SMB NT Trans NT CREATE andx invalid SACL ace size dos attempt	06/22/2020 12:07 p.m.
2102950	GPL NETBIOS SMB too many stacked requests	06/22/2020 12:07 p.m.
2102951	GPL NETBIOS SMB-DS too many stacked requests	06/22/2020 12:07 p.m.
2103091	GPL NETBIOS SMB llsrpc unicode create tree attempt	06/22/2020 12:07 p.m.
2103095	GPL NETBIOS SMB-DS llsrpc unicode create tree attempt	06/22/2020 12:07 p.m.
2103094	GPL NETBIOS SMB-DS llsrpc create tree attempt	06/22/2020 12:07 p.m.
2011527	ET NETBIOS windows recycler .exe request - suspicious	06/22/2020 12:07 p.m.
2001944	ET NETBIOS MS04-007 Kill-Bill ASN1 exploit attempt	06/22/2020 12:07 p.m.
2011526	ET NETBIOS windows recycler request - suspicious	06/22/2020 12:07 p.m.
2000032	ET NETBIOS LSA exploit	06/22/2020 12:07 p.m.
2000017	ET NETBIOS NII Microsoft ASN.1 Library Buffer Overflow Exploit	06/22/2020 12:07 p.m.
2003082	ET NETBIOS NETBIOS SMB-DS DCERPC NetrpPathCanonicalize request (possible MS06-040)	06/22/2020 12:07 p.m.
2003081	ET NETBIOS NETBIOS SMB DCERPC NetrpPathCanonicalize request (possible MS06-040)	06/22/2020 12:07 p.m.
2002203	ET NETBIOS SMB DCERPC PnP QueryResConfList exploit attempt	06/22/2020 12:07 p.m.
2002202	ET NETBIOS SMB DCERPC PnP bind attempt	06/22/2020 12:07 p.m.
2002201	ET NETBIOS SMB-DS DCERPC PnP QueryResConfList exploit attempt	06/22/2020 12:07 p.m.
2002200	ET NETBIOS SMB-DS DCERPC PnP bind attempt	06/22/2020 12:07 p.m.
2002199	ET NETBIOS SMB-DS DCERPC PnP HOD bind attempt	06/22/2020 12:07 p.m.
2002186	ET NETBIOS SMB-DS Microsoft Windows 2000 Plug and Play Vulnerability	06/22/2020 12:07 p.m.
2002064	ET NETBIOS ms05-011 exploit	06/22/2020 12:07 p.m.
2000033	ET NETBIOS MS04011 Lsasrv.dll RPC exploit (WinXP)	06/22/2020 12:07 p.m.
2000046	ET NETBIOS MS04011 Lsasrv.dll RPC exploit (Win2k)	06/22/2020 12:07 p.m.
2009886	ET NETBIOS Remote SMB2.0 DoS Exploit	06/22/2020 12:07 p.m.

Once downloaded and unpacked, the rules need to be added to the **GCENTER** interface.



Defined sources

List of feeds.

Actions

Add public source
Add custom source

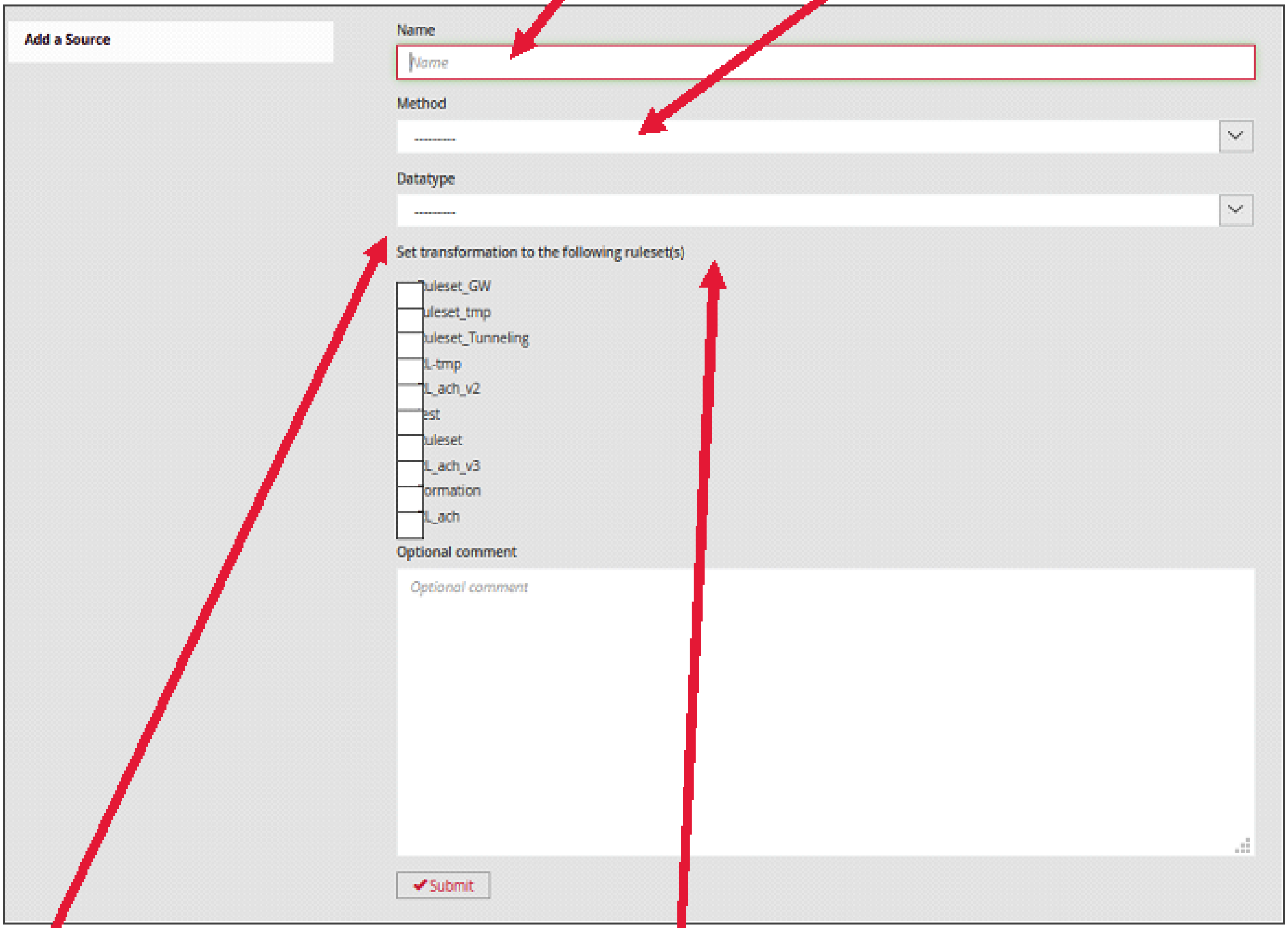
Nous préconisons le package SIGFLOW par défaut, mais l'administrateur peut ajouter à n'importe quelque moment ses propres signatures. En effet les extensions suivantes sont pris en compte par l'interface : **.yara, .rules, .openioc, .csv, .txt.**

Depuis Add custom source, l'opérateur ajoute une source de la manière suivante :

1 Nom de la règle

2 Méthode :

- HTTP URL
- Upload



Add a Source

Name

Name

Method

Datatype

Set transformation to the following ruleset(s)

□ uleset_GW
□ uleset_tmp
□ uleset_Tunneling
□ L-tmp
□ L_ach_v2
□ est
□ uleset
□ L_ach_v3
□ ormation
□ L_ach

Optional comment

Optional comment

✓Submit

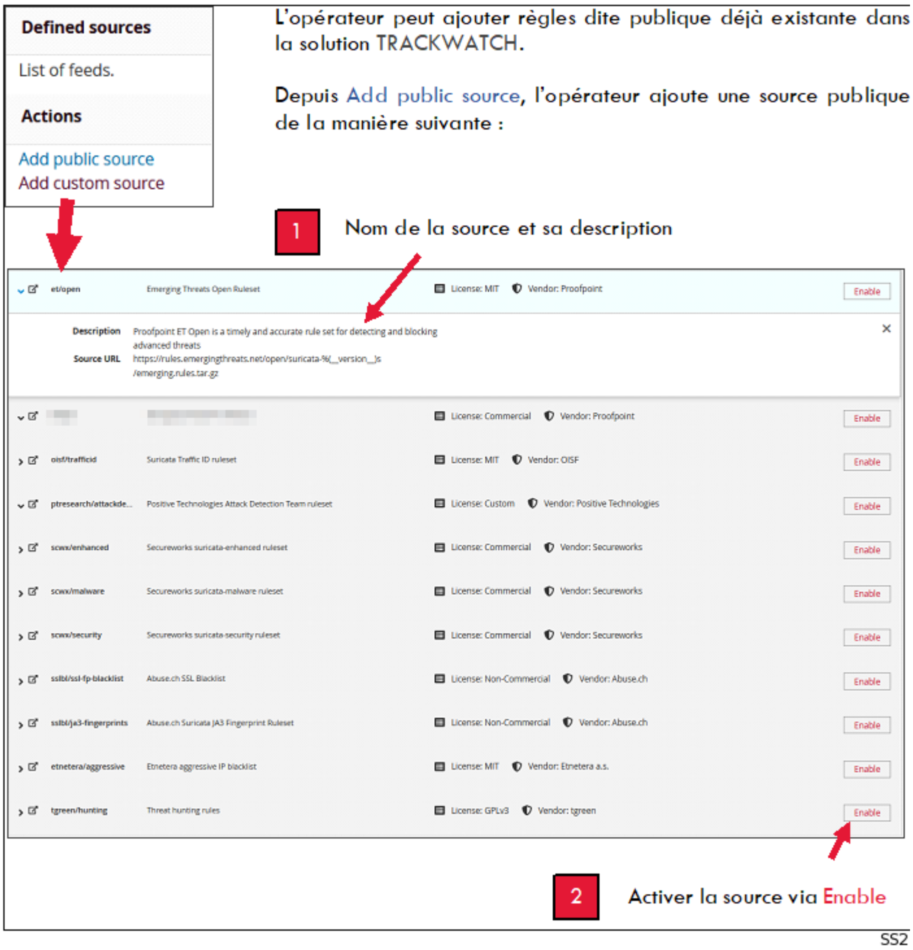
3 Type des données :

- Signatures dans une archive .tar
- Signatures dans un fichier
- Autres

4 Suivant la méthode choisie :

- Les signatures sont importées depuis un dossier local ou via une adresse URL renseignée au niveau du champs (vérification des certificats au choix).

'Submit' pour appliquer l'ajout de la source.



Defined sources

List of feeds.

Actions

Add public source
Add custom source

L'opérateur peut ajouter règles dite publique déjà existante dans la solution TRACKWATCH.

Depuis Add public source, l'opérateur ajoute une source publique de la manière suivante :

1 Nom de la source et sa description

et/open	Emerging Threats Open Ruleset	License: MIT	Vendor: Proofpoint	Enable
[redacted]	[redacted]	License: Commercial	Vendor: Proofpoint	Enable
oisf/trafficid	Suricata Traffic ID ruleset	License: MIT	Vendor: OISF	Enable
ptresearch/attackde...	Positive Technologies Attack Detection Team ruleset	License: Custom	Vendor: Positive Technologies	Enable
scwx/enhanced	Secureworks suricata-enhanced ruleset	License: Commercial	Vendor: Secureworks	Enable
scwx/malware	Secureworks suricata-malware ruleset	License: Commercial	Vendor: Secureworks	Enable
scwx/security	Secureworks suricata-security ruleset	License: Commercial	Vendor: Secureworks	Enable
sslbl/ssl-fp-blacklist	Abuse.ch SSL Blacklist	License: Non-Commercial	Vendor: Abuse.ch	Enable
sslbl/ja3-fingerprints	Abuse.ch Suricata JA3 Fingerprint Ruleset	License: Non-Commercial	Vendor: Abuse.ch	Enable
etnetera/aggressive	Etnetera aggressive IP blacklist	License: MIT	Vendor: Etnetera a.s.	Enable
tgreen/hunting	Threat hunting rules	License: GPLv3	Vendor: tgreen	Enable

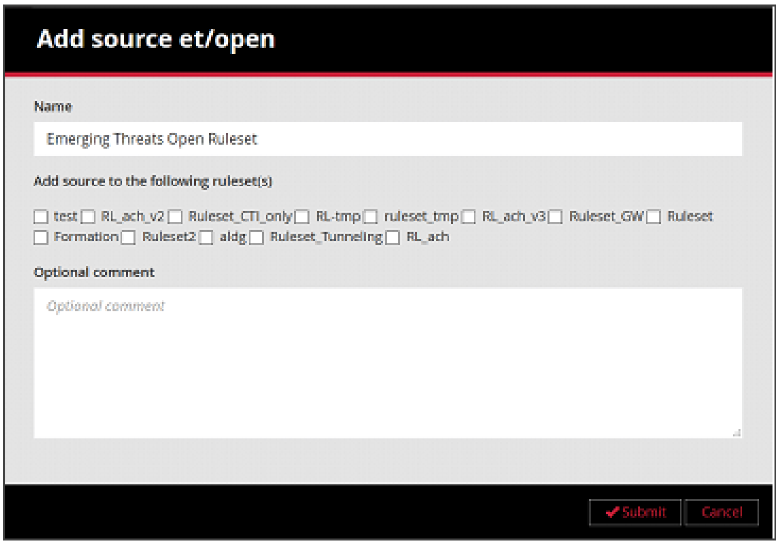
Description: Proofpoint ET Open is a timely and accurate rule set for detecting and blocking advanced threats

Source URL: https://rules.emergingthreats.net/open/suricata-%(__version__)s/emerging.rules.tar.gz

2 Activer la source via Enable

SS2

Once the rules are added, the operator can directly assign this source to different Rulesets



Add source et/open

Name

Emerging Threats Open Ruleset

Add source to the following ruleset(s)

□ test □ RL_ach_v2 □ Ruleset_CTI_only □ RL-tmp □ ruleset_tmp □ RL_ach_v3 □ Ruleset_GW □ Ruleset □ Formation □ Ruleset2 □ aldg □ Ruleset_Tunneling □ RL_ach

Optional comment

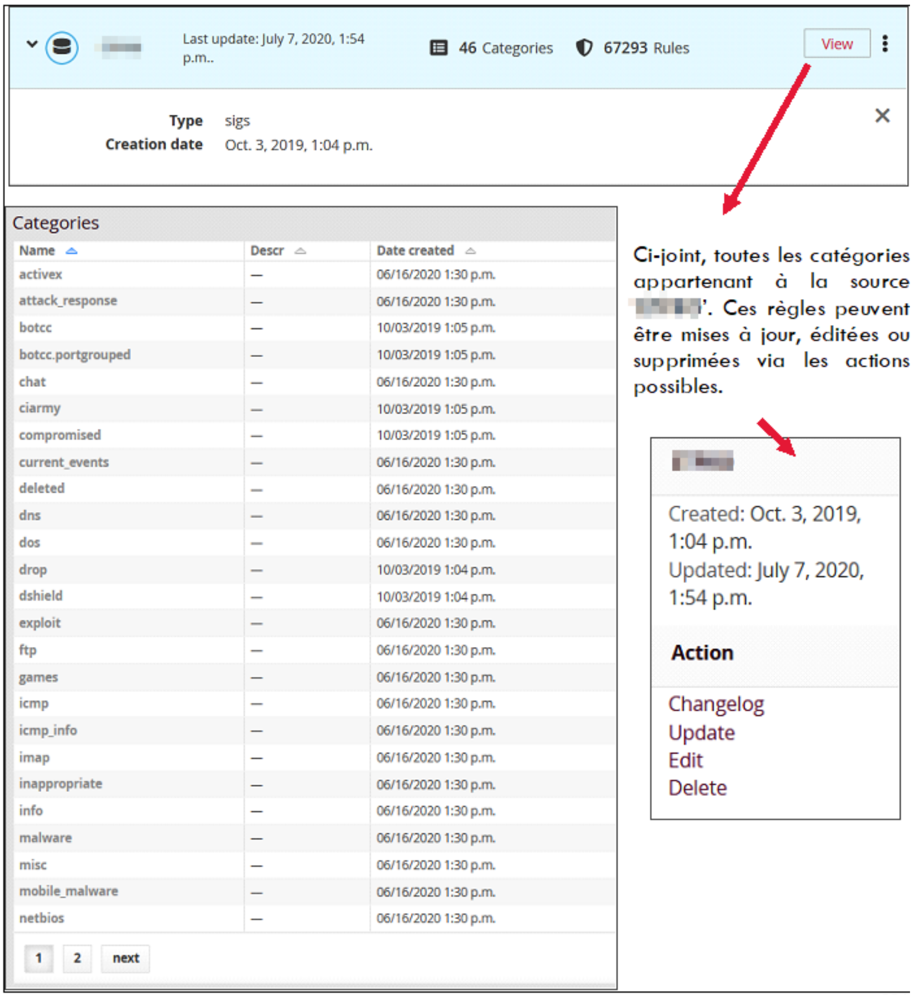
Optional comment

Le nom peut être édité puis la source est ajoutée aux Rulesets déjà présents en cochant la case associée.

Un commentaire optionnel pour le suivi est possible.

Valider avec 'Submit' une fois le choix fait.

Displaying a custom rule is done from the 'View' tab in Add custom source:



[redacted] Last update: July 7, 2020, 1:54 p.m.. 46 Categories 67293 Rules

Type sigs
Creation date Oct. 3, 2019, 1:04 p.m.

Categories

Name	Descr	Date created
activex	—	06/16/2020 1:30 p.m.
attack_response	—	06/16/2020 1:30 p.m.
botcc	—	10/03/2019 1:05 p.m.
botcc.portgrouped	—	10/03/2019 1:05 p.m.
chat	—	06/16/2020 1:30 p.m.
ciarmy	—	10/03/2019 1:05 p.m.
compromised	—	10/03/2019 1:05 p.m.
current_events	—	06/16/2020 1:30 p.m.
deleted	—	06/16/2020 1:30 p.m.
dns	—	06/16/2020 1:30 p.m.
dos	—	06/16/2020 1:30 p.m.
drop	—	10/03/2019 1:04 p.m.
dshield	—	10/03/2019 1:04 p.m.
exploit	—	06/16/2020 1:30 p.m.
ftp	—	06/16/2020 1:30 p.m.
games	—	06/16/2020 1:30 p.m.
icmp	—	06/16/2020 1:30 p.m.
icmp_info	—	06/16/2020 1:30 p.m.
imap	—	06/16/2020 1:30 p.m.
inappropriate	—	06/16/2020 1:30 p.m.
info	—	06/16/2020 1:30 p.m.
malware	—	06/16/2020 1:30 p.m.
misc	—	06/16/2020 1:30 p.m.
mobile_malware	—	06/16/2020 1:30 p.m.
netbios	—	06/16/2020 1:30 p.m.

Ci-joint, toutes les catégories appartenant à la source '[redacted]'. Ces règles peuvent être mises à jour, éditées ou supprimées via les actions possibles.

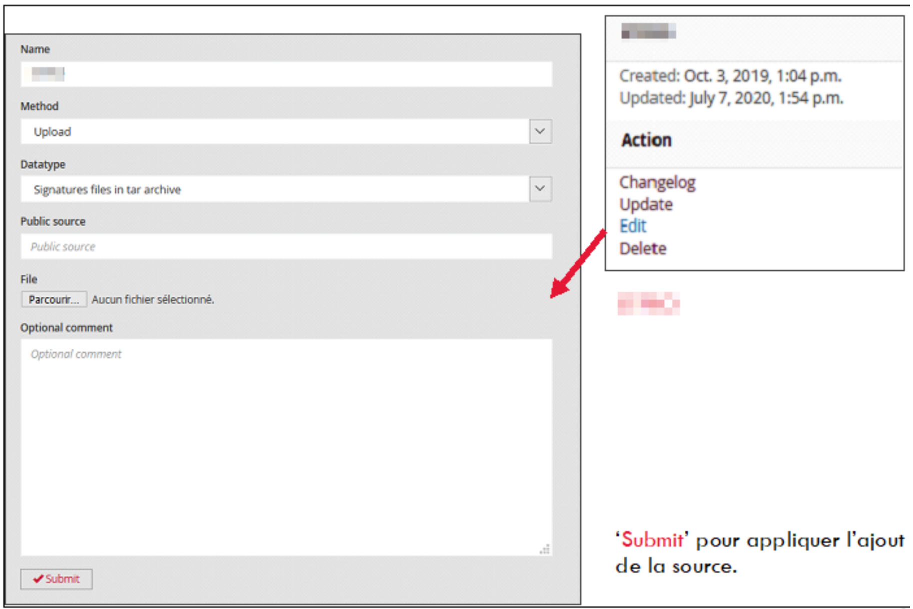
[redacted]

Created: Oct. 3, 2019, 1:04 p.m.
Updated: July 7, 2020, 1:54 p.m.

Action

SS4

These sources update automatically in the case of public / HTTP sources if the **GCENTER** is connected to the internet. Otherwise, a manual update can be done on this interface in order to ensure that the latest signatures are available.



Name: [redacted]
Method: Upload
Datatype: Signatures files in tar archive
Public source: Public source
File: Parcourir... Aucun fichier sélectionné.
Optional comment: Optional comment

[redacted]

Created: Oct. 3, 2019, 1:04 p.m.
Updated: July 7, 2020, 1:54 p.m.

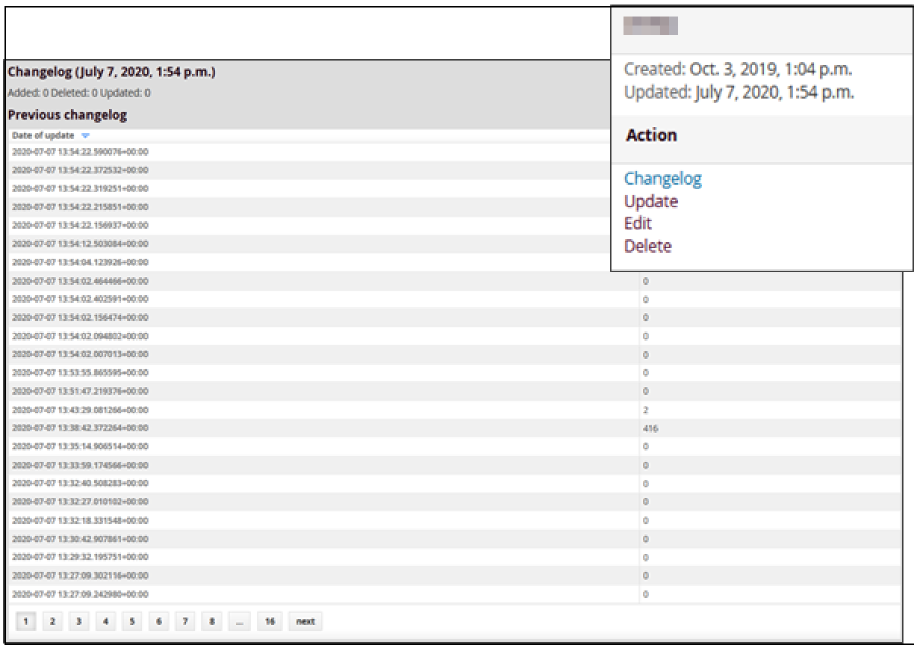
Action

[redacted]

'Submit' pour appliquer l'ajout de la source.

SS6

Updating signatures and checking the history of changes is possible:



[redacted]

Created: Oct. 3, 2019, 1:04 p.m.
Updated: July 7, 2020, 1:54 p.m.

Action

Changelog
Update
Edit
Delete

Changelog (July 7, 2020, 1:54 p.m.)

Added: 0 Deleted: 0 Updated: 0

Previous changelog

Date of update	
2020-07-07 13:54:22.590076+00:00	
2020-07-07 13:54:22.372532+00:00	
2020-07-07 13:54:22.319251+00:00	
2020-07-07 13:54:22.215851+00:00	
2020-07-07 13:54:22.156937+00:00	
2020-07-07 13:54:12.503084+00:00	
2020-07-07 13:54:04.123926+00:00	
2020-07-07 13:54:02.464466+00:00	0
2020-07-07 13:54:02.402591+00:00	0
2020-07-07 13:54:02.156474+00:00	0
2020-07-07 13:54:02.094802+00:00	0
2020-07-07 13:54:02.007013+00:00	0
2020-07-07 13:53:55.865595+00:00	0
2020-07-07 13:51:47.219376+00:00	0
2020-07-07 13:43:29.081266+00:00	2
2020-07-07 13:38:42.372264+00:00	416
2020-07-07 13:35:14.906514+00:00	0
2020-07-07 13:33:59.174566+00:00	0
2020-07-07 13:32:40.508283+00:00	0
2020-07-07 13:32:27.010102+00:00	0
2020-07-07 13:32:18.331548+00:00	0
2020-07-07 13:30:42.907861+00:00	0
2020-07-07 13:29:32.195751+00:00	0
2020-07-07 13:27:09.302116+00:00	0
2020-07-07 13:27:09.242980+00:00	0

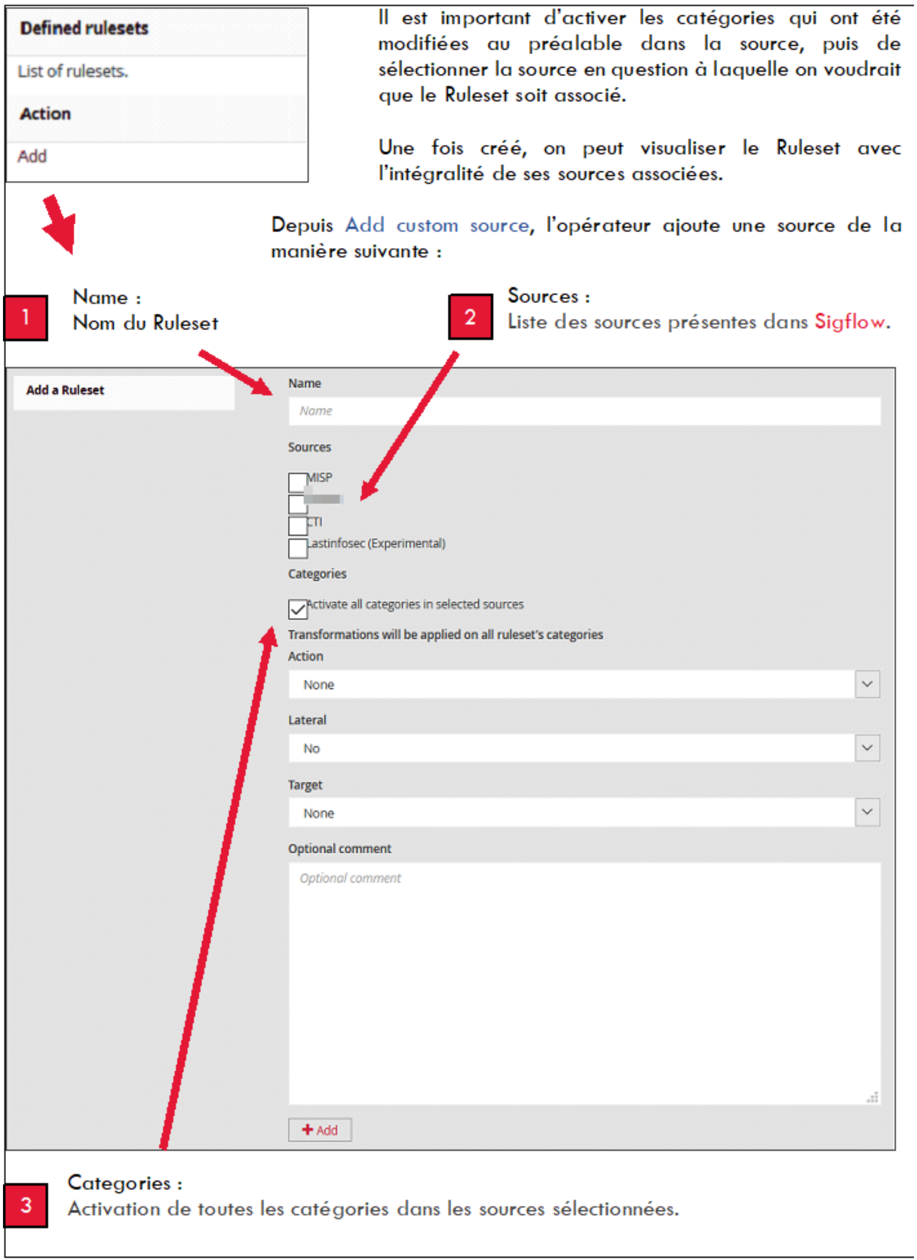
SS7

23.2 Rulesets

Rôle Opérateur

Menu: Operators > Sigflow > Rulesets

Subsequently, a 'Ruleset' must be assigned to the previously added source. The creation of the Ruleset is mandatory in order for the **GCAP** probe to analyse the network flow and issue alerts if the signatures match.



Defined rulesets

List of rulesets.

Action

Add

Il est important d'activer les catégories qui ont été modifiées au préalable dans la source, puis de sélectionner la source en question à laquelle on voudrait que le Ruleset soit associé.

Une fois créé, on peut visualiser le Ruleset avec l'intégralité de ses sources associées.

Depuis Add custom source, l'opérateur ajoute une source de la manière suivante :

1 Name :
Nom du Ruleset

2 Sources :
Liste des sources présentes dans Sigflow.

Add a Ruleset

Name: Name

Sources

□ MISP
□ [redacted]
□ CTI
□ Lastinfosec (Experimental)

Categories

☑ Activate all categories in selected sources

Transformations will be applied on all ruleset's categories

Action: None

Lateral: No

Target: None

Optional comment: Optional comment

+ Add

3 Categories :
Activation de toutes les catégories dans les sources sélectionnées.

SR1

Modifications can be made to the rules in order to adapt a public rule to specific information systems or to a particular need.

The following changes will be applied to all categories of the *Ruleset*.

ACTION:

Determines the action to be applied to the created Ruleset.

Filestore: If a ruleset matches and contains a signature, the packet will be treated and stored like any other packet.

Reject: If the packet is rejected, Sigflow issues an alert for both reset packets (TCP) and ICMP error packets.

Drop: If it finds a matching rule containing the signature, it stops immediately. The packet will no longer be sent and an alert will be issued.

Bypass: If a rule matches and contains a 'bypass', Sigflow will stop scanning the packet and skip to the end of all rules. This will only be for the current packet.

LATERAL:

Signatures are often written with the variables $EXTERNAL\NET and $HOME\NET. This means that they will not match if both sides of a flow are in the $HOME_NET. Thus, lateral movements are not detected. This transformation changes $EXTERNAL_NET into any other variable in order to detect lateral movements.

The option can assume three values:

No: the replacement is not performed

Yes: $EXTERNAL_NET is replaced by whatever IP (any)

Auto: substitution is made if the signature checks certain properties

TARGET:

The keyword 'target' can be used to indicate which side of a flow triggering a signature is the target. If this key is present, related events are enhanced to contain the source and target of the attack.

The option can assume four values:

Auto: an algorithm is used to determine the target if one is present

Destination: the target is the receiving IP

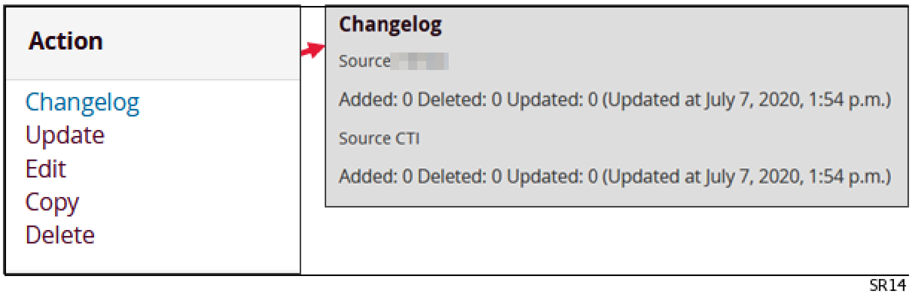
Source: the target is the originating IP

None: no transformation is performed

'Add' to validate the insertion of the ruleset.

23.2.1 Optimisation of rulesets

As with the sources, the ruleset can update itself at any time. It thus updates all its signatures while proposing a differential of the operated changes:



Changelog

Source [redacted]

Added: 0 Deleted: 0 Updated: 0 (Updated at July 7, 2020, 1:54 p.m.)

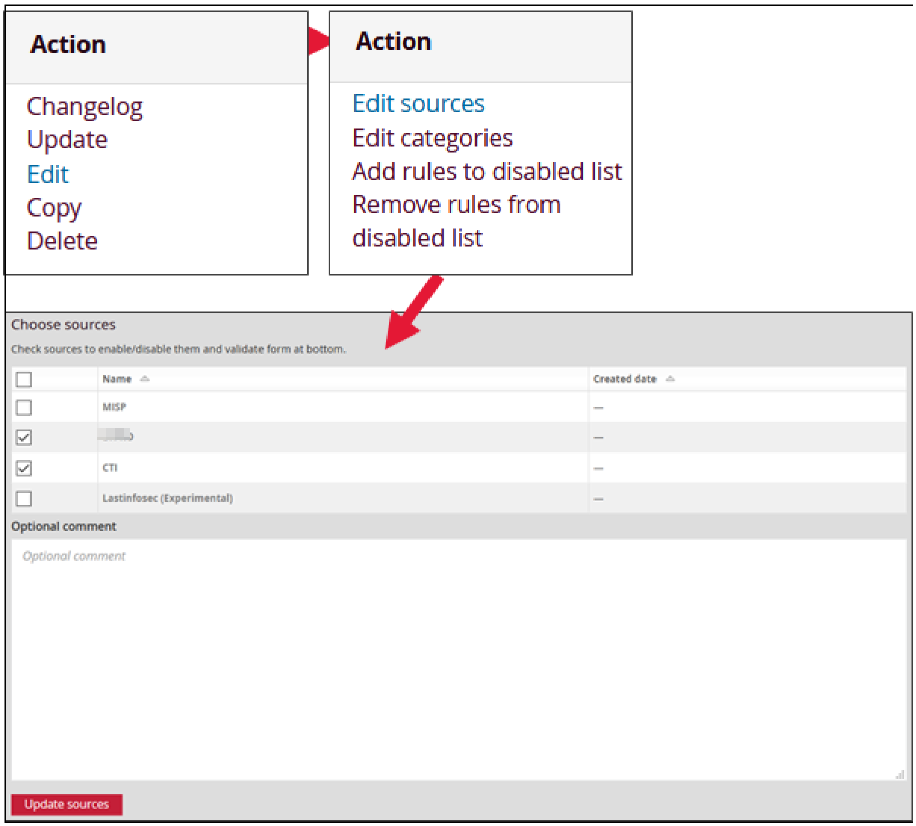
Source CTI

Added: 0 Deleted: 0 Updated: 0 (Updated at July 7, 2020, 1:54 p.m.)

A Ruleset can be edited to allow the operator to make changes to the sources, categories, or rules in the Ruleset.

ACTION EDIT SOURCES:

This option is used to manually enable or disable the action of a source on a Ruleset.



Choose sources

Check sources to enable/disable them and validate form at bottom.

□	Name	Created date
□	MISP	–
☑	[redacted]	–
☑	CTI	–
□	Lastinfosec (Experimental)	–

Optional comment

Optional comment

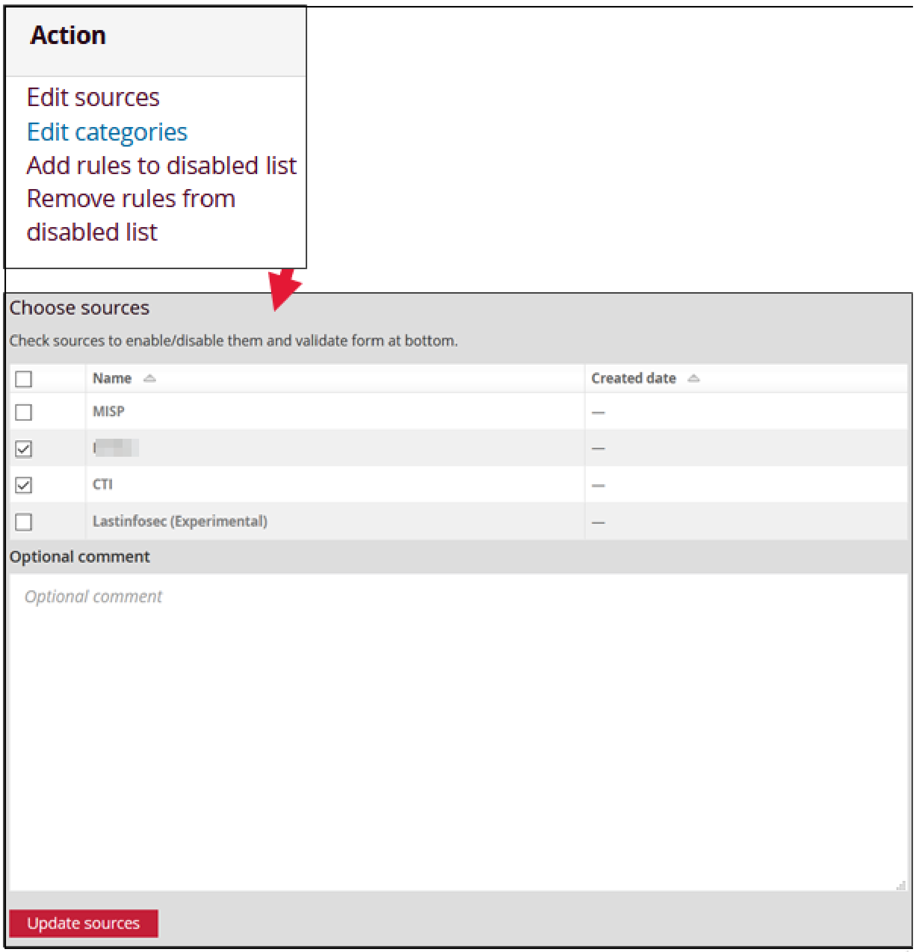
SR15

Once unticked, the signatures will no longer be matched by particular flows and no longer raise an alert on the interface.

ACTION EDIT CATEGORIES:

This option is used to manually enable or disable the action of a category on a Ruleset.

Once unticked, the signatures will no longer be matched by particular flows and no longer raise an alert on the interface.



Choose sources

Check sources to enable/disable them and validate form at bottom.

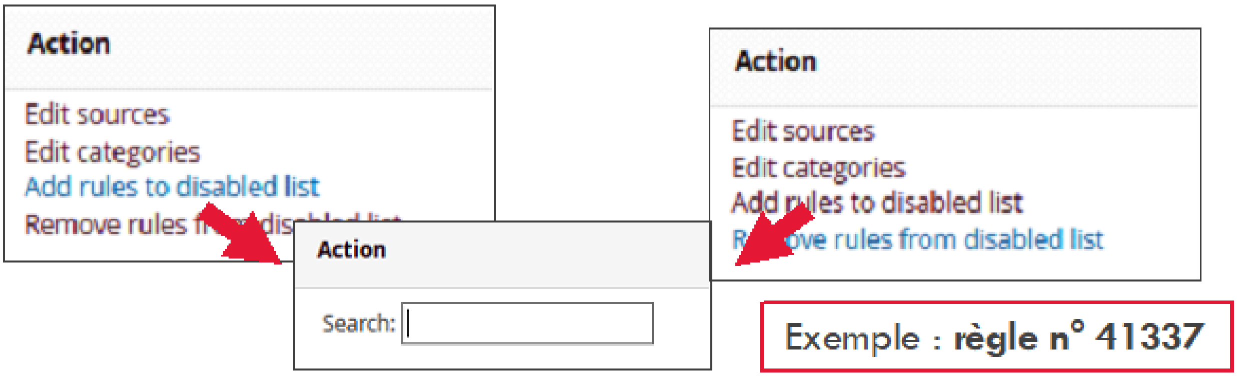
□	Name	Created date
□	MISP	—
☑	[redacted]	—
☑	CTI	—
□	Lastinfosec (Experimental)	—

Optional comment

Optional comment

SR16

It is possible to deactivate a signature related to a Ruleset directly from the SIGFLOW interface. Deactivating a rule does not lead to its permanent deletion.



Action

Edit sources
Edit categories
Add rules to disabled list
Remove rules from disabled list

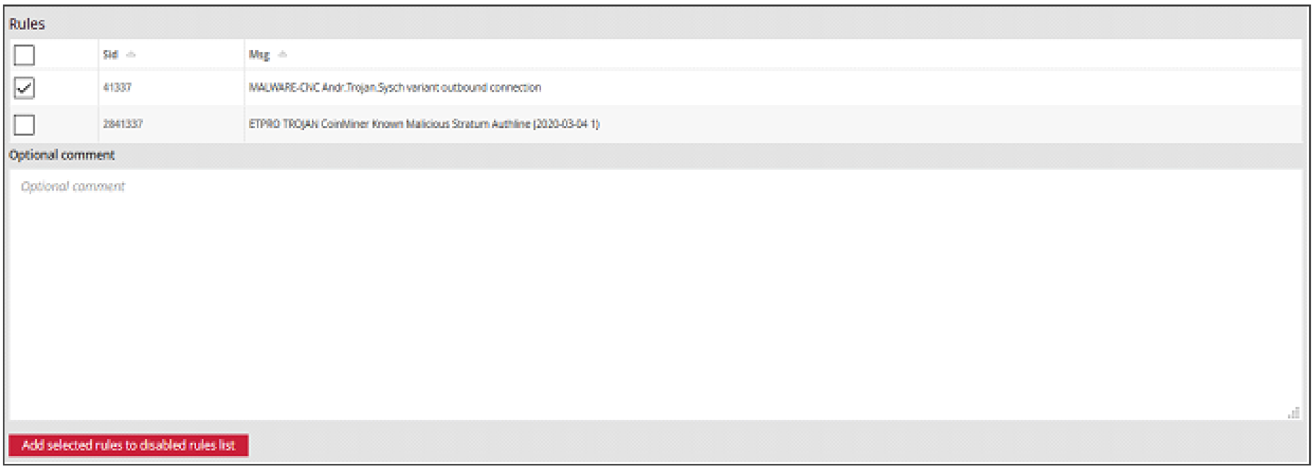
Action

Search:

Action

Edit sources
Edit categories
Add rules to disabled list
Remove rules from disabled list

Exemple : règle n° 41337



Rules

□	Sid	Msg
☑	41337	MALWARE-CNC Andr.Trojan.Sysch variant outbound connection
□	2841337	ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2020-03-04 1)

Optional comment

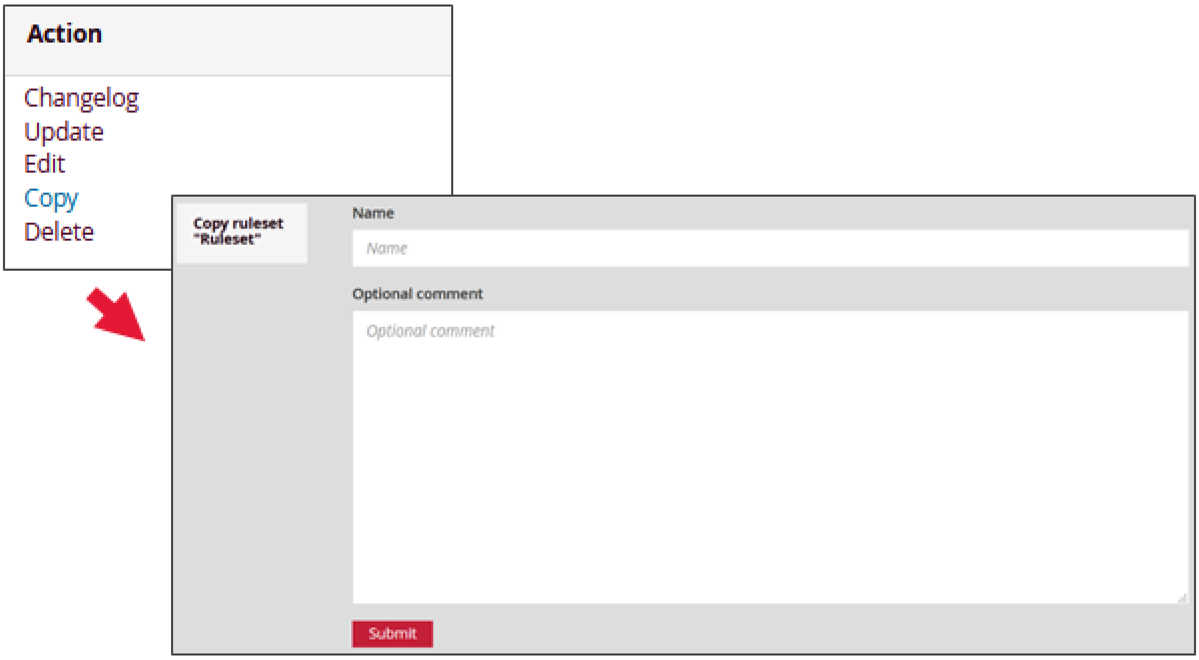
Optional comment

Add selected rules to disabled rules list

The administrator may decide to duplicate the Ruleset in order to assign it to another **GCAP** probe, for example, depending on the network flows that are in transit. The Ruleset is specific. It must be optimised according to the probe to which it will be assigned.

ACTION COPY RULESET:

This option is used to duplicate the Ruleset. The copy will take into account the sources associated with the Ruleset.



Action

Changelog
Update
Edit
Copy
Delete

Copy ruleset "Ruleset"

Name

Name

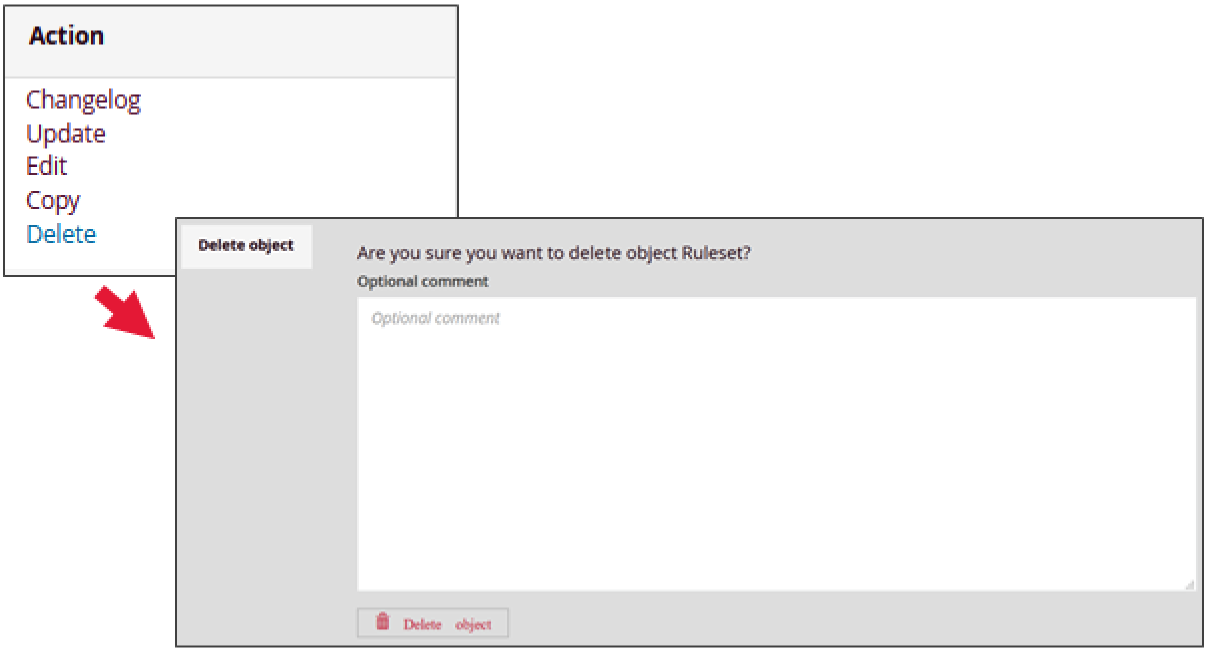
Optional comment

Optional comment

Submit

ACTION DELETE RULESET:

The deletion of the Ruleset is irreversible. However, it will not cause the deletion of the sources and signatures that were linked to the Ruleset.

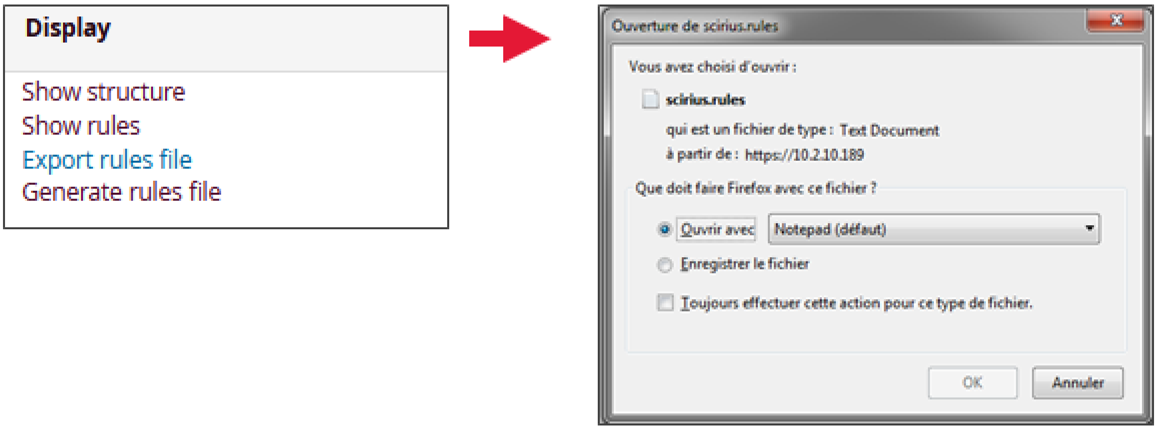


Are you sure you want to delete object Ruleset?

Optional comment

Optional comment

Other viewing options are available via the SIGFLOW interface. The **DISPLAY** section provides an overview of the categories (via **Show structure**) and rules (via **Show rules**). Moreover, thanks to this section, an export of the entire SIGFLOW configuration is possible, taking into account the Ruleset, sources, thresholds, and suppressions created.



Ouverture de scirius.rules

Vous avez choisi d'ouvrir :

scirius.rules

qui est un fichier de type : Text Document

à partir de : https://10.2.10.189

Que doit faire Firefox avec ce fichier ?

● Ouvrir avec Notepad (défaut)

○ Enregistrer le fichier

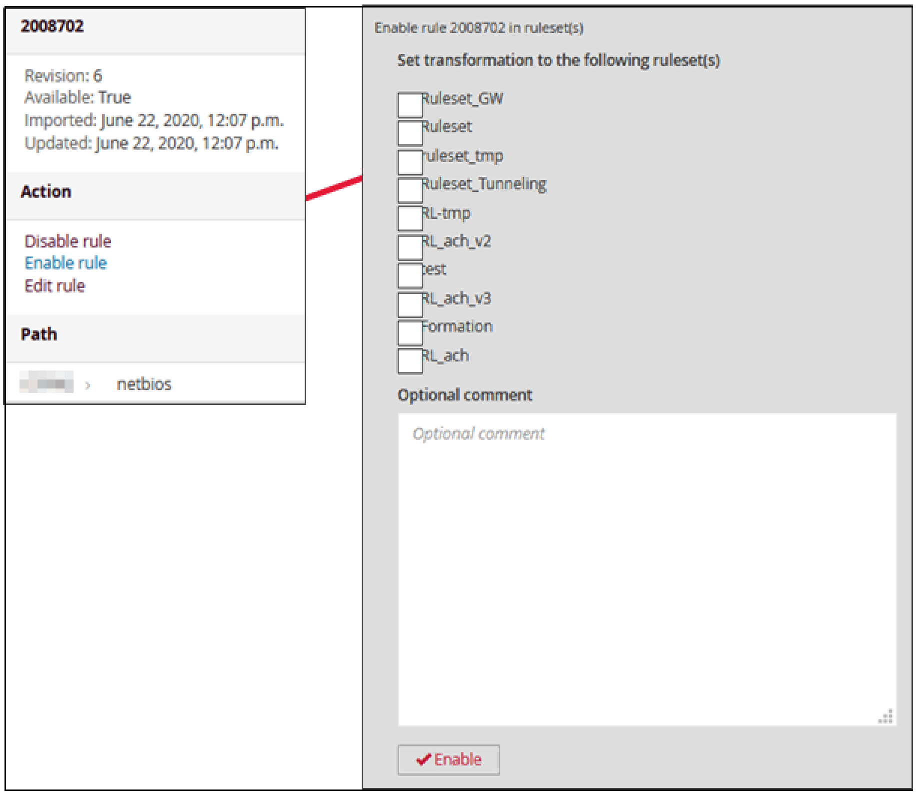
□ Toujours effectuer cette action pour ce type de fichier.

23.3 Changing signatures

Signatures and their categories are the common thread between a *source* and a *ruleset*. It is possible to directly modify the operation of a signature from the **GCenter** interface.

The signatures and their categories can be accessed from a *Ruleset* by clicking on the *View* button of the *Ruleset* and then the category.

Depending on the alerts arriving at the interface, it is possible to be quite specific about the type or even the number of notifications. The rule can be enabled or disabled within the Ruleset.



2008702

Revision: 6
Available: True
Imported: June 22, 2020, 12:07 p.m.
Updated: June 22, 2020, 12:07 p.m.

Action

Disable rule
Enable rule
Edit rule

Path

[redacted] › netbios

Enable rule 2008702 in ruleset(s)

Set transformation to the following ruleset(s)

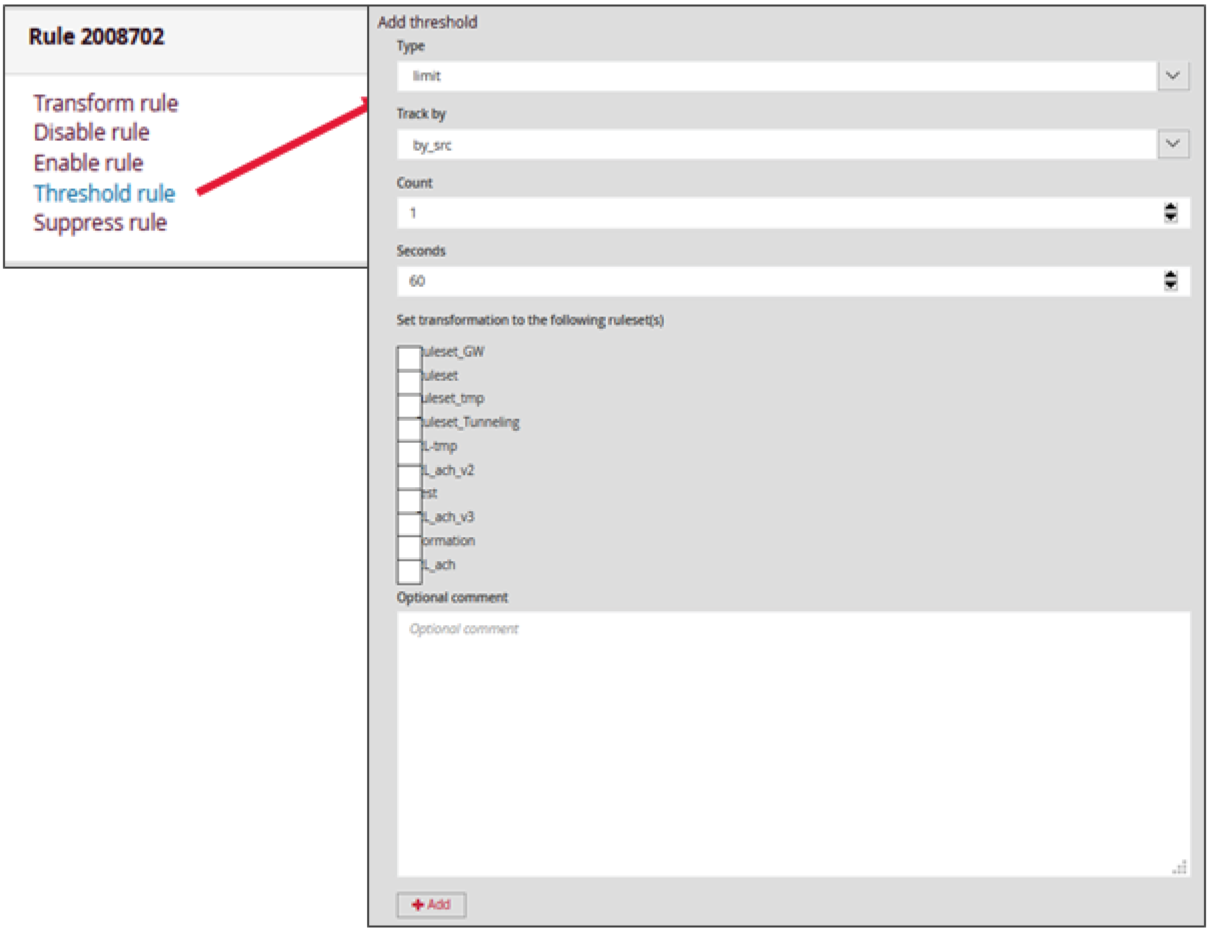
- □ Ruleset_GW
- □ Ruleset
- □ uleset_tmp
- □ Ruleset_Tunneling
- □ RL-tmp
- □ RL_ach_v2
- □ est
- □ RL_ach_v3
- □ ormation
- □ RL_ach

Optional comment

Optional comment

SR4

By clicking on the *"Edit Rule"* link it is possible to generate rules to limit or suppress certain alerts. There are Suppress Rules that remove an alert based on the source or destination IP address and Threshold Rules that limit the number of alerts to be displayed.



Add threshold

Type: limit

Track by: by_src

Count: 1

Seconds: 60

Set transformation to the following ruleset(s)

- □ uleset_GW
- □ uleset
- □ uleset_tmp
- □ uleset_Tunneling
- □ L-tmp
- □ L_ach_v2
- □ est
- □ L_ach_v3
- □ ormation
- □ L_ach

Optional comment: Optional comment

THRESHOLD:

This option is used to program a restriction of alerts above a set limit.

For a threshold, there are three types of rules:

Threshold: This type can be used to set a minimum limit for a rule before alerts are generated. A threshold setting of N indicates that the nth time the rule matches, an alert is triggered.

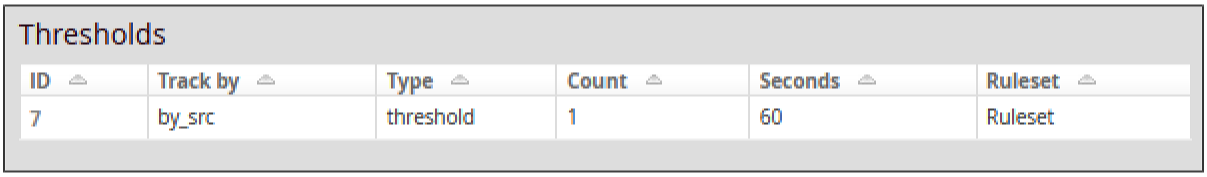
Limit: This type can be used to ensure that it does not overwhelm with alerts. If set to N, it will alert a maximum of N times.

Both: This type is a composite of the "threshold" and "limit" types. It applies both thresholding and limiting. This alert will only generate N alerts if, within X minutes.

Then, it is necessary to:

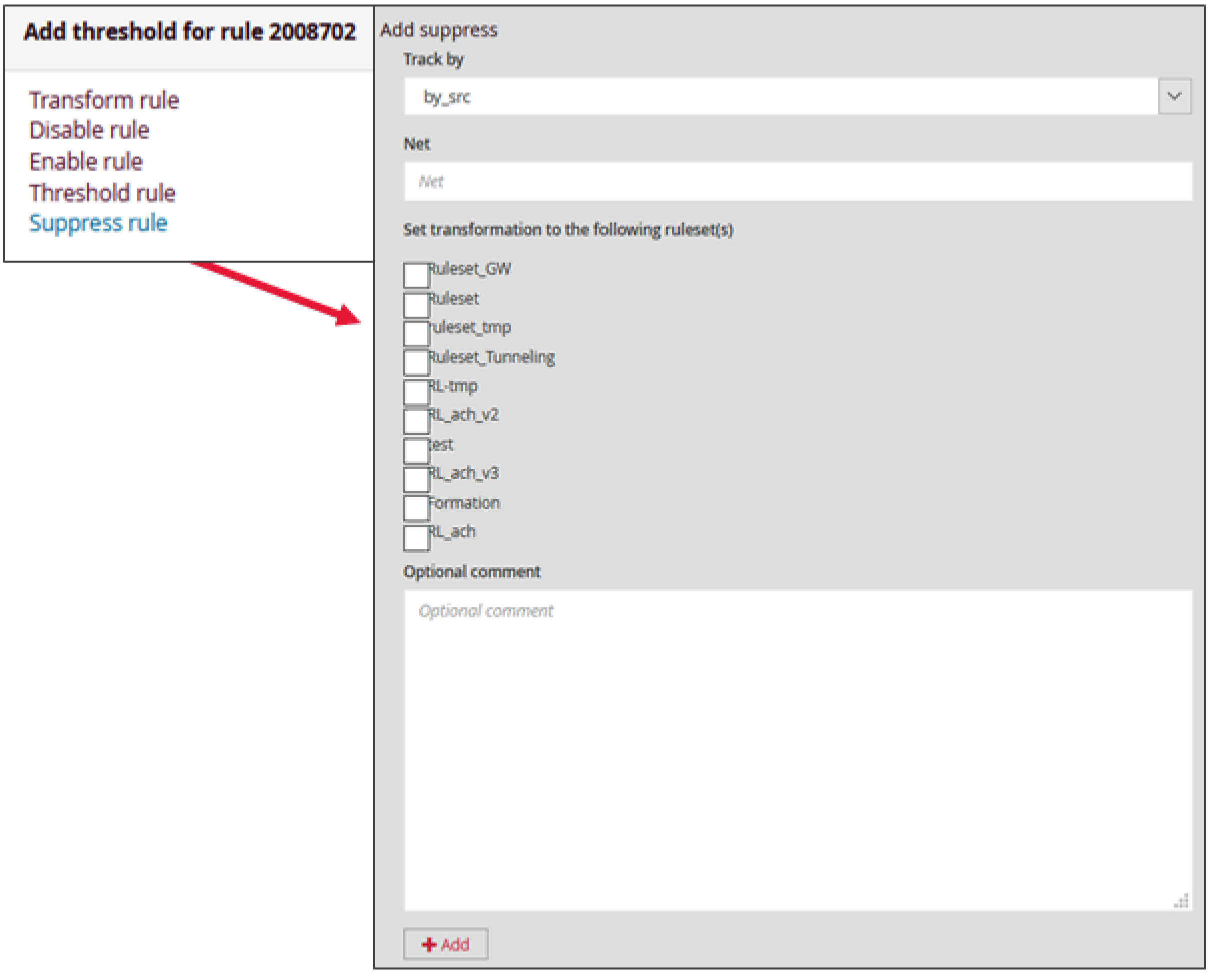
- Define whether the alert will be based on the source or destination IP
- Specify the maximum number of alerts generated for the given period
- Define the period in seconds to generate the alert

The created rules are available in the Ruleset page along with the format of the new rule.



Thresholds

ID	Track by	Type	Count	Seconds	Ruleset
7	by_src	threshold	1	60	Ruleset



Add threshold for rule 2008702

Add suppress

Track by: by_src

Net: Net

Set transformation to the following ruleset(s)

- □ Ruleset_GW
- □ Ruleset
- □ uleset_tmp
- □ Ruleset_Tunneling
- □ RL-tmp
- □ RL_ach_v2
- □ est
- □ RL_ach_v3
- □ ormation
- □ RL_ach

Optional comment: Optional comment

SUPPRESS:

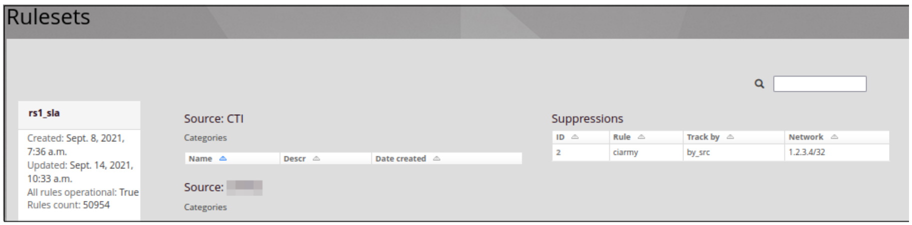
This option provides for the removal of an alert in relation to a given IP address or network.

Multiple IPs can be added separated by ' ,'.

After selecting Suppress Rules:

- Choose the Ruleset to be assigned
- Choose whether the alert's suppression will be based on the source or the destination.
- Define the IP relevant to this rule. (in CIDR format)

The rule is available on the Ruleset page in question:



Rulesets

rs1_sla

Created: Sept. 8, 2021, 7:36 a.m.
Updated: Sept. 14, 2021, 10:33 a.m.
All rules operational: True
Rules count: 50954

Source: CTI

Categories

Name	Descr	Date created

Source: [redacted]

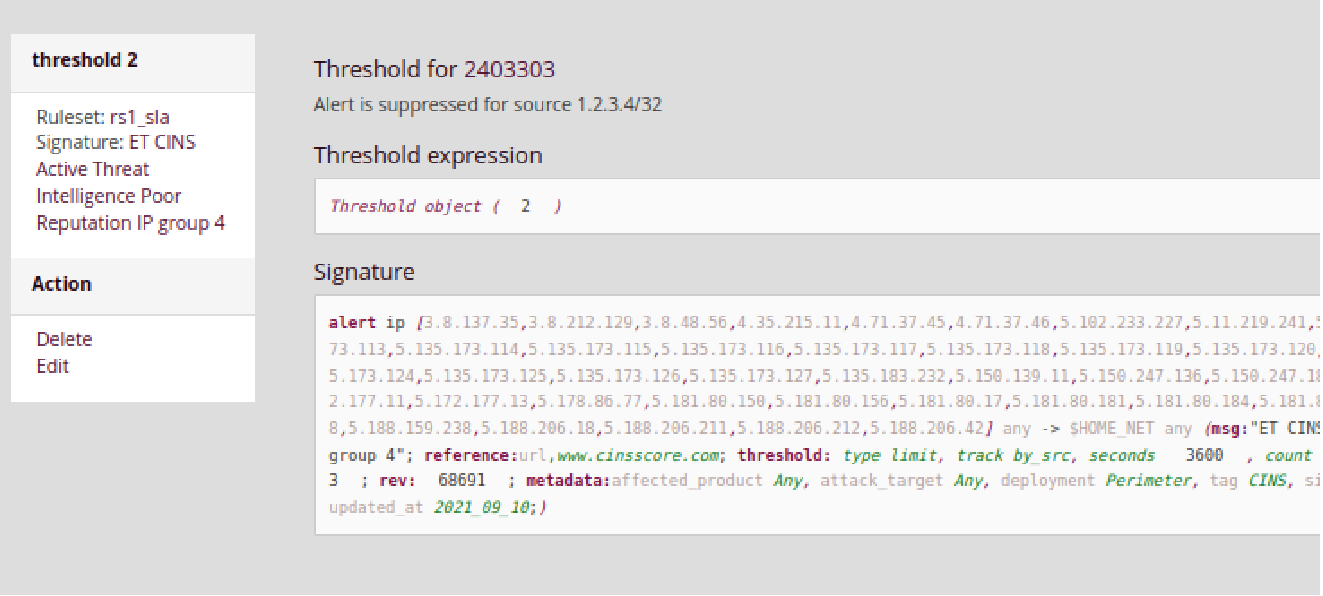
Categories

Suppressions

ID	Rule	Track by	Network
2	ciarmy	by_src	1.2.3.4/32

SHOW_SUPPRESS_RULE

By clicking on the *ID* of the *suppress rule* it can be edited or deleted.



threshold 2

Ruleset: rs1_sla
Signature: ET CINS Active Threat Intelligence Poor Reputation IP group 4

Action

Delete
Edit

Threshold for 2403303

Alert is suppressed for source 1.2.3.4/32

Threshold expression

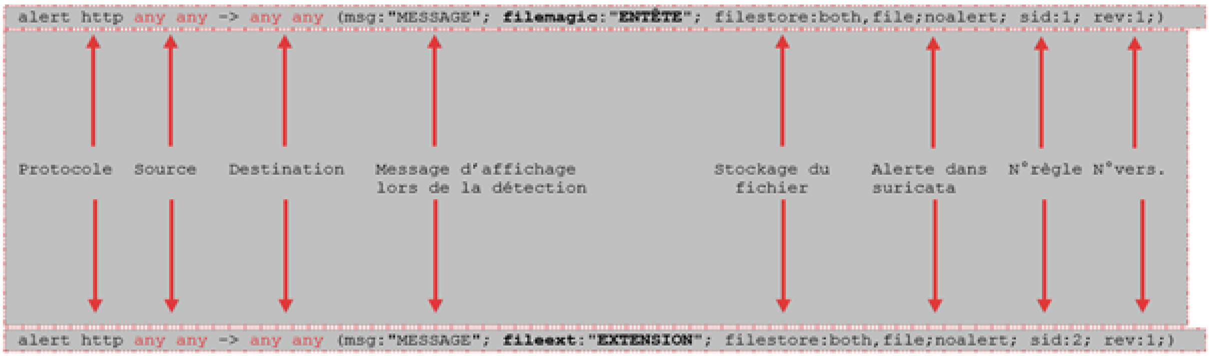
```
Threshold object (  2  )
```

Signature

```
alert ip [3.8.137.35,3.8.212.129,3.8.48.56,4.35.215.11,4.71.37.45,4.71.37.46,5.102.233.227,5.11.219.241,5
73.113,5.135.173.114,5.135.173.115,5.135.173.116,5.135.173.117,5.135.173.118,5.135.173.119,5.135.173.120,
5.173.124,5.135.173.125,5.135.173.126,5.135.173.127,5.135.183.232,5.150.139.11,5.150.247.136,5.150.247.1
2.177.11,5.172.177.13,5.178.86.77,5.181.80.150,5.181.80.156,5.181.80.17,5.181.80.181,5.181.80.184,5.181.
8,5.188.159.238,5.188.206.18,5.188.206.211,5.188.206.212,5.188.206.42] any -> $HOME_NET any (msg:"ET CIN
group 4"; reference:url,www.cinsscore.com; threshold: type limit, track by_src, seconds  3600  , count
3  ; rev:  68691  ; metadata:affected_product Any, attack_target Any, deployment Perimeter, tag CINS, si
updated_at 2021_09_10;)
```

23.3.1 Definition of signatures

All the signatures present in the sources contain references leading to blogs, CVEs, and websites... accessible from the interface. To better understand how a signature works, here is an example of a rule:



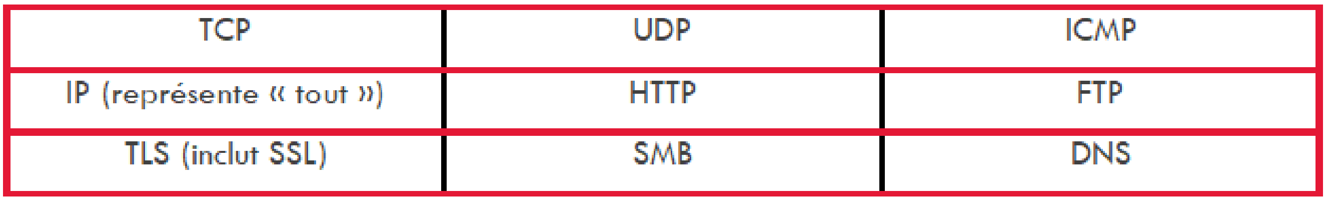
```
alert http any any -> any any (msg:"MESSAGE"; filemagic:"ENTÊTE"; filestore:both,file;noalert; sid:1; rev:1;)
```

```
alert http any any -> any any (msg:"MESSAGE"; fileext:"EXTENSION"; filestore:both,file;noalert; sid:2; rev:1;)
```

In most cases, a rule, a signature is composed of: an action, the header, and rule options. For example:

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

The following protocols can be the subject of a rule:

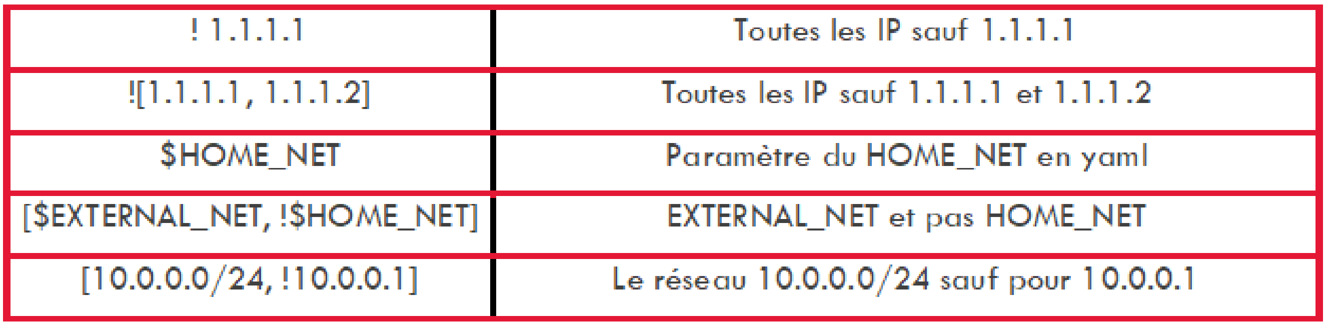


TCP	UDP	ICMP
IP (représente « tout »)	HTTP	FTP
TLS (inclut SSL)	SMB	DNS

In the signature, you can assign IP addresses, both IPv4 and IPv6, combined as well as separate. Both sources and destinations of the signature are affected.

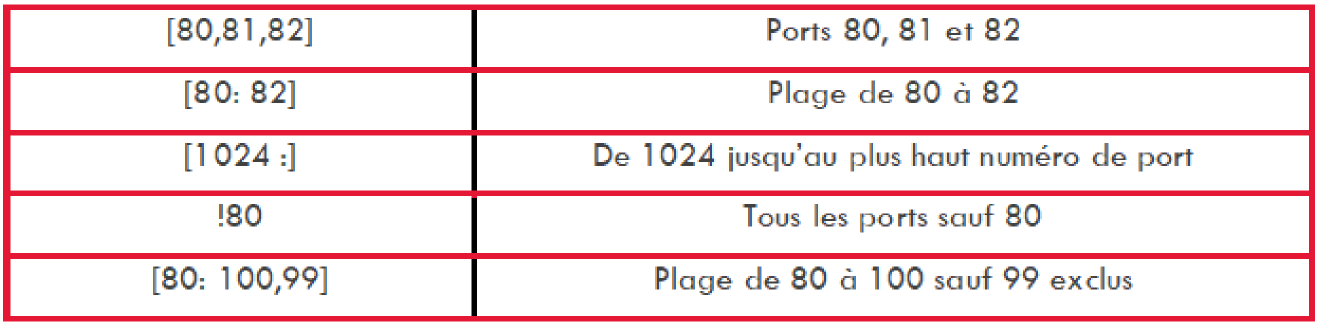
Furthermore, it is possible to define variables such as $HOME_NET or $EXTERNAL_NET to which the *IPs are to be defined* . These variables are used to increase the accuracy of the alerts provided by the signatures.

The following syntax can be used to specify the addresses:



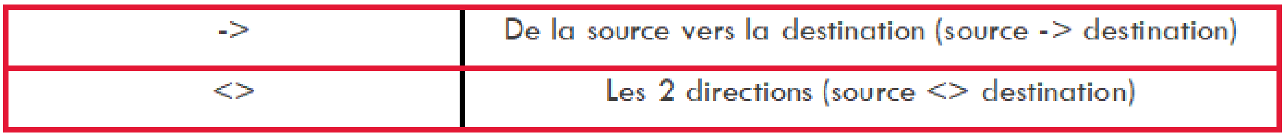
! 1.1.1.1	Toutes les IP sauf 1.1.1.1
![1.1.1.1, 1.1.1.2]	Toutes les IP sauf 1.1.1.1 et 1.1.1.2
$HOME_NET	Paramètre du HOME_NET en yaml
[$EXTERNAL_NET, !$HOME_NET]	EXTERNAL_NET et pas HOME_NET
[10.0.0.0/24, !10.0.0.1]	Le réseau 10.0.0.0/24 sauf pour 10.0.0.1

Similarly, the following syntax can be used to specify ports:



[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

Two directions can be specified to indicate the direction of the flow:



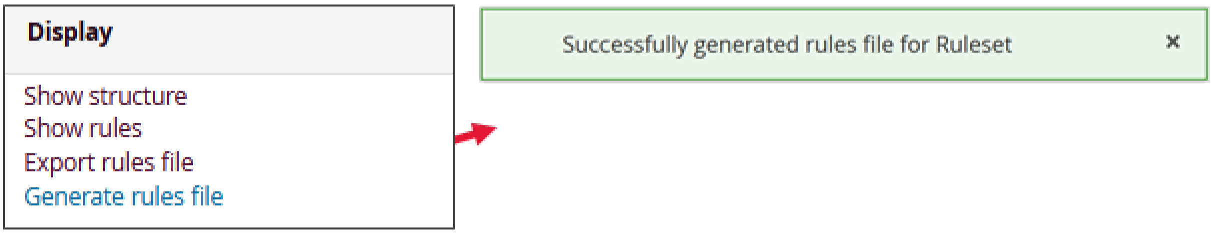
->	De la source vers la destination (source -> destination)
<>	Les 2 directions (source <> destination)

23.4 Generating rulesets

Important:

As long as the rulesets have not been generated after modifications, no configuration will be deployed.

Once the configuration of the sources, rulesets, and any modifications are completed, it is necessary to generate the configuration for the probes and implement it. This is accomplished by using the "**Generate Ruleset**" action, which will freeze the status of the Ruleset and take into account all modifications.



Successfully generated rules file for Ruleset

23.5 Secret Local Rule

It is also possible to define certain rules locally on a GCAP probe that will intentionally not appear in the **GCENTER** interface.

This may occur in the following instances:

- Making signatures confidential without the GCENTER operators being able to see them, according to a 'need to know' concept.
- Modify the local signatures of probes in complex cases.
- If the GCENTER is assigned to a third party and the third party cannot handle markers or signatures of a certain level.

This is discussed in more detail in the [**GCAP** documentation] (https://docs.gatewatcher.com/gcap.html) in the section `Detection Engine > 7. Adding secret rules locally*".

Chapter 24

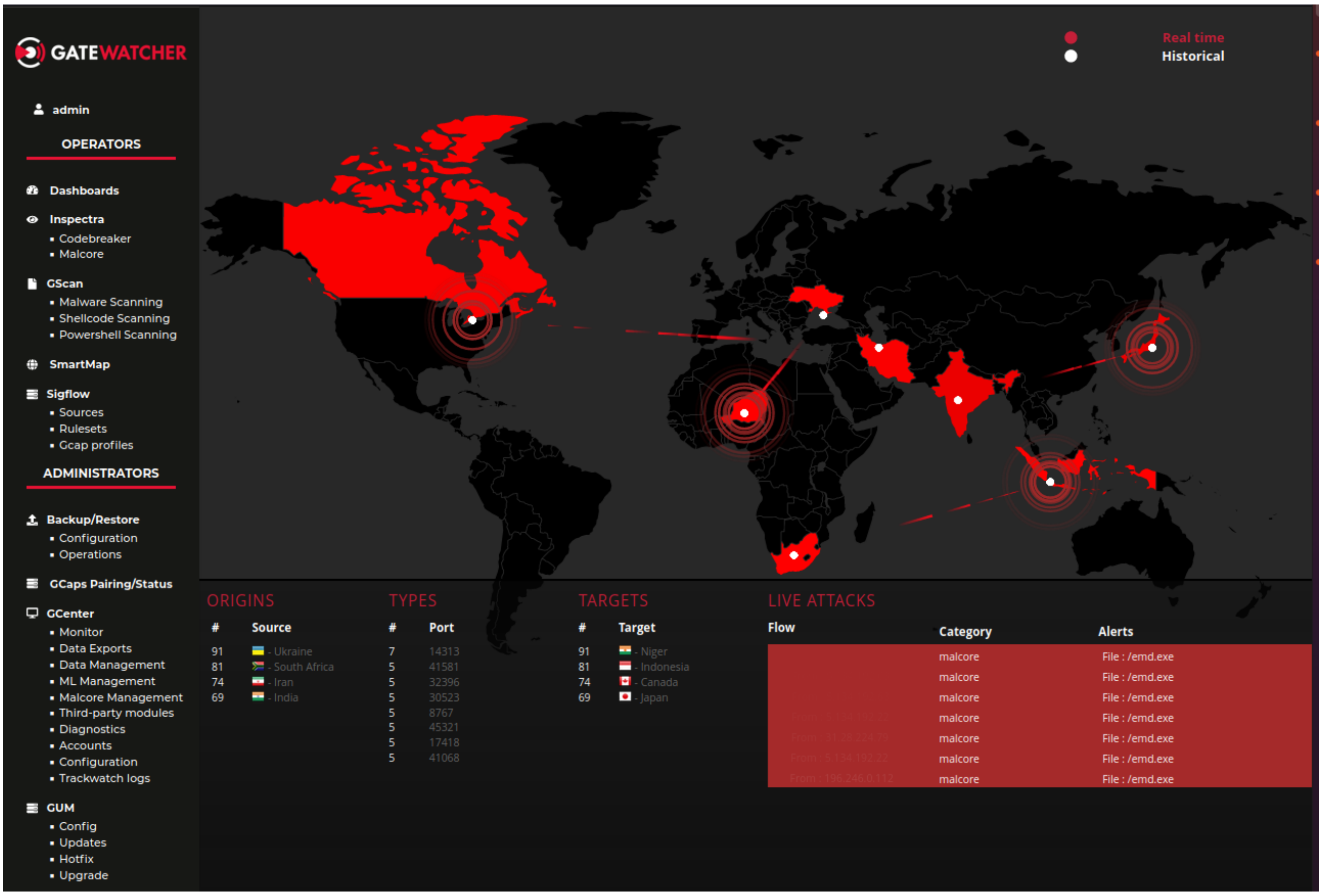
Detection

24.1 SmartMap

Rôle Opérateur

Menu: Operators > SmartMap

The **SmartMap** enables real-time visualisation of attacks and traffic. This allows for intuitive and visual detection of unusual or particularly heavy traffic.



ORIGINS

#	Source
91	- Ukraine
81	- South Africa
74	- Iran
69	- India

TYPES

#	Port
7	14313
5	41581
5	32396
5	30523
5	8767
5	45321
5	17418
5	41068

TARGETS

#	Target
91	- Niger
81	- Indonesia
74	- Canada
69	- Japan

LIVE ATTACKS

Flow	Category	Alerts
	malcore	File : /emd.exe
	malcore	File : /emd.exe
[illegible]	malcore	File : /emd.exe
From : 5.134.192.22	malcore	File : /emd.exe
From : 31.28.224.79	malcore	File : /emd.exe
From : 5.134.192.22	malcore	File : /emd.exe
From : 196.246.0.112	malcore	File : /emd.exe

In order to display the information on the map, the **SmartMap** requires geolocation data on the alerts. The latter will therefore need to be activated from *the configuration section* by an administrator.

24.2 Kibana Dashboard

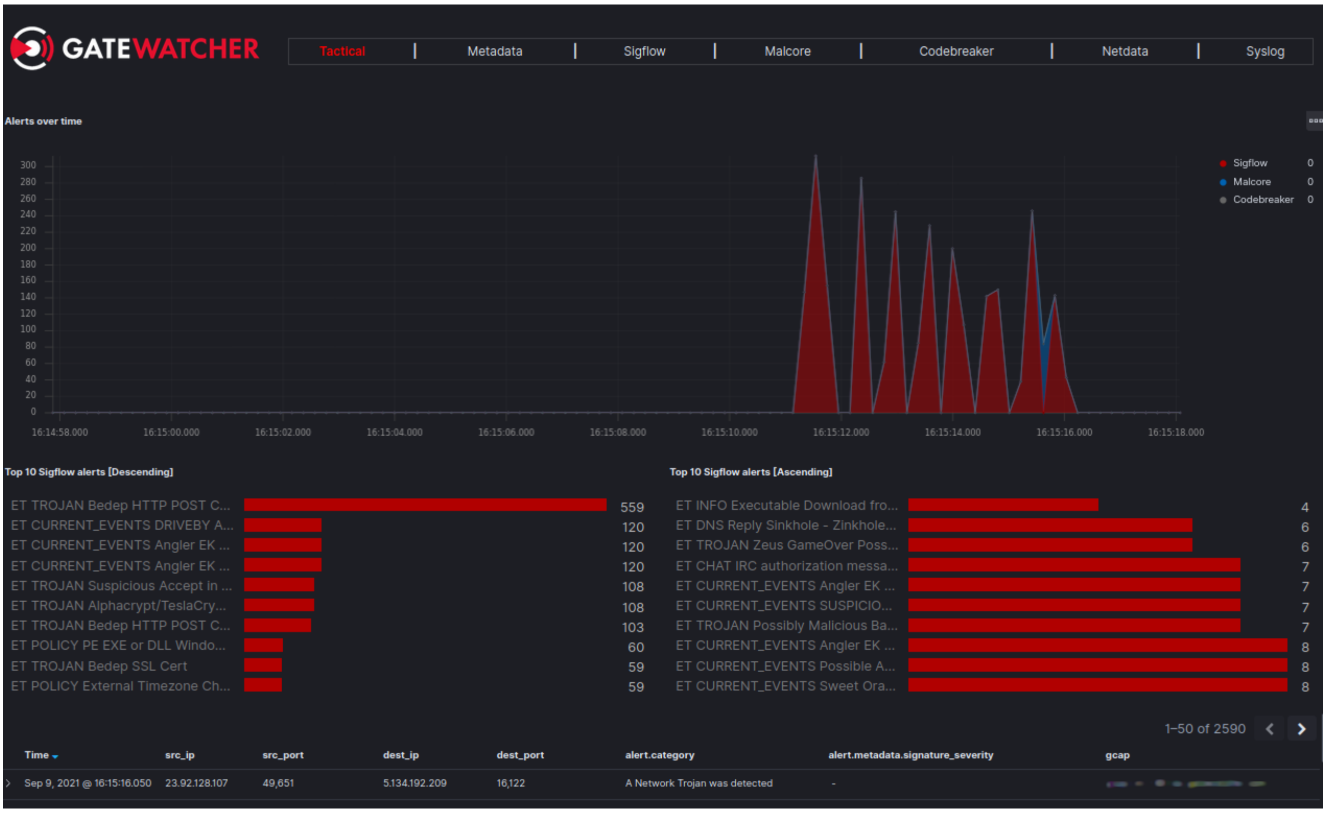
Rôle Opérateur

Menu: Operators > Dashboards

All the information analysed by the Sigflow module is stored in order for the operators to be able to carry out an analysis in the most efficient way possible.

Thus, various dashboards are made available by default.

The information from the **Sigflow** module can be found in the **Tactical** *dashboard. This provides a global view of the threats, including those identified by **Sigflow**.



Top 10 Sigflow alerts [Descending]

ET TROJAN Bedep HTTP POST C...	559
ET CURRENT_EVENTS DRIVEBY A...	120
ET CURRENT_EVENTS Angler EK ...	120
ET CURRENT_EVENTS Angler EK ...	120
ET TROJAN Suspicious Accept in ...	108
ET TROJAN Alphacrypt/TeslaCry...	108
ET TROJAN Bedep HTTP POST C...	103
ET POLICY PE EXE or DLL Windo...	60
ET TROJAN Bedep SSL Cert	59
ET POLICY External Timezone Ch...	59

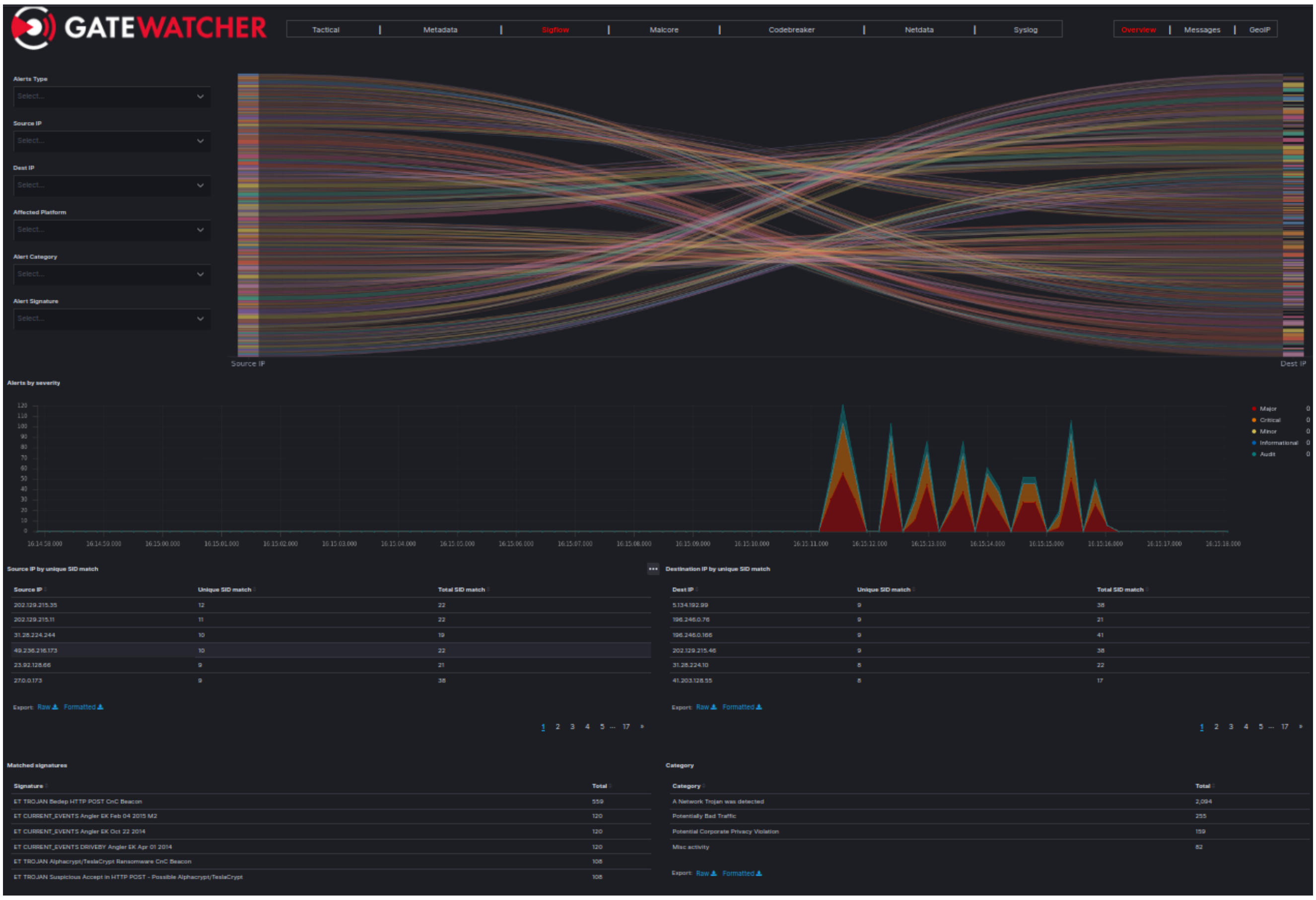
Top 10 Sigflow alerts [Ascending]

ET INFO Executable Download fro...	4
ET DNS Reply Sinkhole - Zinkhole...	6
ET TROJAN Zeus GameOver Poss...	6
ET CHAT IRC authorization messa...	7
ET CURRENT_EVENTS Angler EK ...	7
ET CURRENT_EVENTS SUSPICIO...	7
ET TROJAN Possibly Malicious Ba...	7
ET CURRENT_EVENTS Angler EK ...	8
ET CURRENT_EVENTS Possible A...	8
ET CURRENT_EVENTS Sweet Ora...	8

1–50 of 2590

Time	src_ip	src_port	dest_ip	dest_port	alert.category	alert.metadata.signature_severity	gcap
Sep 9, 2021 @ 16:15:16.050	23.92.128.107	49,651	5.134.192.209	16,122	A Network Trojan was detected	-	[redacted]

More specific data for this module can also be found in the **Sigflow** *dashboard.



Source IP by unique SID match

Source IP	Unique SID match	Total SID match
202.129.215.35	12	22
202.129.215.11	11	22
31.28.224.244	10	19
49.236.216.173	10	22
23.92.128.66	9	21
27.0.0.173	9	38

Export: Raw Formatted

1 2 3 4 5 ... 17 »

Destination IP by unique SID match

Dest IP	Unique SID match	Total SID match
5.134.192.99	9	38
196.246.0.76	9	21
196.246.0.166	9	41
202.129.215.46	9	38
31.28.224.10	8	22
41.203.128.55	8	17

Export: Raw Formatted

1 2 3 4 5 ... 17 »

Matched signatures

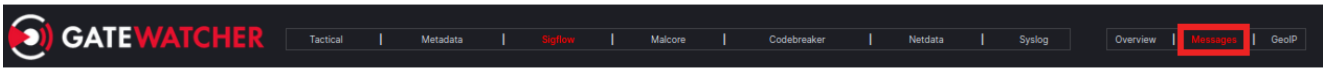
Signature	Total
ET TROJAN Bedep HTTP POST CnC Beacon	559
ET CURRENT_EVENTS Angler EK Feb 04 2015 M2	120
ET CURRENT_EVENTS Angler EK Oct 22 2014	120
ET CURRENT_EVENTS DRIVEBY Angler EK Apr 01 2014	120
ET TROJAN Alphacrypt/TeslaCrypt Ransomware CnC Beacon	108
ET TROJAN Suspicious Accept in HTTP POST - Possible Alphacrypt/TeslaCrypt	108

Category

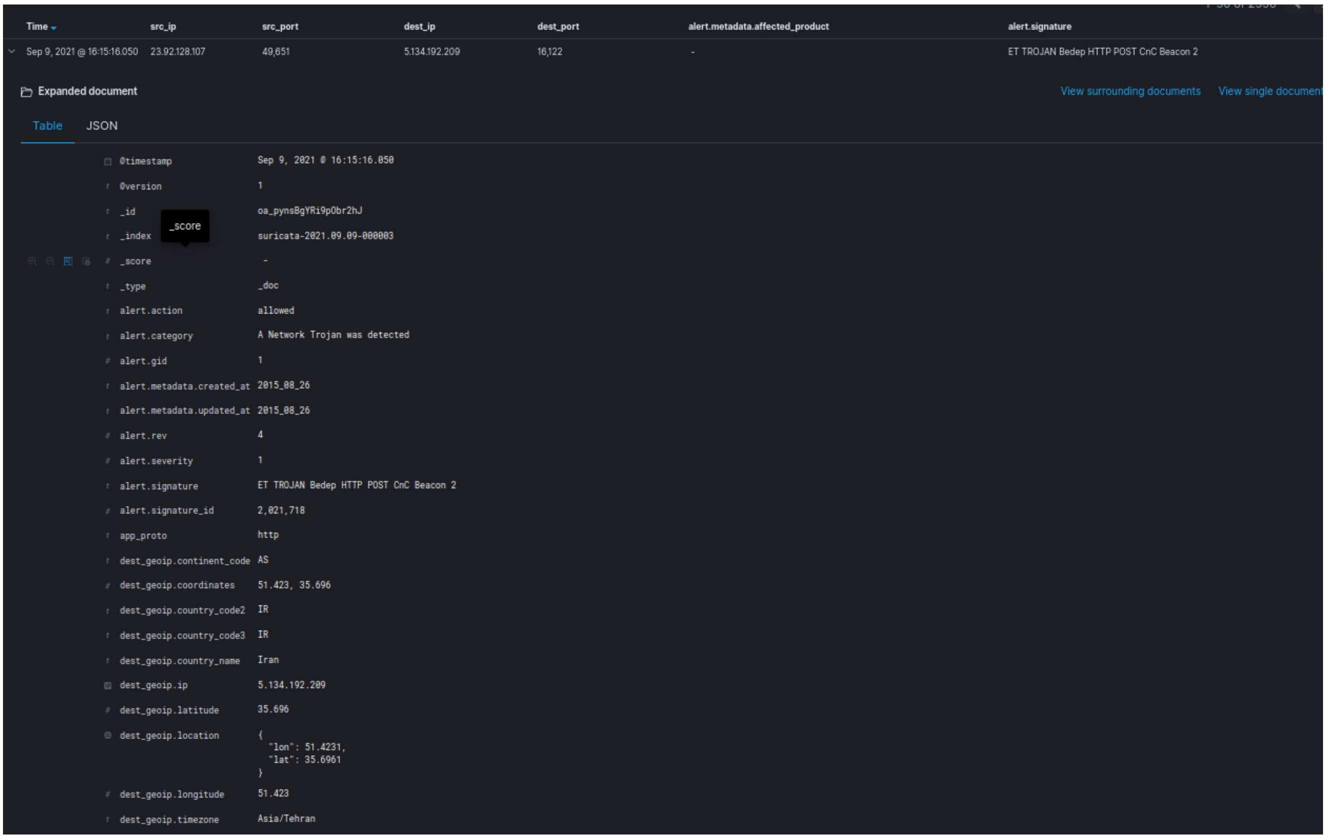
Category	Total
A Network Trojan was detected	2,094
Potentially Bad Traffic	255
Potential Corporate Privacy Violation	159
Misc activity	82

Export: Raw Formatted

As always, it is possible to obtain the full details of the alerts by switching to the **Messages** view



The fields present are those detailed below in the section *Generated events*



Time	src_ip	src_port	dest_ip	dest_port	alert.metadata.affected_product	alert.signature
Sep 9, 2021 @ 16:15:16.050	23.92.128.107	49,651	5.134.192.209	16,122	-	ET TROJAN Bedep HTTP POST CnC Beacon 2

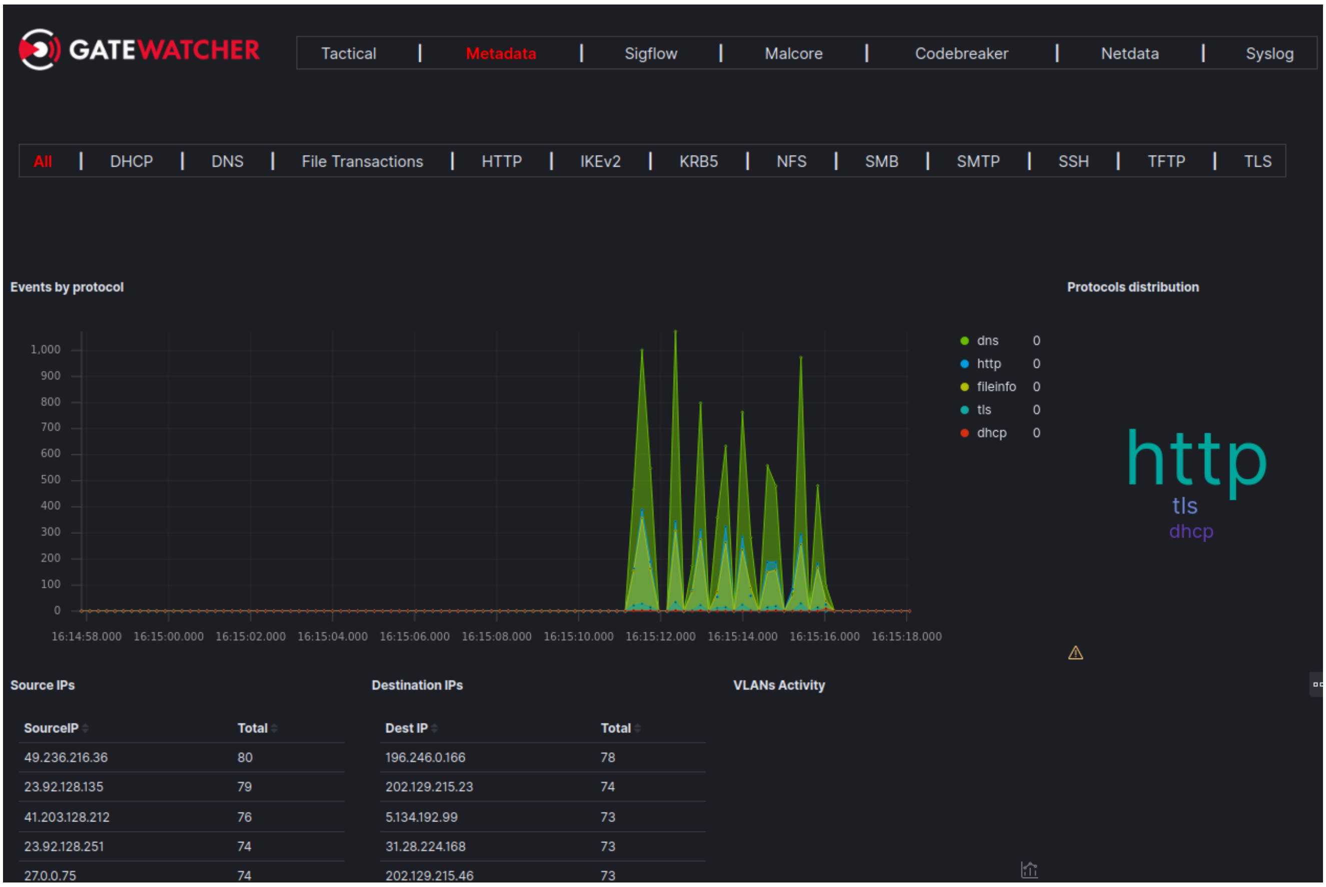
Expanded document

@timestamp	Sep 9, 2021 @ 16:15:16.050
@version	1
_id	oa_pynsBgYRi9pObr2hJ
_index	suricata-2021.09.09-000003
_score	-
_type	_doc
alert.action	allowed
alert.category	A Network Trojan was detected
alert.gid	1
alert.metadata.created_at	2015_08_26
alert.metadata.updated_at	2015_08_26
alert.rev	4
alert.severity	1
alert.signature	ET TROJAN Bedep HTTP POST CnC Beacon 2
alert.signature_id	2,021,718
app_proto	http
dest_geoip.continent_code	AS
dest_geoip.coordinates	51.423, 35.696
dest_geoip.country_code2	IR
dest_geoip.country_code3	IR
dest_geoip.country_name	Iran
dest_geoip.ip	5.134.192.209
dest_geoip.latitude	35.696

dest_geoip.location	{
	"lon": 51.4231,
	"lat": 35.6961
	}

dest_geoip.longitude	51.423
dest_geoip.timezone	Asia/Tehran

Finally, this module also enriches the observed traffic with the metadata that were analysed according to the configuration made on the ***GCAP profile***



Source IPs

SourceIP	Total
49.236.216.36	80
23.92.128.135	79
41.203.128.212	76
23.92.128.251	74
27.0.0.75	74

Destination IPs

Dest IP	Total
196.246.0.166	78
202.129.215.23	74
5.134.192.99	73
31.28.224.168	73
202.129.215.46	73

Chapter 25

Generated events

For suricata, and therefore Sigflow, the fields created depend on the observed flow.

25.1 Document type "alert"

List of fields present in all alerts with event_type == alert:

- @timestamp
- @version
- alert.action
- alert.category
- alert.gid
- alert.rev
- alert.severity
- alert.signature
- alert.signature_id
- dest_ip
- event_type
- flow.bytes_toclient
- flow.bytes_toserver
- flow.pkts_toclient
- flow.pkts_toserver
- flow.start
- flow_id
- gcap
- GCenter
- host
- packet
- packet_info.linktype
- payload_printable
- proto
- severity
- src_ip
- stream
- timestamp_analyzed
- timestamp_detected
- type
- uuid

List of protocols compatible with parsing (app_proto field):

- dcerpc
- dhcp

- dnp3
- dns
- ftp
- http
- ikev2
- krb5
- modbus
- nfs
- ntp
- smb,
- smtp
- ssh
- tftp
- tls

If a protocol changes midstream, 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

Summary table of fields that do not depend on the protocols:

List of metadata used in the source alerts (alert.metadata object in ES):

- alert.metadata.affected_product
- alert.metadata.attack_target
- alert.metadata.created_at
- alert.metadata.deployment
- alert.metadata.former_category
- alert.metadata.impact_flag
- alert.metadata.malware_family
- alert.metadata.performance_impact
- alert.metadata.ruleset
- alert.metadata.service
- alert.metadata.signature_severity
- alert.metadata.tag
- alert.metadata.updated_at

Here is an example of an alert using the metadata affected_product, attack_target, created_at, deployment, signature_severity, tag and updated_at:

```
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (
msg:"ET EXPLOIT MS-SQL SQL Injection closing string plus line comment";
flow: to_server,established;
content:"'|00|";
content:"-|00|-|00|";
reference:url,doc.emergingthreats.net/bin/view/Main/2000488;
classtype:attempted-user;
sid:2000488;
rev:7;
metadata:affected_product Web_Server_Applications, attack_target Web_Server, created_at 2010_
↪07_30, deployment Datacenter, signature_severity Major, tag SQL_Injection, updated_at 2016_
↪07_01;
)
```

25.2 Document type "fileinfo"

List of fields present in all alerts with event_type == fileinfo:

- @timestamp
- @version
- app_proto
- dest_ip
- dest_port
- event_type
- fileinfo.filename
- fileinfo.gaps
- fileinfo.size
- fileinfo.state
- fileinfo.stored
- fileinfo.tx_id
- flow_id
- gcap
- GCenter
- host
- proto
- src_ip
- src_port
- timestamp_analyzed
- timestamp_detected
- type
- uuid

Summary table of fields that do not depend on the protocols:

25.3 Metadata document

List of fields present in all alerts with event_type != ["alert", "fileinfo", "stats"]:

- @timestamp
- @version
- dest_ip
- event_type
- flow_id
- gcap
- GCenter
- host
- proto
- src_ip
- timestamp_analyzed
- timestamp_detected
- type
- uuid

List of protocols compatible with logging (champ event_type):

- **dhcp:**
  - dhcp.assigned_ip
  - dhcp.client_ip
  - dhcp.client_mac
  - dhcp.dhcp_type
  - dhcp.dns_servers
  - dhcp.hostname

  - dhcp.id
  - dhcp.lease_time
  - dhcp.next_server_ip
  - dhcp.params
  - dhcp.rebinding_time
  - dhcp.relay_ip
  - dhcp.renewal_time
  - dhcp.requested_ip
  - dhcp.routers
  - dhcp.subnet_mask
  - dhcp.type
- **dnp3**
- **dns:**
  - body.proba_dga
  - body.severity
  - dga_probability
  - dns.aa
  - dns.answers.rdata
  - dns.answers.rrname
  - dns.answers.rrtype
  - dns.answers.ttl
  - dns.authorities.rrname
  - dns.authorities.rrtype
  - dns.authorities.ttl
  - dns.flags
  - dns.grouped.A
  - dns.grouped.AAAA
  - dns.grouped.CNAME
  - dns.id
  - dns.qr
  - dns.ra
  - dns.rcode
  - dns.rd
  - dns.rrname
  - dns.rrtype
  - dns.tx_id
  - dns.type
  - dns.version
  - headers.content-length
  - headers.content-type
  - tags
- **ftp**
- **http:**
  - http.accept
  - http.accept-charset
  - http.accept-datetime
  - http.accept_encoding
  - http.accept_language
  - http.accept-range
  - http.age
  - http.allow
  - http.authorization
  - http.cache_control
  - http.connection
  - http.content_encoding
  - http.content-language
  - http.content-length
  - http.content-location

  - http.content-md5
  - http.content-range
  - http.content_type
  - http.content-type
  - http.cookie
  - http.date
  - http.dnt
  - http.etags
  - http.from
  - http.hostname
  - http.http_content_type
  - http.http_method
  - http.http_port
  - http.http_refer
  - http.http_user_agent
  - http.last-modified
  - http.length
  - http.link
  - http.location
  - http.max-forwards
  - http.origin
  - http.pragma
  - http.proxy-authenticate
  - http.proxy-authorization
  - http.range
  - http.redirect
  - http.referrer
  - http.refresh
  - http.retry-after
  - http.server
  - http.set-cookie
  - http.status
  - http.te
  - http.trailer
  - http.transfer-encoding
  - http.upgrade
  - http.url
  - http.vary
  - http.via
  - http.warning
  - http.www-authenticate
  - http.x-authenticated-user
  - http.x-flash-version
  - http.x-forwarded-proto
  - http.x-requested-with
- **ikev2:**
  - ikev2.alg_auth
  - ikev2.alg_dh
  - ikev2.alg_enc
  - ikev2.alg_esn
  - ikev2.alg_prf
  - ikev2.errors
  - ikev2.exchange_type
  - ikev2.init_spi
  - ikev2.message_id
  - ikev2.notify
  - ikev2.payload
  - ikev2.resp_spi

  - ikev2.role
  - ikev2.version_major
  - ikev2.version_minor
- **krb5:**
  - krb5.cname
  - krb5.encryption
  - krb5.error_code
  - krb5.failed_request
  - krb5.msg_type
  - krb5.realm
  - krb5.sname
  - krb5.weak_encryption
- **netflow:**
  - icmp_code
  - icmp_type
  - metadata.flowbits
  - netflow.age
  - netflow.bytes
  - netflow.end
  - netflow.max_ttl
  - netflow.min_ttl
  - netflow.pkts
  - netflow.start
  - parent_id
  - tcp.ack
  - tcp.cwr
  - tcp.ecn
  - tcp.fin
  - tcp.psh
  - tcp.rst
  - tcp.syn
  - tcp.tcp_flags
- **nfs:**
  - nfs.file_tx
  - nfs.filename
  - nfs.hhash
  - nfs.id
  - nfs.procedure
  - nfs.rename.from
  - nfs.rename.to
  - nfs.status
  - nfs.type
  - nfs.version
  - rpc.auth_type
  - rpc.creds.gid
  - rpc.creds.machine_name
  - rpc.creds.uid
  - rpc.status
  - rpc.xid
- **smb:**
  - smb.access
  - smb.accessed
  - smb.changed
  - smb.client_dialects
  - smb.client_guid
  - smb.command
  - smb.created
  - smb.dcerpc.call_id

  - smb.dcerpc.interfaces.ack_reason
  - smb.dcerpc.interfaces.ack_result
  - smb.dcerpc.interfaces.uuid
  - smb.dcerpc.interfaces.version
  - smb.dcerpc.opnum
  - smb.dcerpc.req.frag_cnt
  - smb.dcerpc.req.stub_data_size
  - smb.dcerpc.request
  - smb.dcerpc.res.frag_cnt
  - smb.dcerpc.res.stub_data_size
  - smb.dcerpc.response
  - smb.dialect
  - smb.directory
  - smb.disposition
  - smb.filename
  - smb.fuid
  - smb.function
  - smb.id
  - smb.modified
  - smb.named_pipe
  - smb.ntlmssp.domain
  - smb.ntlmssp.host
  - smb.ntlmssp.user
  - smb.request.native_lm
  - smb.request.native_os
  - smb.response.native_lm
  - smb.response.native_os
  - smb.server_guid
  - smb.service.request
  - smb.service.response
  - smb.session_id
  - smb.share
  - smb.share_type
  - smb.size
  - smb.status
  - smb.status_code
  - smb.tree_id
- **smtp:**
  - email.attachment
  - email.body_md5
  - email.from
  - email.status
  - email.subject
  - email.subject_md5
  - email.to
  - smtp.helo
  - smtp.mail_from
  - smtp.rcpt_to
- **ssh:**
  - ssh.client.proto_version
  - ssh.client.software_version
  - ssh.server.proto_version
  - ssh.server.software_version
- **tftp:**
  - tftp.file
  - tftp.mode
  - tftp.packet
- **tls:**

- tls.chain
- tls.fingerprint
- tls.issuerdn
- tls.notafter
- tls.notbefore
- tls.sni
- tls.subject
- tls.version

Summary table of fields that do not depend on the protocols:

Chapter 26

Introduction to the DGA Algorithm

The **Gcenter** embeds an engine capable of detecting domain names generated by DGAs (*Domain Generation Algorithm*). The presence of DGA-generated domain name resolution 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. These domain names contain different properties than legitimate domain names. Conventional detection approaches, such as blacklists, are not relevant in the case of continuously renewed domains. Simple entropy calculations result in a large number of false positives.

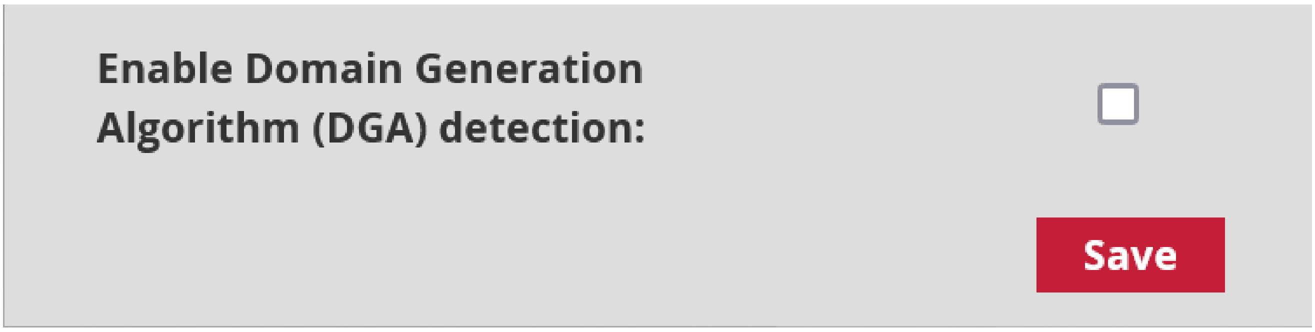
Chapter 27

Activation

Rôle Administrateur

Menu: Administrators > GCENTER > ML Management > DGA Detection Management > Settings

This feature is disabled by default. It can be enabled on the Machine Learning dashboard.



Enable Domain Generation Algorithm (DGA) detection: ☐

Once activated, the domain names present in the 'dns' events captured by the GCAP probes are analysed by the machine learning engine. The machine learning engine calculates a probability for each such event indicating whether the domain name was generated by a DGA. The engine uses a pre-trained model, whose architecture is based on deep neural network type Long Short Term Memory (LSTM) networks.

The engine only uses domain names. No additional contextual information such as NXDomains for example is involved.

Chapter 28

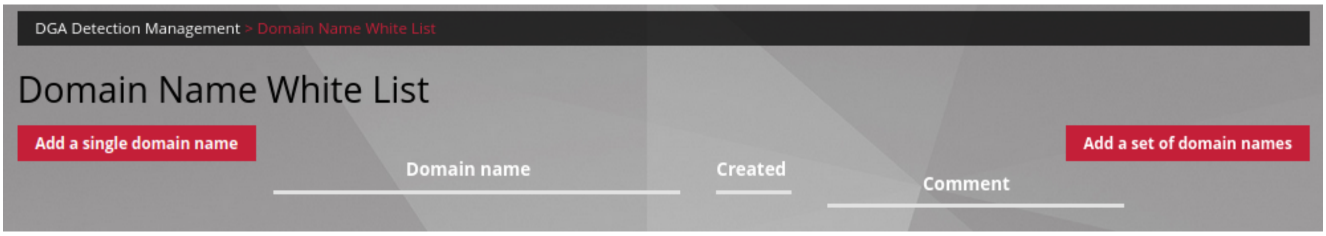
Exception list

Rôle Administrateur

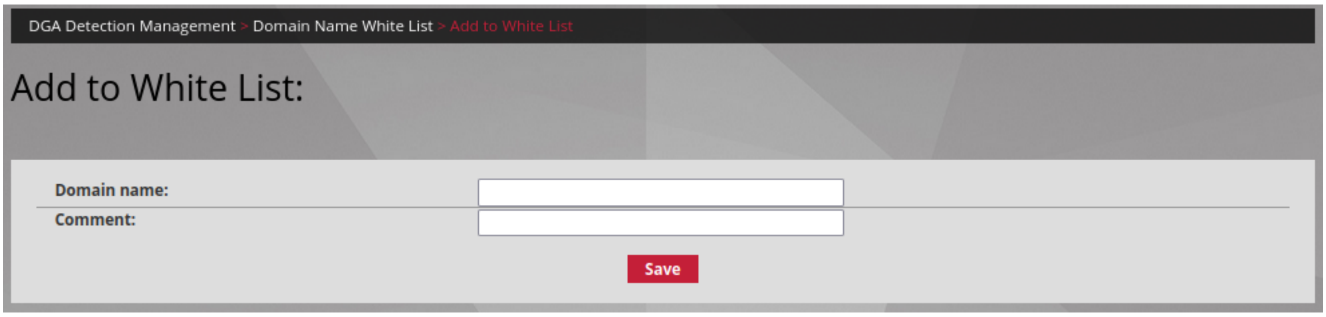
Menu: Administrators > GCENTER > ML Management > DGA Detection Management > White List / Black List

Exception lists can be set up to force the engine to declare domain names as healthy (White List). This enables eliminating alerts related to recurring false positives.

Conversely, a black list enables an alert to be raised for a domain that would not otherwise have been detected (false negative).

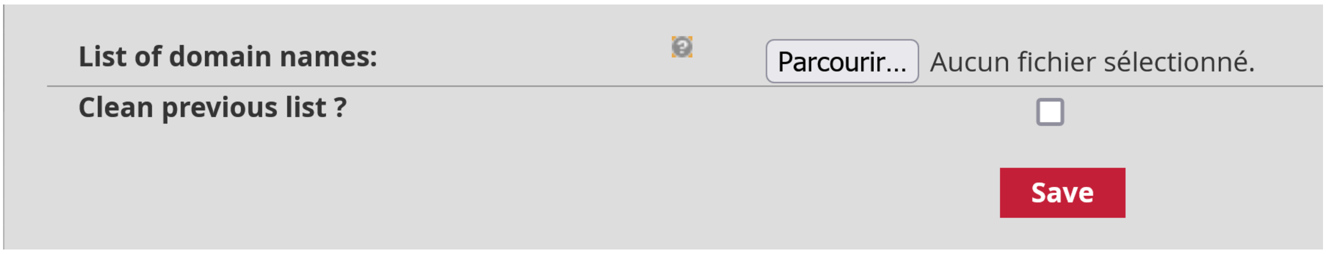

DGA Detection Management > Domain Name White List
Domain Name White List
Add a single domain name
Add a set of domain names
Domain name
Created
Comment

From **Add a single domain name**, it is possible to include a domain in the Machine Learning whitelist via the **Domain name** field. A remark can follow the added domain for more details in the **Comment** field.


DGA Detection Management > Domain Name White List > Add to White List
Add to White List:
Domain name:
Comment:
Save

The changes are recorded by clicking on the **Save** button.

From the **Add a set of domain names**, the administrator updates the Machine Learning whitelist via the **List of domain names** field by selecting a **CSV** file containing the domains. It is necessary to use ';' to separate the various elements of the list.



List of domain names: Aucun fichier sélectionné.

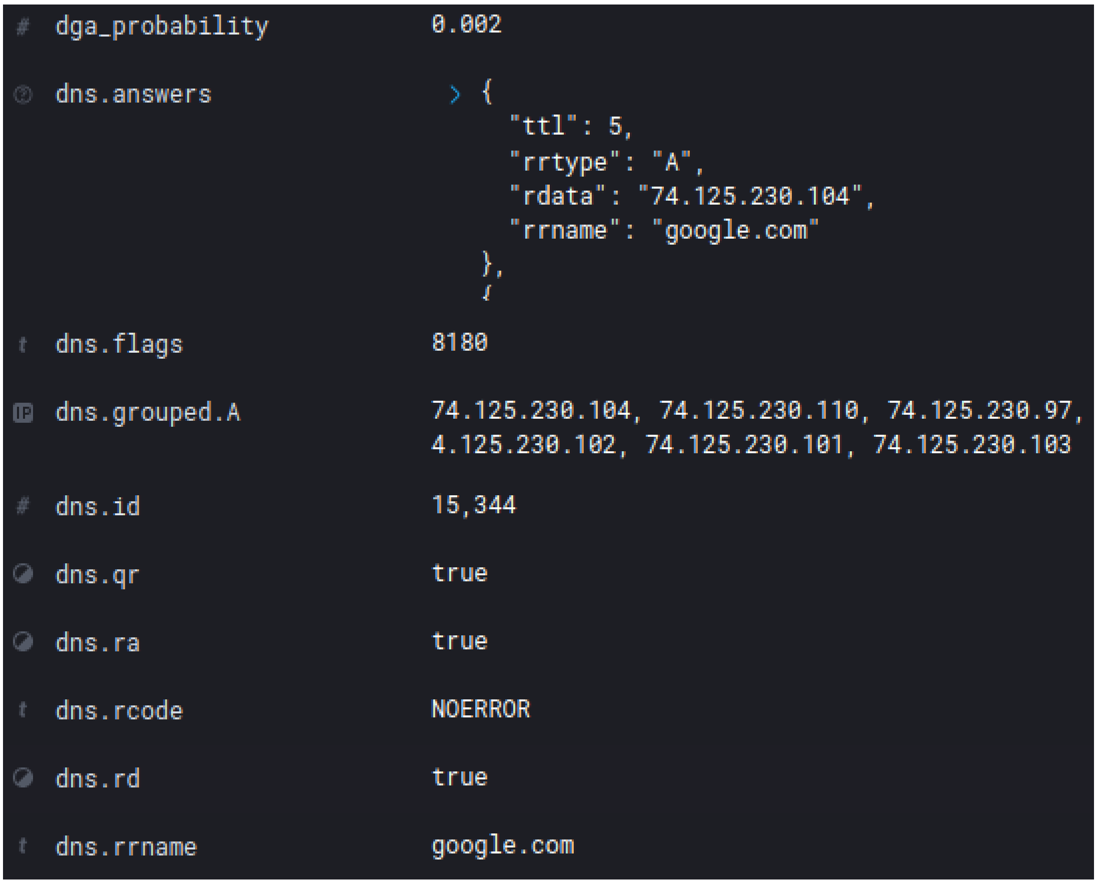
Clean previous list ? □

Furthermore, the administrator can decide to delete the previous list by ticking the **Clean previous list?** box and record all changes by clicking **Save**.

Chapter 29

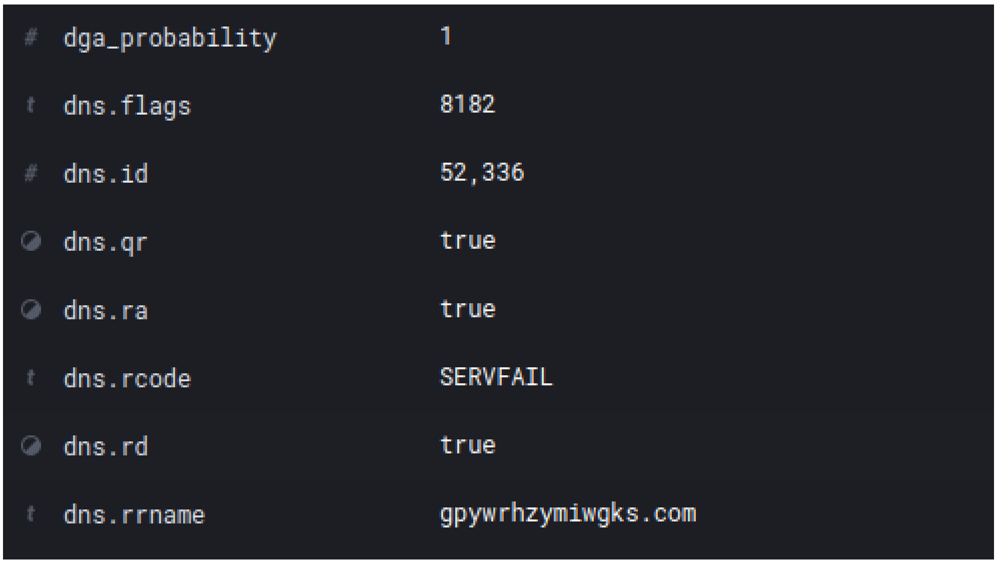
Generated events

The machine learning engine enriches the information already provided by the **Sigflow** module. Thus, for a domain that is not detected as a generated domain, the `dga_probability` field will be added. A value close to `0` indicates a low probability the domain was generated as in the following example:



```
#  dga_probability          0.002

   dns.answers               > {
                                 "ttl": 5,
                                 "rrtype": "A",
                                 "rdata": "74.125.230.104",
                                 "rrname": "google.com"
                               },
                               {

t  dns.flags                8180

IP dns.grouped.A            74.125.230.104, 74.125.230.110, 74.125.230.97,
                            4.125.230.102, 74.125.230.101, 74.125.230.103

#  dns.id                   15,344

   dns.qr                   true

   dns.ra                   true

t  dns.rcode                NOERROR

   dns.rd                   true

t  dns.rrname               google.com
```

On the other hand, a value close to `1` indicates that there is a good chance this domain was the result of a random generation as in this case:



#	dga_probability	1
t	dns.flags	8182
#	dns.id	52,336
◐	dns.qr	true
◐	dns.ra	true
t	dns.rcode	SERVFAIL
◐	dns.rd	true
t	dns.rrname	gpywrhzymiwgks.com

Chapter 30

MISP (Malware Information Sharing Platform)

Rôle Administrateur Statut expérimental

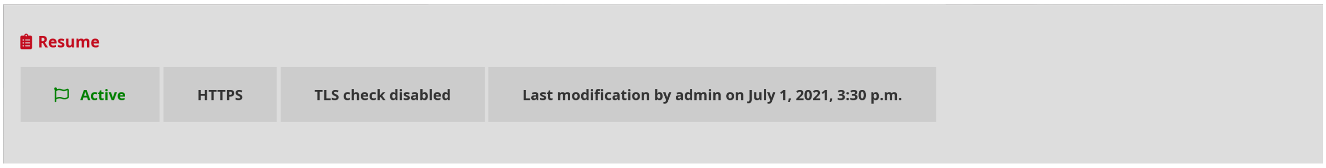
Menu: Administrators > GCenter > Third-Party Modules > MISP

This interface is used to manage the connection between the **GCENTER** and a Malware Information Sharing Platform (MISP) server already present in your infrastructure.

Connecting an MISP server to the TRACKWATCH solution enables the provision of technical threat information as well as a repository of malware, Indicators of Compromise (IOC) and information.

From the **MISP Suricata rules** section, the administrator can view the most recent configuration change of the MISP instance and make changes by clicking **Access**.

The administrator can check the connection status between the MISP instance and the **GCENTER** via **Resume**.



Resume

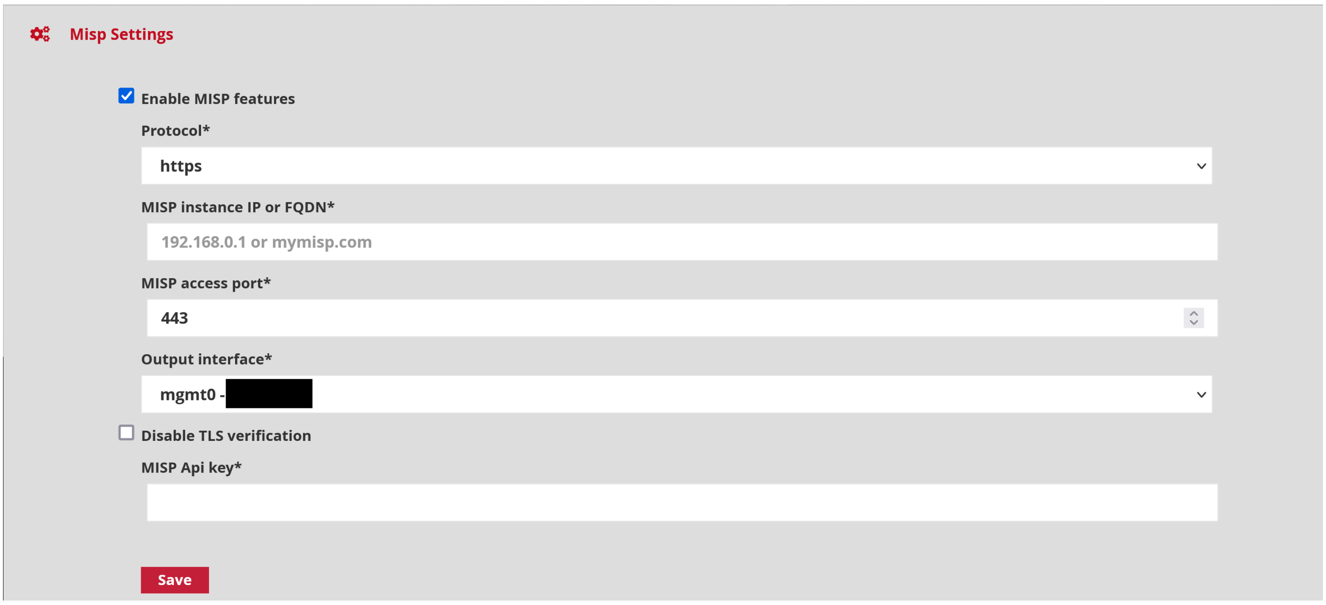
Active

HTTPS

TLS check disabled

Last modification by admin on July 1, 2021, 3:30 p.m.

Once in **Access**, the first step is to specify the IP address or domain of your MISP instance in the **GCENTER** WebUI.



Misp Settings

☑ Enable MISP features

Protocol*

https

MISP instance IP or FQDN*

192.168.0.1 or mymisp.com

MISP access port*

443

Output interface*

mgmt0 -[redacted]

□ Disable TLS verification

MISP Api key*

Protocol: the communication protocol to apply to contact the *MISP* instance. Two options are possible: 'HTTPS' and 'HTTP'. **MISP instance IP or FQDN**: The domain name or IP address of the MISP instance. **MISP access port** is the listening port of the MISP instance. **Output interface** is the physical interface of the **GCENTER** through which it will communicate with the MISP server. **MISP API key** the administrator enters the API key of the MISP instance.

Once the section is completed, simply click on 'Save' to record the information.

The MISP connector enables IOCs to be sent directly from a local MISP to the GATEWATCHER probes. This connector enables adding a quality threat intelligence source, while respecting the ANSSI guidelines on signature qualification.

Now that the service is activated, it can be seen that the **MISP interconnection status** has been modified. The link between the **GCENTER** and the MISP instance is operational.

Chapter 31

Hurukai (by HarfangLab)

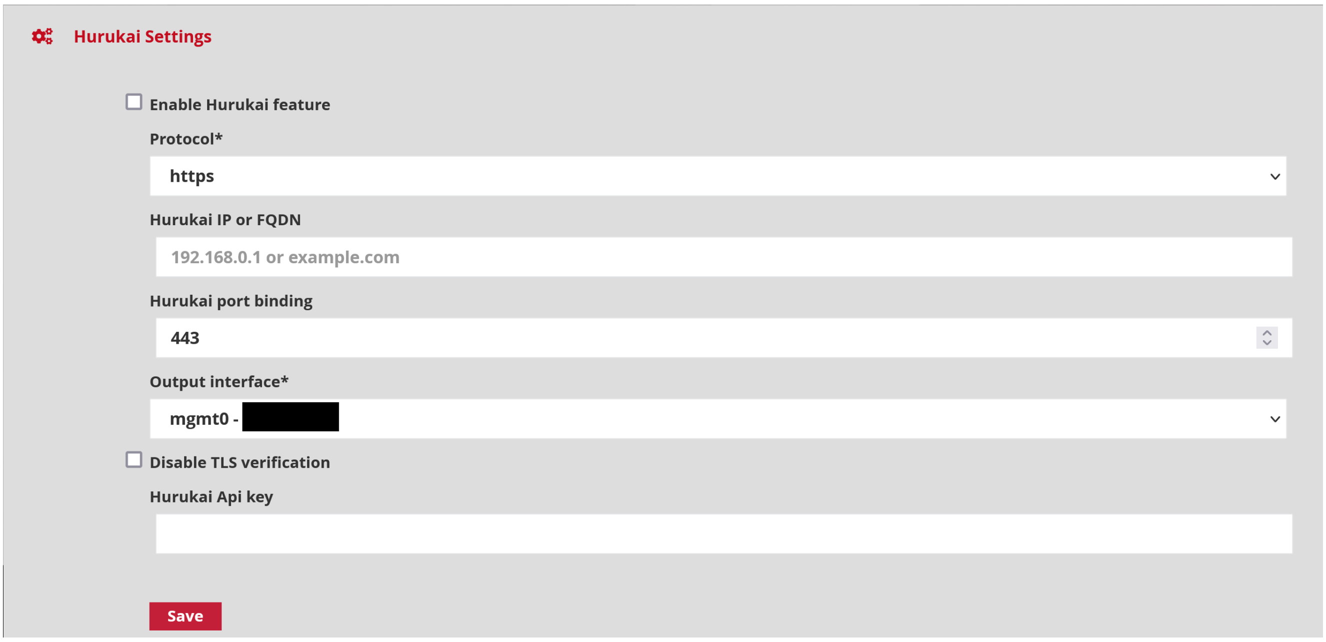
Rôle Administrateur Statut expérimental

Menu: Administrators > GCenter > Third-Party Modules > Hurukai

HarfangLab offers an Endpoint Detection Investigation and Remediation (EDiR) or EDR solution known as Hurukai. This solution enables investigating cyber-attacks without slowing down the company's operations. Hurukai will enable real-time collection of information on endpoints through the use of agents that will be deployed by the solution's management server. The agents are compatible with Windows 7, 8, 8.1, 10, and Windows server 2008, 2012, and 2016 platforms.

The purpose of this section is to connect the **GCENTER** to the Hurukai EDiR via the "Third Party modules" section in the **GCENTER** administration. Then simply move to the "Hurukai" tab to access the function.

To interconnect the two devices, simply enter the IP address or URL and the associated Hurukai communication port in the appropriate fields:



Hurukai Settings

□ Enable Hurukai feature

Protocol*: https

Hurukai IP or FQDN: 192.168.0.1 or example.com

Hurukai port binding: 443

Output interface*: mgmt0 - [redacted]

□ Disable TLS verification

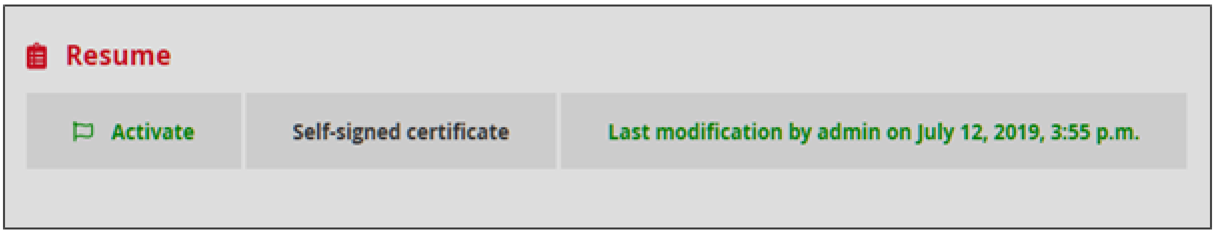
Hurukai Api key:

Protocol communication protocol to apply to contact the *MISP* instance. Two options are possible: 'HTTPS' and 'HTTP'. **Hurukai IP or FQDN**: the domain name or IP address of the Hurukai instance **Hurukai port binding**: the listening port of the Hurukai server **Output interface**: is the physical interface of the **GCENTER** through which it will communicate with the Hurukai server. **Hurukai API key**: is the Hurukai API key.

Once the section is completed, simply click on 'Save' to record the information.

The EDiR search engine instantly identifies anomalies, generating alerts through suspicion-raising functions. Markers of known attacks, attacker tools, bootkits, the presence of unsigned code, and injected code will be identified.

The service is now activated and functional.



Resume

Activate

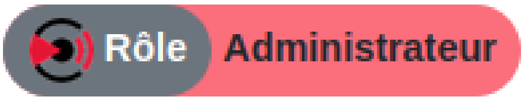
Self-signed certificate

Last modification by admin on July 12, 2019, 3:55 p.m.

Chapter 32

Intelligence

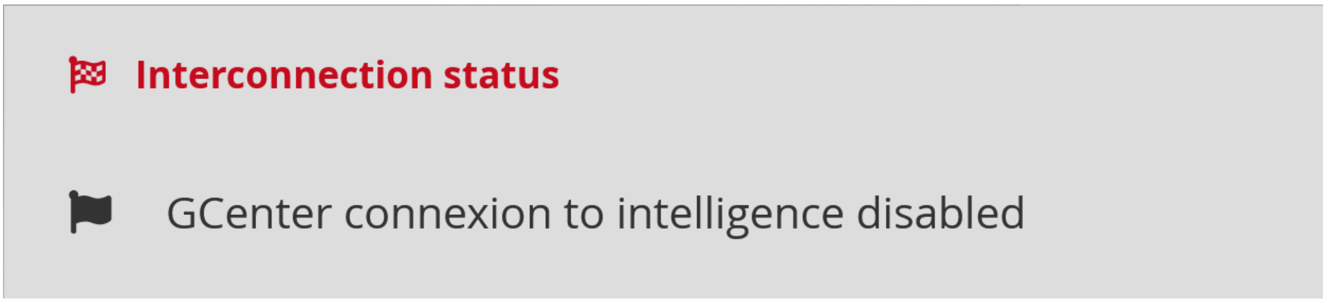
32.1 External


Rôle Administrateur

Menu: Administrators > GCenter > Third-Party Modules > Intelligence

In order to obtain a detailed analysis report of the file detected on the **GCENTER**, a connection must be established between it and the connected Intelligence platform. Once this connection is established, the operator will be able to send files to the Intelligence platform directly from the interface.

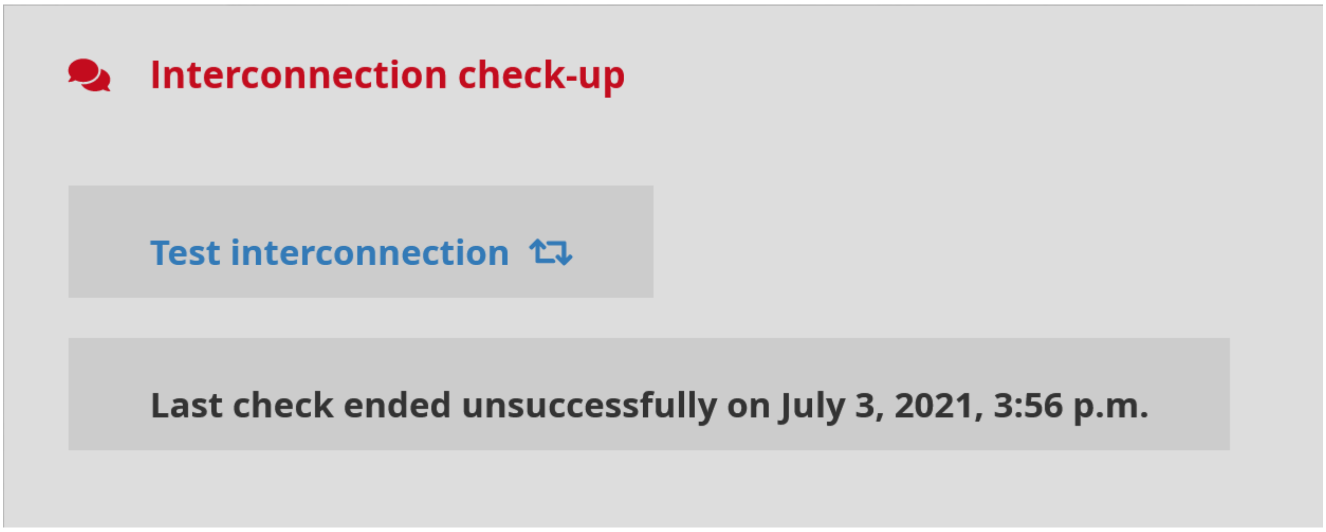
The connection status between the **GCENTER** and the Intelligence platform is displayed in the **Interconnection status** view below:


Interconnection status

GCenter connexion to intelligence disabled

Please note that the link between the two devices of the GATEWATCHER solution is optional although recommended for optimal use of the product once malware has been detected.

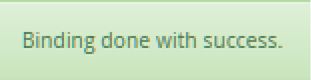
The connectivity can be checked in a single click by the administrator from the **Interconnection check-up** section by pressing the **Interconnection test** button.



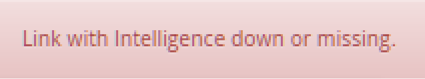
Interconnection check-up

Last check ended unsuccessfully on July 3, 2021, 3:56 p.m.

The interconnection test result will be displayed as follows:

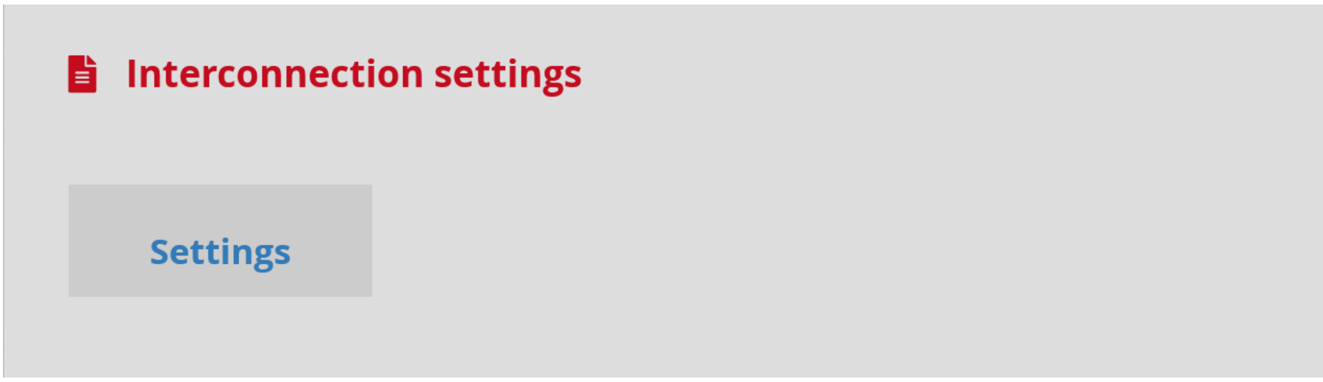


Binding done with success.



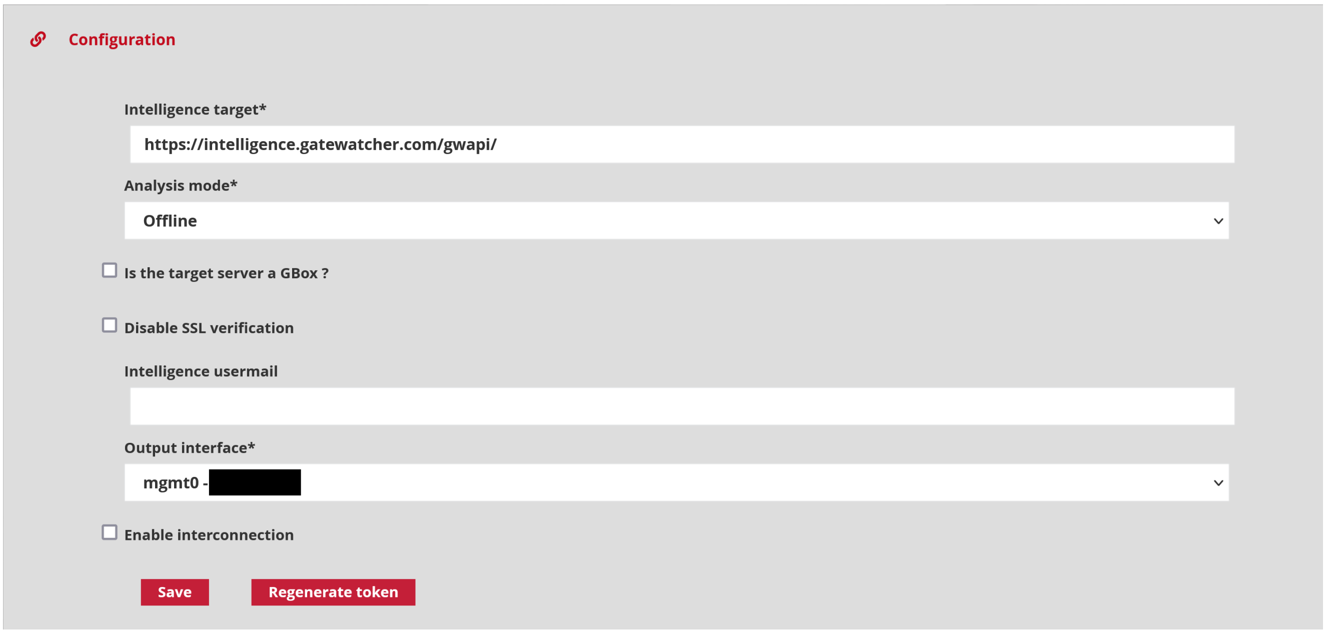
Link with Intelligence down or missing.

Certain information is required for the **GCENTER** to be connected to the platform.



Interconnection settings

Some fields are to be filled in by the administrator from the **Interconnection settings** section by pressing the **Settings** button.



Configuration

Intelligence target*

https://intelligence.gatewatcher.com/gwapi/

Analysis mode*

Offline

□ Is the target server a GBox ?

□ Disable SSL verification

Intelligence usermail

Output interface*

mgmt0 - [redacted]

□ Enable interconnection

Intelligence target: is the address of the Gatewatcher *Intelligence* server (https://intelligence.GATEWATCHER.com/gwapi/_).

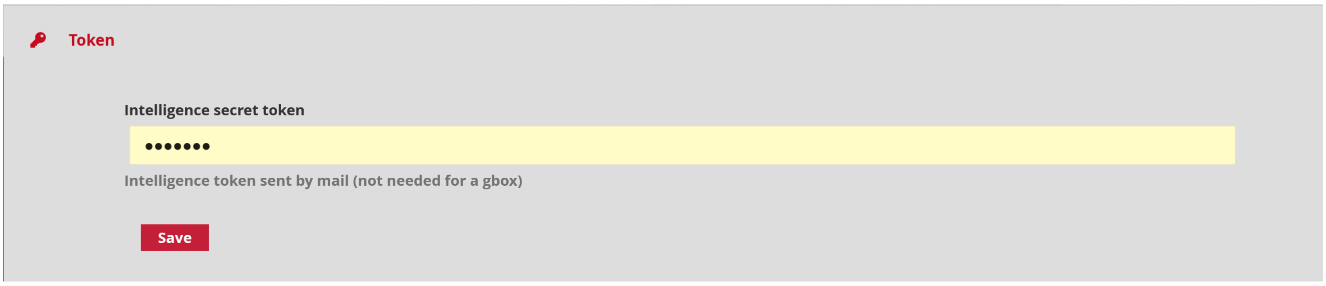
The boxes **Is the target server a GBOX?** and **Disable SSL verification** should only be ticked *when using a* ***GBOX***. Once the address is filled in, the administrator must store the information by clicking on *Save*.

Analysis mode: corresponds to the analysis method of the file sent to the Intelligence server: Online or Offline.

Intelligence usermail: The email address of the intelligence account to which an email will be sent. This will contain a token enabling a **GCENTER** to be connected to https://intelligence.GATEWATCHER.com/packages/list/.

Output interface is the interface of the **GCENTER** through which it will communicate with the Intelligence server.

Once the email containing the connection token is received, it will be necessary to fill in the field **Intelligence secret token**:



Token

Intelligence secret token

•••••••

Intelligence token sent by mail (not needed for a gbox)

This token is unique per user account yet can be used on multiple **GCENTER**. The activation of a new token will be added to the list of other tokens linked to the email address.

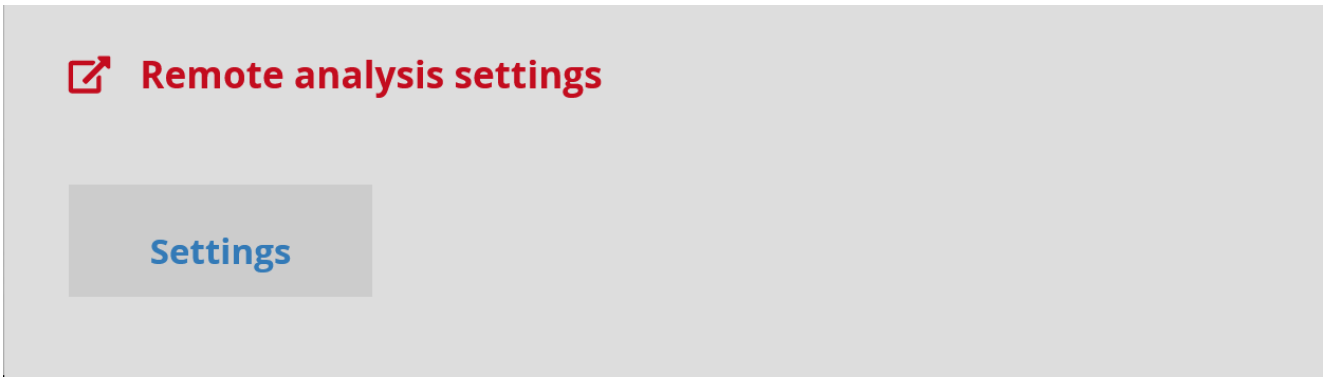
□ Enable interconnection

The last step in activating the service involves ticking the 'Enable interconnection' box. Then click on **Save** or **Regenerate Token**.

Once the service is activated, the condition in the **Interconnection status** field changes: the link between the **GCENTER** and the Intelligence platform is operational.

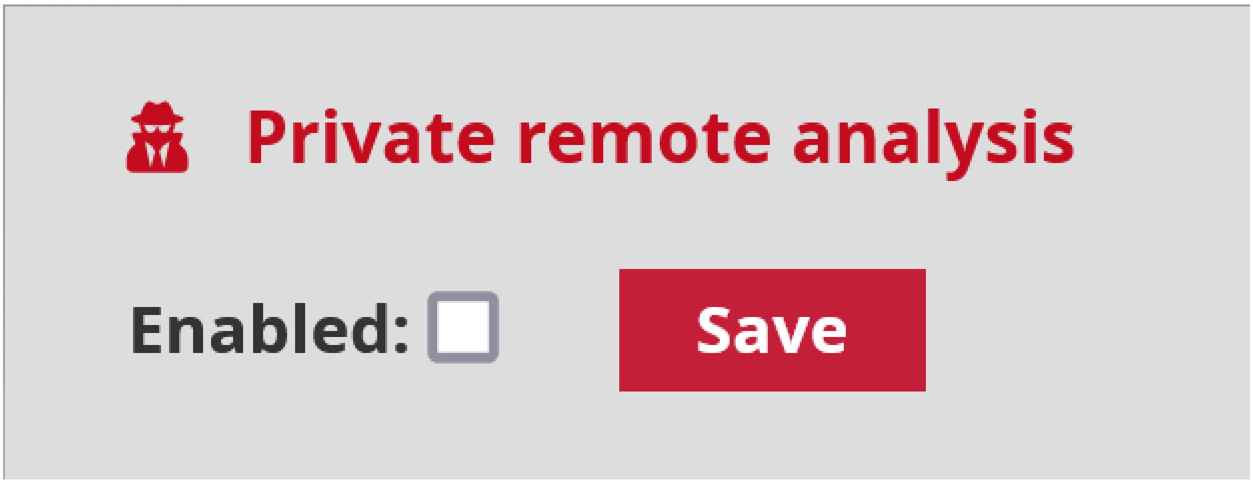
Once the link is established, users will be able to download a detected sample from the analysis platform and run it under the Intelligence engines. Detailed analysis reports of these samples may be retrieved from the *Malcore section of Inspectra*.

As a result of this connection, the administrator may be able to send files to the Intelligence platform for further analysis and download the report.

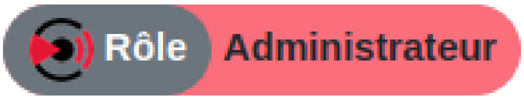


The **Remote analysis settings** section enables the administrator to remain anonymous when sending samples to the platform if the **Private remote analysis** option is enabled.

If the 'Enabled' box is not ticked and/or the administrator does not backup by pressing **Save** then other users of the Intelligence platform will be able to see the details of each analysis the administrator carries out.



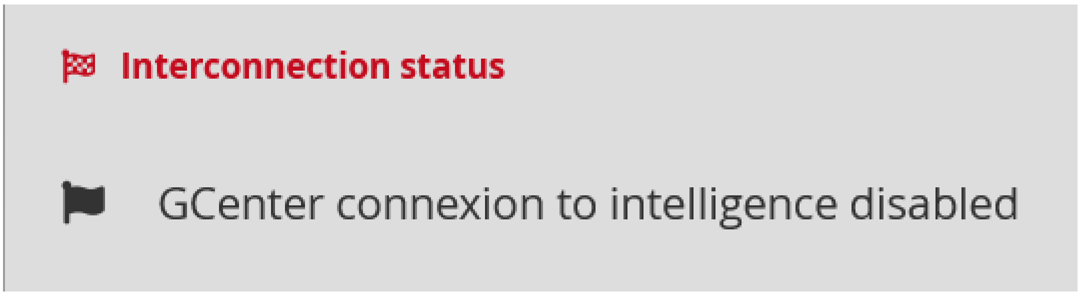
32.2 GBox



Menu: Administrators > GCenter > Third-Party Modules > Intelligence

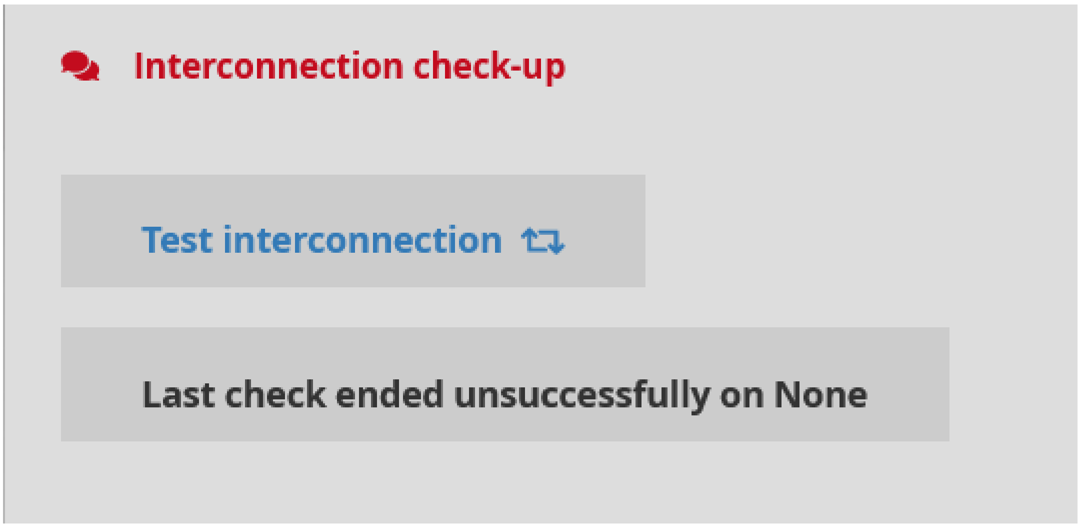
Just like connecting to Gatewatcher's *Intelligence* service, using a **GBox** enables in-depth analysis of malware detected by *Malcore* with the difference being that using a **GBox** enables this without having to send information to an external service. **GBOX** is a physical device installed within the infrastructure, along with the other devices of the TRACKWATCH solution.

The connection status between the **GCENTER** and the **GBOX** is displayed in the **Interconnection status** view below:


Interconnection status

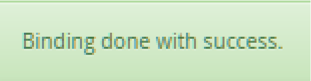
GCenter connexion to intelligence disabled

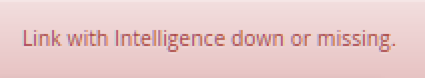
The connectivity can be checked in a single click by the administrator from the **Interconnection check-up** section by pressing the **Interconnection test** button.


Interconnection check-up

Last check ended unsuccessfully on None

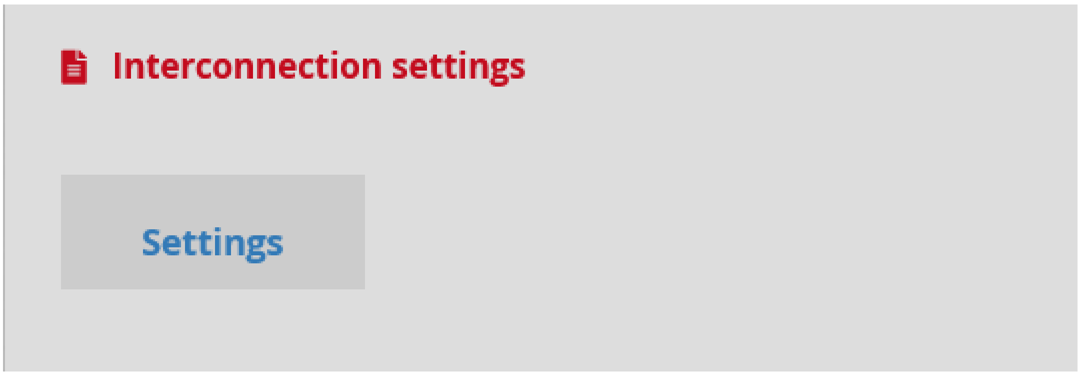
The interconnection test result will be displayed as follows:


Binding done with success.

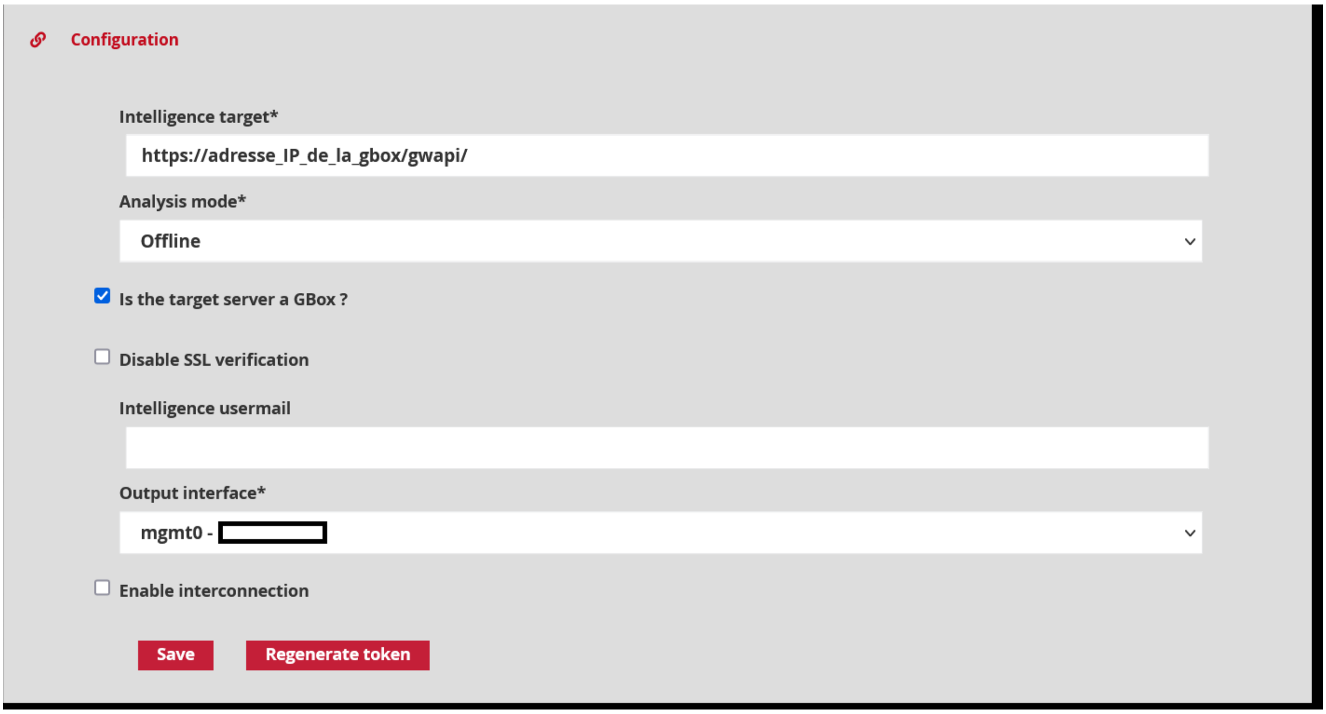

Link with Intelligence down or missing.

An interconnection must be set up between the **GCENTER** and the **GBOX**. The link between the two devices operates via an Application Programming Interface (API) that enables samples to be sent to the **GBOX** for analysis and the results of the testing to be retrieved.

Some details are required so that the **GCENTER** can be connected to the platform and can send the HTTP request correctly.


Interconnection settings

Some fields are to be filled in by the administrator from the **Interconnection settings** section by pressing the **Settings** button.



Configuration

Intelligence target*

https://adresse_IP_de_la_gbox/gwapi/

Analysis mode*

Offline

☑ Is the target server a GBox ?

□ Disable SSL verification

Intelligence usermail

Output interface*

mgmt0 - [redacted]

□ Enable interconnection

Intelligence target: this is the API address of the **GBOX** (of the form: *https://adresse IP de la GBOX/gwapi/*). **Is the target server a GBOX?**: is to be ticked to indicate the use of a GBox **Disable SSL verification**: enables the use of auto-signed certificates. **Analysis mode**: corresponds to the analysis method of the file sent to the Intelligence server: *Offline* or *Online*.

Intelligence usermail: is not required when using a **GBox**.

Output interface is the physical interface of the **GCENTER** through which it will communicate with the **GBOX** server.

□ Enable interconnection

The last step in activating the service involves ticking the **Enable interconnection** box. Then click on **Save**.

Once the link is established, users will be able to download a detected sample from the intelligence analysis platform and run it through the **GBox** engines. Detailed analysis reports for these samples will be available in the [Inspectra - MALCORE] section (../malcore.html#inspectra).

Once the service is activated, the condition in the **Interconnection status** field changes: the link between the **GCENTER** and the **GBox** is operational.

As for the analysis in the **GBOX**, the template used for the samples can be specified in the query. If the template is not specified in the query, the samples are analysed using the default template in the **GBOX** that must therefore be set up beforehand. Samples are transmitted in raw binary format.

The **Remote analysis settings** section is not useful to the administrator in this choice of infrastructure, the **GBOX** being a dedicated server within the solution.

Chapter 33

Syslog

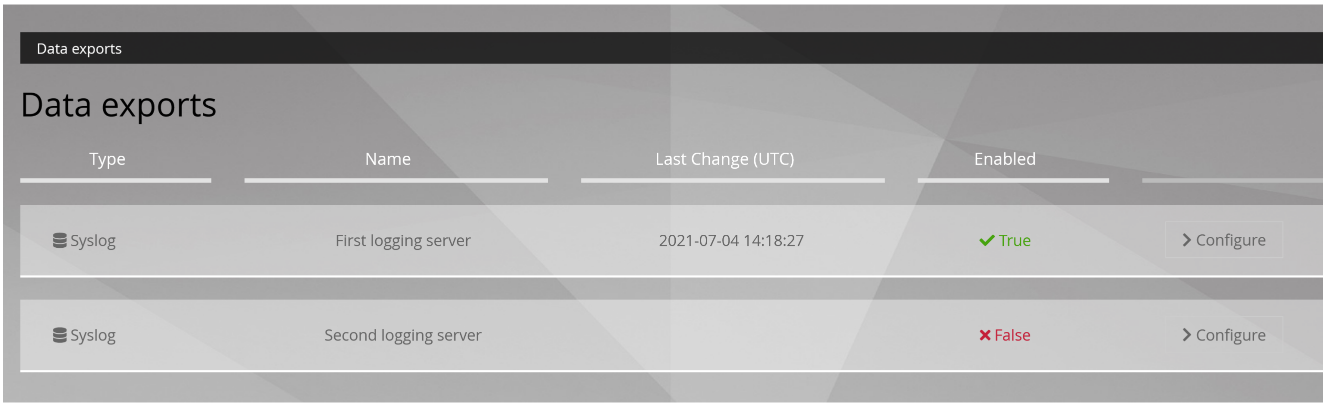
Rôle Administrateur

Menu: Administrators > GCenter > Data export

33.1 Configuration Syslog

From this section the solution administrators are able to export alerts or part of alerts to a security information and event management (SIEM).

The administrator can export the data in real time by targeting a primary and/or secondary Syslog correlator, whose dispatches can be configured.



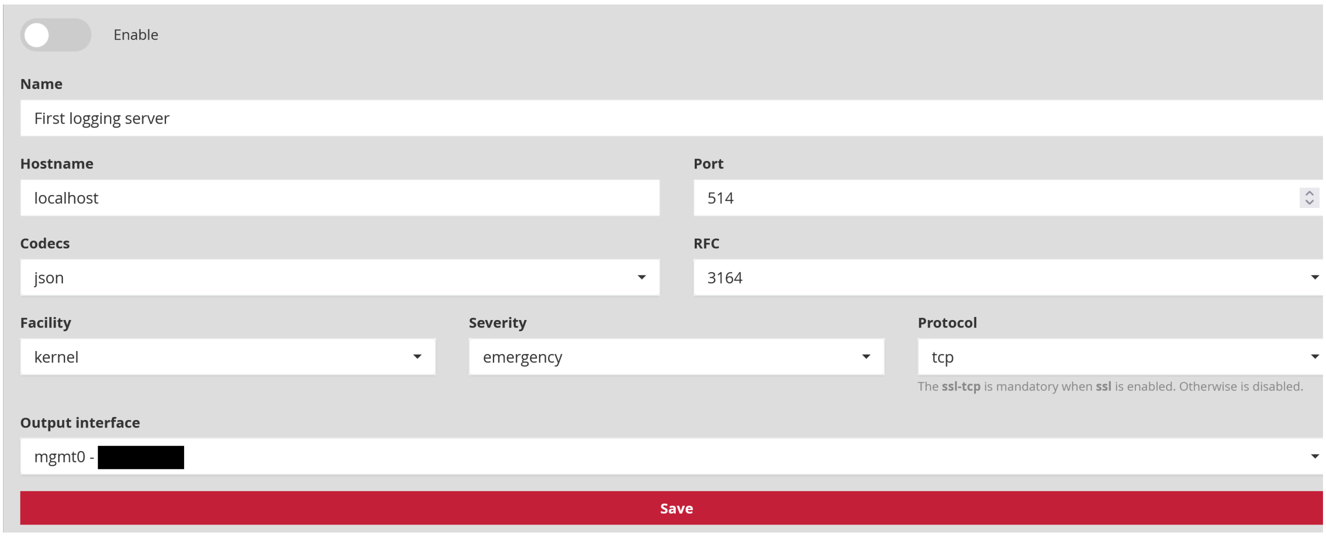
Data exports

Type	Name	Last Change (UTC)	Enabled	
Syslog	First logging server	2021-07-04 14:18:27	✓ True	> Configure
Syslog	Second logging server		✗ False	> Configure

In order for the **TRACKWATCH** solution to communicate its information to a Netdata server, this section must be configured with the necessary information. This configuration is carried out from three tabs:

- *General*
- *Filters*
- *Encryption*

33.1.1 General settings



Enable

Name: First logging server

Hostname: localhost

Port: 514

Codecs: json

RFC: 3164

Facility: kernel

Severity: emergency

Protocol: tcp

The **ssl-tcp** is mandatory when **ssl** is enabled. Otherwise is disabled.

Output interface: mgmt0 - [redacted]

Enable activates or deactivates the Syslog export.

Name (Example: *First logging server*) is the name of the Syslog server assigned by the administrator.

Host name (Example: *localhost* or *192.168.199.1*) is the IP address or the name of the Syslog server for the connection.

Port number: is the listening port of the Syslog server for the connection. The default value is 514.

Codec: (Example: *json*, *idmef*, *cef* ou *plain*) is the codec used for the output data. Output codecs are a convenient way to encode your data prior to export without the need for another filter. By default the value is in json.

** RFC** (Example: *3164* or *5424*) enables selecting the corresponding RFC for the desired message normalisation.

Facility (Example: *kernel*, *user-level*, *mail*, *deamon*, *security/authorization*, *syslogd*, *line printer*, *network news*, *uucp*) refers to the message type used for sending to the Syslog server. The default value is a *kernel*.

Severity (Example: *emergency*, *alert*, *critical*, *error*, *warning*, *notice*, *informational*, *debug*) is the severity rate for Syslog messages. The default value is an emergency.

Protocol (Example: *tcp*, *udp* ou *ssl_tcp*) is the protocol used for data transfer. The default value is in TCP.

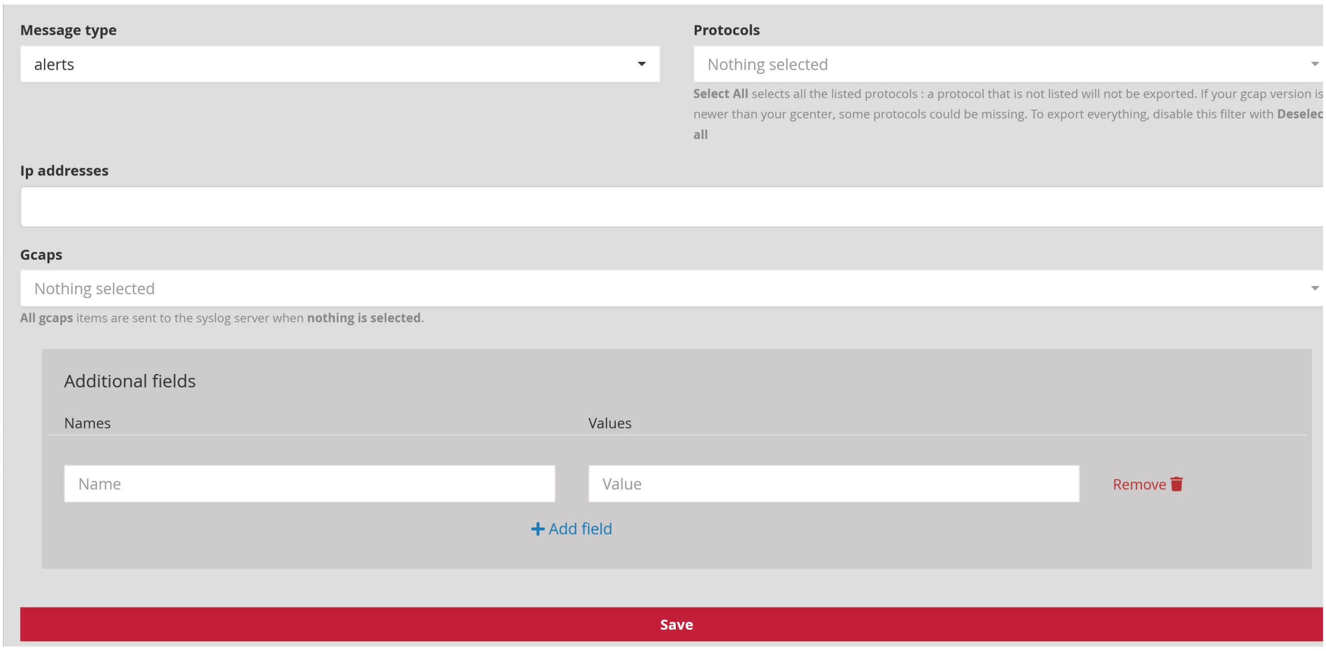
Note:

SSL-TCP is mandatory if SSL encryption is enabled. Otherwise, it is disabled.

Output interface (Example: *mgmt0*, *sup0*) is the selected output interface between the **GCENTER** and the SIEM.

Any modification will only be applied after pressing '** Save**'.

33.1.2 Filtering



Message type

alerts

Protocols

Nothing selected

Select All selects all the listed protocols : a protocol that is not listed will not be exported. If your gcap version is newer than your gcenter, some protocols could be missing. To export everything, disable this filter with **Deselec all**

Ip addresses

Gcaps

Nothing selected

All gcaps items are sent to the syslog server when **nothing is selected**.

Additional fields

Names	Values	
Name	Value	Remove

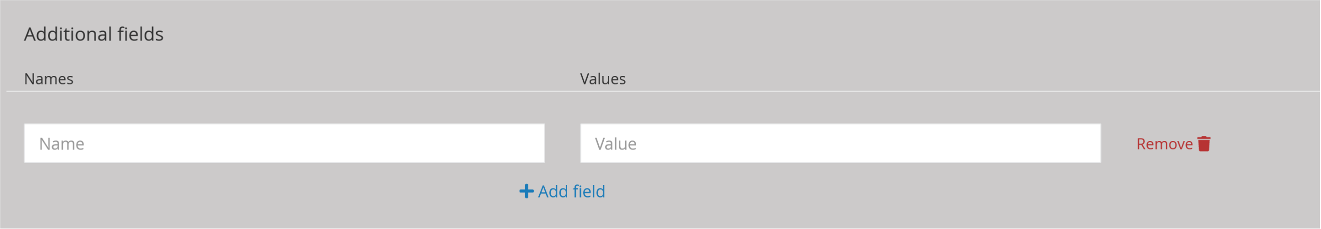
Message type: (Example: *alerts*, *all*) defines the type of event to be sent: only alerts or all information (metadata, fileinfo, ...)

Protocols: (Example: *dcerpc*, *dhcp*, *dnp3*, *dns*, *ftp*, *http*, *ikev2*, *krb5*, *modbus*, *netflow*, *nfs*, *smb*, *smtp*, *ssh*, *tftp*, *tls* et *ntp*) enables selecting the protocols to be exported.

Note:

[Select All] will choose all listed protocols: a protocol that is not listed will not be exported. If the GCAP version is newer than that of the GCENTER, some protocols may be missing. To export everything, deactivate this filter with [Deselect all].

Gcaps: (Example: *GCap1*, *GCap2*) enables filtering by **GCAP**. All **GCAP** data paired with the **GCENTER** is sent to the Syslog server if nothing is selected.



Additional fields

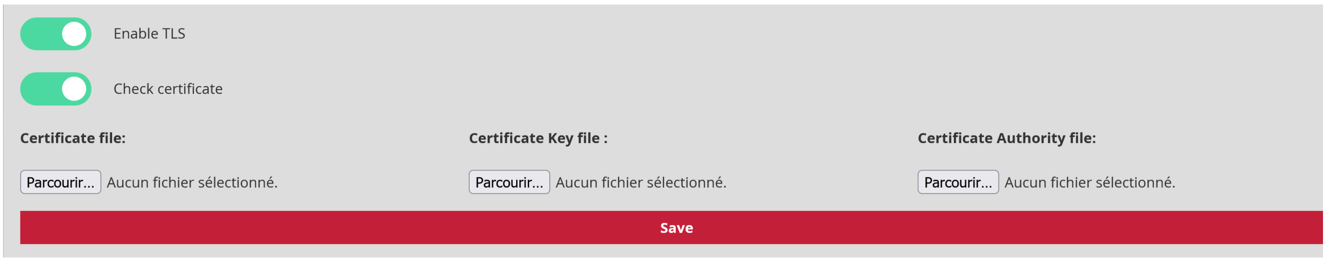
Names	Values	
Name	Value	Remove

Additional fields enables the administrator to add more fields to the transferred data. A name (**Name**) and a description (**value**) can be entered in this window. When using the idmef codec, this field is not supported.

Any modification will only be applied after pressing '** Save**'.

33.1.3 Encryption

This section enables encryption to be added to the data transfer between the **GCENTER** and the syslog receiver. It will be necessary to add a certificate, the associated key, and the certification authority in order to validate this functionality.



Enable TLS

Check certificate

Certificate file: Parcourir... Aucun fichier sélectionné.

Certificate Key file : Parcourir... Aucun fichier sélectionné.

Certificate Authority file: Parcourir... Aucun fichier sélectionné.

Enable TLS: Ability to activate the Transport Layer Security (TLS) service. Disabled by default.

Check certificate: setting to stop checking the validity of the certificate when the TLS service is enabled.

Any modification will only be applied after pressing '** Save**'.

33.2 Logstash

Rôle Administrateur

Menu: Administrators > GCenter > Data export

GCenter can export its logs to the Logstash ETL. A pipeline developed by Gatewatcher enables the JSON content of the exported logs to be retrieved and then manipulated as desired with Logstash filters. The Gcenter integration is therefore very fast. It only requires two steps:

- On Gcenter, configure the data export to Logstash.
- On Logstash, configure the pipeline to receive the flow from GCenter.

33.2.1 Configuring Logstash data export

Select one of the two export pipelines by clicking on **Configure**.

The following table summarises the parameters to be applied in the *GENERAL* tab.

> **Note:**
>
> Values whose format is $VALUE are context specific. They are noted as such so that they can be referred to in the following documentation.

The *FILTERS* tab enables selecting which logs will be exported. See *filtering* in the syslog section.

The "ENCRYPTION" tab enables activating the encryption of the flow generated by the GCenter. The Logstash "syslog" input is not compatible with data encryption. Therefore this feature cannot be used.

33.2.2 Pipeline Logstash

The input used is Syslog. In order to be compatible with any Syslog header, a grok pattern is defined. The JSON content of the log is in the syslog_message field.

```
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 kept, and converted to JSON. The original field (syslog_message) and the elasticsearch specific field (@version) are then removed.

```
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 written directly to disk as files:

```
output {
  file {
    path => '/usr/share/logstash/data/output/%{[type]}-%{+YYYY.MM.dd}.log'
    codec => json_lines
  }
}
```

33.2.3 Quick POC

A POC with a Logstash docker can be achieved in a few minutes. The following commands, provided as a guide, should make this task easier.

Important:

The commands are purely indicative in order to assemble a demonstrator quickly. It does not adhere to the best practices necessary to develop a production component.

On a linux machine having docker, execute the following commands to retrieve the default Logstash configuration files: (procedure tested with Logstash version 7.13.1)

```
mkdir logstash_docker
cd logstash_docker
sudo docker run --name="logstash_tmp" --rm -d -it docker.elastic.co/logstash/logstash:7.13.1
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
```

The resulting folder is `logstash_docker`, within which two subfolders appear: `config` and `pipeline`.

In `config`, the settings can be retained by default, with the exception of the `xpack.monitoring.elasticsearch.hosts` setting, which should be annotated in `logstash.yaml`.

In the `pipeline` folder, replace the default pipeline with the one described in the section above.

A docker using these configuration files and this pipeline can then be started.

```
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:7.13.1
```

Logstash will then create an `output` directory in which the received logs will be written, with one JSON per line.

33.3 Splunk

Rôle Administrateur

Menu: Administrators > GCenter > Data export

GCenter can export its logs to the Splunk SIEM. A Technological Add-On (TA) developed by Gatewatcher enables mapping the logs exported by the GCenter to Splunk data models. The Gcenter integration is therefore very fast. It only requires three steps:

- On Gcenter, configure the data export to Splunk.
- On the Splunk server, install the TA compatible with the GCenter version installed. In this instance, TA-gatewatcher-gcenter-v101.
- On the Splunk server, configure the data reception from the GCenter and associate it with the TA.

Note:

The Splunk TA is still in beta version. The TA content is detailed at the end of this documentation so the administrators can adapt it to their needs.

33.3.1 Configuring Splunk data export

Select one of the two export pipelines by clicking on "Configure"

The following table summarises the parameters to be applied in the "GENERAL" tab.

Note:

Values whose format is $VALUE are context specific. They are noted as such so that they can be referred to in the following documentation.

The "FILTERS" tab enables selecting which logs will be exported. See *filtering* in the syslog section.

The "ENCRYPTION" tab enables encrypting the flow between the GCenter and Splunk if necessary. $PROTOCOL should then be TCP. If encryption is enabled, the Splunk data input configuration (input.conf) must contain the appropriate stanzas. This guide does not cover the encryption configuration between the GCenter and Splunk.

33.3.2 Installing the TA

Download the TA here: TA-gatewatcher-gcenter-v101-0.1.0.spl

Installing the TA is the same as in any Splunk app. The steps are as follows, however, see the documentation for your version of Splunk for more details:
Manage apps > Install an app from a file > choose Gatewatcher TA > "Send"

By clicking on "View objects" in the Splunk app management menu, you can access all the objects provided by the TA:

- The definition of field aliases.
- The definition of eventtypes.
- Associations between eventtypes and tags.

You can enable/disable objects from this interface and change their permissions. By default, permissions are set to "Global" - Read for everyone - Write for admins only.

33.3.3 Configuring data reception

Configuring the data input at the Splunk level must be done consistently with the GCenter configuration.

In Splunk, the configuration will be done in Settings > Data > Data inputs > TCP/UDP

The following table summarises the parameters to be applied for the data input to work:

33.3.4 Composition of the TA

The TA consists of the following files, placed in the application's `default` directory. Changes can be made to these files to adapt the behaviour of the TA to your specific needs and use of the data models. The recommended best practice is to create a local' folder and keep the default' folder intact (see Splunk documentation on `how to edit a configuration file').

33.3.4.1 props.conf

```
[gw:gcenter:101]
KV_MODE = json
MAX_TIMESTAMP_LOOKAHEAD = 31
```

The following section removes the Syslog headers and the `@version` field from elasticsearch, which is not used.

```
SEDCMD-gw-1-remove-header = s/^([^\{]+)//
SEDCMD-gw-2-remove-host = s/\"host\":\"[^\s"]+\",?//
SEDCMD-gw-3-remove-version = s/\"@version\":\"[^\s"]+\",?//
SEDCMD-gw-4-remove-trailing_comma = s/,}/}/
TIME_FORMAT = %Y-%m-%dT%H:%M:%S.%6N%Z
TIME_PREFIX = \"timestamp_detected\":\"
```

The following transformation is called `gw_force_host` in `transforms.conf`. It enables the GCenter name to be associated with the `host` field used by Splunk.

```
TRANSFORMS-host = gw_force_host
```

The following transformation calls the stanzas `sourcetype_*` from `transforms.conf` in order to associate a sourcetype based on the engine that generated the log.

```
TRANSFORMS-override_sourcetype_engine = sourcetype_malcore,sourcetype_codebreaker,sourcetype_sigflow,sourcetype_sigflow_alert
```

The logs cannot exceed 65 kb. GCenter are in UTC.

```
TRUNCATE = 65535
TZ = UTC
category = Splunk App Add-on Builder
pulldown_type = 1
```

The rest of `props.conf` enables field aliases to be associated with each sourcetype. Field evaluations enable logs to be transformed to match data models.

```
[gw:gcenter:101:sigflow:meta]
FIELDALIAS-gw_gcenter_101_sigflow_meta_src = src_ip AS src
FIELDALIAS-gw_gcenter_101_sigflow_meta_dest = dest_ip AS dest
FIELDALIAS-gw_gcenter_101_sigflow_meta_hash = fileinfo.sha256 AS file_hash
FIELDALIAS-gw_gcenter_101_sigflow_meta_alias_1 = tcp.tcp_flags AS tcp_flag
FIELDALIAS-gw_gcenter_101_sigflow_meta_alias_2 = netflow.pkts AS packets
FIELDALIAS-gw_gcenter_101_sigflow_meta_alias_3 = netflow.bytes AS bytes
FIELDALIAS-gw_gcenter_101_sigflow_meta_alias_4 = event_type AS app

FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_02 = http.status AS status
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_03 = http.length AS bytes
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_04 = http.url AS uri_query
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_05 = http.hostname AS url_domain
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_06 = http.http_content_type AS http_content_type
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_07 = http.http_method AS http_method
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_08 = http.http_user_agent AS http_user_agent
FIELDALIAS-gw_gcenter_101_sigflow_meta_http_alias_09 = http.http_refer AS http_referrer

EVAL-action = "allowed"
EVAL-protocol = "ip"
EVAL-transport = lower(proto)
EVAL-url = url_domain+uri_query

[gw:gcenter:101:sigflow:alert]
EVAL-action = "allowed"
EVAL-transport = low(proto)
FIELDALIAS-gw_gcenter_101_sigflow_alert_alias_1 = src_ip AS src
FIELDALIAS-gw_gcenter_101_sigflow_alert_alias_2 = dest_ip AS dest
FIELDALIAS-gw_gcenter_101_sigflow_alert_alias_3 = alert.signature AS signature
FIELDALIAS-gw_gcenter_101_sigflow_alert_alias_4 = alert.signature_id AS signature_id
FIELDALIAS-gw_gcenter_101_sigflow_alert_alias_5 = severity AS severity_id

[gw:gcenter:101:malcore]
FIELDALIAS-gw_gcenter_101_malcore_src = src_ip AS src
FIELDALIAS-gw_gcenter_101_malcore_dest = dest_ip AS dest
FIELDALIAS-gw_gcenter_101_malcore_hash = SHA256 AS file_hash
FIELDALIAS-gw_gcenter_101_malcore_alias_2 = src_ip AS src
FIELDALIAS-gw_gcenter_101_malcore_alias_3 = dest_ip AS dest
```

(continues on next page)

(continued from previous page)

```
FIELDALIAS-gw_gcenter_101_malcore_alias_4 = filename AS file_name
FIELDALIAS-gw_gcenter_101_malcore_alias_5 = http_uri AS file_path
FIELDALIAS-gw_gcenter_101_malcore_alias_6 = total_found AS signature_id

[gw:gcenter:101:codebreaker]
FIELDALIAS-gw_gcenter_101_codebreaker_src = src_ip AS src
FIELDALIAS-gw_gcenter_101_codebreaker_dest = dest_ip AS dest
FIELDALIAS-gw_gcenter_101_codebreaker_hash = SHA256 AS file_hash
FIELDALIAS-gw_gcenter_101_codebreaker_alias_4 = event_type AS category
```

33.3.4.2 transforms.conf

The stanzas in this file are used by `props.conf`. They concern fields indexed by Splunk, like `host` or `sourcetype`.

```
[gw_force_host]
LOOKAHEAD = 65535
DEST_KEY = MetaData:Host
REGEX = \"GCenter\"\:\"([^\"]+)
FORMAT = host::$1

[sourcetype_malcore]
LOOKAHEAD = 65535
REGEX = \"type\"\:\"malcore\"
FORMAT = sourcetype::gw:gcenter:101:malcore
DEST_KEY = MetaData:Sourcetype

[sourcetype_codebreaker]
LOOKAHEAD = 65535
REGEX = \"type\"\:\"codebreaker\"
FORMAT = sourcetype::gw:gcenter:101:codebreaker
DEST_KEY = MetaData:Sourcetype

[sourcetype_sigflow]
LOOKAHEAD = 65535
REGEX = \"type\"\:\"suricata\"
FORMAT = sourcetype::gw:gcenter:101:sigflow:meta
DEST_KEY = MetaData:Sourcetype

[sourcetype_sigflow_alert]
LOOKAHEAD = 65535
REGEX = \"event_type\"\:\"alert\"
FORMAT = sourcetype::gw:gcenter:101:sigflow:alert
DEST_KEY = MetaData:Sourcetype
```

33.3.4.3 eventtype.conf

This file enables associations between logs and events.

Events related to antivirus file analysis (malcore):

```
[malcore_clean]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact="None" code=0 )
description = An event that occurs when malcore analyses a file and none of the engines␣
↪detects a threat
```

(continues on next page)

(continued from previous page)

```
[malcore_infected]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact="None" code=1)
description = An event that occurs when malcore analyses a file and at least one of the␣
↪engines detects a threat
color = et_red

[malcore_suspicious]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact="None" code=2)
description = An event that occurs when malcore analyses a file, none of the engines detects␣
↪a threat but at least one classifies the file as suspicious. Suspicious files can be␣
↪analysed later by retroact, if enabled.
color = et_orange

[malcore_other]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact="None" NOT code IN (0,
↪1,2))
description = An event that occurs when malcore returns a code indicating an exception or a␣
↪failure in the analysis.
color = et_blue
```

Events related to the antivirus reanalysis of suspicious files (retroact):

```
[retroact_clean]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact!="None" code=0 )
description = An event that occurs when retroact analyses a file and none of the engines␣
↪detects a threat
color = et_blue

[retroact_infected]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact!="None" code=2)
description = An event that occurs when retroact analyses a file and at least one of the␣
↪engines detects a threat
color = et_red

[retroact_suspicious]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact!="None" code=2)
description = An event that occurs when retroact analyses a file, none of the engines detects␣
↪a threat but at least one classifies the file as suspicious. Suspicious files can be␣
↪analysed later by retroact, if enabled.
color = et_orange

[retroact_other]
search = (sourcetype=gw:gcenter:101:malcore event_type=malware retroact!="None" NOT code IN␣
↪(0,1,2))
description = An event that occurs when retroact returns a code indicating an exception or a␣
↪failure in the analysis.
color = et_blue
```

Netflow logging activation event on the gcap:

```
[sigflow_netflow]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=netflow)
description = An event that occurs when sigflow generates a netflow event from a network␣
↪event.
```

Events related to file reconstruction by gcap:

```
[sigflow_fileinfo_stored]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=fileinfo fileinfo.stored="true")
description = An event that occurs when sigflow performs a file reconstruction and based on␣
↪its ruleset, stored it on disk to perform malcore analysis afterwards.
color = et_blue

[sigflow_fileinfo_not_stored]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=fileinfo fileinfo.stored="false")
description = An event that occurs when sigflow performs a file reconstruction and based on␣
↪its ruleset, has not stored it on disk.
```

Events related to the sigflow engine can be of two types for each protocol:

- Meta" event: generation of metadata obtained by activating the logging of the protocol on the gcap.
- alert" event: an alert is generated, obtained by activating the protocol parsing on the gcap, and the correspondence between a flow and a sigflow rule.

```
[sigflow_meta_dcerpc]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=dcerpc)
description = An event that occurs when sigflow reconstructs a dcerpc flow and logged its␣
↪metadata.

[sigflow_alert_dcerpc]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=dcerpc)
description = An event that occurs when sigflow reconstructs a dcerpc flow and one of its␣
↪rules matched the content of this flow.
color = et_red

[sigflow_meta_dhcp]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=dhcp)
description = An event that occurs when sigflow reconstructs a dhcp flow and logged its␣
↪metadata.

[sigflow_alert_dhcp]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=dhcp)
description = An event that occurs when sigflow reconstructs a dhcp flow and one of its rules␣
↪matched the content of this flow.
color = et_red

[sigflow_meta_dnp3]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=dnp3)
description = An event that occurs when sigflow reconstructs a dnp3 flow and logged its␣
↪metadata.

[sigflow_alert_dnp3]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=dnp3)
description = An event that occurs when sigflow reconstructs a dnp3 flow and one of its rules␣
↪matched the content of this flow.
color = et_red

[sigflow_meta_dns]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=dns)
description = An event that occurs when sigflow reconstructs a dns flow and logged its␣
↪metadata.
priority = 2

[sigflow_alert_dns]
```

(continues on next page)

(continued from previous page)

```
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=dns)
description = An event that occurs when sigflow reconstructs a dns flow and one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_ftp]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=ftp)
description = An event that occurs when sigflow reconstructs a ftp flow and logged its metadata.

[sigflow_alert_ftp]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=ftp)
description = An event that occurs when sigflow reconstructs a ftp flow and one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_http]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=http)
description = An event that occurs when sigflow reconstructs a http flow and logged its metadata.

[sigflow_alert_http]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=http)
description = An event that occurs when sigflow reconstructs a http flow and one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_ikev2]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=ikev2)
description = An event that occurs when sigflow reconstructs a ikev2 flow and logged its metadata.

[sigflow_alert_ikev2]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=ikev2)
description = An event that occurs when sigflow reconstructs a ikev2 flow and one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_krb5]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=krb5)
description = An event that occurs when sigflow reconstructs a krb5 flow and logged its metadata.

[sigflow_alert_krb5]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=krb5)
description = An event that occurs when sigflow reconstructs a krb5 flow and one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_modbus]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=modbus)
description = An event that occurs when sigflow reconstructs a modbus flow and logged its metadata.

[sigflow_alert_modbus_alert]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=modbus)
```

(continues on next page)

(continued from previous page)

```
description = An event that occurs when sigflow reconstructs a modbus flow and one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_nfs]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=nfs)
description = An event that occurs when sigflow reconstructs a nfs flow and logged its metadata.

[sigflow_alert_nfs]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=nfs)
description = An event that occurs when sigflow reconstructs an nfs flow and one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_ntp]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=ntp)
description = An event that occurs when sigflow reconstructs a ntp flow and logged its metadata.

[sigflow_alert_ntp]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=ntp)
description = An event that occurs when sigflow reconstructs an ntp flow and one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_smb]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=smb)
description = An event that occurs when sigflow reconstructs a smb flow and logged its metadata.

[sigflow_alert_smb]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=smb)
description = An event that occurs when sigflow reconstructs a smb flow and one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_smtp]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=smtp)
description = An event that occurs when sigflow reconstructs a smtp flow and logged its metadata.

[sigflow_alert_smtp]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=smtp)
description = An event that occurs when sigflow reconstructs a smtp flow and one of its rules matched the content of this flow.
color = et_red

[sigflow_meta_ssh]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=ssh)
description = An event that occurs when sigflow reconstructs a ssh flow and logged its metadata.

[sigflow_alert_ssh]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=ssh)
description = An event that occurs when sigflow reconstructs a ssh flow and one of its rules
```

(continues on next page)

(continued from previous page)

```
↪matched the content of this flow.
color = et_red

[sigflow_meta_tftp]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=tftp)
description = An event that occurs when sigflow reconstructs a tftp flow and logged its␣
↪metadata.

[sigflow_alert_tftp]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=tftp)
description = An event that occurs when sigflow reconstructs a tftp flow and one of its rules␣
↪matched the content of this flow.
color = et_red

[sigflow_meta_tls]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=tls)
description = An event that occurs when sigflow reconstructs a tls flow and logged its␣
↪metadata.

[sigflow_alert_tls]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=tls)
description = An event that occurs when sigflow reconstructs a tls flow and one of its rules␣
↪matched the content of this flow.
color = et_red

[sigflow_unknown_alert]
search = (sourcetype=gw:gcenter:101:sigflow* event_type=alert (app_proto=failed OR NOT app_
↪proto=*))
description = An event that occurs when sigflow reconstructs the flow of an unknown protocol,␣
↪and one of its rules matched the content of this flow.
color = et_red

[sigflow_other]
search = (sourcetype=gw:gcenter:101:sigflow* type=suricata NOT event_type IN (netflow,
↪fileinfo,alert,dcerpc,dhcp,dnp3,dns,ftp,http,ikev2,krb5,modbus,nfs,ntp,smb,smtp,ssh,tftp,
↪tls))
description = An event that occurs when sigflow reconstructs the flow of a protocol not␣
↪expected by this add-on.
color = et_blue
```

Events related to the DGA DETECT machine learning engine:

```
[dgadetect_clean]
search = (sourcetype=gw:gcenter:101:sigflow:meta dga_probability=* severity=0)
description = An event that occurs when dgadetect find that a domain name is not suspicious␣
↪(likeky not generated by a Domain Generation Algorithm). This eventtype overlaps the␣
↪sigflow:dns:meta eventtype.

[dgadetect_suspicious]
search = (sourcetype=gw:gcenter:101:sigflow:meta dga_probability=* severity=1)
description = An event that occurs when dgadetect finds that a domain name is suspicious␣
↪(likely generated by a Domain Generation Algorithm).
color = et_red
```

Codebreaker engine related events:

```
[codebreaker_shellcode_expoit]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_type=shellcode␣
↪state=Exploit)
description = An event that occurs when codebreaker detects a shellcode.
color = et_red

[codebreaker_shellcode_suspicious]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_type=shellcode␣
↪state=Suspicious)
description = An event that occurs when codebreaker suspects it has potentially detected a␣
↪shellcode.
color = et_orange

[codebreaker_shellcode_other]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_type=shellcode NOT␣
↪state IN ('Suspicious','Exploit'))
description = An event that occurs when codebreaker returns a code indicating an exception or␣
↪a failure in its shellcode analysis.
color = et_blue

[codebreaker_powershell_expoit]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_type=powershell␣
↪state=Exploit)
description = An event that occurs when codebreaker detects an exploit in a powershell.
color = et_red

[codebreaker_powershell_suspicious]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_type=powershell␣
↪state=Suspicious)
description = An event that occurs when codebreaker suspects it has potentially detected a␣
↪suspicious powershell.
color = et_orange

[codebreaker_powershell_other]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_type=powershell NOT␣
↪state IN ('Suspicious','Exploit'))
description = An event that occurs when codebreaker returns a code indicating an exception or␣
↪a failure in its powershell analysis.
color = et_blue
```

33.3.4.4 tags.conf

This file enables associating tags with the events defined in `eventtype.conf`. These tags enable these events to be fed into Splunk's `Common Information Model`. The default associations are minimal. They must be adapted to your use of data models.

```
[eventtype=malcore_clean]
attack = enabled
malware = enabled

[eventtype=malcore_infected]
attack = enabled
malware = enabled

[eventtype=malcore_suspicious]
attack = enabled
```

(continues on next page)

(continued from previous page)

```
malware = enabled

[eventtype=malcore_other]
attack = enabled
malware = enabled

[eventtype=retroact_clean]
attack = enabled
malware = enabled

[eventtype=retroact_infected]
attack = enabled
malware = enabled

[eventtype=retroact_suspicious]
attack = enabled
malware = enabled

[eventtype=retroact_other]
attack = enabled
malware = enabled

[eventtype=sigflow_netflow]
communicate = enabled
network = enabled

[eventtype=sigflow_fileinfo_stored]
communicate = enabled
network = enabled

[eventtype=sigflow_fileinfo_not_stored]
communicate = enabled
network = enabled

[eventtype=sigflow_meta_dcerpc]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_dcerpc]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_dhcp]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_dhcp]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_dnp3]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_dnp3]
attack = enabled
```

(continues on next page)

(continued from previous page)

```
ids = enabled

[eventtype=dgadetect_clean]
communicate = enabled
network = enabled

[eventtype=dgadetect_suspicious]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_dns]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_dns]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_ftp]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_ftp]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_http]
communicate = enabled
network = enabled
web = enabled

[eventtype=sigflow_alert_http]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_ikev2]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_ikev2]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_krb5]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_krb5]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_modbus]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_modbus_alert]
```

(continues on next page)

(continued from previous page)

```
attack = enabled
ids = enabled

[eventtype=sigflow_meta_nfs]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_nfs]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_ntp]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_ntp]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_smb]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_smb]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_smtp]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_smtp]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_ssh]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_ssh]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_tftp]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_tftp]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_tls]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_tls]
```

(continues on next page)

(continued from previous page)

```
attack = enabled
ids = enabled

[eventtype=sigflow_unknown_alert]
attack = enabled
ids = enabled

[eventtype=sigflow_other]
communicate = enabled
network = enabled

[eventtype=codebreaker_shellcode_expoit]
attack = enabled
malware = enabled

[eventtype=codebreaker_shellcode_suspicious]
attack = enabled
malware = enabled

[eventtype=codebreaker_shellcode_other]
attack = enabled
malware = enabled

[eventtype=codebreaker_powershell_expoit]
attack = enabled
malware = enabled

[eventtype=codebreaker_powershell_suspicious]
attack = enabled
malware = enabled

[eventtype=codebreaker_powershell_other]
attack = enabled
malware = enabled
```

Chapter 34

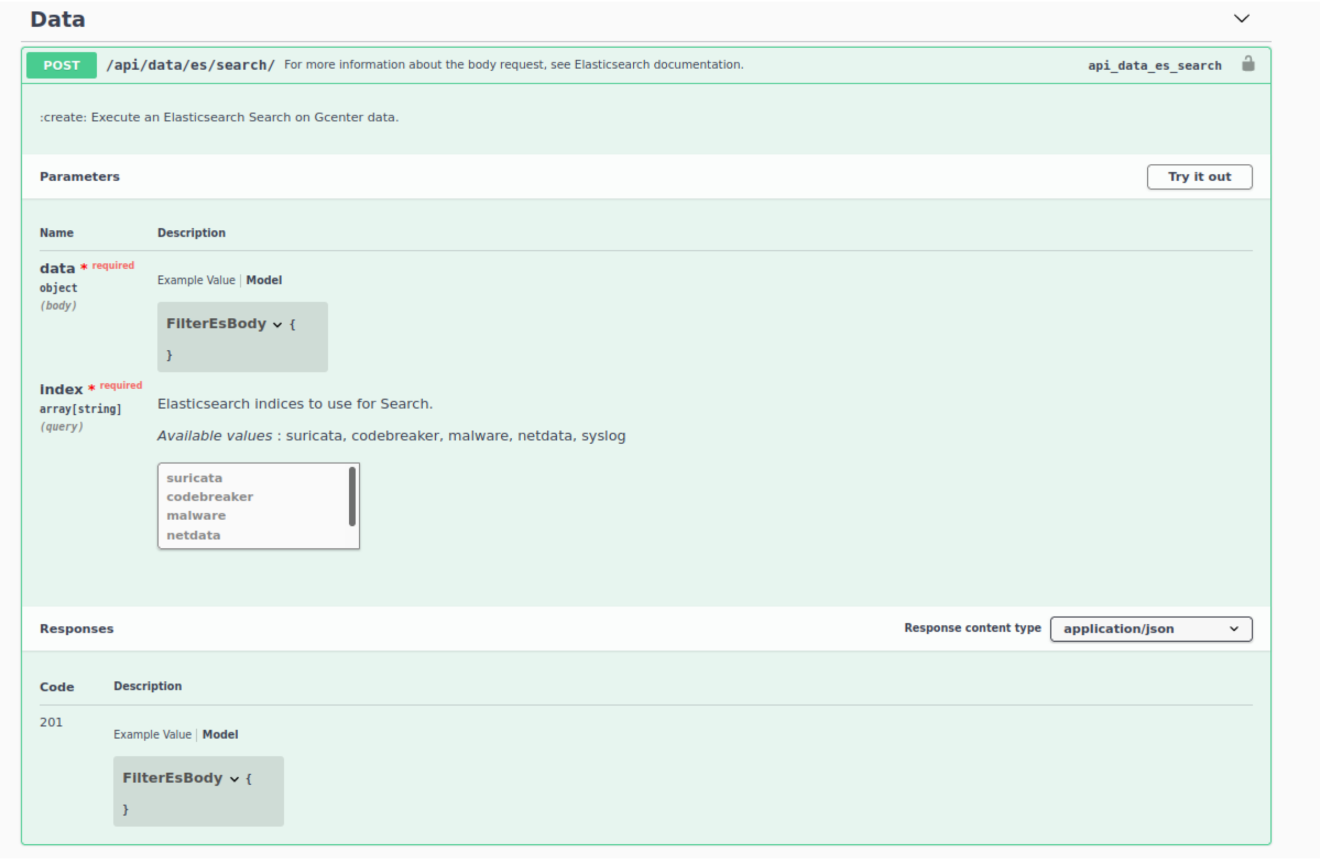
Using the GCENTER API

It can be used in three different ways:

- *Via SWAGGER*
- Via CURL](#use-via-curl)
- Via Package python](#use-via-package-python)

34.1 Use via swagger

By connecting to your GCenter, access the URL **https://hostnameGCENTER/docs/swagger/** You will be able to access the documentation of all our API endpoints.



Data

POST /api/data/es/search/ For more information about the body request, see Elasticsearch documentation. api_data_es_search

:create: Execute an Elasticsearch Search on Gcenter data.

Parameters

Name	Description

data * required
object
(body)
	Example Value | Model
	FilterEsBody {
	}

index * required array[string] *(query)*	Elasticsearch indices to use for Search. *Available values* : suricata, codebreaker, malware, netdata, syslog suricata codebreaker malware netdata

Responses

Response content type: application/json

Code	Description

201	Example Value | Model
	FilterEsBody {
	}

By clicking on the "try it out" button, you can directly test requests. The tool will also generate queries for you to use with curl.

Note:

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

34.2 Use via CURL

For a user who is called **username** and has **operator** rights**.

Retrieving 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
```

Response:

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

The expiration date is determined by the duration set in *Administrators > Configuration > Session age settings* in the GCenter webui

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 request that queries elasticsearch on its suricata* indexes and retrieves 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
```

34.3 Use via python package

This package is a python library implementing many of the endpoints of the GCenter API.

GCenter API package: gwapi-master.tar.gz

34.3.1 Installation

The prerequisites:

- python>=3.5
- requests==2.25.1
- urllib3==1.26.6
- packaging==20.9

The package installation is achieved with the pip utility:

```
pip3 install gwapi.tar.gz
```

34.3.2 Use

34.3.2.1 Import

To use the library, simply import the gwapi package:

```
>>> import gwapi
```

34.3.2.2 Documentation

To display the documentation for any given function:

```
>>> help(gwapi.GcenterApi.auth)
Help on auth function in gwapi.api module:

auth(self, user: 'str', password: 'str') -> 'bool'
    Authentication through the Gcenter API.

    Returns:
        Return true if authenticated.

    Raises:
        RequestException: If status_code!= 200.
```

34.3.2.3 List the library functions

To list all of the library's functions:

```
>>> for func in [func for func in dir(gwapi.GcenterApi) if callable(getattr(gwapi.GcenterApi,␣
↪func)) and not func.startswith("__") and not func.startswith("_")]:
...     print(func)
apply_gcap
auth
...
```

34.3.2.4 Authentication

All API endpoints require authentication.

Authenticate via the GCenter API:

```
>>> api = gwapi.GcenterApi(ip="X.X.X.X", version="2.5.3.101")
>>> api.auth(user="username", password="password")
True
```

34.3.2.5 Elasticsearch query

The elasticsearch API alone is implemented via the GCenter API.

Example of elasticsearch queries via the API:

- Number/List of files reconstructed by gcap over a 24 hour period:

```
query = {
  "size": 10
  "query": {
    "bool": {
      "must": {
        "match": {
         "fileinfo.stored": "true"
        }
      },
      "filter": {
        "range": {
          "@timestamp": {
              "gte": "now-24h",
              "lte": "now"
          }
        }
      }
    }
  }
}
api.get_es_query(index="suricata", query=query)['hits']['hits']
api.get_es_count(index="suricata", query=query)
```

- Number/List of malcore alerts in order of severity over a 24-hour period:

```
query = {
  "size": 10
  "query": {
    "bool": {
      "must": {
        "match": {
         "event_type": "malware"
        }
      },
      "filter": {
        "range": {
          "@timestamp": {
              "gte": "now-24h",
              "lte": "now"
          }
```

(continues on next page)

(continued from previous page)

```
        }
      }
    }
  },
  "sort": {
    "severity": "desc"
  }
}
api.get_es_query(index="malware", query=query)['hits']['hits']
api.get_es_count(index="malware", query=query)
```

- **Number/List of shellcode alerts in order of severity over a 24-hour period:**

```
query = {
  "size": 10
  "query": {
    "bool": {
      "must": {
        "match": {
         "event_type": "shellcode"
        }
      },
      "filter": {
        "range": {
          "@timestamp": {
              "gte": "now-24h",
              "lte": "now"
          }
        }
      }
    }
  },
  "sort": {
    "severity": "desc"
  }
}
api.get_es_query(index="codebreaker", query=query)['hits']['hits']
api.get_es_count(index="codebreaker", query=query)
```

- **Number/List of powershell alerts in order of severity over a 24-hour period:**

```
query = {
  "size": 10
  "query": {
    "bool": {
      "must": {
        "match": {
         "event_type": "powershell"
        }
      },
      "filter": {
        "range": {
          "@timestamp": {
              "gte": "now-24h",
              "lte": "now"
          }
```

(continues on next page)

(continued from previous page)

```
        }
      }
    }
  },
  "sort": {
    "scores.analysis": "desc"
  }
}
api.get_es_query(index="codebreaker", query=query)['hits']['hits']
api.get_es_count(index="codebreaker", query=query)
```

- **Number/list of sigflow alerts in order of severity over a 24-hour period:**

```
query = {
  "size": 10
  "query": {
    "bool": {
      "must": {
        "match": {
         "event_type": "alert"
        }
      },
      "filter": {
        "range": {
          "@timestamp": {
              "gte": "now-24h",
              "lte": "now"
          }
        }
      }
    }
  },
  "sort": {
    "alert.severity": "desc"
  }
}
api.get_es_query(index="suricata", query=query)['hits']['hits']
api.get_es_count(index="suricata", query=query)
```

- **Top 10 signatures of Sigflow alerts:**

```
query = {
  "size": 0
  "query": {
    "match": {
     "event_type": "alert"
    }
  },
  "aggs": {
    "signature": {
      "terms": {
        "field": "alert.signature",
        "order": { "_count": "desc"},
        "size": 10
      }
    }
```

(continues on next page)

(continued from previous page)

```
  }
}
api.get_es_query(index="suricata", query=query)['aggregations']['signature']['buckets']
```

- **Top 10 IP source addresses for Sigflow alerts:**

```
query = {
  "size": 0
  "query": {
    "match": {
     "event_type": "alert"
    }
  },
  "aggs": {
    "src_ip": {
      "terms": {
        "field": "src_ip",
        "order": { "_count": "desc"},
        "size": 10
      }
    }
  }
}
api.get_es_query(index="suricata", query=query)['aggregations']['src_ip']['buckets']
```

- **Top 10 shellcode types:**

```
query = {
  "size": 0
  "query": {
    "match": {
     "event_type": "shellcode"
    }
  },
  "aggs": {
    "sub_type": {
      "terms": {
        "field": "sub_type",
        "order": { "_count": "desc"},
        "size": 10
      }
    }
  }
}
api.get_es_query(index="codebreaker", query=query)['aggregations']['sub_type']['buckets']
```

- **Top 10 malware types:**

```
query = {
  "size": 0
  "query": {
    "match": {
     "event_type": "malware"
    }
  },
  "aggs": {
    "detail_threat_found": {
```

(continues on next page)

(continued from previous page)

```
      "terms": {
        "field": "detail_threat_found",
        "order": { "_count": "desc"},
        "size": 10
      }
    }
  }
}
api.get_es_query(index="malware", query=query)['aggregations']['detail_threat_found']['buckets
↪']
```

- **Ranking of the source/ destination IP addresses of Sigflow alerts in descending order:**

```
query = {
  "size": 0
  "query": {
    "match": {
     "event_type": "alert"
    }
  },
  "aggs": {
    "couple": {
      "composite": {
        "sources":[
          {
            "src_ip":{
              "terms":{
                "field": "src_ip",
                "order": "desc"
              }
            }
          },
          {
            "dest_ip":{
              "terms":{
                "field": "dest_ip",
                "order": "desc"
              }
            }
          }
        ],
        "size": 65535
      }
    }
  }
}
api.get_es_query(index="suricata", query=query)['aggregations']['couple']['buckets']
```

- **Count/List the last 10 alerts having the status Infected in malcore:**

```
>>> query = {
...   "size": 10
...   "query": {
...     "match": {
...       "state": "Infected"
...     }
```

(continues on next page)

(continued from previous page)

```
...   }
... }
>>> api.get_es_query(index="malware", query=query)
[{'_index': 'malware-2021.06.29-000007', '_type': '_doc', '_id': 'uGn0VnoBfk3pKEfjbjFz', '_
↪score': 0.00024064493, '_source': {'timestamp_detected': '2021-06-29T08:37:09.043Z'...}]
>>> api.get_es_count(index="malware", query=query)
4189
```

34.3.2.6 Alertes

The API enables GCenter alerts to be displayed in two forms:

- The latest alerts sent by the Gcaps (sigflow, malcore, codebreaker).
- The last alerts sent by the Gcaps in the form of a cluster: alerts that occurred in the same time frame, i.e. the last hour or the last day for example, and that are all linked to the same IP address.

Retrieve GCenter alerts:

```
# Display alerts in RAW format
>>> from datetime import datetime, timedelta
>>> import json
>>> delta = datetime.utcnow() - timedelta(days=5)
>>> alerts = api.get_gcenter_alerts(date_from=delta.isoformat(),
...                                  date_to=datetime.utcnow().isoformat(),
...                                  gcap_id="all",
...                                  ip="1.1.1.1",
...                                  sort_by="date_asc",
...                                  risk_min=0,
...                                  risk_max=10)
>>> print(json.dumps(alerts, indent=4))
[
    {
        "id": "2021-06-29T08:28:21.932Z",
        "name": "ASCII text, with very long lines",
        "date": "2021-06-29T08:27:21",
        "gcap": {
            "id": 1
            "fqdn": "gcap.example.com",
            "is_paired": true
        },
        "description": "Infected: JS/Downloader.S200, JS:Trojan.JS.Downloader.AZ, JS/Downldr.
↪CZ!Eldorado, JS/Kryptik.AYN trojan, JS:Trojan.JS.Downloader.AZ (B)",
        "src_ip": "1.1.1.1",
        "dest_ip": "2.2.2.2",
        "risk": 13
        "type": "malcore"
    },
    {
        "id": "2021-06-29T08:31:22.816Z",
        "name": "ASCII text, with very long lines",
        "date": "2021-06-29T08:30:53",
        "gcap": {
            "id": 1
            "fqdn": "gcap.example.com",
            "is_paired": true
        },
```

(continues on next page)

(continued from previous page)

```
        "description": "Infected: JS/Downloader.S200, JS:Trojan.JS.Downloader.AZ, JS/Downldr.
↪CZ!Eldorado, JS/Kryptik.AYN trojan, JS:Trojan.JS.Downloader.AZ (B)",
        "src_ip": "1.1.1.1",
        "dest_ip": "2.2.2.2",
        "risk": 13
        "type": "malcore"
    }
]
# Display alerts in Cluster format
>>> alerts = api.get_gcenter_clusters_alerts(date_from=delta.isoformat(),
...                                 date_to=datetime.utcnow().isoformat(),
...                                 gcap_id="all",
...                                 ip="1.1.1.1",
...                                 sort_by="src",
...                                 frequency="hour")
>>> print(json.dumps(alerts, indent=4))
[
    {
        "id": "1.1.1.1-2021-06-29T08:00:00.000Z",
        "ip": "1.1.1.1",
        "number_alerts": 1
        "average_risk": 1.0
        "risk_score": 1
        "date": "2021-06-29T08:00:00",
        "description": "The cluster 1.1.1.1 has 1 alert registered the 2021-06-29 08:00:00␣
↪(malcore and codebreaker: 1)",
        "malcore_codebreaker": 1
        "type_ip": "src",
        "gcap": {
            "id": 1
            "fqdn": "gcap.example.com",
            "is_paired": true
        }
    }
]
```

34.3.2.7 Data export

Data export includes netdata and syslog functions.

Netdata export configuration:

```
# Netdata export configuration
>>> api.set_netdata(enabled=True, ip="10.10.10.10", port=80, iface="mgmt0", key="xxxxxxxx-
↪xxxx-xxxx-xxxx-xxxxxxxxxxxx")
# Disabling Netdata export
>>> api.set_netdata(enabled=False)
```

Syslog export configuration 1:

```
# Configuration of the syslog export general tab.
>>> api.set_syslog_general(id=1, hostname="10.10.10.10", port=514)
# Configuring filters for syslog export 1.
>>> api.clear_syslog_filters(id=1)
>>> api.set_syslog_filters(id=1, ips=["10.10.10.10"], gcap=[gcap_choice], protocols=["dns",
↪"http"])
```

(continues on next page)

(continued from previous page)

```
# Configuring certificates for syslog export 1. The certificates must be in PEM format.
>>> api.set_syslog_certificate(id=1, cert="-----BEGIN CERTIFICATE-----...", cert_key="-----
↪BEGIN RSA PRIVATE KEY-----", ca="-----BEGIN CERTIFICATE------...")
# Disabling syslog export 1.
>>> api.disable_syslog(id=1)
```

34.3.2.8 Gcap Profiles

The Gcap Profiles section of the Operators menu is partially configurable via the API. The "Detection Rulesets" and "Base Variables" sections are configurable.

To apply changes to gcap:

```
>>> api.apply_gcap(gcap_id=1)
{'detail': 'Gcap config file updated with success'}
```

Functions not requiring any changes to be applied:

```
# List the Gcaps associated with GCenter
>>> api.get_gcaps()
[{'id': 1, 'fqdn': 'gcap.example.com', 'is_paired': True, 'last_rule_update': '2021-07-
↪01T13:42:03.709091', 'status': 'online'}]
# Display the Gcap data associated with GCenter
>>> api.get_gcap_by_id(gcap_id=1)
{'id': 1, 'fqdn': 'gcap.example.com', 'is_paired': True, 'last_rule_update': '2021-07-
↪01T13:42:03.709091', 'status': 'online'}
# Display the template associated with Gcaps
>>> api.get_gcap_template()
{'profile': 'intuitio'}
# Change the template associated with the Gcaps among the values: ["minimal", "balanced", "lpm
↪", "paranoid", "intuitio"]
>>> api.set_gcap_template(template="balanced")
{'profile': 'balanced'}
# Display the Gcap's interfaces
>>> api.get_gcap_interfaces(gcap_id=1)
[
    {
        "enabled": true,
        "name": "mon0",
        "mtu": 1500
        "is_cluster": false,
        "cluster_interfaces": [
            "mon0"
        ]
    }
]
# Display the single-tenant configuration
>>> api.get_gcap_single_tenant(gcap_id=1)
{'enabled': False, 'enable_shellcode': True, 'enable_powershell': True}
# Display the multi-tenant configuration
>>> api.get_gcap_multi_tenant(gcap_id=1)
{'enabled': True, 'ruleset': [{'id': 502, 'ruleset': 3, 'codebreaker_shellcode': True,
↪'codebreaker_powershell': True, 'name': 'mon1'}], 'is_by_interface': True}
>>> api.get_gcap_profile(gcap_id=1)
{'files_hash': ['md5'], 'max_pending_packets': 4096, 'file_store_stream_depth_enable': True,
↪'file_store_stream_depth_mb': 10, 'stream_memcap_b': 32000000000, 'stream_prealloc_sessions
```

(continues on next page)

(continued from previous page)

```
↪': 1000000, 'stream_reassembly_memcap_b': 16000000000, 'stream_reassembly_depth_mb': 10,
↪'stream_reassembly_toserver_chunk_size_b': 2560, 'stream_reassembly_toclient_chunk_size_b':␣
↪2560, 'flow_memcap': 17179869184, 'flow_prealloc': 1048576, 'stream_reassembly_randomize_
↪chunk_size': True, 'xff_enable': True, 'xff_mode': 'extra-data', 'xff_deployment': 'reverse
↪', 'xff_header': 'X-Forwarded-For', 'payload': True, 'payload_buffer_size': 4096, 'payload_
↪printable': True, 'packet': True, 'file_resend_interval': 600, 'http_body': False, 'http_
↪body_printable': False, 'ftp_memcap': 10485760, 'smb_stream_depth': 10485760, 'http_enable
↪': True, 'dns_udp_enable': True, 'dns_tcp_enable': True, 'tls_enable': True, 'smtp_enable':␣
↪True, 'smb_enable': True, 'ssh_enable': True, 'netflow_enable': True, 'dnp3_enable': True,
↪'ftp_enable': True, 'dhcp_enable': True, 'ikev2_enable': True, 'krb5_enable': True, 'nfs_
↪enable': True, 'tftp_enable': True, 'parsing_dcerpc_enabled': 1, 'parsing_dnp3_enabled': 1,
↪'parsing_dns_udp_enabled': 1, 'parsing_dns_tcp_enabled': 1, 'parsing_ftp_enabled': 1,
↪'parsing_http_enabled': 1, 'parsing_modbus_enabled': 1, 'parsing_smb_enabled': 1, 'parsing_
↪smtp_enabled': 1, 'parsing_ssh_enabled': 1, 'parsing_tls_enabled': 1, 'parsing_dhcp_enabled
↪': 1, 'parsing_ikev2_enabled': 1, 'parsing_krb5_enabled': 1, 'parsing_nfs_enabled': 1,
↪'parsing_ntp_enabled': 1, 'parsing_tftp_enabled': 1}
# Show vlans configuration
>>> api.get_gcap_vlans(gcap_id=1)
[{'id': 496, 'ruleset': 3, 'codebreaker_shellcode': True, 'codebreaker_powershell': True,
↪'name': 'default'}, {'id': 497, 'ruleset': 3, 'codebreaker_shellcode': True, 'codebreaker_
↪powershell': True, 'name': '120'}, {'id': 498, 'ruleset': 3, 'codebreaker_shellcode': False,
↪ 'codebreaker_powershell': False, 'name': '110'}]
```

Functions requiring changes to be applied:

```
# Configure the single-tenant
>>> api.set_gcap_single_tenant(
...     gcap_id=1,
...     enabled=True,
...     ruleset_id=3,
...     shellcode=True,
...     powershell=True
... )
{'enabled': True, 'ruleset': 3, 'enable_shellcode': True, 'enable_powershell': True}
# Configure multi-tenant per interface. It must be done for each interface.
>>> api.set_gcap_multi_tenant_interface(
...     gcap_id=1,
...     interface="mon0",
...     ruleset_id=3,
...     shellcode=True,
...     powershell=True
... )
{'enabled': True, 'ruleset': [{'ruleset': 3, 'codebreaker_shellcode': True, 'codebreaker_
↪powershell': True, 'name': 'mon0'}], 'is_by_interface': True}
# Remove multi-tenant configuration (vlans + interfaces)
>>> api.reset_gcap_tenant(gcap_id=1)
True
# Configure the gcap variables. For the moment only the logging and protocol parsing␣
↪configuration is implemented.
>>> PARSING_PROTOS = [
...     "dcerpc", "dhcp", "dnp3", "dns_udp", "dns_tcp", "ftp",
...     "http", "ikev2", "krb5", "modbus", "nfs", "ntp", "smb",
...     "smtp", "ssh", "tftp", "tls"
... ]
>>> LOGGING_PROTOS = [
...     "dhcp", "dnp3", "dns_udp", "dns_tcp", "ftp", "http", "ikev2",
```

(continues on next page)

(continued from previous page)

```
...     "krb5", "netflow", "nfs", "smb", "smtp", "ssh", "tftp", "tls"
... ]
>>> for proto in PARSING_PROTOS:
...     api.set_gcap_profile(gcap_id=1, proto=proto, parsing=True, logging=None)
>>> for proto in LOGGING_PROTOS:
...     api.set_gcap_profile(gcap_id=1, proto=proto, parsing=None, logging=True)
# Add a vlan.
>>> api.set_gcap_vlan(
...     gcap_id=1,
...     vlan="110",
...     ruleset_id=3,
...     shellcode=False,
...     powershell=False
... )
{'id': 495, 'ruleset': 3, 'codebreaker_shellcode': False, 'codebreaker_powershell': False,
↪'name': '110'}
# Configure multi-tenant per vlan
>>> api.set_gcap_multi_tenant_vlan(
...     gcap_id=1,
...     vlan="110",
...     ruleset_id=3,
...     shellcode=False,
...     powershell=False
... )
{'enabled': True, 'ruleset': [{'ruleset': 3, 'codebreaker_shellcode': True, 'codebreaker_
↪powershell': True, 'name': 'default'}, {'ruleset': 3, 'codebreaker_shellcode': True,
↪'codebreaker_powershell': True, 'name': '120'}, {'ruleset': 3, 'codebreaker_shellcode':␣
↪False, 'codebreaker_powershell': False, 'name': '110'}], 'is_by_interface': False}
# Delete a vlan
>>> api.delete_gcap_vlan(
...     gcap_id=1,
...     vlan="110"
... )
True
# Modify the vlan configuration. The vlan must be deleted and recreated.
>>> api.delete_gcap_vlan(
...     gcap_id=1,
...     vlan="110"
... )
True
>>> api.set_gcap_vlan(
...     gcap_id=1,
...     vlan="110",
...     ruleset_id=3,
...     shellcode=False,
...     powershell=False
... )
{'id': 495, 'ruleset': 3, 'codebreaker_shellcode': False, 'codebreaker_powershell': False,
↪'name': '110'}
```

34.3.2.9 Licence

It is possible to configure and view the GCenter license via the API.

Configure the GCenter license:

```
>>> api.get_serial_number()
'XXXXXXX'
>>> api.get_licence()
{'key': 'XXX...', 'license_expiry_alert': 90, 'details': {'antimalware_engines': 16, 'cie':␣
↪False, 'codebreaker': True, 'days_left': 7, 'end_date': '2021-07-08', 'expired': False,
↪'full': True, 'license_expiry_alert': 90, 'machine_learning': True, 'malcore': True, 'max_
↪gcaps': 100, 'model': '', 'nozomi': False, 'registered_mail': 'trial@gatewatcher.com',
↪'registered_owner': 'Trial', 'retroact': True, 'serial_number': 'XXX', 'sigflow': True,
↪'start_date': '2021-07-01', 'valid': True}}
>>> api.set_licence(key="XXX", expiry_alert=90)
```

34.3.2.10 Network

It is possible to view the network configuration of the GCenter via the API.

```
# Display the configuration of all GCenter network interfaces
>>> api.get_gcenter_interfaces()
[{'name': 'mgmt0', 'fullname': 'mgmt0 - 3.3.3.3', 'hostname': '3.3.3.3'}, {'name': 'vpn0',
↪'fullname': 'vpn0 - 4.4.4.4', 'hostname': '4.4.4.4'}, {'name': 'icap0', 'fullname': 'icap0 -
↪ 5.5.5.5', 'hostname': '5.5.5.5'}, {'name': 'sup0', 'fullname': 'sup0 - 6.6.6.6', 'hostname
↪': '6.6.6.6'}]
# Display the configuration of all GCenter network interfaces
>>> api.get_gcenter_interface_by_name("mgmt0")
{'name': 'mgmt0', 'fullname': 'mgmt0 - 3.3.3.3', 'hostname': '3.3.3.3'}
```

34.3.2.11 Malcore

It is possible to configure and view the Malcore settings via the API.

```
>>> api.set_malcore_settings(days=10, rescan=3, gbox=False)
>>> api.get_malcore_settings()
{'retroact_number_of_days_between_rescans': 10, 'retroact_number_of_rescan': 3, 'gbox_analysis
↪': False}
```

34.3.2.12 Sigflow

**It is possible to view Sigflow rulesets via the API.

```
# List the rulesets associated with GCenter
>>> api.get_sigflow_rulesets()
[{'id': 3, 'name': 'ALL', 'descr': '', 'created_date': '2021-06-24T13:45:35.627132Z', 'has_
↪files': True}]
# List only the rulesets whose files were generated
>>> api.get_sigflow_rulesets(with_files=True)
[{'id': 3, 'name': 'ALL', 'descr': '', 'created_date': '2021-06-24T13:45:35.627132Z', 'has_
↪files': True}]
# Display the ruleset configuration associated with the GCenter
>>> api.get_sigflow_ruleset_by_id(ruleset_id=3)
{'id': 3, 'name': 'ALL', 'descr': '', 'created_date': '2021-06-24T13:45:35.627132Z', 'has_
↪files': True}
```

34.3.2.13 Status

It is possible to view the status of GCenter components via the API.

Display the status of the GCenter components:

```
# Check that the API is working: no authentication required
>>> api.get_api_status()
True
# Display the GCenter status
>>> api.get_gcenter_status()
{'version': '2.5.3.101-XXXX', 'serial_number': 'XXXXXXX'}
# Display the GCenter's overall status and associated errors
>>> api.get_healthchecks_status()
{'healthy': 'Bad', 'errors': ['Malware Analysis Engine has one or more issues: Last known␣
↪good status: 2021-06-25T12:58:46.336013']}
# View the update status
>>> api.get_updates_status()
{'status': 'Good', 'errors': []}
# Display the user's authentication status
>>> api.get_user_status()
{'message': 'success', 'authenticated': False}
```

34.3.2.14 User

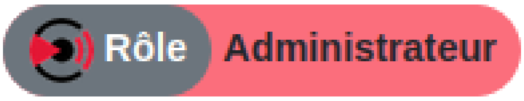
It is possible to view GCenter user data via the API.

Display the GCenter user data:

```
# Display the data of all users
>>> api.get_users()
[{'id': 1, 'username': 'admin', 'roles': [{'name': 'gwrights.gcap_mgmt'}, {'name': 'gwrights.
↪sigflow_mgmt'}, {'name': 'gwrights.user_mgmt'}, {'name': 'gwrights.gcenter_mgmt'}, {'name':
↪'gwrights.common'}, {'name': 'gwrights.dashboards'}, {'name': 'gwrights.samples'}], 'groups
↪': []}, {'id': 2, 'username': 'operator', 'roles': [{'name': 'gwrights.dashboards'}, {'name
↪': 'gwrights.sigflow_mgmt'}, {'name': 'gwrights.common'}, {'name': 'gwrights.samples'}],
↪'groups': [{'id': 2, 'name': 'operators'}]}, {'id': 3, 'username': 'administrator', 'roles
↪': [{'name': 'gwrights.user_mgmt'}, {'name': 'gwrights.common'}, {'name': 'gwrights.gcenter_
↪mgmt'}, {'name': 'gwrights.gcap_mgmt'}], 'groups': [{'id': 1, 'name': 'administrators'}]}]
# Display a user's data
>>> api.get_user_by_id(user_id=1)
{'id': 1, 'username': 'admin', 'roles': [{'name': 'gwrights.gcap_mgmt'}, {'name': 'gwrights.
↪sigflow_mgmt'}, {'name': 'gwrights.user_mgmt'}, {'name': 'gwrights.gcenter_mgmt'}, {'name':
↪'gwrights.common'}, {'name': 'gwrights.dashboards'}, {'name': 'gwrights.samples'}], 'groups
↪': []}
```

Chapter 35

Home Page

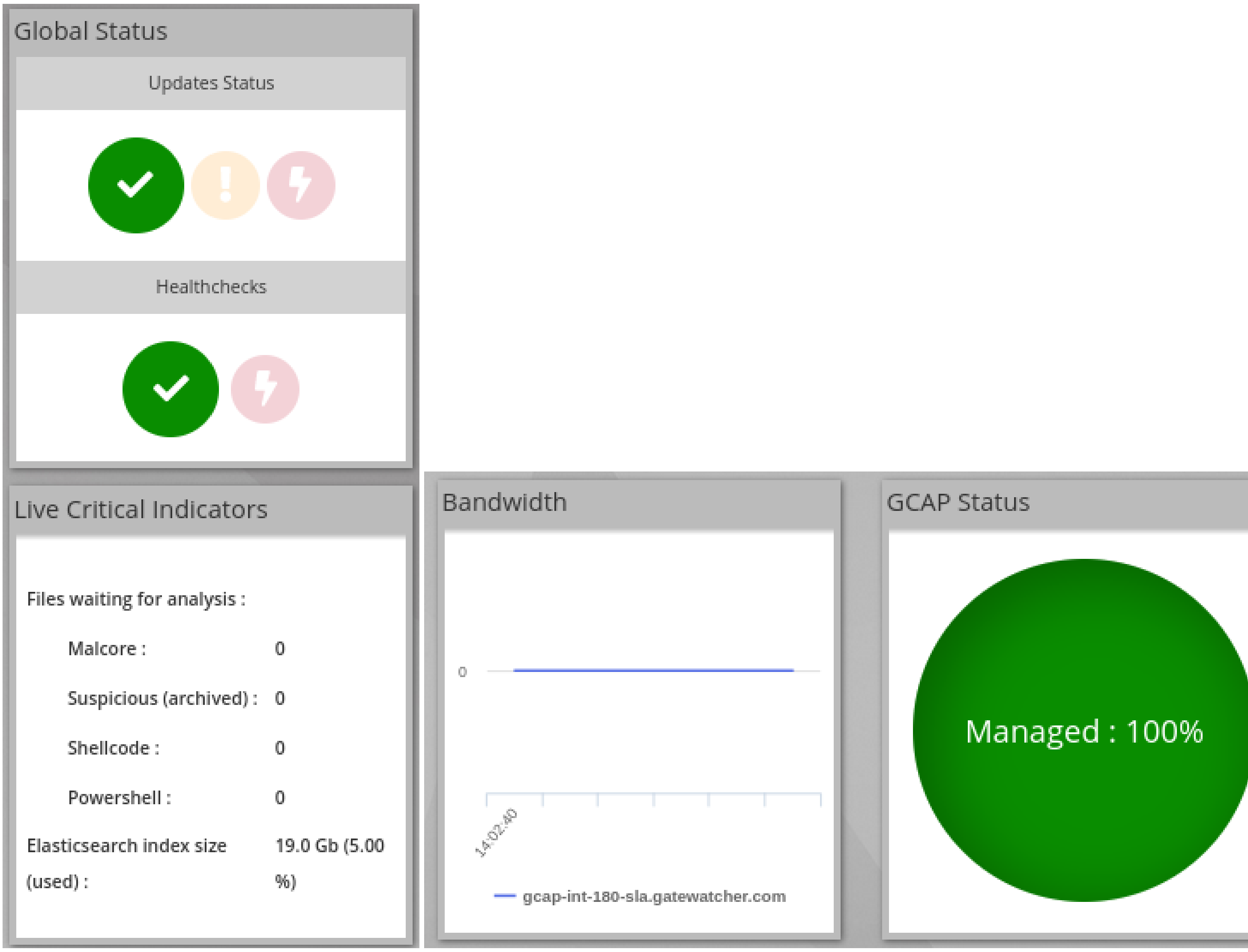


Rôle Administrateur

Menu: Home Page

A quick view of the solution's status is available directly from the *Home Page*. This page can be accessed at any time by clicking on the **Gatewatcher** logo located in the left menu.

It displays the overall status of the **TRACKWATCH** solution as well as the files awaiting analysis. Further down the page, **GCAP** status and update information is also available.



Global Status

Updates Status

Healthchecks

Live Critical Indicators

Files waiting for analysis :

Malcore :	0
Suspicious (archived) :	0
Shellcode :	0
Powershell :	0
Elasticsearch index size (used) :	19.0 Gb (5.00 %)

Bandwidth

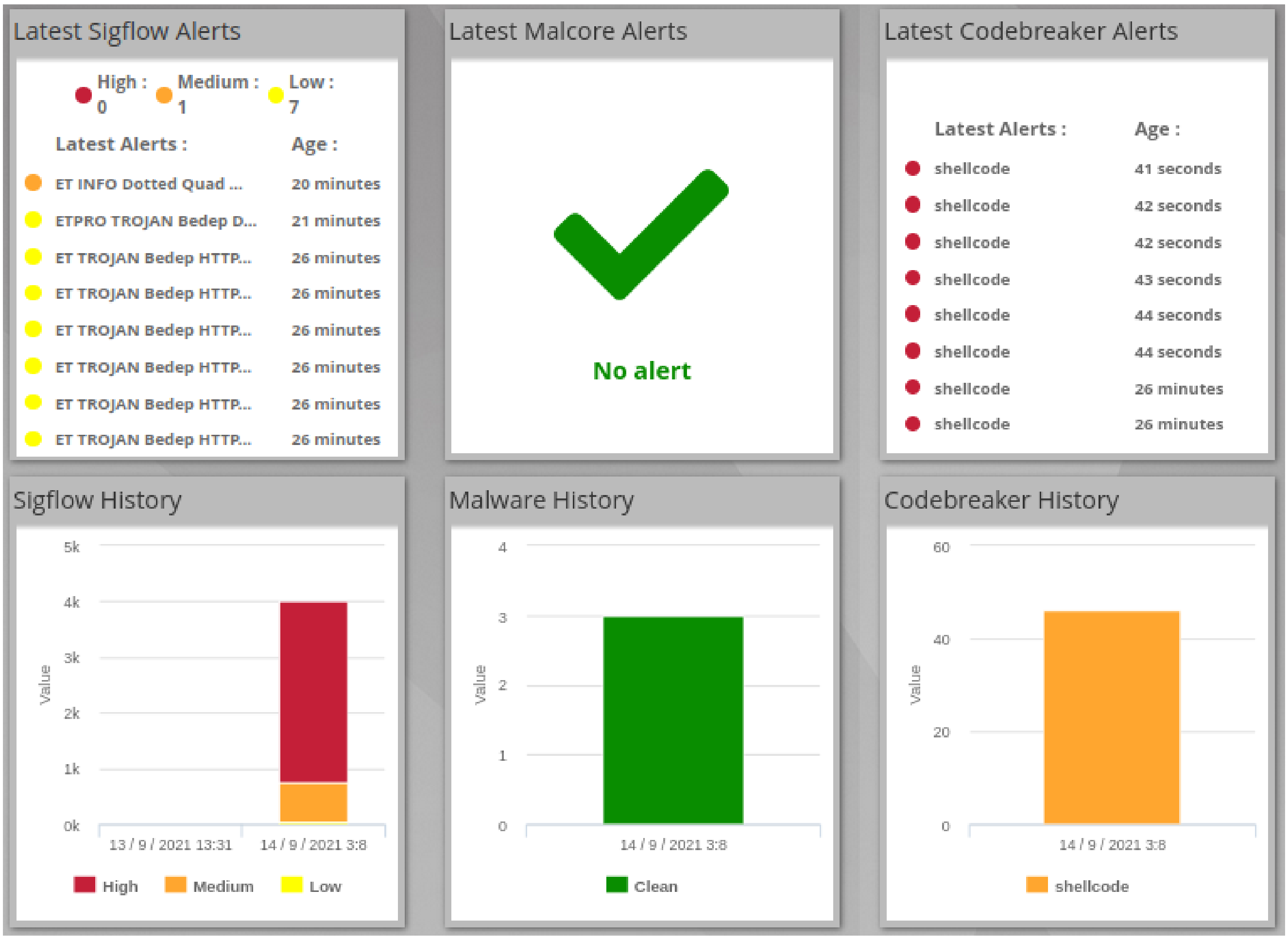
GCAP Status

Managed : 100%

Rôle Opérateur

Menu: Home Page

As an operator, the *Home Page* content will be different. A summary of the latest alerts will be shown.



Latest Sigflow Alerts

● High : 0 ● Medium : 1 ● Low : 7

	Latest Alerts :	Age :
●	ET INFO Dotted Quad ...	20 minutes
●	ETPRO TROJAN Bedep D...	21 minutes
●	ET TROJAN Bedep HTTP...	26 minutes
●	ET TROJAN Bedep HTTP...	26 minutes
●	ET TROJAN Bedep HTTP...	26 minutes
●	ET TROJAN Bedep HTTP...	26 minutes
●	ET TROJAN Bedep HTTP...	26 minutes
●	ET TROJAN Bedep HTTP...	26 minutes

Latest Malcore Alerts

✓ No alert

Latest Codebreaker Alerts

	Latest Alerts :	Age :
●	shellcode	41 seconds
●	shellcode	42 seconds
●	shellcode	42 seconds
●	shellcode	43 seconds
●	shellcode	44 seconds
●	shellcode	44 seconds
●	shellcode	26 minutes
●	shellcode	26 minutes

Chapter 36

Embedded Dashboards

Rôle Administrateur

Menu: Administrators > GCenter > Monitor

From this section, TRACKWATCH administrators are allowed to view real-time information pertaining to the devices.

This interface is used to monitor the **GCenter** in terms of CPU, memory, network, and disk load via dynamic dashboards.

The GATEWATCHER administrator can access information on the monitored services to ensure they are functioning properly:

- Basic host stats
- Malcore stats
- Malcore database stats
- Elastic search stats
- GCENTER global db stats
- Gweb stats
- Live feed service stats
- Network stats

The *Basic host stats* section appears by default. The other sections are visible by clicking on the section name or the **Show** button.

It is possible to hover over the charts to view the measured values. On charts with several plotted values, it is also possible to choose which element will be plotted by clicking on the legend to show or hide them.

In addition, depending on the position of the mouse cursor on any chart, the position on the other charts is also synchronised. This enables you to access all the necessary information at a given time **T**.

⏪ Enables you to move over the chart to the left. This manipulation is possible thanks to a drag to the right with the mouse.

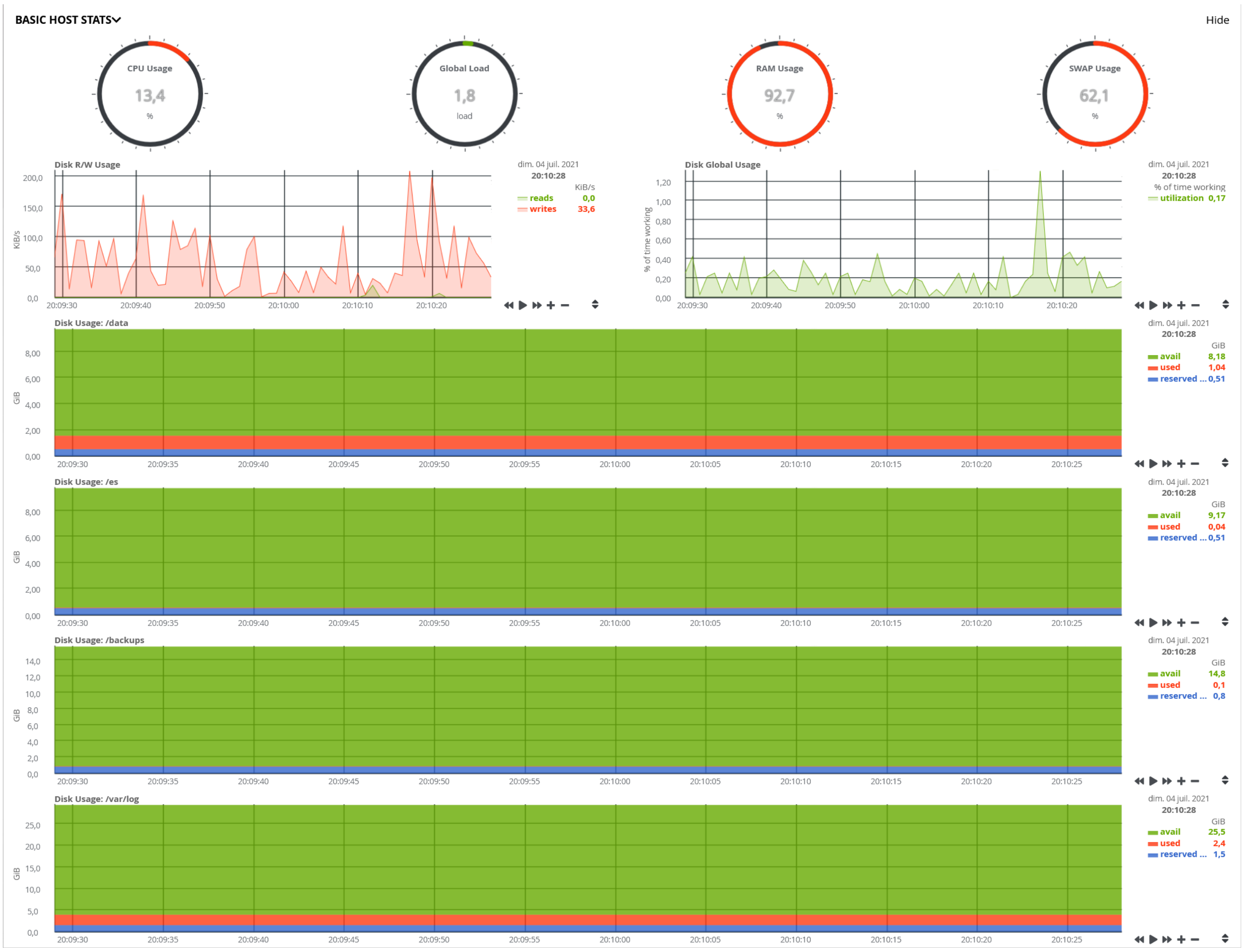
⏩ Enables you to move over the chart to the right. This manipulation is possible thanks to a drag to the left with the mouse.

▶ Enables all charts to be reset to their default auto-refresh setting. The administrator can also double-click on the content of the chart with his mouse.

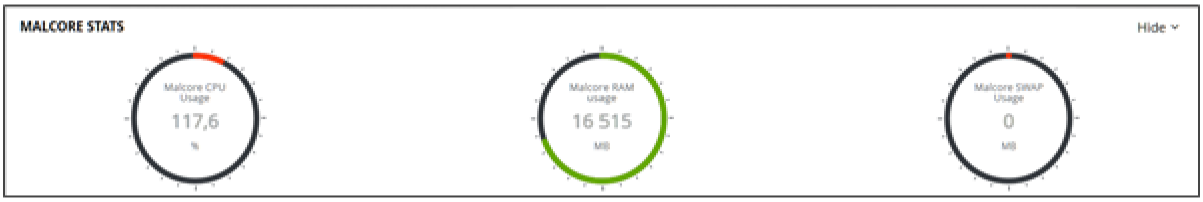
+
− It is possible to zoom into the chart or press Shift and select the area of the chart to zoom in. Zooming is also possible by pressing Shift or Ctrl with the mouse wheel.

⌄
⌃ The administrator can drag with the mouse, using this feature to change the chart vertically. It is possible to double-click to reset between two statuses, the default chart and the one that corresponds to all values.

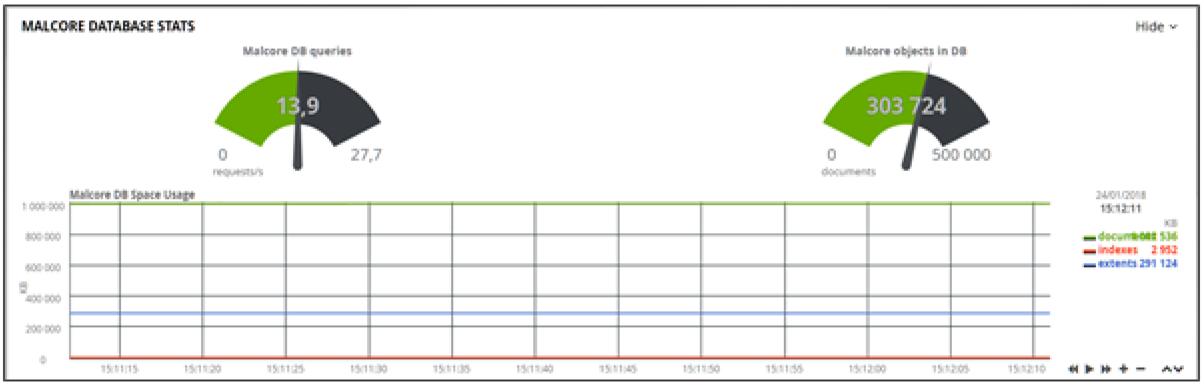
BASIC HOST STATS provides real-time information from the **GCENTER** with overall system indicators such as average CPU occupancy rate, disk writes, and swap occupancy rate. Used, free, and reserved capacity for individual directories are also monitored.



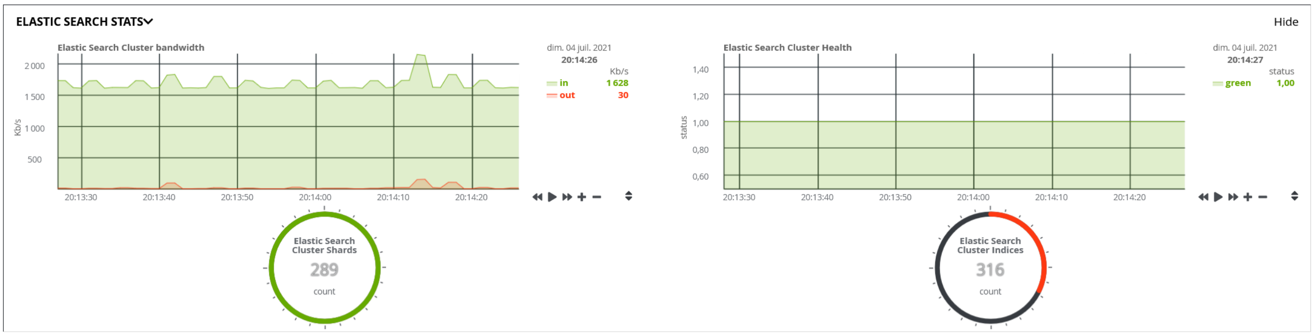
MALCORE STATS provides status information in terms of used CPU, RAM, and SWAP capacity for the MALCORE engine.



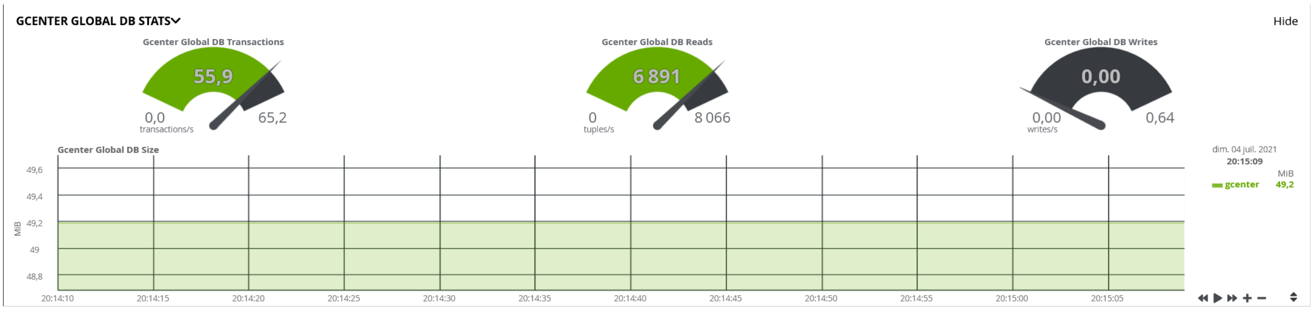
MALCORE DATABASE STATS provides statistical information pertaining to the MALCORE Engine database.



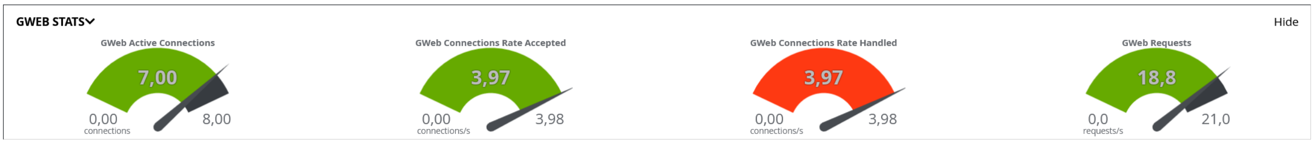
ELASTIC SEARCH STATS provides information on the status of the ElasticSearch cluster. This is responsible for recording and then indexing the data captured by the **GCAP** probe in the **GCENTER**. The cluster bandwidth is monitored.



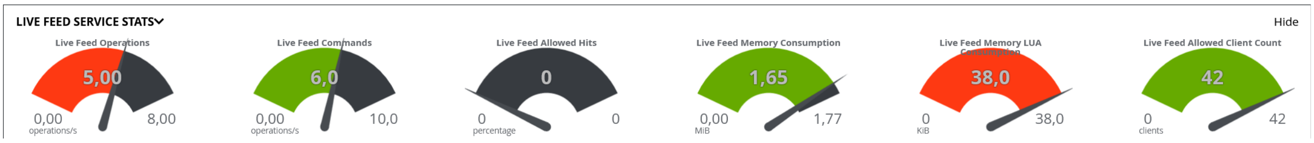
GCENTER GLOBAL DB STATS provides information on how much the **GCENTER** global database is consuming.



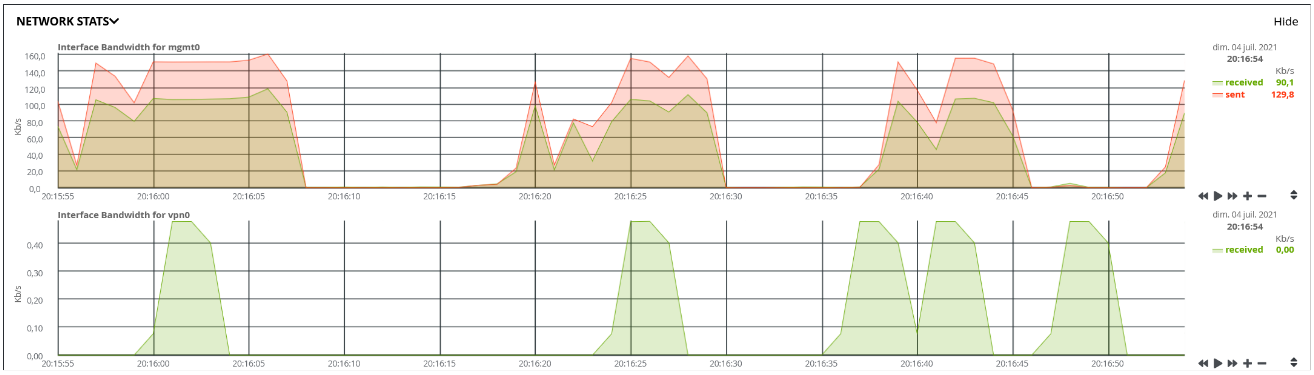
GWEB STATS provides information regarding the **GCENTER**'s Nginx web server.



LIVE FEED SERVICE STATS provides information on all the services comprising the **GCENTER**.



NETWORK STATS provides information on the network interfaces bandwidth connected to the **GCENTER**. The more physical interfaces connected to the equipment, the more tables there will be.


NETWORK STATS
Hide
Interface Bandwidth for mgmt0
Kb/s
160,0
140,0
120,0
100,0
80,0
60,0
40,0
20,0
0,0
20:15:55
20:16:00
20:16:05
20:16:10
20:16:15
20:16:20
20:16:25
20:16:30
20:16:35
20:16:40
20:16:45
20:16:50
dim. 04 juil. 2021
20:16:54
Kb/s
received 90,1
sent 129,8
Interface Bandwidth for vpn0
Kb/s
0,40
0,30
0,20
0,10
0,00
20:15:55
20:16:00
20:16:05
20:16:10
20:16:15
20:16:20
20:16:25
20:16:30
20:16:35
20:16:40
20:16:45
20:16:50
dim. 04 juil. 2021
20:16:54
Kb/s
received 0,00

Chapter 37

Nagios

Rôle Administrateur

Menu: Administrators > GCenter > Configuration > Nagios

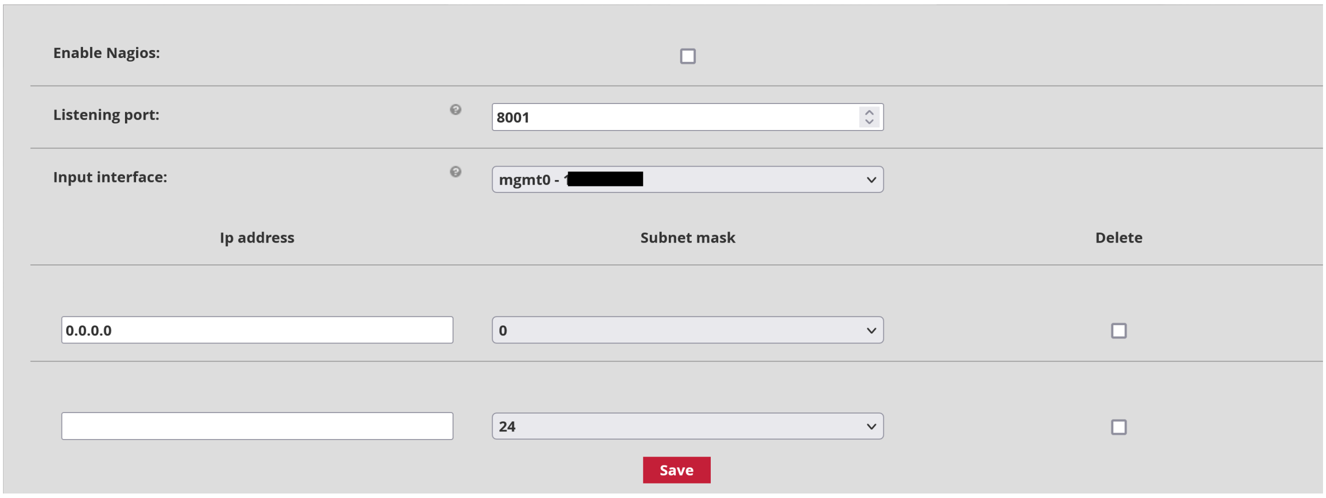
It is thus possible to expose various metrics on a given port in order for the Gcenter to be overseen by a monitoring system such as Nagios, Centreon, Zabbix, or others.

First of all, the service must be activated.

Enable Nagios: allows a third-party server to request metrics regarding the gcenter's operation.

Listening port: is the monitoring interface on which the metrics will be displayed.

Input interface: is the interface on which the **GCENTER** will be listening.



Enable Nagios: □

Listening port: 8001

Input interface: mgmt0 - [redacted]

Ip address	Subnet mask	Delete
0.0.0.0	0	□
	24	□

The following fields enable listing the networks authorised to contact the supervision server (IP address in the form *xxx.xxx.xxx.xxx*) and the associated subnet mask (from *0 to 32*).

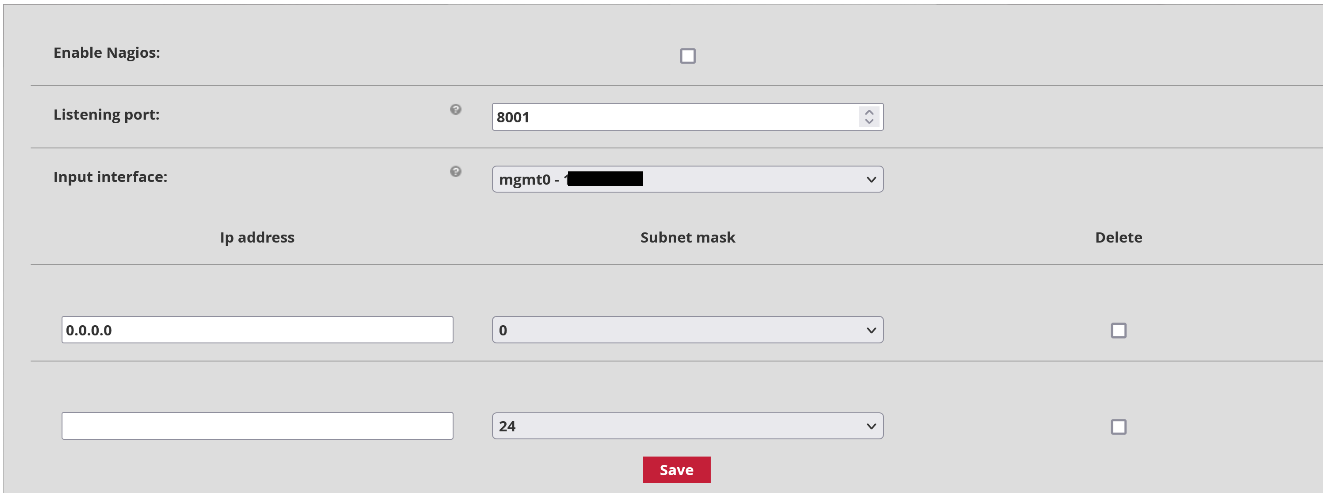
It is thus possible to display a certain number of metrics on a given port in order for it to be *polled* by a monitoring system such as Nagios, Centreon, or Zabbix, etc.

First of all, the service must be activated.

Enable Nagios allows activating the monitoring via a *polling* system.

Listening port: is the monitoring interface on which the metrics will be displayed.

Input interface: is the interface on which the **GCENTER** will be listening.



Enable Nagios: □

Listening port: 8001

Input interface: mgmt0 - [redacted]

Ip address	Subnet mask	Delete
0.0.0.0	0	□
	24	□

The following fields enable listing the IP addresses or networks authorised to contact the supervision server. An IP address, in the form *xxx.xxx.xxx.xxx* , must be entered in the **IP address** field. The subnet mask must be selected with a value in the **Subnet mask** field ranging from *0 to 32*.

Once these values are entered, the administrator can register the addition of the servers by pressing **Save**.

Once this is accomplished, the following *endpoints* will be made available to the monitoring servers

Chapter 38

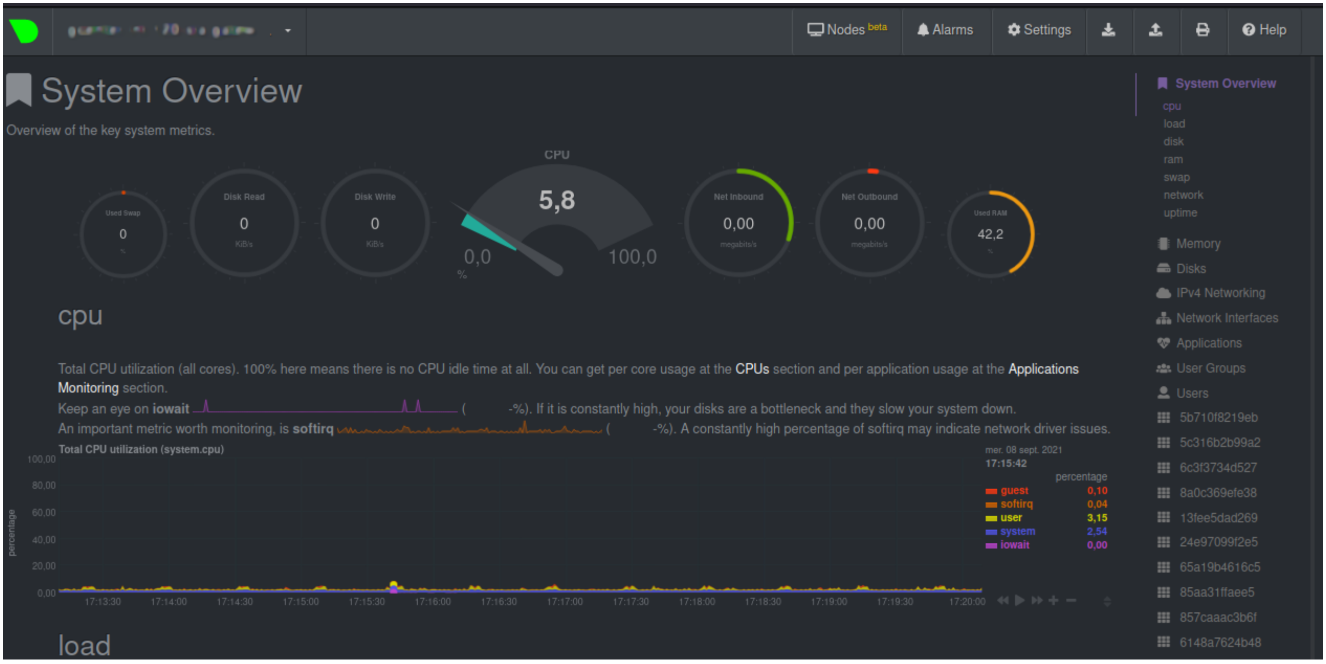
Netdata

Rôle Administrateur

Address: https://ip.du.gcenter/gstats

A *Netdata* server is also embedded in the TRACKWATCH solution.

This server is accessible to administrators via the URL https://ip.du.gcenter/gstats.



System Overview

Overview of the key system metrics.

cpu

Total CPU utilization (all cores). 100% here means there is no CPU idle time at all. You can get per core usage at the **CPUs** section and per application usage at the **Applications Monitoring** section.

Keep an eye on **iowait** (-%). If it is constantly high, your disks are a bottleneck and they slow your system down.

An important metric worth monitoring, is **softirq** (-%). A constantly high percentage of softirq may indicate network driver issues.

Total CPU utilization (system.cpu)

mer. 08 sept. 2021
17:15:42

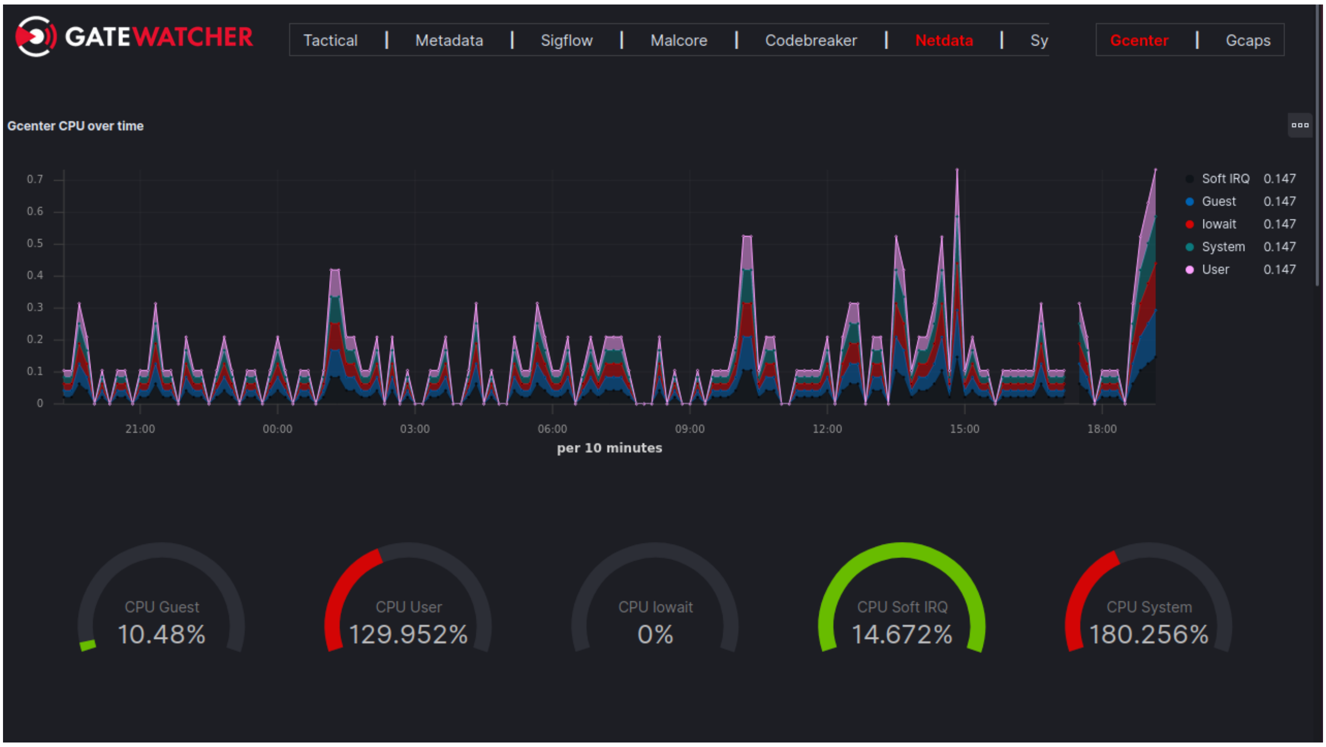
	percentage
guest	0,10
softirq	0,04
user	3,15
system	2,54
iowait	0,00

load

This interface provides administrators with a wide range of metrics on the various devices in the TRACKWATCH solution.

Via the menu at the top of the page it is possible to select the equipment to be observed. The **GCenter** will be found there, as well as the **GCap** that are paired with it.

Alternatively, this data can also be viewed from the kibana **Netdata** *dashboard* accessible from the `Operators > Dashboards` menu.



38.1 Netdata export

Rôle Administrateur

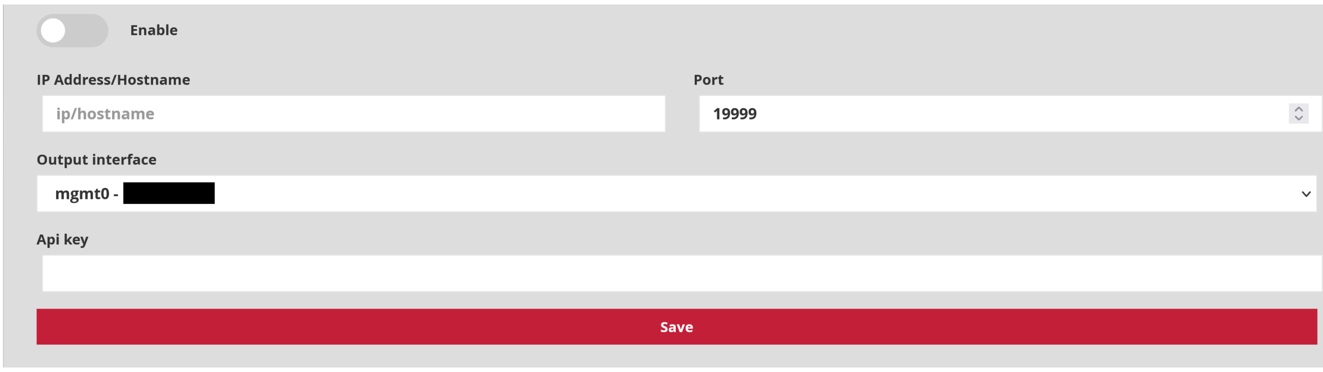
Address: ADMINISTRATORS > GCenter > Configuration > Netdata Export

Although the TRACKWATCH solution includes a Netdata server, the administrator may want to export the real-time system data to an existing Netdata server.

In order for the **TRACKWATCH** solution to communicate its information to a Netdata server, this section must be configured with the necessary information. This configuration is carried out from two tabs:

- *General*
- *Encryption*

38.1.1 Netdata - General settings



○ Enable

IP Address/Hostname: ip/hostname

Port: 19999

Output interface: mgmt0 - [redacted]

Api key:

Enable: enables/disables the service.

IP Address/Hostname: the fqdn or IP address of the Netdata server.

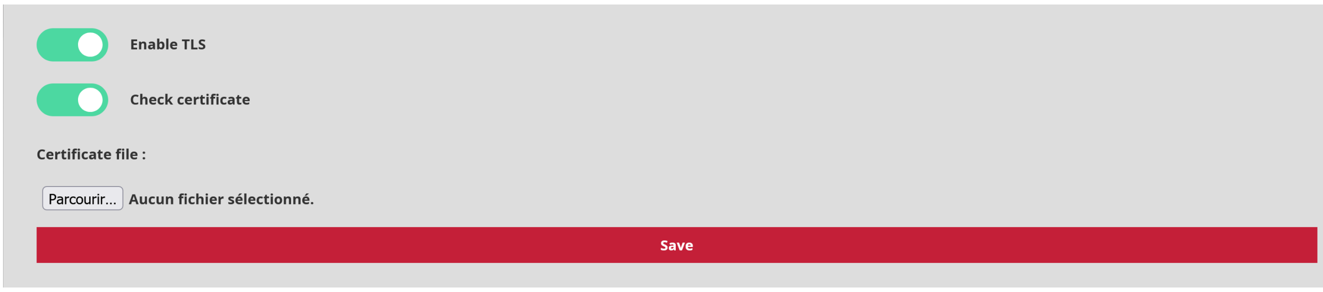
Port: the listening port of the Netdate server.

Output interface: the exit in interface to use to reach the Netdata server.

API key: The API key of the Netdata server.

38.1.2 Netdata - Encryption

This section is required for the administrator to set up encryption of the communication between the **GCENTER** and its Netdata server. A certificate will be required to enable this feature.



Enable TLS

Check certificate

Certificate file :

Enable TLS: Enable/Disable encryption. Disabled by default.

Check certificate: Enables/disables checking the validity of the certificate when the TLS service is enabled.

Any modification will only be applied after pressing** Save**.

More information is available in the [Using a Netdata Server] section (monitoring/netdata.html#using-a-netdata-server)

Chapter 39

Using a NETDATA server

This guide provides an overview of the steps required to set up a netdata monitoring server and its interconnection to a GCenter in order to ensure its monitoring.

Note:

The Netdata version compatible with GCenter and GCap is 1.19

39.1 Installation 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 of 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
```

39.2 Configuration

Stream.conf and gcenter configuration

Generate uuid

```
sudo docker exec -it netdata uuidgen
```

Stream configuration with the previously generated uuid.

Netdata recommends using edit-config

```
sudo docker exec -it netdata /etc/netdata/edit-config stream.conf
```

```
[dd236090-a42d-43e2-b0ba-ff8eaa6216a2] << Replace the uuid here
    enabled = yes
    default history = 36000
    default memory mode = ram
    health enabled by default = auto
    allow from = *
    default postpone alarms on connect seconds = 60
```

Configuring the netdata.conf

```
sudo docker exec -it netdata /etc/netdata/edit-config netdata.conf
```

```
[global]
      ...
      hostname = netdata-docker.gatewatcher.com
      ...
      timezone = Europe/Paris
```

Configuring netdata export in gcenter

Note:

Read: ref:*monitoring:Netdata Export.*

For netdata to send notifications, health_alarm_notify.conf must be configured

```
sudo docker exec -it netdata /etc/netdata/edit-config health_alarm_notify.conf
```

Reference: Alarm Configuration

39.3 Creating alerts for Netdata

Alerts are created 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 facilitate managing the alerts, it is advisable to create a **.conf* file for each category of alert.

Here are a few examples:

Description	Link
Alert in case of a lack of or overload of traffic	`traffic.conf`
Alert if Gcap analysis services are disabled	`suricata_status.conf`
Alert if a Gcap/Gcenter restart has taken place	`reboot.conf`
RAM overload alert	`ram.conf`
Alert for "dropped" network packets on Gcap	`drop.conf`
Alert in case of disk filling, here the data partition of Gcap	`disk.conf`
CPU overload alert	`cpu.conf`

Create your own alerts

Alert creation is based on the metrics collected by netdata.

To find out what these metrics are, log in to the netdata interface of your Gcenter.

```
https:// IP or FQDN of Gcenter /gstats
```

Taking the example of RAM monitoring

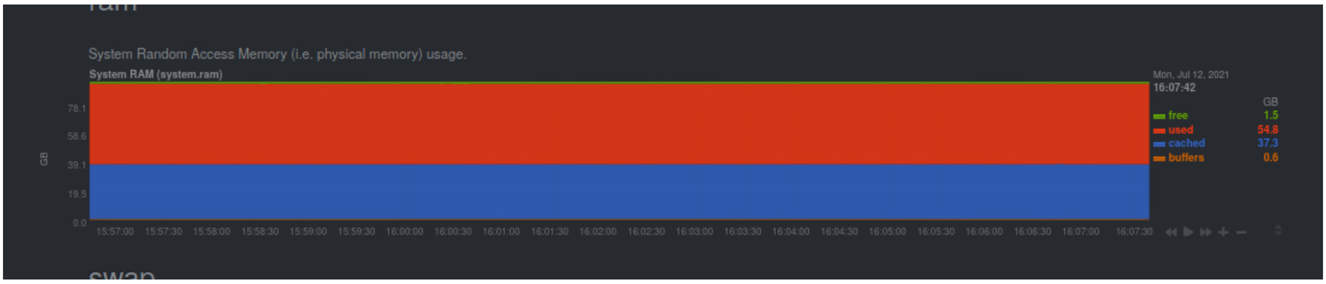


Fig. 1: The name of the Graph is system.ram and the curve to monitor used

The alert in ram.conf will be written as follows:

We name the alarm

```
1>>  alarm: ram_usage
```

The chart in Netdata is called:

```
2>> on: system.ram
```

It is indicated that the 10 min average of the used curve is calculated

```
3>> lookup: average -10m percentage of used
```

The unit is specified

```
4>> units: %
```

The time interval between each calculation is defined.

```
5>> every: 1m
```

Alert and critical thresholds are defined

```
6>> warn: $this > 70
7>> crit: $this > 90
```

The delay time for the alarm to be cancelled after triggering is defined.

```
8>> delay: down 15m multiplier 1.5 max 1h
```

Description of the alarm

```
9>> info: average RAM utilisation over the last 10 minutes
```

Define who will be alerted (see health_alarm_notify.conf)

```
10>> to: sysadmin
```

This part of the **GCENTER** enables the management of users and associated groups, the history of authentications on the platform, and also the association with a Lightweight Directory Access Protocol (LDAP) server.

From this configuration interface, the administrator will be able to customise the parameters of the **GCENTER** management solution via these five tabs:

- *Authentications history*
- *Creations/Deletions history*
- *Permissions history*
- [Users management](#local user)
- *LDAP configuration*

Chapter 40

Local users

Rôle Administrateur

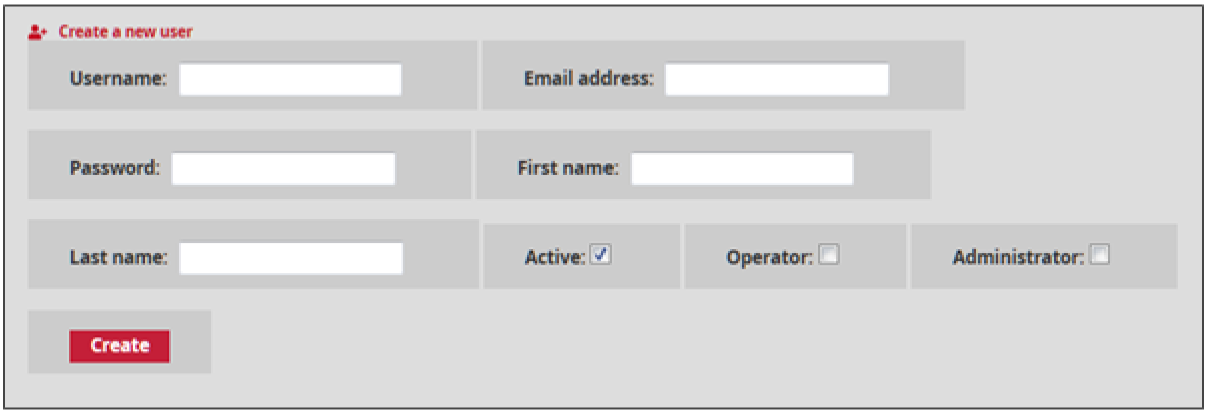
Menu: Administrators > GCenter > Accounts > User management

From the user account configuration menu of the TRACKWATCH solution, it is possible to create user accounts each having different rights. The proposed groups fully comply with the Military Programming Law.

The creation of a user and the associated profile can be configured from this view. Indeed, depending on the commands or actions carried out, it will be necessary to belong to a given group.

Within this documentation, the details of the group allowed to perform the action are specified in each section by the Rôle Administrateur and Rôle Opérateur badges respectively. This is the case if Administrator rights are required or if Operator rights are required.

The administrator fills in the name/first name/email/password of the user to be created. These completed fields will then be used to trace the user in the history if changes are made.



Create a new user

Username:
Email address:
Password:
First name:
Last name:
Active: ☑
Operator: □
Administrator: □

Username is the field to be filled in by the administrator to enter the full name of the new user of the **GCENTER** management platform. This value can only contain letters, numbers and characters [@/./+/-/-/_.].

First name, **Last name**, and **Email address** are optional fields upon user creation. They provide information on the profile's first name, last name, and email address respectively.

Password is for the user's password for the created account. This password must contain a minimum of seven characters.

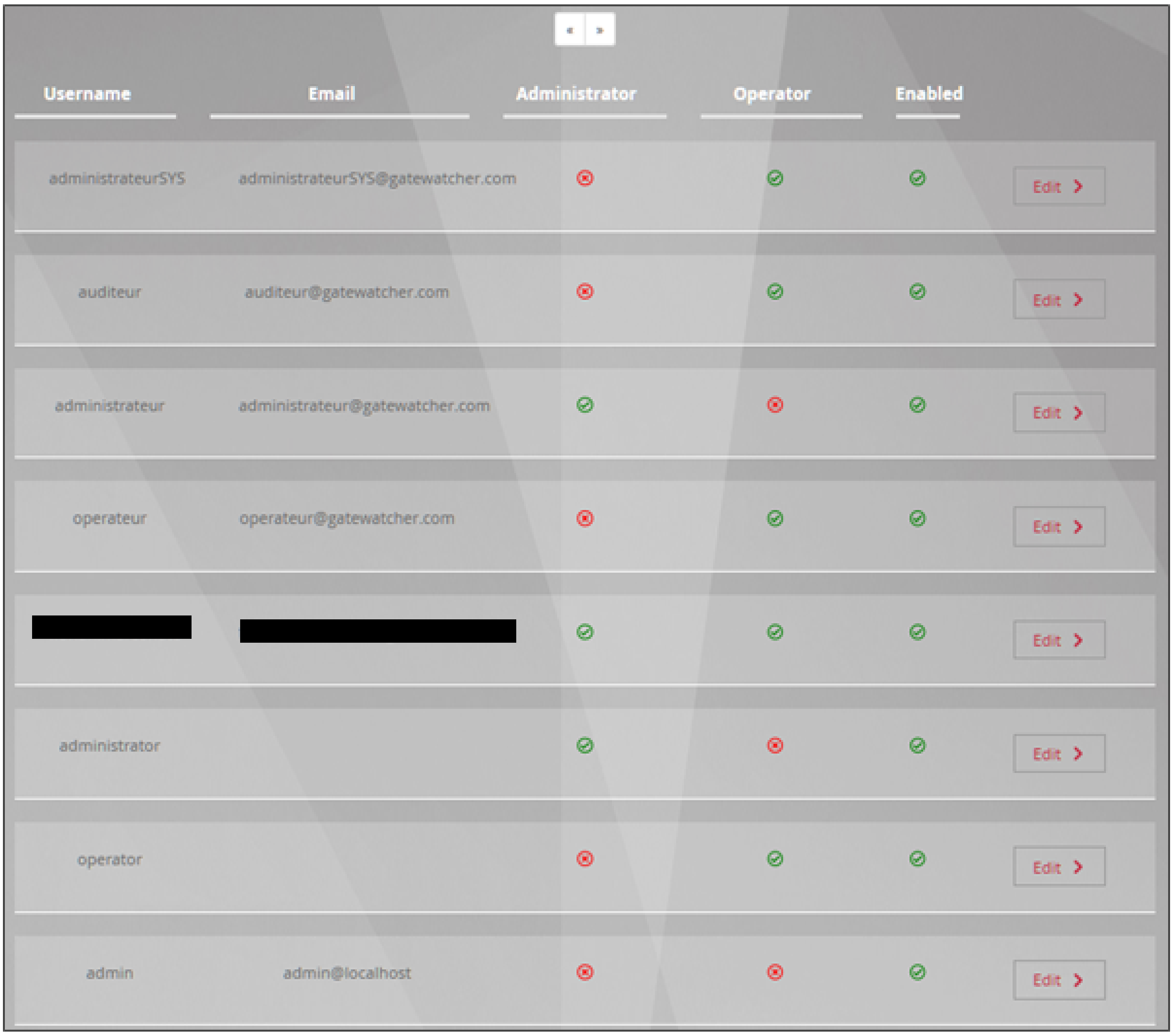
Operator and Administrator** represent groups. Once the box is ticked, the user will have the appropriate permissions for the selected group.

Active: Enables/disables the user account.

- The **Operator** group will be able to: add or delete detection rules, view generated alert logs, scan files, view the Smartmap, and have an overview of the Suricata signatures in the Sigflow area.
- The **Administrator** group will be able to: update the operating system, software, reboot the equipment, edit and view the network configuration, update the detection interfaces, view the version, attributes, add or delete a probe. The **Administrator** group can enable or disable the sending of additional technical information to operators, enable or disable the storage of additional technical information while defining the duration, and consult all the operating and alert logs generated.

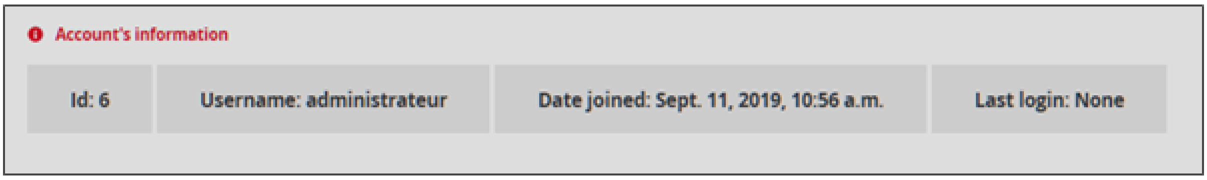
Any of this information can be taken into account after the administrator saves the changes by pressing **Create**.

Below is a list of all the users created by the system administrator with the information related to each profile ('Enabled' being the status of the profile, activated or deactivated):



Username	Email	Administrator	Operator	Enabled	
administrateurSYS	administrateurSYS@gatewatcher.com	✗	✓	✓	Edit >
auditeur	auditeur@gatewatcher.com	✗	✓	✓	Edit >
administrateur	administrateur@gatewatcher.com	✓	✗	✓	Edit >
operateur	operateur@gatewatcher.com	✗	✓	✓	Edit >
[redacted]	[redacted]	✓	✓	✓	Edit >
administrator		✓	✗	✓	Edit >
operator		✗	✓	✓	Edit >
admin	admin@localhost	✗	✗	✓	Edit >

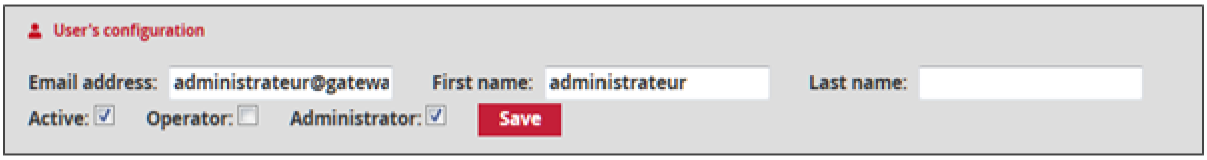
The **Edit** button will be used to modify the user profile in question. Various permissions are possible for a user depending on the group membership. It is possible to decide to assign administrative rights to a user according to their scope of action.



Account's information

Id: 6	Username: administrateur	Date joined: Sept. 11, 2019, 10:56 a.m.	Last login: None

The **Account's information** contains the user's profile information, i.e. user ID, full name, creation date, and the last time the user logged on to the **GCENTER** management platform.



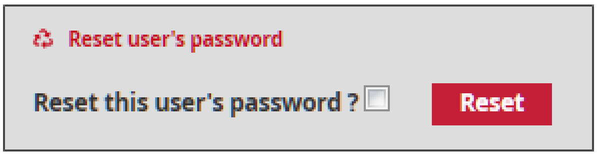
User's configuration

Email address: administrateur@gatewa First name: administrateur Last name:

Active: ☑ Operator: □ Administrator: ☑

User's configuration enables modifying the email address, first and last name of the user profile. In addition, the groups created by default in accordance with the Military Programming Law appear. They may or may not be assigned to the profile by ticking the check box provided for this purpose. The administrator can enable or disable the platform user via the **Active** option. The consequence of this option will result in an inability to connect to the **GCENTER** interface.

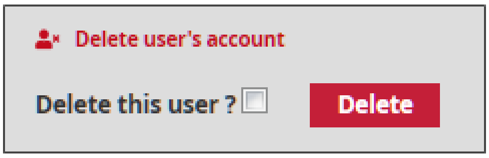
Any modification will only be applied after pressing **Save**.



Reset user's password

Reset this user's password ? □

Reset user's password enables the password associated with the user account to be regenerated if it is lost or forgotten. The platform will propose a new password to log in again once the 'Reset' button is selected.



Delete user's account

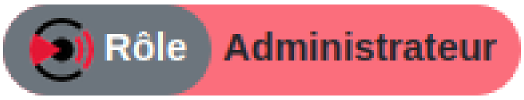
Delete this user ? □

In **Delete user's account** , the **Delete** option enables the administrator to remove any user profile from the platform.

The administration interface therefore enables the rights to be fully configured at all levels of the **GCENTER** administration. Any creation of a user from the **GCENTER** will be taken into account by the **GCAP** probe. The user will be added to its database.

Chapter 41

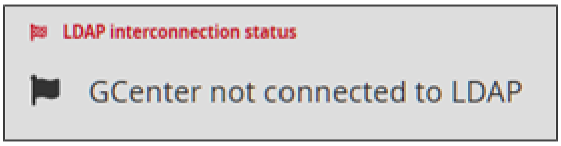
LDAP Integration / ActiveDirectory



Rôle Administrateur

Menu: Administrators > GCenter > Accounts > LDAP Configuration

The TRACKWATCH user account configuration menu enables the use of Lightweight Directory Access Protocol (LDAP) as the authentication backend rather than the internal backend.

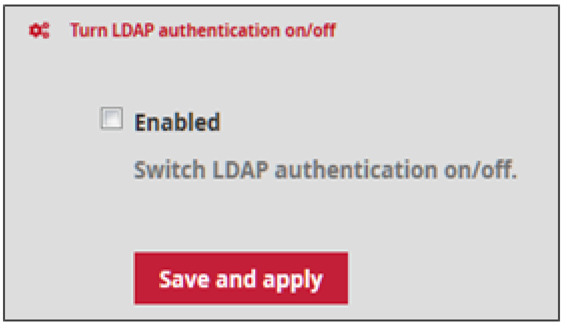


LDAP interconnection status

GCenter not connected to LDAP

This interface is used to manage the connection between the **GCENTER** and an LDAP/ActiveDirectory server.

LDAP interconnection status enables easy identification of the connection status.



Turn LDAP authentication on/off

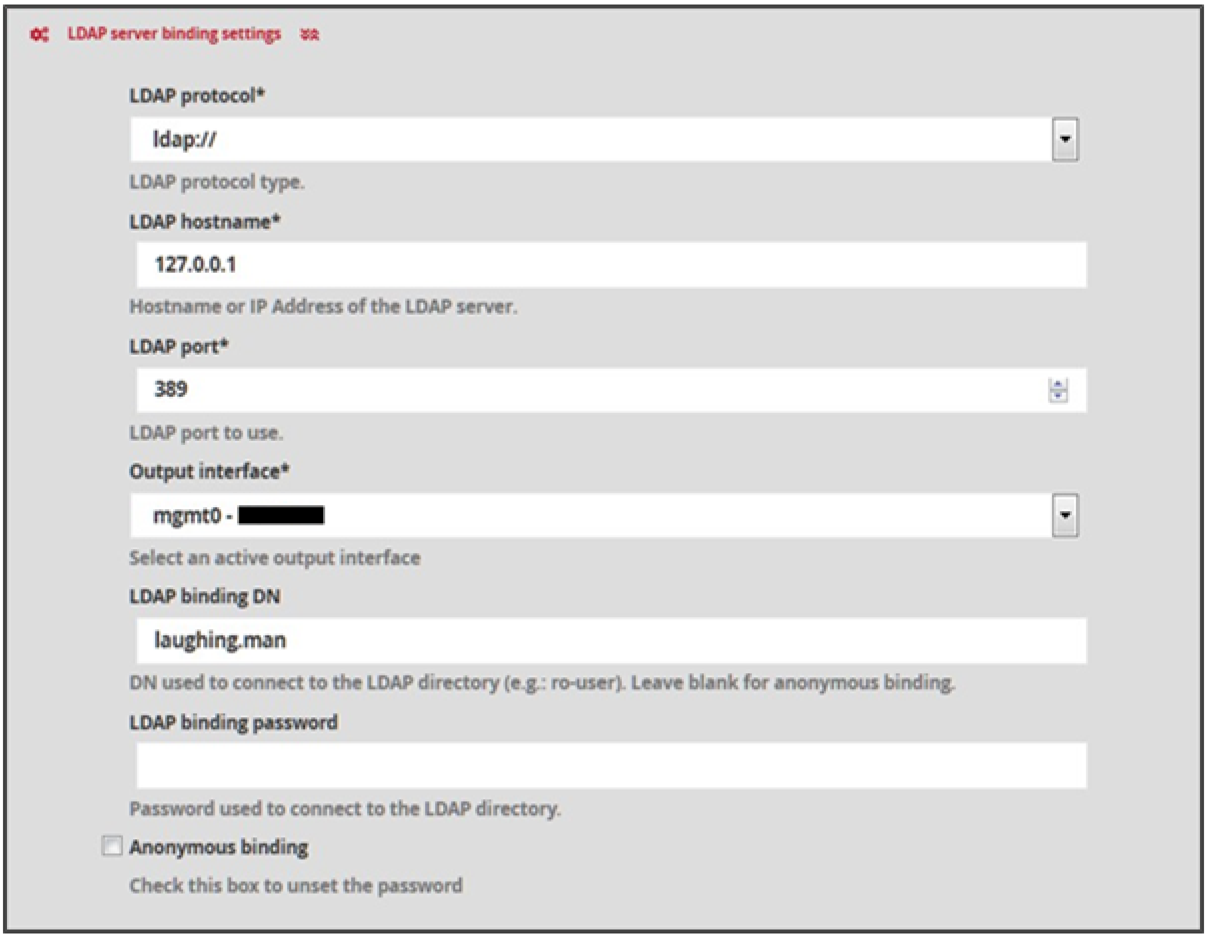
☐ Enabled

Switch LDAP authentication on/off.

In the **Turn LDAP authentication on/off** section tick the **Enabled** box to activate the service and then click **Save and apply** to take the change into account.

Saving and applying the new LDAP option configuration will cause a restart of the application and therefore a disconnection from the user page.

Once the administrator clicks **Confirm**, it will be necessary to reconnect to the interface. Before this manipulation, the connection options to the LDAP server can be set in the **LDAP server binding settings** section:



LDAP server binding settings

LDAP protocol*

ldap://

LDAP protocol type.

LDAP hostname*

127.0.0.1

Hostname or IP Address of the LDAP server.

LDAP port*

389

LDAP port to use.

Output interface*

mgmt0 - [redacted]

Select an active output interface

LDAP binding DN

laughing.man

DN used to connect to the LDAP directory (e.g.: ro-user). Leave blank for anonymous binding.

LDAP binding password

Password used to connect to the LDAP directory.

□ Anonymous binding

Check this box to unset the password

LDAP protocol: corresponds to the type of authentication protocol selected: LDAP or LDAPS

LDAP hostname: full FQDN address or IP of the LDAP/ActiveDirectory server

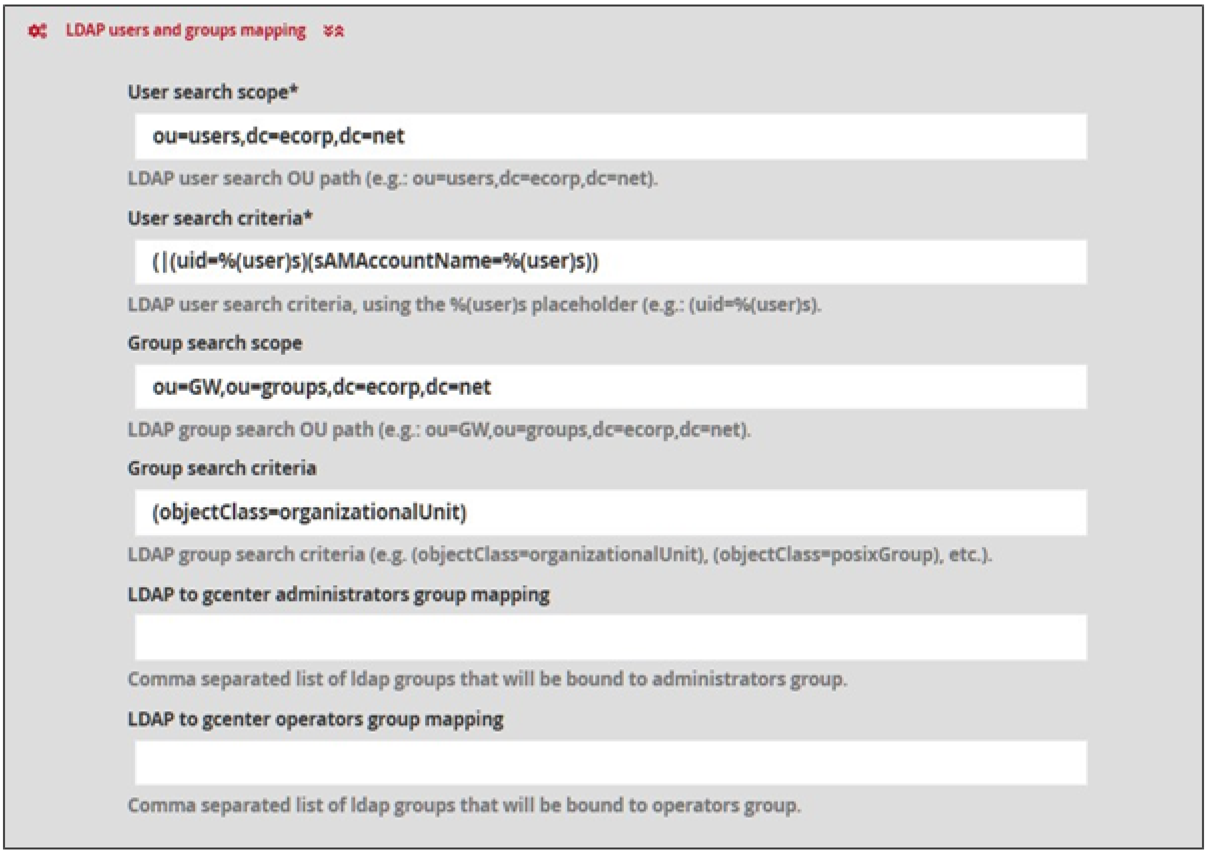
LDAP port: corresponds to the port number of the LDAP service. (Example: *389*)

Output interface: The output interface to be used to reach the LDAP server.

LDAP binding DN: corresponds to the Distinguished Name (DN) used to connect to the LDAP directory. Leave the field empty if the connection is anonymous. (Example: *CN=adro,OU=Service Accounts,OU=Example,DC=Example,DC=com,ro-user*)

LDAP binding password: password used to connect to the directory. Leave the field empty if the connection is anonymous.

Anonymous binding: enables the use of a password for authentication to be disabled.



LDAP users and groups mapping

User search scope*

ou=users,dc=ecorp,dc=net

LDAP user search OU path (e.g.: ou=users,dc=ecorp,dc=net).

User search criteria*

(|(uid=%(user)s)(sAMAccountName=%(user)s))

LDAP user search criteria, using the %(user)s placeholder (e.g.: (uid=%(user)s).

Group search scope

ou=GW,ou=groups,dc=ecorp,dc=net

LDAP group search OU path (e.g.: ou=GW,ou=groups,dc=ecorp,dc=net).

Group search criteria

(objectClass=organizationalUnit)

LDAP group search criteria (e.g. (objectClass=organizationalUnit), (objectClass=posixGroup), etc.).

LDAP to gcenter administrators group mapping

Comma separated list of ldap groups that will be bound to administrators group.

LDAP to gcenter operators group mapping

Comma separated list of ldap groups that will be bound to operators group.

The **LDAP users and groups mapping** section:

User search scope: Basic OU (Organisational Unit) for user search (Example: *ou=users,dc=ecorp,dc=net*)

User search criteria: LDAP user search criteria, by means of the %(user) space provided (Example: *(|(uid=%(user)s)(sAMAccountName=%(user)s))*)

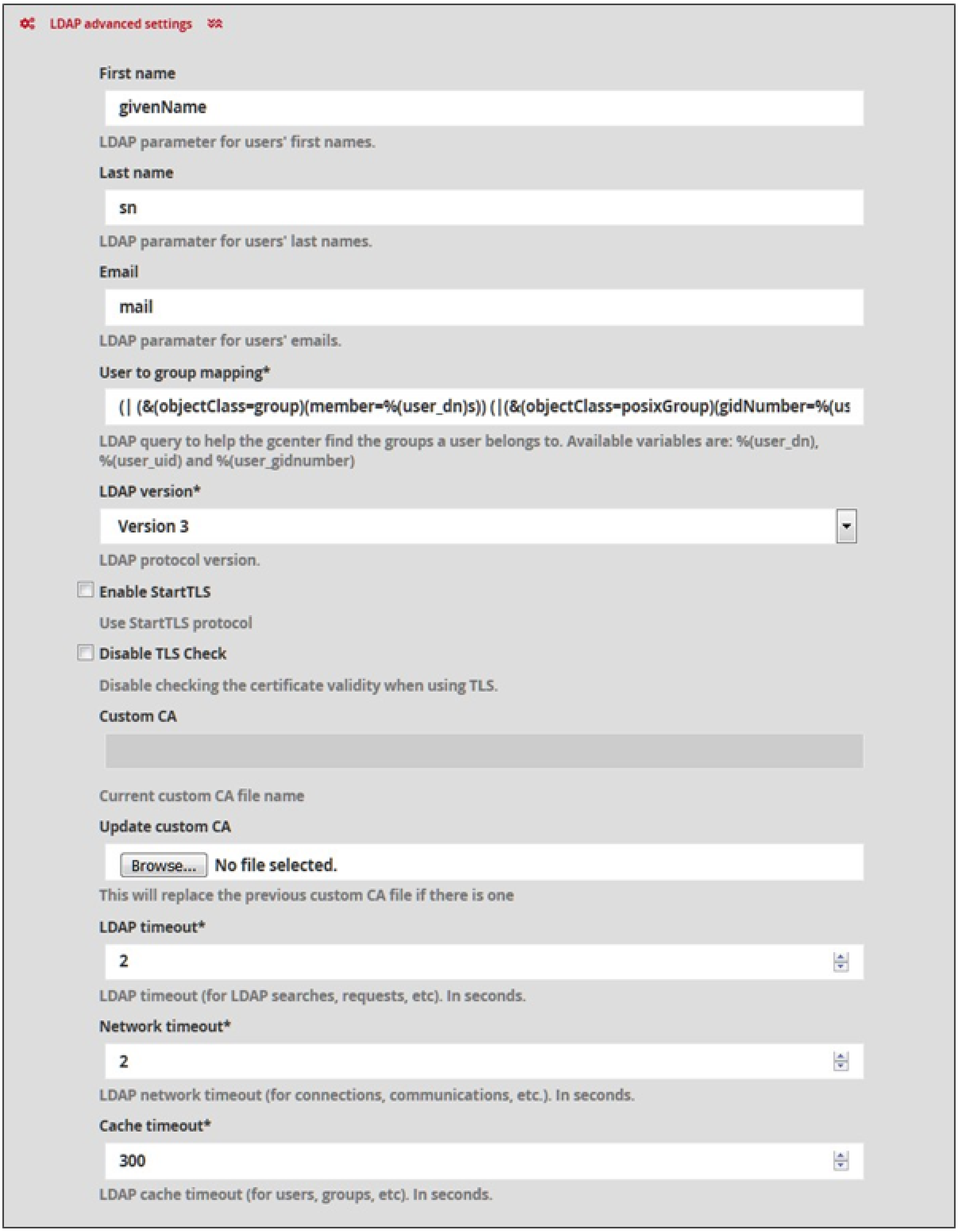
Group search scope: Basic OU (Organisational Unit) for group search (Example: *ou=GW,ou=groups,dc=ecorp,dc=net*)

Group search criteria: Search criteria for LDAP groups, using the %(group) space provided (Example: *(objectClass=organizationalUnit)*)

LDAP to GCENTER administrators group mapping: is a comma-separated list of LDAP groups related to the solution's administrators group.

LDAP to GCENTER operators group mapping: is a comma-separated list of LDAP groups related to the solution operators group.

The **LDAP advanced settings** section enables accessing the advanced LDAP options.



LDAP advanced settings

First name

givenName

LDAP parameter for users' first names.

Last name

sn

LDAP paramater for users' last names.

Email

mail

LDAP paramater for users' emails.

User to group mapping*

(| (&(objectClass=group)(member=%(user_dn)s)) (|(&(objectClass=posixGroup)(gidNumber=%(us

LDAP query to help the gcenter find the groups a user belongs to. Available variables are: %(user_dn), %(user_uid) and %(user_gidnumber)

LDAP version*

Version 3

LDAP protocol version.

□ Enable StartTLS

Use StartTLS protocol

□ Disable TLS Check

Disable checking the certificate validity when using TLS.

Custom CA

Current custom CA file name

Update custom CA

Browse... No file selected.

This will replace the previous custom CA file if there is one

LDAP timeout*

2

LDAP timeout (for LDAP searches, requests, etc). In seconds.

Network timeout*

2

LDAP network timeout (for connections, communications, etc.). In seconds.

Cache timeout*

300

LDAP cache timeout (for users, groups, etc). In seconds.

The LDAP parameters can be modified from this interface for the first name of the user, the last name, the email, the type, the version, the timeout of the service (in seconds) after each request, connection, or communication. The time before the timeout (in seconds) of the cache for users or groups is also configurable.

First name: LDAP parameter corresponding to the user's first name (Example: *givenName*)

Last name: LDAP parameter corresponding to the user's last name (Example: *sn*)

Email: LDAP parameter corresponding to the user's email address (Example: *email*)

User to group mapping: LDAP query to help find the groups to which a user belongs. The available variables are: %(user_dn), %(user_uid) et %(user_gidnumber)

LDAP version: version LDAP to be selected (*Version2* | *Version3*)

Enable StartTLS: allows activating the use of StartTLS. Disabled by default.

Disable TLS check: setting to stop checking the validity of the certificate when the TLS service is enabled.

Custom CA: Information about the customised CA used.

Update custom CA: replaces the custom CA certificate.

LDAP timeout: modifiable timeout in seconds for LDAP searches or other queries (Example: *2*)

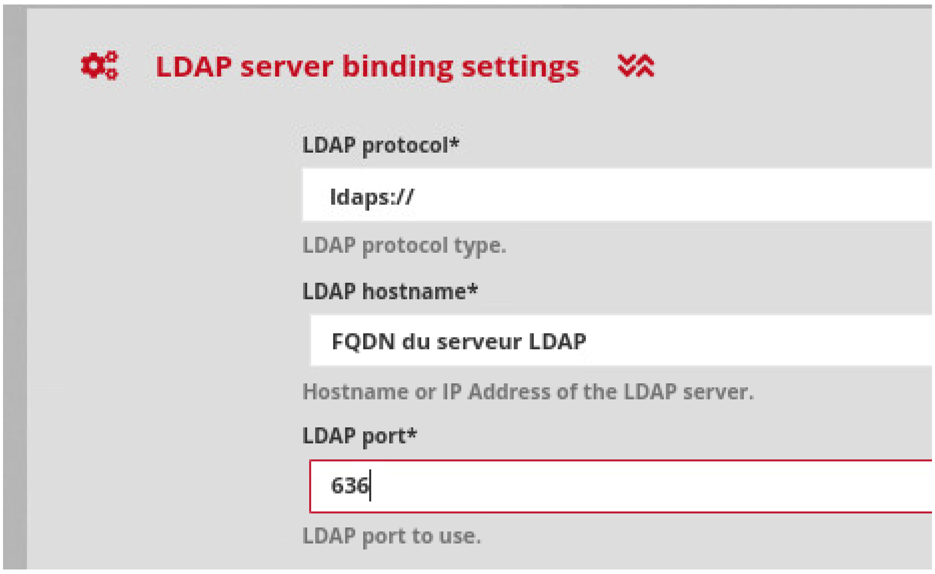
Network timeout: delay in seconds for network connections or communications (Example: *2*)

Cache timeout: LDAP cache expiration time in seconds for users and groups (Example: *300*)

For an LDAPS configuration:

From the standard LDAP configuration explained above, it is necessary to:

- Enter in "LDAP server binding settings":
  - `LDAP protocol: ldaps://`
  - `LDAP_port: 636`
- Enter the certificate of the certification authority in "LDAP advanced settings".



LDAP server binding settings

LDAP protocol*

ldaps://

LDAP protocol type.

LDAP hostname*

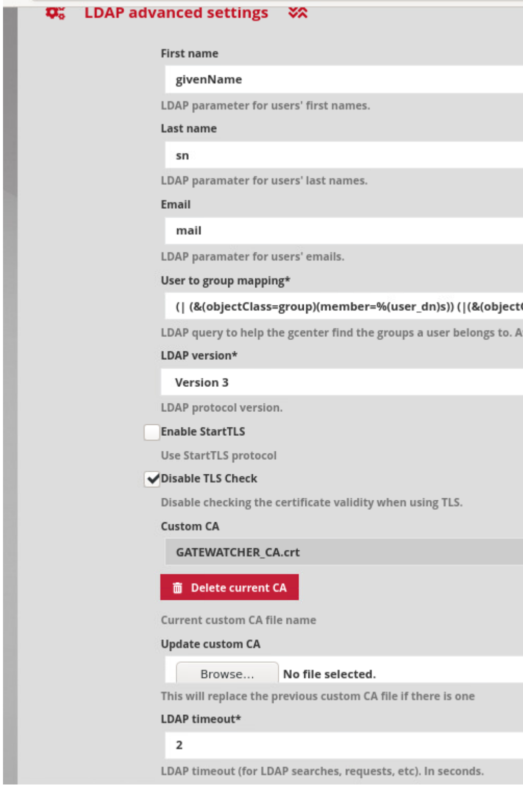
FQDN du serveur LDAP

Hostname or IP Address of the LDAP server.

LDAP port*

636

LDAP port to use.



LDAP advanced settings

First name

givenName

LDAP parameter for users' first names.

Last name

sn

LDAP paramater for users' last names.

Email

mail

LDAP paramater for users' emails.

User to group mapping*

(| (&(objectClass=group)(member=%(user_dn)s)) (|(&(object

LDAP query to help the gcenter find the groups a user belongs to. A

LDAP version*

Version 3

LDAP protocol version.

□ Enable StartTLS

Use StartTLS protocol

☑ Disable TLS Check

Disable checking the certificate validity when using TLS.

Custom CA

GATEWATCHER_CA.crt

Current custom CA file name

Update custom CA

No file selected.

This will replace the previous custom CA file if there is one

LDAP timeout*

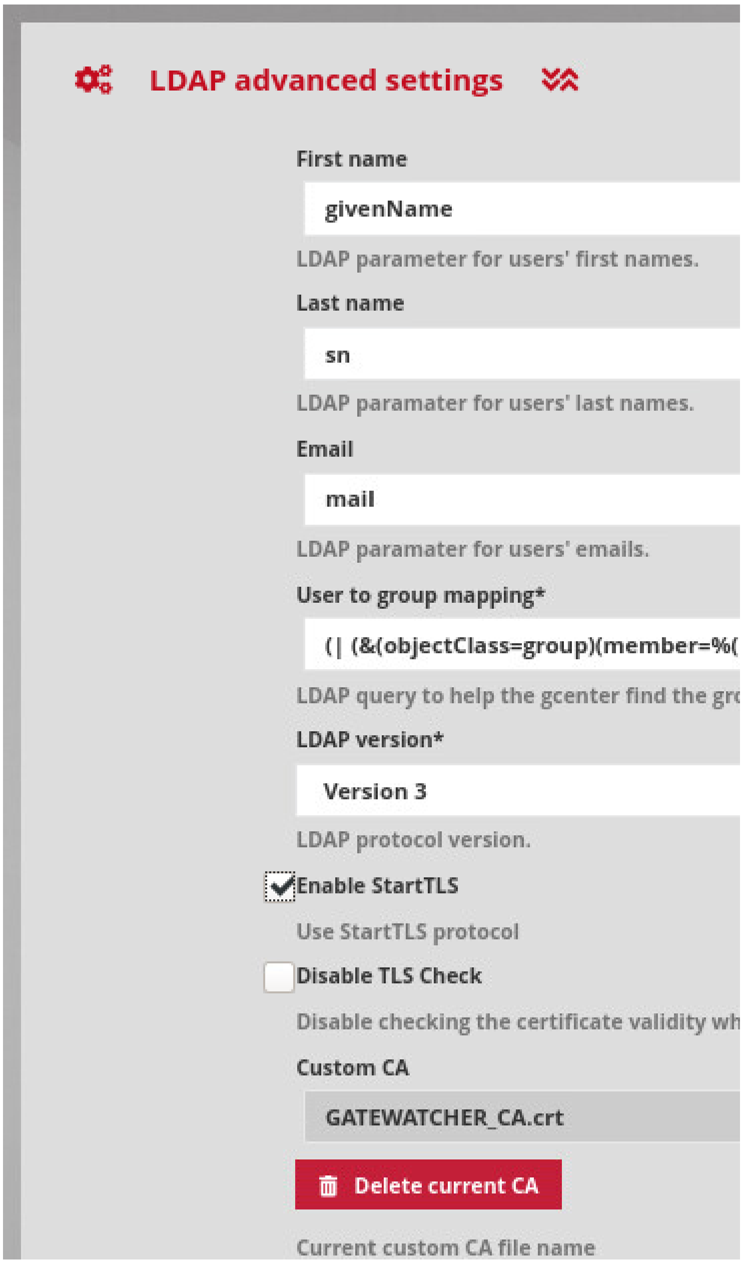
2

LDAP timeout (for LDAP searches, requests, etc). In seconds.

For an LDAP over TLS configuration:

From the standard LDAP configuration explained above, it is necessary to:

- Fill in the certificate of the certification authority in "LDAP advanced settings".
- Tick the "Enable StartTLS" box in "LDAP advanced settings".



LDAP advanced settings

First name

givenName

LDAP parameter for users' first names.

Last name

sn

LDAP paramater for users' last names.

Email

mail

LDAP paramater for users' emails.

User to group mapping*

(| (&(objectClass=group)(member=%(

LDAP query to help the gcenter find the gro

LDAP version*

Version 3

LDAP protocol version.

☑ Enable StartTLS

Use StartTLS protocol

□ Disable TLS Check

Disable checking the certificate validity wh

Custom CA

GATEWATCHER_CA.crt

Current custom CA file name

Chapter 42

Audit trail

Rôle Administrateur

Menu: Administrators > GCenter > Accounts

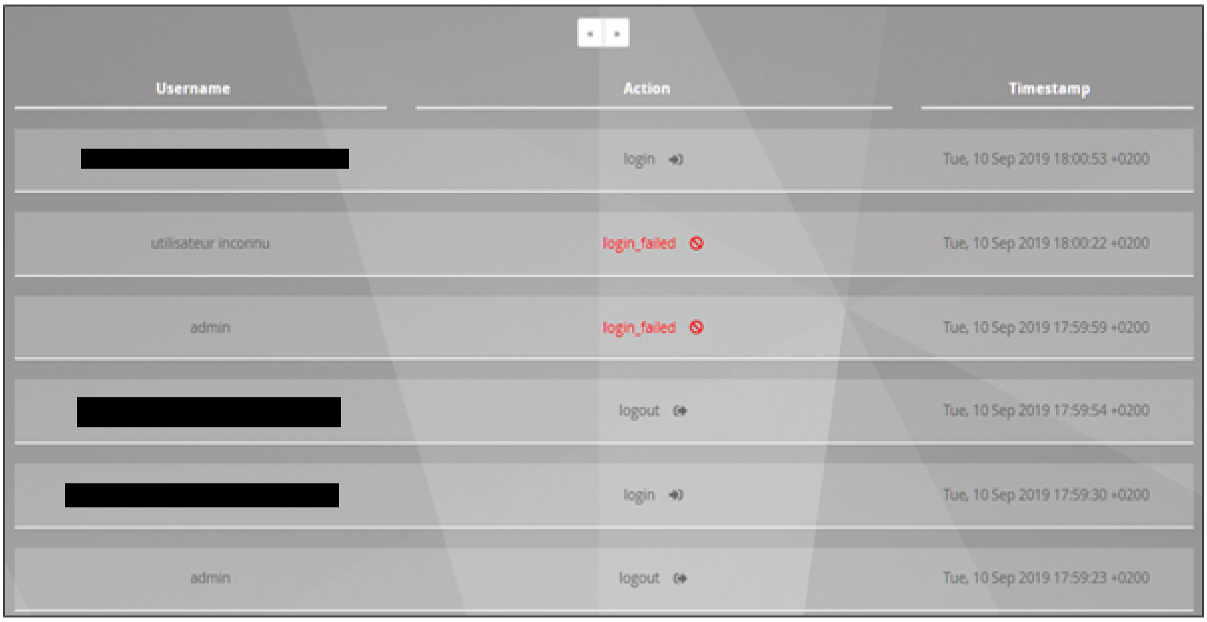
The TRACKWATCH solution will record the various actions carried out on the human–computer interaction (HCI) linked to user management on the management platform over time, in order to ensure traceability. This traceability is carried out both for the connection of users and for the creation/deletion or modification of permissions.

42.1 Authentications history

Rôle Administrateur

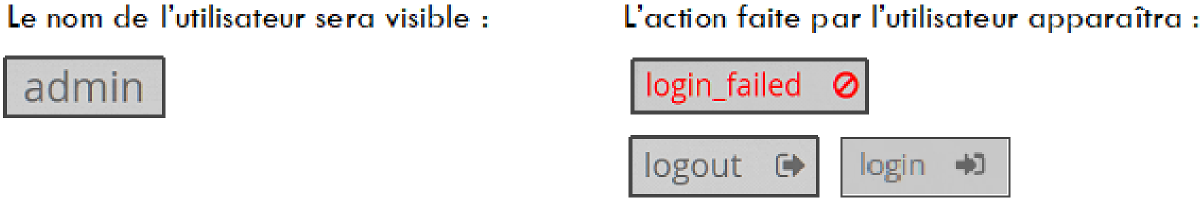
Menu: Administrators > GCenter > Accounts > Authentications history

The history of all authentications on the **GCENTER** is available.



Username	Action	Timestamp
[redacted]	login	Tue, 10 Sep 2019 18:00:53 +0200
utilisateur inconnu	login_failed	Tue, 10 Sep 2019 18:00:22 +0200
admin	login_failed	Tue, 10 Sep 2019 17:59:59 +0200
[redacted]	logout	Tue, 10 Sep 2019 17:59:54 +0200
[redacted]	login	Tue, 10 Sep 2019 17:59:30 +0200
admin	logout	Tue, 10 Sep 2019 17:59:23 +0200

A connection history of the user logins on the platform is present in the form of a timestamp in the format [**day**, **xx month year hh**: **mm**: ss].



Le nom de l'utilisateur sera visible :

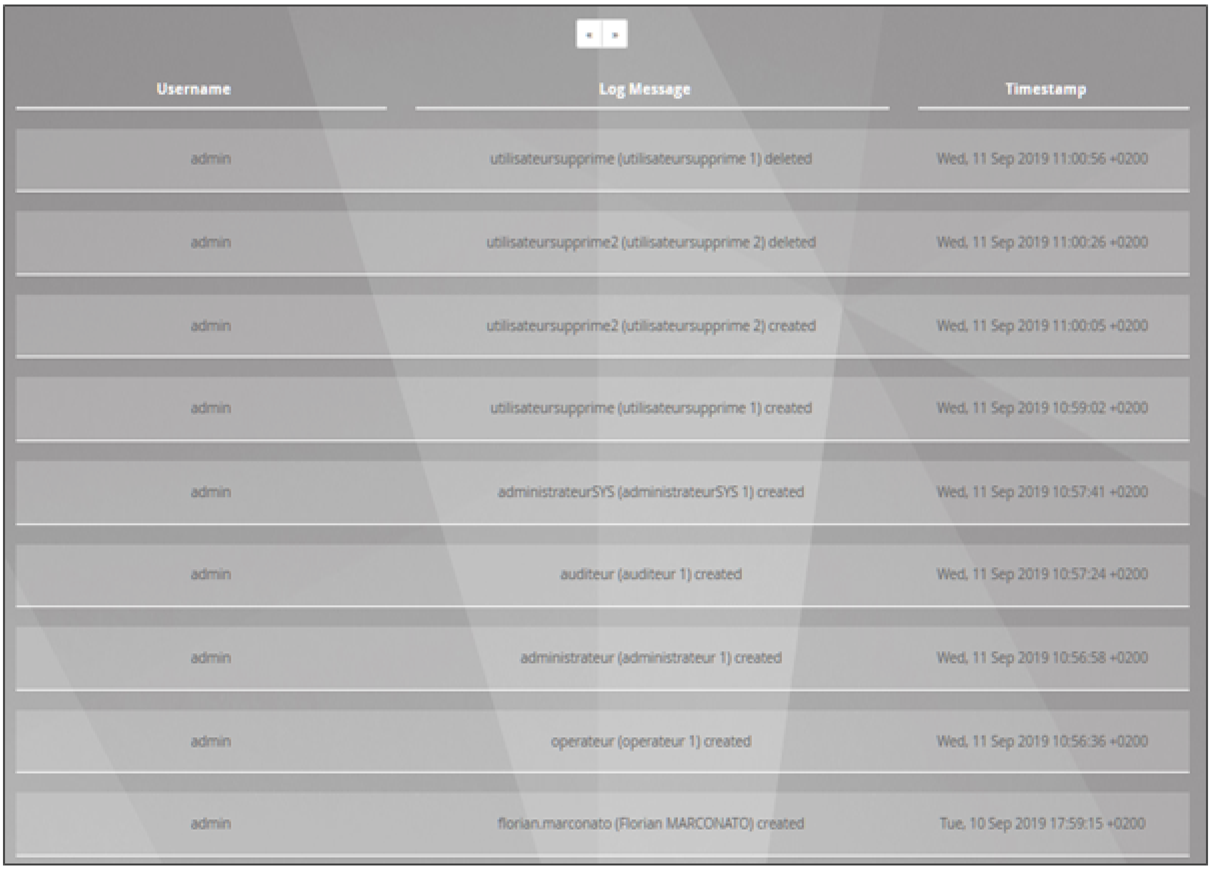
L'action faite par l'utilisateur apparaîtra :

42.1.1 Creations/Deletions history

Rôle Administrateur

Menu: Administrators > GCenter > Accounts > Creation/Deletion history

The history of all creations or deletions of **GCENTER** users is available. All the modifications made by an administrator account of the system on a user can be found at this level.

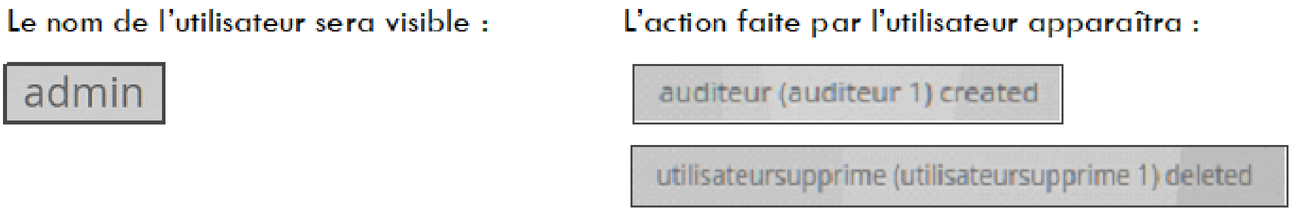


Username	Log Message	Timestamp
admin	utilisateursupprime (utilisateursupprime 1) deleted	Wed, 11 Sep 2019 11:00:56 +0200
admin	utilisateursupprime2 (utilisateursupprime 2) deleted	Wed, 11 Sep 2019 11:00:26 +0200
admin	utilisateursupprime2 (utilisateursupprime 2) created	Wed, 11 Sep 2019 11:00:05 +0200
admin	utilisateursupprime (utilisateursupprime 1) created	Wed, 11 Sep 2019 10:59:02 +0200
admin	administrateurSYS (administrateurSYS 1) created	Wed, 11 Sep 2019 10:57:41 +0200
admin	auditeur (auditeur 1) created	Wed, 11 Sep 2019 10:57:24 +0200
admin	administrateur (administrateur 1) created	Wed, 11 Sep 2019 10:56:58 +0200
admin	operateur (operateur 1) created	Wed, 11 Sep 2019 10:56:36 +0200
admin	florian.marconato (Florian MARCONATO) created	Tue, 10 Sep 2019 17:59:15 +0200

In the **Username** column, the administrator's name responsible for adding or deleting the user is visible.

The **Log message** column contains information such as the user's name and the action associated with the account (*created* or *deleted*).

A history of user logins created and deleted on the platform is present in the form of a **Timestamp** in the format [**day** , **xx month year hh**: **mm**: ss].



Le nom de l'utilisateur sera visible :

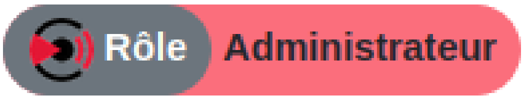
admin

L'action faite par l'utilisateur apparaîtra :

auditeur (auditeur 1) created

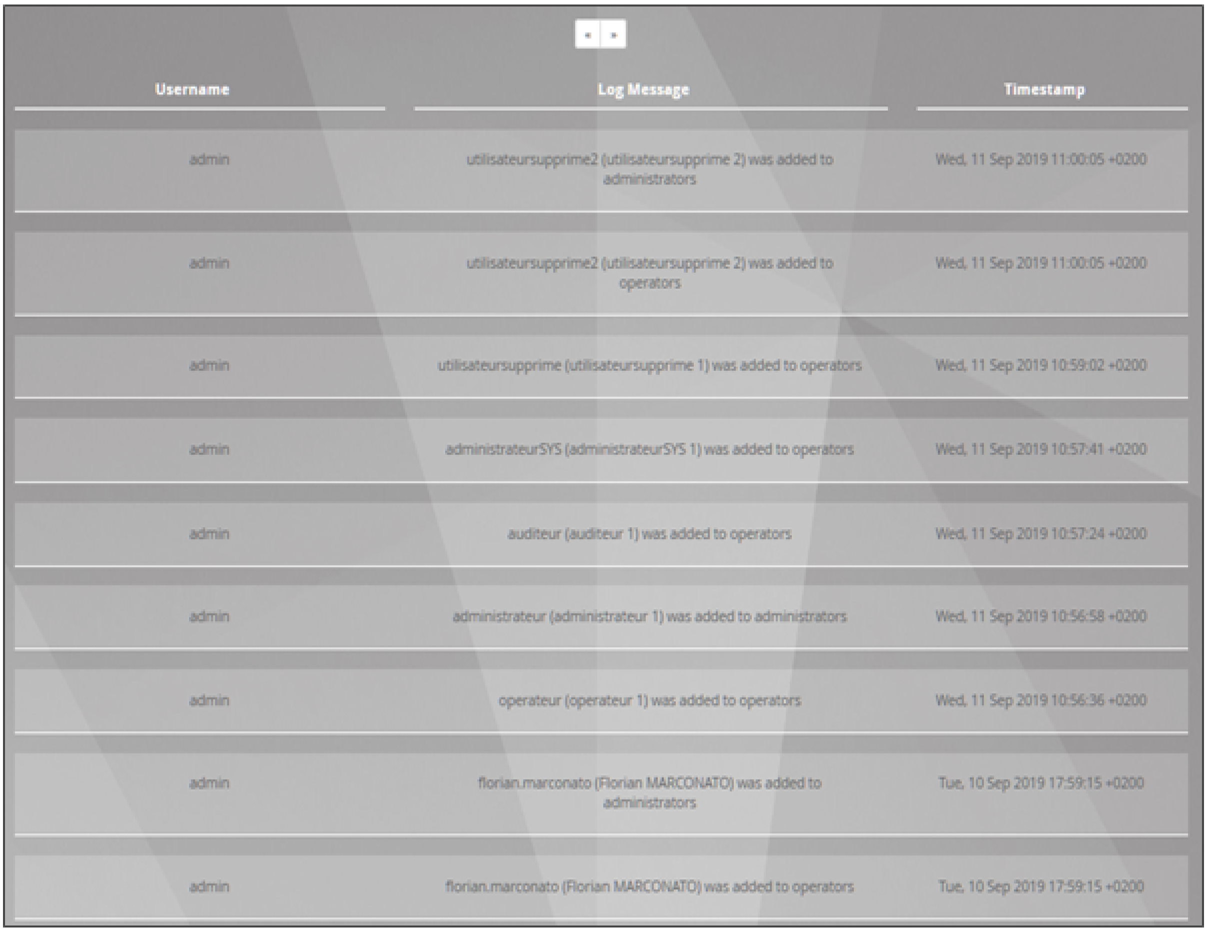
utilisateursupprime (utilisateursupprime 1) deleted

42.1.2 Permissions history



Menu: Administrators > GCenter > Accounts > Permission history

The history of all user permissions on the **GCENTER** is available. All changes to the rights on a profile are visible via this page.

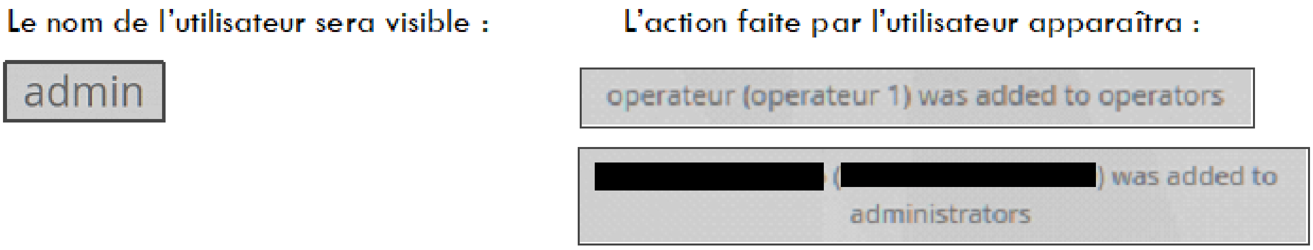


Username	Log Message	Timestamp
admin	utilisateursupprime2 (utilisateursupprime 2) was added to administrators	Wed, 11 Sep 2019 11:00:05 +0200
admin	utilisateursupprime2 (utilisateursupprime 2) was added to operators	Wed, 11 Sep 2019 11:00:05 +0200
admin	utilisateursupprime (utilisateursupprime 1) was added to operators	Wed, 11 Sep 2019 10:59:02 +0200
admin	administrateurSYS (administrateurSYS 1) was added to operators	Wed, 11 Sep 2019 10:57:41 +0200
admin	auditeur (auditeur 1) was added to operators	Wed, 11 Sep 2019 10:57:24 +0200
admin	administrateur (administrateur 1) was added to administrators	Wed, 11 Sep 2019 10:56:58 +0200
admin	operateur (operateur 1) was added to operators	Wed, 11 Sep 2019 10:56:36 +0200
admin	florian.marconato (Florian MARCONATO) was added to administrators	Tue, 10 Sep 2019 17:59:15 +0200
admin	florian.marconato (Florian MARCONATO) was added to operators	Tue, 10 Sep 2019 17:59:15 +0200

In the **Username** column, the administrator's name responsible for modifying the user's group is visible. Note that belonging to a particular group results in changes to the rights of the user profile on the platform.

In **Log message**, we find several pieces of information such as the name of the user and the action associated with the account (*was added to...*).

A history of the allocation of rights on the platform's user logins is present as a timestamp in the format [day**, ** xx month year hh**: **mm**: **ss].



Le nom de l'utilisateur sera visible :

admin

L'action faite par l'utilisateur apparaîtra :

operateur (operateur 1) was added to operators

[redacted] ([redacted]) was added to administrators

The **ADMINISTRATORS- Backup/Restore** section of the **GCENTER** enables data backup and configuration restore.

The **GCenter** backup includes:

- Sigflow Rulesets with changes (delete, threshold)
- the ***GCAP*** *profiles*
- All the configuration part of the **GCenter** present in *Administrators > GCenter* including the license

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

Chapter 43

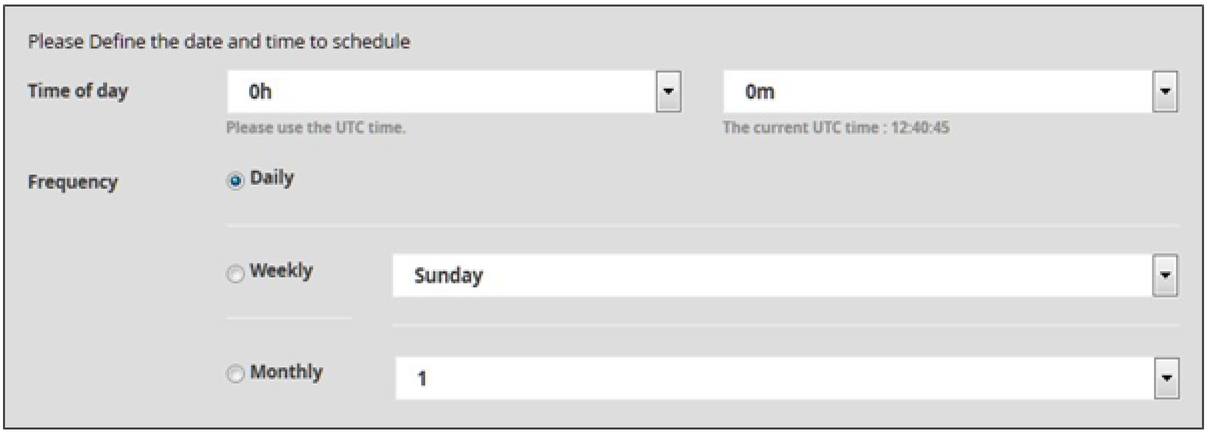
Configuration

Rôle Administrateur

Menu: Administrators > Backup / Restore > Configuration

The TRACKWATCH administrator can decide at any time to make a backup of the configuration.

They can also, if they wish, check the box **Enable scheduled backups**, in order to schedule backups on a regular basis. In such a case, a menu is displayed, allowing the user to configure the exact time of the backup.



Please Define the date and time to schedule

Time of day: 0h ▾ | 0m ▾

Please use the UTC time.

The current UTC time : 12:40:45

Frequency: ● Daily

○ Weekly: Sunday ▾

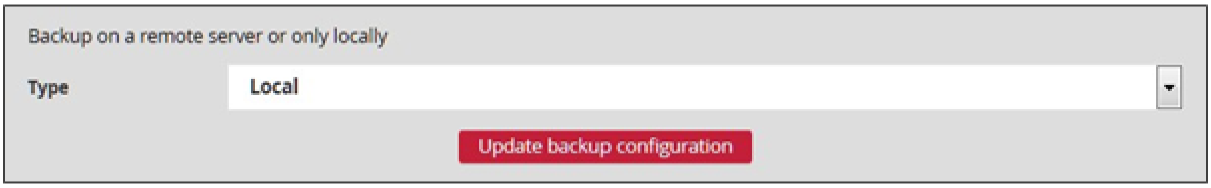
○ Monthly: 1 ▾

Time of day is the moment of the day at which the backup of the **GCENTER** configuration will be launched. The time of day and minutes are selected using the related drop-down menus.

Frequency: Enables you to select the number of times the configuration will be backed up. (*Daily*, *Weekly*, *Monthly*).

Once the optional planning part is configured, it is necessary to choose the type of backup desired. Three types of backup are available:

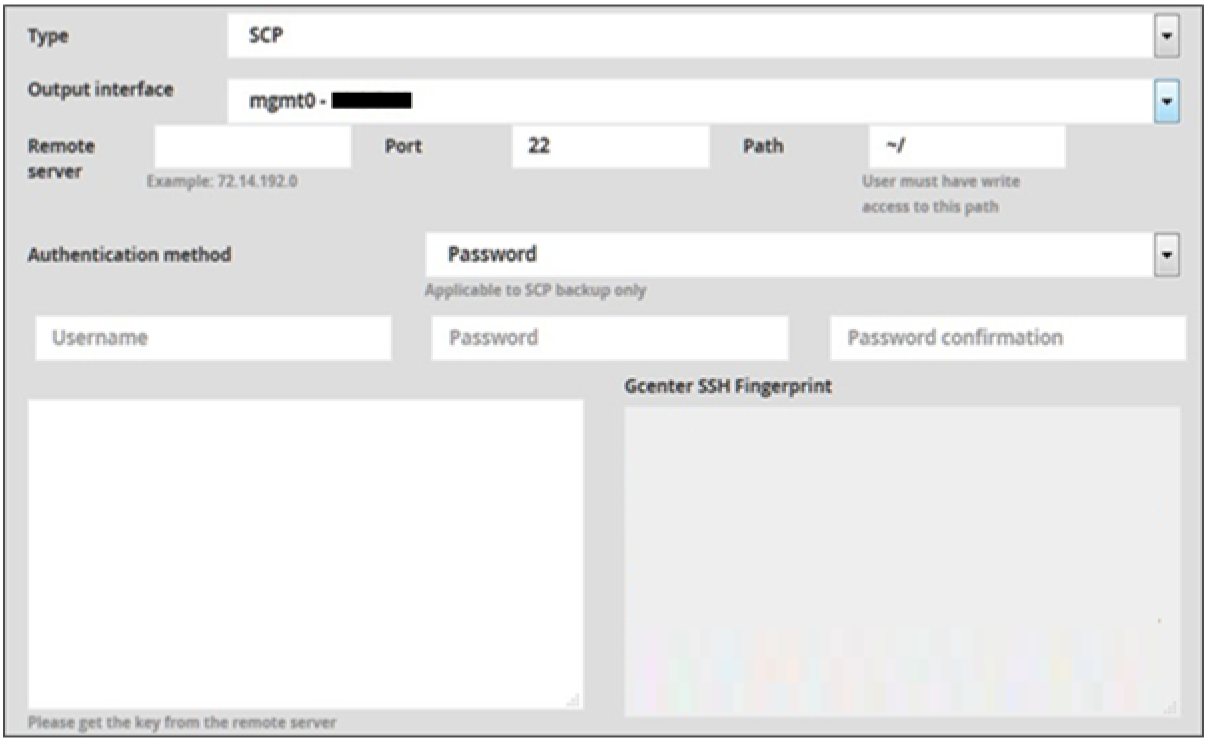
- Local: the backup is only done locally, directly downloadable on the **GCENTER** web interface, in the Operations tab of the same section.



Backup on a remote server or only locally

Type: Local ▾

- SCP: enables externalisation of the backup to a remote SSH server.



Type: SCP

Output interface: mgmt0 - [redacted]

Remote server: Example: 72.14.192.0

Port: 22

Path: ~/ User must have write access to this path

Authentication method: Password Applicable to SCP backup only

Username

Password

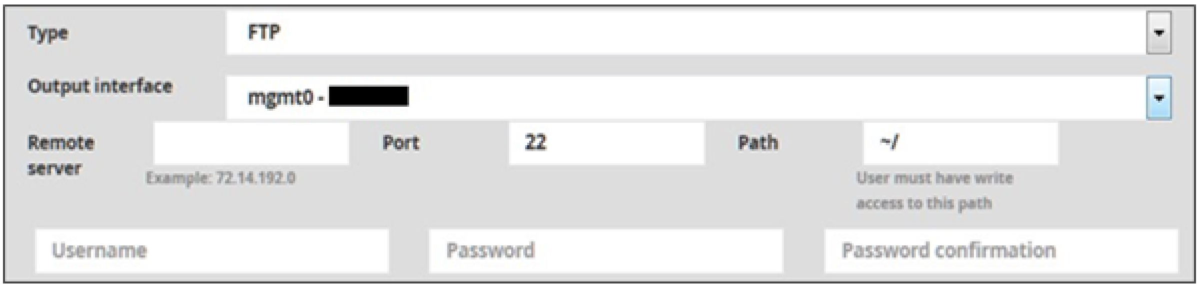
Password confirmation

Gcenter SSH Fingerprint

Please get the key from the remote server

Remote server: is the IP address or the FQDN of the remote server (Example: *72.14.192.0*) **Port**: is the listening port of the SSH server **Path**: is the location where the file will be saved on the remote server (the user account employed must have read and write rights to this path). **Authentication method**: Depending on the *password* or *public key* method, the administrator must, in addition to entering the connection account, respectively provide the password or ensure that the public key of the **GCENTER**, present in the **Gcenter SSH Fingerprint** field, is entered on the remote server (by placing it in the file: *~/.ssh/authorized_keys*).

- FTP: enables externalisation of the backup to a remote FTP server.



Type: FTP

Output interface: mgmt0 - [redacted]

Remote server: Example: 72.14.192.0

Port: 22

Path: ~/ User must have write access to this path

Username

Password

Password confirmation

Remote server is the IP address or the FQDN of the remote server (Example: *72.14.192.0*) **Port**: is the listening port of the FTP server '**Path**: is the location where the file will be saved on the remote server (the user account employed must have read and write rights to this path). **Username**: the name of the user **Password**: the user's password.

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 downloaded correctly.

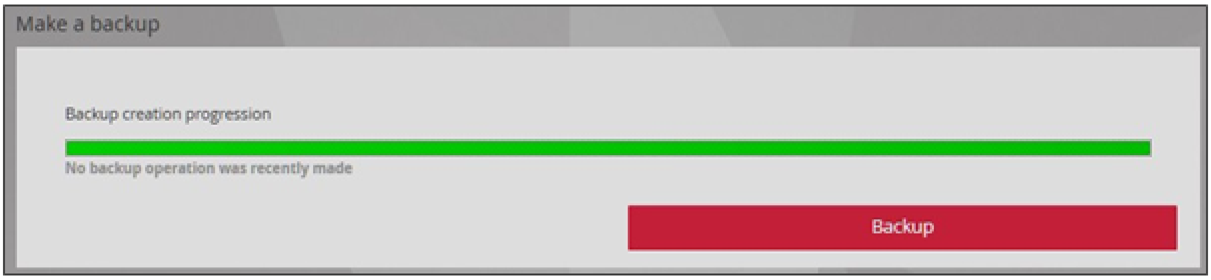
Once the configuration is complete, it will be necessary to click on **Update backup configuration** to save the changes.

43.1 Operations

Rôle Administrateur

Menu: Administrators > Backup / Restore > Operations

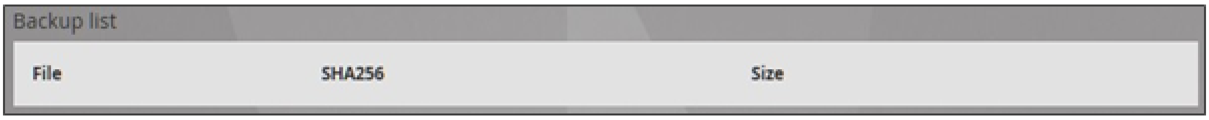
This menu enables the administrator to initiate the process of backing up the **GCENTER** configuration and/or restoring the configuration using a GATEWATCHER backup file.



No backup operation was recently made

Backup will start the solution's backup process. After this step, an archive '*GCENTERName.local-backup.gwc*' of several gigabytes is downloaded.

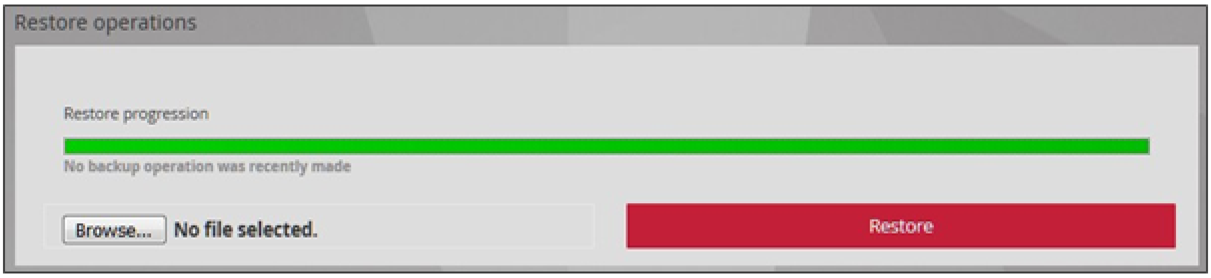
The backup archives that are already saved locally on the **GCENTER** are displayed in this menu.


Backup list

File	SHA256	Size

The file is downloadable from 'Download', the timestamp of the last save in UTC in the format [**year/month/day hh**: **mm**: **ss**], the Shasum and the size in MB and GB are available in the columns 'Backup', 'SHA256' and 'Size' respectively.

The latter must be saved so that it can be sent to the administrators of the TRACKWATCH solution or to GATEWATCHER support. Indeed, this archive can only be extracted by an advanced administrator having knowledge of the backup data extraction password.



No backup operation was recently made

No file selected.

Once extracted, the administrator will be able to recover the system from **Restore** to a working state following an incident, for example, by importing the archive.

Chapter 44

Data Management

In order for the TRACKWATCH solution to function properly, the **GCENTER** server works with log files. These log files record all the traffic captured by the **GCAP** probe as well as the information from the GScan. This information can proliferate quickly taking up a lot of disk space.

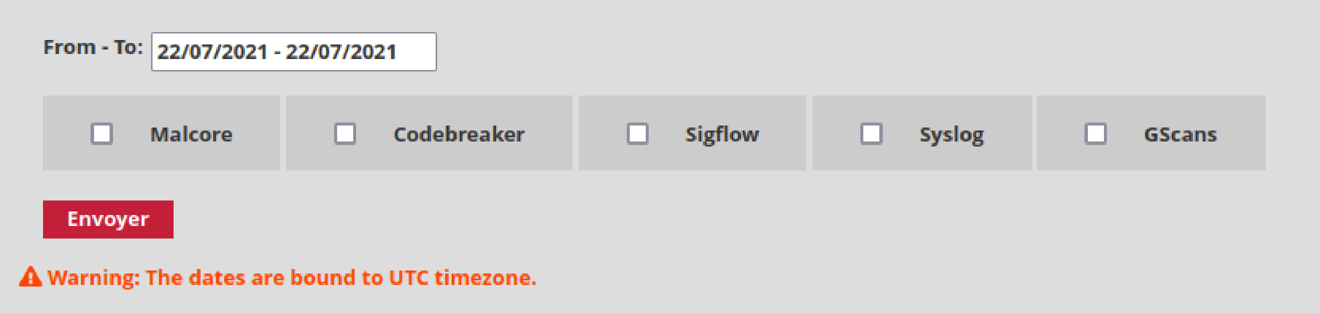
Although *a retention policy* may be in place, this data can, if the need arises, be manually deleted by the administrator at any time prior to the data retention period expiring.

44.1 Data deletion

Rôle Administrateur

Menu: Administrators > GCenter > Data Management

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.



From - To: 22/07/2021 - 22/07/2021

□ Malcore □ Codebreaker □ Sigflow □ Syslog □ GScans

Envoyer

⚠ Warning: The dates are bound to UTC timezone.

Over a given period of time, the information tables of the analysis engines MALCORE, CODEBREAKER, SIGFLOW, and the GSCAN portion including the MALCORE and CODEBREAKER modules can be cleared. This period is selected by the administrator, who validates it by pressing **Apply**. However, this duration cannot exceed the total retention time of the data already preconfigured in the solution. The same applies to the ICAP and Syslog services.

> **Important:**
>
> Data not yet processed will also be deleted.

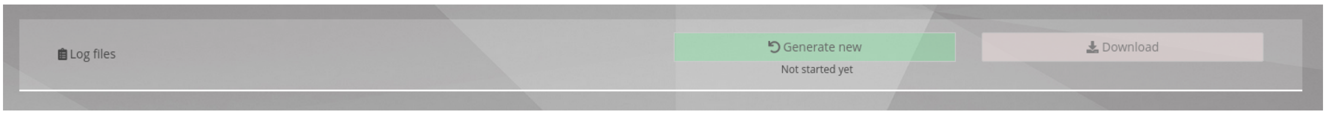
After ticking the appropriate boxes over a period of time, the administrator must validate the action by clicking **Send**.

Chapter 45

Diagnostics

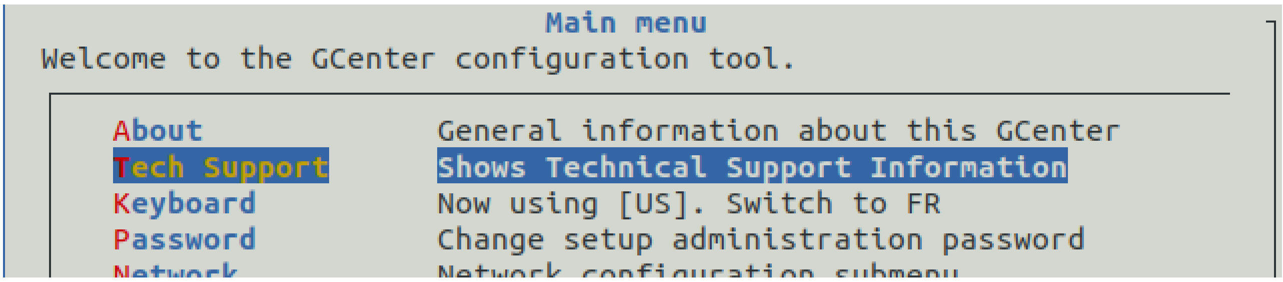
This portion of the **ADMINISTRATORS** section of the **GCENTER** enables administrators of the TRACKWATCH solution to verify or debug certain configuration settings. It will also enable GATEWATCH support to identify and resolve any possible malfunctions.

From this diagnostic interface, the administrator has the ability to export the configuration parameters of the **GCENTER**:

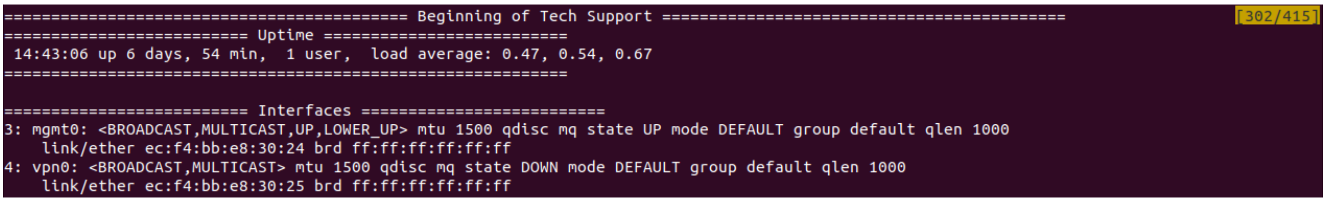


It is also possible from the *setup* menu to generate a "Tech Support".

This is done by logging into the **GCenter** as a *setup* user, then selecting the *Tech Support* entry.



```
                         Main menu
 Welcome to the GCenter configuration tool.

      About              General information about this GCenter
      Tech Support       Shows Technical Support Information
      Keyboard           Now using [US]. Switch to FR
      Password           Change setup administration password
      Network            Network configuration submenu
```



```
=========================================== Beginning of Tech Support ===========================================     [302/415]
========================== Uptime ==========================
 14:43:06 up 6 days, 54 min,  1 user,  load average: 0.47, 0.54, 0.67
============================================================

========================== Interfaces ==========================
3: mgmt0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000
    link/ether ec:f4:bb:e8:30:24 brd ff:ff:ff:ff:ff:ff
4: vpn0: <BROADCAST,MULTICAST> mtu 1500 qdisc mq state DOWN mode DEFAULT group default qlen 1000
    link/ether ec:f4:bb:e8:30:25 brd ff:ff:ff:ff:ff:ff
```

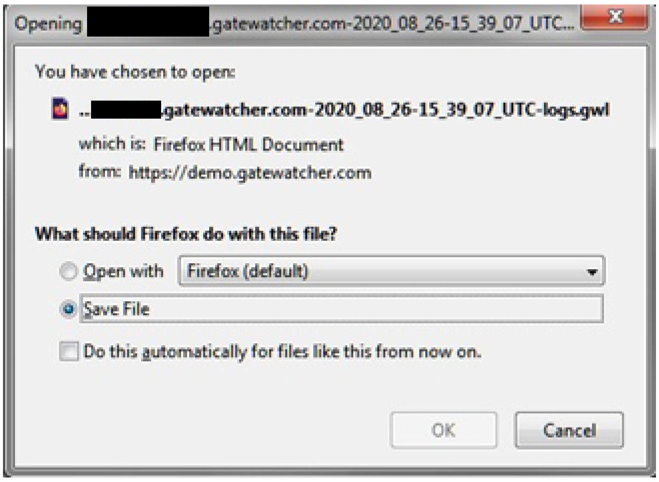
This command enables you to easily copy and paste a Gcenter health status.

45.1 Log files

Rôle Administrateur

Menu: Administrators > GCenter > Diagnostics

System logs providing details of the **GCENTER** equipment and its configuration can be exported from this interface. This export will be highly useful for the GATEWATCHER support team for any type of diagnosis. The export file log is protected by a password only known by the GATEWATCHER administrator team.



Opening [redacted].gatewatcher.com-2020_08_26-15_39_07_UTC...

You have chosen to open:

..[redacted]gatewatcher.com-2020_08_26-15_39_07_UTC-logs.gwl

which is: Firefox HTML Document

from: https://demo.gatewatcher.com

What should Firefox do with this file?

○ Open with Firefox (default)

● Save File

□ Do this automatically for files like this from now on.

After this step, a '*GATEWATCHER_logs.gwp*' archive of several megabytes is downloaded. The latter must be saved so it can be sent to the GATEWATCHER support.

Indeed, this archive can only be extracted by an advanced administrator having knowledge of the data extraction password.

Once extracted, the administrator will have access to all the configuration parameters of the **GCENTER** management server and will be able to diagnose any problem. Messages from all logs will be accessible as well as all system calls from the system.

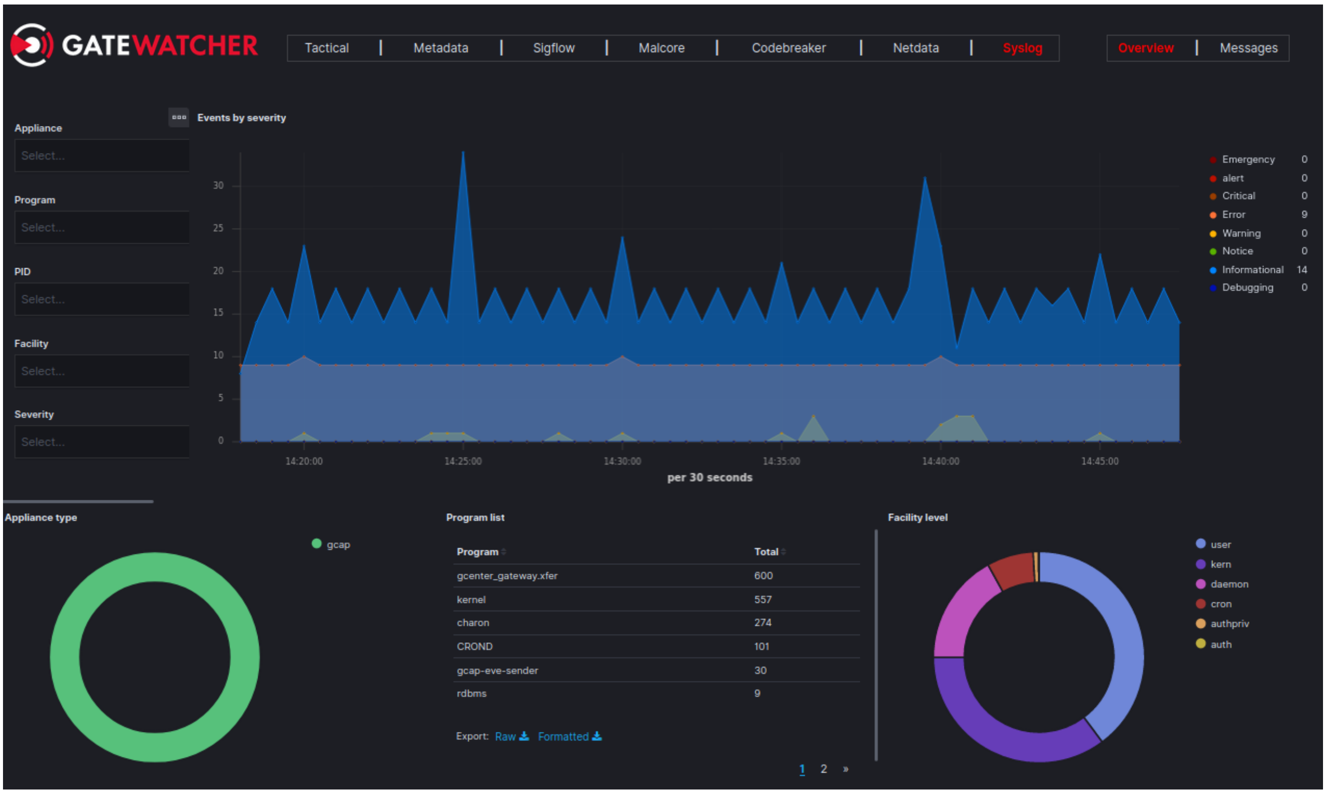
Chapter 46

Solution logs

Rôle Administrateur

Menu: Administrators > GCenter > Trackwatch Logs

This entry redirects to a kibana dashboard displaying the different logs of the TRACKWATCH solution.



Emergency	0
alert	0
Critical	0
Error	9
Warning	0
Notice	0
Informational	14
Debugging	0

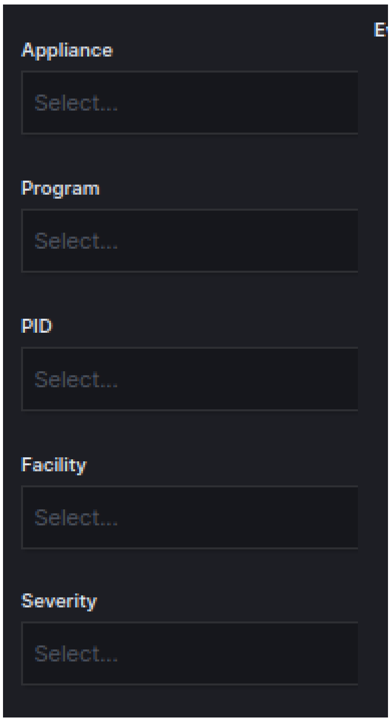
Program list

Program	Total
gcenter_gateway.xfer	600
kernel	557
charon	274
CROND	101
gcap-eve-sender	30
rdbms	9

Export: Raw Formatted

1 2 »

From this dashboard it is possible to filter the different fields from the left menu



Appliance

Select...

Program

Select...

PID

Select...

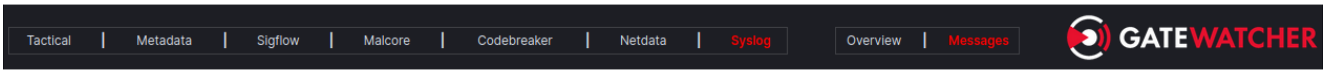
Facility

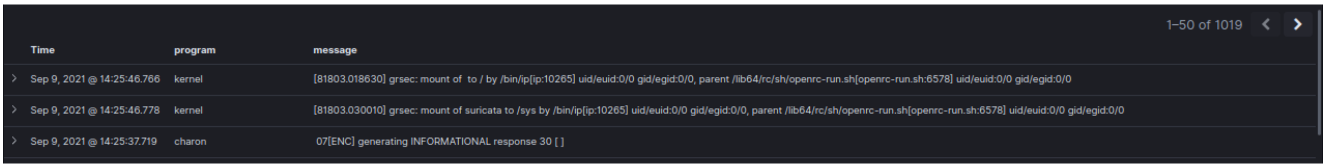
Select...

Severity

Select...

The logs of the various applications are displayed at the bottom of the overview screen, or by clicking on the **Messages** view.





1–50 of 1019

Time	program	message
Sep 9, 2021 @ 14:25:46.766	kernel	[81803.018630] grsec: mount of to / by /bin/ip[ip:10265] uid/euid:0/0 gid/egid:0/0, parent /lib64/rc/sh/openrc-run.sh[openrc-run.sh:6578] uid/euid:0/0 gid/egid:0/0
Sep 9, 2021 @ 14:25:46.778	kernel	[81803.030010] grsec: mount of suricata to /sys by /bin/ip[ip:10265] uid/euid:0/0 gid/egid:0/0, parent /lib64/rc/sh/openrc-run.sh[openrc-run.sh:6578] uid/euid:0/0 gid/egid:0/0
Sep 9, 2021 @ 14:25:37.719	charon	07[ENC] generating INFORMATIONAL response 30 [ ]

Chapter 47

Emergency mode

In order to preserve the solution's detection capacity, the **GCenter** can enter into a special regime called **Emergency Mode**.

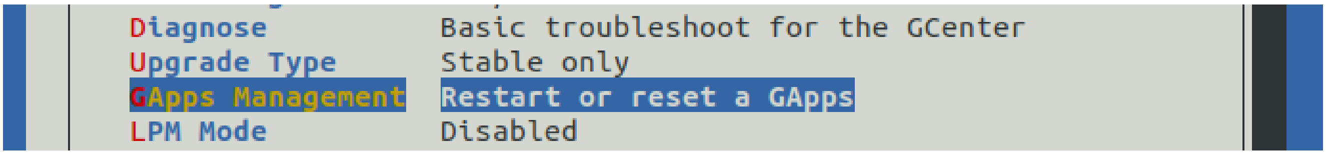
This mode is automatically triggered in the event of heavy usage of the **GCenter** disk space used to store data. In such a case, the solution will automatically apply the *Data Deletion* procedure thus ensuring the continuity of detection services.

Chapter 48

GApps management

GApps represent the many services that make up the TRACKWATCH solution. It may be necessary in some instances to restart or reset them.

This can be done by logging in to the GCenter via ssh as the *setup* user and selecting the *GApps Management* entry.

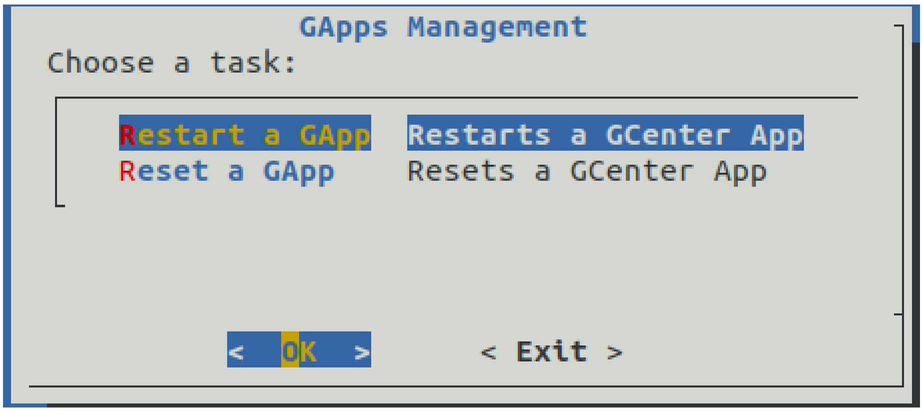


```
Diagnose              Basic troubleshoot for the GCenter
Upgrade Type          Stable only
GApps Management      Restart or reset a GApps
LPM Mode              Disabled
```

Next, the choice is offered to restart a service or to reset it.

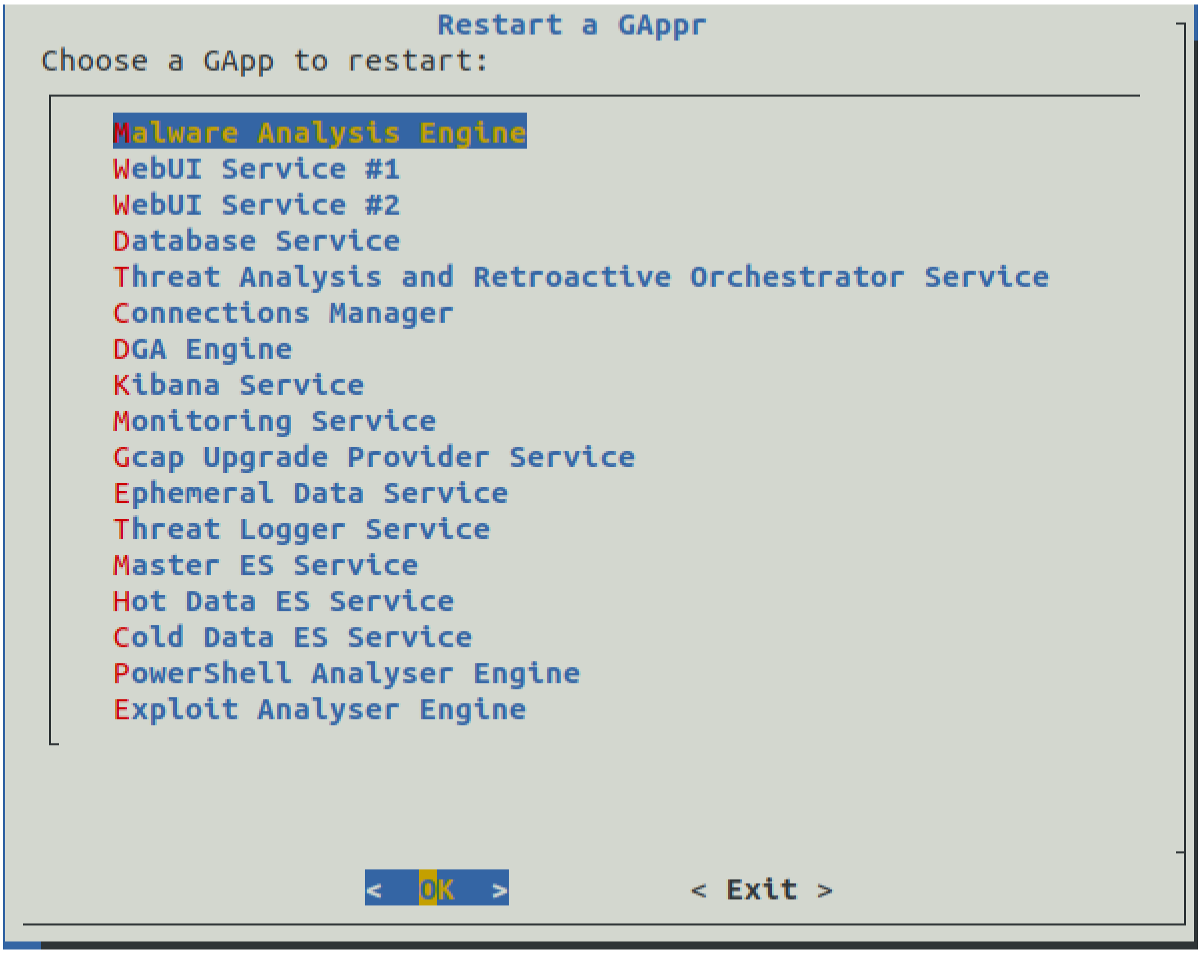
Warning:

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



```
             GApps Management
Choose a task:

    Restart a GApp    Restarts a GCenter App
    Reset a GApp      Resets a GCenter App


          <  OK  >        < Exit >
```

Finally, simply select the service from the list to be restarted or reset.



```
Restart a GAppr
Choose a GApp to restart:

    Malware Analysis Engine
    WebUI Service #1
    WebUI Service #2
    Database Service
    Threat Analysis and Retroactive Orchestrator Service
    Connections Manager
    DGA Engine
    Kibana Service
    Monitoring Service
    Gcap Upgrade Provider Service
    Ephemeral Data Service
    Threat Logger Service
    Master ES Service
    Hot Data ES Service
    Cold Data ES Service
    PowerShell Analyser Engine
    Exploit Analyser Engine

            <  OK  >            < Exit >
```

Chapter 49

MPL: reminders

Some reminders of the main principles of the MPL:

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 Defence Code amended by Act no. 2015-917 of 28 July 2015 - Art. 27

- Establish organisational and technical measures
- Define procedures for identifying and reporting security incidents affecting vital information systems (SIIV)

The objectives are to protect national critical infrastructures against cyber attacks, reduce exposure to risks, and optimise the quality of services provided by organisations.

Requirements for OIVs and security incident detection service provider (PDIS) actors are to be taken into account on **TRACKWATCH** 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

Chapter 50

MPL applied to GCENTER

Here we will discuss the specific configuration steps that will enable the TRACKWATCH solution to meet the requirements of the Military Programming Law.

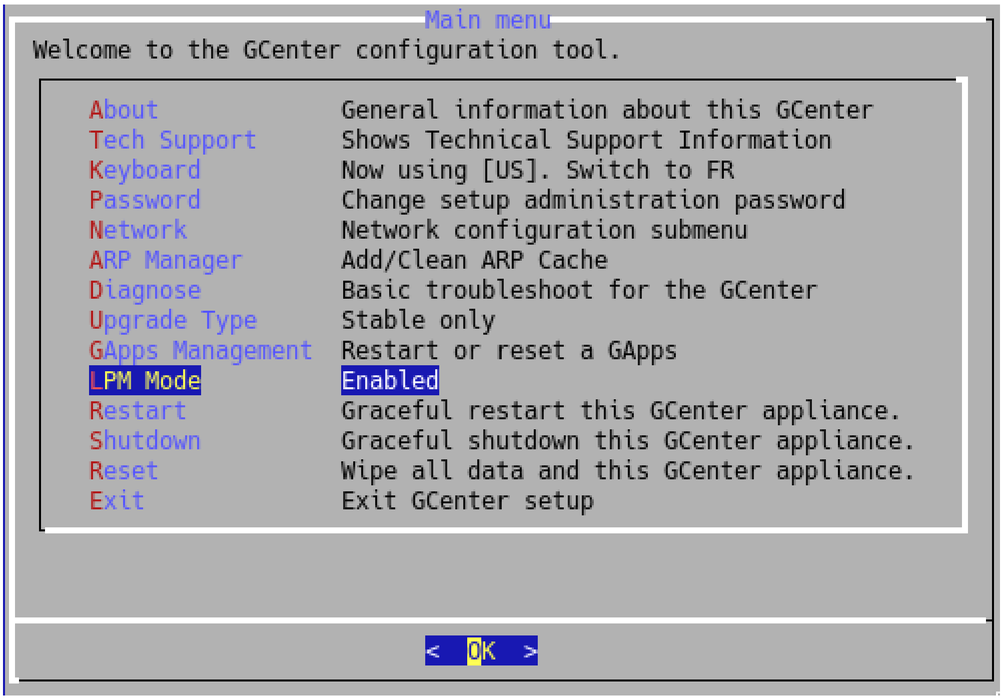
Although a number of actions are performed automatically when entering MPL mode, the administrator will have to customise and modify some of the parameters manually:

- Strengthening (GRsec, binaries, PAX and modules) `automatic action`
- GScan `automatic action`
- AD/LDAP `manual action required`
- USB port `automatic action`
- Offline Update - manual action required
- Upgrade Hotfix `automatic action`
- Interface separation `manual action required`
- Certificate integration `manual action required`
- IDRAC Disabled `manual action required`
- The groups `manual action required`

50.1 Automatic action

50.1.1 Strengthening (GRsec, binaries, PAX, and modules)

To perform a strengthening of the **GCENTER** and enter MPL mode, follow the procedure below by connecting to the **SETUP** interface:



```
Main menu
Welcome to the GCenter configuration tool.

  About               General information about this GCenter
  Tech Support        Shows Technical Support Information
  Keyboard            Now using [US]. Switch to FR
  Password            Change setup administration password
  Network             Network configuration submenu
  ARP Manager         Add/Clean ARP Cache
  Diagnose            Basic troubleshoot for the GCenter
  Upgrade Type        Stable only
  GApps Management    Restart or reset a GApps
  LPM Mode            Enabled
  Restart             Graceful restart this GCenter appliance.
  Shutdown            Graceful shutdown this GCenter appliance.
  Reset               Wipe all data and this GCenter appliance.
  Exit                Exit GCenter setup

                       <  OK  >
```

- Connect via the **GCENTER** setup account (SSH or terminal)
- Select the 'MPL Mode' tab that is disabled by default
- Validate the option to switch to MPL mode

The equipment will then restart with the configuration correctly loaded.

This will enable the **GCENTER** to reduce its attack surface and thus reduce the risk. Indeed, by using this mode, it integrates the GRSECURITY improvements, including PaX. Enabling the attack surface to be reduced even at the core level.

50.1.2 GScan Service

In the same way, some functions are disabled. This is the case of the **GScan** service that is disabled for the detection of potential malware or shellcodes.

This feature automatically deactivates itself after enabling MPL mode in the SETUP.

50.1.3 USB Port

When the **TRACKWATCH** solution is in MPL mode, the USB ports are automatically disabled once the keyboard or other peripheral device is disconnected. The **GCENTER** or **GCAP** probe must be rebooted and the device must be reconnected prior to startup to ensure that it is supported. This limits access to the device's TTY.

The change is made automatically after switching to MPL mode from the **SETUP** profile settings menu.

50.1.4 Hotfix upgrade

In the context of an IS subject to the MPL, the **GCENTER** will not be able to apply a *hotfix* type of modification to the solution in order to correct minor problems on the solution without rebooting.

This *GUM* parameter is automatically deactivated after validation of the MPL mode in the **SETUP**.

However, patches can still be applied via the *upgrade* process.

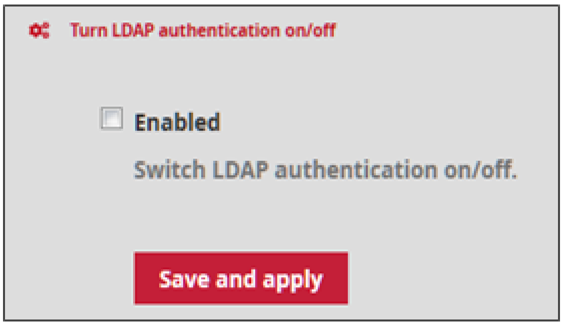
50.2 Manual action

The following list of actions should only be performed by an administrator of the TRACKWATCH solution.

50.2.1 AD/LDAP account

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.



Turn LDAP authentication on/off

□ Enabled

Switch LDAP authentication on/off.

Uncheck the **Enabled** box and click **Save and apply** to apply the change. This change will cause the application to restart, resulting in a disconnection from the user page. Once the administrator clicks **Confirm**, it will be necessary to reconnect to the interface.

After this manipulation, a green banner validates the modification. The LDAP interconnection status section indicates that the **GCENTER** is now disconnected from the Active Directory or LDAP.

50.2.2 IDRAC Disabled

The **TRACKWATCH** solution is installed on Dell equipment. The latter offers the possibility of configuring an IP address independent of the capture environment enabling it to be remotely controlled. These connection interfaces are referred to as IDRAC by the brand manufacturer. According to the ANSSI, it is recommended they be deactivated for obvious security reasons. However, they can be reactivated at any time by the administrator to facilitate maintenance.

50.2.3 Separation of interfaces

In the context of an IS subject to the MPL, 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 the event flow generated by the **GCAP** probes must be on two different interfaces respectively [MGMT0] and [VPN0].

This change does not take effect automatically after the MPL mode is activated, even if the network cables are correctly connected. It is precisely from the **SETUP** interface that the administrator can make the change and manually add a new IP address for the [VPN0] interface. Only the [MGMT0] and [VPN0] interfaces are affected. Refer to the setup document in order to make the change.

Details of the flows in this mode are described in the [*Flow Matrix*] section (install.html#flow-matrix)

The sending of logs to a security information and event management (SIEM) in an operating zone will be done through a dedicated interface. We separate the management interface (administrator) from the log export interface (operator).

> important:: In MPL mode, the [ICAP0] interface is disabled and the [SUP0] interface must be in a different network than [MGMT0].

50.2.4 Offline Update

In order for the **TRACKWATCH** 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 the [Manual Engine Update] section (update.html#manual-engine-update) of this document. This corresponds to a manual update.
- Or via a location on the network, disconnected from the internet. This corresponds to a *Local* update (see section *Local mode*).

50.2.5 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 defence.

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.

The *SSL Settings* section indicates how to add your own SSL configuration.

50.2.6 Groups

In order to respect the separation of roles within the TRACKWATCH solution, two profiles are available.

The system administrator performs several types of tasks. Changes to the network configuration, viewing, editing, and updating detection rules and packages.

The profile may add, delete, edit, activate, deactivate, and view information about detection rules. The system administrator will manage the creation, import, export, and destruction of cryptographic elements, consult the version, alert logs, perform system and software updates, and have user management for the creation, deletion, and modification of accounts associated with the roles. In addition to being able to modify the global parameters of the **GCENTER**, the administrator will also be able to stop, start, and restart the functionalities or the solution itself.

The operator can view all of the operating logs and alerts generated. In addition, the operator will also be able to activate and deactivate the storage of additional technical information while defining the duration.

The profile will be able to download the captured data, interact with the analysis and download platform if configured, scan files, observe the SmartMap and most importantly read or modify information related to the detection rules (addition, deletion, specific actions).

In the administration interface of the **GCENTER**, default groups are already created to facilitate managing the client's users.

Profiles are managed from the *user management*.

Download link for this documentation : `PDF Documentation GCenter`