Documentation GCENTER 2.5.3.101

Gatewatcher

Date de création: Decembre, 2020

Dernière mise à jour : Octobre, 2024

Contents

Chapter 1

Chemin d'upgrade

La règle générale concernant les chemins de mise à jour est qu'**il est nécessaire d'être sur le dernier hotfix** avant d'installer une mise à jour majeure.

Il en va de même pour **l'application des hotfix qui doit être effectuée dans l'ordre** (par exemple v100 -> v100-hf1 -> v100-hf2 -> ..).

Dans le cas contraire, cela sera notifié dans la note de mise à jour de la version concernée.

Chapter 2

Release Notes

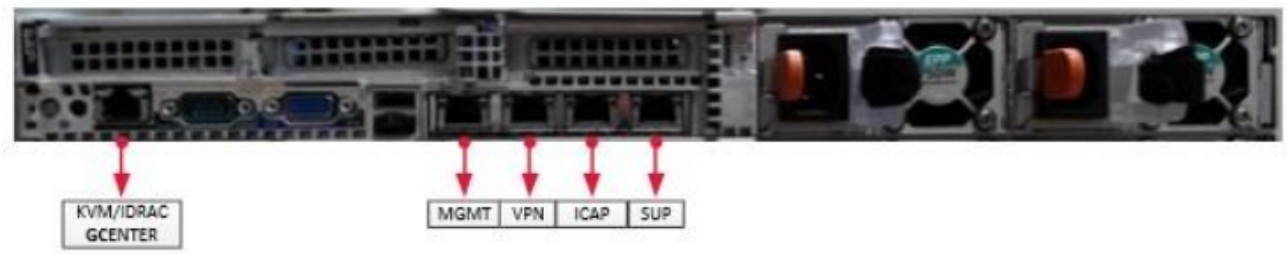
Les notes de versions sont référencées dans le tableau suivant. Ces notes de version (ou *Release Note*) contiennent la liste des changements apportés par la version données, la liste des problématiques connues mais également des notes importantes liées au processus d'upgrade.

Chapter 3

Présentation des équipements

3.1 GCenter

Le **GCENTER** est l'équipement de gestion centralisée de la solution TRACKWATCH, il permet d'une part de recevoir et d'analyser les alertes émises depuis les sondes **GCAP** et d'autre part de configurer la solution TRACKWATCH de façon intuitive.



Le **GCENTER** dispose donc de 5 interfaces ayant les rôles suivants :

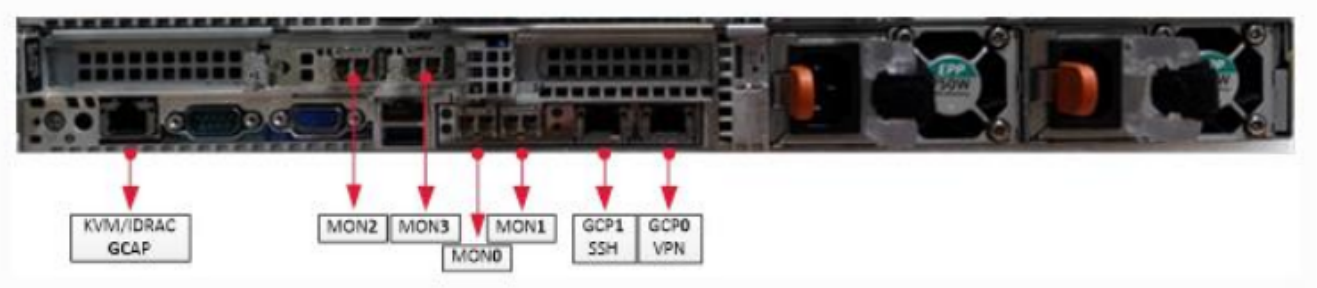
- **KVM/IDRAC** : Interface d'administration à distance
- **SUP0** : Interaction avec Nagios
- **ICAP0** : Interaction avec le Proxy
- **VPN0** : Interface dédiée aux VPN avec les **GCAP** (optionnel)
- **MGMT0** : Interface de management

Note:

Bien que le nom des interfaces puisse laisser penser que ces interfaces sont dédiées, il est possible d'utiliser ces interfaces pour d'autres besoins via les options "output interfaces".

3.2 GCAP

Les sondes **GCAP** permettent d'analyser le flux reçu afin de détecter, capturer, reconstruire, trier et transmettre les fichiers, codes malveillants, évènements au **GCENTER**



En plus des 3 interfaces de gestion, les sondes **GCAP** disposent d'un nombre variable d'interface de capture :

- **KVM/IDRAC** : Interface d'administration à distance
- **GCP0** : Interface VPN (et optionnellement interface de management)
- **GCP1** : Interface dédiée de management (optionnel)
- **mon0-monX** : Interface de capture

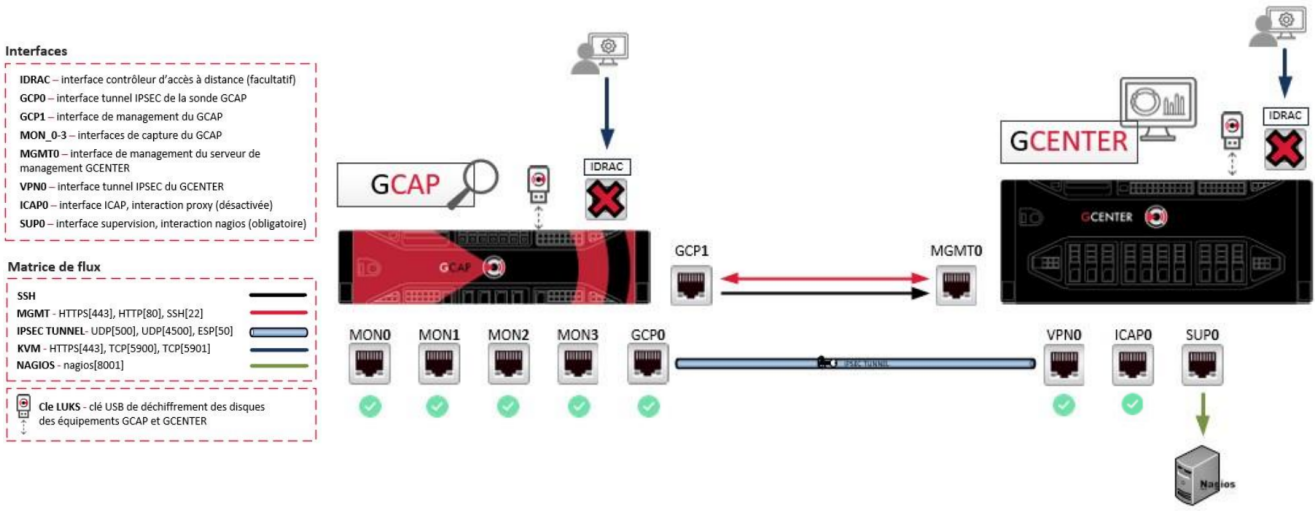
L'utilisation de l'interface **GCP1** afin de séparer le flux de management du trafic IPSec du VPN peut être obligatoire dans le cas d'environnement sensible. Dans le cas contraire il est possible de n'utiliser que l'interface **GCP0** pour faire transiter les flux de management et VPN.

Chapter 4

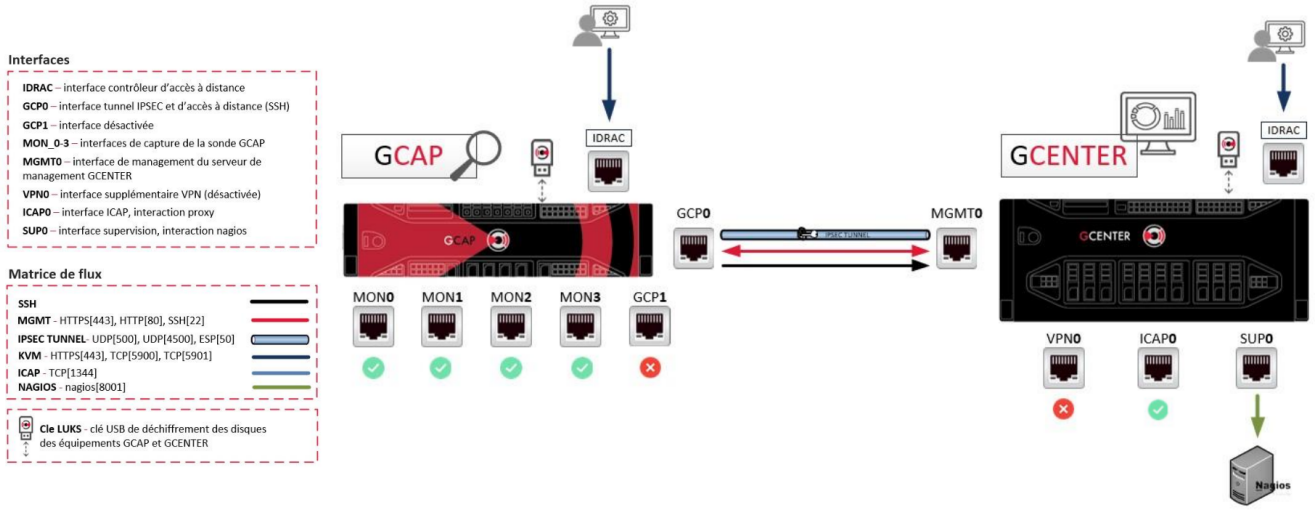
Matrice de flux

Comme expliqué précédemment, deux modes de communication sont possible concernant la communication entre les **GCAP** et le **GCENTER**.

Le premier mode, qui est le mode obligatoire dans le cas d'un environnement sensible est le suivant :



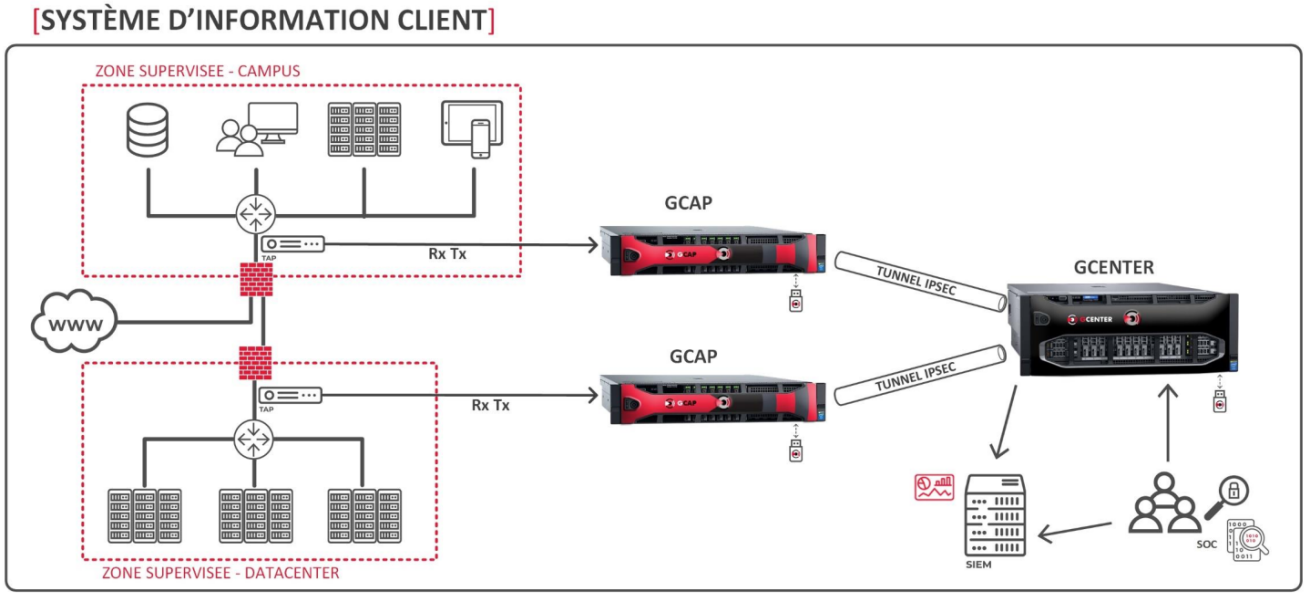
Le second mode, permet quant à lui de mutualisé une interface pour y faire transiter les flux de management et du VPN.

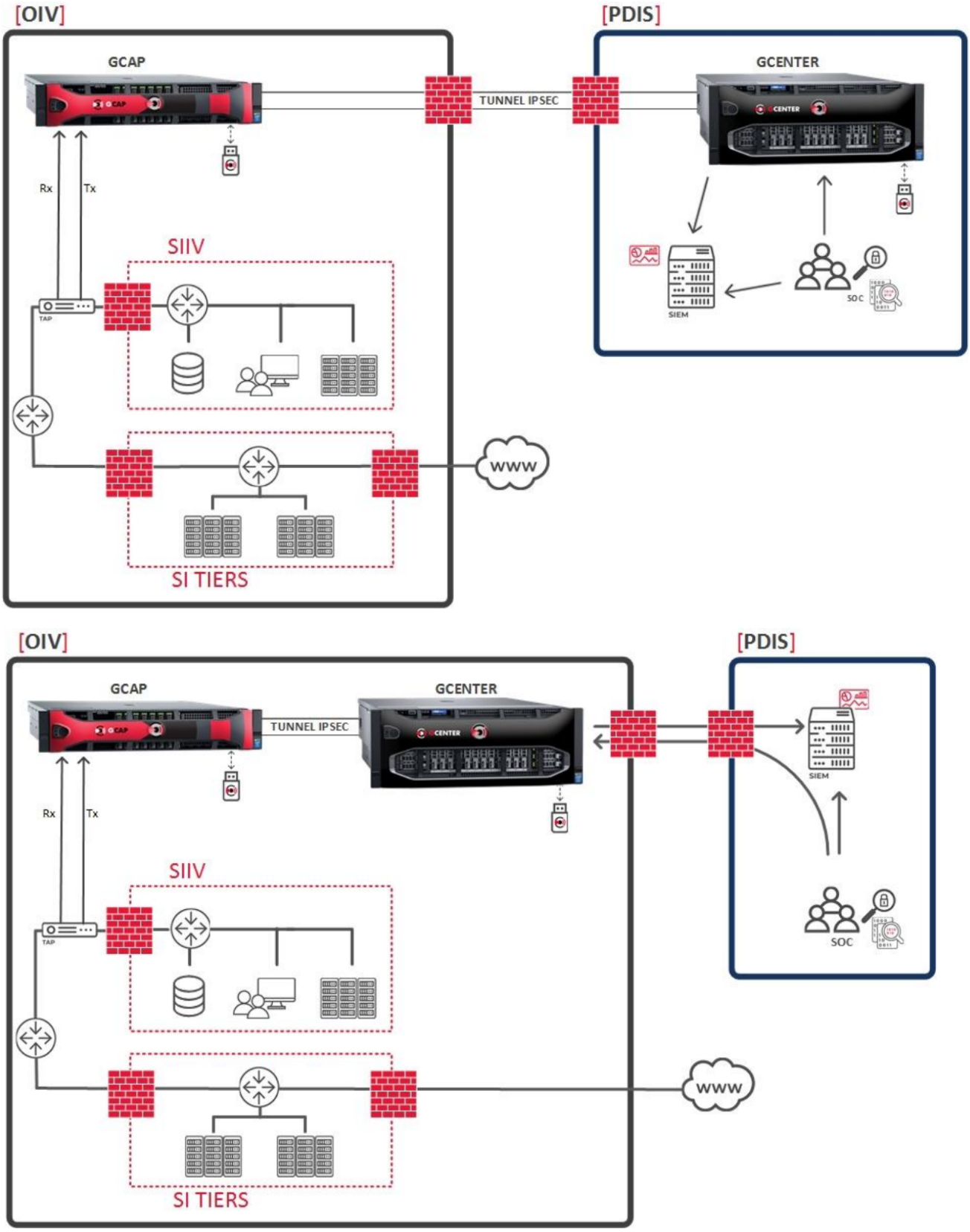


Chapter 5

Exemple d'architectures

Bien que l'implantation de la solution TRACKWATCH soit dépendante de l'architecture du SI, voici trois exemples d'implémentation type.





Dans le cas de système d'information sensible (soumis à la LPM par exemple), parmi les exemples fournis seuls les deux derniers sont possibles.

Chapter 6

Configuration

6.1 Configuration initiale

Note:

L'installation et la configuration des sondes **GCAP** sont abordées dans la documentation GCAP disponible à l'adresse https://docs.gatewatcher.com/gcap.html.

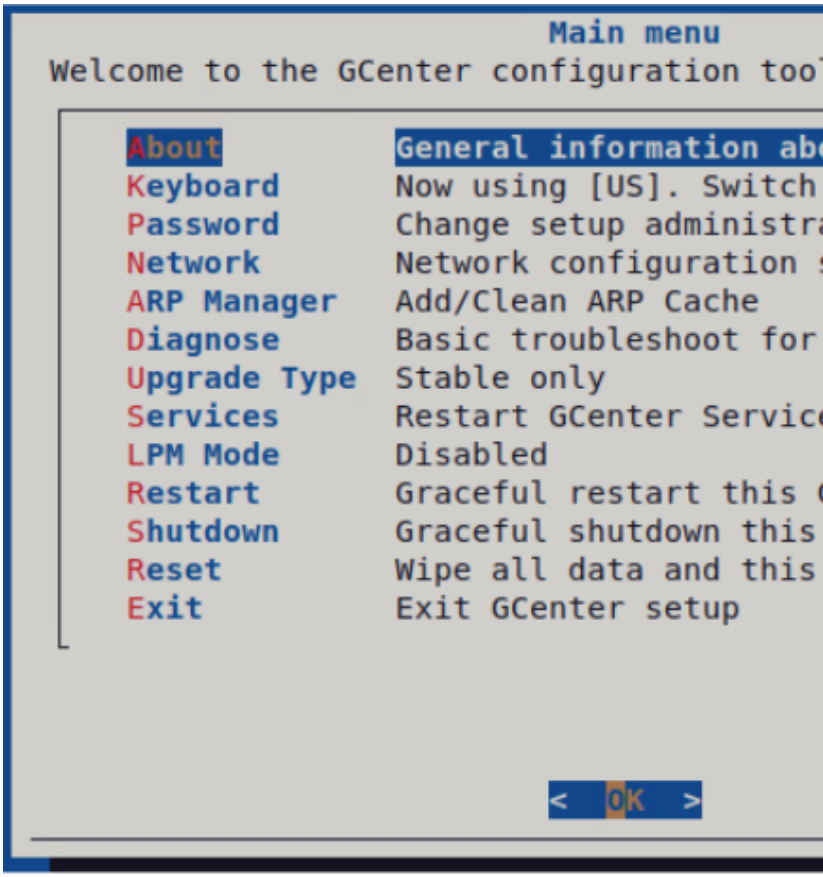
Bien qu'une grande partie de la solution soit déjà configurée par les équipes Gatewatcher, il sera nécessaire d'effectuer, a minima, la configuration réseau du GCenter afin de pouvoir accéder à l'interface.

Lors de la première connexion il sera nécessaire d'accéder au **GCENTER** via l'interface iDRAC ou un terminal afin d'effectuer la configuration réseau.

L'utilisateur à utiliser est l'utilisateur **setup**, par défaut le mot de passe de cet utilisateur est : **default**.

Important:

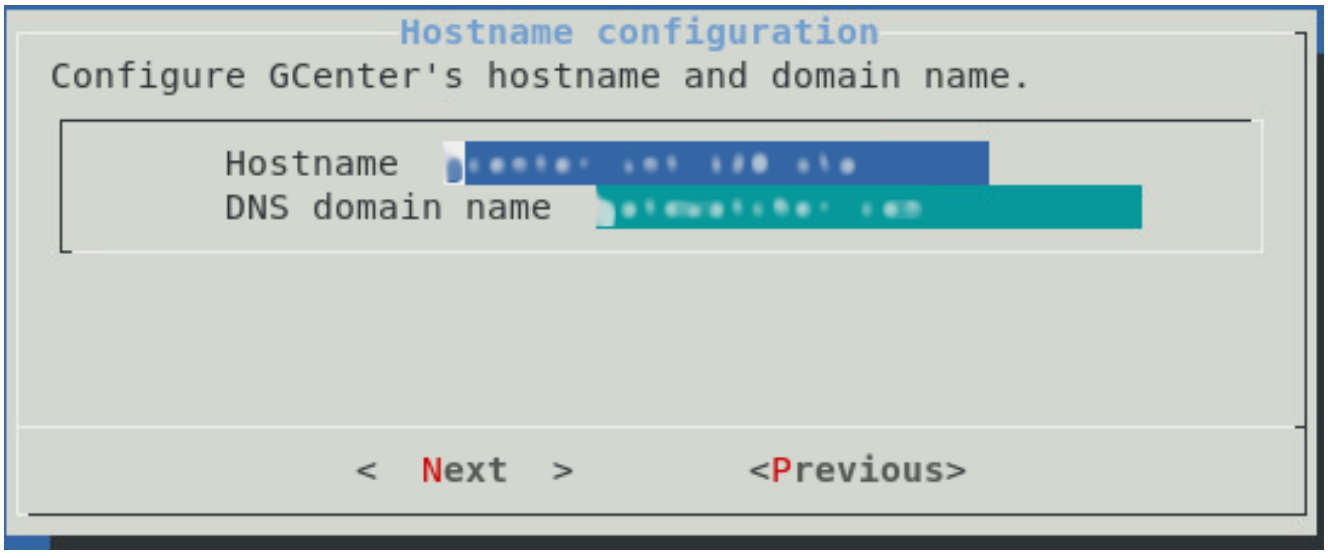
Il est important de changer ce mot de passe dès que possible.

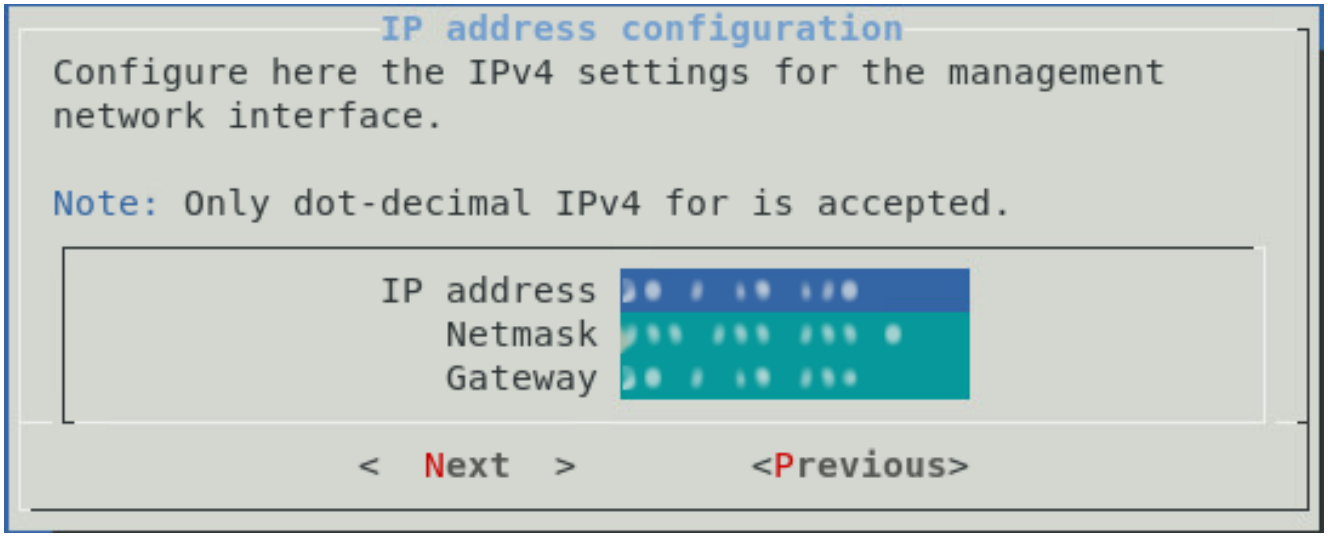


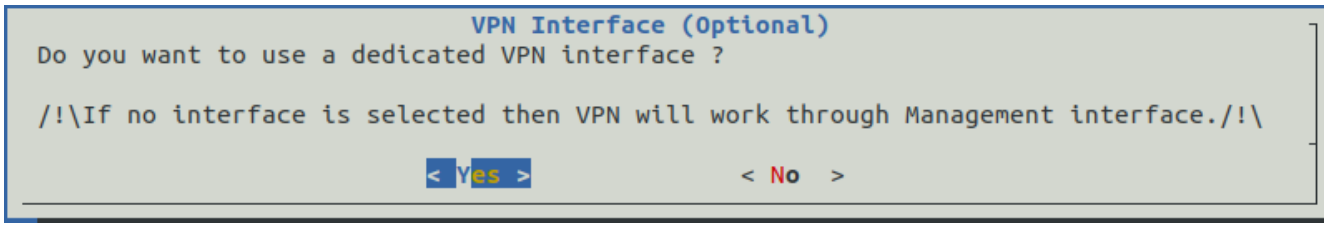
Une fois connecté, le menu de configuration s'affichera :

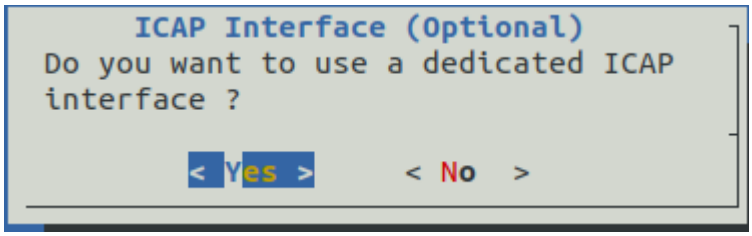
Si nécessaire, sélectionner l'entrée *Keyboard* afin d'utiliser une configuration de touche azerty.

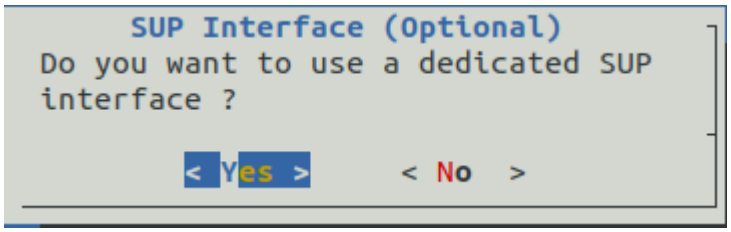
Puis en sélectionnant l'entrée *Network*, il suffira de répondre au différentes questions. Voici un exemple des questions posées lors de la configuration initiale

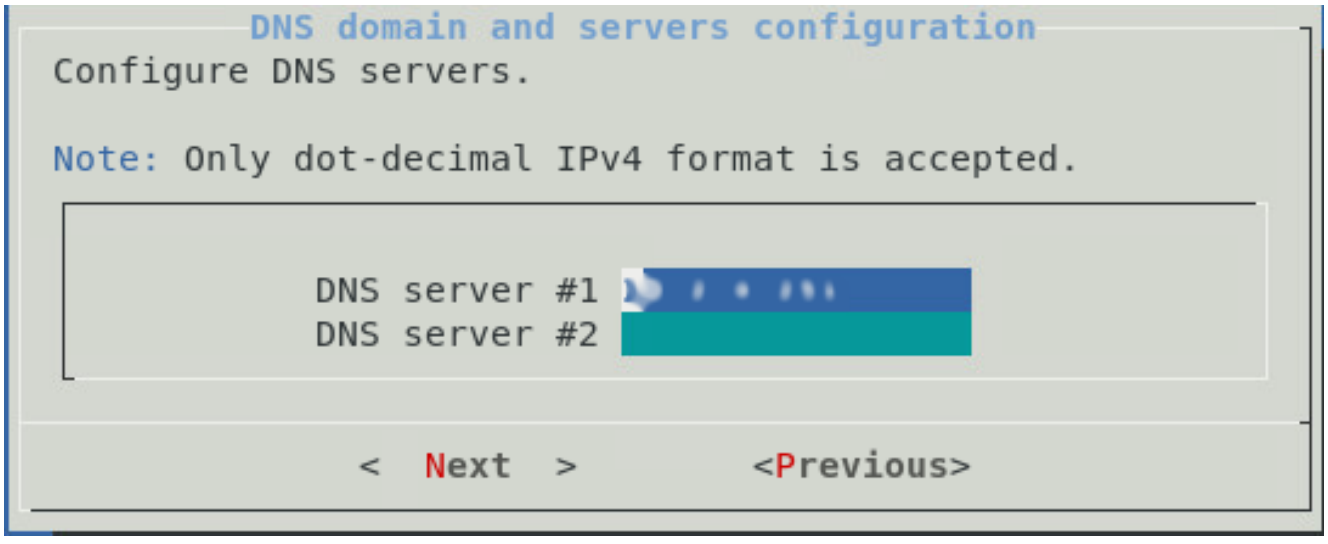


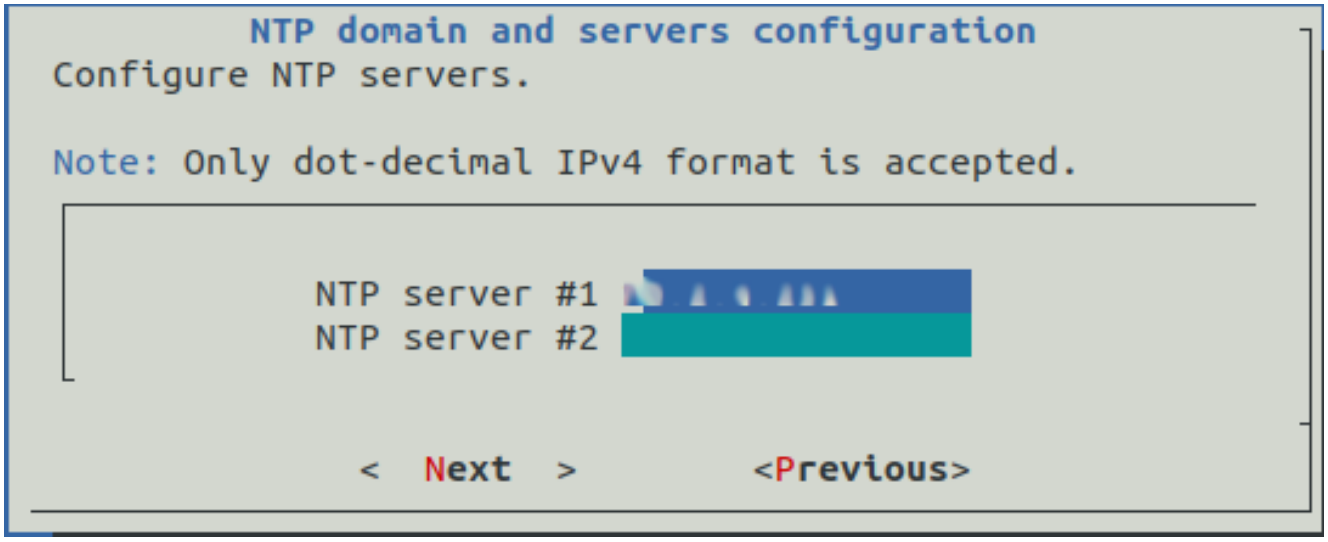

IP address configuration
Configure here the IPv4 settings for the management network interface.
Note: Only dot-decimal IPv4 for is accepted.
IP address
Netmask
Gateway
< Next >
<Previous>

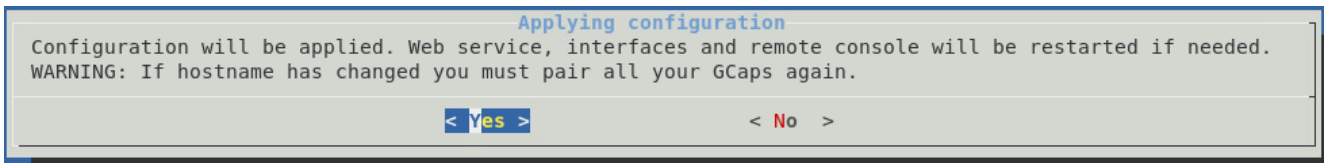

VPN Interface (Optional)
Do you want to use a dedicated VPN interface ?
/!\If no interface is selected then VPN will work through Management interface./!\
< Yes >
< No >

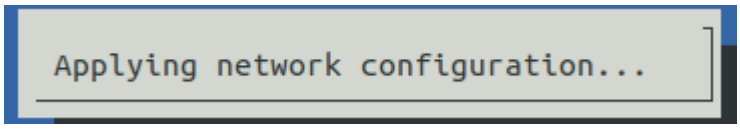

ICAP Interface (Optional)
Do you want to use a dedicated ICAP interface ?
< Yes >
< No >


SUP Interface (Optional)
Do you want to use a dedicated SUP interface ?
< Yes >
< No >


DNS domain and servers configuration
Configure DNS servers.
Note: Only dot-decimal IPv4 format is accepted.
DNS server #1
DNS server #2
< Next >
<Previous>

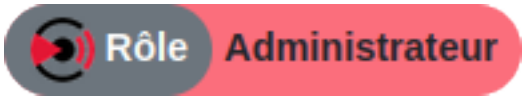






Une fois cette première configuration effectuée, il est possible de se connecter à l'interface du **GCENTER** via un navigateur web en https à l'adresse configurée.

6.2 Configuration globale



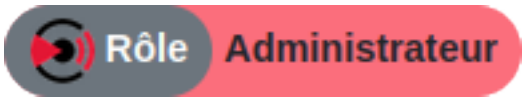
Une fois connecté à l'interface, dans le menu présent sur la gauche se trouve deux sections : Operators et Administrators correspondant aux actions pouvent être effectuées par les utilisateurs de ces groupes.

La partie *Gcenter - Configuration* de la section **ADMINISTRATORS** du **GCENTER** est tout particulièrement importante car elle permettra d'apporter des modifications majeures sur l'équipement, les fonctionnalités, les interconnexions ou même sur les résultats d'analyse.

Depuis cette interface de configuration, l'administrateur pourra personnaliser les paramètres de la solution de management **GCENTER** avec ces sept onglets :

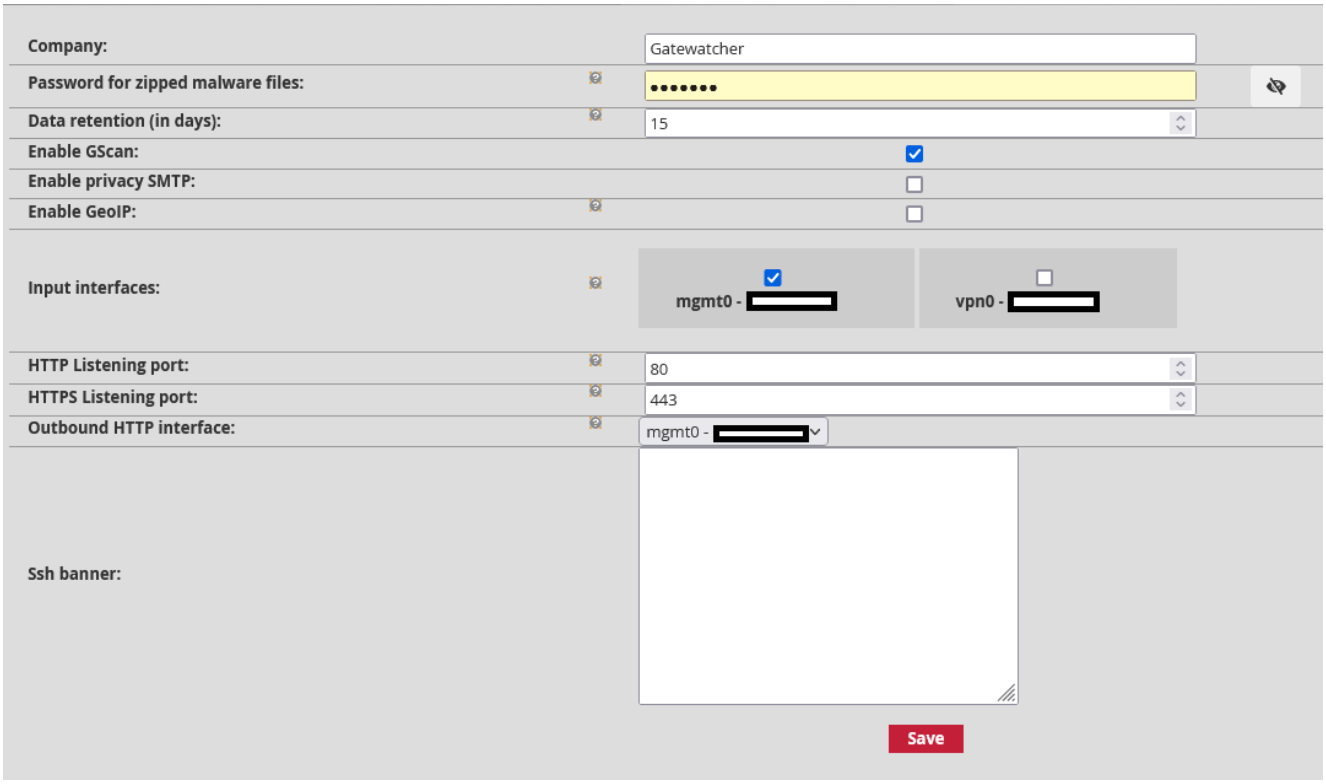
- *Nagios*
- *Global settings*
- *Netdata Export*
- *Proxy settings*
- *SSL settings*
- *Session age settings*
- *Licenses*

6.2.1 Global Settings



Menu : Administrators > GCenter > Configuration > Global Settings

Chacune des sous options du menu va être détaillée pour une meilleure compréhension du produit. Ces options vont vous permettre d'affiner au maximum vos critères pour optimiser au mieux le fonctionnement général.



Company (valeur par défaut : vide): Ce champ permet d'ajouter le nom de la société sur les rapports d'analyse de détection. Ces rapports peuvent être téléchargés après avoir fait une association entre la solution TRACKWATCH et la plateforme Intelligence.

Password for zipped malware files (valeur par défaut : vide) : permet de changer le mot de passe qui protégera l'archive lors du téléchargement des malwares et de les décompresser afin d'éviter un clic malheureux. Ce mot de passe sera le même pour le téléchargement des shellcodes. Le détail de cette fonctionnalité est décrit plus en détail dans les parties *Malcore*

Data retention (in days) (valeur par défaut : 15) : permet de choisir le nombre de jours où les fichiers et l'index de la solution TRACKWATCH sont conservés sur disque. A noter que la configuration s'applique en deux étapes : la première sur le **GCENTER** au niveau de ce champs, la deuxième au niveau de la sonde de détection **GCAP** dans les paramètres de configuration.

GScan enable (valeur par défaut : activé) : permet d'analyser de manière locale en temps réel des malwares ou des exécutables suspects. Dans le cadre de la Loi de Programmation Militaire, la fonctionnalité GScan est désactivée par défaut dans cette interface de gestion.

Privacy SMTP enable (valeur par défaut : désactivé) fait en sorte de respecter les droits relatifs à la protection des données personnelles en cachant le champ *email.subject* des alertes SMTP dans les dashboards GATEWATCHER pour les emails privés. Un email est considéré comme privé si son sujet commence par les mots *privé*, *prive* ou *private* (non sensible à la casse). Cette option est désactivée par défaut.

GeoIP enable (valeur par défaut : désactivé) : active la géolocalisation des ip sources et destination dans les

évènements. Cette option doit être activée pour que la fonction *SmartMap* puisse fonctionner. Les champs suivants seront ajoutés aux évènements

Input interface : permet d'activer/désactiver les interfaces sur lequel le **GCENTER** se mettra en écoute sur les ports ci-après .

HTTP listening port (valeur par défaut : 80) : le port d'écoute lié au protocole http.

HTTPs listening port (valeur par défaut : 80) : le port d'écoute lié au protocole https.

Outbound HTTP interface : l'interface physique de sortie pour tous les flux http.

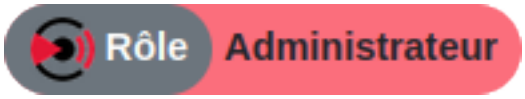
SSH banner (valeur par défaut : vide) : bannière SSH présentée lors de la pré-authentification sur l'ensemble des GCaps appairés ainsi que le GCenter.

Une fois les modifications effectuées, il sera nécessaire d'enregistrer ces changements en cliquant sur le bouton **Save**.

Important:

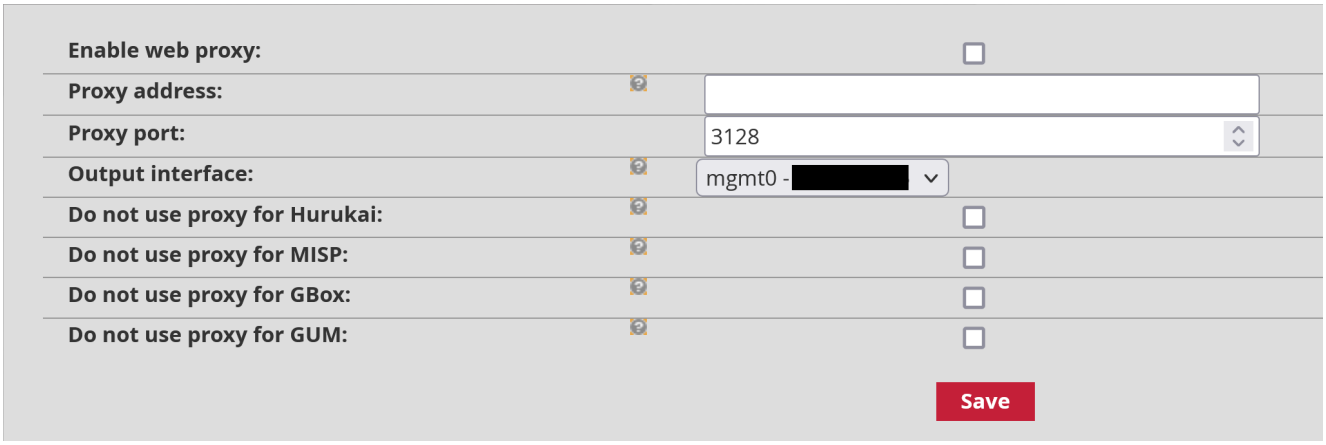
Si les équipements **GCENTER** et **GCAP** sont dans un environnement faisant partie du cadre LPM (Loi de Programmation Militaire) le service GSCAN est automatiquement désactivé et ne peut être activé. Pour plus d'informations, se reporter à la section LPM de ce document pour la désactivation du GScan.

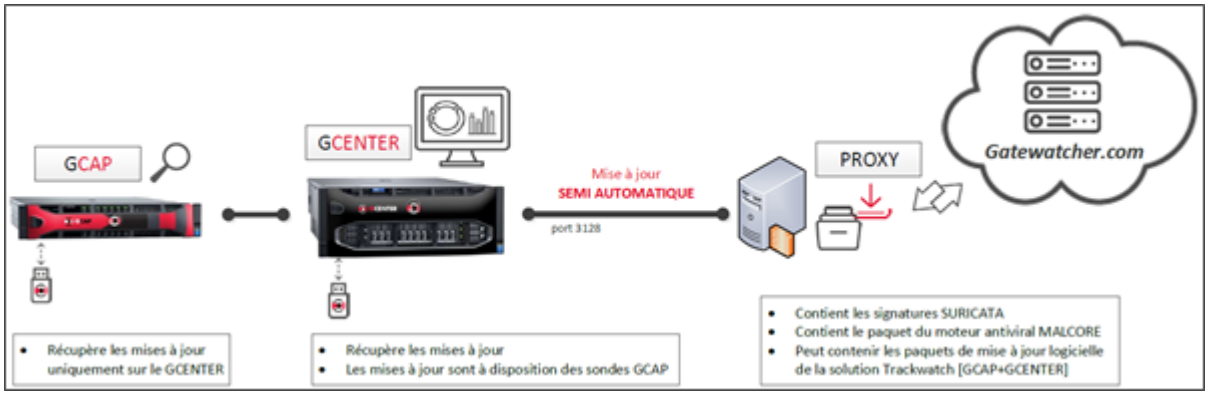
6.2.2 Proxy Settings



Menu : Administrators > GCenter > Configuration > Proxy Settings

La solution TRACKWATCH offre la possibilité de configurer un serveur mandataire (ou *proxy*) afin de récupérer les updates (mise à jour de signatures) via celui-ci.





Enable Web Proxy : Active/Désactive l'utilisation du proxy

Proxy address : Adresse du serveur mandataire sous forme d'adresse IP ou de FQDN

Proxy port : Port d'écoute du proxy (1-65535)

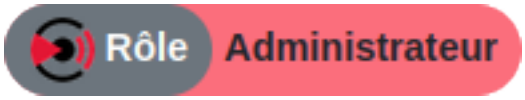
Output interface : l'interface du **GCENTER** à utiliser pour joindre le proxy.

Do not use proxy for Hurukai/MISP/GBOX/GUM : permet à l'administrateur de décider s'il souhaite utiliser les paramètres du proxy pour l'intégration avec des serveurs *Hurukai/MISP* ou pour l'accès à une *GBOX* ou *GUM*.

Une fois les modifications effectuées, il sera nécessaire d'enregistrer ces changements en cliquant sur le bouton **Save**.

Ce mode de mise à jour fait partie de la conformité de la Loi de Programmation Militaire (LPM). De ce fait l'entité concernée fera ses mises à jour sur un serveur de mise à jour dédié. Pour plus d'informations, se reporter à l'*annexe concernant les spécificités liés à la LPM* de ce document et la section *update*.

6.2.3 SSL Settings



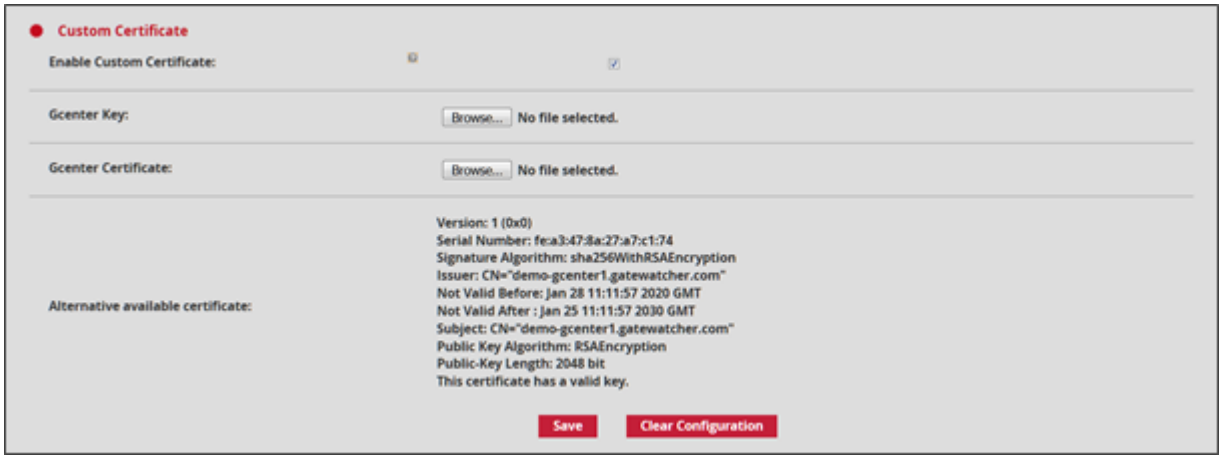
Menu : Administrators > GCenter > Configuration > SSL Settings

Cette interface permet de configurer le certificat SSL (Secure Socket Layer) du **GCENTER**. Le certificat généré attestera de l'identité du GCENTER et permettra de chiffrer les données échangées. Il est également possible depuis cette page de configurer l'authentification mutuelle (mTLS).

La section *Security details* permet d'obtenir des informations sur le certificat en cours d'utilisation pas le **GCENTER**.

In use certificate details : affiche les informations sur le certificat comme la date d'émission et d'expiration, l'émetteur de ce certificat, etc. **CA certificate informations** : affiche les informations que le serveur possède sur l'autorité de certification permettant d'identifier l'identité des correspondants dans la partie *Dual Authentication*.

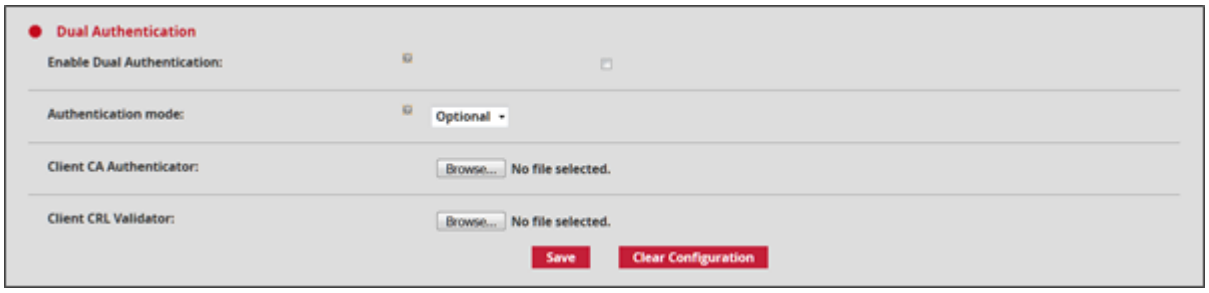
CRL informations : énumère les identifiants qui ont été révoqués ou invalidés et qui ne sont plus dignes de confiances.



La section **Custom Certificate**, permet d'utiliser un certificat spécifique.

Pour cela il suffit de spécifique la clé privée dans le champs **GCenter Key** et le certificat au format PEM dans le champs **GCENTER certificate** et également d'activer ce certificat en cochant la case **Enable Custom Certificate**

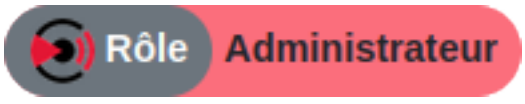
Enfin, la section *Dual Authentication* permet d'activer l'authentification mutuelle (mTLS). Cela permet à l'utilisateur de s'assurer de l'identité du serveur, mais également au serveur de s'assurer de l'identité de l'utilisateur.



Afin de valider cette option, il est nécessaire d'ajouter auparavant le certificat de l'autorité émettant les certificats utilisateurs au format PEM dans le champ **Client CA Authentication**, ainsi que la liste des certificats révoqués dans le champ **Client CRL Validation**. Puis sélectionner le type d'authentification *Forced* (rendant obligatoire pour les utilisateurs l'utilisation d'un certificat émis par l'autorité de certification) ou *Optional* (qui ne vérifie que si un certificat est présent) depuis 'Authentication mode' après avoir activé l'option **Enable Dual Authentication**.

Une fois les modifications effectuées, il sera nécessaire d'enregistrer ces changements en cliquant sur le bouton **Save** pour chacune des sections modifiées.

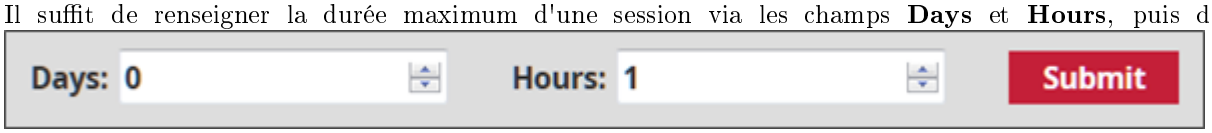
6.2.4 Session age settings



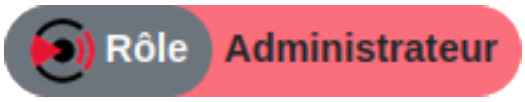
Menu : Administrators > GCenter > Configuration > Session age settings

Cette section permet de configurer la durée totale maximum d'une session sur l'interface web du GCenter.

Il suffit de renseigner la durée maximum d'une session via les champs **Days** et **Hours**, puis de valider.



6.2.5 Licenses



Menu : Administrators > GCenter > Configuration > License

La section License, permet d'obtenir des informations sur la licence en cours, d'en vérifier la validité et des fonctionnalités disponibles.

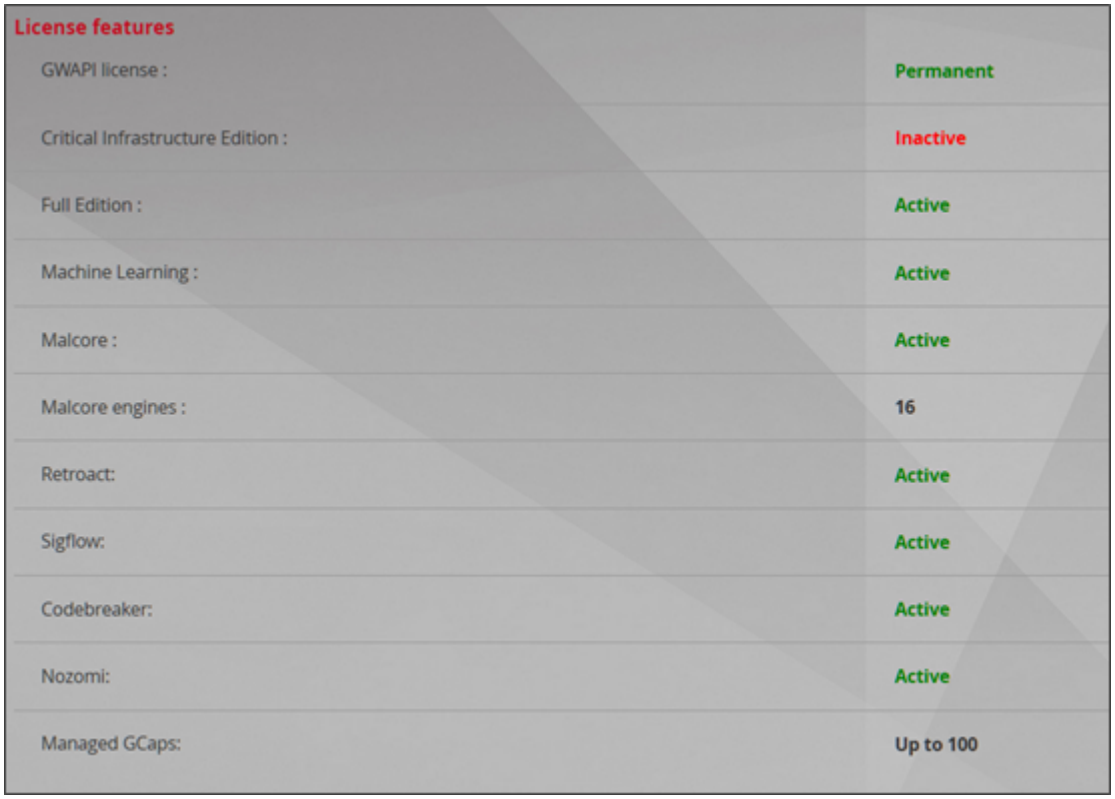
La section *Licence details* permet d'obtenir des informations sur le matériel pour lequel cette licence a été émise via son modèle et son numéro de série, mais également la période de validité de celle-ci et l'adresse de contact associée et le type de license.

Puis dans la partie *Licence features*, il est possible de constater la disponibilité des différents modules qui seront expliqués dans la suite de cette documentation.

Enfin, il est possible en bas de page de renseigner une nouvelle licence, et également de régler la notification dans l'interface d'une date d'expiration proche en renseignant le nombre de jour avant l'expiration.

Pour l'obtention de licence **GCENTER** merci de vous rapprocher de votre ingénieur d'affaire GATEWATCHER ou contacter le à l'adresse commerciaux@GATEWATCHER.com.

Une fois la licence, validée et activée le contenu de la page se met à jour et affiche le détail du contenu de la licence.



En cas de licence absente ou expirée, l'interface redirigera automatiquement vers cette page afin de résoudre la situation.

Chapter 7

Présentation

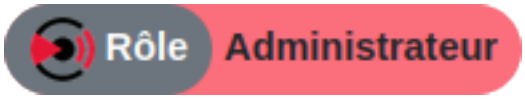
Le **GCAP** est la sonde permettant la capture des flux réseaux. Elle permet de générer les alertes, fournir des méta-données sur les différents protocoles et reconstruire les fichiers capturés. Ces données sont ensuite transmises au **GCenter** afin de continuer l'analyse des éléments, enrichir et mettre à disposition les informations générées.

Plus d'information sur le **GCAP** sont disponibles dans sa documentation

Chapter 8

Appairage

8.1 Ajouter un GCAP



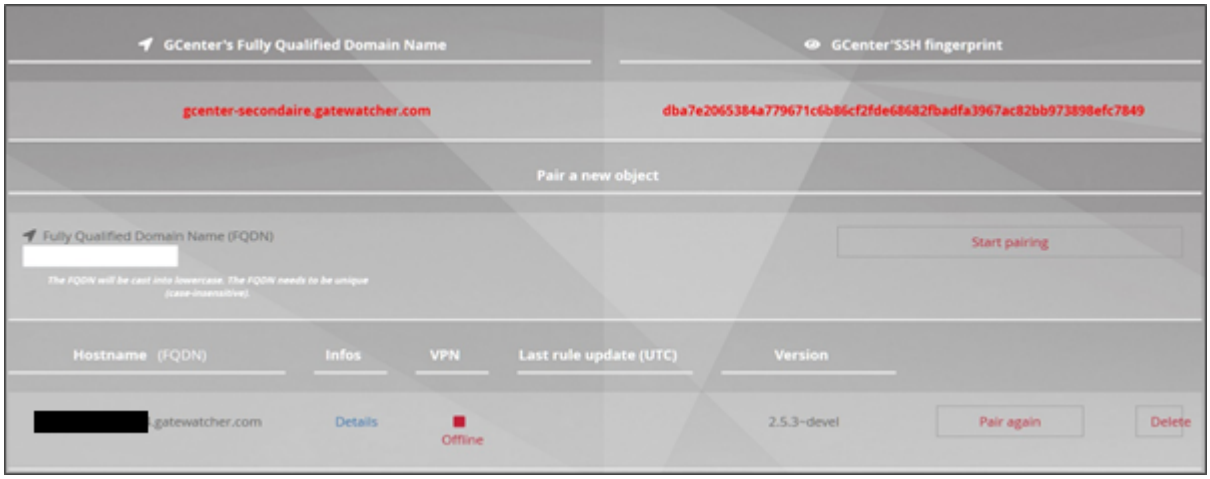
Menu : Administrators > GCAP Pairing/Status

Pour que les équipements de la solution TRACKWATCH puissent communiquer, il faut dans un premier temps ajouter une sonde **GCAP**.

L'appairage permet de configurer le tunnel IPSec entre le **GCAP** et le **GCENTER**.

Il est nécessaire de renseigner le champ **Fully Qualified Domain Name FQDN**(Exemple : '*nomduGCAP.domaine.com*') de la section *Pair a new object.*

Suite à cela, il faut appuyer sur le bouton **Start pairing** pour démarrer le processus.



Cette action génèrera un OTP sur l'interface Web du **GCENTER**. Celui-ci doit être renseigné sur la sonde **GCAP** afin de lier avec succès les équipements.

Le champ **GCENTER's Fully Qualified Domain Name** est utilisé pour vérifier les certificats du tunnel et de la connexion réseau qui sera établi.

Your OTP Token is : rve9rtz3mz47fjni4oyh4fdpb

GCENTER'SSH fingerprint permet de s'assurer que le **GCAP** communique avec le bon **GCENTER**. Il s'agit de l'empreinte du **GCENTER**. Ce processus est décrit plus en détail dans la documentation du **GCAP**.

Une fois le processus d'appairage terminé, il est possible de vérifier via l'interface du **GCENTER** si l'association s'est bien déroulée.

Les statuts Online, Undetermined et Offline déterminent l'état du lien VPN.

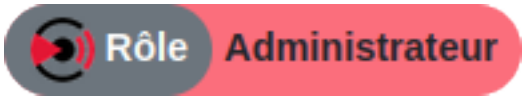
Le VPN côté client est dans un état inconnu **GCENTER** :

Le VPN côté client est déconnecté du **GCENTER** :

Le VPN côté client est associé au **GCENTER** :

Les statuts de diagnostics sont présents depuis l'onglet 'VPN' pour que l'administrateur puisse rapidement s'assurer de la bonne association.

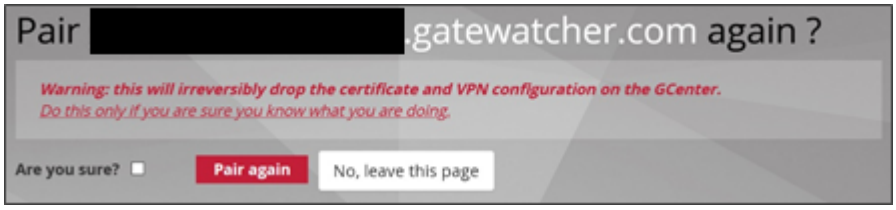
8.2 Re-appairer un GCAP



Menu : Administrators > GCAP Pairing/Status

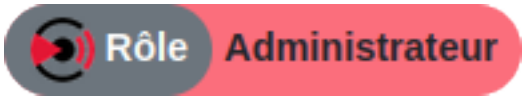
Si nécessaire, un **GCAP** peut être ré-appairé au **GCenter**.

Pour cela, il suffit de cliquer sur **Pair again** et de refaire la même opération pour associer la sonde au **GCENTER**.



L'administrateur doit cocher la case 'Are you sure?' avant de valider l'action.

8.3 Supprimer un GCAP



Menu : Administrators > GCAP Pairing/Status

Il est possible de retirer un **GCAP** de la plateforme de management avec le bouton **Delete**.

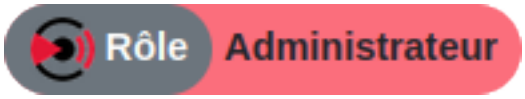
L'administrateur doit cocher la case 'Are you sure?' avant de valider l'action.

Cela supprimera toutes les données relatives à l'appairage du GCAP comme les certificats ou la configuration. Les logs (metadonnées ou alertes) produites par le passé et indexées dans elasticsearch ne seront pas modifiées

Chapter 9

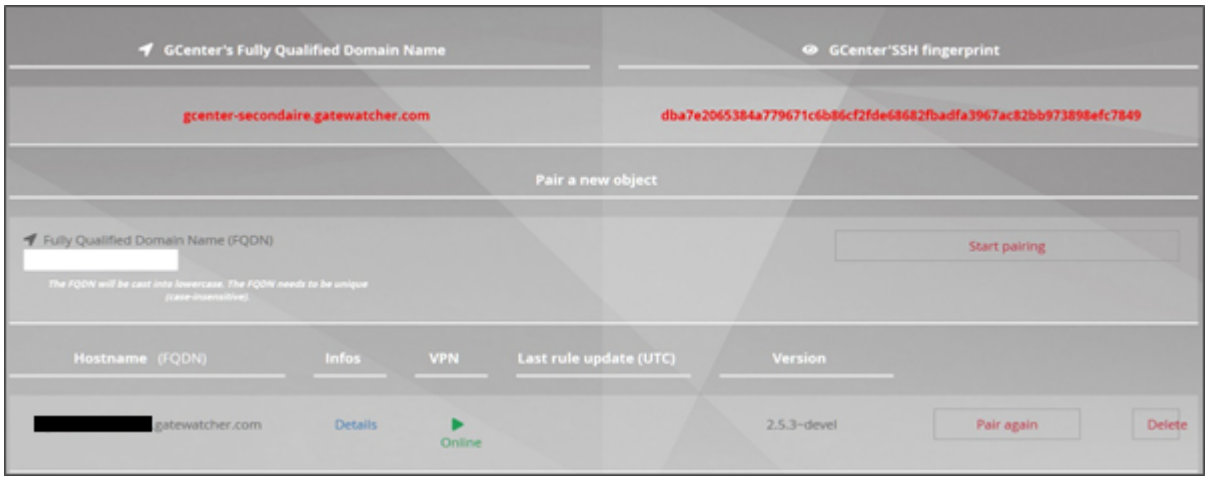
Paramétrage

9.1 Détail d'un GCAP



Menu : Administrators > GCAP Pairing/Status

Une fois le tunnel VPN à l'état *Online*, il est possible d'avoir accès à des renseignements sur la sonde **GCAP**.



Ce tableau permet de voir simplement l'état de toutes les sondes **GCAP** associées au **GCENTER**.

Hostname (FQDN) : le nom pleinement qualifié de la sonde.

Last rule update (UTC) : correspond à l'horodatage de la dernière mise à jour en UTC au format [**année-mois-jour hh** : **mm** : **ss**] des règles de signature du moteur Sigflow.

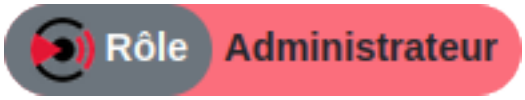
Version' : correspond à la version logicielle (Exemple : '_2-5-3~_prod') de la sonde de détection **GCAP**.

La colonne **Infos**, apporte davantage d'informations sur la sonde **GCAP** , grâce au bouton **Details**.

En effet des données d'acquisition du réseau, du système ou encore du moteur Sigflow sont remontées au **GCENTER**. L'administrateur a accès en temps réel à la supervision des éléments de la sonde de capture **GCAP** (débit du disque dur, processeur, mémoire, trafic réseau, interfaces réseaux, ...).

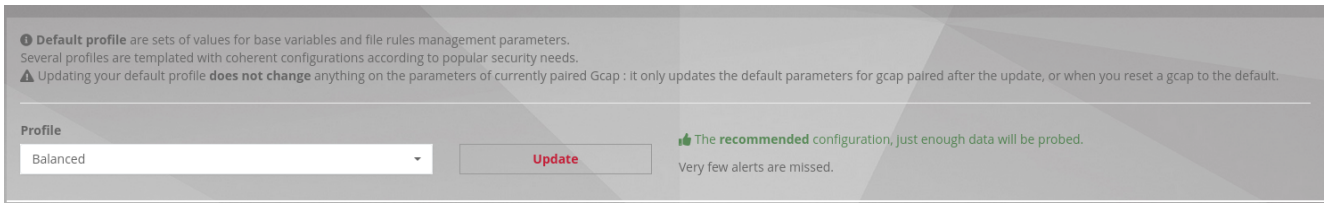
Les métriques suivantes sont remontées :

9.2 Définir un profil par défaut



Menu : Administrators > GCAP Pairing/Status

Les profiles par défaut sont des ensembles de valeurs pour *Base variables* et *Files rules management*.



Plusieurs profils sont disponibles selon les besoins de sécurité courants :

- Minimal : la configuration minimal.
- Balanced : la configuration recommandé par Gatewatcher.
- LPM : la configuration nécessaire en mode LPM.
- Paranoid : tout les paramètres sont activés.
- Intuitio : Configuration pour le NDR.

La mise à jour de votre profil par défaut ne change rien sur les paramètres du Gcap actuellement apairé.

La gestion des mises à jour s'effectue via le module nommé **GUM** (**G**atewatcher**U**pdate**M**anager).

Ce module est utilisé afin de mettre à jour la solution, et cela aussi bien pour la mise à jour des signatures de détection ou des moteurs anti-viraux (update), que pour l'application de patch correctif (*Hotfix*) ou les montées de version de GCenter ou des GCap (upgrade).

Chapter 10

Montée de version (Upgrade)

À la différence des *updates*, les *upgrades* (montés de versions ou *hotfix*) ne sont pas automatisables est doivent être réalisées par un administrateur **après avoir pris connaissance des *notes de version et des notes de mise à jour***

Dans le cas de mise à jour mineure (par exemple le passage de la v2.3.5.101 à la 2.3.5.101-hf1) il existe deux manières d'effectuer l'upgrade :

- En appliquant uniquement le *hotfix* HF1 tel que décrit dans la *section suivante*
- En effectuant un upgrade complet tel que décrit *plus bas* Ces deux solutions sont équivalentes.

Cependant, dans le cas d'une mise à jour majeure (par exemple de la v2.3.5.100 vers la 2.3.5.101) seule la *procédure d'upgrade* est applicable.

10.1 Hotfix

Menu : Administrators > GUM > Hotfix

Important:

Le menu Hotfix n'est pas disponible lorsque la solution TRACKWATCH est déployée dans un environnement soumis à la LPM, il sera alors nécessaire de passer par une montée de version.

Plus de détails sont disponibles dans la section de la documentation dédiée aux spécificités de déploiement dans le cadre de la LPM

Un Hotfix permet d'appliquer une correction ou une modification donnée sans avoir à procéder à un upgrade complet de la solution. Dans la majorité des cas, les hotfix ne nécessiteront pas de redémarrage du service.

Tous les paquets de correction sont téléchargeables via notre plateforme de téléchargement https://update.gatewatcher.com/hotfix. Les correctifs sont classés par version du **GCENTER**.

Depuis l'interface Web du **GCENTER** , l'administrateur pourra déposer le correctif précédemment téléchargé et cliquer sur **Send hotfix**.

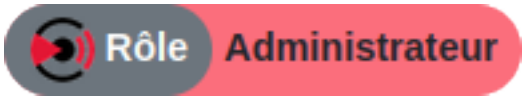
L'application du correctif sera prise en compte après avoir appuyé sur **Apply** depuis **Saved package list**.

A l'issue de cette manipulation, l'équipement ne redémarrera pas cependant l'application de ces paquets de correction génère un redémarrage automatique de la WebUI du **GCENTER**. Un rafraîchissement manuel de page peut être nécessaire.

Les paquets de correction deviennent cumulatif à partir de la version 2.5.3.101.

Le descriptif de chaque paquet de correction dans des notes de versions est disponible depuis le site https://releases.gatewatcher.com.

10.2 Upgrade



Menu : Administrators > GUM > Upgrade

Important:

Tous les objects KIBANA (dashboards, visualisation, search, ...) créés en version 2.5.3.100 seront supprimés au premier démarrage version 2.5.3.101. Un export/import des paramètres est nécessaire pour conserver la configuration des objects lors de l'upgrade en 2.5.3.101

Cette section permet d'effectuer une montée de version de la solution TRACKWATCH.

Tous les paquets de montée de version sont téléchargeables via notre plateforme de téléchargement https://update.GATEWATCHER.com. Ils se trouvent dans la rubrique suivant la version **2.5.3.X** puis **GCENTER** , **GCAP** ou **GBOX**.

Dans https://update.GATEWATCHER.com/upgrade/2.5.3.101/GCENTER/, le moment, les états, le SHA256, ainsi que le statut des derniers correctifs sont respectivement renseignés. Un paquet complet regroupant les dernières corrections sur la version est aussi disponible sous le nom de GCENTER-2.5.3.101-xxxx_prod-hfx.gwp.

L'administrateur pourra alors déposer la mise à jour fonctionnelle précédemment téléchargé et cliquer sur **Submit**.

L'application du paquet de montée de version sera prise en compte après avoir appuyé sur **Apply** depuis **Saved package lists**.

A l'issue de cette manipulation, l'équipement redémarrera.

Le descriptif de chaque paquet de correction dans des notes de versions est disponible depuis le site https://releases.GATEWATCHER.com.

Chapter 11

Mise à jour des signatures (Update)

11.1 Mode de mise à jour

Le produit peut se mettre à jour de trois manières différentes suivant les besoins du système d'information dans lequel la solution est déployée : mise à jour *Online*, mise à jour *Manuelle* et mise à jour *Locale*.

11.1.1 Mode online

La mise à jour online permet d'automatiser les mises à jour et de réduire les tâches d'administration.

Les mises à jour se font automatiquement depuis https://update.GATEWATCHER.com et https://gupdate.GATEWATCHER.com.

Note:

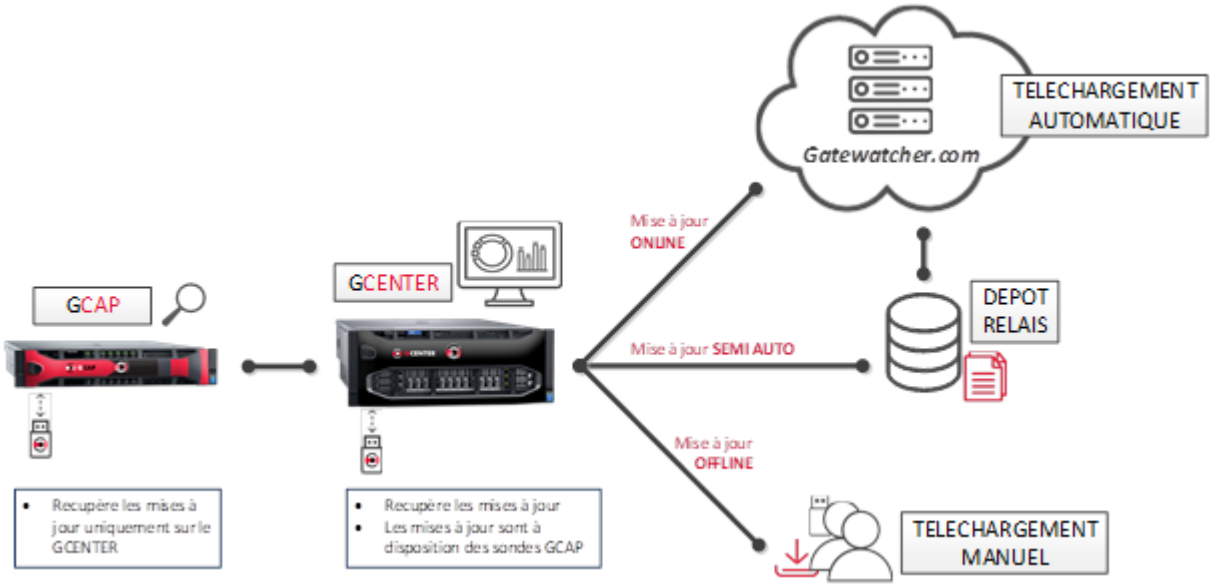
Dans le cas du mode *online* planifié, la planification ne s'applique que sur le moteur **SigFlow**. Les mises à jour du moteur **Malcore** sont effectuées toutes les 15 minutes.

11.1.2 Mode manuel

La mise à jour manuelle est adaptée aux environnements isolés. L'administrateur doit d'abord télécharger manuellement les packages de mise à jour sur un poste d'administration, puis les téléverser sur le Gcenter via l'interface web.

11.1.3 Mode local

Afin de répondre à des contraintes de sécurité particulières, le **GCenter** est capable d'aller chercher ses mises à jour sur un dépôt local.

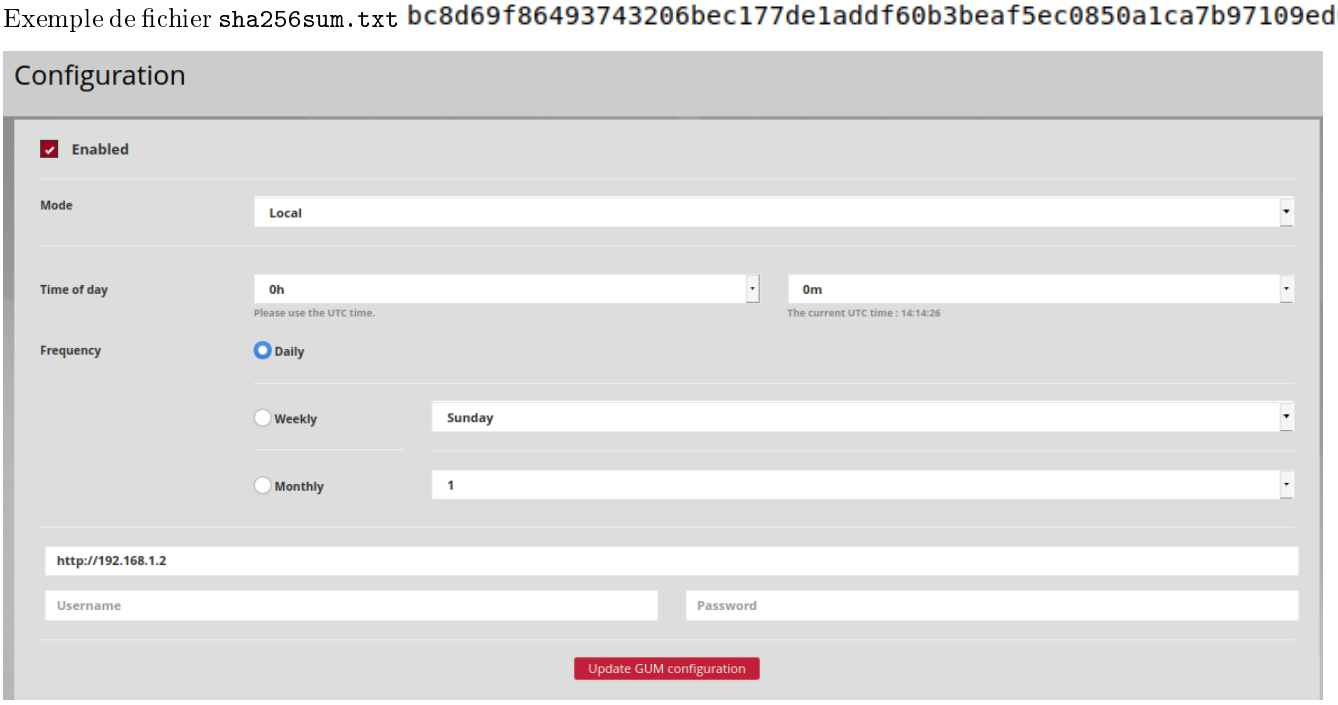


Les étapes de configuration d'un dépôt local sont les suivantes :

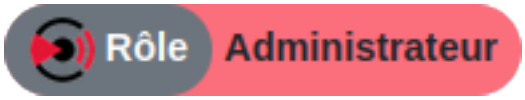
- Prérequis : Un serveur Web en écoute sur le port 80
- Créer l'arborescence suivante: "2.5.3.10X/GCenter" selon la version du GCenter (2.5.3.100 ou 2.5.3.101) (Dans l'exemple de configuration suivant cette arborescence devra être créée à la racine du serveur)
- Récupérer un fichier gwp (latest_full.gwp pour un GCenter V100, latest_full_v3.gwp pour une 2.5.3.101) sur https://update.gatewatcher.com/update/
- Dans "2.5.3.10X/GCenter", mettre le fichier gwp récupéré précédemment.
- Dans "2.5.3.10X/GCenter", mettre un fichier sha256sum.txt qui contient une entrée "sha256sum NomDuFichier"

Exemple de fichier `sha256sum.txt`

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



11.2 Configuration



Menu : Administrators > GUM > Config

Le menu GUM permet d'entrer les paramètres nécessaires à l'utilisation du mode online ou du mode local.

La configuration des paramètres d'update (mise à jour des signatures) s'active en cochant la case **Enabled**.

Le mode peut être sélectionné dans la liste :

- *Local*
- *Online*

La définition du moment où les mises à jour se fait via les champs **Time of day** et **Frequency**.

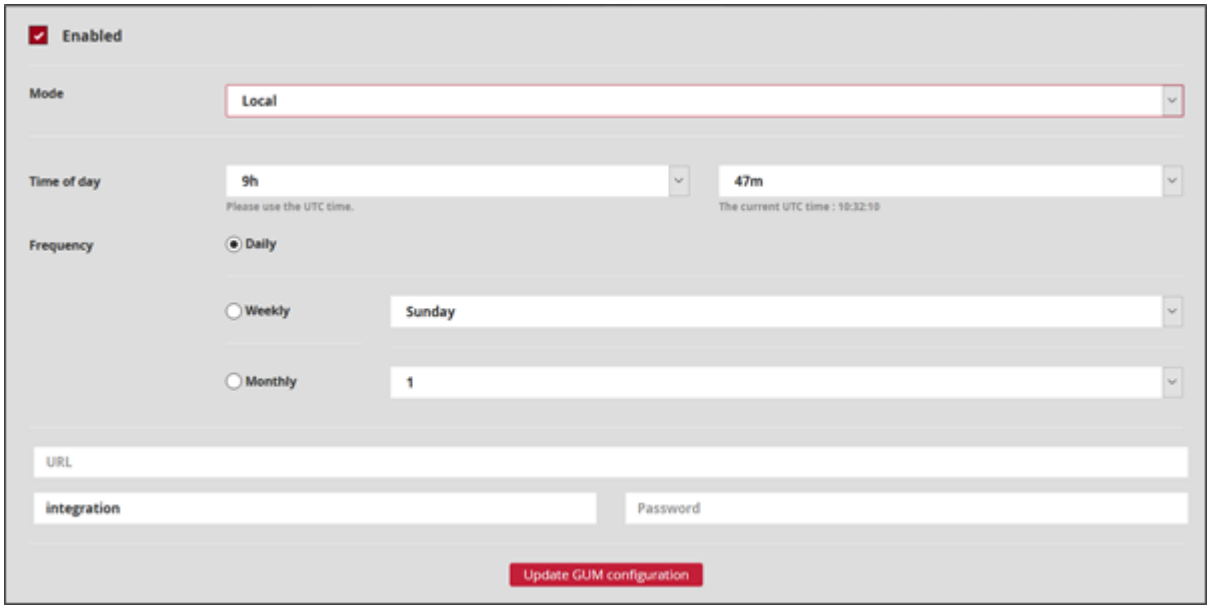
URL permet de renseigner l'adresse où **GUM** doit aller vérifier les mises à jour. Dans le cas d'une mise à jour *Online*,

Dans le cas du mode online, un compte **intelligence** sera nécessaire pour que le téléchargement du package de mise à jour puisse se faire depuis le site. Ce couple utilisateur et mot de passe doivent être renseignés dans les champs **Username** et **Password** situés sous l'adresse. Le champ **URL** sera automatiquement renseigné lors de la sélection du mode **Online** : les packages de mise à jour sont récupérés depuis les serveurs GateWatcher https://update.GATEWATCHER.com/update/.

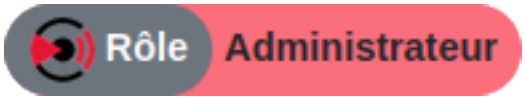
Dans le cas du mode local, il sera nécessaire de spécifier l'adresse du dépôt local.

La solution TRACKWATCH offre également la possibilité de configurer un serveur mandataire pour joindre ce dépôt. Cette option est paramétrable dans la partie *Proxy Settings*.

La validation du formulaire depuis le bouton 'Update GUM configuration' est obligatoire pour que les informations renseignées soient prises en compte.



11.3 Mise à jour manuelle des moteurs



Menu : Administrators > GUM > Update

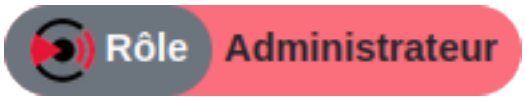
```
important:: Depuis la version 2.5.3.101, merci d'utiliser les mise à jours identifiés par
↪une version 3.
```

Toutes les mises à jour sont disponibles via notre plateforme de téléchargement https://update.GATEWATCHER.com. Une fois le package de mise à jour téléchargé, l'update des moteurs MALCORE et SIGFLOW se fait sur le **GCENTER**.

Trois packages peuvent être utilisés pour effectuer les mises à jour manuellement. Les packages *sigflow* pour mettre à jour les règles de détection, les packages *malcore* pour mettre à jour les moteurs antiviraux, et *full* mettre à jour les deux moteurs en même temps.

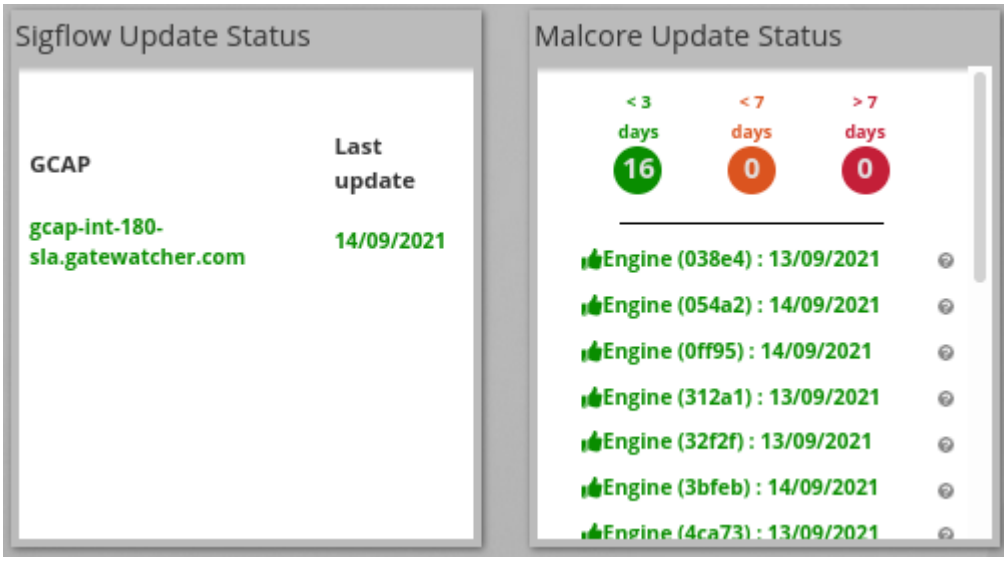
Depuis l'interface Web du **GCENTER** , dans la section **GUM/Updates**, l'administrateur pourra déposer le paquet de mise à jour et appliquer celui-ci en sélectionnant **Apply**.

11.4 Vérification des mises à jour



Menu : Home Page

La date de dernière mise à jour des moteurs *Sigflow* et *Malcore* est visible directement depuis la HomePage, accessible en cliquant sur le Logo **Gatewatcher** en haut du menu à gauche.



Chapter 12

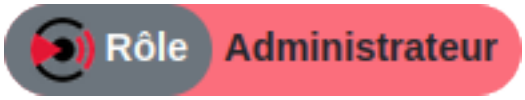
Présentation

Les moteurs de détection MALCORE et RETROACT permettent:

- La détection des malwares par une analyse statique et heuristique multi-moteurs en temps réel des fichiers.
- L'analyse via 16 moteurs Anti-Virus.
- Une performance d'analyse à plus de 6 millions de fichiers par 24h.
- La détection des malwares par une ré-analyse des fichiers à potentiel malicieux, après leur passage, avec de nouvelles signatures et méthodes heuristiques.

Chapter 13

Configuration

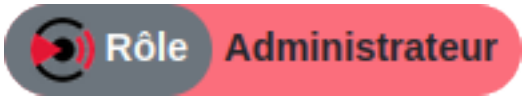


Menu : Administrators > GCenter > Malcore Management

L'interface de management MALCORE permet de modifier les paramètres d'analyse du **GCENTER**. Depuis cette section, l'administrateur pourra ajuster les paramètres globaux de détection du **GCENTER** :

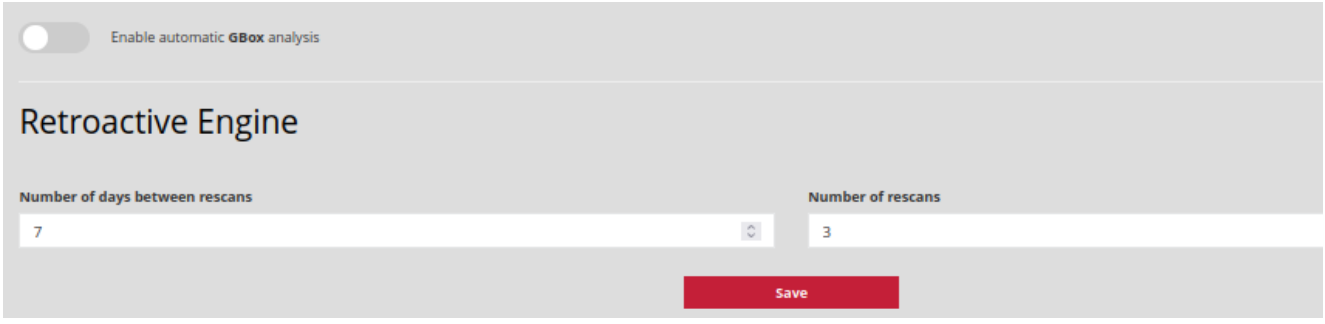
- *Global settings*
- *Profiles*
- *White List*
- *Black List*

13.1 Global settings



Menu : Administrators > GCenter > Malcore Management > Global Settings

Le moteur d'analyse **RETROACT** permet une détection en post compromission en réanalysant a posteriori les fichiers dont le potentiel malicieux a été suspecté par l'analyse heuristique de MALCORE. Ces analyses ultérieures se font sur une période paramétrable, plusieurs jours/semaines/mois après le passage du fichier, avec les nouvelles signatures et méthodes heuristiques.



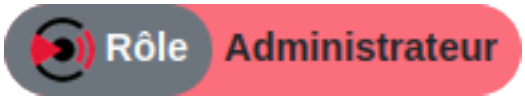
Number of days between rescans : Cela correspond au nombre de jours passés entre chaque réanalyse de fichiers.

Number of rescans : correspond au nombre de rescans à effectuer.

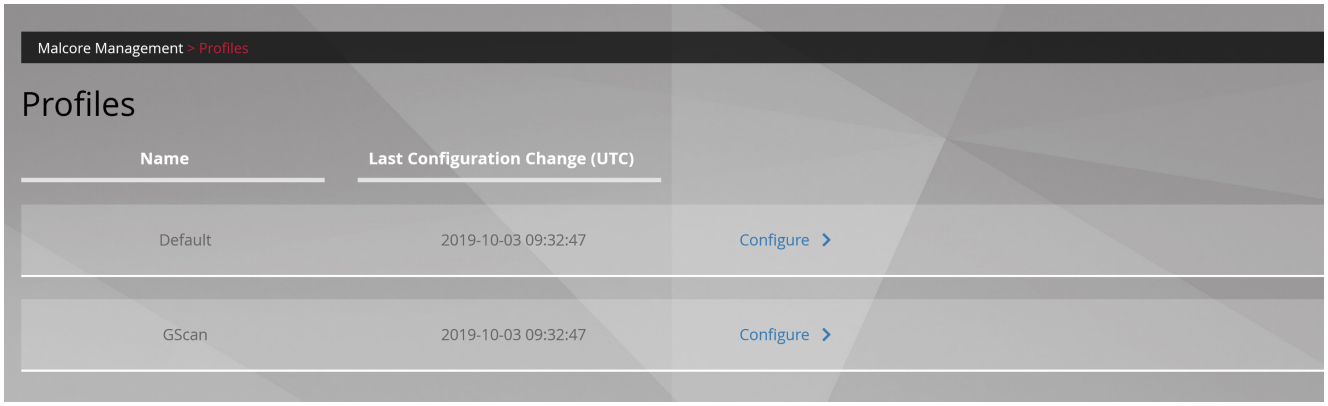
Par exemple, si **Number of days between rescans** est fixé à 3 et **Number of rescans** à 3, le fichier suspicieux sera réanalysé à J+3, J+6 et J+9.

Enable automatic GBOX analysis : permet à l'administrateur d'activer l'envoi automatique de tous les fichiers infectés ou suspicieux à l'équipement **GBOX** si le lien est opérationnel.

13.2 Profiles



Menu : Administrators > GCenter > Malcore Management > Profiles

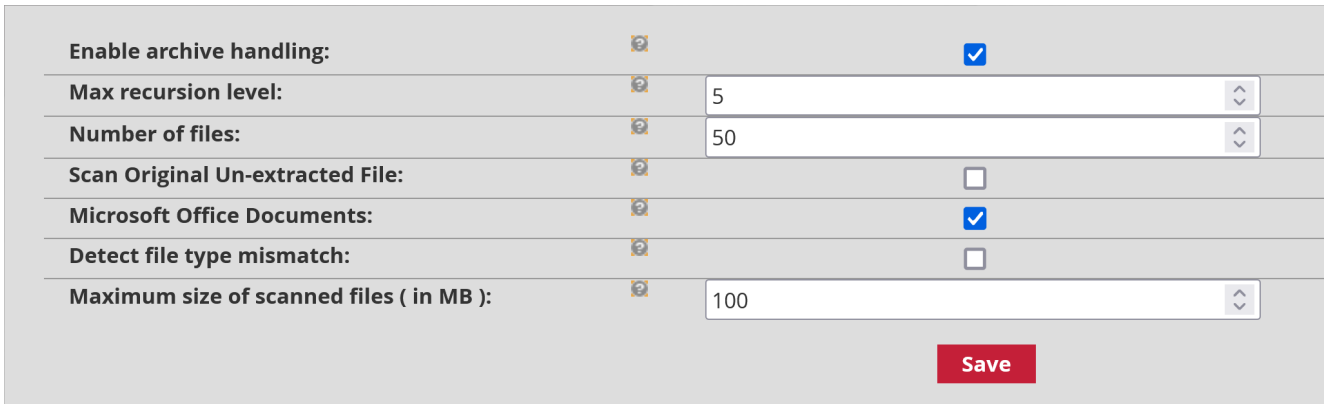


L'ensemble des profils **MALCORE** apparaît sur cette vue.

Chaque profil peut cependant être modifié selon les besoins via le bouton **Configure**.

Le profil **Default** sera utilisé pour traiter des fichiers envoyés pour analyse par les gcaps.

Le profil **Gscan** sera utilisé pour l'analyse des fichiers soumis par l'interface gscan



Enable archive handling : permet d'activer le scan de tous types d'archive par **MALCORE** (.zip, .rar, .upx).

Max recursion level : indique le niveau de profondeur maximum dans lequel **MALCORE** va continuer à scanner les fichiers. Par exemple, un *.zip* contient un dossier, qui contient un dossier, qui contient des fichiers. Dans ce cas, il y trois niveaux de profondeur d'archives. Si on indique deux dans le niveau maximum de récursion possible, alors tous les fichiers dans des niveaux supérieurs ne seront pas scannés par **MALCORE**. Définir une limite ici permet de ne pas surcharger **MALCORE** mais en contrepartie il n'analysera pas tous les niveaux de fichiers. Par défaut cette valeur est à 5.

Number of files : il s'agit du nombre maximum de fichiers que **MALCORE** peut analyser par archive. Si ce nombre est dépassé, alors **MALCORE** suspectera quelque chose. Le nombre par défaut est de 50 fichiers.

Scan Original Un-extracted File : demande à **MALCORE** que l'archive soit considérée en elle-même en tant que fichier.

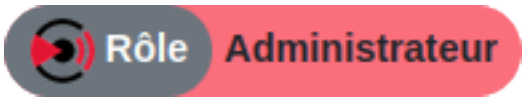
Microsoft Office Documents : demande à **MALCORE** de considérer les documents Office comme des documents Office (.docx, .xlsx) et non comme une archive.

Detect file type mismatch : si cette option est cochée, lorsqu'il y aura un décalage entre le type de fichier et son extension, le fichier apparaîtra en *Mismatch* au niveau des dashboards dans l'interface WEB **GCENTER**.

Maximum size of scanned files (in MB): : correspond à la taille maximale des fichiers qui sont analysés par **MALCORE**.

Chacune de ces informations sont prises en compte après que l'administrateur ait sauvegardé les modifications en appuyant sur '**Save**'.

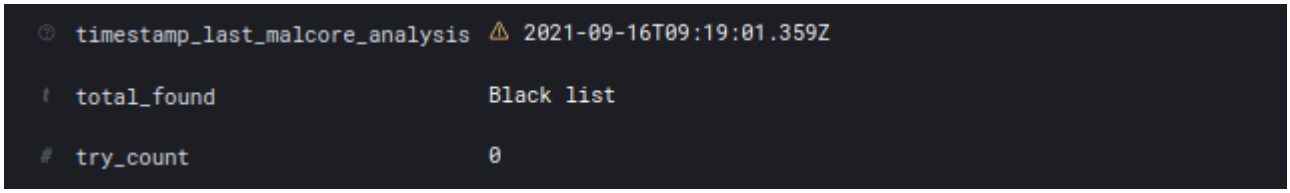
13.3 Liste d'exceptions



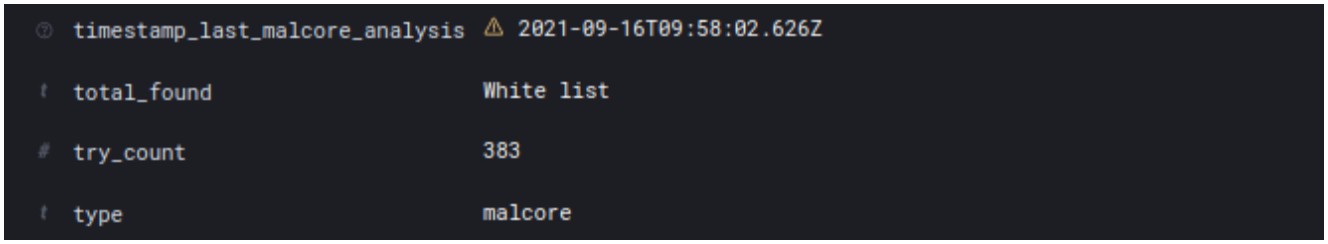
Menu : Administrators > GCenter > Malcore Management > White list / Black List

Il est possible, dans les paramètres de **Malcore**, de gérer des listes d'exceptions nommées Whitelist (pour les hash autorisés) et Blacklist (pour les hash interdit).

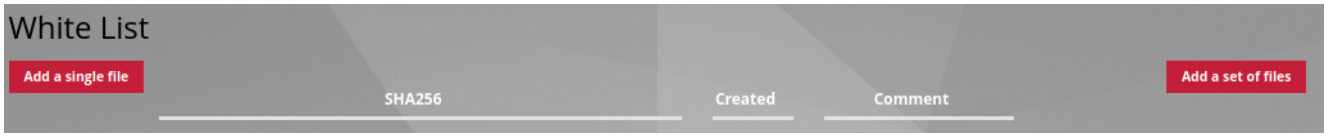
Dans le cas où un fichier qui doit être analysé a un hash SHA256 présent dans la *Blacklist*, le résultat de l'analyse apparaitra comme ceci:



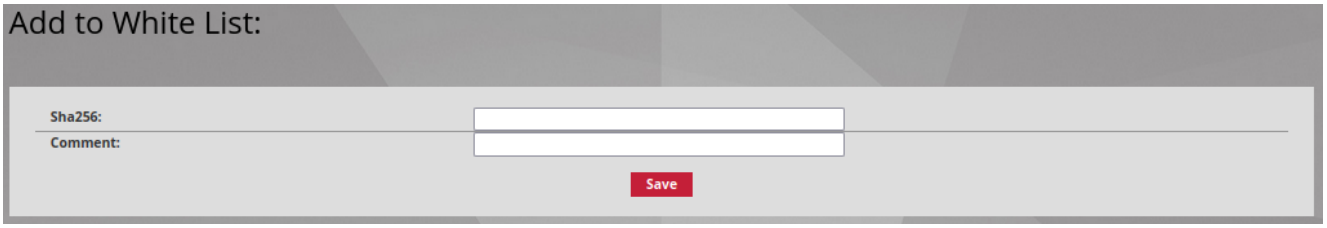
Dans le cas d'une *Whitelist*:



Il est possible d'ajouter un hash dans ces listes soit unitairement via l'interface du **GCenter** soit par lot, en injectant un fichier CSV.



En cliquant sur **Add a single file**, il est possible d'ajouter un hash de manière unitaire en renseignant le champ **Sha256** et un commentaire (optionnel) pour davantage de détails dans le champ **Comment**.



Chacune de ces informations est prise en compte après que l'administrateur ait sauvegardé les modifications en appuyant sur **Save**.

En cliquant sur **Add a set of files**, l'administrateur peut, en sélectionnant sur son poste un fichier en **csv**, ajouter une liste de hash en cliquant sur le bouton du champ **List of SHA256**. Il faudra utiliser des ';' pour séparer les différents éléments de la liste.

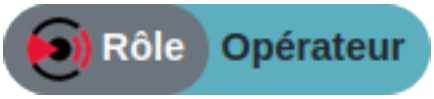
L'administrateur peut décider de supprimer la liste précédente en cochant la case **Clean previous list?** et sauvegarder toutes les modifications en cliquant sur **Save**.

Tous les ajouts et modifications faits depuis les sections White List et Black List des paramètres de configuration du moteur MALCORE seront pris en compte dans l'analyse du flux ainsi que pour les fichiers scannés via le GScan.

Chapter 14

Détection

14.1 Inspectra



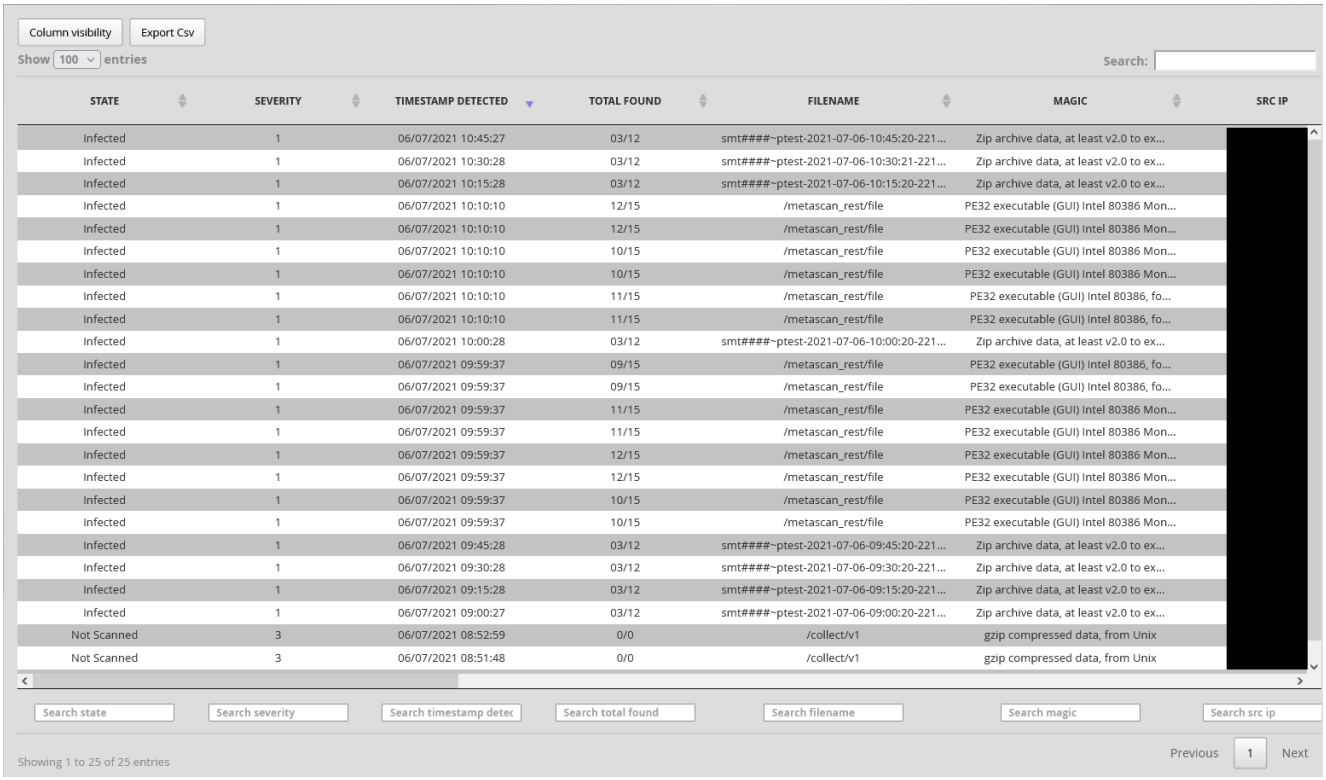
Menu : Operators > Inspectra > Malcore

Depuis la section '**OPERATORS - Inspectra - Malcore**', l'opérateur accède à un tableau recensant les fichiers vus comme étant suspicieux ou infectés au travers du moteur de détection **MALCORE**.

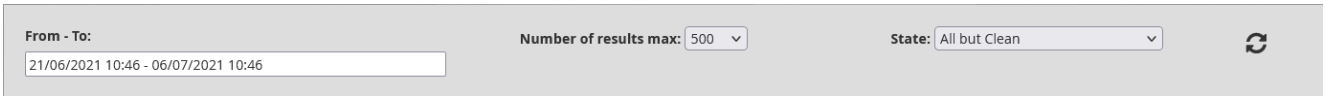
Le module ***RETROACT*** sera chargé de mettre en évidence, si la fonctionnalité est activée, les fichiers suspicieux.

L'état suspicieux est dû aux moteurs heuristiques. Ces derniers arrivent à détecter des éléments anormaux. Dans le cas de fichiers suspicieux, ces derniers seront reanalysés par **RETROACT**.

Les fichiers suspicieux sont détectés grâce aux différents moteurs antiviraux (1 en version CIE et 16 dans les autres versions) fonctionnant en parallèle. Ces moteurs ont été sélectionnés pour leur complémentarité et la pertinence de leur détection commune, leur technologie de détection, et l'origine des informations de sécurité utilisées.



De la fenêtre au-dessus de ce tableau, l'opérateur peut cliquer dans le champ '**From - To**' pour définir la plage de temps (au format *jj/mm/aaaa HH:MM*) des données qui s'affichent.



'**Number of results max:**' est le nombre maximum de fichiers (lignes) affichés dans le tableau.

'**State**' permet de sélectionner l'état des alertes affichées en fonction de la recherche souhaitée.

Les colonnes du tableau sont déplaçables et des recherches dynamiques peuvent être faites sur chacune d'entre elles:

L'opérateur peut choisir la visibilité des colonnes dans le tableau en cliquant sur le bouton **Column visibility**:


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

De plus, une vision verticale de l'alerte s'affiche grâce à un *clic droit* de la souris.

Une exportation rapide en CSV des données en fonction de la date de décision sélectionnée:

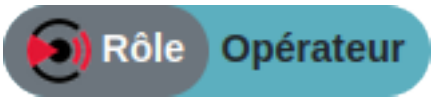
Une analyse interactive de l'élément est possible grâce à un *clic droit* de la souris. Avec '**Download malware**' il est possible de télécharger le malware et l'enregistrer sur le poste dans un fichier protégé par un mot de passe au format `.zip`. Ce mot de passe est modifiable *ici*.

TRACKWATCH est capable de fournir une analyse plus approfondie du malware détecté grâce à la fonctionnalité de **Remote analysis**'. Si la *configuration* est préalablement faite, l'opérateur peut décider que l'échantillon soit analysé dans la plateforme https://intelligence.gatewatcher.com/, soit un serveur ***GBOX***.

Le rapport d'analyse résultant de l'envoi du fichier infecté pour une analyse plus approfondie peut être téléchargé avec '**Download analysis report**'.

Les paramètres d'analyse du moteur **MALCORE** sont modifiables dans les paramètres du *profil par défaut*.

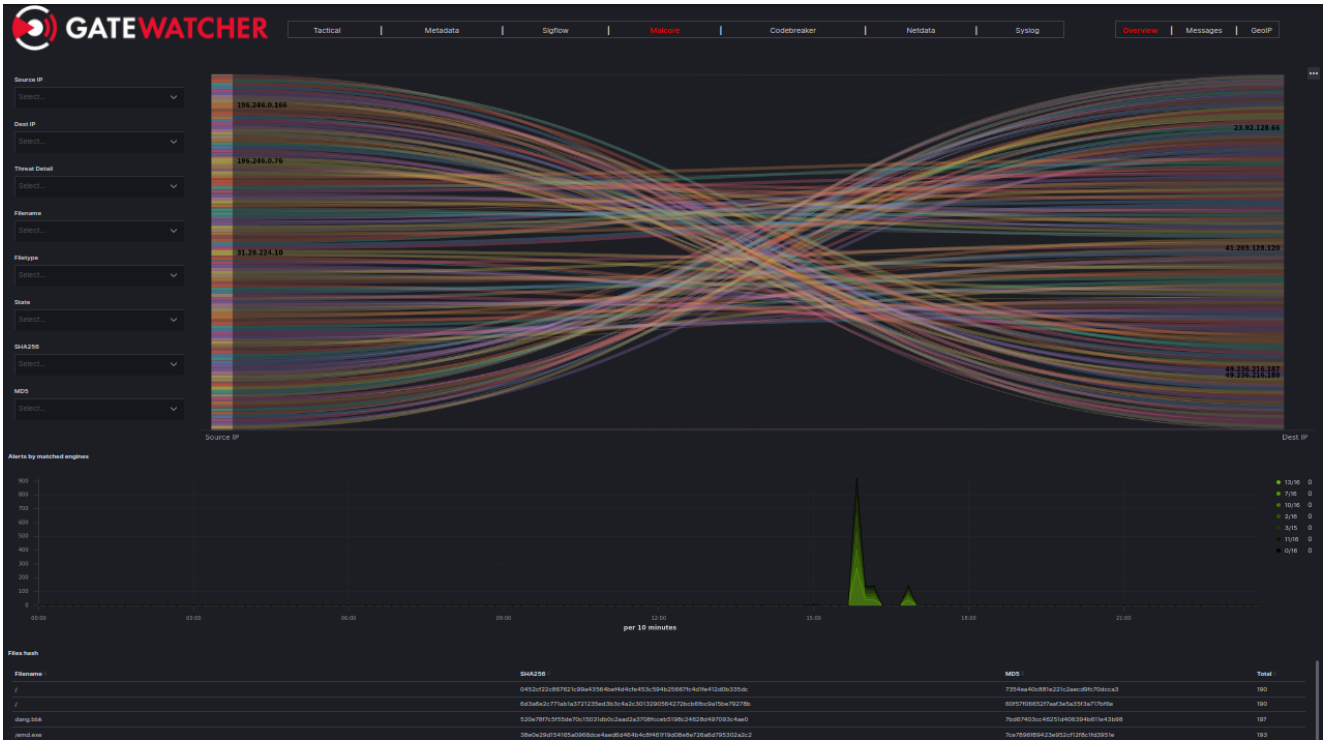
14.2 Dashboards



Menu : Operators > Dashboards > Malcore

En plus des informations déjà présentes dans le tableau **Inspectra**, les données collectées par Malcore sont également disponibles dans le *dashboard* Kibana de **Malcore**.

On y retrouvera les données mises en forme


GATEWATCHER
Tactical
Metadata
Sigflow
Malcore
Codebreaker
Netdata
Syslog
Overview
Messages
GeoIP
Source IP
Dest IP
Threat Detail
Filename
Filetype
State
SHA256
MD5
196.246.0.166
196.246.0.76
31.28.224.10
23.92.128.66
41.203.128.120
Source IP
Dest IP
Alerts by matched engines
per 10 minutes
Files hash
Filename
SHA256
MD5
Total

Chapter 15

Événements générés

attention:: Les id des moteurs sont susceptibles de changer au cours du temps.

15.1 Exemple de 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",
    "SHA256": "9f07b7d90dc159c18619741bbbe05a2eb512a53865ba5101ba9f5668ec01c427",
    "timestamp_last_malcore_analysis": "2021-07-05T18:15:35.546Z",
    "file": "1198",
    "detail_scan_result_i": 1,
```

(suite sur la page suivante)

(suite de la page précédente)


```
    "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 Tableau récapitulatif des champs

L'export syslog possède des champs additionnels :

- 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.

Avertissement:

Ces champs sont affectés par un bug connu (voir release note.)

Avertissement:

L'enrichissement à l'origine de ces champs sera déprécié en v2.5.3.102.

Chapter 16

Détection par gscan

Menu : Operators > GScan > Malware Scanning

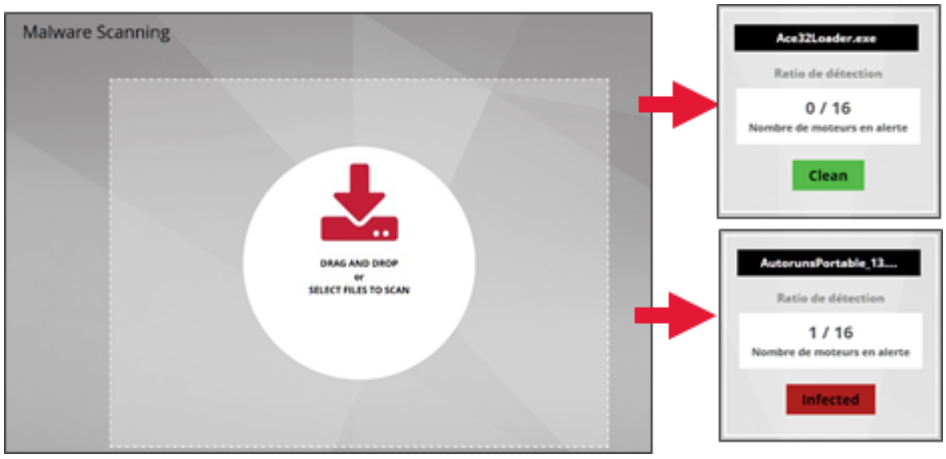
Note:

Dans le cas d'un déploiement dans un environnement soumis à la LPM, la fonctionnalité GScan est désactivée

Gscan permet à un opérateur de soumettre un fichier via l'interface web du GCenter afin qu'il soit analysé par malcore

Afin de lancer l'analyse d'un fichier, il suffit de glisser le fichier dans la zone **DRAG and DROP or SELECT FILES TO SCAN** ou de cliquer sur cette zone afin d'envoyer vos exécutables suspects.

Attention la taille maximale du fichier ne doit pas dépasser les 10MB. Il n'y a pas de limitation du nombre d'analyses de fichiers. Le résultat du scan montre quasi instantanément le statut de l'échantillon après analyse. Ce résultat peut-être à l'état : Clean ou Infected au travers des 16 moteurs.



Chapter 17

Présentation

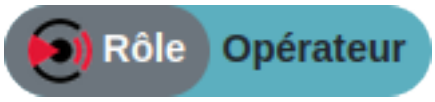
Le moteur d'analyse CODEBREAKER permet :

- La détection des techniques d'exploitation offusquées, discrètes et sophistiquées.
- Le désencodage de payloads encodés.
- La détection de Shellcodes polymorphes.

Codebreaker couvre les shellcodes destinés à des plateformes Windows ou Linux en 32 et 64bits.

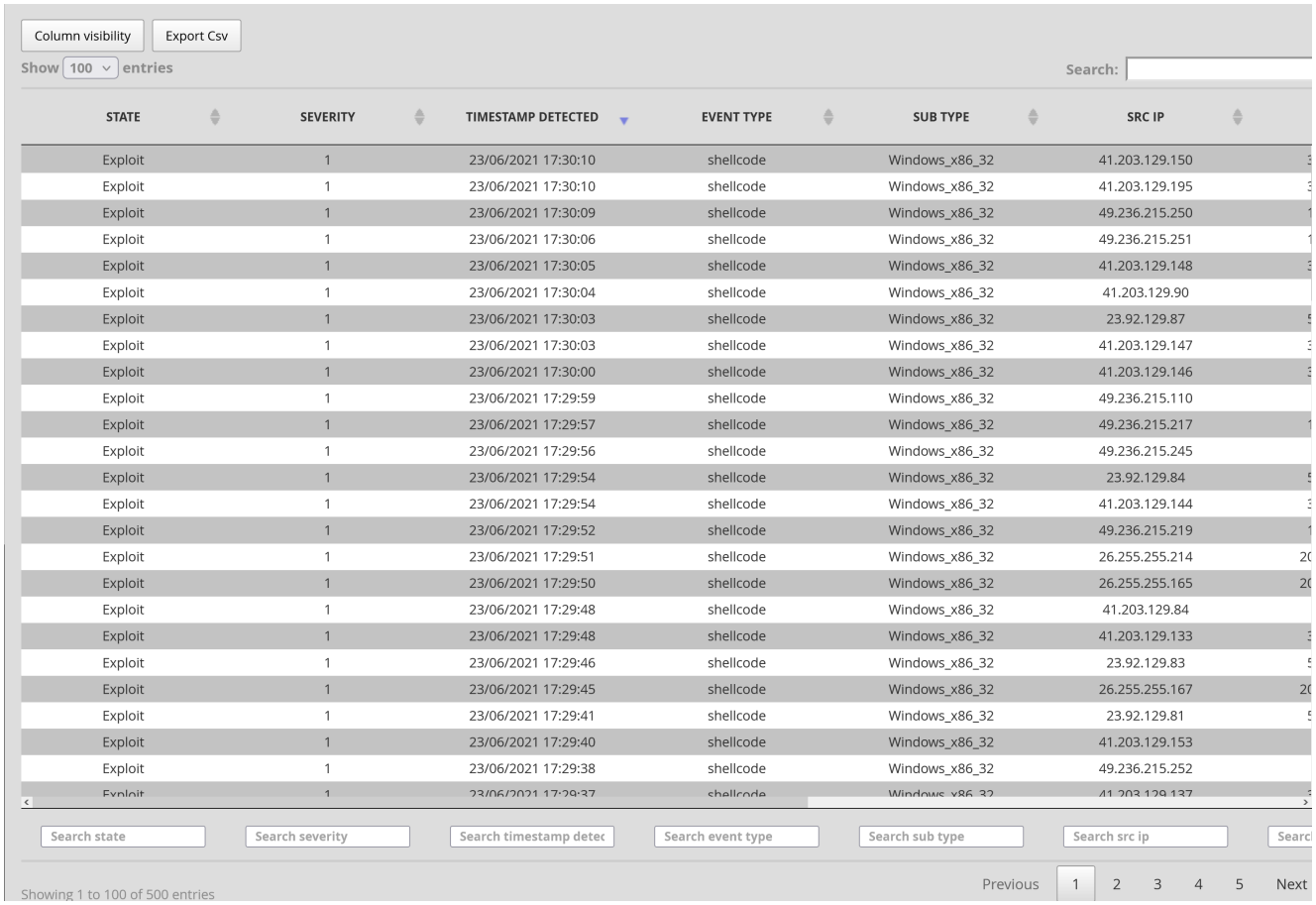
Chapter 18

Détection



Menu : OPERATORS > Inspectra > Codebreaker

Depuis la section '**OPERATORS - Inspectra - Codebreaker**', l'opérateur accède à un tableau recensant les shellcodes encodés ou non, polymorphes, et les powershells au travers du moteur de détection **CODEBREAKER**.



Au-dessus de ce tableau, l'opérateur peut cliquer dans le champ '**From - To**' pour définir la plage de temps (au format *jj/mm/aaaa HH:MM*) des données qui s'affichent.

Number of results max: est le nombre maximum de résultats affichés dans le tableau.

Les colonnes du tableau sont déplaçables et des recherches dynamiques peuvent être faites sur chacune d'entre

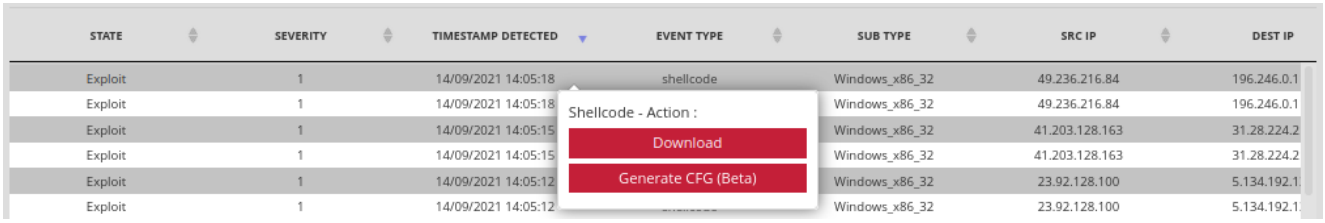
elles:

L'opérateur peut choisir la visibilité des colonnes dans le tableau en cliquant sur le bouton *Column visibility*.

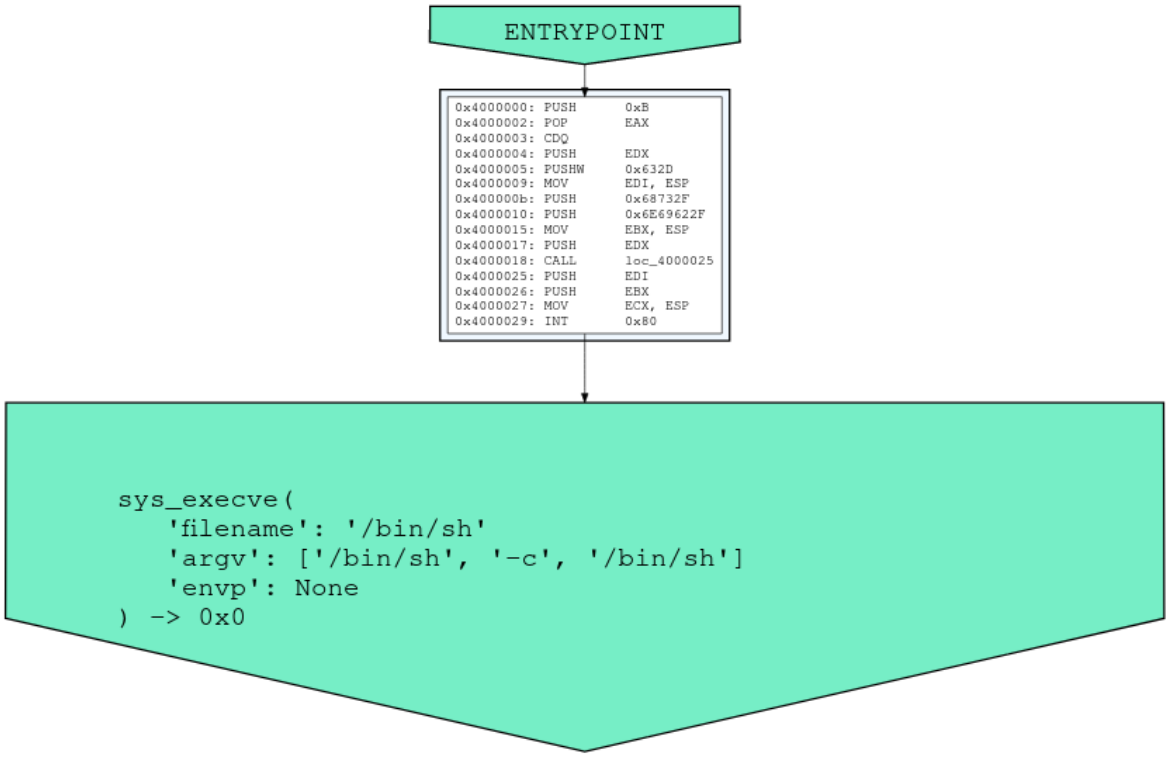
Il est également possible d'effectuer une exportation rapide en CSV des données en fonction de la date de décision sélectionnée:

Une analyse interactive de l'élément est possible grâce à un ***clic droit*** de la souris. Avec '**Download**' il est possible de télécharger le Shellcode/PowerShell et l'enregistrer sur le poste dans un fichier protégé par un mot de passe au format `.zip`. Ce mot de passe est modifiable *ici*.

L'opérateur peut également utiliser la fonction '**Generate CFG**' pour obtenir une version graphique et simplifiée des instructions du Shellcode détecté.



Ci-dessous, un exemple d'une génération CFG d'un shellcode simple détecté par le moteur d'analyse **CODEBREAKER**:



Enfin, comme le reste des informations analysées par la solution TRACKWATCH, les données générées par Codebreaker sont disponibles dans le *dashboard* Kibana qui lui est dédié.

Chapter 19

Événements générés

19.1 Codebreaker Shellcode

19.1.1 Exemple de log Codebreaker Shellcode

```
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": {
        "call": "ws2_32_recv",
```

(suite sur la page suivante)

(suite de la page précédente)


```
        "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 Tableau récapitulatif des compteurs Codebreaker Shellcode

19.2 Codebreaker Powershell

19.2.1 Modifications des évènements Codebreaker Powershell

19.2.2 Exemple de log Codebreaker Powershell


```
json
{
    "flow_id": "2248143006711922",
    "@version": "1",
    "timestamp_detected": "2021-07-06T17:39:29.442Z",
    "MD5": "c2eae0da7d9e27a10ae889cef2d21d0d",
    "SHA256": "04fa65e0e344dfff0396ca9fe3e36ce55f1c2777c698874458b97289383e5de5",
```


(suite sur la page suivante)

(suite de la page précédente)


```
  "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 Tableau récapitulatif des champs Codebreaker Powershell

Chapter 20

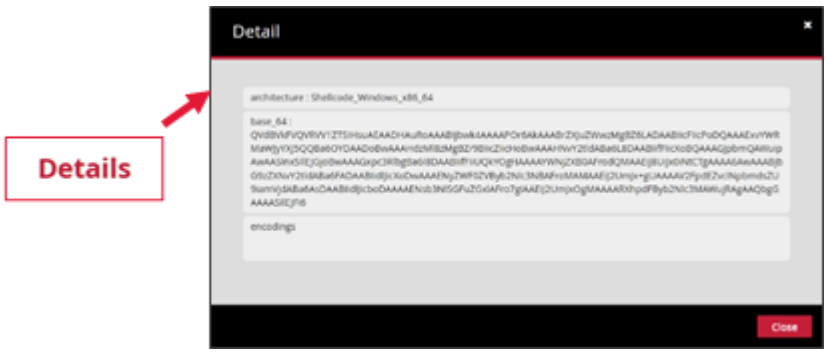
GScan

20.1 Shellcode Scanning

Menu : Operators > GScan > Shellcode Scanning

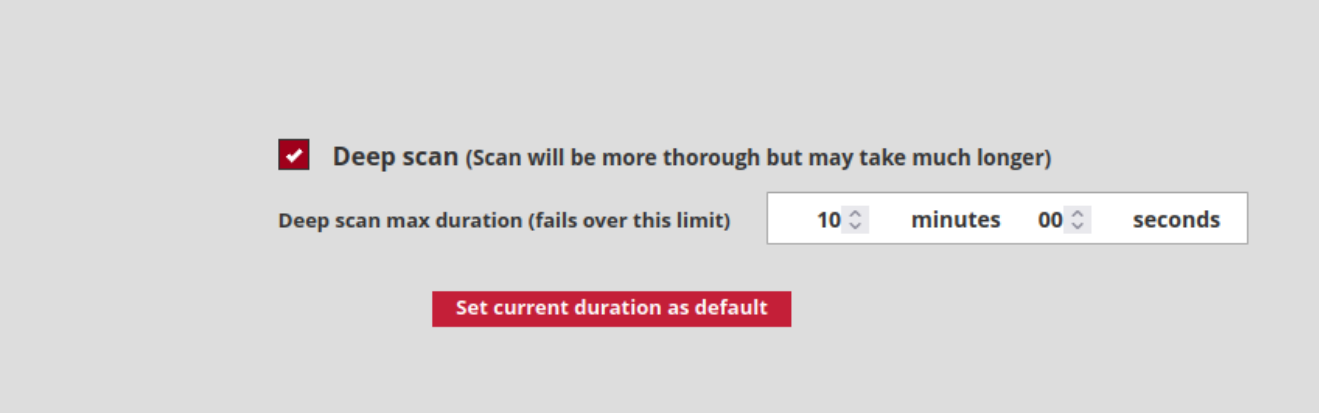
GScan shellcode permet de soumettre manuellement des fichiers afin qu'ils soient analysés par le moteur de détection codebreaker.

Cette information est présente dans les 'Details'.



La fonctionnalité **Deep Scan** permet d'améliorer la détection de pattern ou de méthode d'obfuscation inconnue.

Il est possible de configurer le temps d'analyse et d'activer/désactiver la fonctionnalité.

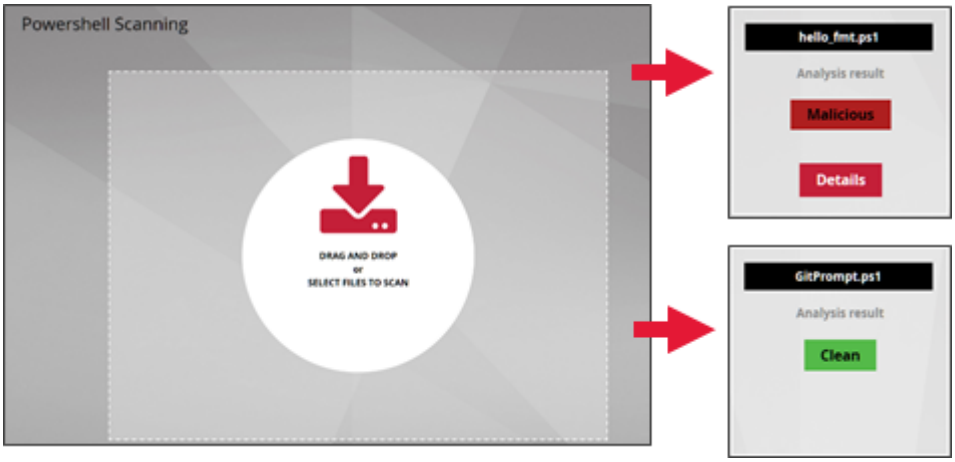


20.2 Powershell Scanning

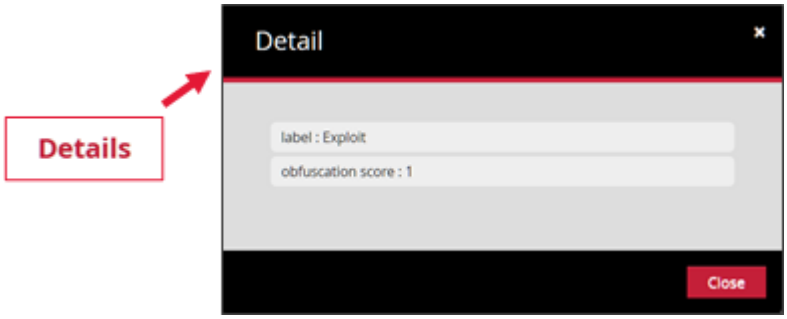
Menu : Operators > GScan > Powershell Scanning

Cette interface laisse la possibilité de scanner des fichiers contenant des scripts POWERSHELL et détecter de potentielles menaces pouvant servir de porte d'entrée pour installer des logiciels malveillants sur Windows.

En ce qui concerne les powershells malveillants, la détection se base sur un modèle de Machine Learning supervisé, et sur le fait que ces scripts utilisent généralement des techniques d'obfuscation ou qui s'y apparentent (base64, concaténation, conversion de type, etc. . .).

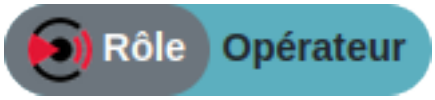


Quelques informations en plus sont accessibles depuis l'onglet 'Details'.



Le résultat peut-être à l'état : Clean ou Malicious en fonction du score d'obfuscation.

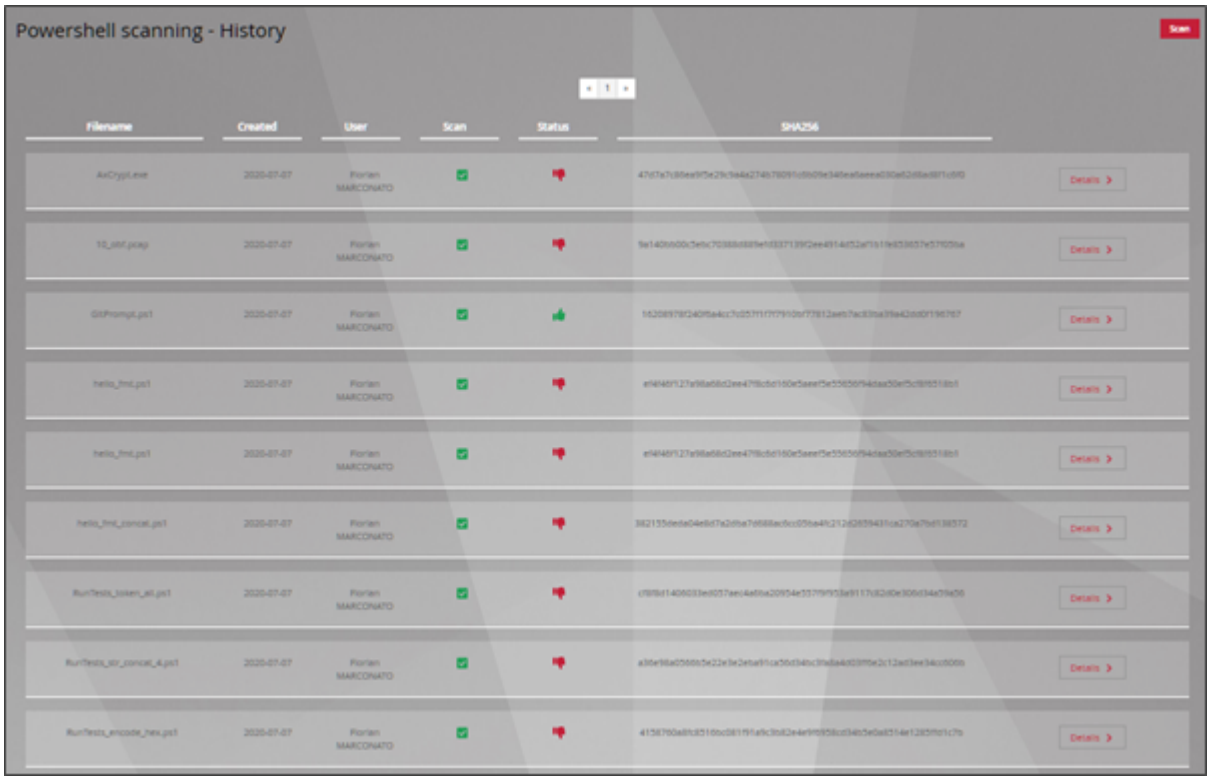
20.3 Historique



Menu :

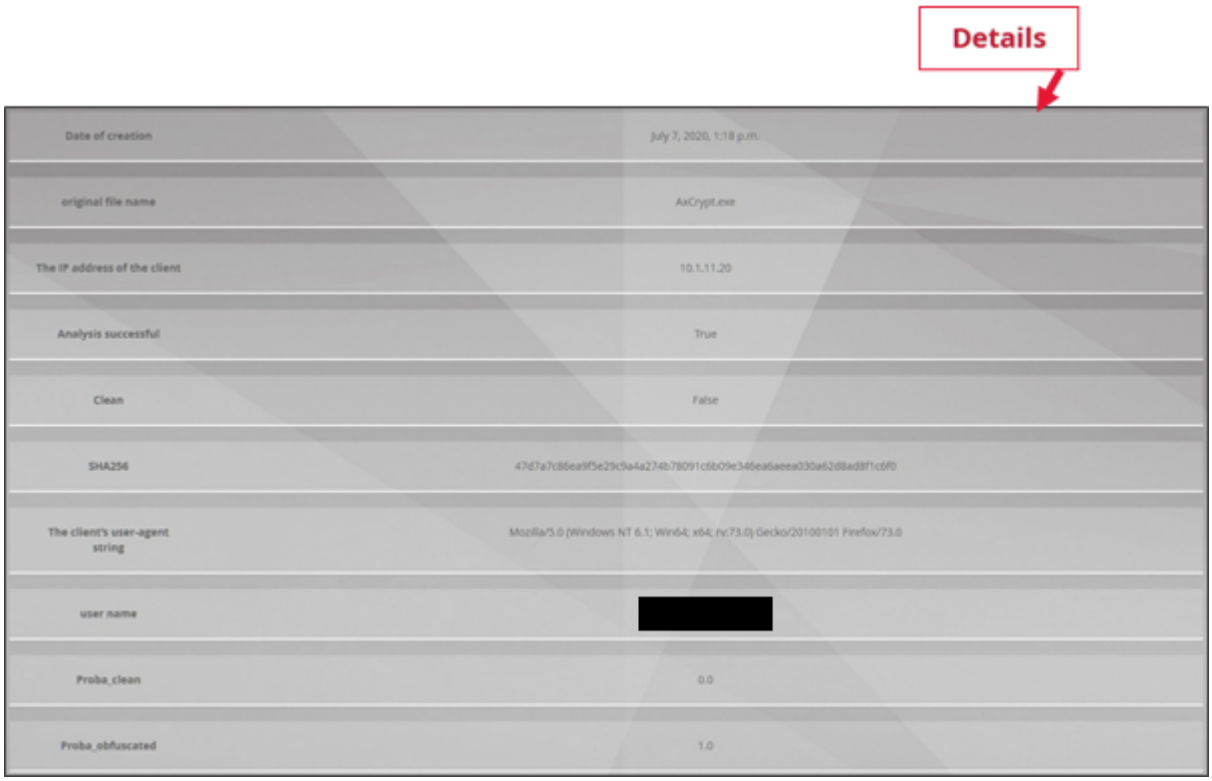
- Operators > GScan > Malware Scanning
- Operators > GScan > Shellcode Scanning
- Operators > GScan > Powershell Scanning

Pour tous les scans MALCORE, CODEBREAKER ou POWERSHELL, un historique des fichiers scannés par moteur d'analyse est disponible.



La liste des fichiers qui ont été scannés est visible sur l'interface.

Les informations détaillées sont accessibles via 'Details'.


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
Proba_clean
0.0
Proba_obfuscated
1.0

Chapter 21

Présentation

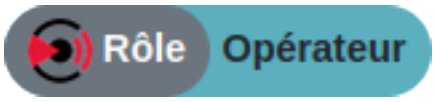
SIGFLOW analyse l'ensemble du trafic réseau et peut, suivant des **règles**, générer des alertes, des métadonnées ou des contenus. Ces règles, qui peuvent provenir de différentes sources, doivent décrire les caractéristiques des attaques qui devront être détectées mais doivent également être optimisées pour réduire les faux positifs. Gatewatcher propose un ensemble de règles qui peut être téléchargé depuis sa plateforme de mise à jour. Les paragraphes suivants détaillent les manipulations nécessaires pour fournir ces règles au module SIGFLOW du GCAP à travers le GCENTER.

Les étapes de base de configuration sont les suivantes :

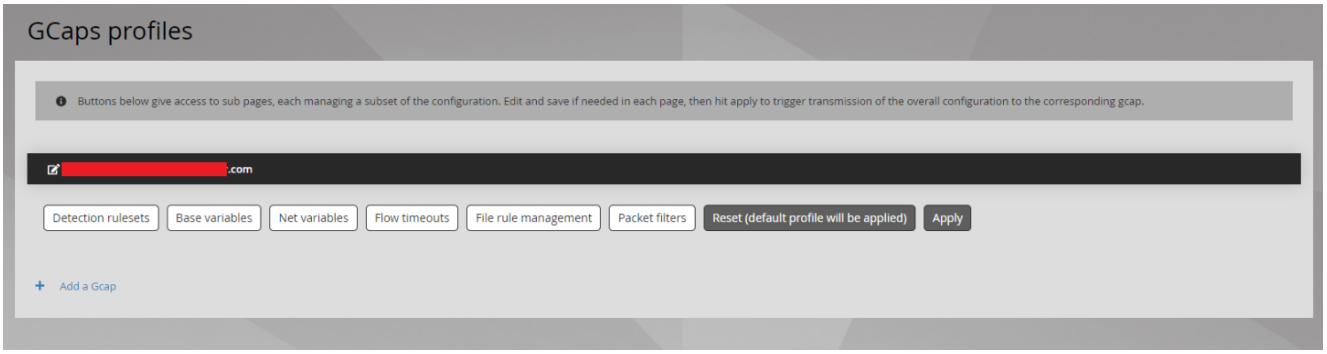
- *Gestion des sources de règles disponibles*
- *Création des ruleset à partir des sources*
- *Générer les rulesets* (important)
- *Application de ruleset sur le gcap*
- *Configuration avancée des paramètres du gcap*

Chapter 22

GCAP Profiles



Menu : Operators > Sigflow > GCap Profiles

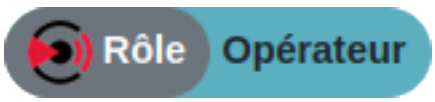


Depuis cette interface de configuration, les utilisateurs pourront appliquer une politique de règles spécifiques et personnaliser les paramètres depuis les catégories suivantes :

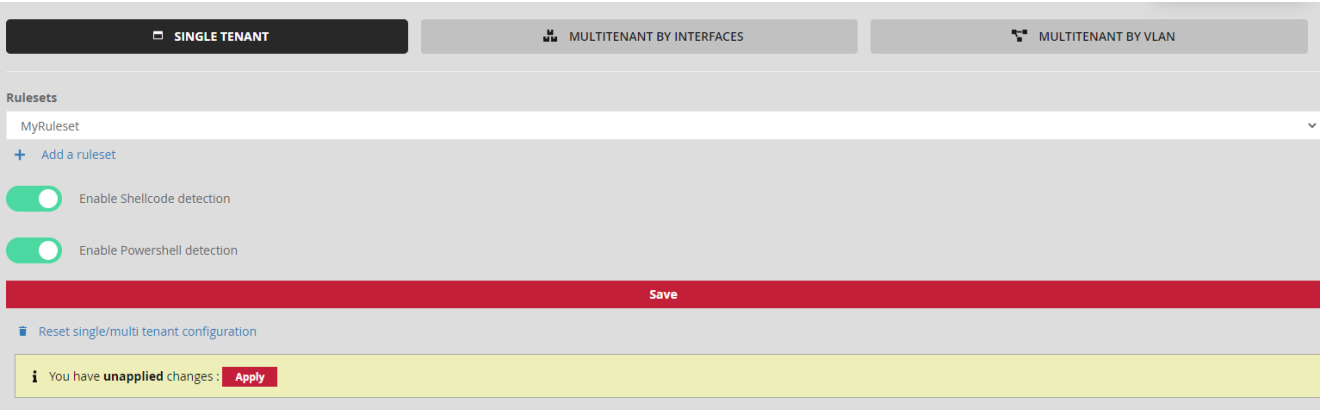
- *Detection Ruleset*
- *Base variables*
- *Net variables*
- *Flow timeouts*
- *Files rules management*
- *BPF filter*

Afin que le moteur de détection puisse démarrer sur la sonde GCap, l'utilisateur doit d'abord y appliquer un ruleset. Voir la section *Sigflow/Rulesets* concernant la création d'un ruleset".

22.1 Detection Rulesets



Menu : Operators > Sigflow > GCAP Profiles



La section **Detection Rulesets** permet l'application des Rulesets SIGFLOW précédemment créés aux GCAP appairés sur le GCENTER. Il est également possible de configurer le module codebreaker pour le GCAP qui comprend l'activation ou la désactivation de la détection des shellcodes et des powershells de façon séparés.

Note:

Il est nécessaire de générer les règles d'un ruleset avant de l'appliquer aux GCAPs. Dans le cas contraire, aucune règle ne sera appliquée.

Note:

Codebreaker n'est pas configurable via le menu **Detection Rulesets** avec la licence CIE.

Le menu Detection Rulesets du GCAP permet 3 options de configuration:

- **Le single tenant:**
  - Attribuer un ruleset pour toutes les interfaces de monitoring du GCAP,
  - Activer/désactiver codebreaker pour toutes les interfaces de monitoring du GCAP.
- **Le multi-tenant by interface:**
  - Attribuer un ruleset par interface de monitoring du GCAP,
  - Activer/désactiver codebreaker par interface de monitoring du GCAP.
- **Le multi-tenant by vlan:**
  - Attribuer un ruleset par vlan,
  - Attribuer un ruleset pour le vlan par défaut (les vlans non créés via l'interface),
  - Activer/désactiver codebreaker par vlan,
  - Activer/désactiver codebreaker pour le vlan par défaut (les vlans non créés via l'interface).

Note:

Ces options de configuration sont exclusives. Cela signifie qu'il ne sera pas possible d'application une configuration single tenant et multi-tenant by vlan en même temps.

22.1.1 Single-tenant

Note:

Les modifications de cet onglet nécessitent la sauvegarde et l'application de la configuration du GCAP via le bouton save puis apply.

Configuration du single-tenant:

1. Se rendre dans l'onglet `Single-tenant`,
2. Sélectionner un ruleset à appliquer pour toutes les interfaces,
3. Activer ou désactiver la détection des shellcodes pour toutes les interfaces,
4. Activer ou désactiver la détection des powershells pour toutes les interfaces,
5. Appliquer la configuration via le bouton "save".

22.1.2 Multi-tenant by interface

Le **multi-tenant by interface** permet d'appliquer une configuration single-tenant pour chacune des interfaces du GCAP et donc d'avoir une supervision différente par interface. En effet il est possible d'appliquer un ruleset SIGFLOW différent ainsi que de configurer codebreaker pour chacune des interfaces du GCAP.

Note:

Une optimisation des règles SIGFLOW au préalable est conseillée avant de choisir cette option de configuration. Les règles doivent en effet être adaptées à l'environnement monitoré.

Note:

Il est nécessaire de vérifier que plusieurs interfaces de monitoring sont activées sur le GCAP avant d'appliquer une configuration multi-tenant by interface.

Note:

Les modifications de cet onglet nécessitent la sauvegarde et l'application de la configuration du GCAP via le bouton save puis apply.

Note:

Seuls les interfaces de monitoring activées apparaissent dans l'interface du GCENTER.

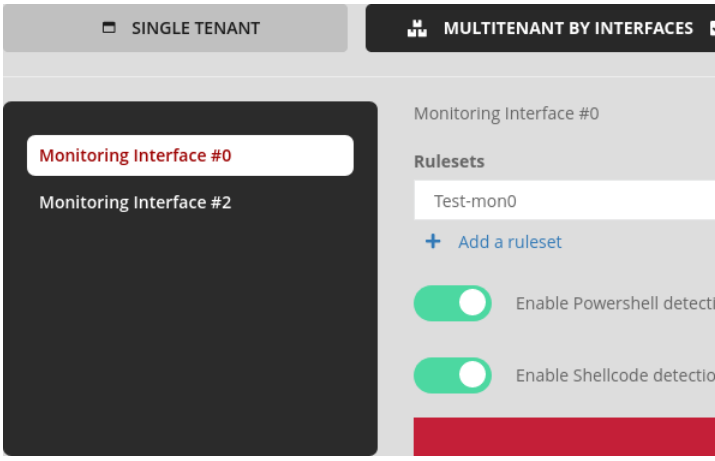
Configuration du multi-tenant by interface:

1. Se rendre dans l'onglet `Multi-tenant by interface`,
2. Sélectionner un ruleset à appliquer pour chaque interface,
3. Activer ou désactiver la détection des shellcodes pour chaque interface,
4. Activer ou désactiver la détection des powershells pour chaque interface,
5. Appliquer la configuration via le bouton "save".

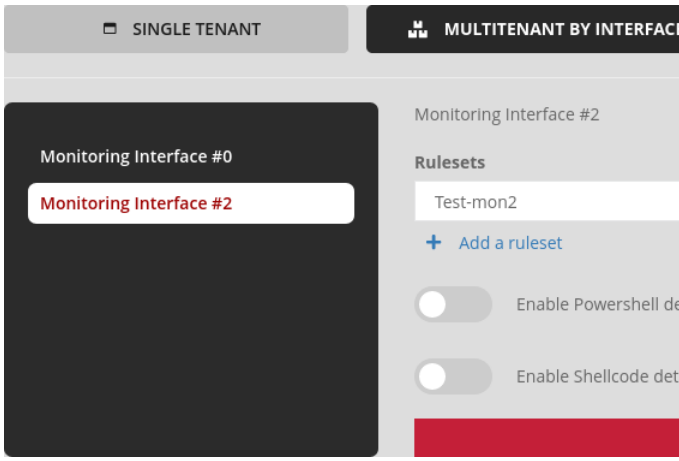
Exemple de configurations:

- **interface mon0:**

  - Ruletset nommé "Test-mon0",



  - Activation de la detection des shellcodes/powershells.
- **interface mon2:**
  - Ruletset nommé "Test-mon2",



  - Désactivation de la détection des shellcodes/powershells.

22.1.3 Multi-tenant by vlan

Le **multi-tenant by vlan** permet d'appliquer une configuration pour chaque vlan précédemment créé dans l'interface et d'avoir une supervision différente sur des réseaux différents. Il est donc possible d'appliquer un ruleset SIGFLOW ainsi que de configurer codebreaker de manière indépendante pour chaque vlan. Un vlan nommé "default" est créé par défaut dans l'interface. Il permet d'appliquer un ruleset SIGFLOW et de configurer codebreaker pour l'ensemble des vlans qui ne sont pas explicitement déclarés dans l'interface.

Note:

Une optimisation des règles SIGFLOW au préalable est conseillée avant de choisir cette option de configuration. Les règles doivent en effet être adaptées à l'environnement monitoré.

Note:

Les modifications de cet onglet nécessitent la sauvegarde et l'application de la configuration du GCAP via le bouton save puis apply.

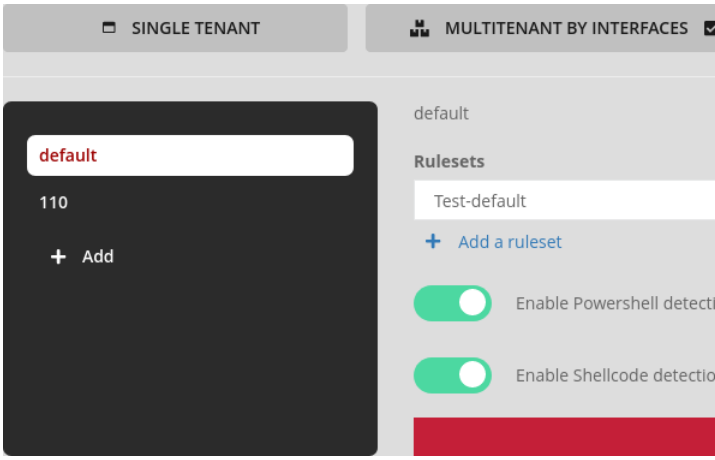
Configuration du multi-tenant by vlan:

1. Se rendre dans l'onglet `Multi-tenant by vlan`,
2. Sélectionner un ruleset à appliquer pour le vlan "default",

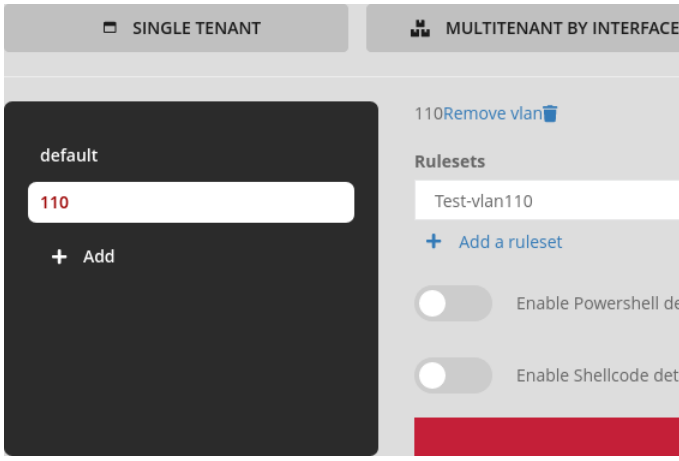
3. Activer ou désactiver la détection des shellcodes pour le vlan "default",
4. Activer ou désactiver la détection des powershells pour le vlan "default",
5. Créer autant de vlan que nécessaire via le bouton "Add",
6. Le nom du vlan doit correspondre au numéro de vlan entre 0 et 4096,
7. Sélectionner ensuite un ruleset à appliquer pour chaque vlan,
8. Activer ou désactiver la détection des shellcodes pour chaque vlan,
9. Activer ou désactiver la détection des powershells pour chaque vlan,
10. Appliquer la configuration via le bouton "save".

Exemple de configurations:

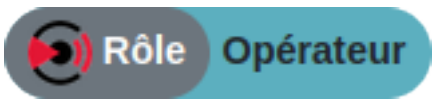
- **vlan "default":**
  - Ruletset nommé "Test-default",
  - Activation de la détection des shellcodes/powershells.



- **vlan "110":**
  - Ruletset nommé "Test-vlan110",
  - Désactivation de la detection des shellcodes/powershells.



22.2 Base variables



Menu : Operators > Sigflow > GCAP Profiles

La section **Base variables** va permettre à l'opérateur d'ajuster les paramètres de capture de la sonde grâce aux fonctions avancées de Suricata configurable depuis **GCENTER**. Les modifications de cette configuration entrainent des répercussions sur les remontées d'alertes depuis la sonde **GCAP** vers le **GCENTER**. L'activation de certaines options va permettre l'émission d'alertes, d'anomalies, de métadonnées, d'informations sur les fichiers et des enregistrements spécifiques aux protocoles.

Les alertes sont des enregistrements d'événements provoqués par la correspondance d'une règle avec le trafic réseau. Une alerte sera générée avec des métadonnées associées, comme l'enregistrement de la couche applicative (HTTP, DNS, etc).

Le menu se découpe en trois sections:

- General
- Stream
- Parsing

22.2.1 Base Variables - General

L'onglet **Base Variables - General** permet la configuration des paramètres avancés de la sonde GCAP (Suricata).

Note:

Les modifications de cet onglet nécessitent la sauvegarde et l'application de la configuration du GCAP via le bouton save puis apply.

Les valeurs par défaut des variables de l'onglet général:

Liste des variables de l'onglet General:

- **File resend interval (seconds):** intervalle de temps (en seconde) où, si un fichier identique est vu sur le réseau, il ne sera pas de nouveau envoyé vers le GCENTER par le GCAP. Seules les métadonnées le seront avec le champ Replica à True. Au-delà de ce délai, si le même fichier est vu sur le réseau, il sera de nouveau envoyé vers le GCENTER.
- **Max pending packets:** Nombre de paquets simultanés que le moteur SURICATA peut gérer. Cela peut aller d'un paquet à des dizaines de milliers de paquets. Ce paramètre jouera sur les performances et sur l'utilisation de la mémoire (RAM). Un nombre élevé de paquets en cours de traitement permet d'obtenir de meilleures performances et d'utiliser plus de mémoire, et inversement. Choisir un faible nombre de paquets en cours de traitement tout en ayant plusieurs cœurs de CPU, peut avoir pour conséquence de ne pas utiliser la totalité de la capacité de la sonde (Exemple : utiliser un seul *core* tout en ayant 3 paquets en attente de traitement).
- **Enable XFF:** Activation de la gestion de l'entête HTTP *X-Forwarded-For* en ajoutant un nouveau champ ou en écrasant l'adresse ip source ou destination (suivant le sens du flux) par l'ip renseignée dans cet entête. Le comportement (ajout de champ ou écrasement) est géré par la directive **XFF mode**. Cette directive est utile dans le cas de traitement de flux derrière un reverse proxy par exemple.
- **XFF mode:** Comportement attendu lors de l'activation de XFF. Deux types de modes de fonctionnement sont disponibles extra-data ou overwrite. A noter qu'en mode 'overwrite', si l'adresse IP rapportée dans l'entête HTTP X-Forwarded-For est d'une version différente du paquet reçu, alors elle passera en mode 'extra-data'.
- **XFF deployment:** Type de déploiement de XFF. Deux types de déploiement sont disponibles : *reverse* ou *forward*. Dans un déploiement *reverse*, l'adresse IP utilisée est la dernière, alors que dans un déploiement *forward*, l'adresse IP utilisée est alors la première.
- **Xff header:** C'est le nom de l'entête HTTP où l'adresse IP réelle est présente. Si plus d'une adresse IP est présente, la dernière adresse IP sera celle prise en compte.
- **Payload:** Ajoute un champ contenant la charge utile encodée en base 64 d'un flux déclenchant une alerte.
- **Payload buffer size:** taille maximale de la mémoire tampon de la charge utile à ajouter dans l'alerte.
- **Payload printable:** Ajoute un champ contenant la charge utile (*Payload*) au format ASCII (dit 'humain').
- **Packet:** dump du paquet capturé encodé en base64.
- **HTTP body:** Ajoute un champ contenant le body des requêtes HTTP encoder en base64. Pour fonctionner, ce paramètre nécessite des métadonnées.
- **HTTP body printable:** Ajoute un champ contenant le body des requêtes HTTP au format ASCII (dit "humain"). Pour fonctionner, ce paramètre nécessite des métadonnées.
- **Flow memcap:** allocation maximale pour les flux en octet.
- **Flow prealloc:** allocation initiale du flux.
- **FTP memcap (B) :** 'allocation maximale pour les flux.

- **SMB Stream Depth (B):** La taille des fichiers qui peuvent être restaurés et stockés dépend de la valeur en mégaoctets. Au-delà de cette valeur, aucune reconstruction ne sera effectuée. Si cette valeur est atteinte, le fichier peut être tronqué et peut ne pas être stocké complètement. Cela signifie qu'après cette valeur, la session SMB ne sera plus suivie. De plus, les valeurs négatives désactivent l'option. Le réglage à 0 de cette valeur permet de stocker n'importe quelle taille de fichier.
- **Files hash:** Permet de faire le choix de la fonction de hachage pour les fichiers reconstruit (md5, sha1 et sha256). Par défaut, md5 est sélectionné. Le hash sha256 sera dans tous les cas ajouté par le module *Malcore*.

22.2.2 Base Variables - Stream

```
 caution:: La modification des paramètres de cette section peut causer des dysfonctionnements␣
↪de la solution TRACKWATCH. Cette partie est réservée au support et aux utilisateurs avancés.
Seule la variable "file_store_stream_depth_mb" peut être modifiée, sans jamais dépasser 100␣
↪MB.
```

L'onglet **Base Variables - Stream** permet la configuration des paramètres de reconstruction des fichiers ainsi que du module **Stream-engine** de la sonde GCAP (Suricata). Le module **Stream-engine** de la sonde permet le suivi des connexions TCP.

Note:

Les modifications de cet onglet nécessitent la sauvegarde et l'application de la configuration du GCAP via le bouton save puis apply.

Le moteur est composé de deux parties:

- **Stream-tracking engine:** Permet de suivre l'état des connexions TCP,
- **Reassembly-engine:** Reconstruit le flux afin qu'il soit analysé par Suricata.

Les valeurs par défaut des variables de l'onglet stream:

Liste des variables de l'onglet Stream:

- **Enable File-Store stream depth:** Permet d'activer le contrôle de la taille des fichiers stockés.
- **File-store stream depth (Mb):** Fixe la taille maximum des fichiers qui peuvent être restaurés et stockés en mégaoctets. Si cette valeur est atteinte, le fichier peut être tronqué et peut ne pas être stocké complètement. Cela signifie qu'après cette valeur, la session HTTP ne sera plus suivie. Une valeur négative désactive l'option et la valeur 0 permet de stocker n'importe quelle taille de fichier. Si cette option n'est pas activée, alors la valeur de 'Stream reassembly depth (Mb)' sera prise en compte.
- **Stream memcap (B):** Cette valeur est la valeur maximale en octets allouée au suivi des sessions TCP. Afin d'éviter un manque de ressources, un memcap peut être utilisé pour limiter la mémoire utilisée.
- **Stream Prealloc sessions:** C'est la quantité de sessions que le moteur SURICATA doit garder disponible en mémoire. Ce moteur fonctionne indépendamment du traitement des paquets et possède un 'thread' de gestion assurant le paramétrage de cette valeur à l'intérieur du memcap afin d'allouer de la mémoire. L'option permet d'éviter à SURICATA d'être surchargé par la création rapide de sessions et lui demande de garder un certain nombre de sessions prêtes en mémoire. Il spécifie le nombre d'éléments à pré-allouer au démarrage du logiciel. Ceci diminue le coût des allocations en cours de fonctionnement aux dépens de l'utilisation mémoire initiale du logiciel.
- **Stream reassembly memcap (B)** Le moteur de reconstitution de flux doit conserver des segments de données en mémoire afin de pouvoir le reconstruire. Pour éviter le manque de ressources, un memcap est utilisé pour limiter la mémoire utilisée. Cette option est la quantité maximale d'octets que le moteur de flux peut utiliser pour restaurer un fichier.
- **Enable the randomizable of chunks size:** Le but de ce paramètre est d'éviter de rendre la reconstitution de morceaux trop prévisible. Pour cela, leur taille sera modifiée par un facteur aléatoire qui sera ajouté.
- **Stream reassembly depth (Mb)** C'est la taille du flux réseau en mégaoctets. Le fait de reconstruire un flux de données est une opération très importante qui pourra se contrôler avec la notion de 'depth'. La valeur par défaut est un paramètre qui peut être remplacé par les analyseurs de protocoles qui effectuent

l'extraction des fichiers. L'inspection sera ignorée si cette valeur est atteinte pour un débit en particulier. Le réglage à 0 de cette valeur permet de stocker n'importe quelle taille de flux.
- **Stream reassembly to server chunk size (B)** La reconstruction d'un flux de données se fait par morceaux. La taille de ces morceaux est à définir au niveau de ce champ pour que le flux soit inspecté et reconstruit à partir de cette valeur.
- **Stream reassembly to client chunk size (B)** La reconstruction d'un flux de données se fait par morceaux. La taille de ces morceaux est à définir au niveau de ce champ pour que le flux soit inspecté et reconstruit en fonction de celle-ci.

22.2.3 Base Variables - Parsing

L'onglet **Base Variables - Parsing** permet la configuration du **parsing** et du **logging** des protocoles utilisés par la sonde GCAP. Les protocoles pouvant être analysés et journalisés sont présent dans l'interface **GCenter**. Dans le cas où une sonde **GCAP** a une version d'avance sur le GCenter, il est possible que certains protocoles aient été ajoutés.

Ce point est abordé plus en détail dans la documentation **GCAP** dans la section `Moteur de détection > 3. Sélectionner les protocoles analysés`.

Terminologie des termes parsing et logging:

- La **parsing** consiste à activer la détection des signatures SIGFLOW pour un protocole donné. En effet si ce dernier est activé pour un protocole alors le flux qui est identifié par une signature lèvera une alerte SIGFLOW dans le dashboard Kibana.
- La **logging** consiste à activer la génération de métadonnées pour un protocole donné. En effet, si ce dernier est activé pour un protocole alors chaque session observée lèvera une alerte pour ce protocole dans le dashboard Kibana.

Note:

La configuration par défaut des protocoles varie en fonction du profil du GCAP utilisé.

Note:

Les modifications de cet onglet nécessitent la sauvegarde et l'application de la configuration du GCAP via le bouton save puis apply.

Voici la liste des protocoles configurables avec l'option parsing:

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

Voici la liste des protocoles configurables avec l'option logging:

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

Voici la configuration par défaut de l'option parsing pour chaque protocole en fonction du profil utilisé:

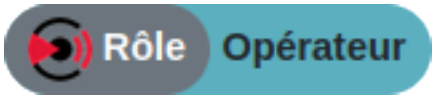
Voici la configuration par défaut de l'option logging pour chaque protocole en fonction du profil utilisé:

En plus de ces protocoles, il est également possible de générer des données NetFlow.

Avertissement:

L'activation de la génération de données NetFlow va créer beaucoup de meta-données

22.3 Net variables



Menu : Operators > Sigflow > GCAP Profiles

La section **Net variables** va permettre à l'opérateur de définir les variables réseaux utilisées dans les règles sigflow.

Note:

Les modifications de cette section nécessitent la sauvegarde et l'application de la configuration du GCAP via le bouton save puis apply.

Au niveau de la structure d'une règle SIGFLOW, juste après 'alert' et le mot clé indiquant le protocole, il est possible d'utiliser des variables qui vont permettre de définir des groupes d'adresses IP.

Dans l'exemple suivant :

```
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;)
```

Ces flux doivent aller de $HOME_NET vers $EXTERNAL_NET.

La première partie $HOME_NET est la source, la seconde $EXTERNAL_NET est la destination. Avec la source et la destination, vous spécifiez la source du trafic et la destination du trafic, respectivement. Vous pouvez attribuer

des adresses IP (IPv4 et IPv6 sont pris en charge) et des plages IP. Ces paramètres seront utilisés à la place des variables dans les règles de détection.

Cette section permet de définir le contenu de ces variables.

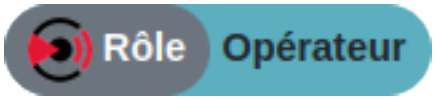
Pour appliquer ces modifications, il sera nécessaire de cliquer sur le bouton **Save and Apply**.

La règle s'adapte aux besoins et peut changer en fonction du paramètre sélectionné au niveau du menu déroulant de chaque environnement. 'list', 'default (equals to HOME_NET)' et 'exclude (opposite of HOME_NET)' permettent respectivement de définir l'action de la règle par rapport à un groupe d'adresse, par rapport aux adresses renseignées dans l'environnement HOME_NET ou par rapport à toutes les adresses ne faisant pas partie de l'environnement HOME_NET.

Il n'est pas nécessaire de définir une adresse pour chacune des variables existantes. Par défaut, quand rien n'est renseigné, cela équivaut à appliquer la règle sur tout le trafic.

La configuration utilisée par défaut:

22.4 Flow timeouts



Menu : Operators > Sigflow > GCAP Profiles

```
caution:: La modification des paramètres de cette section peut causer des dysfonctionnements␣
↪de la solution TRACKWATCH. Cette partie est réservée au support et aux utilisateurs avancés.
```

La section **Flow timeouts** va permettre de configurer le temps (en secondes) pendant lequel Suricata garde un flux en mémoire en fonction de son état. Les protocoles udp, tcp, icmp sont configurables.

Note:

Les modifications de cette section nécessitent la sauvegarde et l'application de la configuration du GCAP via le bouton save puis apply.

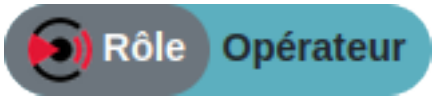
La configuration utilisée par défaut en fonction du protocole (toutes les valeurs sont en secondes):

Pour chaque protocole, il existe différents états dans lesquels un flux peut se trouver:

- **Protocole TCP:**
  - **New:** La période pendant laquelle l'établissement de la connexion se fait. Ce champ est le temps écoulé en secondes après la dernière activité de ce flux dans ce type d'état.
  - **Established:** La période pendant lequel le transfert des données se fait. Ce champ est le temps écoulé en secondes après la dernière activité de ce flux dans ce type d'état.
  - **Closed:** La période pendant laquelle la fin de la connexion se fait. Ce champ est le temps écoulé en secondes après la dernière activité de ce flux dans ce type d'état.
- **Protocoles UDP et ICMP:**
  - **New:** L'état pendant lequel les paquets sont envoyés depuis une seule direction. Ce champ est le temps écoulé en secondes après la dernière activité de ce flux dans ce type d'état.
  - **Established:** L'état pendant lequel les paquets sont envoyés dans les deux sens. Ce champ est le temps écoulé en secondes après la dernière activité de ce flux dans ce type d'état.

Les modes 'Emergency_new', 'Emergency_established' et 'Emergency_closed' sont les modes d'urgence des 3 états des protocoles TCP, UDP et ICMP.

22.5 Files rules management



Menu : Operators > Sigflow > GCAP Profiles

La section **Files rules management** va permettre de configurer les types de fichier que la sonde va extraire pour un protocole donné. Les protocoles compatibles sont: HTTP, SMTP, SMB, NFS, FTP. Les fichiers sont extraits puis enregistrés sur le disque avec des métadonnées qui incluent des informations comme l'horodatage, l'adresse IP source/destination, le protocole, le port source/destination, la taille, le md5sum, etc... L'extraction de fichiers fonctionne en parallèle des signatures SIGFLOW définies pour ces mêmes protocoles. Chaque ligne de la section **Files rules management** correspond à une règle d'extraction d'un type de fichier.

Note:

Un trop grand nombre de règles d'extraction de fichiers peut avoir un impact significatif sur les performances de la sonde.

Note:

Les modifications de cette section nécessitent la sauvegarde et l'application de la configuration du GCAP via le bouton save puis apply.

Voici la liste des champs configurables pour une entrée de la section Files rules management:

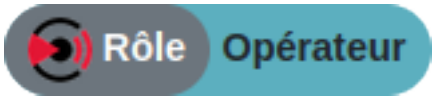
- **Protocole:** Permet de sélectionner le protocole pour lequel le fichier sera extrait parmi: HTTP, SMTP, SMB, NFS, FTP.
- **Type:** Permet de définir la façon dont suricata va reconnaitre le fichier:
  - extension: Correspond à l'extension du fichier.
  - filemagic: Correspond au type du fichier extrait. La commande **file** sous linux permet d'obtenir cette information:

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

- **Value:** L'identifiant du fichier qui sera reconstruit en fonction du type configuré précédemment:
  - **Type extension:**
    - Fichier javascript: js,
    - Fichier executable windows: exe.
  - **Type filemagic:**
    - Fichier javascript: Javascript,
    - Fichier executable windows: PE32 executable.
- **Enable** et **Delete** sont respectivement les cases à cocher pour activer et supprimer la règle d'extraction des fichiers.

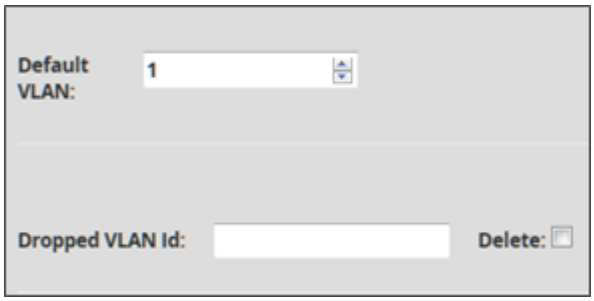
Les règles utilisés en fonction du profil GCAP utilisé:

22.6 Packet filtering



Menu : Operators > Sigflow > GCAP Profiles

Packet filtering va permettre à l'opérateur d'ajuster les paramètres de capture de la sonde de détection grâce aux fonctions avancées de Sigflow.



Le but de cette fonctionnalité est d'agir directement sur le périphérique de capture de la solution TRACKWATCH en modifiant la méthode d'acquisition des paquets grâce à BPF (Barkeley Packet Filter). Le trafic sera donc ignoré pour un identifiant de VLAN donné dans le champ 'Dropped VLAN Id'.

Le numéro de VLAN par défaut est à renseigner sur l'interface Web du **GCENTER** dans 'Default VLAN'. Par défaut, la valeur est à 1. Une fois le VLAN renseigné, une fenêtre apparait pour que l'opérateur puisse rajouter les informations réseaux sur le trafic qu'il souhaite vouloir faire disparaitre de ses notifications.

L'opérateur peut supprimer une règle de filtrage via la case **Delete**. Les modifications sont sauvegardées lors de la validation du formulaire en cliquant sur le bouton **Save**. Cependant afin de les appliquer il sera nécessaire de cliquer sur le bouton **Save and Apply** sur la page de configuration.

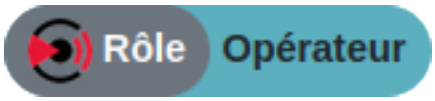
Chapter 23

Gestion des règles

Les signatures du moteur **Sigflow** sont organisées de la manière suivantes :

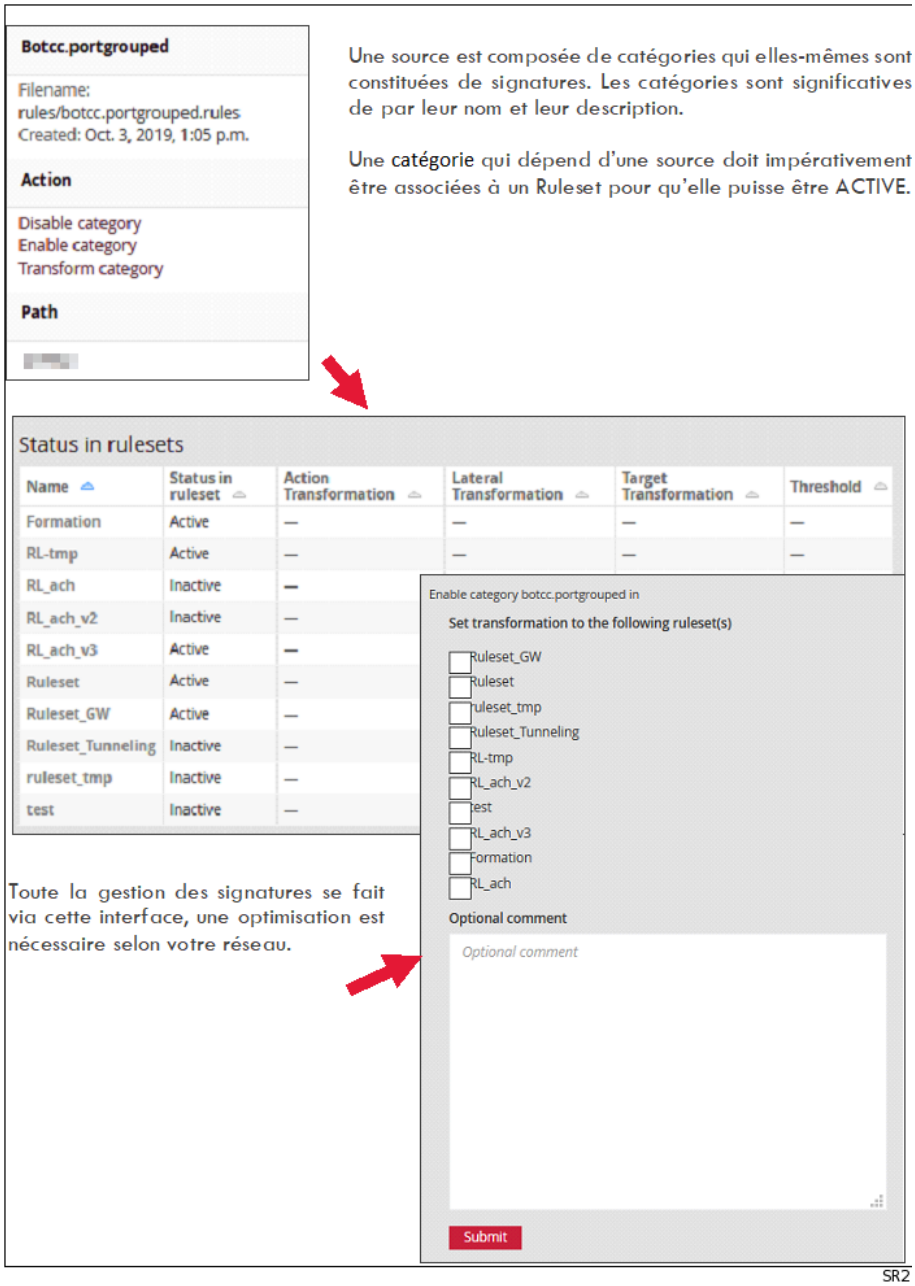
- Une liste de source mettant à disposition des signatures
- Une liste de signatures pouvant être adaptées au besoin de l'environnement à surveiller
- Une liste de *Ruleset* permettant de faire le lien entre les signatures et leur sources et un **GCAP**

23.1 Sources



Menu : Operators > Sigflow > Sources

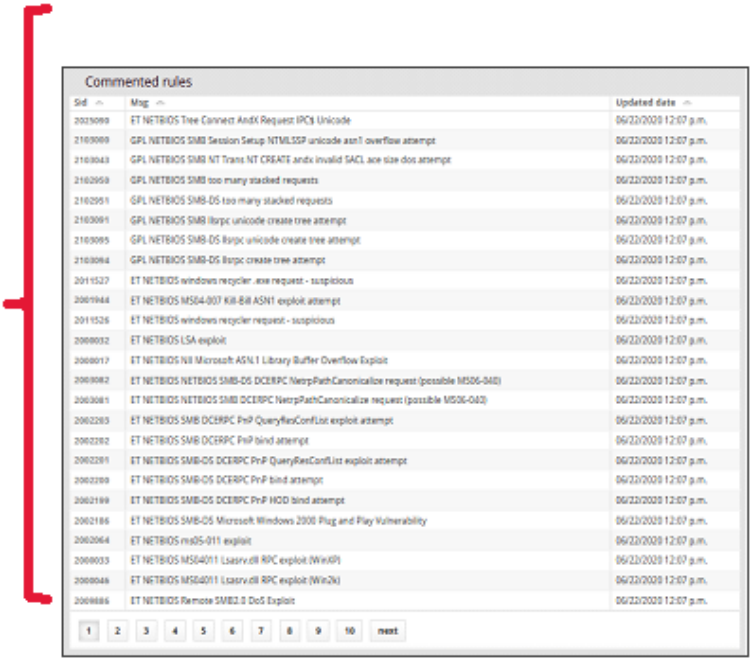
Les sources permettent de déclarer des endroits où sont mises à disposition les signatures.


Botcc.portgrouped
Filename:
rules/botcc.portgrouped.rules
Created: Oct. 3, 2019, 1:05 p.m.
Action
Disable category
Enable category
Transform category
Path
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.
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.

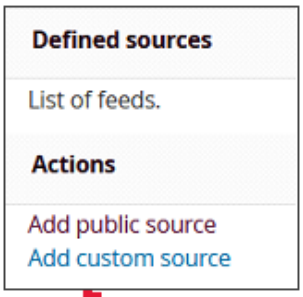
SR2

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.



Une fois téléchargées puis décompressées, les règles devront être ajoutées dans l'interface du **GCENTER**.



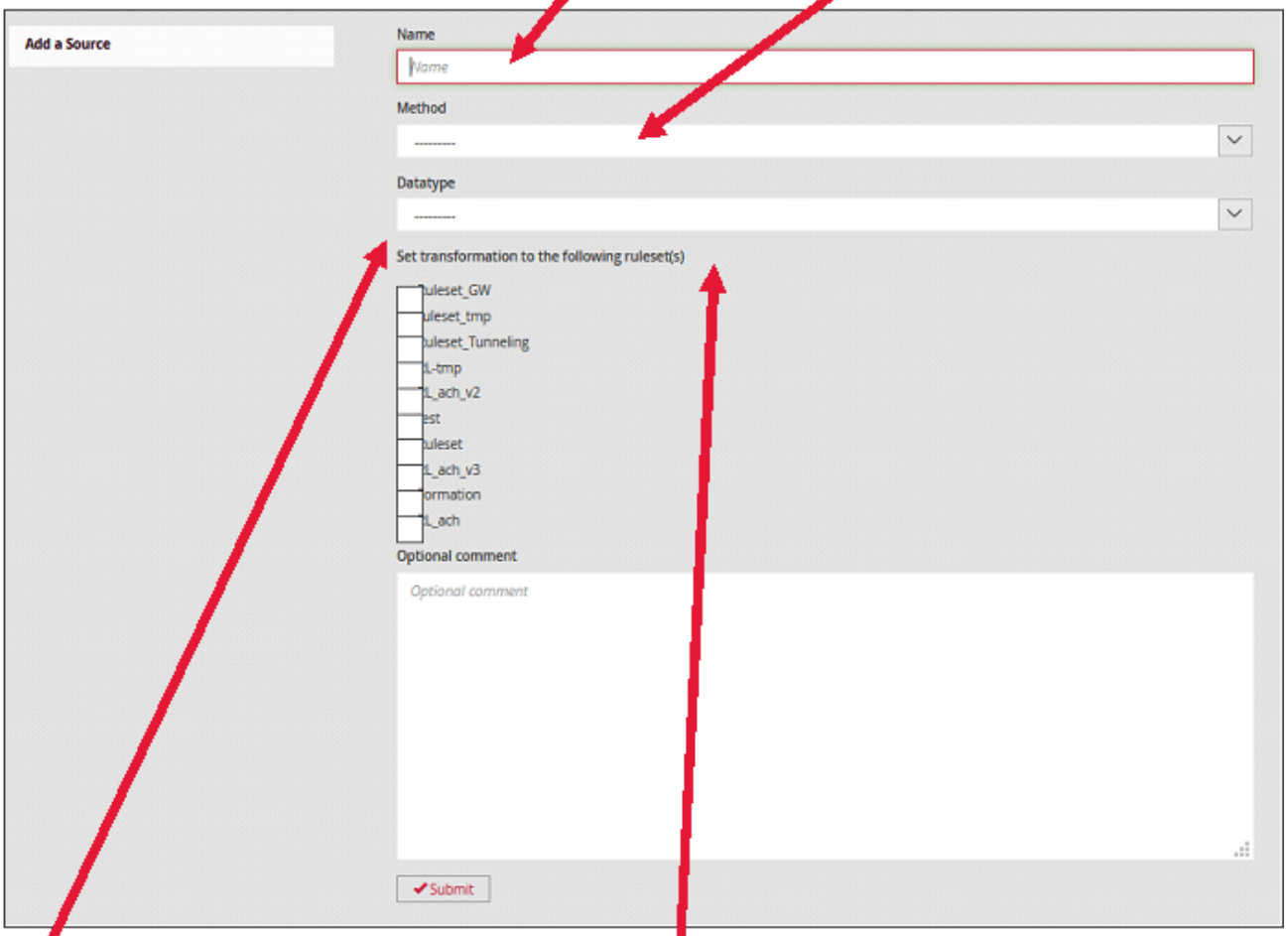
Nous préconisons le package SIGFLOW par défaut, mais l'administrateur peut ajouter à n'importe quelque moment ses propres signatures. En effet les extensions suivantes sont pris en compte par l'interface : **.yara, .rules, .openioc, .csv, .txt.**

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

Méthode :
- HTTP URL
- Upload

1 Nom de la règle

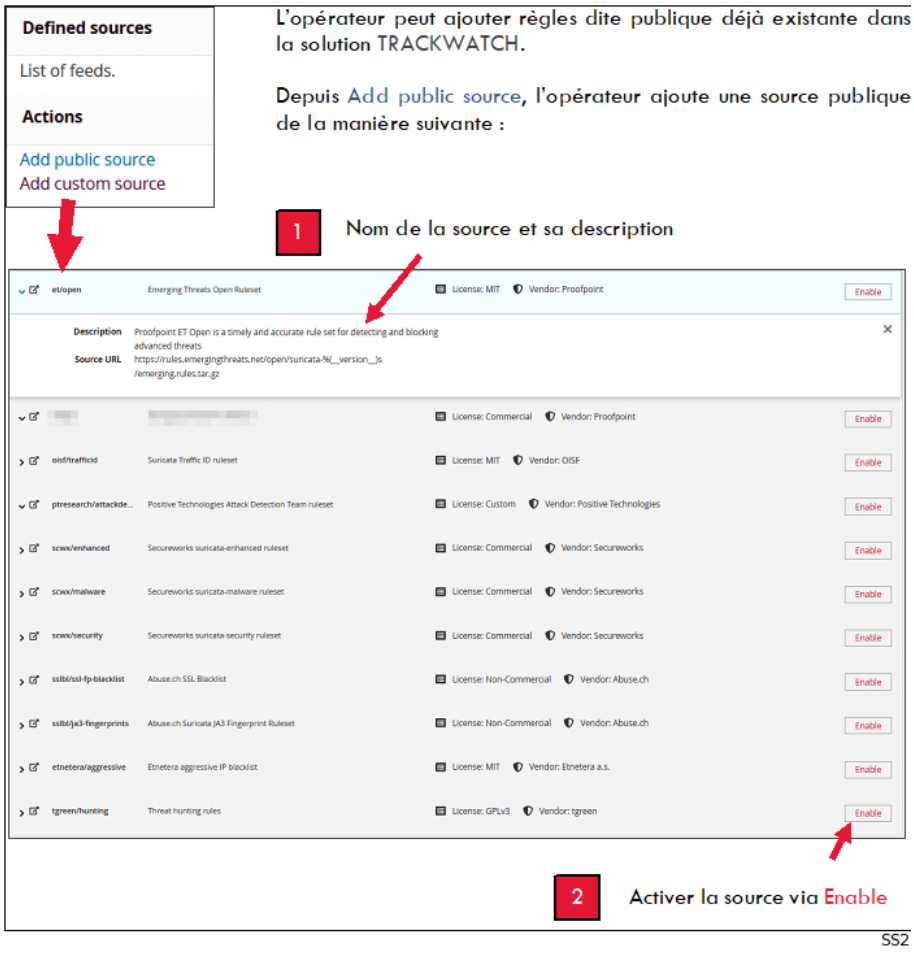
2



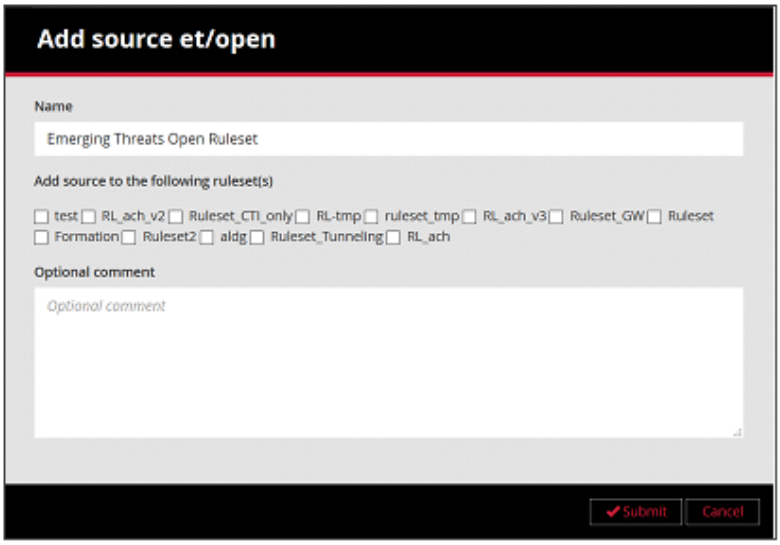
3 Type des données :
- Signatures dans une archive .tar
- Signatures dans un fichier
- Autres

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.



Une fois les règles ajoutées, l'opérateur peut directement affecter cette source à différents Rulesets

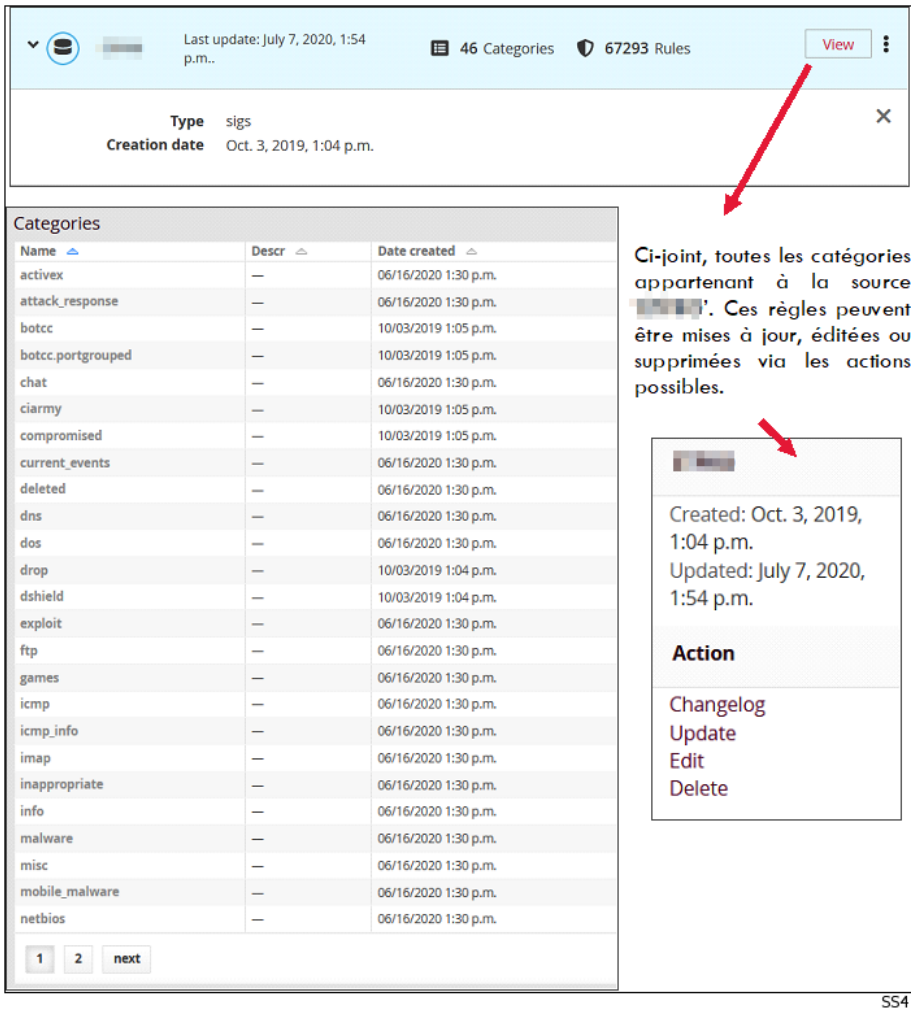


Le nom peut être édité puis la source est ajoutée aux Rulesets déjà présents en cochant la case associée.

Un commentaire optionnel pour le suivi est possible.

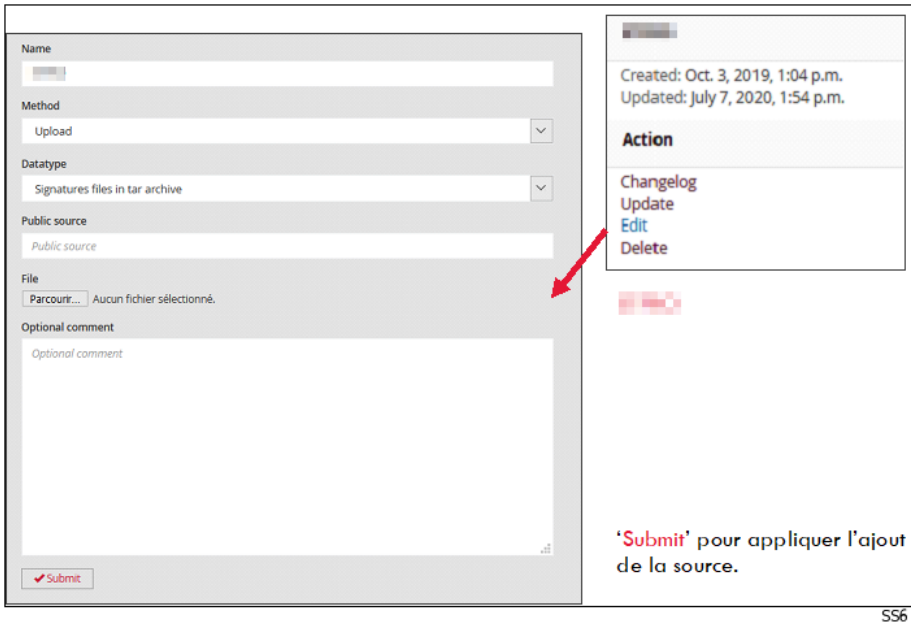
Valider avec 'Submit' une fois le choix fait.

La visualisation d'une règle custom se fait depuis l'onglet 'View' dans Add custom source:



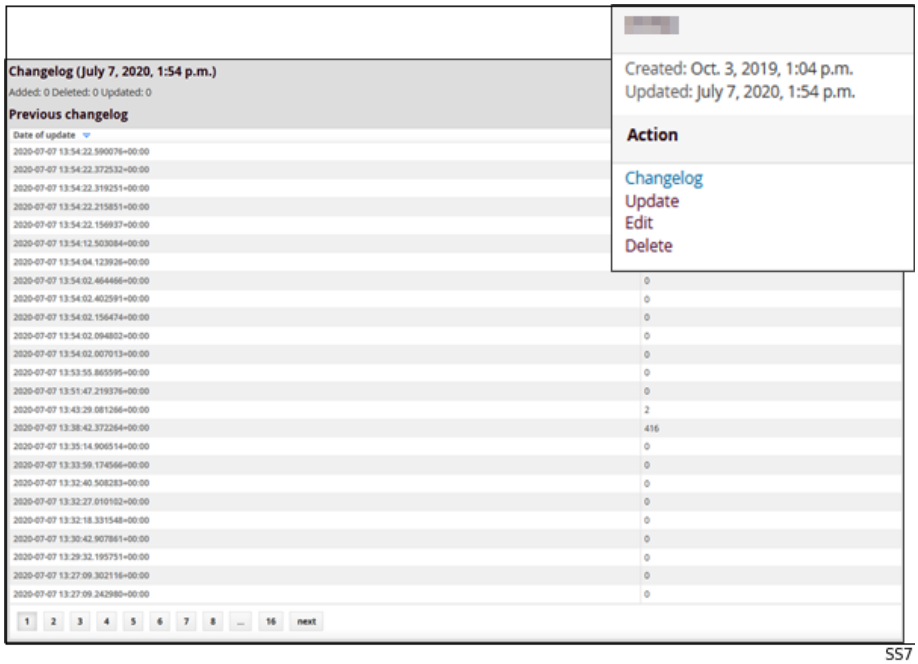
SS4

Ces sources se mettent à jour automatiquement dans le cas de source publique / HTTP si le **GCENTER** est connecté à internet, sinon, une mise à jour manuelle peut être faite au niveau de cette interface afin d'avoir les dernières signatures de disponibles.



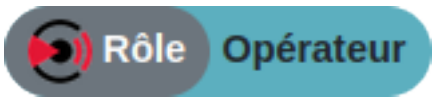
SS6

La mise à jour des signatures et la vérification de l'historique des changements sont possibles :



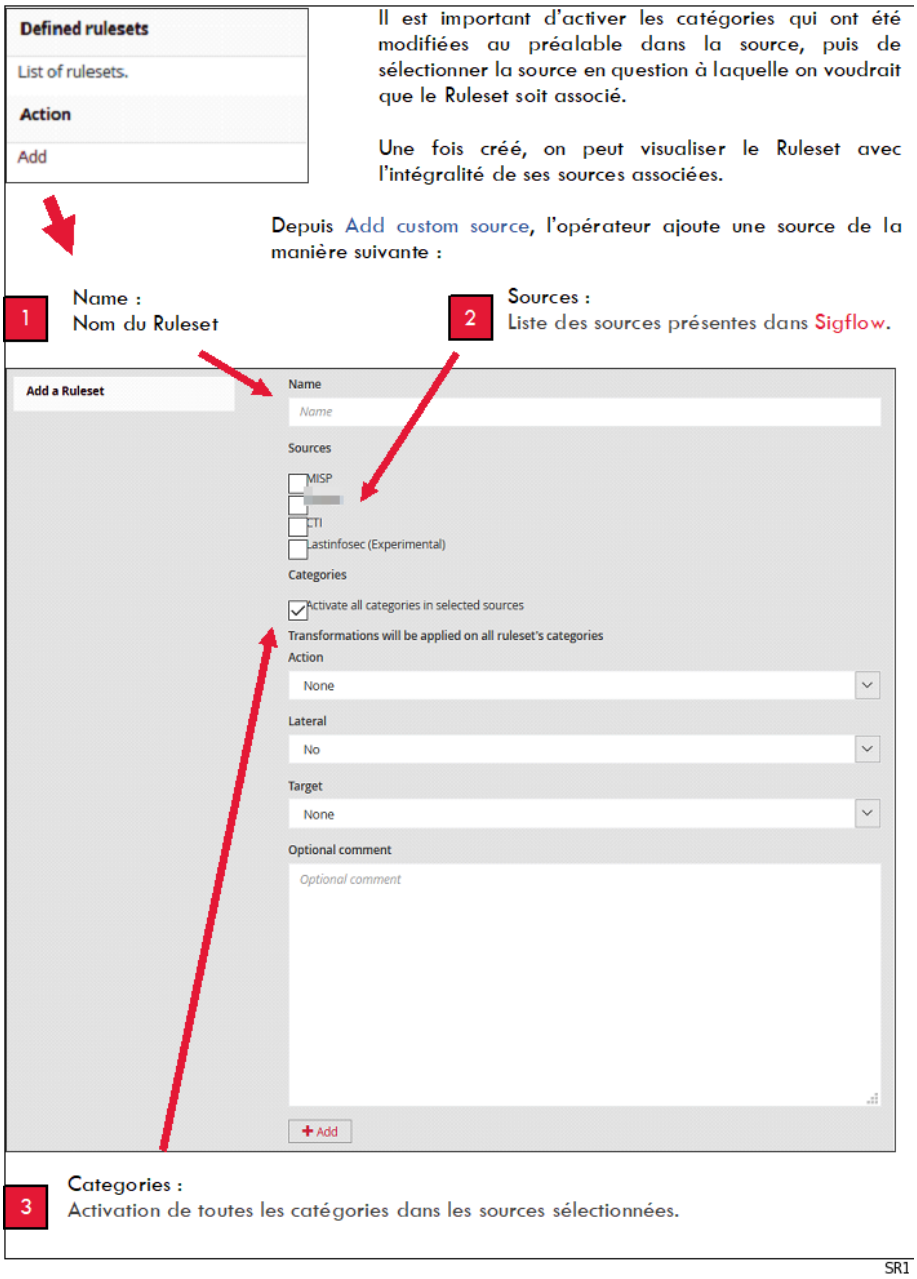
SS7

23.2 Rulesets



Menu : Operators > Sigflow > Rulesets

Dans un second temps il va falloir attribuer un 'Ruleset' associé à la source ajoutée précédemment. La création du Ruleset est obligatoire pour que la sonde **GCAP** puisse analyser le flux réseau et remonter des alertes si les signatures correspondent.



Des modifications peuvent être effectuées sur les règles afin d'adapter une règle publique à des spécificités de système d'information, ou à un besoin spécifique.

Les modifications suivantes seront appliquées à toutes les catégories du *Ruleset*

ACTION :

Détermine l'action à appliquer sur le Ruleset créé.

Filestore : Si une règle correspond et contient une signature, le paquet sera traité et stocké comme tout autre paquet.

Reject : S'il s'agit d'un rejet du paquet, Sigflow génère une alerte pour des paquets de réinitialisation (TCP) et des paquets d'erreurs ICMP.

Drop : Si trouve une règle qui correspond contenant la signature, il s'arrête immédiatement. Le paquet ne sera plus envoyé et une alerte sera générée.

Bypass : Si une règle correspond et contient un 'bypass', Sigflow arrête de scanner le paquet et passe à la fin de toutes les règles (uniquement pour le paquet actuel).

LATERAL :

Les signatures sont souvent écrites avec les variables $EXTERNAL_NET et $HOME_NET, ce qui signifie qu'elles ne correspondront pas si les deux côtés d'un flux se trouvent dans le $HOME_NET. Ainsi, les mouvements latéraux ne sont pas détectés. Cette transformation change $EXTERNAL_NET en n'importe quelle variable pour pouvoir détecter les mouvements latéraux.

L'option peut avoir trois valeurs :

Non : le remplacement n'est pas effectué

Oui : $EXTERNAL_NET est remplacé par n'importe quel IP (any)

Auto : la substitution est effectuée si la signature vérifie certaines propriétés

TARGET :

Le mot-clé 'target' peut être utilisé pour dire quel côté d'un flux déclenchant une signature est la cible. Si cette clé est présente, les événements connexes sont améliorés pour contenir la source et la cible de l'attaque.

L'option peut avoir quatre valeurs :

Auto : un algorithme est utilisé pour déterminer la cible s'il y en a une

Destination : la cible est l'IP de destination

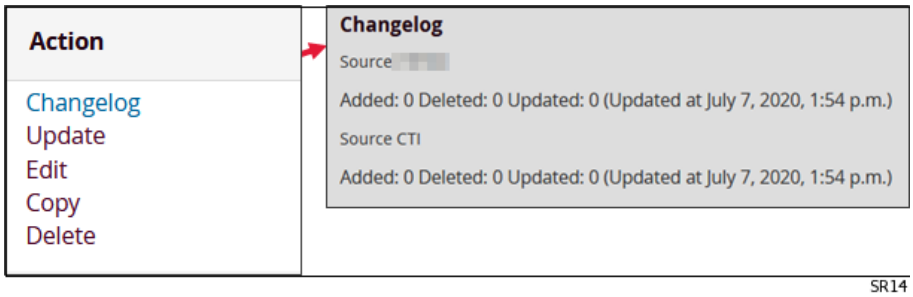
Source : la cible est la source IP

Aucune : aucune transformation n'est effectuée

'Add' pour valider l'ajout du ruleset.

23.2.1 Optimisation des rulesets

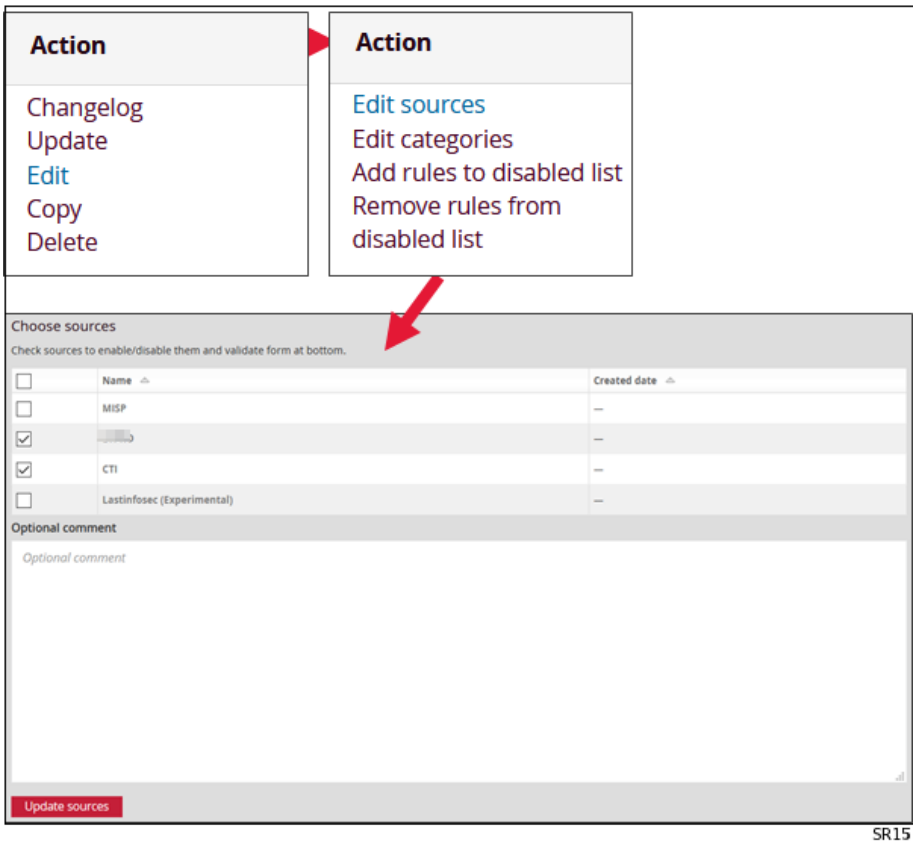
Comme pour les sources, le Ruleset peut se mettre à jour à n'importe quel moment. Il met de ce fait toutes ses signatures à jour tout en proposant un différentiel des changements opérés :



Un Ruleset peut être édité afin que l'opérateur puisse faire des modifications sur les sources, catégories ou règles présentes dans le Ruleset.

ACTION EDIT SOURCES :

Cette option sert à activer ou désactiver manuellement l'action d'une source sur un Ruleset.



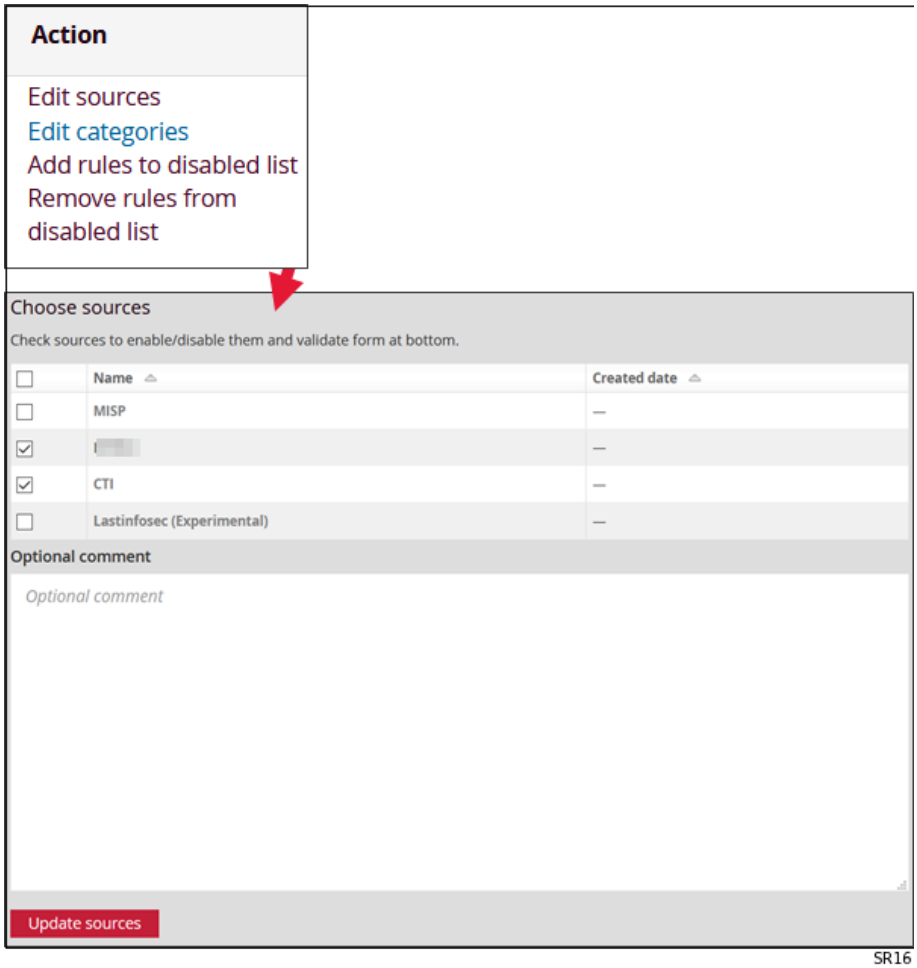
SR15

Une fois décochées, les signatures ne seront plus matchées par des flux en particulier et ne remonteront plus d'alerte sur l'interface.

ACTION EDIT CATEGORIES :

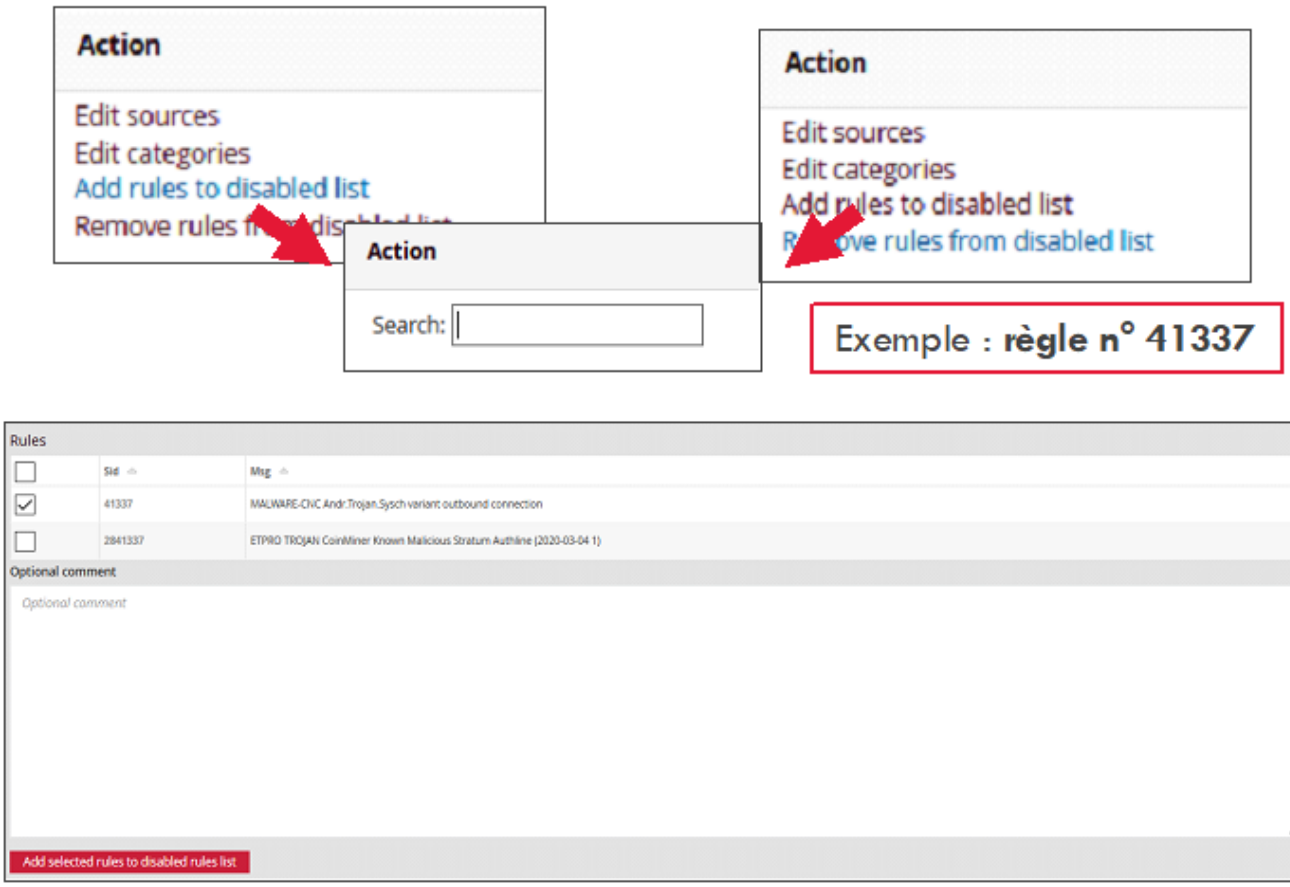
Cette option sert à activer ou désactiver manuellement l'action d'une catégorie sur un Ruleset.

Une fois décochées, les signatures ne seront plus matchées par des flux en particulier et ne remonteront plus d'alerte sur l'interface.



SR16

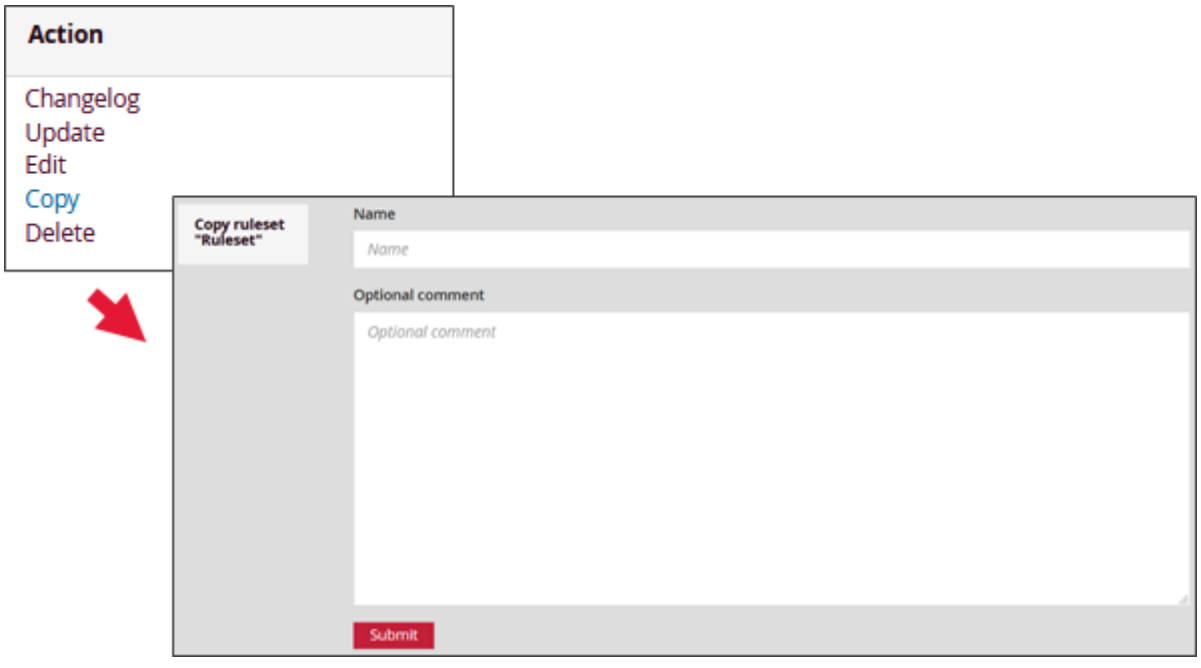
Il est possible de désactiver une signature associée à un Ruleset directement depuis l'interface SIGFLOW. La désactivation d'une règle ne provoque pas sa suppression définitive.



L'administrateur peut décider de faire un duplicata du Ruleset afin de l'attribuer à une autre sonde **GCAP** par exemple en fonction des flux réseau qui transitent. Le Ruleset est spécifique et doit être optimisé en fonction de la sonde à laquelle il sera attribué.

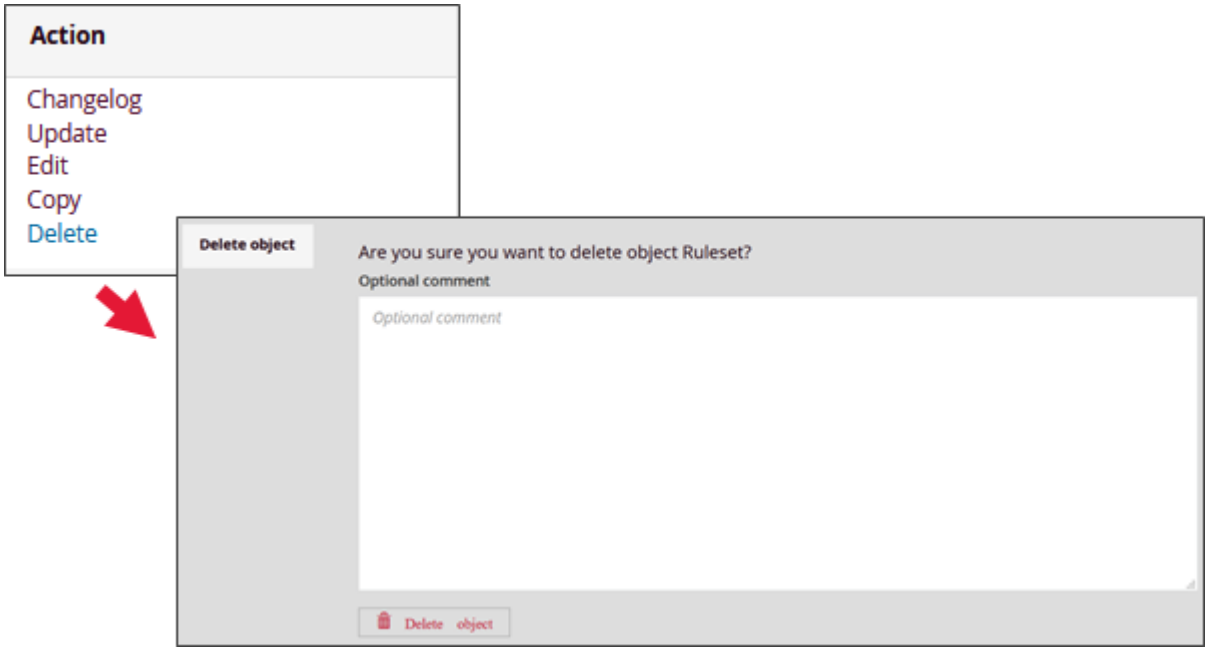
ACTION COPY RULESET :

Cette option sert à dupliquer le Ruleset, la copie prendra en compte les sources associées au Ruleset.

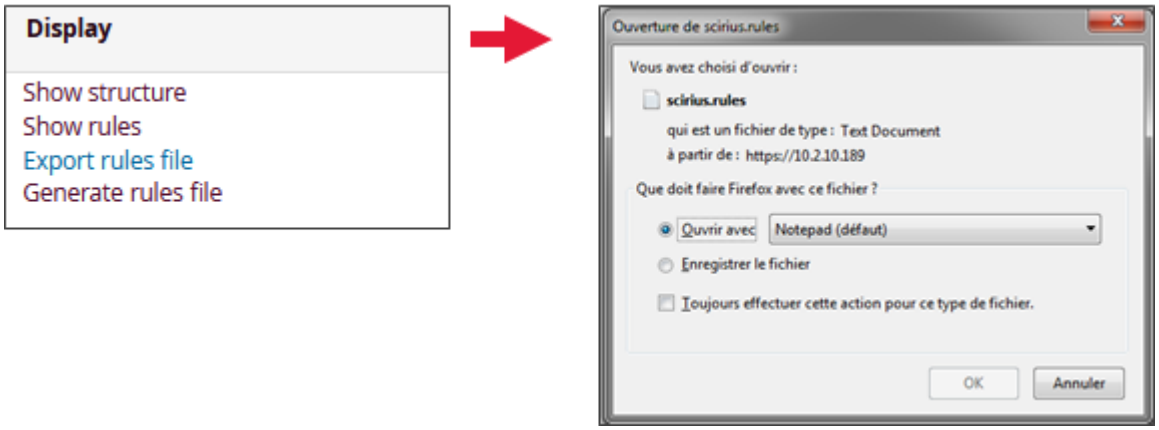


ACTION DELETE RULESET :

La suppression du Ruleset est irréversible mais ne provoquera pas la suppression des sources et signatures qui étaient liées au Ruleset.



D'autres options de visionnage sont disponibles avec l'interface SIGFLOW. La rubrique **DISPLAY** permet d'avoir la vision des catégories (via **Show structure**) et celle des règles (via **Show rules**). De plus grâce à cette rubrique, un export de toute la configuration SIGFLOW est possible en prenant en compte les Ruleset, les sources, les thresholds et les suppress créés.

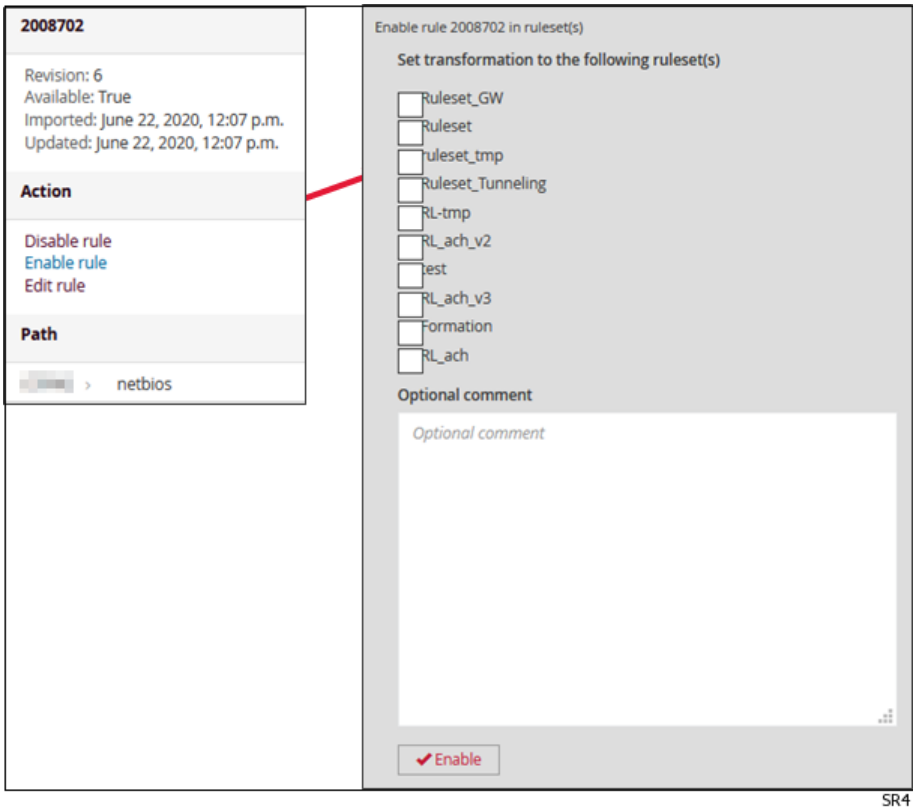


23.3 Modification de signatures

Les signatures (et leurs catégories) sont le point commun entre une *source* et un *rulesets*. Il est possible d'agir directement sur le fonctionnement d'une signature depuis l'interface du **GCenter**.

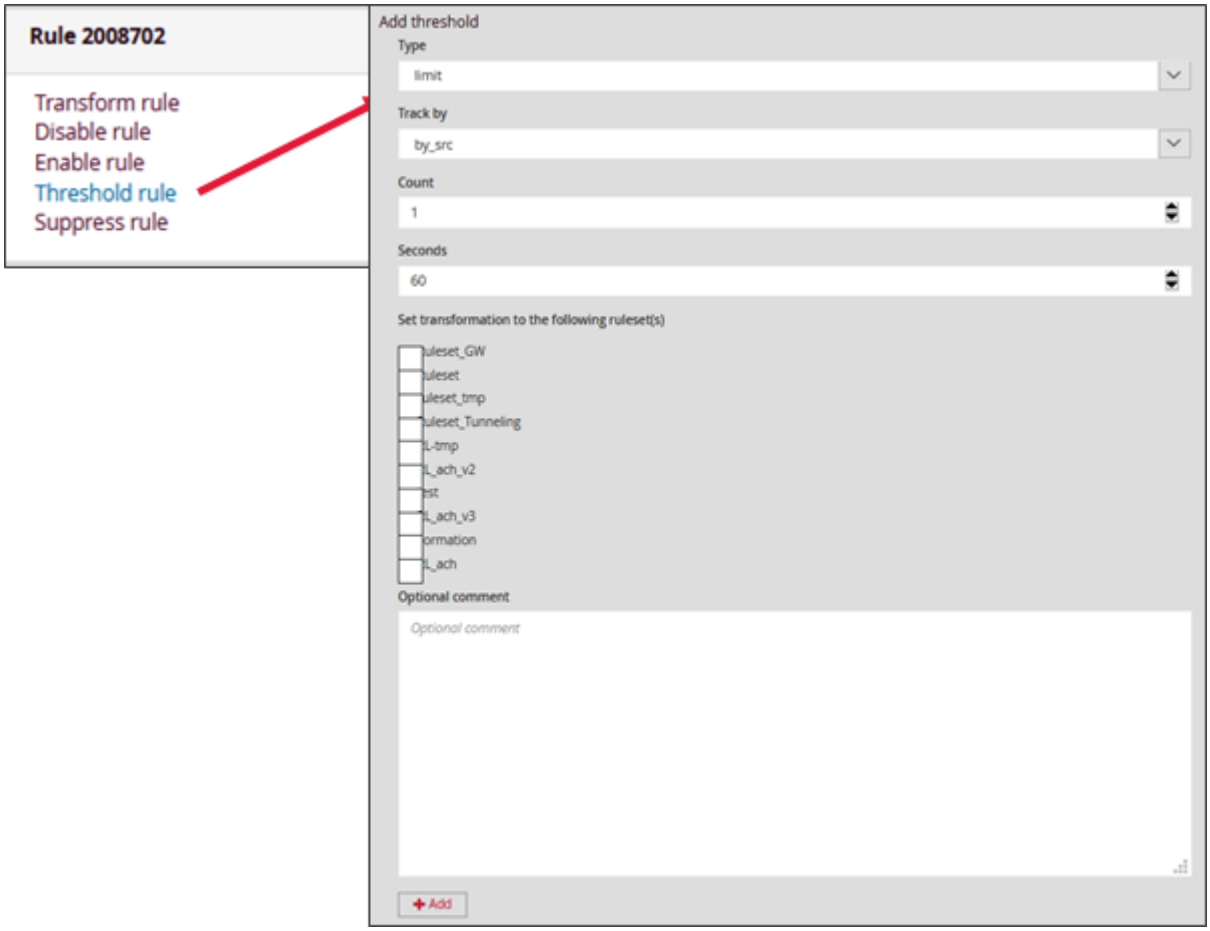
On peut accéder aux signatures et à leurs catégories depuis un *Ruleset* en cliquant sur le bouton *View* du *Ruleset* puis la catégorie.

Suivant les alertes qui arrivent au niveau de l'interface, il est possible d'être très précis sur le type ou même le nombre de notifications. La règle peut être activée ou désactivée au sein du Ruleset.



SR4

En cliquant sur le lien *"Edit Rule"* il est possible de générer des règles afin de limiter ou supprimer certaines alertes. Il y a les Suppress Rules, qui suppriment une alerte en fonction d'une IP source ou de destination, ou alors une Threshold Rules qui limite le nombre d'alertes à afficher.



THRESHOLD :

Cette option sert à programmer une limitation des alertes au-delà d'un seuil paramétré.

Pour un threshold, il y a 3 types de règles :

Threshold : Ce type peut être utilisé pour définir un seuil minimum pour une règle avant de générer des alertes. Un réglage de seuil de N signifie qu'à la nième fois que la règle correspond, une alerte est générée.

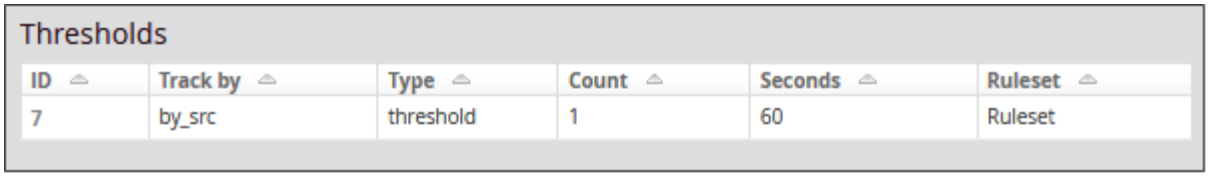
Limit : Ce type peut être utilisé pour s'assurer que vous ne soyez pas inondé d'alertes. S'il est défini sur N, il alertera au maximum N fois.

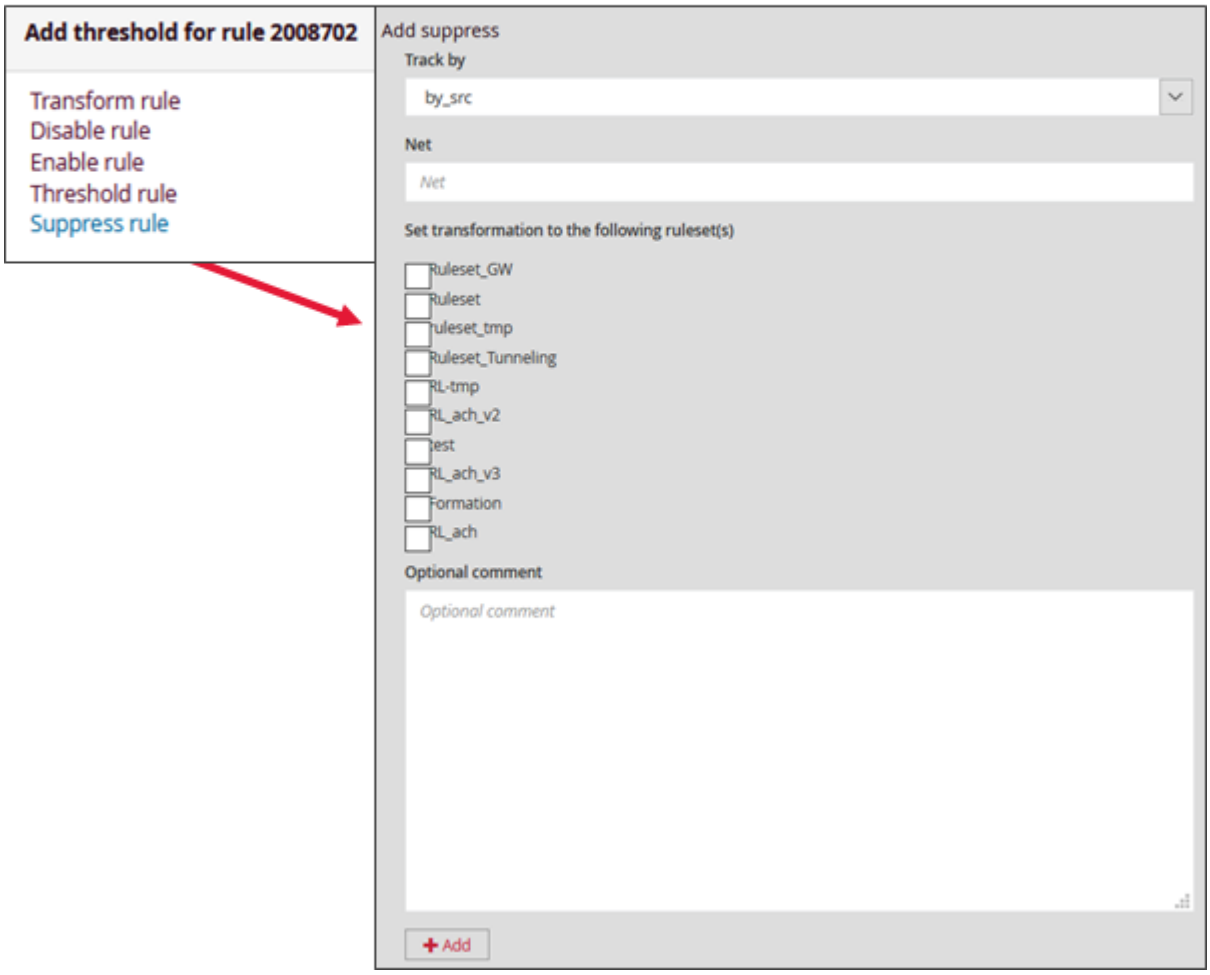
Both : Ce type est une combinaison des types "threshold" et "limit". Il applique à la fois le seuillage et la limitation. Cette alerte ne générera N alerte que si, dans les X minutes.

Il est nécessaire ensuite de :

- Définir si l'alerte se fera en se basant via l'IP source ou de destination
- Préciser le nombre d'alertes maximums générées pour la période donnée
- Définir la période en seconde définie pour générer l'alerte

Les règles créées se retrouvent disponibles dans la page du Ruleset avec le format de la nouvelle règle.





SUPPRESS :

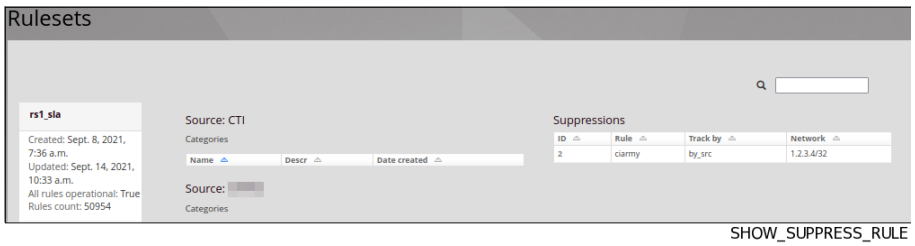
Cette option sert à supprimer une alerte par rapport à une adresse IP ou un réseau donné.

Plusieurs IP peuvent être ajoutées en étant séparées par des ' ,'

Après avoir sélectionné Suppress Rules :

- Choisir le Ruleset qui sera affecté
- Choisir si la suppression de l'alerte se fera en fonction de la source ou de la destination.
- Définir l'IP concernée par cette règle. (au format CIDR)

La règle est disponible dans la page du Ruleset en question :

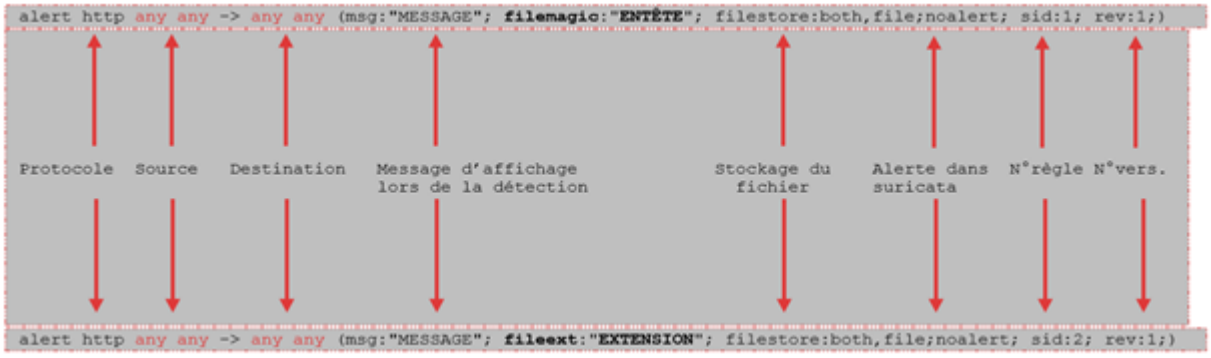


SHOW_SUPPRESS_RULE

En cliquant sur l'*ID* de la *suppress rule* il est possible de l'éditer ou de la supprimer.

23.3.1 Définition des signatures

Toutes les signatures présentes dans les sources ont des références menant à des blogs, CVE, sites internet... accessibles depuis l'interface. Pour comprendre un peu mieux comment fonctionne une signature, voici un exemple d'une règle :



Dans la plupart des cas, une règle, une signature est composée : d'une action, de l'entête et des options de règle. Par exemple :

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

Les protocoles suivants peuvent faire l'objet d'une règle :

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

Dans la signature, vous pouvez attribuer des adresses IP, de type IPv4 et IPv6 combinés ainsi que séparés. Les sources et les destinations de la signature sont impactées.

De plus, il est possible de définir des variables telles que $HOME_NET ou $EXTERNAL_NET auxquelles *des IP seront à définir*. Ces variables sont utilisées pour augmenter la précision des alertes que remontent les signatures.

La syntaxe suivante peut être utilisée pour spécifier les adresses :

! 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

De la même manière, la syntaxe suivante peut être utilisée pour spécifier les 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

Deux directions peuvent être définies pour indiquer le sens du flux :

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

23.4 Génération des rulesets

```
important:: Tant que les rulesets n'ont pas été générés après modifications, aucune
↪configuration ne sera déployée.
```

Une fois la configuration des sources, rulesets et modifications éventuelles réalisées il est nécessaire de générer la configuration pour les sondes et de la déployer. Cette action se fait grâce à l'action « **Generate Ruleset** » qui figera l'état du Ruleset et prendra en compte toutes les modifications.

23.5 Règle secrète locale

Il est également possible de définir certaines règles localement sur une sonde GCAP qui n'apparaitront volontairement pas dans l'interface **GCENTER**.

Cela peut se présenter dans les cas suivants :

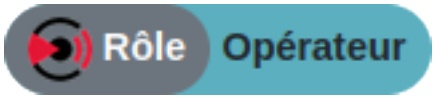
- Rendre des signatures confidentielles sans que les opérateurs du GCENTER puissent les voir (notion de 'besoin d'en connaitre')
- Faire une modification des signatures locales des sondes dans des cas complexes
- Lorsque le GCENTER est confié à un tiers et que ce dernier ne peut manier des marqueurs ou des signatures d'un certain niveau

Cette procédure est détaillée dans la documentation **GCAP** à la section "*Moteur de détection > 7. Ajouter des règles secrètes localement*".

Chapter 24

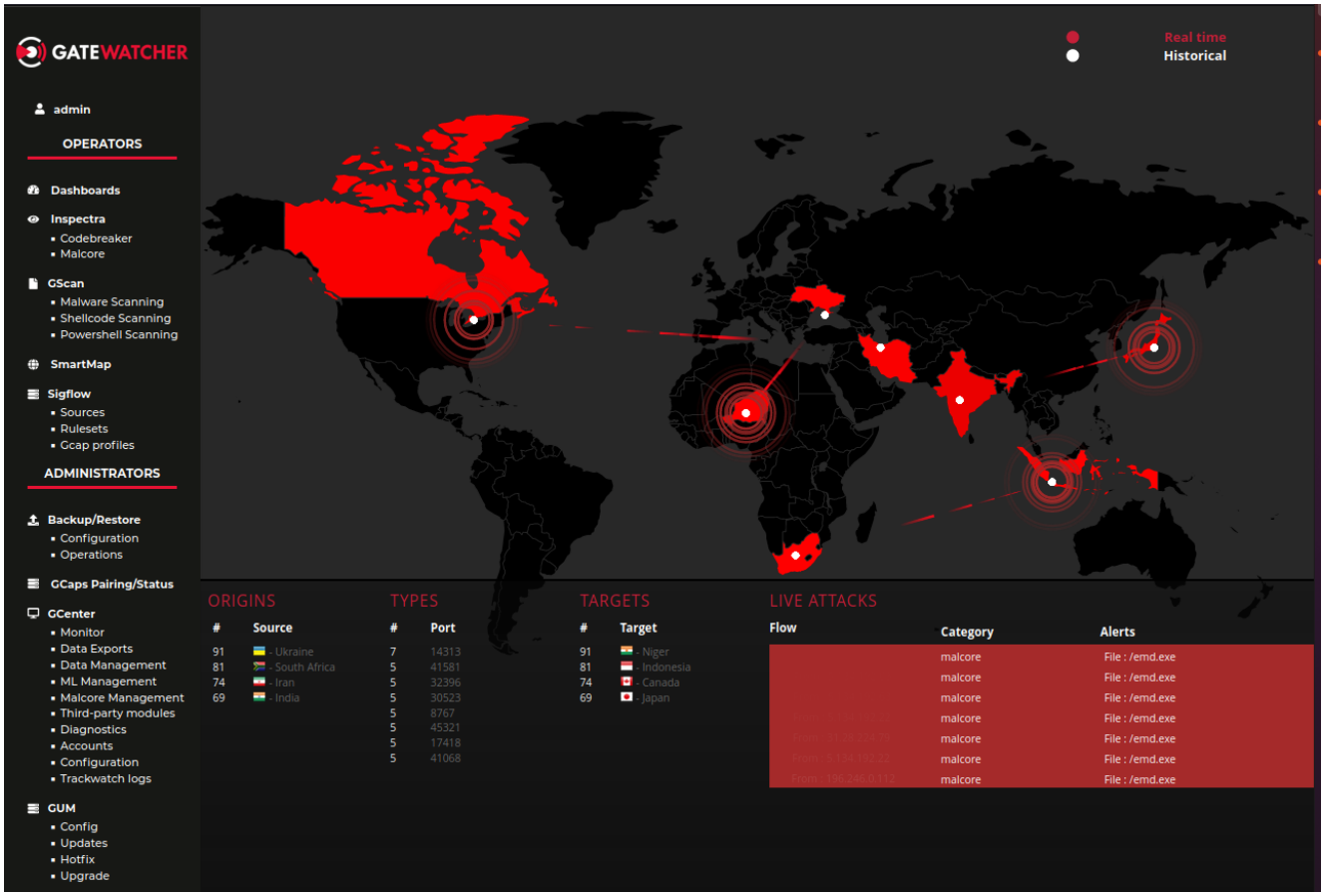
Détection

24.1 SmartMap



Menu : Operators > SmartMap

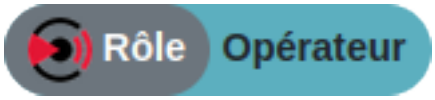
La **SmartMap** permet de visualiser en temps réel les attaques et le trafic. Cela permet de manière intuitive et visuelle de détecter le trafic inhabituel ou particulièrement soutenu.



Afin de pouvoir afficher les informations sur la carte, la **SmartMap** nécessite d'avoir les informations de géolocalisation sur les alertes. Ces dernières devront donc être activées depuis *la section configuration* par un

administrateur.

24.2 Dashboard Kibana



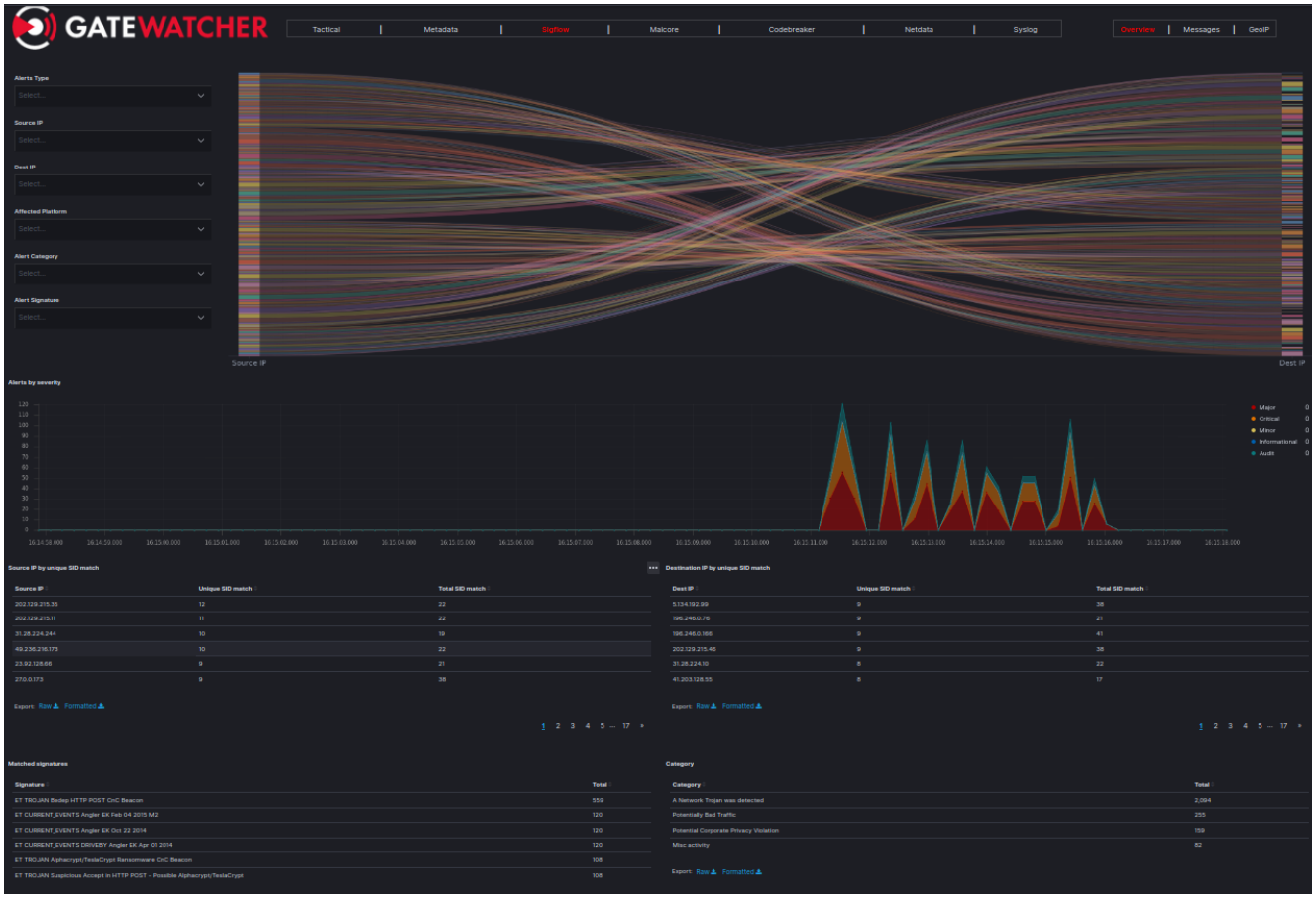
Menu : Operators > Dashboards

Toutes les informations analysées par le module Sigflow sont stockées afin de permettre aux opérateurs d'effectuer une analyse de la manière la plus efficace possible.

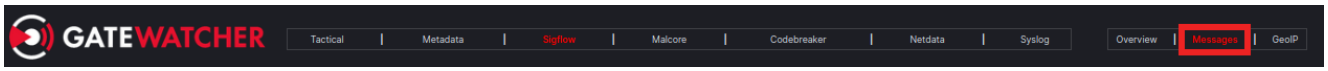
Ainsi différents tableaux de bord (ou *dashboards*) sont mis à disposition par défaut.

Les informations du module **Sigflow** se retrouvent dans le *dashboard* **Tactical**, qui offre une vision globale des menaces, dont celles levées par **Sigflow**

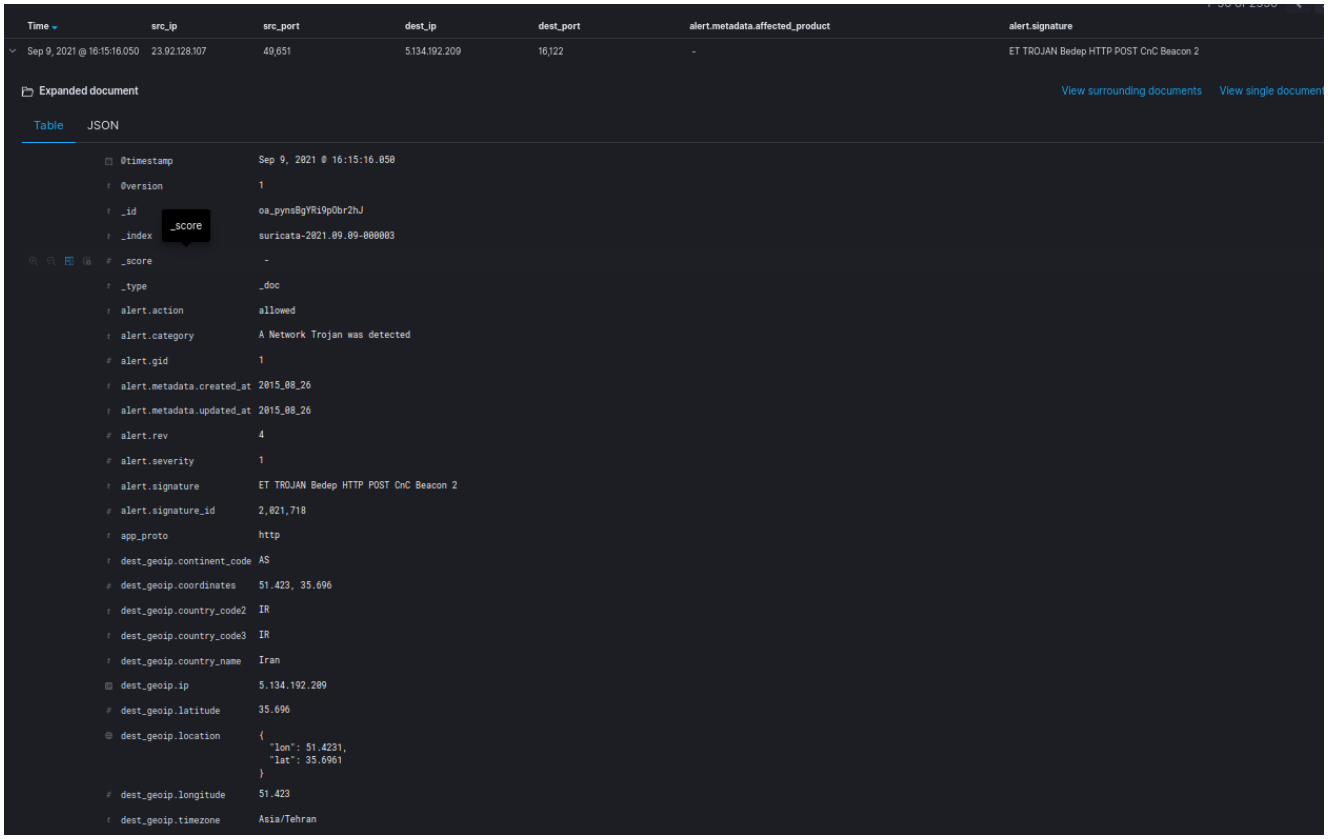
Des données plus spécifiques à ce module peuvent également être trouvées dans le *dashboard* **Sigflow**.



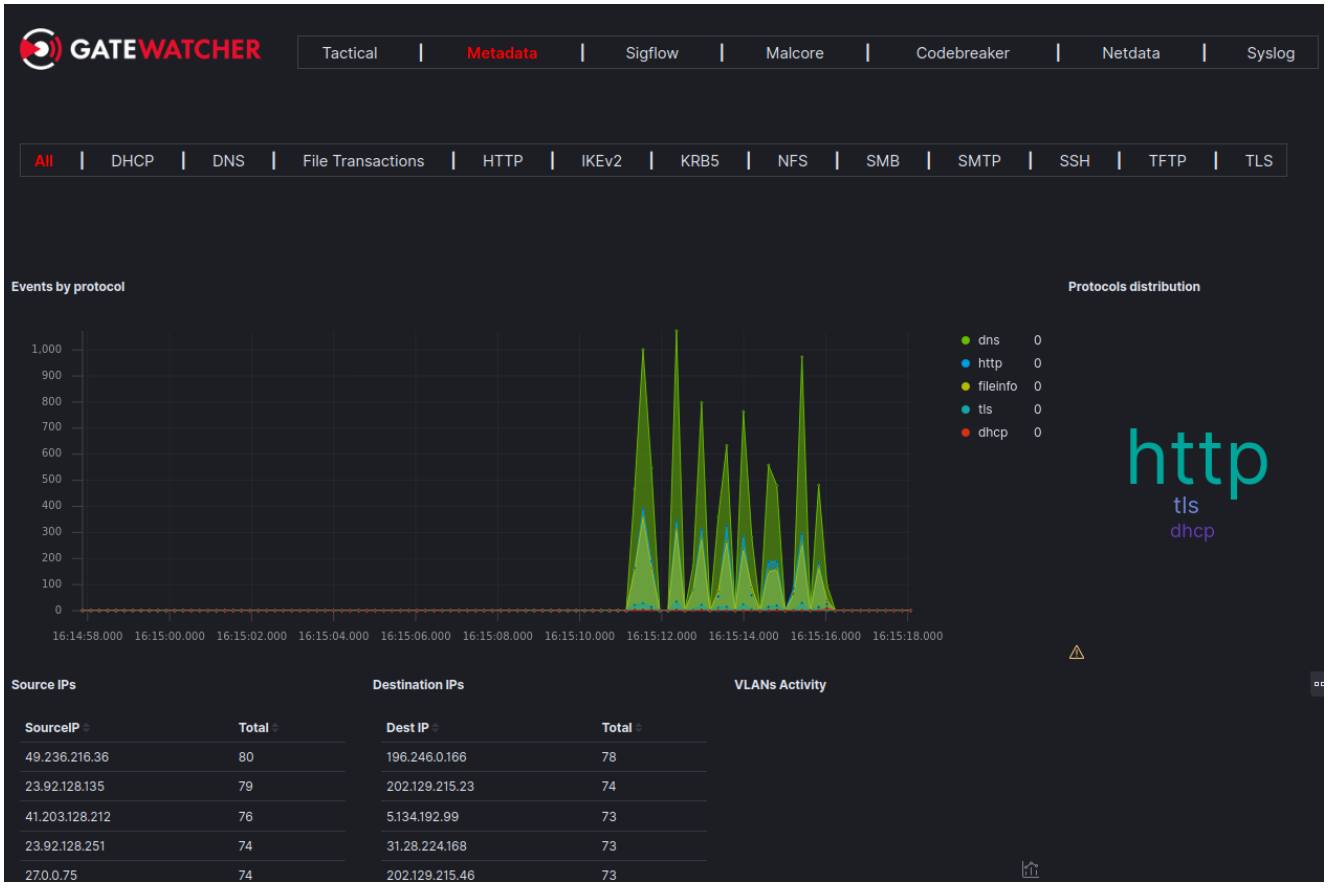
Comme toujours, il possible d'avoir le détail complet des alertes en basculant sur la vue **Messages**



Les champs présents sont ceux détaillés ci-après dans la section *Évènements générés*



Enfin, ce module enrichit également le trafic observé avec les meta-données qui ont pu être analysées (suivant la configuration effectuée sur le *profil du* ***GCAP***)



Chapter 25

Évènements générés

Pour suricata, et donc Sigflow, les champs produits dépendent du flux observé.

25.1 Document de type "alert"

Liste des champs présents dans toutes les alertes avec 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

Liste des protocoles compatibles avec le parsing (champ app_proto):

- dcerpc
- dhcp

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

Si un protocole change en cours de route (par exemple si SMTP est upgradé en TLS via STARTTLS) ou si les protocoles utilisés ne sont pas les mêmes dans les deux sens du flux, les champs suivants peuvent apparaître :

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

Tableau récapitulatif des champs qui ne dépendent pas des protocoles:

Liste des métadonnées utilisées dans les alertes des sources (objet alert.metadata dans 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

Voici un exemple d'alerte qui utilise les métadonnées affected_product, attack_target, created_at, deployment, signature_severity, tag et 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 de type "fileinfo"

Liste des champs présents dans toutes les alertes avec 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

Tableau récapitulatif des champs qui ne dépendent pas des protocoles:

25.3 Document de méta-données

Liste des champs présents dans toutes les alertes avec 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

Liste des protocoles compatibles avec le 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

Tableau récapitulatif des champs qui ne dépendent pas des protocoles:

Chapter 26

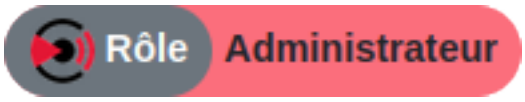
Présentation de l'algorithme DGA

Le **Gcenter** embarque un moteur capable de détecter des noms de domaines ayant été générés par des DGA (*Domain Generation Algorithm*). La présence de noms de domaines créés par DGA sur un réseau est un fort indicateur de compromission.

En effet, les logiciels malveillants peuvent utiliser des requêtes HTTP vers des noms de domaine générés automatiquement, afin de contacteur leurs serveurs de commande et de contrôle (aussi appelés CnC, C&C ou C2). Ces noms de domaine ont des propriétés différentes des noms de domaines légitimes. Les approches classiques de détection comme les listes noires ne sont pas pertinentes dans le cas de domaines renouvelés en permanence. Les simples calculs d'entropie génèrent une grande quantité de faux positifs.

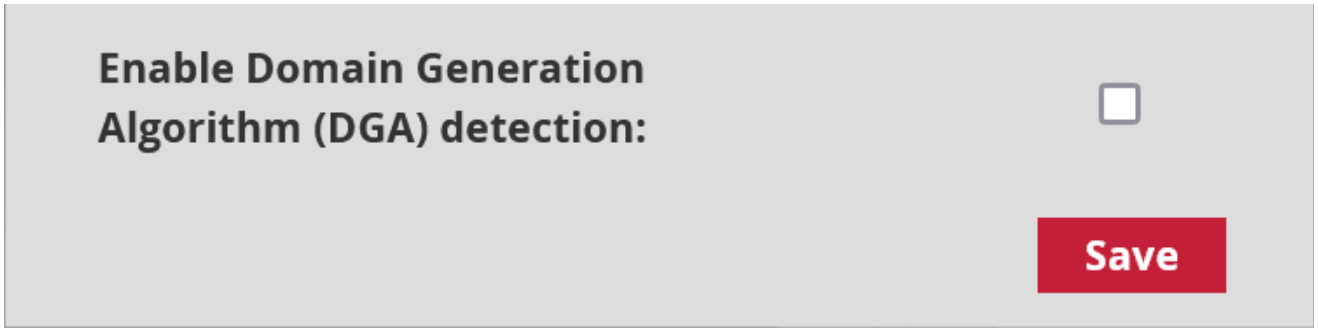
Chapter 27

Activation



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

Cette fonctionnalité est désactivée par défaut. Elle est activable au niveau du dashboard Machine learning.

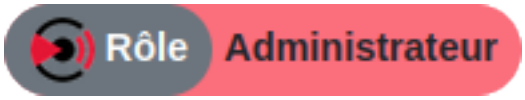


Une fois activée, les noms de domaine présents dans les évènements 'dns' capturés par les sondes GCAP sont analysés par le moteur de machine learning. Celui-ci renvoie une probabilité, pour chaque évènement de ce type, que le nom de domaine ait été généré par un DGA. Le moteur utilise un modèle pré-entraîné, dont l'architecture est basée sur un réseau de neurones profond de type LSTM (Long Short Term Memory networks).

Le moteur utilise seulement les noms de domaine : aucune information contextuelle supplémentaire telle que NXDomains par exemple n'est utilisée.

Chapter 28

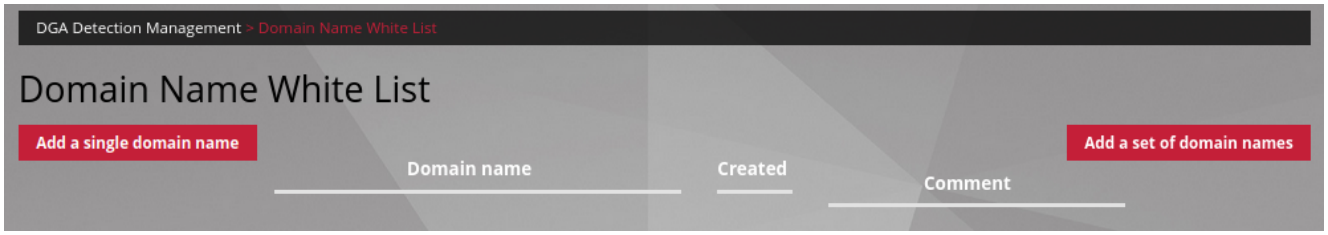
Listes d'exceptions



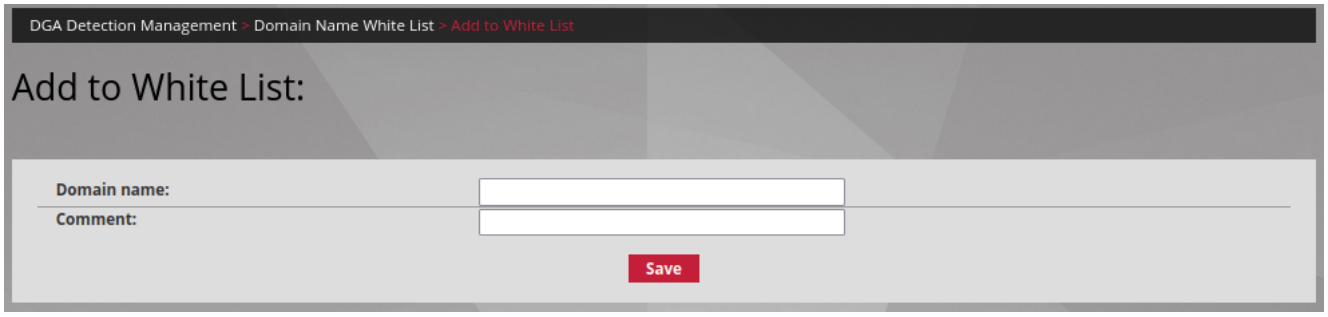
Menu : Administrators > GCENTER > ML Management > DGA Detection Management > White List / Black List

Des listes d'exceptions peuvent être mises en place afin de forcer le moteur à déclarer des noms de domaine comme sains (White List). Cela permet de supprimer les alertes liées à des faux positifs récurrents.

À l'inverse, une liste noire permet de lever une alerte pour un domaine qui n'aurait pas été détecté sinon (faux négatif).

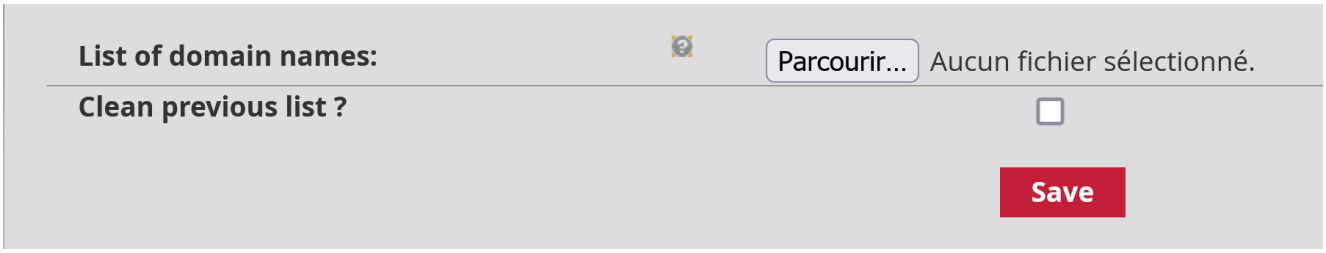


Depuis **Add a single domain name**, il est possible d'ajouter un domaine dans la liste blanche de MachineLearning via le champ **Domain name**. Un commentaire peut suivre le domaine ajouté pour davantage de détails dans le champ **Comment**.



La sauvegarde des modifications se fait en cliquant sur le bouton **Save**.

Depuis **Add a set of domain names**, l'administrateur met à jour la liste blanche de MachineLearning via le champ **List of domain names** en sélectionnant sur son poste un fichier **CSV** contenant les domaines. Il faudra utiliser des ';' pour séparer les éléments de la liste.

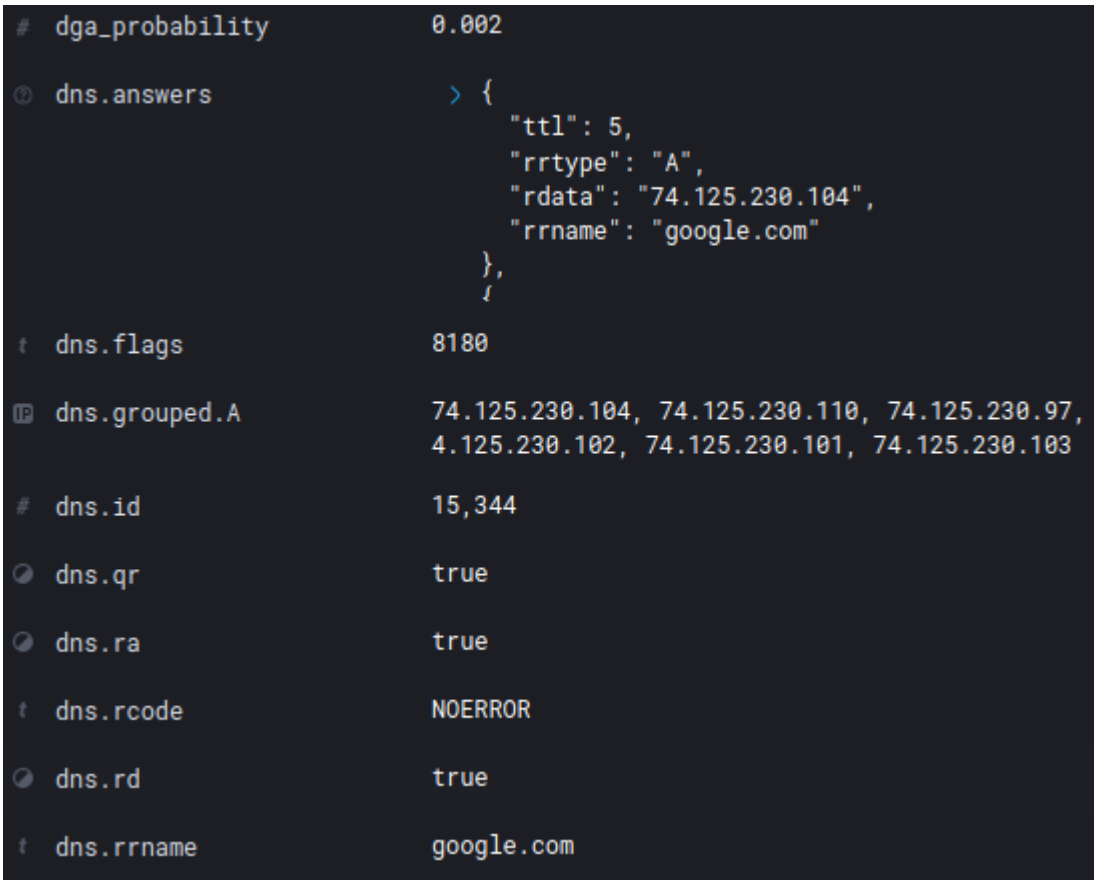


De plus, l'administrateur peut décider de supprimer la liste précédente en cochant la case **Clean previous list?** et sauvegarder toutes les modifications en cliquant sur **Save**.

Chapter 29

Événements générés

Le moteur de machine learning enrichit les informations déjà fournies par le module **Sigflow**. Ainsi pour un domaine n'étant pas détecté comme un domaine généré le champ `dga_probability` sera ajouté. Une valeur proche de `0` indique une faible probabilité que le domaine ait été généré comme dans l'exemple suivant

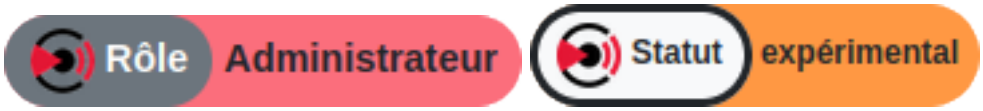


A contrario, une valeur proche de `1` indique qu'il y a de fortes chances que ce domaine soit le résultat d'une génération aléatoire comme ici

#	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)



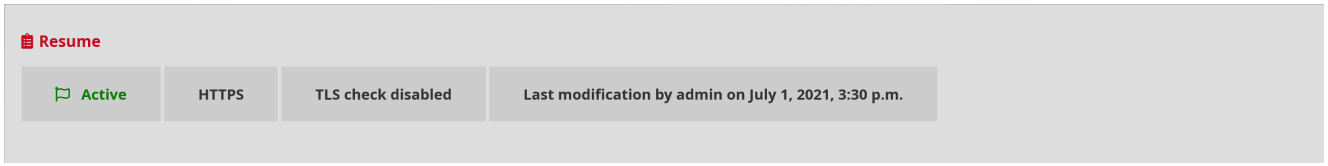
Menu : Administrators > GCenter > Third-Party Modules > MISP

Cette interface est utilisée pour gérer la connexion entre le **GCENTER** et un serveur MISP (Malware Information Sharing Platform) déjà présent dans votre infrastructure.

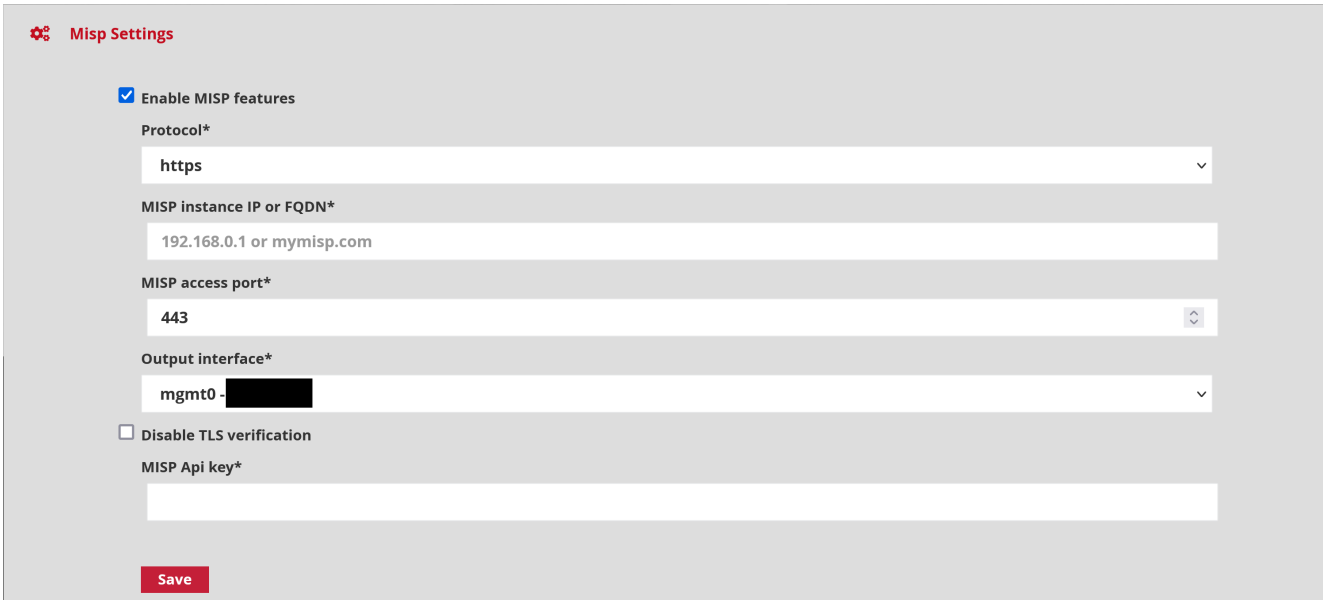
La connexion d'un serveur MISP avec la solution TRACKWATCH permet d'apporter des informations techniques liées aux menaces ainsi qu'un référentiel de logiciels malveillants, d'IOC (Indicateurs de Compromis) et d'informations.

Depuis la partie **MISP Suricata rules** , l'administrateur peut voir la dernière modification de la configuration de l'instance MISP et apporter des changements en cliquant sur **Access**.

L'administrateur peut vérifier l'état de connexion entre l'instance MISP et le **GCENTER** via **Resume**.



Une fois dans **Access** , la première étape est de renseigner l'adresse IP ou le domaine de votre instance MISP dans la WebUI du **GCENTER**.



Protocol : le protocole de communication à utiliser pour contacter l'instance *MISP*. Deux options sont possibles : 'HTTPS' et 'HTTP'. **MISP instance IP or FQDN** : le nom de domaine ou l'adresse IP de l'instance MISP. **MISP access port** : le port d'écoute de l'instance MISP **Output interface** est l'interface physique du **GCENTER** par laquelle il communiquera avec le serveur MISP. **MISP API key** l'administrateur renseigne la clé API de l'instance MISP.

Une fois la section remplie il suffit de cliquer sur 'Save' pour sauvegarder les informations.

Le connecteur MISP permet d'apporter des IOC directement depuis un MISP local vers les sondes GATEWATCHER. Ce connecteur permet de rajouter une source de threat intelligence de qualité tout en respectant les consignes de l'ANSSI sur la qualification des signatures.

Maintenant que le service est activé, on peut remarquer que le statut au niveau de **MISP interconnection status** a été modifié, le lien entre le **GCENTER** et l'instance MISP est opérationnel.

Chapter 31

Hurukai (by HarfangLab)

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

HarfangLab propose une solution d'EDiR (Endpoint Detection Investigation and Remediation) ou d'EDR se nommant Hurukai. Cette solution permet d'investiguer sur les cyberattaques sans ralentir le fonctionnement de l'entreprise. Hurukai va permettre la collecte en temps réel d'informations sur les terminaux grâce à des agents qui seront déployés par le serveur de management de la solution. Les agents sont compatibles avec les plateformes Windows 7, 8, 8.1, 10 et Windows server 2008, 2012 et 2016.

Le but de cette partie est d'associer le **GCENTER** à l'EDiR Hurukai via la section « Third Party modules » dans l'administration du **GCENTER**. Puis il suffit de se déplacer dans l'onglet « Hurukai » pour accéder à la fonctionnalité.

Pour interconnecter les deux équipements, il suffit de renseigner l'adresse IP ou l'URL ainsi que le port de communication associé d'Hurukai dans les champs adéquats :

Protocol le protocole de communication à utiliser pour contacter l'instance *MISP*. Deux options sont possibles : 'HTTPS' et 'HTTP'. **Hurukai IP or FQDN** : le nom de domaine ou l'adresse IP de l'instance Hurukai **Hurukai port binding** : le port d'écoute du serveur Hurukai **Output interface** : l'interface physique du **GCENTER** par laquelle il communiquera avec le serveur Hurukai. **Hurukai API key** : la clé API du serveur Hurukai.

Une fois la section remplie il suffit de cliquer sur 'Save' pour sauvegarder les informations.

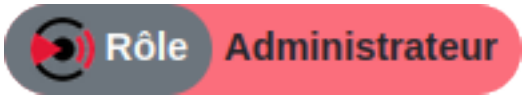
Le moteur de recherche de l'EDiR identifie instantanément les anomalies et génère des alertes grâce à des fonctions de levée de doute. Les marqueurs d'attaques connues, les outils des attaquants, les bootkits, la présence de code non signé ou de code injecté seront identifiés.

Le service est maintenant activé et fonctionnel.

Chapter 32

Intelligence

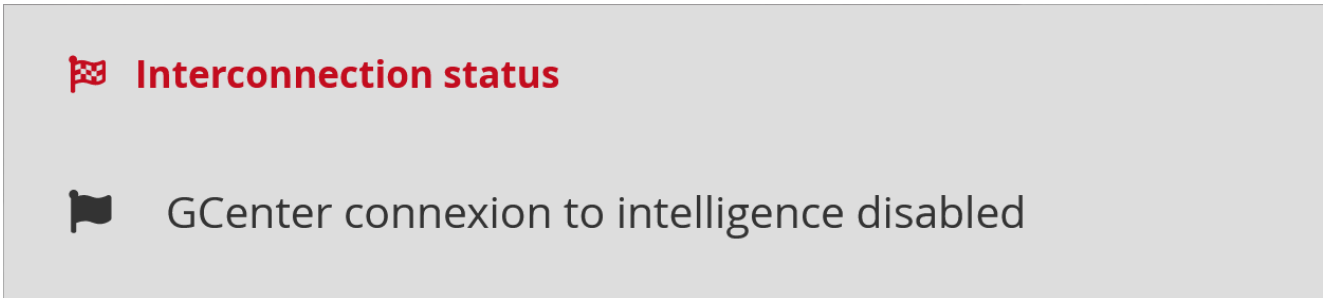
32.1 Externe



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

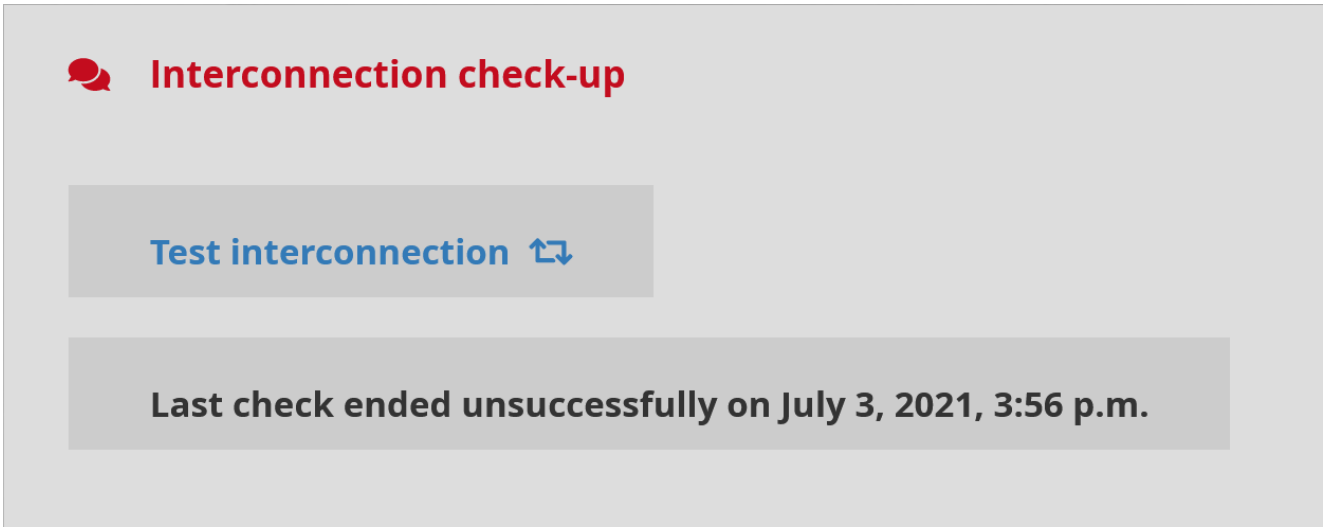
Pour avoir un rapport d'analyse détaillé du fichier détecté sur le **GCENTER** , il est nécessaire d'établir une connexion entre celui-ci et la plateforme connectée Intelligence. Suite à cette connexion, l'opérateur sera capable d'envoyer des fichiers à la plateforme Intelligence directement depuis l'interface.

L'état du statut de connexion entre le **GCENTER** et la plateforme Intelligence est donné avec la vue **Interconnection status** ci-dessous :

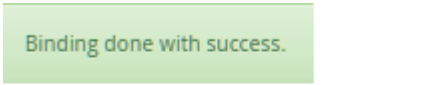


À noter que le lien entre les deux équipements de la solution GATEWATCHER est optionnel mais conseillé pour une utilisation optimale du produit une fois un malware détecté.

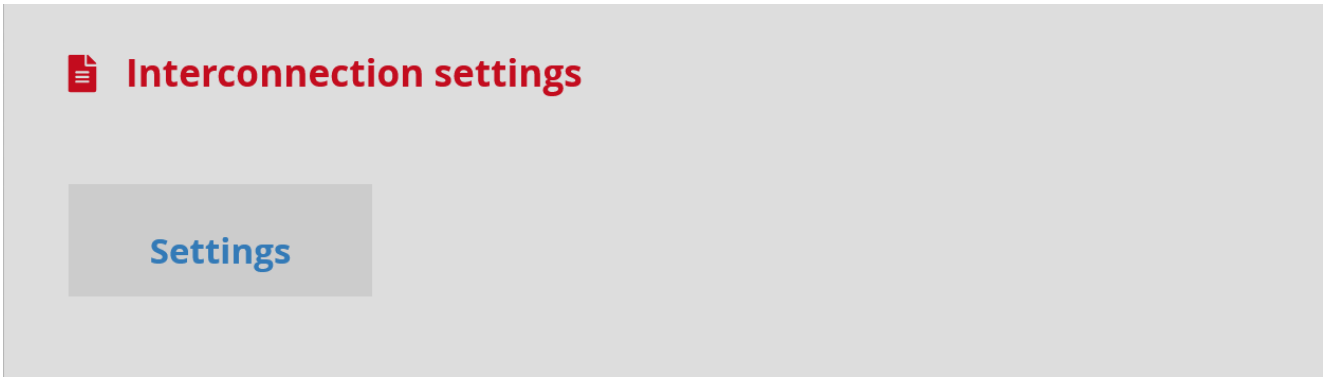
L'interconnexion peut être vérifiée en un seul clic par l'administrateur depuis la section **Interconnection check-up** en appuyant sur le bouton **Test interconnexion**.



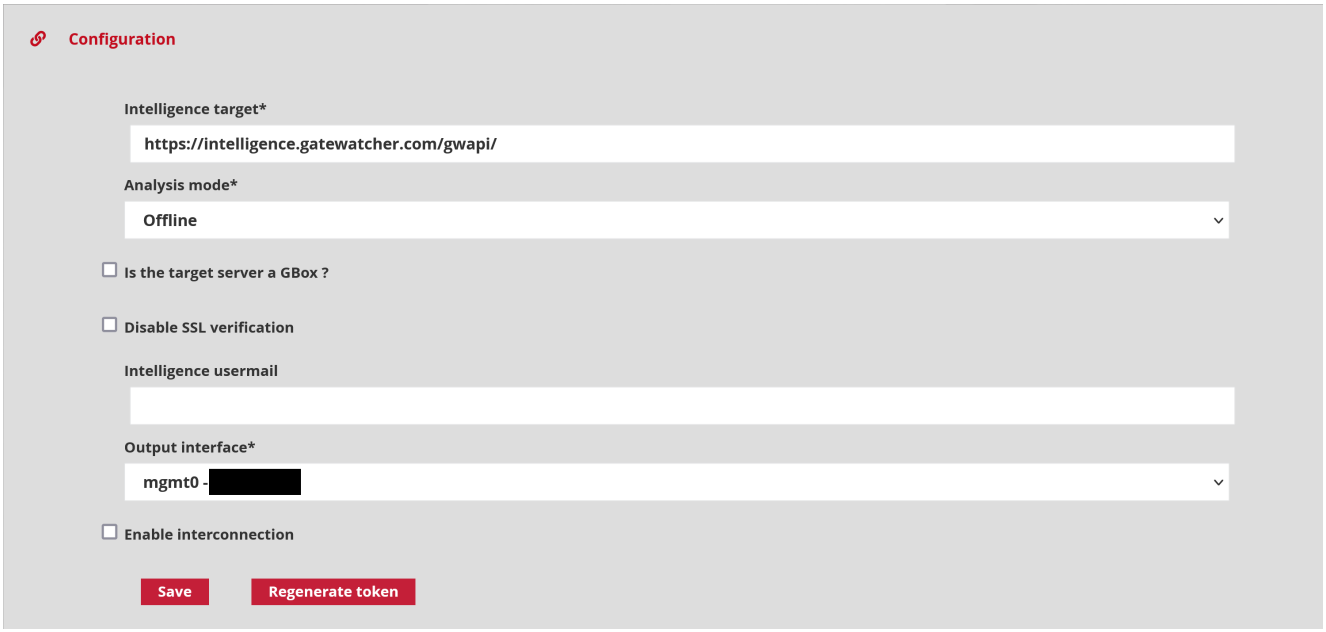
Le résultat de ce test d'interconnexion sera affiché de la manière suivante :



Quelques informations sont nécessaires pour que le **GCENTER** puisse être connecté à la plateforme.



Certains champs sont à renseigner par l'administrateur depuis la section **Interconnection settings** en appuyant sur le bouton **Settings**.



Intelligence target : il s'agit de l'adresse du serveur *Intelligence* de Gatewatcher (https://intelligence.GATEWATCHER.com/gwapi/_).

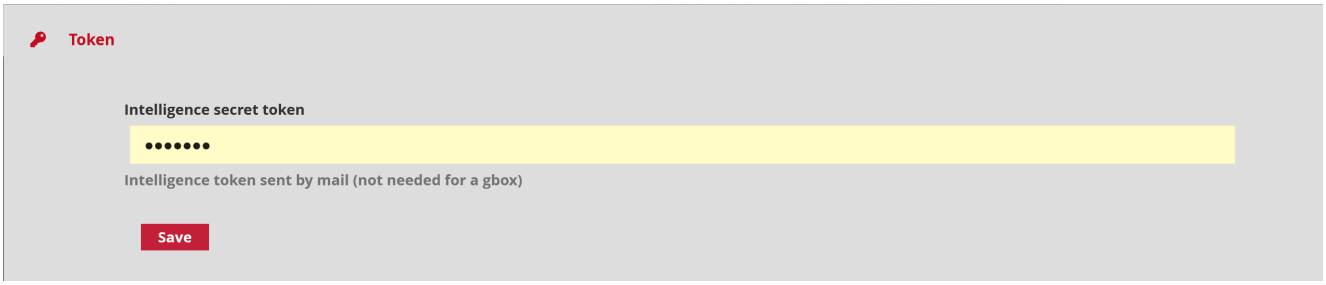
Les cases **Is the target server a GBOX ?** et **Disable SSL verification** ne sont à cocher qu'*en cas d'utilisation d'une **GBOX***. Une fois l'adresse renseignée, l'administrateur doit sauvegarder l'information en cliquant sur *Save*.

Analysis mode : correspond au mode d'analyse du fichier envoyé au serveur Intelligence : Online ou Offline.

Intelligence usermail : adresse e-mail du compte intelligence à laquelle un mail sera envoyé. Celui-ci contiendra un jeton permettant de connecter un **GCENTER** à https://intelligence.GATEWATCHER.com/packages/list/.

Output interface est l'interface du **GCENTER** par laquelle il communiquera avec le serveur Intelligence.

Une fois le mail contenant le token de connexion reçu, il sera nécessaire de renseigner le champ **Intelligence secret token** :



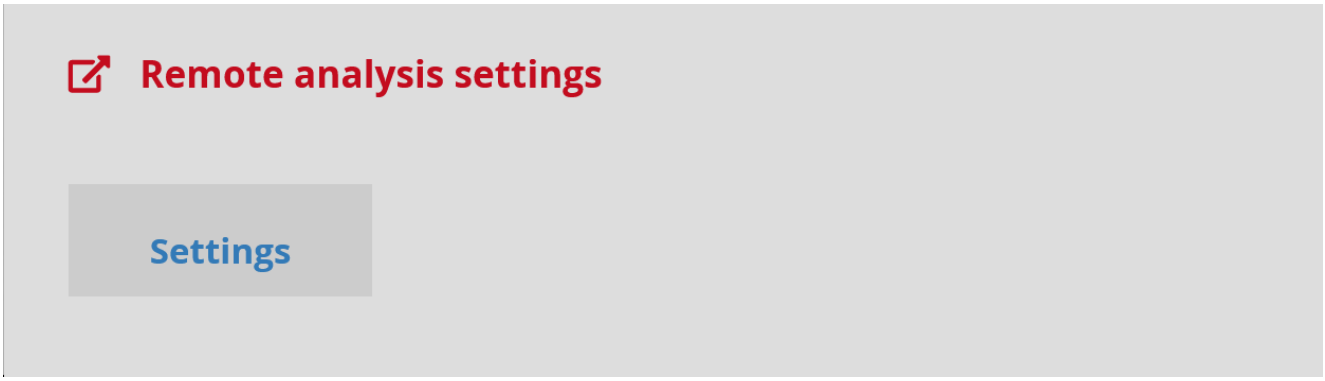
Ce token est unique par compte utilisateur mais peut-être utilisée sur plusieurs **GCENTER**. L'activation d'un nouveau token s'ajoutera à la liste des autres tokens liés à l'adresse mail.

La dernière étape pour l'activation du service consiste à cocher la case 'Enable interconnection'. Puis cliquer sur **Save** ou **Regenerate Token**.

Une fois le service activé, le statut au niveau du champ **Interconnection status** est modifié : le lien entre le **GCENTER** et la plateforme Intelligence est opérationnel.

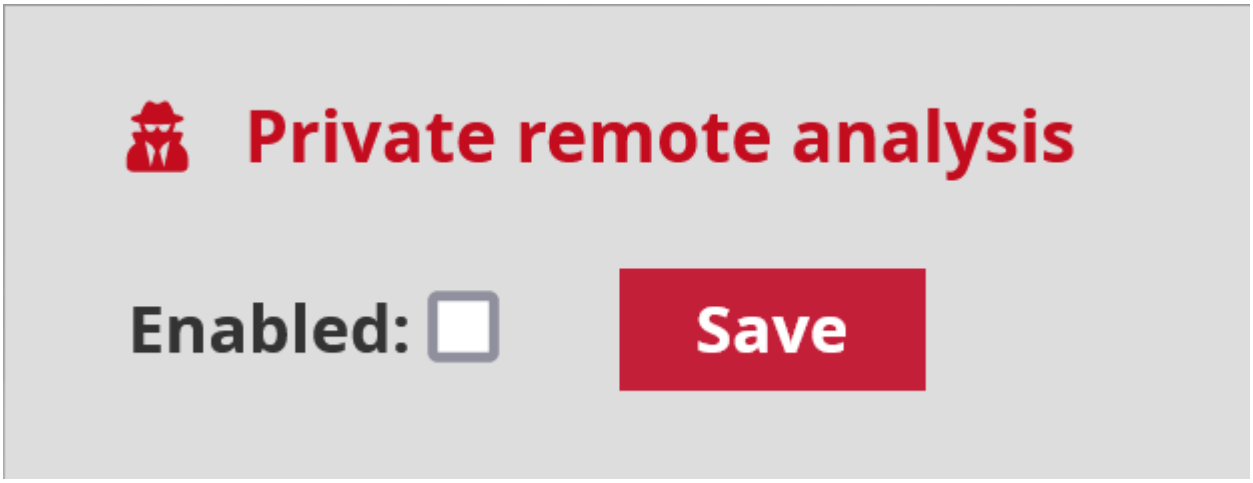
Une fois le lien établi, les utilisateurs pourront télécharger un échantillon détecté depuis la plateforme d'analyse et le faire passer sous les moteurs d'Intelligence. Les rapports d'analyse détaillés de ces échantillons pourront être récupérés depuis la section *Malcore d'Inspectra*.

Suite à cette connexion, l'administrateur pourra être capable d'envoyer des fichiers à la plateforme Intelligence pour une analyse plus approfondie et télécharger le rapport.

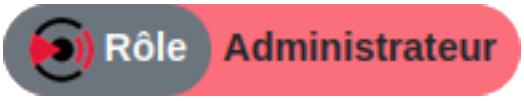


La section **Remote analysis settings** permet à l'administrateur de rester anonyme lors de l'envoi d'échantillons à la plateforme si l'option **Private remote analysis** est activée.

Si la case 'Enabled' n'est pas cochée et/ou que l'administrateur ne sauvegarde pas en appuyant sur **Save** alors, les autres utilisateurs de la plateforme Intelligence pourront voir le détail de chacune des analyses que l'administrateur fera.



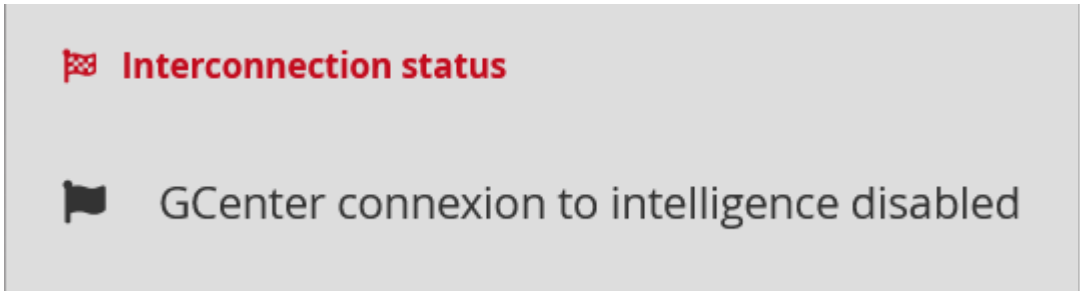
32.2 GBox



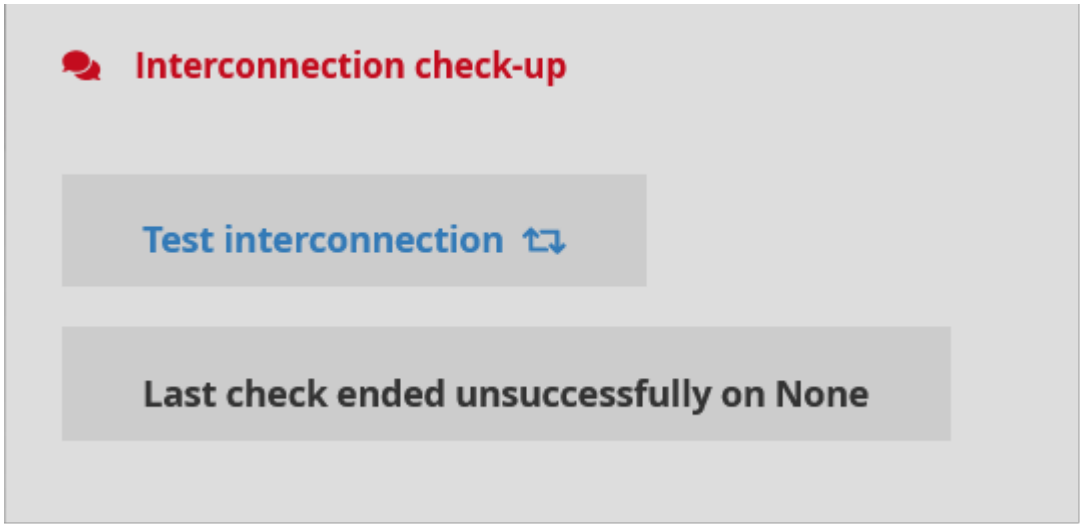
Menu : Administrators > GCenter > Third-Party Modules > Intelligence

Tout comme la connexion aux service *Intelligence* de Gatewatcher, l'utilisation d'une **GBox** permet d'effectuer une analyse approfondie des malware détectés par *Malcore* à la différence près que l'utilisation d'une **GBox** permet cela sans avoir à envoyer d'information à un service externe. La **GBox** est un équipement physique installé au sein de l'infrastructure, avec les autres équipements de la solution TRACKWATCH.

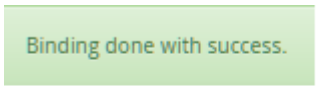
L'état du statut de connexion entre le **GCENTER** et la **GBOX** est donné avec la vue **Interconnection status** ci-dessous:

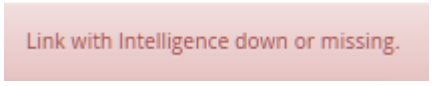


L'interconnexion peut être vérifiée en un seul clic par l'administrateur depuis la section **Interconnection check-up** en appuyant sur le bouton **Test interconnexion**.



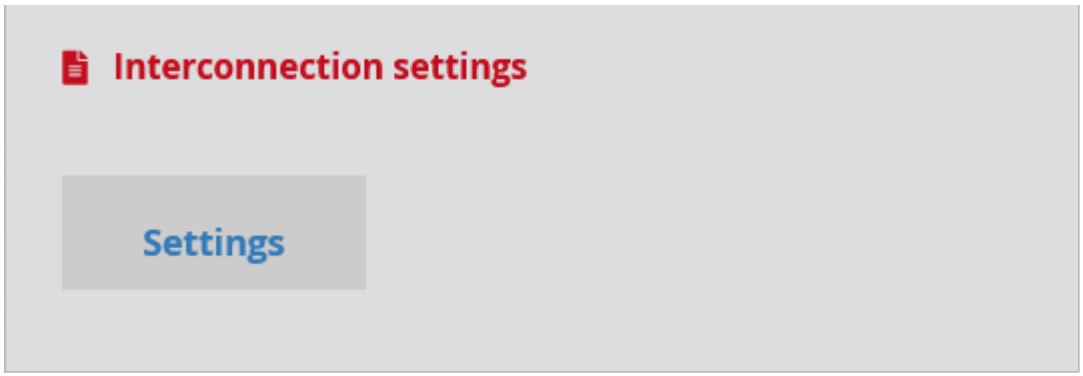
Le résultat de ce test d'interconnexion sera affiché de la manière suivante :



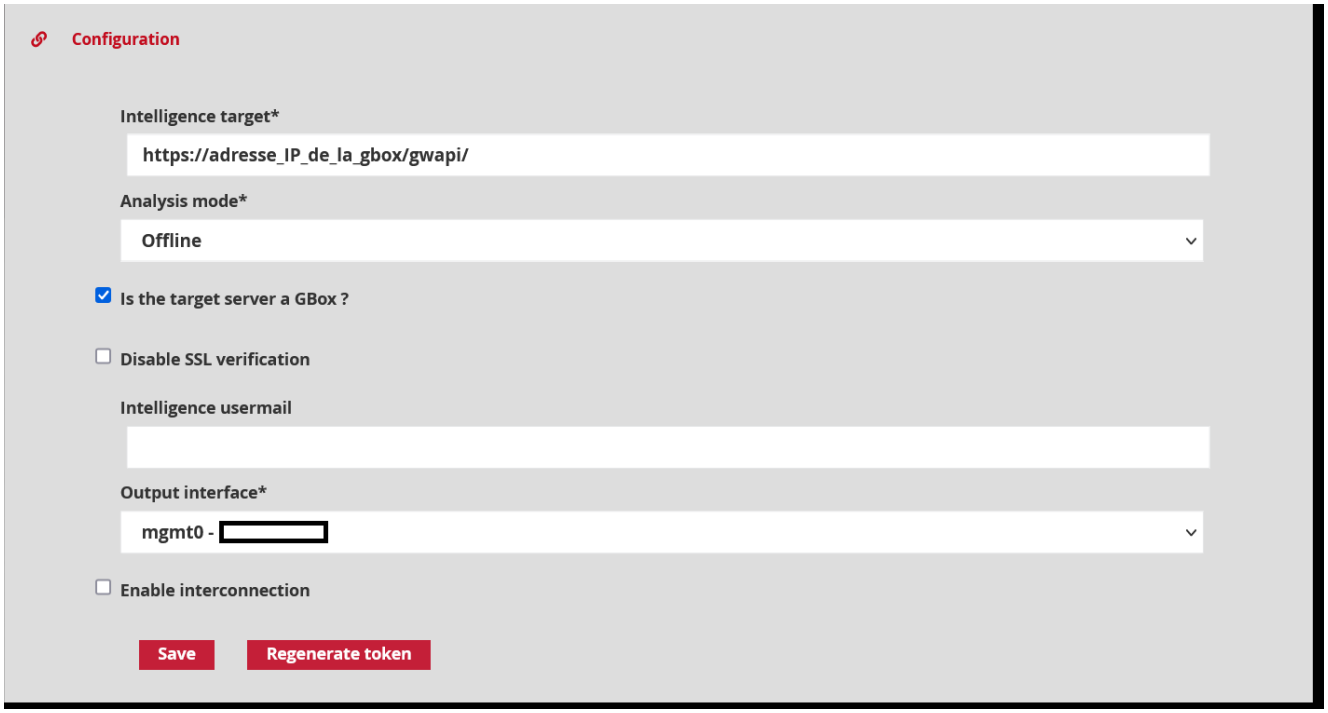


Une interconnexion doit être établie entre le **GCENTER** et la **GBOX**. Le lien entre les deux équipements fonctionne via une API (Application Programming Interface) qui permet d'envoyer des échantillons à la **GBOX** pour analyse et de récupérer les résultats des analyses.

Quelques informations sont nécessaires pour que le **GCENTER** puisse être connecté à la plateforme et puisse envoyer correctement la requête HTTP.



Certains champs sont à renseigner par l'administrateur depuis la section **Interconnection settings** en appuyant sur le bouton **Settings**.



Intelligence target : il s'agit de l'adresse de l'API de la **GBOX** (de la forme : *https://adresse IP de la GBOX/gwapi/*). **Is the target server a GBOX ?** : est à cocher pour indiquer l'utilisation d'une GBox **Disable SSL verification** : permet l'utilisation de certificat auto-signés. **Analysis mode** correspond au mode d'analyse du fichier envoyé au serveur Intelligence : *Offline* ou *Online*.

Intelligence usermail : n'est pas nécessaire dans le cas de l'utilisation d'un **GBox**

Output interface est l'interface physique du **GCENTER** par laquelle il communiquera avec le serveur **GBOX**.

La dernière étape pour l'activation du service consiste à cocher la case **Enable interconnection**. Puis cliquer sur **Save**.

Une fois le lien établi, les utilisateurs pourront télécharger un échantillon détecté depuis la plateforme d'analyse de renseignement et le faire passer sous les moteurs de la **GBox**. Les rapports d'analyse détaillés de ces échantillons pourront être récupérés depuis la partie *Inspectra - MALCORE*.

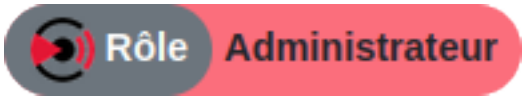
Une fois le service activé, le statut au niveau du champ **Interconnection status** est modifié : le lien entre le **GCENTER** et la **GBox** est opérationnel.

En ce qui concerne l'analyse dans la **GBOX**, le template (model) utilisé pour les échantillons peut être spécifié dans la requête. Si le template n'est pas spécifié dans la requête, les échantillons sont analysés en utilisant celui présent par défaut dans la **GBOX** qui doit donc être paramétré au préalable. Les échantillons sont transmis au format binaire brut.

La section **Remote analysis settings** n'est pas utile à l'administrateur dans ce choix d'infrastructure, la **GBOX** étant un serveur dédié au sein de la solution.

Chapter 33

Syslog

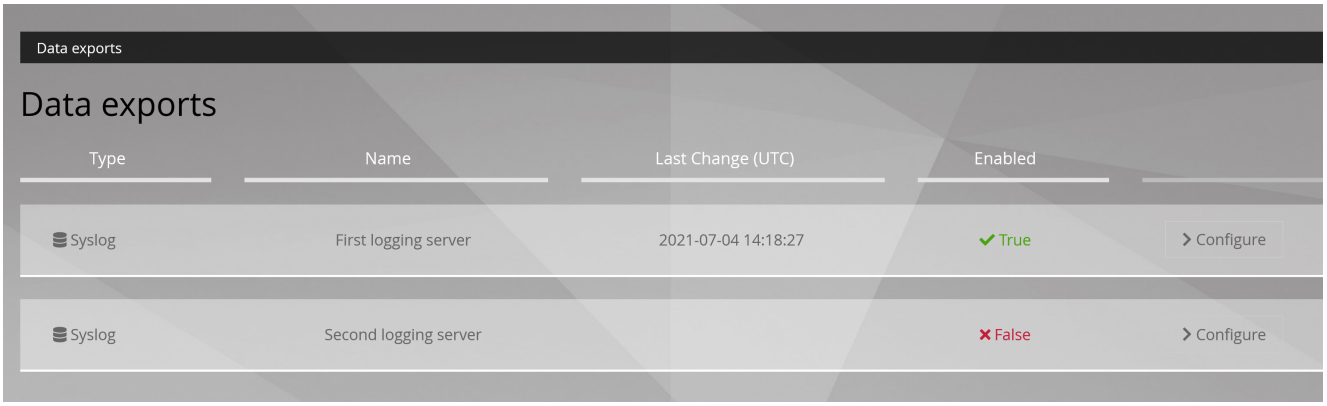


Menu : Administrators > GCenter > Data export

33.1 Configuration Syslog


Depuis cette section les administrateurs de la solution sont capables d'exporter les alertes ou une partie des alertes vers un SIEM.

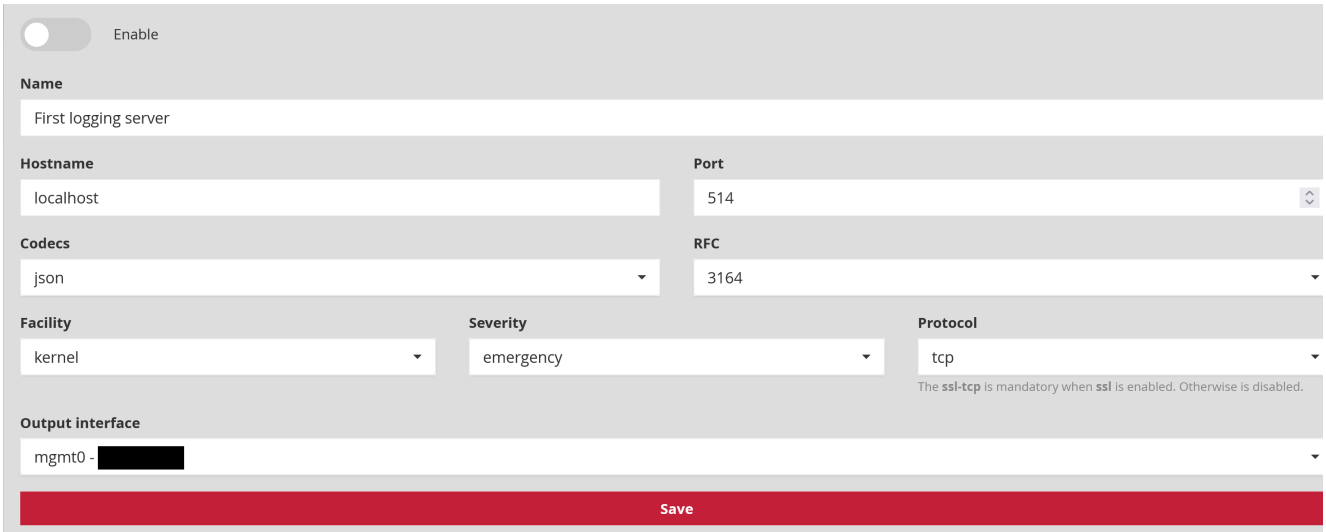
L'administrateur peut exporter les données en temps réel en ciblant un corrélateur de log de type Syslog primaire et/ou secondaire dont il peut paramétrer les envois :



Pour que la solution **TRACKWATCH** puisse communiquer ses informations à un serveur Syslog, il faut que cette partie soit paramétrée avec les informations nécessaires. Cette configuration se fait depuis trois onglets:

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

33.1.1 Paramètres généraux



Enable permet d'activer ou désactiver l'export Syslog.

Name (Exemple : *First logging server*) est le nom du serveur Syslog attribué par l'administrateur.

Host name (Exemple : *localhost* ou *192.168.199.1*) est l'adresse IP ou le nom du serveur Syslog pour la connexion.

Port number : est le port d'écoute du serveur Syslog pour la connexion. La valeur par défaut est à 514.

Codec : (Exemple : *json*, *idmef*, *cef* ou *plain*) est le codec utilisé pour les données de sortie. Les codecs de sortie sont une méthode pratique pour coder vos données avant l'exportation sans avoir besoin d'un autre filtre. Par défaut la valeur est en json.

RFC (Exemple : *3164* ou *5424*) permet de sélectionner la RFC correspondante à la normalisation des messages voulue.

Facility (Exemple : *kernel*, *user-level*, *mail*, *deamon*, *security/authorization*, *syslogd*, *line printer*, *network news*, *uucp*) correspond à la catégorie de message utilisée pour l'envoi vers le serveur Syslog. La valeur par défaut est à *kernel*.

Severity (Exemple : *emergency*, *alert*, *critical*, *error*, *warning*, *notice*, *informational*, *debug*) correspond au taux de gravité pour les messages Syslog. La valeur par défaut est à emergency.

Protocol (Exemple : *tcp*, *udp* ou *ssl_tcp*) est le protocole utilisé pour le transfert des données. La valeur par défaut est en TCP.

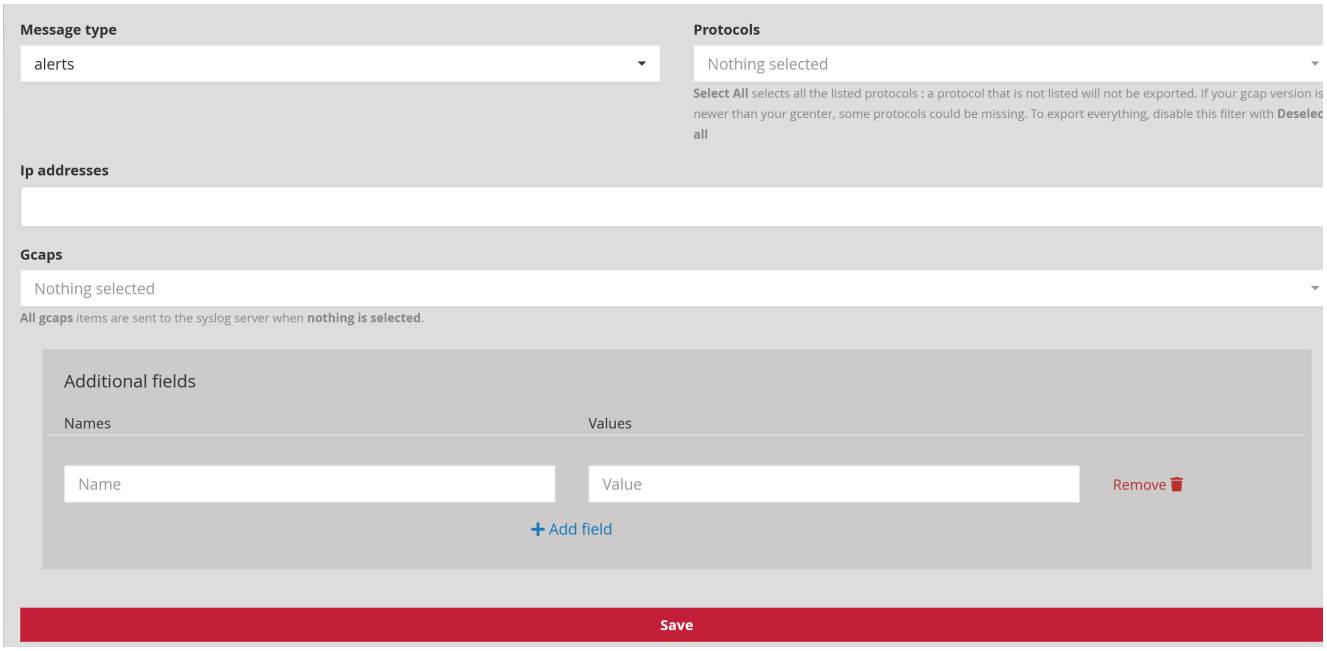
Note:

Le protocole SSL-TCP est obligatoire lorsque le chiffrement SSL est activé. Sinon, il est désactivé.

Output interface (Exemple : *mgmt0*, *sup0*) correspond à l'interface sélectionnée de sortie entre le **GCENTER** et le SIEM.

La prise en compte de toute modification est effective qu'après avoir appuyé sur '**Save**'.

33.1.2 Filtrage



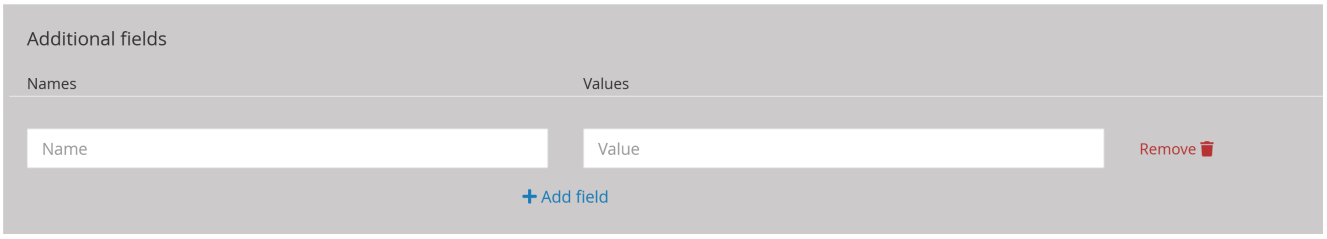
Message type : (Exemple : *alerts*, *all*) définit le type d'évènement à envoyer : uniquement les alertes ou toutes les informations (méta-données, fileinfo, ...)

Protocols : (Exemple : *dcerpc*, *dhcp*, *dnp3*, *dns*, *ftp*, *http*, *ikev2*, *krb5*, *modbus*, *netflow*, *nfs*, *smb*, *smtp*, *ssh*, *tftp*, *tls* et *ntp*) permet de sélectionner les protocoles à exporter.

Note:

[Select All] sélectionne tous les protocoles listés: un protocole qui n'est pas listé ne sera pas exporté. Si la version du GCAP est plus récente que celle du GCENTER, certains protocoles peuvent manquer. Pour tout exporter, désactivez ce filtre avec [Deselect all].

Gcaps : (Exemple : *GCap1*, *GCap2*) permet de filtrer par **GCAP**. Toutes les données des **GCAP** appairés au **GCENTER** sont envoyés au serveur Syslog si rien n'est sélectionné.

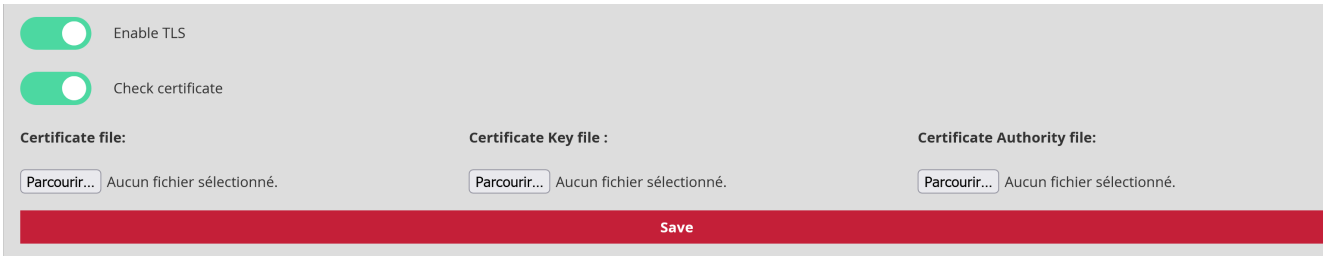


Additional fields permet à l'administrateur d'ajouter des champs supplémentaires aux données transférées. Un nom (**Name**) et une description (**value**) peuvent être renseignés dans cette fenêtre. Dans le cas de l'utilisation du codec idmef, ce champs n'est pas supporté.

La prise en compte de toute modification est effective qu'après avoir appuyé sur '**Save**'.

33.1.3 Chiffrement

Cette partie permet d'ajouter du chiffrement dans le transfert de ses données entre le **GCENTER** et le receveur syslog. Il sera nécessaire d'ajouter un certificat, la clé associée ainsi que l'autorité de certification afin de valider cette fonctionnalité.

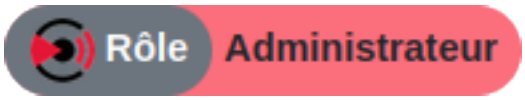


Enable TLS : possibilité d'activer le service TLS (Transport Layer Security). Désactivée par défaut.

Check certificate : paramètre qui consiste à arrêter la vérification de la validité du certificat lorsque le service TLS est activé.

La prise en compte de toute modification est effective qu'après avoir appuyé sur '**Save**'.

33.2 Logstash



Menu : Administrators > GCenter > Data export

Le GCenter peut exporter ses logs vers l'ETL Logstash. Un pipeline développé par Gatewatcher permet de récupérer le contenu JSON des logs exportés afin de pouvoir le manipuler ensuite comme on le souhaite avec les filtres Logstash. L'intégration du Gcenter est donc très rapide, et ne nécessite que deux étapes :

- Sur le Gcenter, configurer l'export de données vers Logstash.
- Sur Logstash, configurer le pipeline de réception du flux provenant du GCenter.

33.2.1 Configuration de l'export de données Logstash

Choisir l'un des deux pipelines d'export en cliquant sur **Configure**.

Le tableau suivant résume les paramètres à appliquer dans l'onglet *GENERAL*.

Note:

Les valeurs dont le format est de type $VALEUR sont spécifiques au contexte et sont notées comme telles afin qu'il puisse y être fait référence dans la suite de la documentation.

L'onglet *FILTERS* permet de choisir quels logs seront exportés. Voir *filtrage* dans la section syslog.

L'onglet "ENCRYPTION" permet d'activer le chiffrement du flux généré par le GCenter. L'input "syslog" de Logstash n'est pas compatible avec le chiffrement des données, et cette fonctionnalité ne peut donc pas être utilisée.

33.2.2 Pipeline Logstash

L'input utilisé est de type Syslog. Afin d'être compatible avec n'importe quel en-tête Syslog, un motif grok est spécifié. Le contenu JSON du log se trouve dans le champ syslog_message.

```
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$'
  }
}
```

On ne garde que le champ syslog_message, et on le convertit en JSON. Le champ d'origine (syslog_message) et le champ propre à elasticsearch (@version) sont ensuite retirés.

```
filter {
  prune {
    whitelist_names => [ "syslog_message" ]
  }

  json {
    source => "syslog_message"
  }

  mutate {
    remove_field => [ "@version","syslog_message" ]
  }

 }
```

N'importe quel output peut être ensuite utilisé. Dans cet exemple, on écrit les logs directement sur le disque sous forme de fichiers:

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

33.2.3 POC rapide

Un POC avec un docker Logstash peut être réalisé en quelques minutes. Les commandes suivantes, données à titre indicatif, devraient faciliter cette tâche.

Sur une machine linux possédant docker, exécuter les commandes suivantes afin de récupérer les fichiers de configuration par défaut de Logstash : (procédure testée avec la version 7.13.1 de Logstash)

```
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
```

On obtient alors un dossier `logstash_docker`, au sein duquel deux sous-dossiers sont apparus : `config` et `pipeline`.

Dans `config`, les paramètres peuvent être gardés par défaut, à l'exception du paramètre `xpack.monitoring.elasticsearch.hosts` qui doit être commenté dans `logstash.yaml`.

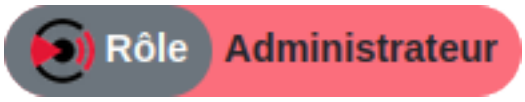
Dans le dossier `pipeline`, remplacer le pipeline par défaut par le pipeline décrit dans la section ci-dessus.

Un docker utilisant ces fichiers de configuration et ce pipeline peut ensuite être démarré :

```
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 va alors créer un répertoire `output` dans lequel les logs reçus seront écrits, avec un JSON par ligne.

33.3 Splunk



Menu : Administrators > GCenter > Data export

Le GCenter peut exporter ses logs vers le SIEM Splunk. Un Technological Add-On (TA) développé par Gatewatcher permet de mapper les logs exportés par le GCenter vers les modèles de données Splunk. L'intégration du GCenter est donc très rapide, et nécessite trois étapes :

- Sur le GCenter, configurer l'export de données vers Splunk.
- Sur le serveur Splunk, installer le TA compatible avec la version du GCenter installé. En l'occurrence, TA-gatewatcher-gcenter-v101.
- Sur le serveur Splunk, configurer la réception des données en provenance du GCenter et les associer au TA.

Note:

Le TA Splunk est encore en version bêta. Le contenu du TA est détaillé à la fin de cette documentation afin que les administrateurs puissent l'adapter à leurs besoins.

33.3.1 Configuration de l'export de données Splunk

Choisir l'un des deux pipelines d'export en cliquant sur "Configure".

Le tableau suivant résume les paramètres à appliquer dans l'onglet "GENERAL"

Note:

Les valeurs dont le format est de type $VALEUR sont spécifiques au contexte et sont notées comme telles afin qu'il puisse y être fait référence dans la suite de la documentation.

L'onglet "FILTERS" permet de choisir les logs qui seront exportés. Voir *filtrage* dans la section syslog.

L'onglet "ENCRYPTION" permet d'activer si nécessaire le chiffrement du flux entre le GCenter et Splunk. $PROTOCOL devra alors être TCP. Si le chiffrement est activé, la configuration de l'entrée de donnée Splunk (input.conf) devra contenir les stanzas appropriées. Ce guide ne couvre pas la configuration du chiffrement entre le GCenter et Splunk.

33.3.2 Installation du TA

Télécharger le TA ici : TA-gatewatcher-gcenter-v101-0.1.0.spl

L'installation du TA se fait comme pour toute app Splunk. Les étapes sont les suivantes (consultez la documentation relative à votre version de Splunk pour plus de détails) :
Gérer les apps > Installer une application depuis un fichier > choisir le TA Gatewatcher > "Envoyer"

Dans le menu de gestion des apps Splunk, en cliquant sur "Afficher les objets", vous pouvez accéder à l'ensemble des objets apportés par le TA :

- La définition des alias de champ.
- La définition des eventtypes.
- Les associations entre eventtype et tags.

Vous pouvez activer/désactiver les objets depuis cette interface et modifier leurs permissions (par défaut, les permissions sont à "Global" - Lecture pour tout le monde - Écriture pour les admins seulement).

33.3.3 Configuration de la réception des données

La configuration de l'entrée de données au niveau de Splunk doit être faite en cohérence avec la configuration du GCenter.

Dans Splunk, la configuration se fera dans Paramètres > Données > Entrées de données > TCP/UDP

Le tableau suivant résume les paramètres à appliquer pour que l'entrée de donnée fonctionne :

33.3.4 Composition du TA

Le TA est composé des fichiers ci-après, placé dans le répertoire `default` de l'application. Vous pouvez apporter des modifications à ces fichiers pour adapter le comportement du TA à vos besoins spécifiques et à votre usage des modèles de données. La bonne pratique recommandée consiste à créer un dossier `local` et à garder le dossier "default" intact (voir la documentation de Splunk "how to edit a configuration file").

33.3.4.1 props.conf

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

La section suivante supprime les en-têtes Syslog et le champ `@version` d'elasticsearch, qui n'est pas utilisé.

```
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\":\"
```

La transformation suivante appelle `gw_force_host` dans `transforms.conf`, et permet d'associer le nom du GCenter au champ `host` utilisé par Splunk.

```
TRANSFORMS-host = gw_force_host
```

La transformation suivante appelle les stanzas `sourcetype_*` de `transforms.conf` afin d'associer un sourcetype en fonction du moteur qui a généré le log.

```
TRANSFORMS-override_sourcetype_engine = sourcetype_malcore,sourcetype_codebreaker,sourcetype_
↪sigflow,sourcetype_sigflow_alert
```

Les logs ne peuvent pas dépasser 65 ko, les GCenter sont en UTC.

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

La suite de `props.conf` permet d'associer à chaque sourcetype les alias de champ et les évaluations de champ permettant de transformer les logs pour les faire correspondre aux modèles de données.

```
[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
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

Les stanzas présentes dans ce fichier sont utilisées par `props.conf`, et concernent les champs indexés par Splunk, comme `host` ou `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

Ce fichier permet de réaliser des associations entre les logs et des événements.

Evénements relatifs à l'analyse antivirale des fichiers (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

[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 lated by retroact, if enabled.
```

(suite sur la page suivante)

(suite de la page précédente)

```
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
```

Evénements relatifs à la réanalyse antivirale des fichiers suspicious (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 lated 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
```

Evénement relatif à l'activation du logging netflow sur le 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.
```

Evénements relatifs à la reconstruction de fichiers par le gcap :

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

Les événements relatifs au moteur sigflow peuvent être de deux types pour chaque protocole :

- Evénement "meta" : génération de métadonnées, obtenues par l'activation du logging du protocole sur le gcap.
- Evénement "alert" : génération d'une alerte, obtenues par l'activation du parsing du protocole sur le gcap, et la correspondance entre un flux et une règle sigflow.

```
[sigflow_meta_dcerpc]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=dcerpc)
description = An event that occurs when sigflow has reconstructed a dcerpc flow and has␣
↪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 has reconstructed a dcerpc flow and that 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 has reconstructed a dhcp flow and has 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 has reconstructed a dhcp flow and that 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 has reconstructed a dnp3 flow and has 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 has reconstructed a dnp3 flow and that 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 has reconstructed a dns flow and has logged␣
↪its metadata.
priority = 2

[sigflow_alert_dns]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=dns)
description = An event that occurs when sigflow has reconstructed a dns flow and that 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 has reconstructed a ftp flow and has logged␣
↪its metadata.

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

(suite sur la page suivante)

(suite de la page précédente)

```
description = An event that occurs when sigflow has reconstructed a ftp flow and that 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 has reconstructed a http flow and has 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 has reconstructed a http flow and that 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 has reconstructed a ikev2 flow and has 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 has reconstructed a ikev2 flow and that 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 has reconstructed a krb5 flow and has 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 has reconstructed a krb5 flow and that 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 has reconstructed a modbus flow and has␣
↪logged its metadata.

[sigflow_alert_modbus_alert]
search = (sourcetype=gw:gcenter:101:sigflow:alert event_type=alert app_proto=modbus)
description = An event that occurs when sigflow has reconstructed a modbus flow and that 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 has reconstructed a nfs flow and has 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 has reconstructed a nfs flow and that one of␣
```

(suite sur la page suivante)

(suite de la page précédente)

```
↪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 has reconstructed a ntp flow and has 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 has reconstructed a ntp flow and that 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 has reconstructed a smb flow and has 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 has reconstructed a smb flow and that 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 has reconstructed a smtp flow and has 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 has reconstructed a smtp flow and that 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 has reconstructed a ssh flow and has 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 has reconstructed a ssh flow and that one of␣
↪its rules 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 has reconstructed a tftp flow and has 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 has reconstructed a tftp flow and that one of␣
↪its rules matched the content of this flow.
```

(suite sur la page suivante)

(suite de la page précédente)

```
color = et_red

[sigflow_meta_tls]
search = (sourcetype=gw:gcenter:101:sigflow:meta event_type=tls)
description = An event that occurs when sigflow has reconstructed a tls flow and has 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 has reconstructed a tls flow and that 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 has reconstructed the flow of an unknown␣
↪protocol, and that 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 has reconstructed the flow of a protocol not␣
↪expected by this add-on.
color = et_blue
```

Événements relatifs au moteur de machine learning DGA DETECT :

```
[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 overlap 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 find that a domain name is suspicious␣
↪(likeky generated by a Domain Generation Algorithm).
color = et_red
```

Événements relatifs au moteur codebreaker :

```
[codebreaker_shellcode_expoit]
search = (sourcetype=gw:gcenter:101:codebreaker type=codebreaker event_type=shellcode␣
↪state=Exploit)
description = An event that occurs when codebreaker has detected 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
```

(suite sur la page suivante)

(suite de la page précédente)

```
[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 has detected 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

Ce fichier permet d'associer des tags aux événements définis dans `eventtype.conf`. Ces tags permettront de faire rentrer ces événements dans le `Common Information Model` de Splunk. Les associations proposées par défaut sont minimales et doivent être adaptées à votre usage des modèles de données.

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

[eventtype=malcore_infected]
attack = enabled
malware = enabled

[eventtype=malcore_suspicious]
attack = enabled
malware = enabled

[eventtype=malcore_other]
attack = enabled
malware = enabled

[eventtype=retroact_clean]
attack = enabled
malware = enabled

[eventtype=retroact_infected]
```

(suite sur la page suivante)

(suite de la page précédente)

```
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
ids = enabled

[eventtype=dgadetect_clean]
communicate = enabled
network = enabled

[eventtype=dgadetect_suspicious]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_dns]
```

(suite sur la page suivante)

(suite de la page précédente)

```
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]
attack = enabled
ids = enabled

[eventtype=sigflow_meta_nfs]
communicate = enabled
network = enabled

[eventtype=sigflow_alert_nfs]
attack = enabled
ids = enabled
```

(suite sur la page suivante)

(suite de la page précédente)

```
[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]
attack = enabled
ids = enabled

[eventtype=sigflow_unknown_alert]
attack = enabled
ids = enabled

[eventtype=sigflow_other]
communicate = enabled
network = enabled
```

(suite sur la page suivante)

(suite de la page précédente)

```
[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

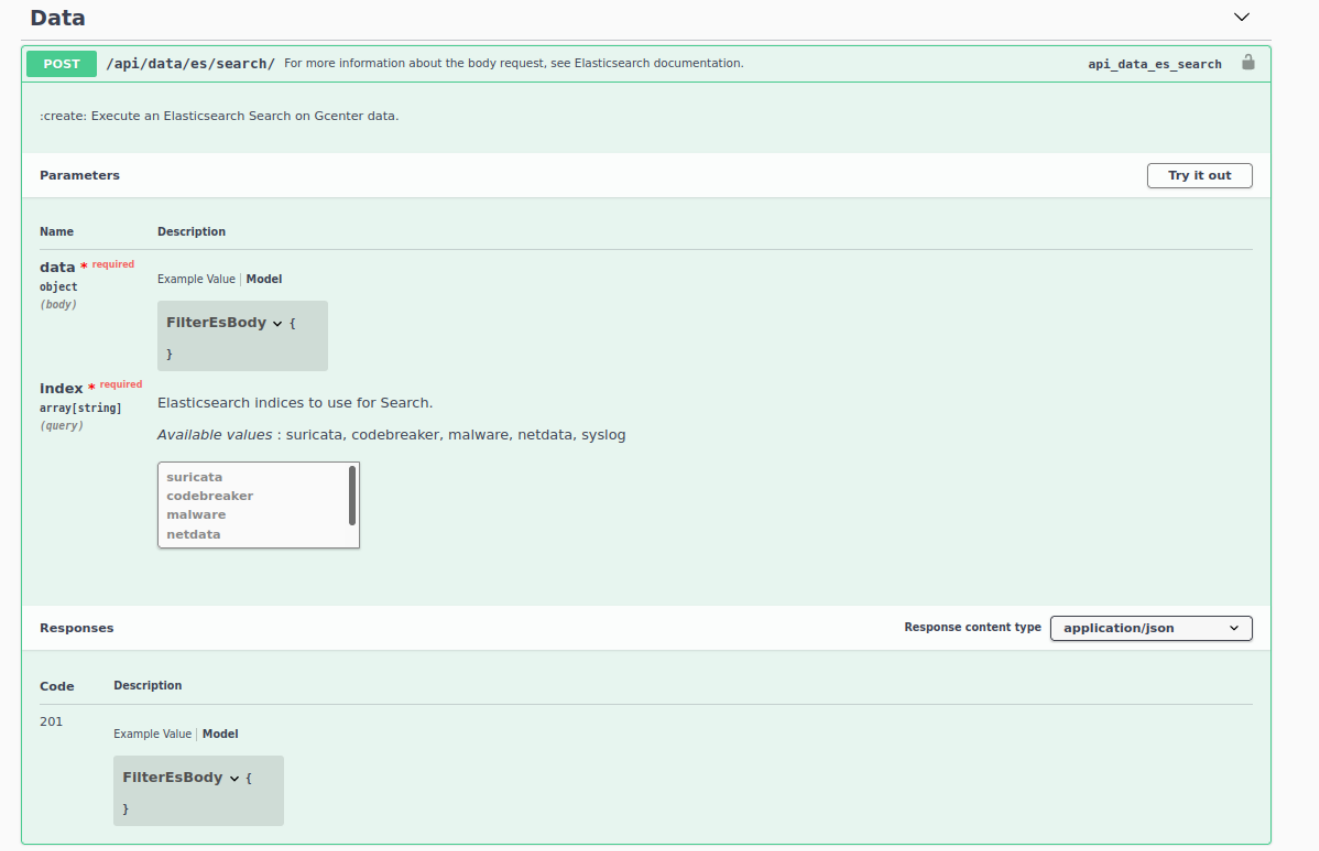
Utilisation de l'API du GCENTER

Elle peut être utilisée de trois manières différentes:

- *Via SWAGGER*
- *Via CURL*
- *Via Package python*

34.1 Utilisation via swagger

En vous connectant à votre GCenter, accédez à l'URL **https://hostnameGCENTER/docs/swagger/** Vous aurez accès à la documentation de l'ensemble de nos endpoints API.



En cliquant sur le bouton « try it out », vous pourrez directement tester des requêtes, et l'outil vous générera aussi des requêtes à utiliser avec curl.

Note:

Un known bug affecte le endpoint /api/alerts (voir la release note du GCenter). Il est recommandé de privilégier le requêtage des données par l'API elasticsearch sur le endpoint /api/data/es/search.

34.2 Utilisation via CURL

Pour un utilisateur appelé **username** et disposant des droits **opérateurs**.

Récupération du token d'API :

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

Réponse :

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

La date d'expiration est définie par la durée définie dans *Administrators* > *Configuration* > *Session age settings* dans la webui du GCenter

Envoi d'une requête :

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

Exemple d'une requête qui interrogera elasticsearch sur ses index suricata* et récupérera 100 logs sur les 24 dernières heures :

```
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 Utilisation via Package python

Ce package est une bibliothèque python qui implémente une grande partie des endpoints de l'API du GCenter.

Package API GCenter: gwapi-master.tar.gz

34.3.1 Installation

Les prérequis:

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

L'installation du package se fait avec l'utilitaire pip:

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

34.3.2 Utilisation

34.3.2.1 Import

Pour utiliser la bibliothèque il suffit d'importer le package gwapi:

```
>>> import gwapi
```

34.3.2.2 Documentation

Pour afficher la documentation de n'importe quelle fonction:

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

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 Lister les fonctions de la bibliothèque

Pour lister toutes les fonctions de la bibliothèque:

```
>>> 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 Authentification

L'ensemble des endpoints de l'API nécessite d'être authentifié.

S'authentifier via l'API du GCenter:

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

34.3.2.5 Requête Elasticsearch

Seule l'API search d'elasticsearch est implémentée via l'API du GCenter.

Exemple de requêtes elasticsearch via l'API:

- **Nombre/liste des fichiers reconstruits par le gcap sur une période de 24H:**

```
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)
```

- **Nombre/liste des alertes malcore par ordre de gravité sur une période de 24H:**

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

(suite sur la page suivante)

(suite de la page précédente)

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

- **Nombre/liste des alertes shellcode par ordre de gravité sur une période de 24H:**

```
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)
```

- **Nombre/liste des alertes powershell par ordre de gravité sur une période de 24H:**

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

(suite sur la page suivante)

(suite de la page précédente)

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

- **Nombre/liste d'alerte sigflow par ordre de gravité sur une période de 24H:**

```
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 des signatures des alertes Sigflow:**

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

(suite sur la page suivante)

(suite de la page précédente)

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

- **TOP 10 des adresses IP sources des alertes Sigflow:**

```
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 des types de shellcode:**

```
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 des types de malware:**

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

(suite sur la page suivante)

(suite de la page précédente)

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

- **Classement décroissant des couples adresses IP sources/IP destinations des alertes Sigflow:**

```
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']
```

- **Compter/Lister les 10 dernières alertes avec le statut Infected dans malcore:**

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

(suite sur la page suivante)

(suite de la page précédente)

```
...   }
... }
>>> 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

L'API permet d'afficher les alertes du GCenter sous 2 formes:

- Les dernières alertes envoyées par les Gcaps (sigflow, malcore, codebreaker).
- Les dernières alertes envoyées par les Gcaps sous forme de cluster: des alertes survenues dans le même laps de temps (la dernière heure ou le dernier jour par exemple), et qui sont toutes liées à la même adresse IP.

Récupérer les alertes du GCenter:

```
# Afficher les alertes au format RAW
>>> 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
        },
```

(suite sur la page suivante)

(suite de la page précédente)

```
        "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"
    }
]
# Afficher les alertes au format Cluster
>>> 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 alerts 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 Export des données

L'Export des données comprend les fonctionnalités netdata et syslog.

Configuration de l'export netdata:

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

Configuration de l'export syslog 1:

```
# Configuration de l'onglet général de l'export syslog.
>>> api.set_syslog_general(id=1, hostname="10.10.10.10", port=514)
# Configuration des filtres pour l'export syslog 1.
>>> api.clear_syslog_filters(id=1)
>>> api.set_syslog_filters(id=1, ips=["10.10.10.10"], gcap=[gcap_choice], protocols=["dns",
↪"http"])
```

(suite sur la page suivante)

(suite de la page précédente)

```
# Configuration des certificats pour l'export syslog 1. Les certificats doivent être au␣
↪format PEM.
>>> api.set_syslog_certificate(id=1, cert="-----BEGIN CERTIFICATE-----...", cert_key="-----
↪BEGIN RSA PRIVATE KEY-----", ca="-----BEGIN CERTIFICATE-----...")
# Désactivation de l'export syslog 1.
>>> api.disable_syslog(id=1)
```

34.3.2.8 Gcap Profiles

La section Gcap Profiles du menu Operators est en partie configurable via l'API. Les sections "Detection Ruletsets" et "Base Variables" sont configurables.

Pour appliquer les modifications sur le gcap:

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

Fonctions qui ne nécessitent pas d'appliquer de modification:

```
# Lister les Gcaps associés au GCenter
>>> api.get_gcaps()
[{'id': 1, 'fqdn': 'gcap.example.com', 'is_paired': True, 'last_rule_update': '2021-07-
↪01T13:42:03.709091', 'status': 'online'}]
# Afficher les données d'un Gcap associé au 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'}
# Afficher le template associé aux Gcaps
>>> api.get_gcap_template()
{'profile': 'intuitio'}
# Modifier le template associé aux Gcaps parmi les valeurs: ["minimal", "balanced", "lpm",
↪"paranoid", "intuitio"]
>>> api.set_gcap_template(template="balanced")
{'profile': 'balanced'}
# Afficher les interfaces d'un Gcap
>>> api.get_gcap_interfaces(gcap_id=1)
[
    {
        "enabled": true,
        "name": "mon0",
        "mtu": 1500,
        "is_cluster": false,
        "cluster_interfaces": [
            "mon0"
        ]
    }
]
# Afficher la configuration single-tenant
>>> api.get_gcap_single_tenant(gcap_id=1)
{'enabled': False, 'enable_shellcode': True, 'enable_powershell': True}
# Afficher la configuration multi-tenant
>>> 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,
```

(suite sur la page suivante)

(suite de la page précédente)

```
↪'file_store_stream_depth_mb': 10, 'stream_memcap_b': 32000000000, 'stream_prealloc_sessions
↪': 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}
# Afficher la configuration les vlans
>>> 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'}]
```

Fonctions qui nécessitent d'appliquer les modifications:

```
# Configurer le 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}
# Configurer le multi-tenant par interface. Il doit être fait pour chaque 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}
# Supprimer la configuration multi-tenant (vlans + interfaces)
>>> api.reset_gcap_tenant(gcap_id=1)
True
# Configurer les variables du gcap. Pour l'instant seule la configuration du logging et du␣
↪parsing des protocoles est implémentée.
>>> PARSING_PROTOS = [
...     "dcerpc", "dhcp", "dnp3", "dns_udp", "dns_tcp", "ftp",
...     "http", "ikev2", "krb5", "modbus", "nfs", "ntp", "smb",
...     "smtp", "ssh", "tftp", "tls"
... ]
>>> LOGGING_PROTOS = [
```

(suite sur la page suivante)

(suite de la page précédente)

```
...     "dhcp", "dnp3", "dns_udp", "dns_tcp", "ftp", "http", "ikev2",
...     "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)
# Ajouter un 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'}
# Configurer le multi-tenant par 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}
# Supprimer un vlan
>>> api.delete_gcap_vlan(
...     gcap_id=1,
...     vlan="110"
... )
True
# Modifier la configuration d'un vlan. Il faut supprimer le vlan et le recréer.
>>> 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

Il est possible de configurer et de visualiser la licence du GCenter via l'API.

Configurer la licence du GCenter:

```
>>> 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

Il est possible et de visualiser la configuration réseau du GCenter via l'API.

```
# Afficher la configuration de toutes les interfaces réseau du GCenter
>>> 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'}]
# Afficher la configuration d'une interface réseau du GCenter
>>> 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

Il est possible de configurer et de visualiser les paramètres de Malcore via l'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

Il est possible de visualiser les rulesets Sigflow via l'API.

```
# Lister les rulesets associés au GCenter
>>> api.get_sigflow_rulesets()
[{'id': 3, 'name': 'ALL', 'descr': '', 'created_date': '2021-06-24T13:45:35.627132Z', 'has_
↪files': True}]
# Lister seulement les rulesets dont les fichiers ont été générés
>>> api.get_sigflow_rulesets(with_files=True)
[{'id': 3, 'name': 'ALL', 'descr': '', 'created_date': '2021-06-24T13:45:35.627132Z', 'has_
↪files': True}]
# Afficher la configuration d'un ruleset associé au 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

Il est possible de visualiser le statut des composants du GCenter via l'API.

Afficher le statut des composants du GCenter:

```
# Vérifier que l'API fonctionne: ne nécessite pas d'authentication
>>> api.get_api_status()
True
# Afficher le statut du GCenter
>>> api.get_gcenter_status()
{'version': '2.5.3.101-XXXX', 'serial_number': 'XXXXXXX'}
# Afficher le statut global du GCenter et des erreurs associées
>>> api.get_healthchecks_status()
{'healthy': 'Bad', 'errors': ['Malware Analysis Engine has one or more issues: Last known␣
↪good state: 2021-06-25T12:58:46.336013']}
# Afficher le statut des mises à jour
>>> api.get_updates_status()
{'status': 'Good', 'errors': []}
# Afficher les statuts d'authentification de l'utilisateur
>>> api.get_user_status()
{'message': 'success', 'authenticated': False}
```

34.3.2.14 User

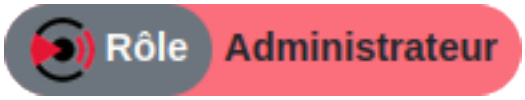
Il est possible de visualiser les données des utilisateurs du GCenter via l'API.

Afficher les données des utilisateurs du GCenter:

```
# Afficher les données de tous les utilisateurs
>>> 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'}]}]
# Afficher les données d'un utilisateur
>>> 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

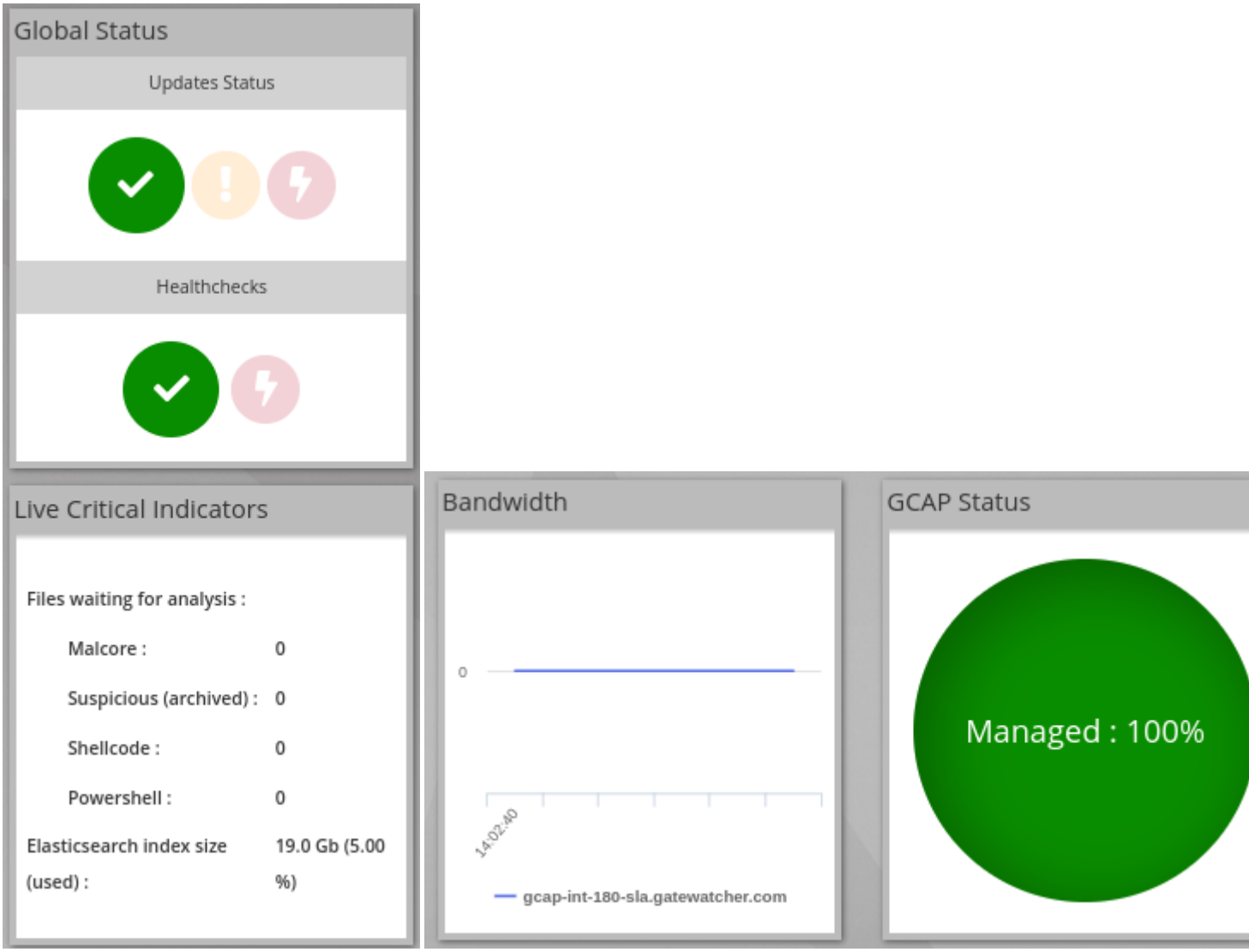
Home Page



Menu : Home Page

Une vue rapide de l'état de la solution est disponible directement depuis la *Home Page*. Cette dernière est accessible à tout moment en cliquant sur le logo **Gatewatcher** dans le menu de gauche.

On y trouvera le statut global de la solution **TRACKWATCH** ainsi que les fichiers en attente d'analyse. Plus bas sur la page, les statuts des **GCAP** et les informations de mise à jour sont également affichés.



Rôle Opérateur

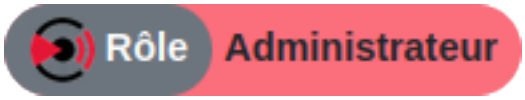
Menu : Home Page

En tant qu'opérateur, le contenu de la *Home Page* est différent. Le récapitulatif des dernières alertes sera affiché.


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
Sigflow History
5k
4k
3k
2k
1k
0k
Value
13 / 9 / 2021 13:31
14 / 9 / 2021 3:8
High
Medium
Low
Malware History
4
3
2
1
0
Value
14 / 9 / 2021 3:8
Clean
Codebreaker History
60
40
20
0
Value
14 / 9 / 2021 3:8
shellcode

Chapter 36

Dashboards embarqués



Menu : Administrators > GCenter > Monitor

Depuis cette section les administrateurs de la solution TRACKWATCH ont la permission de visualiser en temps réel des informations sur les équipements.

Cette interface est utilisée pour monitorer le **GCenter** en termes de charge CPU, mémoire, réseau et disque via des dashboards dynamiques.

L'administrateur GATEWATCHER peut accéder aux informations des services monitorés pour s'assurer du bon fonctionnement de ces derniers :

- Basic host stats
- Malcore stats
- Malcore database stats
- Elastic search stats
- GCENTER global db stats
- Gweb stats
- Live feed service stats
- Network stats

La section *Basic host stats* est affichée par défaut, les autres sections sont visible en cliquant sur le nom de la section ou sur le bouton **Show**.

Il est possible de survoler les graphiques pour obtenir les valeurs mesurées. Sur des graphiques avec plusieurs valeurs tracées, on peut aussi choisir quel élément sera tracé en cliquant sur la légende pour les afficher/cacher.

De plus, suivant la position du curseur de la souris sur n'importe quel graphique, la position sur les autres graphiques se synchronise également. Cela permet d'avoir toutes les informations nécessaires à un instant **T** voulu.


Permet de se déplacer sur le graphique vers la gauche, cette manipulation est possible grâce à un glissement vers la droite avec la souris.


Permet de se déplacer sur le graphique vers la droite, cette manipulation est possible grâce à un glissement vers la gauche avec la souris.

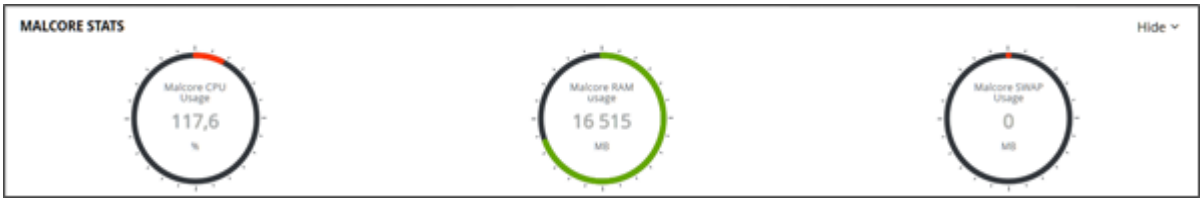

Permet de réinitialiser tous les graphiques à leur état d'auto rafraîchissement par défaut. L'administrateur peut également double cliquer sur le contenu du graphique avec sa souris.

Possibilité de zoomer dans le graphique ou appuyer sur Maj et sélectionner la zone du graphique pour zoomer. Le zoom est également possible en appuyant sur MAJ ou Ctrl avec la molette de la souris.

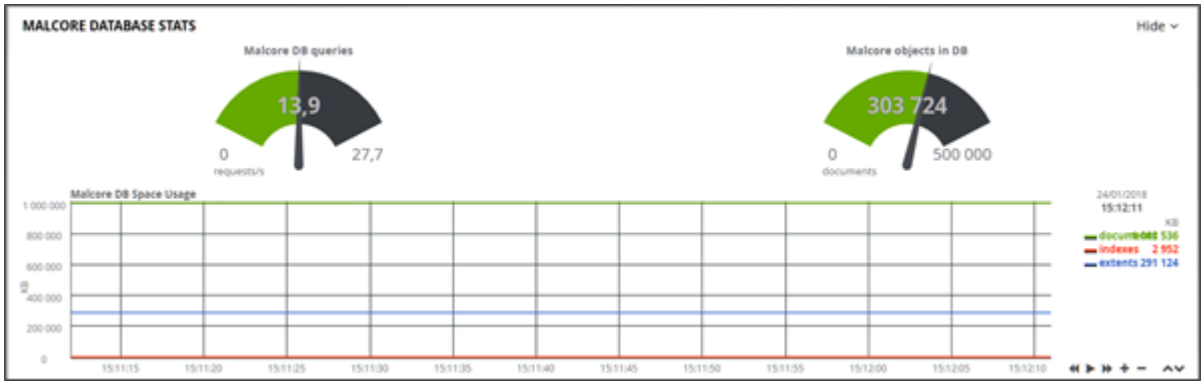
L'administrateur peut faire glisser avec sa souris et utiliser ce paramètre pour modifier le graphique verticalement. Il est possible de double-cliquer pour réinitialiser entre deux états, le graphique par défaut et celui qui correspond à toutes les valeurs.

BASIC HOST STATS offre les informations en temps réel du **GCENTER** avec des indicateurs globaux du système comme la moyenne des taux d'occupation des CPU, les écritures disques, le taux d'occupation du swap. Les capacités utilisées, libres et réservées pour différents répertoires sont également monitorées.

MALCORE STATS offre des informations sur l'état en termes de capacité utilisée du CPU, de la RAM et de la SWAP, pour le moteur MALCORE.

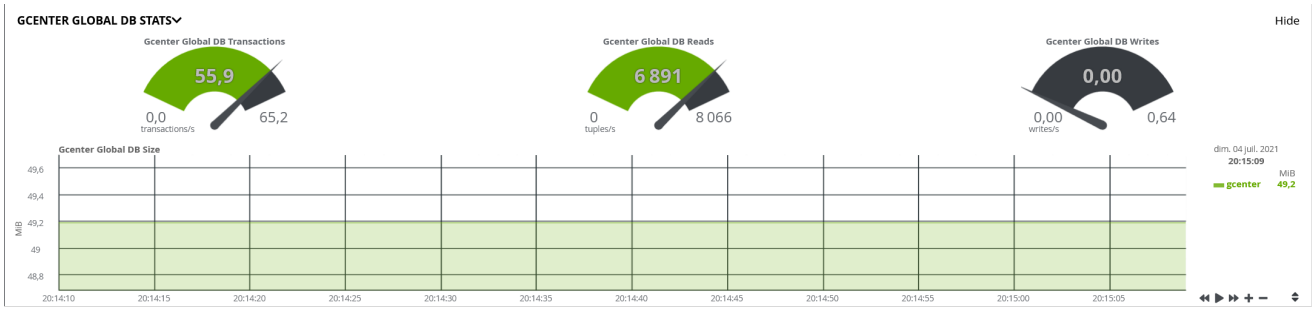


MALCORE DATABASE STATS offre des informations sur des statistiques concernant la base de données du moteur MALCORE.



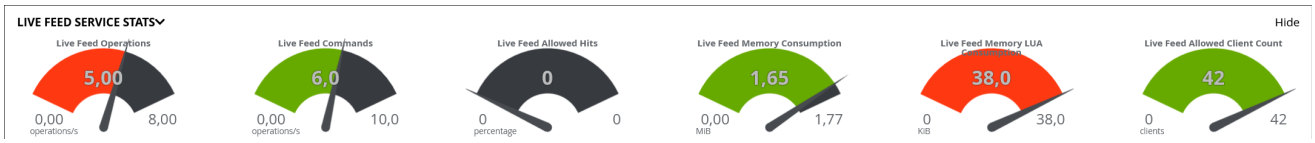
ELASTIC SEARCH STATS offre des informations sur l'état du cluster ElasticSearch qui est chargé d'enregistrer puis d'indexer les données capturées par la sonde **GCAP** dans le **GCENTER**. La bande passante du cluster est supervisée.

GCENTER GLOBAL DB STATS offre des informations sur ce que consomme la base de données globale du **GCENTER**.

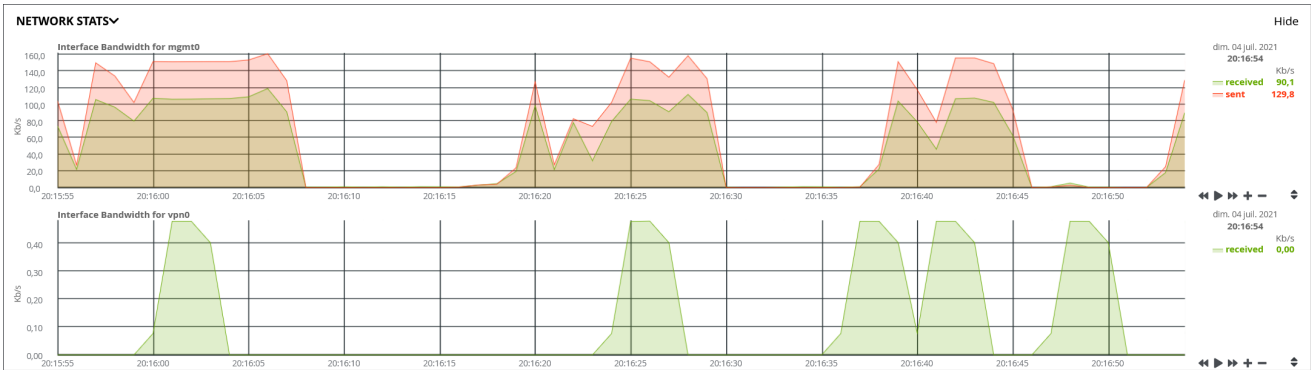


GWEB STATS offre des informations sur le serveur Web Nginx du **GCENTER**.

LIVE FEED SERVICE STATS offre des informations sur l'ensemble des services qui composent le **GCENTER**.

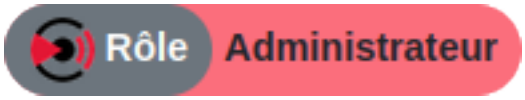


NETWORK STATS offre des informations sur la bande passante des interfaces réseaux connectées au **GCENTER**. Plus il y aura d'interfaces physiques de connectées à l'équipement, plus il y aura de tableaux.


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



Menu : Administrators > GCenter > Configuration > Nagios

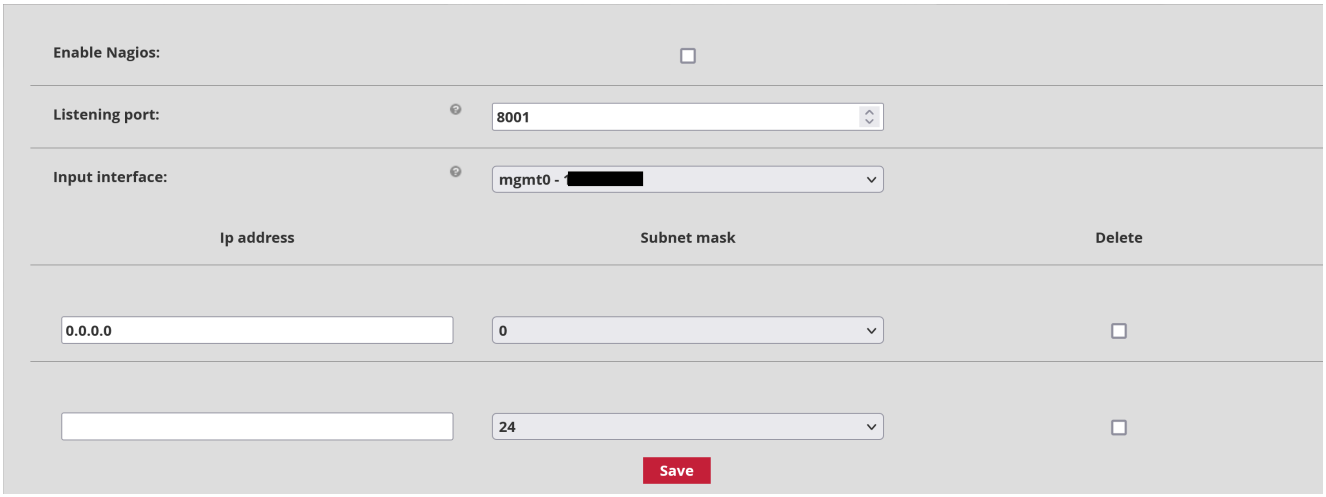

Il est ainsi possible d'exposer un certain nombre de métriques sur un port donné afin que le Gcenter soit surveillé par un système de supervision comme Nagios, Centreon, Zabbix ou autre.

Il sera tout d'abord nécessaire d'activer le service.

Enable Nagios : autorise un serveur tiers à venir requêter les métriques relatives au fonctionnement du gcenter.

Listening port : correspond au port d'écoute sur lequel seront exposées les métriques.

Input interface : est l'interface sur laquelle le **GCENTER** sera en écoute.



Les champs suivants permettent de lister les réseaux autorisés à contacter le serveur de supervision (Adresse IP (sous la forme *xxx.xxx.xxx.xxx*) et masque de sous réseau associé (de *0 à 32*).

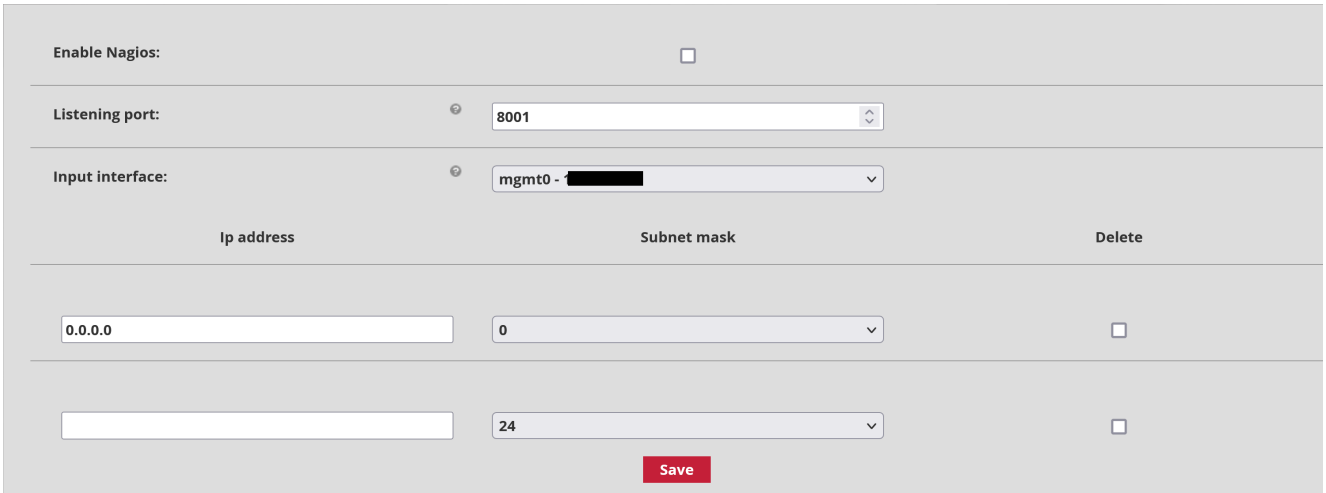
Il est ainsi possible d'exposer un certain nombre de métriques sur un port donné afin que celui-ci soit *poller* par un système de supervision (de type Nagios, Centreon, Zabbix,...).

Il sera tout d'abord nécessaire d'activer le service.

Enable Nagios permet d'activer la supervision via un système de *polling*.

Listening port : correspond au port d'écoute sur lequel seront exposées les métriques.

Input interface : est l'interface sur laquelle le **GCENTER** sera en écoute.



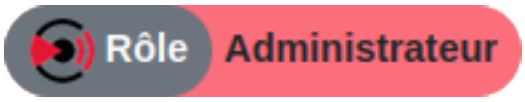
Les champs suivants permettent de lister les adresses IP ou réseaux autorisés à contacter le serveur de supervision. Une adresse IP (sous la forme *xxx.xxx.xxx.xxx*) doit être renseignée dans le champ **IP address** et sélectionner le masque de sous réseau associé (sélection d'une valeur au niveau de **Subnet mask** allant de *0 à 32*).

Une fois ces valeurs renseignées, l'administrateur peut sauvegarder l'ajout des serveurs en appuyant sur **Save**.

Une fois cette action effectuée, les *endpoints* suivants seront mise à disposition des serveurs de supervision

Chapter 38

Netdata



Adresse : https://ip.du.gcenter/gstats

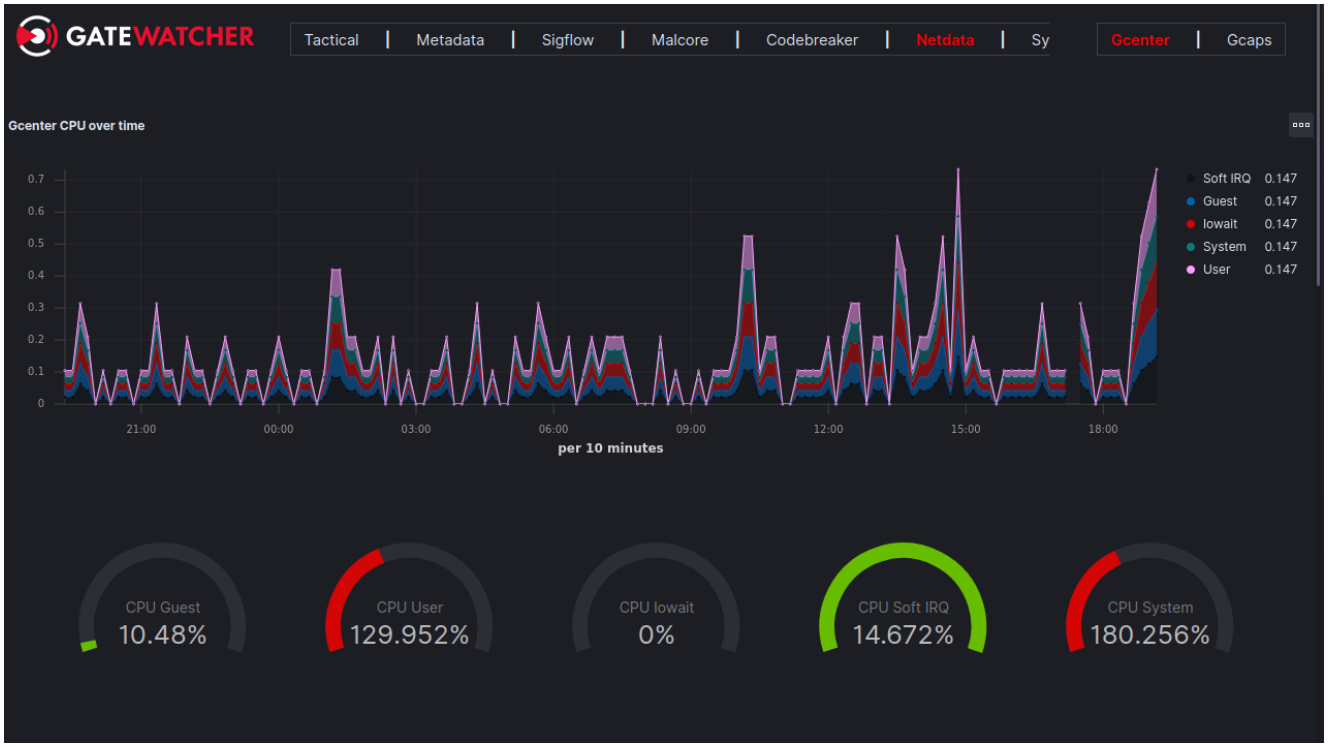
Un serveur *Netdata* est également embarqué dans la solution TRACKWATCH.

Celui-ci est accessible aux administrateurs via l'URL https://ip.du.gcenter/gstats.

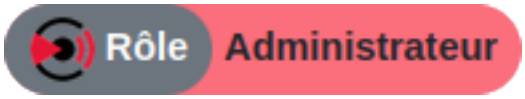
Cette interface met à disposition des administrateurs un grand nombre de métriques sur les différents équipements de la solution TRACKWATCH.

Il est possible via le menu en haut de page de sélectionner l'équipement que l'on souhaite observer. On y trouvera le **GCenter** mais également les **GCap** qui y sont appairés.

Alternativement, ces données seront également consultables depuis le *dashboard* kibana **Netdata** accessible depuis le menu `Operators > Dashboards`



38.1 Netdata export



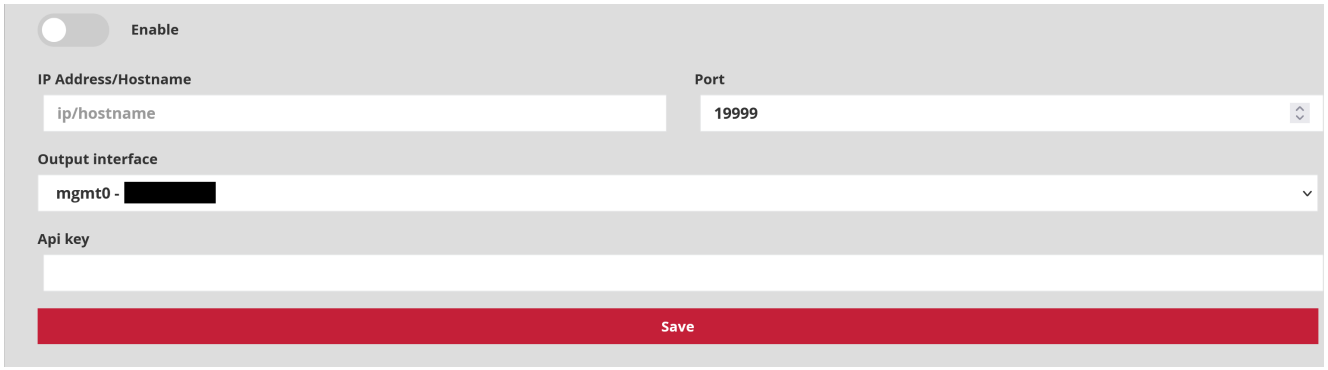
Adresse : ADMINISTRATORS > GCenter > Configuration > Netdata Export

Bien que la solution TRACKWATCH embarque un serveur Netdata, l'administrateur peut vouloir exporter les données système en temps réel vers un serveur Netdata déjà existant.

Pour que la solution **TRACKWATCH** puisse communiquer ses informations à un serveur Netdata, il faut que cette partie soit paramétrée avec les informations nécessaires. Cette configuration se fait depuis deux onglets:

- *General*
- *Encryption*

38.1.1 Netdata - Paramètres généraux



Enable : active/désactive le service.

IP Address/Hostname : le fqdn ou l'adresse IP du serveur Netdata.

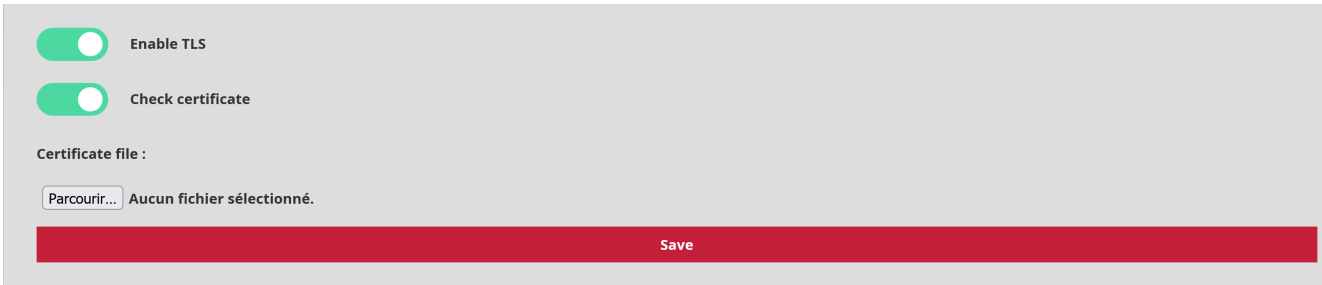
Port : le port d'écoute du serveur Netdata.

Output interface : l'interface de sortie à utiliser pour joindre le serveur Netdata.

API key : la clé API du serveur Netdata.

38.1.2 Netdata - Chiffrement

Cette partie est nécessaire pour que l'administrateur puisse mettre en place le chiffrement de la communication entre le **GCENTER** et son serveur Netdata. Un certificat sera nécessaire afin d'activer cette fonctionnalité.



Enable TLS : Activation/Désactivation du chiffrement. Désactivée par défaut.

Check certificate : active/désactive la vérification de la validité du certificat lorsque le service TLS est activé.

La prise en compte de toute modification est effective qu'après avoir appuyé sur **Save**.

Plus d'informations sont disponibles dans la section *Utilisation d'un serveur Netdata*

Chapter 39

Utilisation d'un serveur NETDATA

Ce guide donne à titre indicatif les étapes nécessaires à la mise en place d'un serveur de monitoring netdata, et son interconnexion à un GCenter afin d'en assurer la surveillance.

Note:

La version Netdata compatible avec le GCenter et GCap est la 1.19

39.1 Installation via docker

Installer le docker netdata

```
docker pull netdata/netdata:v1.19.0
```

Pour pouvoir éditer la configuration de netdata depuis la machine hôte, il faut lancer un container temporaire pour récupérer les fichiers de configuration.

```
mkdir netdataconfig
docker run -d --name netdata_tmp netdata/netdata
docker cp netdata_tmp:/usr/lib/netdata netdataconfig/
docker rm -f netdata_tmp
```

Lancement du container final

```
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

Configuration du stream.conf et gcenter

Générer l'uuid

```
sudo docker exec -it netdata uuidgen
```

Configuration stream avec l'uuid généré précédemment.

Netdata recommande d'utiliser edit-config

```
sudo docker exec -it netdata /etc/netdata/edit-config stream.conf
```

```
[dd236090-a42d-43e2-b0ba-ff8eaa6216a2] << Remplacer l'uuid ici
    enabled = yes
    default history = 36000
    default memory mode = ram
    health enabled by default = auto
    allow from = *
    default postpone alarms on connect seconds = 60
```

Configuration de netdata.conf

```
sudo docker exec -it netdata /etc/netdata/edit-config netdata.conf
```

```
[global]
      ...
      hostname = netdata-docker.gatewatcher.com
      ...
      timezone = Europe/Paris
```

Configurer l'export netdata dans le gcenter

Note:

A lire *Netdata export*.

Pour que netdata envoi des notifications, il faut configurer health_alarm_notify.conf

```
sudo docker exec -it netdata /etc/netdata/edit-config health_alarm_notify.conf
```

Référence : Alarm Configuration

39.3 Création d'alertes pour Netdata

La création des alertes se fait dans le dossier du conteneur :

```
/usr/lib/netdata/conf.d/health.d
```

Afin que les nouvelles alertes soient prisent en compte, il est nécessaire de redémarrer le conteneur docker.

Pour clarifier la gestion de vos alertes, il est conseillé de créer un fichier **.conf* par catégorie d'alerte.

Voici des exemples :

Description	Lien
Alerte en cas d'absence/surcharge de trafic	`traffic.conf`
Alerte en cas de désactivation des services d'analyse du Gcap	`suricata_status.conf`
Alerte si un redémarrage de Gcap/Gcenter a eu lieu	`reboot.conf`
Alerte en cas de surcharge RAM	`ram.conf`
Alerte en cas de packets réseau "droppés" sur le Gcap	`drop.conf`
Alerte en cas de remplissage disque (ici la partition /data du Gcap)	`disk.conf`
Alerte en cas de surcharge CPU	`cpu.conf`

Créer vos propres alertes

La création des alertes se base sur les métriques que netdata collecte.

Pour connaître ces métriques, il faut se connecter à l'interface Netdata de votre Gcenter.

```
https:// IP ou FQDN du Gcenter /gstats
```

Prenons l'exemple du monitoring RAM

Figure1: Le nom du Graph est system.ram et la courbe à surveiller used

L'alerte dans ram.conf sera rédigée comme suit :

On nomme l'alarme

```
1>>  alarm: ram_usage
```

On nomme le graphique dans Netdata :

```
2>> on: system.ram
```

On indique que l'on calcule la moyenne sur 10 min de la courbe used

```
3>> lookup: average -10m percentage of used
```

On spécifie l'unité

```
4>> units: %
```

On spécifie l'intervalle de temps entre chaque calcul

```
5>> every: 1m
```

On défini les seuil alerte et critique

```
6>> warn: $this > 70
7>> crit: $this > 90
```

On défini le délais pour faire disparaître l'alarme après déclenchement

```
8>> delay: down 15m multiplier 1.5 max 1h
```

Description de l'alarme

```
9>> info: average RAM utilization over the last 10 minutes
```

Définir qui sera alerté (voir health_alarm_notify.conf)

```
10>> to: sysadmin
```

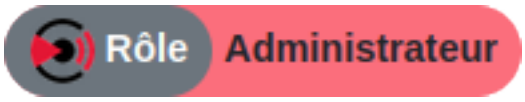
Cette partie du **GCENTER** permet la gestion des utilisateurs et des groupes associés, l'historique des authentifications sur la plateforme mais aussi l'association avec un serveur LDAP.

Depuis cette interface de configuration, l'administrateur pourra personnaliser les paramètres de la solution de management **GCENTER** avec ces cinq onglets :

- *Authentications history*
- *Creations/Deletions history*
- *Permissions history*
- *Users management*
- *LDAP configuration*

Chapter 40

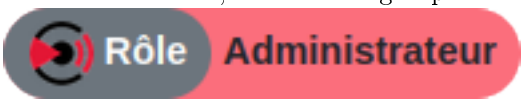
Utilisateurs locaux

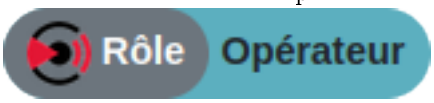


Menu : Administrators > GCenter > Accounts > User management

Depuis le menu de configuration des comptes utilisateurs de la solution TRACKWATCH, il est possible de créer des comptes utilisateurs ayant chacun des droits différents. Les groupes proposés respectent entièrement la Loi de Programmation Militaire.

La création d'un utilisateur ainsi que le profil qui lui sera associé peuvent être paramétrés depuis cette vue. En effet selon les commandes ou actions effectuées, il sera nécessaire de faire partie d'un groupe donné.

Au sein de cette documentation, le détail du groupe autorisé à effectuer l'action est spécifié dans chaque section par les badge 

et 

respectivement quand les droits Administrateur sont nécessaires ou quand les droits opérateurs sont nécessaires.

L'administrateur renseigne le nom/prénom/mail/mot de passe, de l'utilisateur qu'il souhaite créer. Ces champs remplis serviront par la suite à tracer l'utilisateur dans l'historique en cas de changements.

Username est le champ à remplir par l'administrateur pour renseigner le nom complet du nouvel utilisateur de la plateforme de management **GCENTER**. Cette valeur ne peut contenir que des lettres, des chiffres et des caractères [@/./+/-/-/_.].

First name, **Last name** et **Email address** sont des champs optionnels à la création de l'utilisateur et informent respectivement sur le prénom, le nom et l'adresse mail du profil.

Password est prévu pour le mot de passe du compte utilisateur créé. Ce mot de passe devra obligatoirement contenir un minimum de sept caractères.

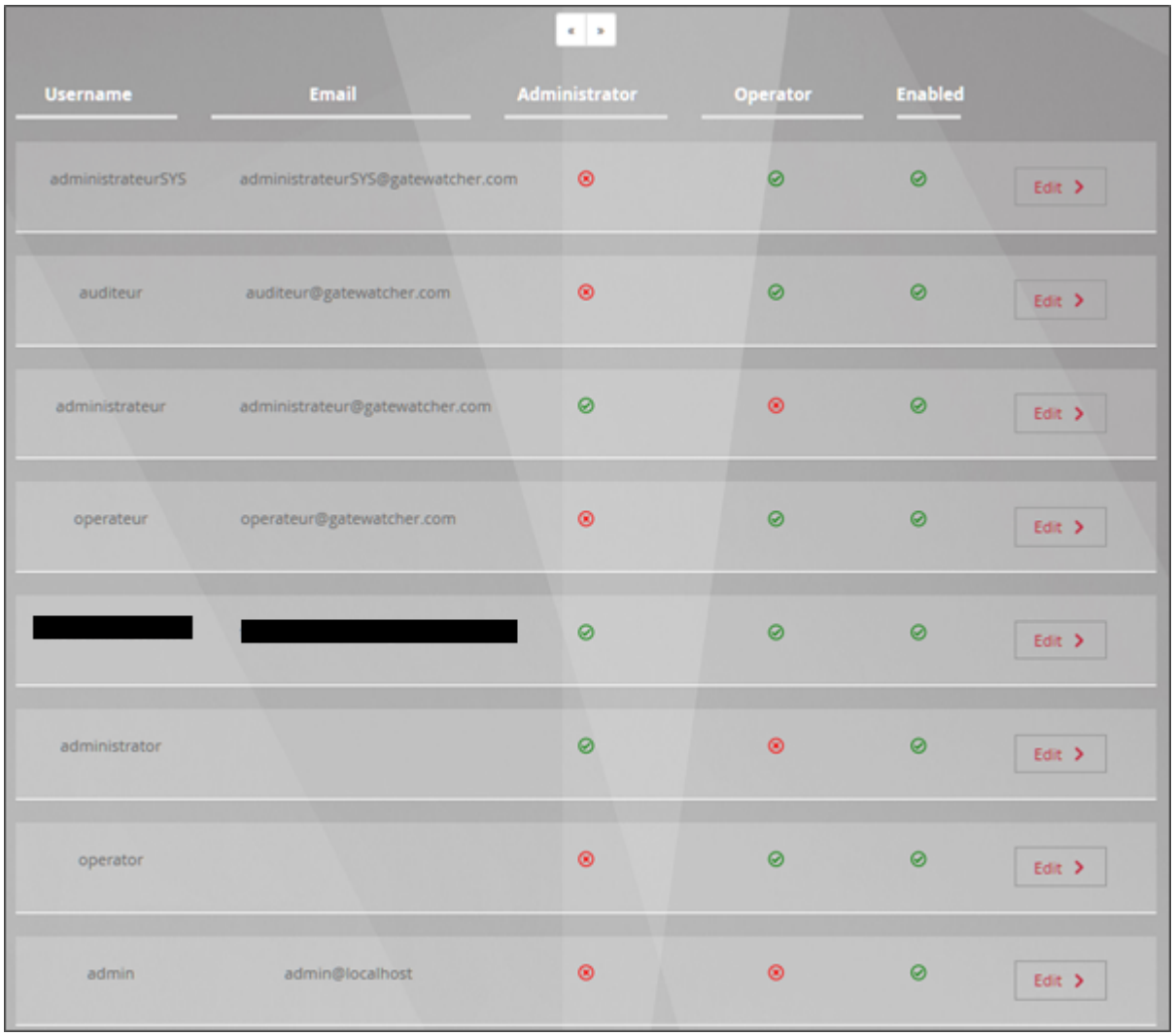
Operator et **Administrator** représentent des groupes. Une fois la case cochée, l'utilisateur aura les droits adéquates au groupe sélectionné.

Active : permet d'activer/désactiver le compte utilisateur.

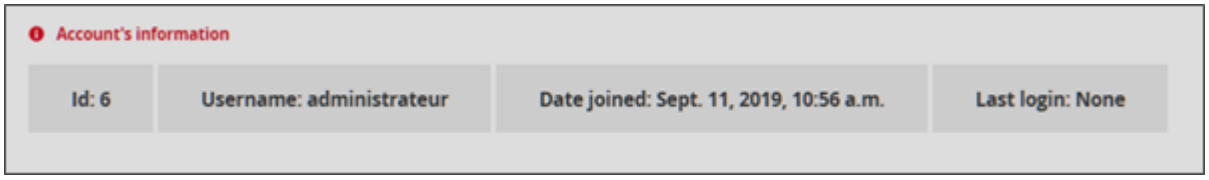
- Le groupe **Operator** pourra : ajouter ou supprimer des règles de détection, consulter les journaux d'alertes générés, faire du scan de fichiers, observer la Smartmap ou encore avoir une vision sur les signatures Suricata dans la partie Sigflow.
- Le groupe **Administrator** pourra : mettre à jour le système d'exploitation, les logiciels, redémarrer l'équipement, éditer et consulter la configuration réseau, mettre à jour les interfaces de détection, consulter la version, les attributs, ajouter ou supprimer une sonde, activer ou désactiver l'envoi des informations techniques complémentaires aux opérateurs, activer ou désactiver le stockage des informations techniques complémentaires tout en définissant la durée, consulter l'ensemble des journaux de fonctionnement et d'alertes générés.

Chacune de ces informations est prise en compte après que l'administrateur ait sauvegardé les modifications en appuyant sur **Create**.

Ci-dessous, on retrouve la totalité des utilisateurs créés par l'administrateur de la solution avec les informations liées à chaque profil ('Enabled' étant l'état du profil, activé ou désactivé) :



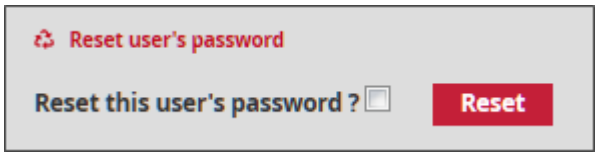
Le bouton **Edit** servira à l'édition du profil utilisateur en question. Différentes permissions sont possibles pour un utilisateur en fonction de l'appartenance du groupe. Il est possible de choisir d'attribuer les droits d'administration à un utilisateur en fonction de son rayon d'action.



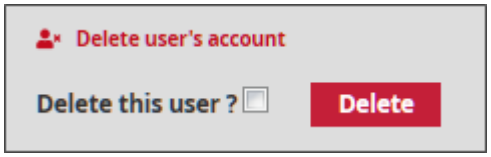
Account's information reprend les informations du profil utilisateur à savoir son numéro d'identifiant, son nom complet, sa date de création ainsi que la dernière fois qu'il s'est connecté à la plateforme de management **GCENTER**.

User's configuration permet de modifier l'adresse mail, le prénom et le nom du profil utilisateur. De plus les groupes créés par défaut respectant la Loi de Programmation Militaire apparaissent et peuvent être attribués ou pas au profil en cochant la case prévue à cet effet. L'administrateur peut activer ou désactiver l'utilisateur de la plateforme via l'option **Active**. La conséquence de cette action sera une impossibilité de connexion à l'interface **GCENTER**.

La prise en compte de toute modification ne sera effective qu'après avoir appuyé sur **Save**.



Reset user's password permet de régénérer le mot de passe associé au compte utilisateur en cas de perte ou d'oubli. La plateforme proposera un nouveau mot de passe pour s'identifier à nouveau une fois que le bouton 'Reset' soit sélectionné.

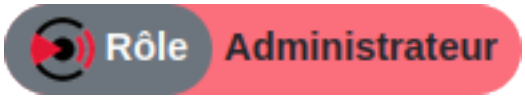


Dans **Delete user's account** , l'option **Delete** permet à l'administrateur de supprimer n'importe quel profil utilisateur de la plateforme.

L'interface d'administration permet donc de paramétrer entièrement les droits sur tous les niveaux de l'administration du **GCENTER**. Toute création d'un utilisateur, depuis le **GCENTER** , sera prise en compte par la sonde **GCAP** et l'utilisateur sera ajouté dans sa base de données.

Chapter 41

Intégration LDAP / ActiveDirectory

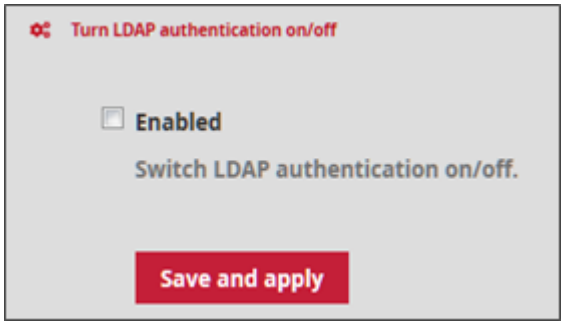


Menu : Administrators > GCenter > Accounts > LDAP Configuration

Le menu de configuration des comptes utilisateurs de la solution TRACKWATCH, permet d'utiliser le LDAP (Lightweight Directory Access Protocol) en tant que backend d'authentification plutôt que le backend interne.

Cette interface est utilisée pour gérer la connexion entre le **GCENTER** et un serveur LDAP/ActiveDirectory.

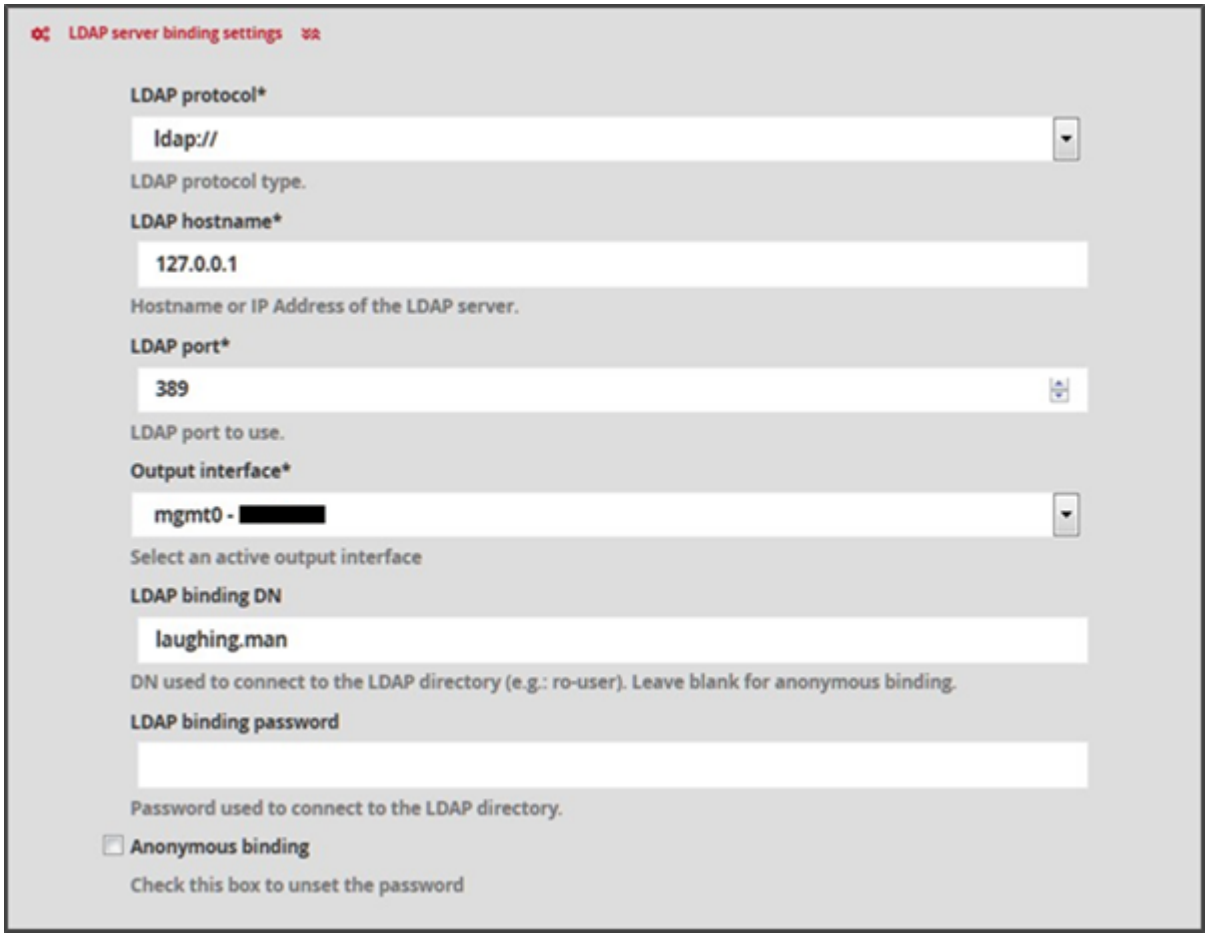
LDAP interconnection status permet de connaître facilement le statut de connexion.



Dans la section **Turn LDAP authentication on/off** cocher la case **Enabled** pour activer le service puis cliquer sur **Save and apply** pour prendre en compte la modification.

Sauvegarder et appliquer la nouvelle configuration de l'option LDAP provoquera un redémarrage de l'application et donc une coupure de connexion à la page des utilisateurs.

Une fois que l'administrateur a cliqué sur **Confirm**, il sera nécessaire de se reconnecter à l'interface. Avant cette manipulation, les options de connexion au serveur LDAP sont paramétrables dans la section **LDAP server binding settings** :



LDAP protocol : correspond au type de protocole d'authentification choisi : LDAP ou LDAPS

LDAP hostname : adresse FQDN complète ou l'IP du serveur LDAP/ActiveDirectory

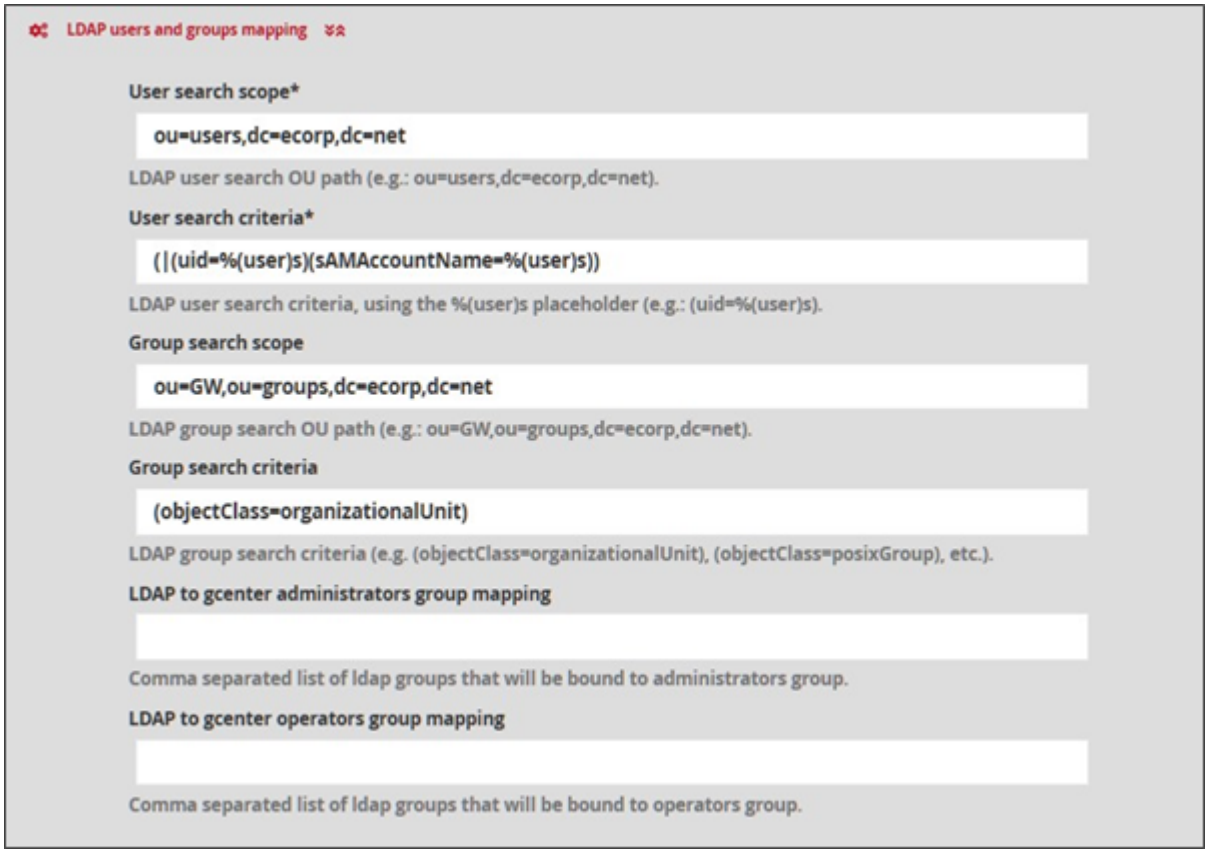
LDAP port : correspond au numéro de port du service LDAP. (Exemple : *389*)

Output interface : l'interface de sortie à utiliser pour joindre le serveur LDAP.

LDAP binding DN : correspond au DN (Distinguished Name) utilisé pour se connecter au répertoire LDAP. Laisser le champ vide si la liaison est anonyme. (Exemple : *CN=adro,OU=Service Accounts,OU=Example,DC=Example,DC=com,ro-user*)

LDAP binding password : mot de passe utilisé pour se connecter au répertoire. Laisser le champ vide si la liaison est anonyme.

Anonymous binding : permet de désactiver l'utilisation d'un mot de passe pour l'authentification.



La section **LDAP users and groups mapping** :

User search scope : OU (Unité d'Organisation) de base pour la recherche des utilisateurs (Exemple : *ou=users,dc=ecorp,dc=net*)

User search criteria : Critères de recherche de l'utilisateur LDAP, en utilisant l'espace réservé %(user) (Exemple : *(|(uid=%(user)s)(sAMAccountName=%(user)s))*)

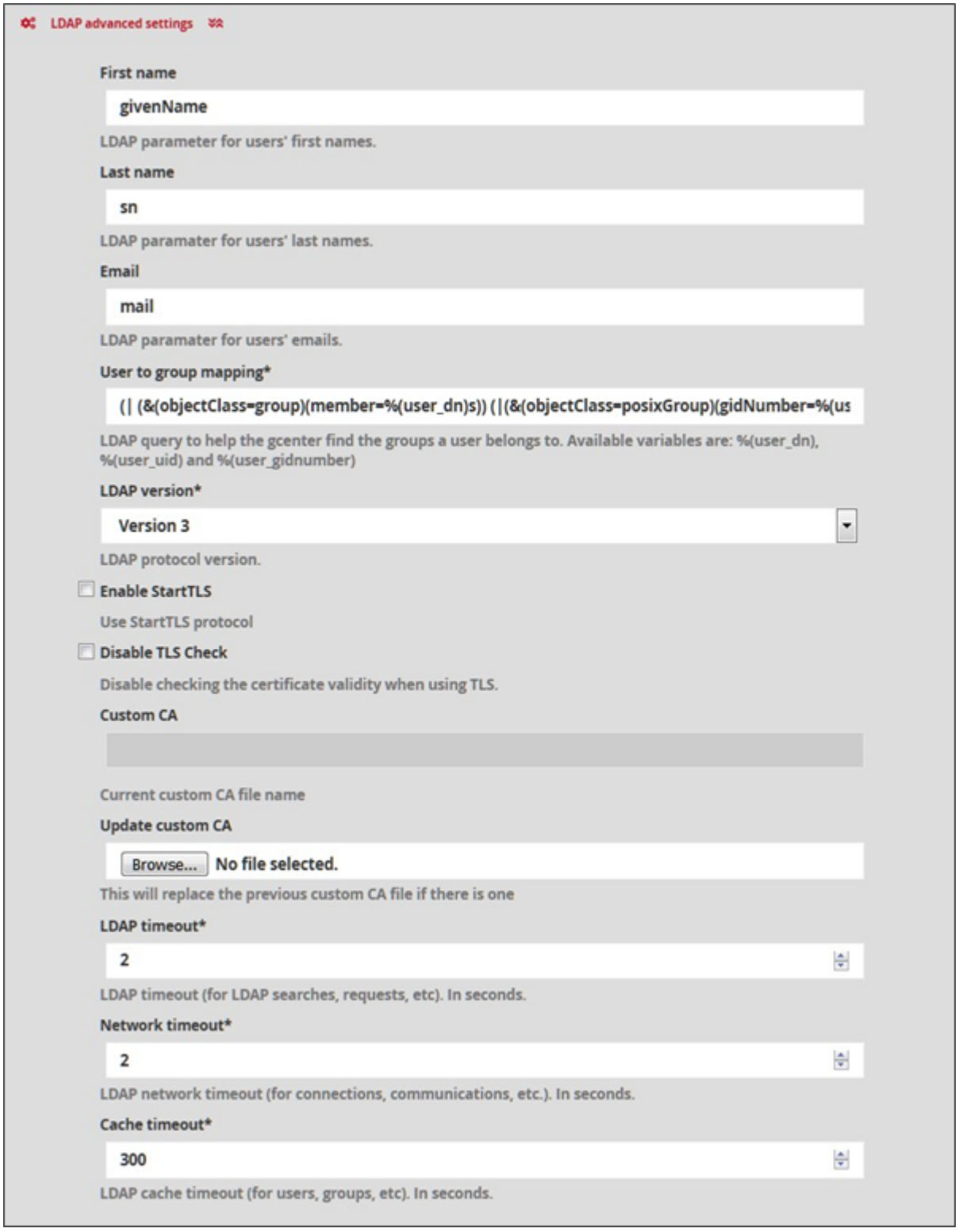
Group search scope : OU (Unité d'Organisation) de base pour la recherche des groupes (Exemple : *ou=GW,ou=groups,dc=ecorp,dc=net*)

Group search criteria : Critères de recherche des groupes LDAP, en utilisant l'espace réservé %(group) (Exemple : *(objectClass=organizationalUnit)*)

LDAP to GCENTER administrators group mapping : est une liste séparée par des virgules des groupes LDAP qui sont liés au groupe des administrateurs de la solution.

LDAP to GCENTER operators group mapping : est une liste séparée par des virgules des groupes LDAP qui sont liés au groupe des opérateurs de la solution.

La section **LDAP advanced settings** permet d'accéder aux options avancées du LDAP.



Les paramètres LDAP pour le prénom de l'utilisateur, le nom, le mail, le type, la version, le timeout du service (en seconde) après chaque requête, connexion, ou communication, sont modifiables depuis cette interface. Le temps avant le timeout (en seconde) du cache pour les utilisateurs ou les groupes est aussi paramétrable.

First name : paramètre LDAP correspondant au prénom de l'utilisateur (Exemple : *givenName*)

Last name : paramètre LDAP correspondant au nom de l'utilisateur (Exemple : *sn*)

Email : paramètre LDAP correspondant à l'adresse mail de l'utilisateur (Exemple : *mail*)

User to group mapping : requête LDAP pour aider le à trouver les groupes auxquels un utilisateur appartient.

Les variables disponibles sont : %(user_dn), %(user_uid) et %(user_gidnumber)

LDAP version : version LDAP à sélectionner (*Version2* | *Version3*)

Enable StartTLS : possibilité d'activer l'utilisation du StartTLS. Désactivée par défaut.

Disable TLS check : paramètre qui consiste à arrêter la vérification de la validité du certificat lorsque le service TLS est activé.

Custom CA : Information sur la CA personnalisée utilisé.

Update custom CA : remplacera le certificat de la CA personnalisée.

LDAP timeout : délai d'attente en secondes modifiable pour les recherches ou autres requêtes LDAP (Exemple : *2*)

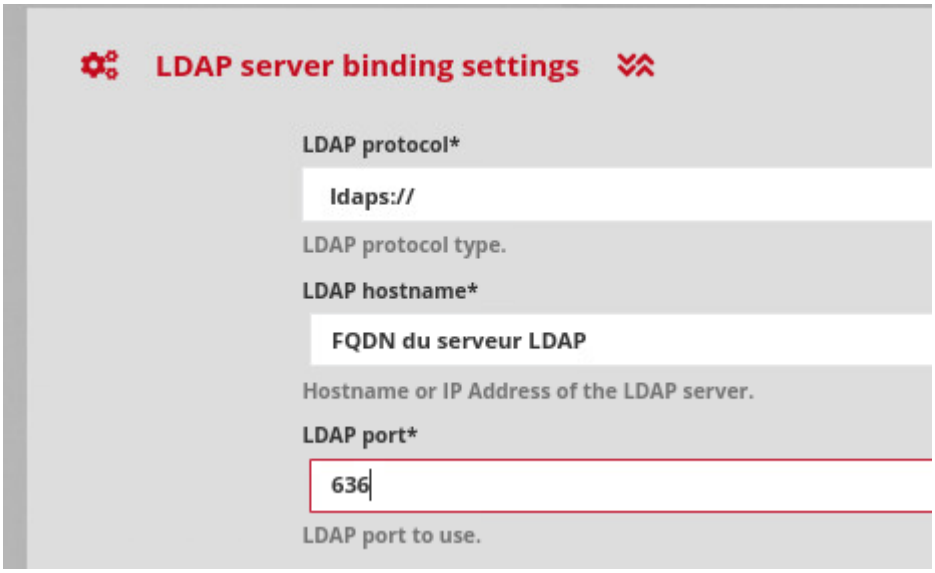
Network timeout : délai d'attente du réseau en secondes pour les connexions ou les communications (Exemple : *2*)

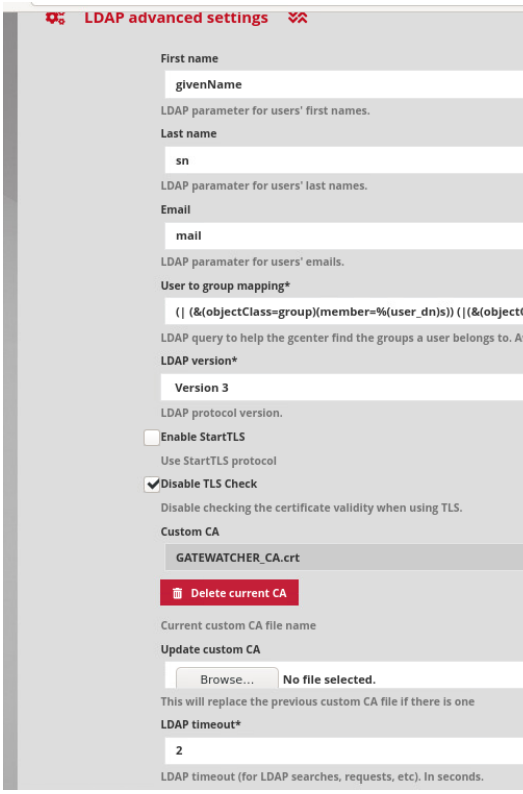
Cache timeout : délai d'expiration du cache LDAP en secondes pour les utilisateurs et les groupes (Exemple : *300*)

Pour une configuration de LDAPS :

Il faut, à partir de la configuration LDAP standard expliquée ci-dessus :

- Renseigner dans "LDAP server binding settings":
  - `LDAP protocol`: `ldaps://`
  - `LDAP_port`: `636`
- Renseigner le certificat de l'autorité de certification dans "LDAP advanced settings"

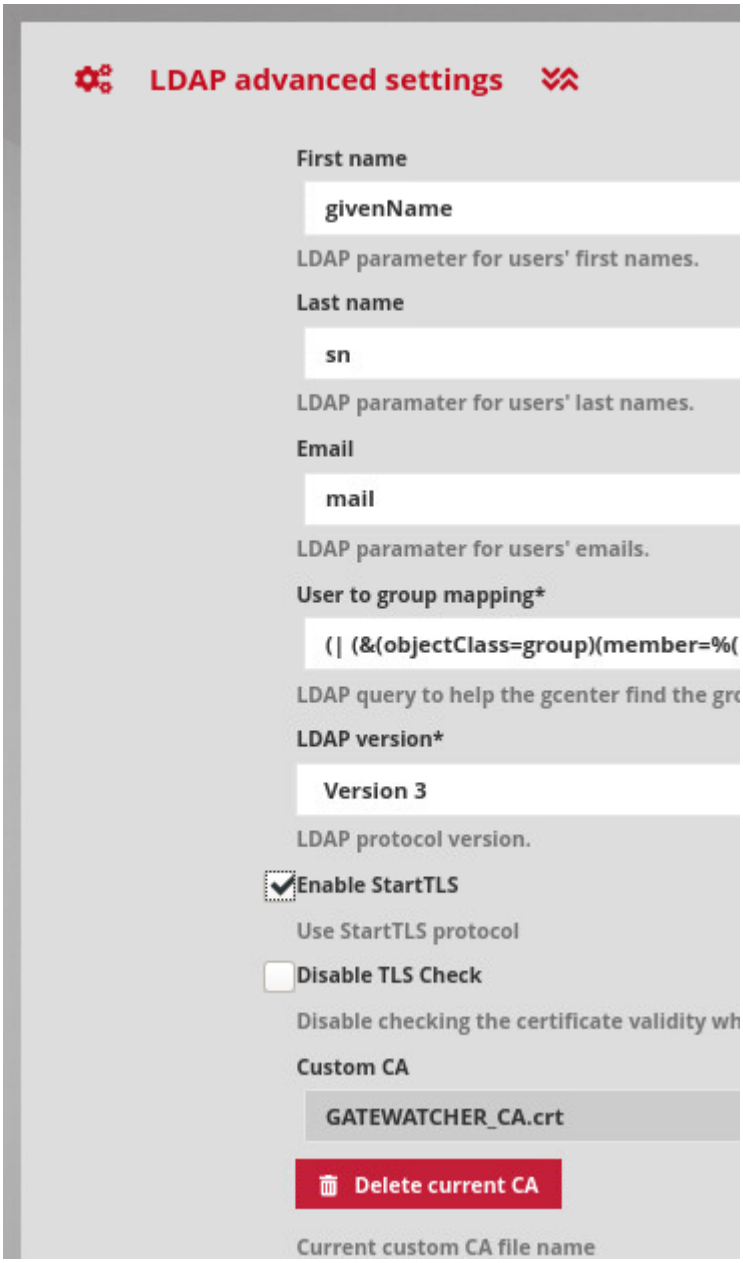




Pour une configuration de LDAP over TLS :

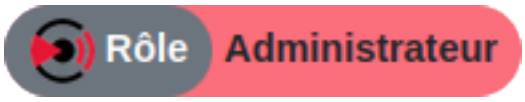
Il faut, à partir de la configuration LDAP standard expliquée ci-dessus :

- Renseigner le certificat de l'autorité de certification dans "LDAP advanced settings".
- Cocher la case "Enable StartTLS" dans "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 gr
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
Delete current CA
Current custom CA file name

Chapter 42

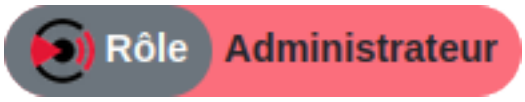
Audit trail



Menu : Administrators > GCenter > Accounts

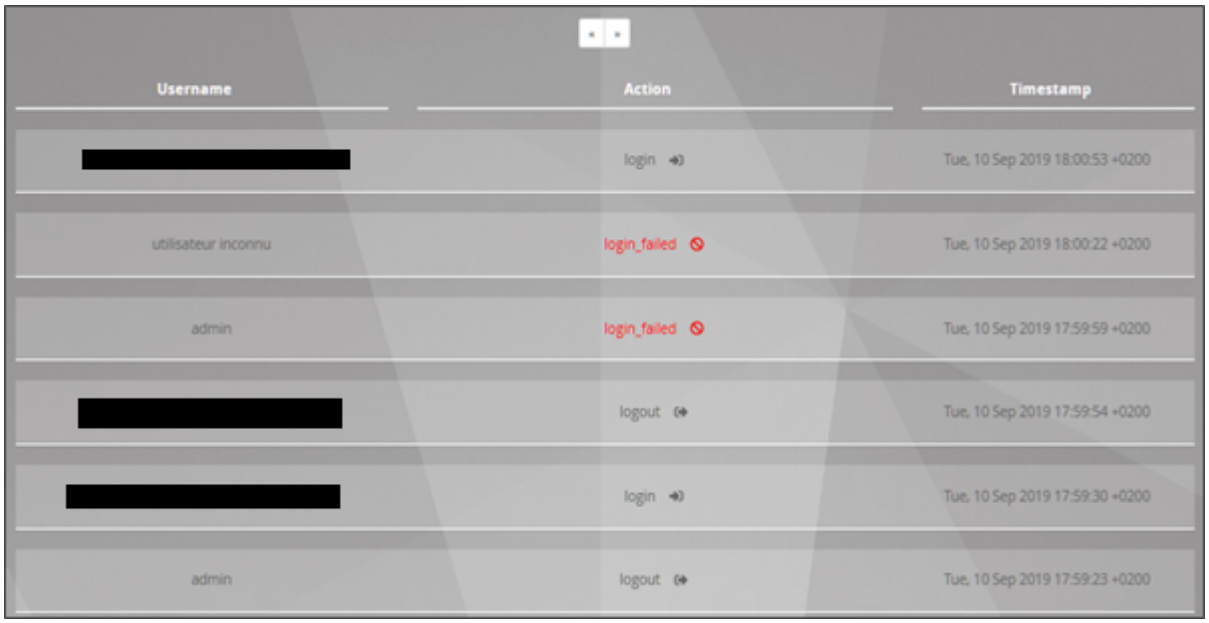
La solution TRACKWATCH va enregistrer les différentes actions effectuées sur l'ihm lié à la gestion des utilisateurs sur la plateforme de management au fil du temps, ceci afin d'en assurer la traçabilité. Cette traçabilité est effectuée aussi bien pour la connexion des utilisateurs que pour la création / suppression ou encore modification de permissions.

42.1 Authentications history



Menu : Administrators > GCenter > Accounts > Authentications history

L'historique de toutes les authentifications sur le **GCENTER** est disponible.

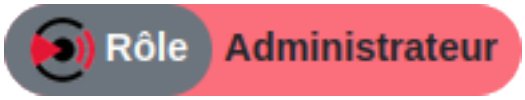


Un historique de connexion des logins utilisateurs sur la plateforme est présent sous forme d'un timestamp au format [**jour** , **xx mois année hh** : **mm** : **ss**].

Le nom de l'utilisateur sera visible :

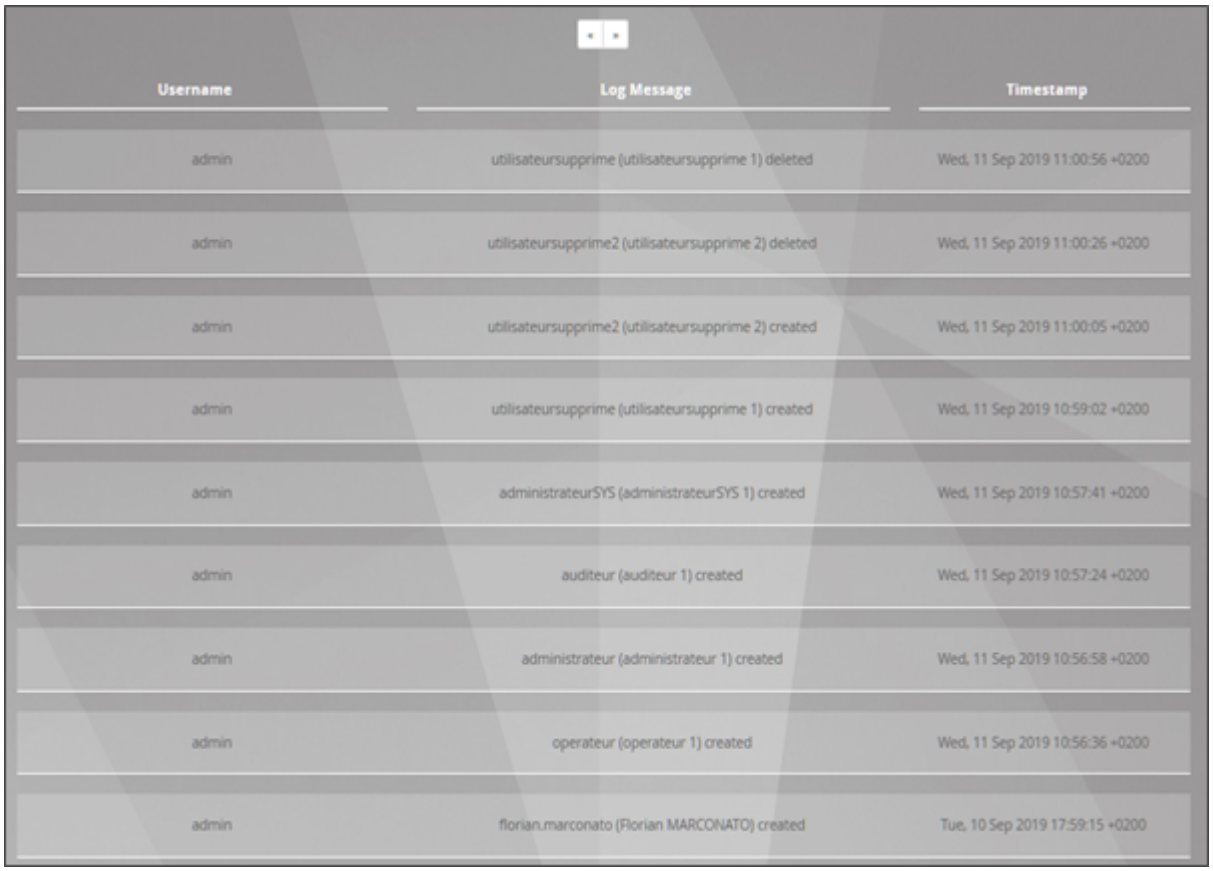
L'action faite par l'utilisateur apparaîtra :

42.1.1 Creations/Deletions history



Menu : Administrators > GCenter > Accounts > Creation/Deletion history

L'historique de toutes les créations ou suppressions des utilisateurs du **GCENTER** est disponible. On retrouve à ce niveau toutes les modifications faites par un compte administrateur de la solution sur un utilisateur.



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

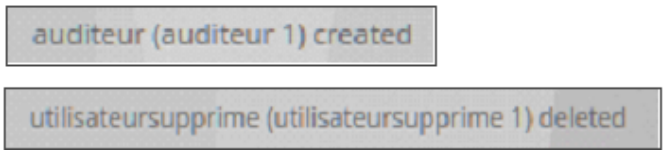
Dans la colonne **Username** le nom de l'administrateur responsable de l'ajout ou la suppression de l'utilisateur est visible.

Log message comporte plusieurs informations comme le nom de l'utilisateur et son action associée au compte (*created* ou *deleted*).

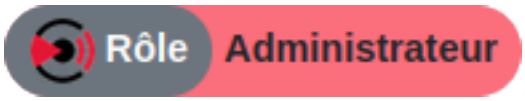
Un historique des créations et suppressions des logins utilisateurs sur la plateforme est présent sous forme d'un **Timestamp** au format [**jour** , **xx mois année hh** : **mm** : **ss**].

Le nom de l'utilisateur sera visible :

L'action faite par l'utilisateur apparaîtra :



42.1.2 Permissions history



Menu : Administrators > GCenter > Accounts > Permission history

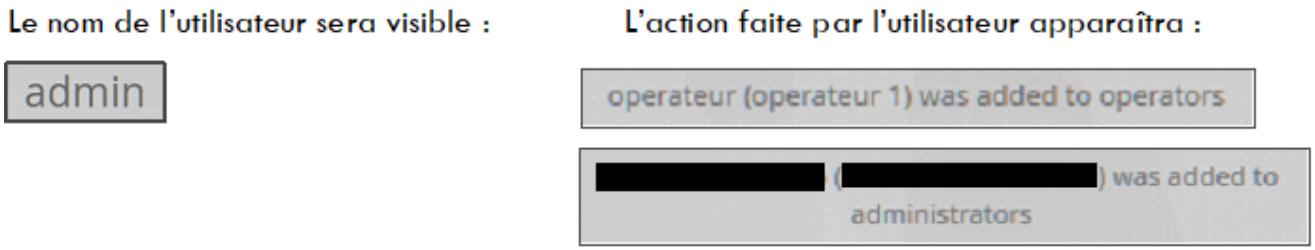
L'historique de toutes les permissions des utilisateurs sur le **GCENTER** est disponible. Toutes les modifications de droits sur un profil sont visibles via cette page.

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

Dans la colonne **Username** le nom de l'administrateur responsable de la modification du groupe de l'utilisateur est visible. A savoir que l'appartenance à tel ou tel groupe engendre des modifications de droit du profil utilisateur sur la plateforme.

Dans **Log message**, on retrouve plusieurs informations comme le nom de l'utilisateur et son action associée au compte (*was added to...*).

Un historique de l'attribution des droits sur les logins utilisateurs de la plateforme est présent sous forme d'un timestamp au format [**jour , xx mois année hh : mm : ss**].



La section **ADMINISTRATORS- Backup/Restore** du **GCENTER** permet de sauvegarder les données et d'effectuer une restauration de la configuration.

La sauvegarde du **GCenter** comprend :

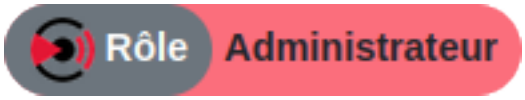
- les Rulesets *Sigflow* avec les modifications (suppress, threshold)
- les *profils des* ***GCAP***
- Toute la partie configuration du **GCenter** présente dans *Administrators* > *GCenter* y compris la licence

Note:

Dans le cas d'une réinstallation ou d'un reset du **GCenter**, il sera nécessaire de renseigner une licence afin d'accéder au menu **Restore**

Chapter 43

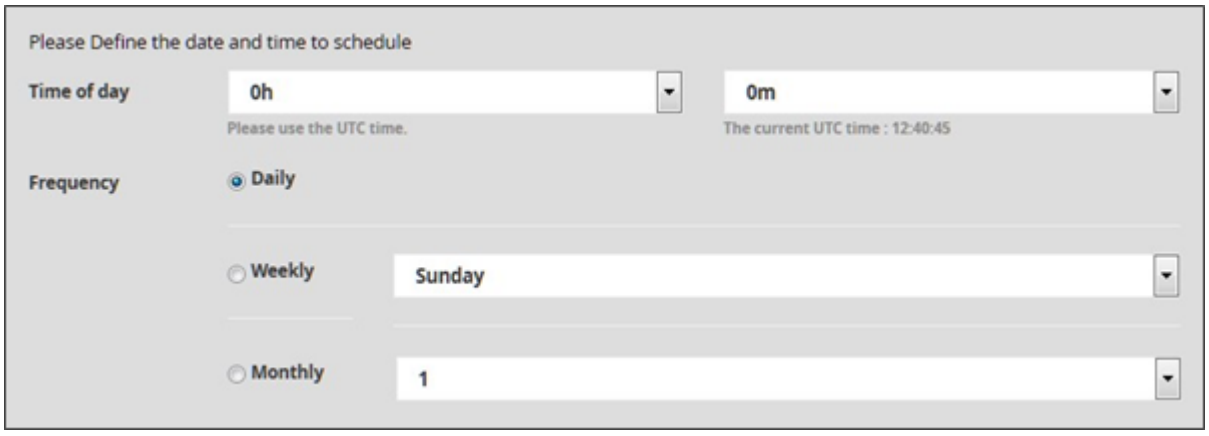
Configuration



Menu : Administrators > Backup / Restore > Configuration

L'administrateur de la solution TRACKWATCH peut décider à tout moment de faire une sauvegarde de la configuration.

Il peut également, s'il le souhaite, cocher la case **Enable scheduled backups**, afin de planifier les sauvegardes de manière régulière. Dans ce cas un menu se déroule et laisse la possibilité de configurer précisément le moment de la sauvegarde.

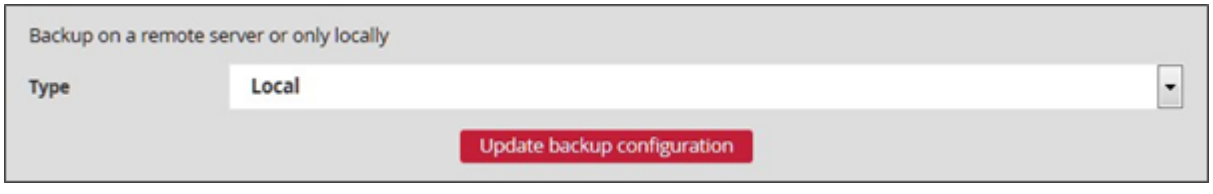


Time of day est le moment de la journée auquel le backup de la configuration du **GCENTER** sera lancé. La sélection de l'heure et des minutes se fait avec les menus déroulants associés.

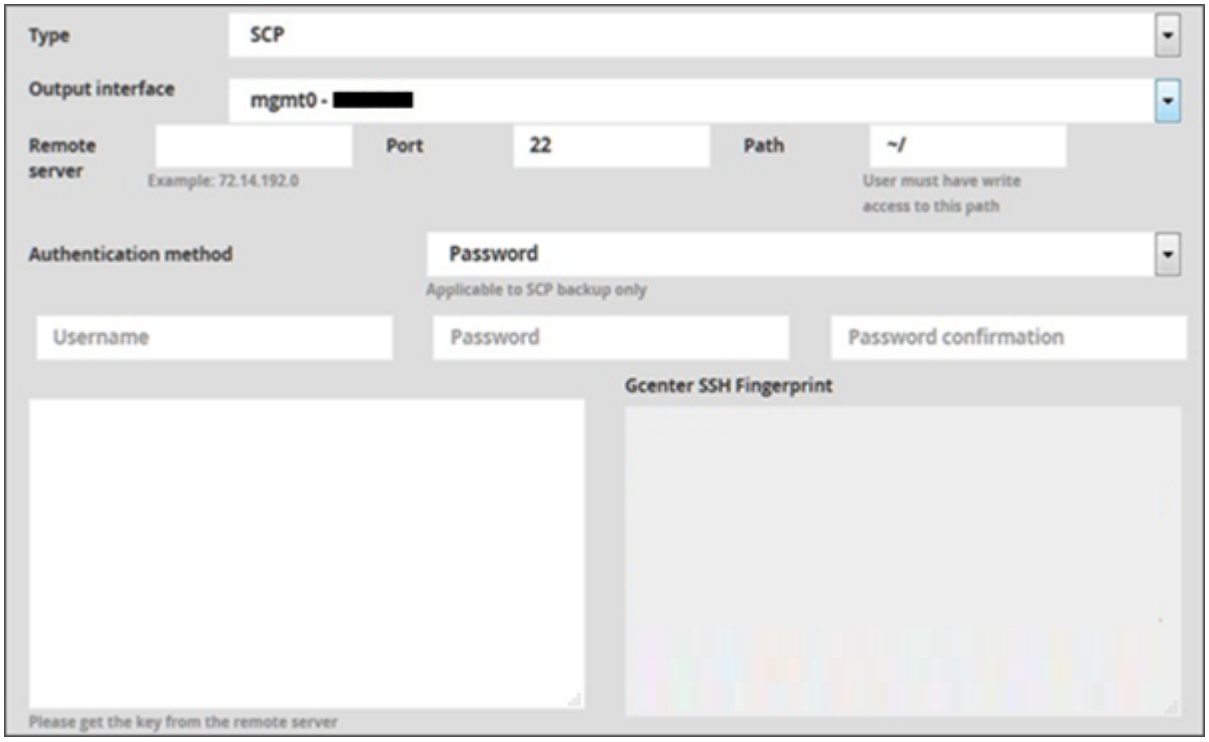
Frequency : permet de sélectionner la fréquence des sauvegardes de configuration. (*Daily*, *Weekly*, *Monthly*).

Une fois la partie planification optionnelle configurée il est nécessaire de choisir le type de sauvegarde souhaité. 3 types de sauvegarde sont disponibles :

- Local : la sauvegarde se fait uniquement en local, directement téléchargeable sur l'interface Web du **GCENTER** , au niveau de l'onglet Operations de la même partie.

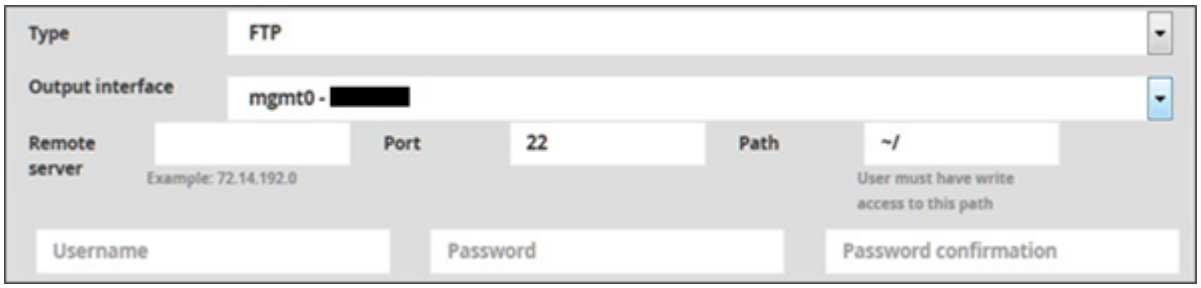


- SCP : permettant d'externaliser la sauvegarde sur un serveur SSH distant.



Remote server : est l'adresse IP ou le FQDN du serveur distant (Exemple : *72.14.192.0*) **Port** : est le port d'écoute du serveur SSH **Path** : est le chemin où sera sauvegardé le fichier sur le serveur distant (Le compte utilisateur utilisé devra avoir les droits en lecture/écriture sur ce chemin). **Authentication method** : Selon la méthode par mot de passe (*password*) ou par clé publique (*public key*), l'administrateur devra, en plus de renseigner le compte de connexion, respectivement fournir le mot de passe ou s'assurer que la clé publique du **GCENTER** (présente dans le champ **Gcenter SSH Fingerprint**) soit renseignée sur le serveur distant (en la plaçant dans le fichier : *~/.ssh/authorized_keys*).

- FTP : permettant d'externaliser la sauvegarde sur un serveur FTP distant.



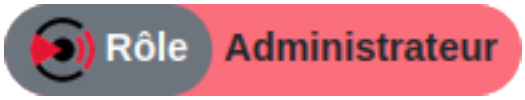
Remote server est l'adresse IP ou le FQDN du serveur distant (Exemple : *72.14.192.0*) **Port** : est le port d'écoute du serveur FTP '**Path** : est le chemin où sera sauvegardé le fichier sur le serveur distant (Le compte utilisateur utilisé devra avoir les droits en lecture/écriture sur ce chemin). **Username** : le nom d'utilisateur **Password** : le mot de passe de l'utilisateur.

Important:

À noter qu'il est nécessaire de modifier le range des ports passifs du serveur FTP avec les valeurs suivantes : [59000:59100] ; pour que le backup puisse se télécharger correctement.

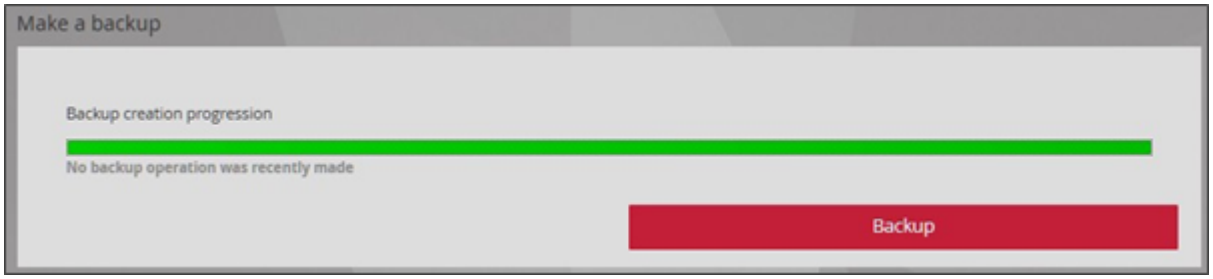
Une fois la configuration terminée il sera nécessaire de cliquer sur **Update backup configuration** pour enregistrer les modifications.

43.1 Operations



Menu : Administrators > Backup / Restore > Operations

Ce menu permet à l'administrateur de lancer le processus de sauvegarde de la configuration du **GCENTER** et/ou faire une restauration de la configuration grâce à un fichier de sauvegarde GATEWATCHER.

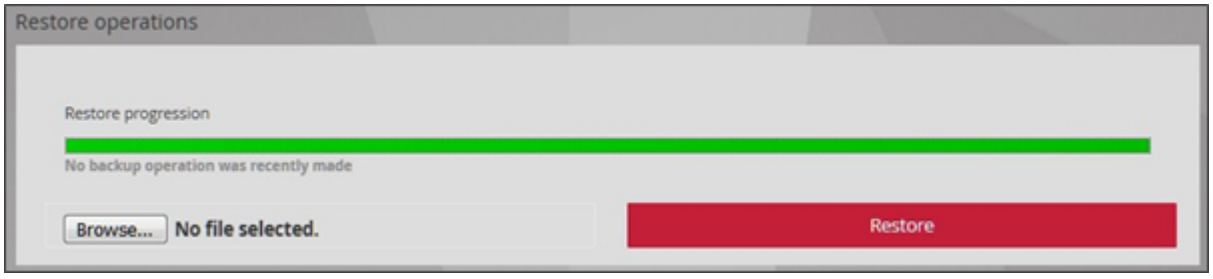


Backup va lancer le processus de backup de la solution. Suite à cette action, une archive '*NomDuGCENTER.local-backup.gwc*' de quelques gigabytes est téléchargée.

Les archives de backup qui sont déjà sauvegardées au préalable en local sur le **GCENTER** sont présentes dans ce menu.

Le fichier est téléchargeable depuis 'Download', l'horodatage de la dernière sauvegarde en UTC au format [**année/mois/jour hh** : **mm** : **ss**], le Shasum et la taille en MB et GB sont disponibles dans les colonnes respectives 'Backup', 'SHA256' et 'Size'.

Cette dernière est à enregistrer pour qu'elle soit envoyée aux administrateurs de la solution TRACKWATCH ou au support GATEWATCHER. En effet cette archive ne pourra être extraite que par un administrateur avancé ayant connaissance du mot de passe d'extraction des données backup.



Une fois extraite, l'administrateur pourra restaurer le système, depuis **Restore** dans un état de bon fonctionnement suite à par exemple un incident en important l'archive.

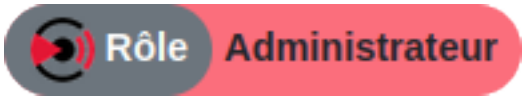
Chapter 44

Gestion des données

Pour que la solution TRACKWATCH puisse fonctionner correctement, le serveur **GCENTER** travaille avec des fichiers de logs. Ceux-ci recensent tous les échanges capturés par la sonde **GCAP** ainsi que les informations du GScan. Ces informations peuvent se multiplier rapidement et occuper une place importante sur le disque.

Bien qu'*une politique de rétention* soit en place, ces données peuvent, si le besoin s'en fait sentir, être supprimées à la main par l'administrateur à n'importe quel moment avant que la durée de rétention des données ne soit écoulée.

44.1 Data deletion



Menu : Administrators > GCenter > Data Management

Après une sauvegarde complète ou incrémentielle par la fonctionnalité de backup, les anciens logs se suppriment automatiquement, en fonction de la durée de rétention de données, libérant ainsi de l'espace disque.

On peut vider les tables d'informations des moteurs d'analyses MALCORE, CODEBREAKER, SIGFLOW et de la partie GSCAN comprenant les modules MALCORE et CODEBREAKER, sur une période donnée. Cette période est sélectionnée par l'administrateur, qui la valide en appuyant sur **Apply**, mais celle-ci ne pourra pas dépasser la durée totale de rétention des données déjà préconfigurées dans la solution. Il en va de même pour les services ICAP et Syslog.

```
important:: Les données n'ayant pas encore été traitées seront aussi supprimées.
```

Après avoir coché la ou les cases voulues sur une période de temps, l'administrateur doit valider l'action en cliquant sur **Envoyer**.

Chapter 45

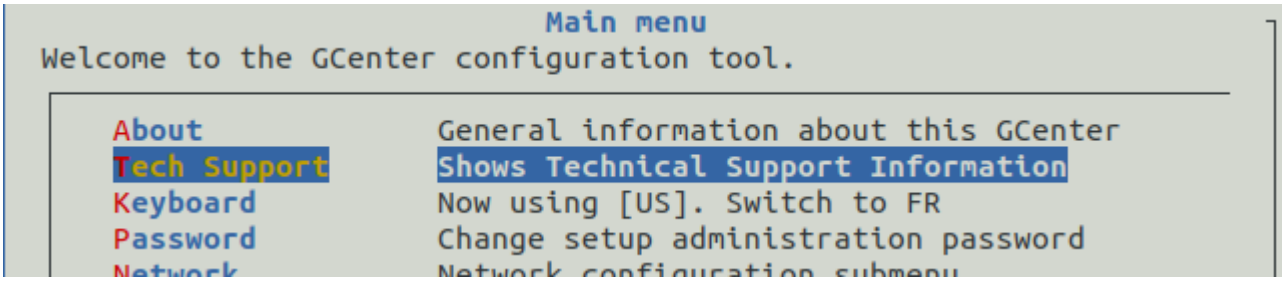
Diagnostiques

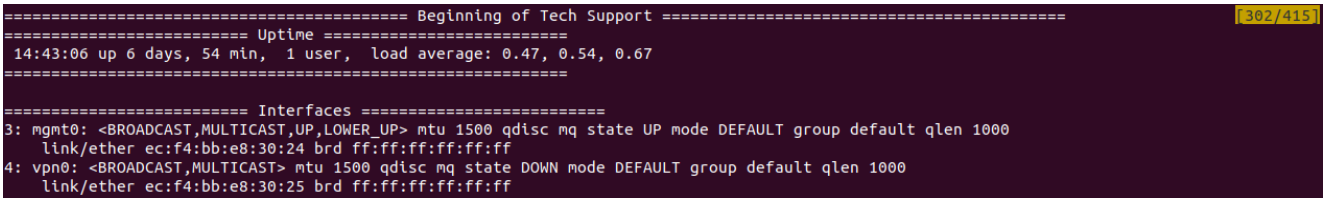
Cette partie de la section **ADMINISTRATORS** du **GCENTER** permet aux administrateurs de la solution TRACKWATCH de vérifier ou débugger certains paramètres de configuration. Elle permettra également au support GATEWATCHER d'identifier et de résoudre les potentiels dysfonctionnements.

Depuis cette interface de diagnostique, l'administrateur pourra exporter les paramètres de configuration du **GCENTER**:

Il est également possible depuis le menu *setup* de générer un "Tech Support".

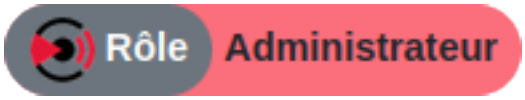
Pour cela il faut se connecter en SSH sur le **GCenter** en tant qu'utilisateur *setup*, puis sélectionner l'entrée *Tech Support*.





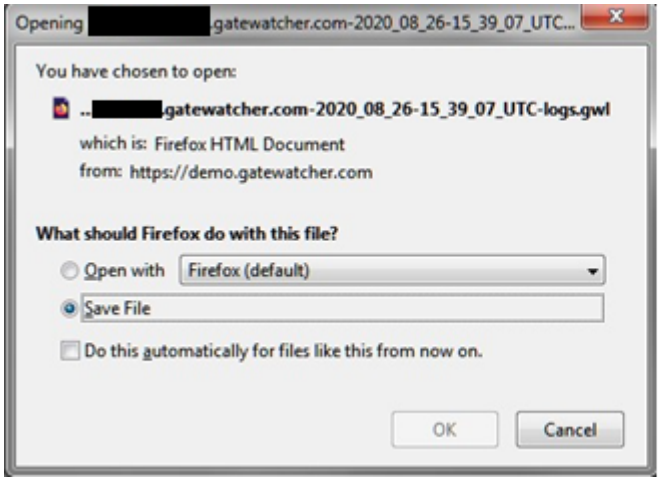
Cette commande permet de copier/coller un état de santé du Gcenter facilement.

45.1 Log files



Menu : Administrators > GCenter > Diagnostics

Des logs systèmes qui apporteront les détails de l'équipement **GCENTER** et de sa configuration pourront être exportés depuis cette interface. Cet export sera très utile pour l'équipe support GATEWATCHER pour tout type de diagnostics. Le fichier d'export de log est protégé par un mot de passe que seule l'équipe administrateur GATEWATCHER connaît.



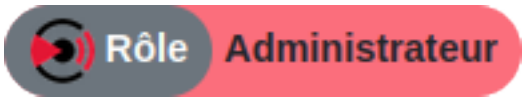
Suite à cette action, une archive '*GATEWATCHER_logs.gwp*' de quelques mégabytes est téléchargée. Cette dernière est à enregistrer pour qu'elle soit envoyée au support GATEWATCHER.

En effet cette archive ne pourra être extraite que par un administrateur avancé ayant connaissance du mot de passe d'extraction des données.

Une fois extraite, l'administrateur aura accès à l'ensemble des paramètres de configuration du serveur de management **GCENTER** et diagnostiquer l'éventuel problème. Les messages de tous les journaux seront accessibles ainsi que tous les appels systèmes de la solution.

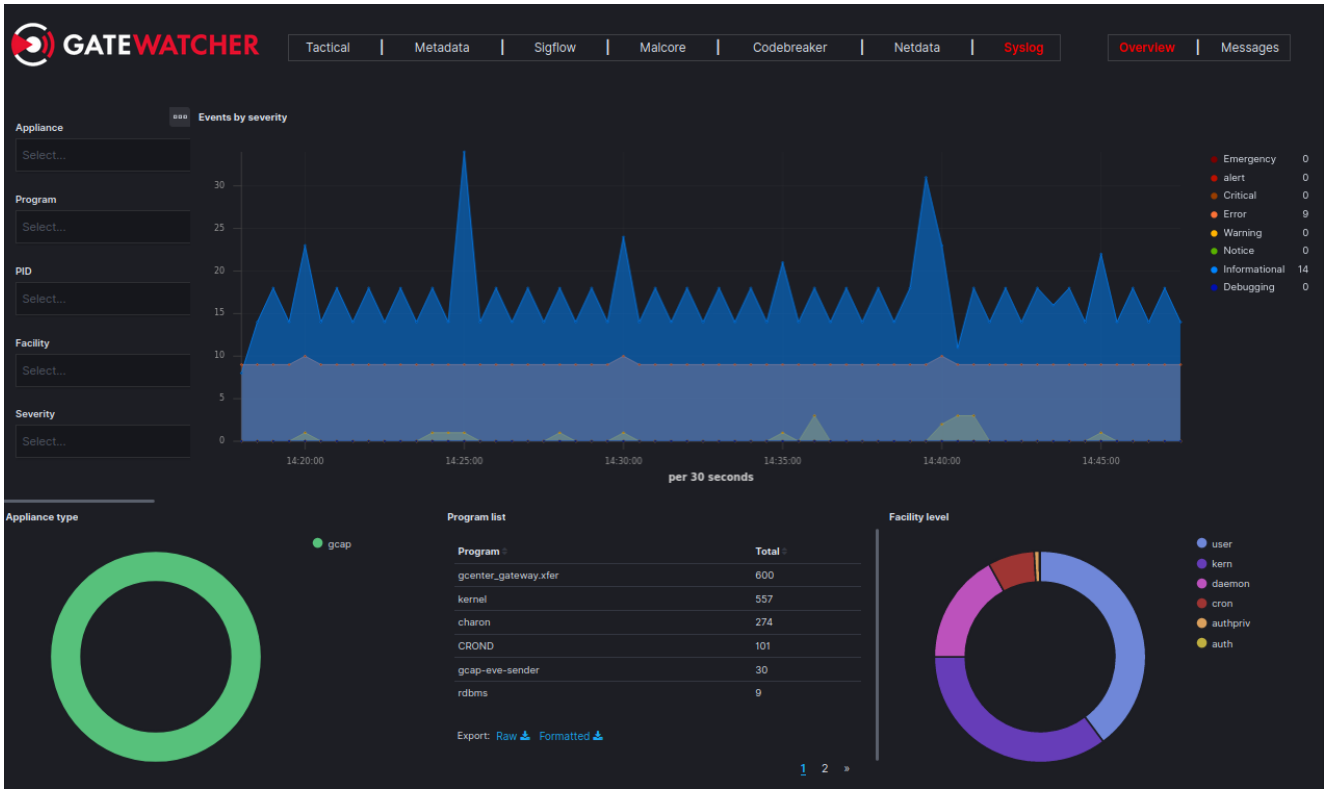
Chapter 46

Journaux de la solution

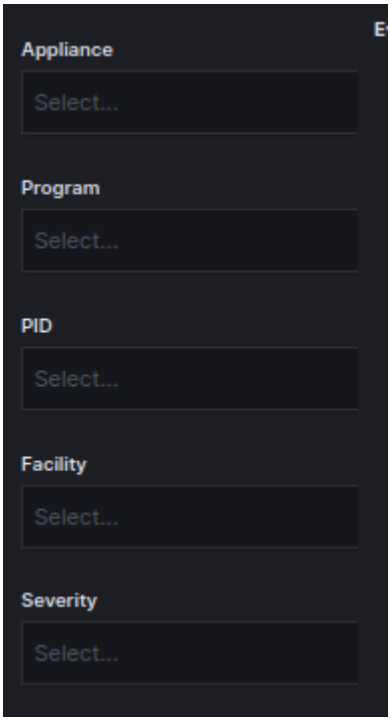


Menu : Administrators > GCenter > Trackwatch Logs

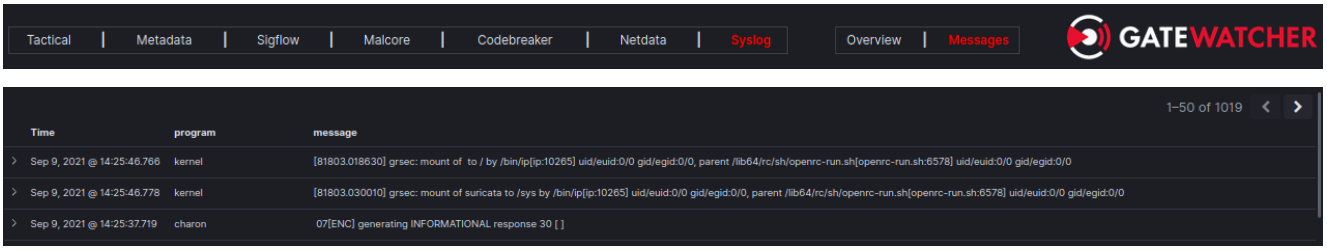
Cette entrée redirige sur un dashboard kibana contenant les différents logs de la solution TRACKWATCH.



Il est possible depuis ce tableau de bord de filtrer sur les différents champs depuis le menu de gauche



Le logs des différentes application étant affichés en base de l'écran overview, ou en cliquant sur la vue **Messages** .



Chapter 47

Emergency mode

Afin de préserver la capacité de détection de la solution, le **GCenter** peut passer dans un mode particulier appelé **Emergency Mode**.

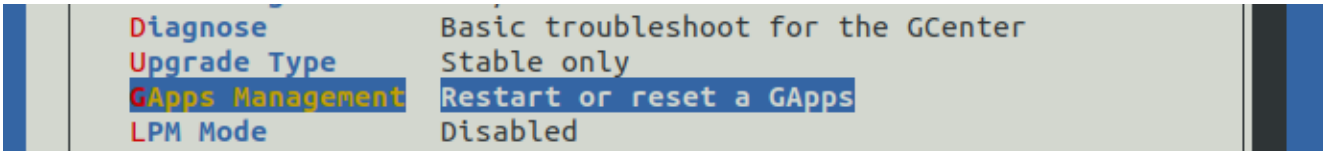
Ce mode se déclenche automatiquement dans le cas d'une utilisation importante de l'espace disque du **GCenter** utilisé pour stocker les données. Dans un tel cas, la solution appliquera automatiquement la procédure de *Data Deletion* afin d'assure une continuité des services de détection.

Chapter 48

Gestion des GApps

Les GApps représentent les différents services composant la solution TRACKWATCH. Il peut être nécessaire dans certains cas de devoir les redémarrer ou les réinitialiser.

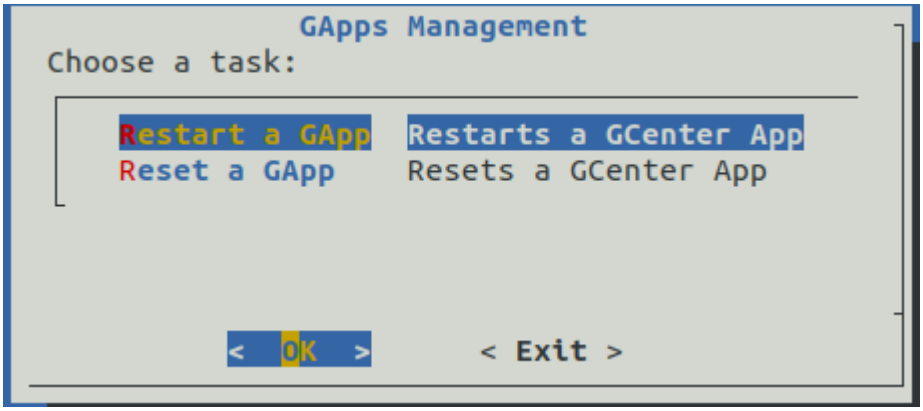
Pour cela, l'administrateur doit se connecter sur le GCenter en ssh en tant qu'utilisateur *setup*, puis sélectionner l'entrée *GApps Management*.



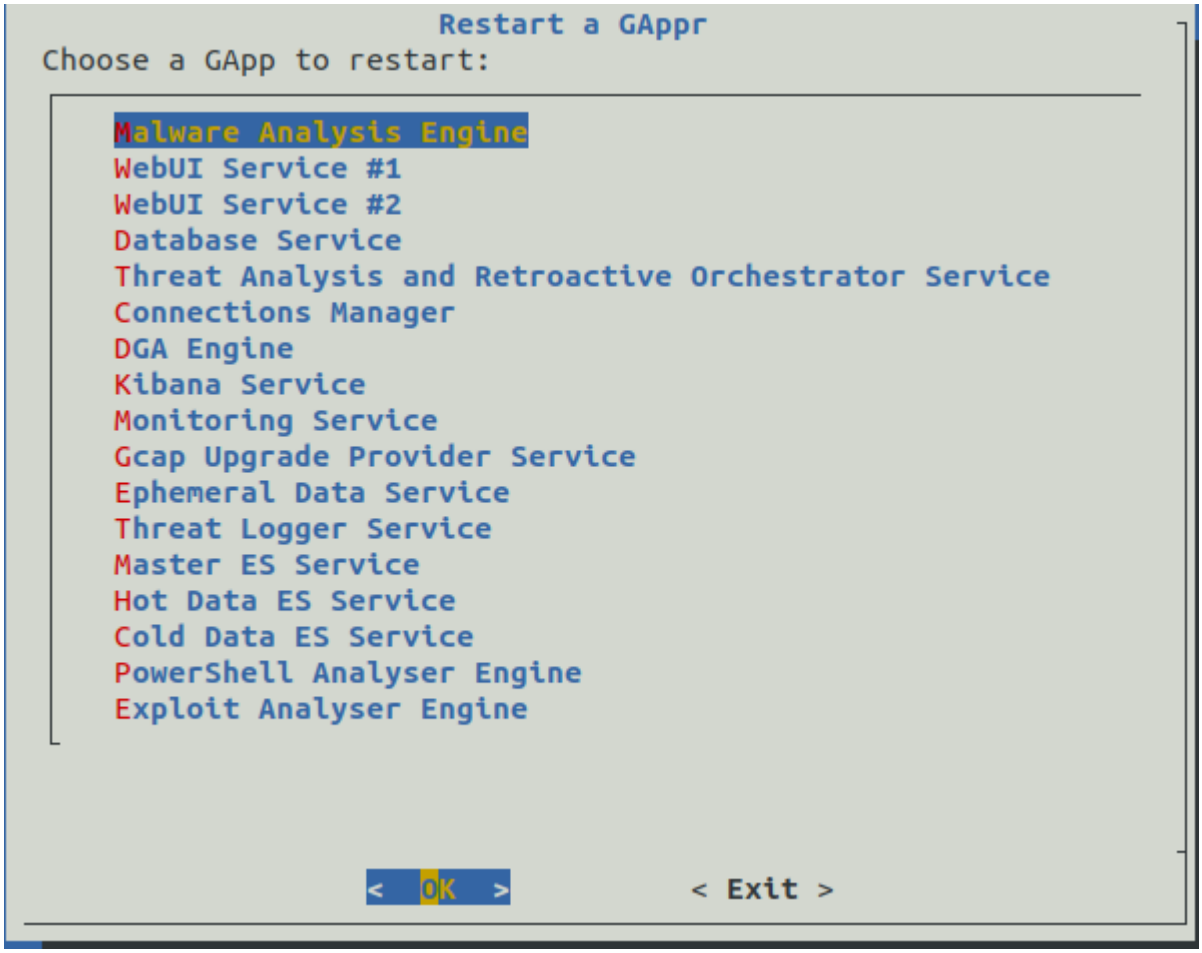
Ensuite, le choix est proposé de redémarrer un service ou de le réinitialiser.

Avertissement:

Réinitialiser un service revient à le remettre à sa configuration d'usine, il peut être nécessaire d'avoir à réappliquer certaines configuration ou update.



Enfin il suffira de sélectionner dans la liste le service à redémarrer ou réinitialiser.


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

LPM : rappels

Quelques rappels sur les grands principes de la LPM:

Loi de Programmation Militaire

- Loi n°2013-1168 du 18 décembre 2013

Article 22 : mise en application supervisée par l'ANSSI auprès des OIV

- Imposer des mesures de sécurité,
- Imposer des contrôles sur les systèmes d'information les plus critiques
- Rendre obligatoire la déclaration des incidents constatés par les OIV sur leurs systèmes d'information

Article L. 1332-6-1 du Code de la Défense modifié par LOI n°2015-917 du 28 juillet 2015 - art. 27

- Instaurer des mesures organisationnelles et techniques
- Définir des modalités d'identification et de notification des incidents de sécurité affectant les SIIV

Les objectifs sont de protéger les infrastructures vitales nationales contre les attaques informatiques, réduire l'exposition aux risques et optimiser la qualité des services fournis par les organisations.

Des exigences pour les OIV et les acteurs PDIS sont à prendre en compte sur les équipements **TRACKWATCH**:

- Mettre en place une politique de sécurité des systèmes d'information
- Conduire une homologation de sécurité
- Communiquer les éléments sur le SIIV mis en place par l'opérateur à l'ANSSI
- Observer les alertes de sécurité et réagir à celles-ci.
- Limiter les accès
- Cloisonner les réseaux
- Sélectionner les technologies qualifiées

Chapter 50

LPM appliqué au GCENTER

Nous aborderons ici les points de configuration spécifiques qui permettra à la solution TRACKWATCH d'être en conformité avec la Loi de Programmation Militaire.

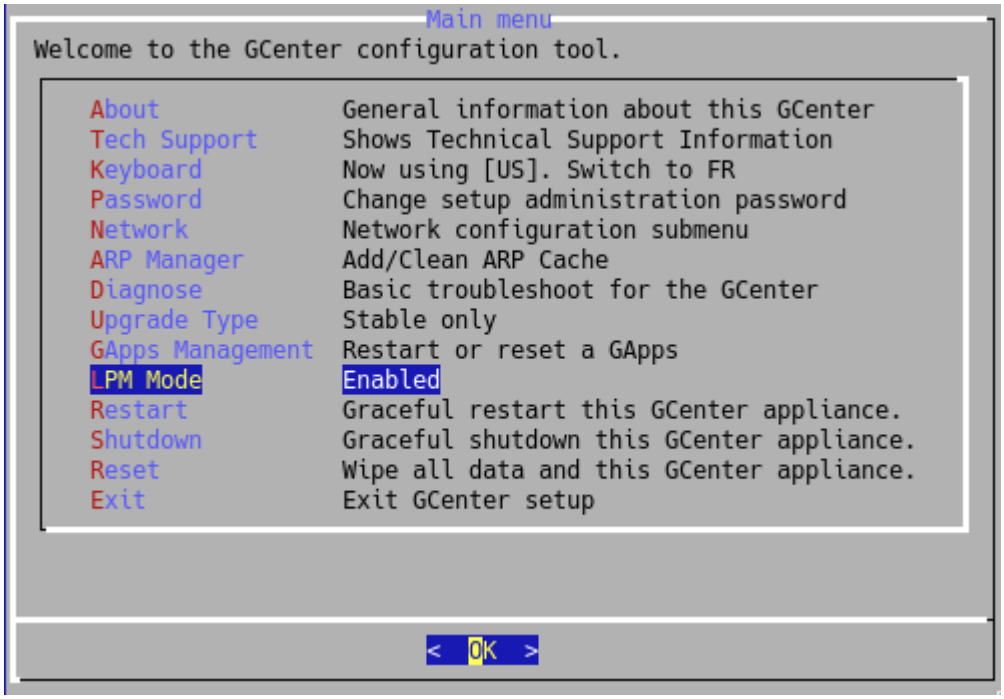
Bien qu'un certain nombre d'actions soient effectuées automatiquement lors du passage en mode LPM, l'administrateur devra personnaliser et modifier certains des paramètres manuellement:

- Durcissement (GRsec, binaires, PAX et modules) `action automatique`
- GScan `action automatique`
- AD/LDAP `action manuelle requise`
- Port USB `action automatique`
- Update Hors-ligne `action manuelle requise`
- Upgrade Hotfix `action automatique`
- Séparation des interfaces `action manuelle requise`
- Intégration du certificat `action manuelle requise`
- IDRAC Désactivé `action manuelle requise`
- Les groupes `action manuelle requise`

50.1 Action automatique

50.1.1 Durcissement (GRsec, binaires, PAX et modules)

Pour procéder au durcissement de l'équipement **GCENTER** et passer en mode LPM, il faut suivre la procédure suivante en se connectant à l'interface **SETUP**:



- Se connecter via le compte setup du **GCENTER** (SSH ou terminal)
- Sélectionner l'onglet 'LPM Mode' désactivé par défaut
- Valider le souhait de passer en mode LPM

L'équipement redémarrera alors avec la configuration correctement chargée.

Cela va permettre de réduire la surface d'attaque du **GCENTER** et ainsi de réduire le risque. En effet grâce à ce mode, il intègre les améliorations de GRSECURITY, dont PaX. Permettant ainsi de réduire la surface d'attaque y compris au niveau du noyau.

50.1.2 Service GScan

Dans la même optique, certaines fonctions sont désactivées. C'est le cas du service **GScan** qui est désactivé pour la détection de potentiels malwares ou shellcodes.

Cette fonctionnalité se désactive automatiquement après la validation du mode LPM dans le SETUP.

50.1.3 Port USB

Lorsque la solution **TRACKWATCH** est en mode LPM, les ports USB se désactivent automatiquement une fois le clavier (ou autre périphérique) débranché. Il faut alors redémarrer l'équipement **GCENTER** ou la sonde **GCAP** puis rebrancher, avant le démarrage, le périphérique afin que celui-ci soit pris en charge. Cette mesure limite l'accès au TTY de l'appliance.

La modification se fait automatiquement après le passage en mode LPM depuis le menu de configuration des paramètres du profil **SETUP**.

50.1.4 Upgrade hotfix

Dans le cadre d'un SI soumis à la LPM, le **GCENTER** ne pourra pas appliquer de modification de type *hotfix* appliquant des modification à la solution afin de corriger des problématiques mineures sur la solution sans redémarrage.

Ce paramètre *GUM* se désactive automatiquement après la validation du mode LPM dans le **SETUP**.

L'application des correctifs reste cependant possible via le processus d'*upgrade*.

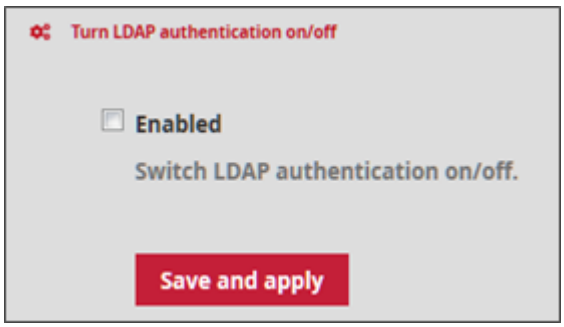
50.2 Action manuelle

La liste des actions ci-dessous sont à effectuer par un administrateur de la solution TRACKWATCH.

50.2.1 Compte AD/LDAP

Dans le cadre d'un SI soumis à la LPM, il y a certaines contraintes, notamment sur le fait que le **GCENTER** ne soit pas connecté avec un Active Directory ou un LDAP. Il faut vérifier que c'est bien le cas.

Pour cela il faut se rendre dans la section ADMINISTRATORS du **GCENTER** puis cliquez sur Accounts et LDAP configuration.



Décochez la case **Enabled** puis cliquez sur **Save and apply** pour prendre en compte la modification. Cette modification provoquera un redémarrage de l'application et donc une coupure de connexion à la page des utilisateurs. Une fois que l'administrateur a cliqué sur **Confirm**, il sera nécessaire de se reconnecter à l'interface.

Après cette manipulation, un bandeau vert valide la modification et la partie LDAP interconnection status indique que le **GCENTER** est à présent déconnecté de l'Active Directory ou du LDAP.

50.2.2 IDRAC Désactivé

La solution **TRACKWATCH** est installée sur des équipements de marque Dell et ce dernier offre la possibilité en temps normal de configurer une adresse IP indépendante de l'environnement de capture permettant la prise en main à distance. Ces interfaces de connexions sont nommées IDRAC par le constructeur de la marque. Il est préconisé selon l'ANSSI de les désactiver pour des raisons de sécurité évidentes. Mais elles peuvent être réactiver à tout moment par l'administrateur pour faciliter la maintenance.

50.2.3 Séparation des interfaces

Dans le cadre d'un SI soumis à la LPM, le **GCENTER** doit avoir une configuration spéciale de ses interfaces réseau. En effet afin de garantir cette conformité et un bon niveau de sécurité, le flux de management et celui des évènements générés par les sondes **GCAP**, doivent être sur deux interfaces différentes respectivement [MGMT0] et [VPN0].

Cette modification n'est pas effective automatiquement après l'activation du mode LPM, même si les câbles réseau sont correctement branchés. C'est justement depuis l'interface **SETUP** que l'administrateur peut effectuer la modification et rajouter manuellement une nouvelle adresse IP pour l'interface [VPN0]. Seules les interfaces [MGMT0] et [VPN0] sont impactées. Se référer au document de paramétrage du setup afin de procéder au changement.

Le détail des flux dans ce mode sont décrit dans la section Matrice de flux

L'envoi des logs vers un SIEM dans une zone d'exploitation se fera donc au travers d'une interface dédiée. Nous séparons l'interface de management (administrateur) de l'interface d'export des logs (opérateur).

Important:

En mode LPM, l'interface [ICAP0] est désactivée et l'interface [SUP0] doit être dans un réseau différent que [MGMT0].

50.2.4 Update Hors-Ligne

Pour que la solution **TRACKWATCH** puisse rentrer dans le cadre de la Loi de Programmation Militaire, les mises à jour des signatures doivent se faire en mode *Manuel* ou *Local*.

Il y a donc 2 possibilités:

- soit depuis l'interface Web du **GCENTER**, (voir la section *Mise à jour manuelle des moteurs* de ce document). Cela correspond à une mise à jour manuelle.
- soit via un emplacement sur le réseau, déconnecté d'internet. Cela correspond donc à une mise à jour *Locale* (voir la section *Mode local*).

50.2.5 Intégration du certificat

Afin de respecter les exigences particulières concernant l'utilisation de mécanismes cryptographiques, **GATEWATCHER** conseille de se référer aux documents écrits par l'autorité nationale en matière de sécurité et de défense des systèmes d'information.

La Loi de Programmation Militaire impose des règles et des recommandations concernant la gestion des clés utilisées, les mécanismes d'authentification, le choix et le dimensionnement des mécanismes cryptographiques. Tous ces prérequis sont disponibles dans le RGS Référentiel Général de Sécurité (RGS B1, RGS B2 et RGS B3) de l'ANSSI.

La section *SSL Settings*, indique comment ajouter votre propre configuration SSL.

50.2.6 Les groupes

Afin de respecter la séparation des rôles au sein de la solution TRACKWATCH, 2 profils sont disponibles.

L'administrateur système réalise plusieurs types de tâches. Des modifications de la configuration réseau, consultation, édition ou encore la mise à jour des règles de détection et des packages.

Le profil pourra ajouter, supprimer, éditer, activer, désactiver et consulter des informations relatives aux règles de détection. L'administrateur système gèrera (création, import, export, destruction) les éléments cryptographiques, consultera la version, les journaux d'alertes, fera les mises à jour systèmes et logicielles, aura une gestion des utilisateurs (création, suppression, modification des comptes associés aux rôles). En plus de pouvoir modifier les paramètres globaux du **GCENTER**, l'administrateur aura la capacité d'arrêter, de démarrer ou de redémarrer les fonctionnalités ou la solution en elle-même.

L'opérateur, consultera lui l'ensemble des journaux de fonctionnement et des alertes générées. De plus il pourra aussi activer ou désactiver le stockage des informations techniques complémentaires tout en définissant la durée.

Le profil pourra télécharger les données capturées, interagir avec la plateforme d'analyse et de téléchargement si configurée, scanner des fichiers, observer la SmartMap et surtout lire ou modifier des informations relatives aux règles de détection (ajout, suppression, actions particulières).

Dans l'interface d'administration du **GCENTER**, des groupes par défaut sont déjà créés afin de faciliter la gestion des utilisateurs du client.

La gestion des profils se fait depuis la *gestion des utilisateurs*.

Lien de téléchargement de cette documentation : `PDF Documentation GCenter`