Note de Version
GCenter Version 2.5.3.102

Version de la note : V3

Date de création : Janvier, 2023

Dernière mise à jour : Mai, 2023

Contents

Chapter 1

Présentation de la version 2.5.3.102 du GCenter

Cette note de version décrit :

- les nouvelles fonctionnalités et améliorations
- les correctifs
- les problèmes connus
- la comptabilité logicielle
- la compatibilité matérielle
- les hotfix
- la procédure de mise à jour

Chapter 2

Nouvelles fonctionnalités et améliorations

2.1 WebUI – Nouvelles interfaces NDR et options

2.1.1 Page d'accueil et tableau d'aperçu global

La nouvelle page d'accueil et le nouveau tableau d'aperçu global, présente une synthèse des risques stratégiques en se basant sur la chaîne de frappe et le référentiel MITRE.

2.1.2 Tableau de bord des alertes

Un nouveau tableau de bord est disponible et présente une synthèse des alertes classée par niveau de risque et agrégée par signature.

2.1.3 Tableau de bord des utilisateurs

Un nouveau tableau de bord est disponible et présente la liste des utilisateurs classée par niveau de risque.

2.1.4 Tableau de bord des hôtes

Un nouveau tableau de bord est disponible et présente la liste des hôtes classée par niveau de risque.

2.1.5 Cartographie des relations

En se basant sur les différents flux d'alertes, la solution est capable de générer dynamiquement une cartographie de l'environnement surveillé en affichant les utilisateurs, les hôtes, les risques associés et leurs relations.
Cette nouvelle visualisation permet d'identifier plus rapidement les principales menaces.

2.1.6 Tableaux de bord d'investigation

La navigation dans les tableaux de bord d'investigation a été revue, avec la création dynamique de filtres depuis les autres tableaux de bord pour faciliter la recherche des éléments.

2.1.7 Création de Tags

Il est possible de créer des tags et de les associer à des utilisateurs, hôtes et alertes.

2.1.8 Création de Notes

Il est possible de créer des notes et de les associer à des utilisateurs, hôtes et alertes.

2.1.9 Gestion des règles d'association

Un nouveau menu est disponible pour permettre de personnaliser les règles d'association lors de la découverte des utilisateurs et des hôtes.
Il est possible entre autres de définir les sous-réseaux d'adresses IP concernés, de faire des déclarations statiques ou bien encore des exclusions.

2.1.10 Limitation des métadata

Un nouveau menu est disponible pour permettre de limiter le volume de métadata indexé par le GCenter pour les protocoles suivants : DNS, HTTPS, HTTP, SMB.

2.1.11 Mode Sombre

La nouvelle interface graphique bénéficie de l'option « mode sombre ».

2.2 WebUI – Administration

2.2.1 Configuration des sondes GCap

Le paramétrage des GCaps a été simplifié pour définir les variables réseaux, les règles de fichiers, activer les différents protocoles qui seront analysés.

2.2.2 Menu Diagnostique

La génération du tech support est maintenant possible via la WebUI du GCenter (menu `` `Diagnostics` ``).

2.2.3 Menu de mise à jour

Dans la partie `` `GUM` ``, les menus `` `Hotfix` `` et `` `Upgrade` `` ont été fusionnés dans `` `Software update` ``.

2.3 Fonctionnalités d'analyste / CTI

2.3.1 Découverte des hôtes

Un nouveau mécanisme a été implémenté pour créer et maintenir une liste de tous les hôtes du réseau surveillé.
Cette découverte passive est réalisée grâce aux informations issues des différents protocoles analysés par le GCap.

2.3.2 Découverte des utilisateurs

Un nouveau mécanisme a été implémenté pour créer et maintenir une liste de tous les utilisateurs du réseau surveillé.
Cette découverte passive se base sur les informations du protocole Kerberos.

2.3.3 Calcul de risque agrégé par hôte

Pour chaque hôte, un calcul de risque est introduit en se basant sur les risques individuels (alertes) et le nombre de menaces uniques associées.

2.3.4 Calcul de risque unifié

Un nouveau module réalise le calcul du risque de chaque alerte déclenchée par les différents moteurs d'analyse et de détection.

2.3.5 Identification du type d'hôte

Un nouveau mécanisme a été implémenté pour identifier le type d'hôte (ordinateur, serveur, machine virtuelle, mobile, pare-feux...) du réseau surveillé.
Cette identification se base principalement sur l'analyse des user-agents et des adresses MAC.

2.3.6 Persitance et enrichissement de l'identité des hôtes

Les données relatives à la découverte des hôtes sont stockées et enrichies à travers le temps pour créer une synthèse pour chaque hôte.
Les principales informations disponibles sont :

- nom d'hôte
- adresse IP associée
- adresse MAC associée
- système d'exploitation
- protocoles utilisés et leur proportion
- détails des menaces détectées
- tactiques MITRE associées
- score du risque agrégé
- chronologie du score du risque
- top 10 des URLs visitées
- top 10 des adresses IP contactées
- tags
- notes

2.3.7 Persitance et enrichissement de l'identité des utilisateurs

Les données relatives à la découverte des hôtes sont stockées et enrichies à travers le temps pour créer une synthèse pour chaque utilisateur.
Les principales informations disponibles sont :

- nom d'hôte
- adresse IP associée
- vu pour la dernière fois
- protocoles utilisés et leur proportion
- détails des menaces détectées
- tactiques MITRE associées
- score du risque agrégé
- chronologie du score du risque
- top 10 des URLs visitées
- top 10 des adresses IP contactées
- tags
- notes

2.3.8 Interconnexion avec la CTI

Le GCenter est maintenant capable de recevoir directement les flux de la Cyber Threat Intelligence de Gatewatcher (nommée LastInfoSec/LIS) pour générer automatiquement de nouvelles règles de détection.

2.3.9 Retro-Hunting et CTI

Un nouveau moteur de retro-hunting réanalyse les métadata et communications passées en utilisant les nouveaux IOCs issus des flux de la CTI de Gatewatcher (LIS).

2.3.10 Redirection vers la plate-forme CTI

Il est possible en cliquant sur une alerte d'être redirigé vers le portail web de la plate-forme CTI de Gatewatcher (LIS) et d'effectuer une recherche automatique pour essayer d'obtenir des informations complémentaires à propos de l'alerte initiale (à noter qu'une licence spécifique LIS est requise pour activer cette fonctionnalité).

2.3.11 Alertes : aide à l'investigation et à la réponse

Lorsque l'on clique sur une alerte, plusieurs actions sont proposées :

- redirection vers différents tableaux de bord pour l'investigation
- téléchargement des fichiers (échantillons)
- affichage de détails sur la menace
- envoi de l'échantillon vers une sandbox
- téléchargement du rapport généré par la sandbox

Les actions sont contextualisées et dépendent du contenu de l'alerte.
Dans le cas d'une redirection vers un tableau de bord pour l'investigation, un filtre est créé automatiquement avec les éléments de l'alerte pour améliorer l'expérience utilisateur et le temps d'analyse.

2.3.12 Association au référentiel MITRE ATT&CK

Chaque alerte est associée automatiquement avec les tactiques et techniques du référentiel MITRE.

2.4 Détection

2.4.1 Moteur de détection DGA

Une nouvelle version de notre moteur de détection de DGA (Domain Generated Algorithm) est disponible avec :

- une optimisation de l'algorithme afin de réduire les faux positifs
- des événements dédiés aux DGA (avec les alertes que l'on retrouve dans le type « C&C »)
- la possibilité d'ajouter des domaines dans une liste blanche ou liste noire depuis une alerte générée

---

2.4.2 Moteur de détection Shellcode

Le moteur de détection Shellcode (Goasm) a été amélioré :

- ajout de quota et de nettoyage automatique pour éviter la saturation
- optimisation du code pour augmenter la stabilité et la performance
- nouvelles fonctions Windows ainsi que des correctifs implémentés
- le hash (sha256, md5) dans les alertes ne correspond plus au contenu du « .data », mais aux résultats de l'analyse (permet de reconnaître des shellcodes identiques dans des trames réseau différentes)
- les alertes de type Shellcodes possèdent une action « Display Data » pour afficher le hexdump du « .data »

2.4.3 Moteur de détection Powershell

Le moteur de détection Powershell (Gps) a été amélioré :

- ajout de quota et de nettoyage automatique pour éviter la saturation
- optimisation du code pour augmenter la stabilité et la performance
- amélioration de l'extraction, de l'analyse et du scoring pour réduire les faux positifs
- le hash (sha256, md5) dans les alertes ne correspond plus au contenu du « .data », mais aux résultats de l'analyse (permet de reconnaitre des commandes powershells identiques dans des trames réseau différentes)
- les alertes Powershell possèdent une action « Display Data » pour afficher le hexdump du « .data »

2.4.4 Moteur de détection Malcore

Le moteur de détection Malcore a été amélioré :

- ajout d'un orchestrateur pour détecter des pannes et réaliser des actions automatiques afin de les corriger
- activation des 16 moteurs de détection si la licence le permet
- amélioration du contenu des alertes et métadata qui sont maintenant extraites du fileinfo

---

2.4.5 Règles Yara

Des règles Yara peut être ajoutées au moteur Malcore pour améliorer la capacité de détection.

2.4.6 Amélioration du traitement des fichiers suspicieux

Une nouvelle option est disponible dans la chaîne d'analyse afin de marquer les fichiers suspicieux pour qu'ils soient automatiquement réanalysés à la prochaine mise à jour des moteurs et cela jusqu'à que ces fichiers ne soient plus détectés comme suspicieux.

2.5 API

2.5.1 API et Swagger

La majorité des interactions possibles avec la solution est réalisable au travers de l'API.
Plus de 200 points d'API sont disponibles, décrits grâce à Swagger et testables au travers de la WebUI du GCenter (URL: https://FQDN//docs/swagger/).

2.6 Système

2.6.1 Changement du système d'exploitation

Une refonte complète du système d'exploitation du GCenter a eu lieu en V2.5.3.102.

2.6.2 Mise à jour du noyau

Le noyau du système d'exploitation a été mis à jour avec la dernière version LTS (Long-Term Support).

2.6.3 Optimisation de la communication entre le GCap et le GCenter

Un nouveau composant gère la communication entre la sonde et le manager.
Le mécanisme de transmission des fichiers a été optimisé (nouveau protocole de communication, base de données pour les fichiers reçus...).

2.6.4 Refonte du mécanisme de traitement des fichiers

Une refonte complète du mécanisme de traitement des fichiers a été implémenté pour :

- fiabiliser l'enrichissement
- avoir l'intégralité des informations liées à un fichier reconstruit
- pourvoir systématiquement retrouver un fichier à partir d'un flow-id

---

2.6.5 Base de données pour le NDR

Une nouvelle base de données a été créée pour stocker les données relatives au NDR (utilisateurs, hôtes, alertes, risques...).

2.6.6 Amélioration des mises à jour

Des améliorations ont été apportées dans le mécanisme de mise à jour de la solution.

2.6.7 Optimisation des performance pour l'accès aux données liées aux évènements

Une refonte complète de l'architecture pour le traitement et le stockage des données liés aux évènements a été réalisée.
Elle permet d'optimiser les temps de réponse et limiter les problèmes liés à un nombre trop important de données stockées.

2.6.8 Netdata : augmentation de la durée de rétention

La durée de rétention des métriques remontées via Netdata a été augmentée.

2.6.9 Licences

Un nouveau système de licences plus granulaire est disponible.

Chapter 3

Correctifs

3.1 Statut des dernières mises à jour

Lors de la restauration d'un GCenter, l'information liée à l'état des mises à jour (update) des signatures sur les GCaps n'est pas restaurée.
Le statut se mettra à jour lorsque le GCap récupérera un nouveau fichier de règles.

Ce problème est corrigé en V2.5.3.102.

3.2 Appairage à un GCap impossible si aucune passerelle n'est renseignée pour l'interface VPN

L'appairage entre le GCenter et le GCap échouera si aucune passerelle par défaut n'est renseignée lors de la configuration réseau de l'interface *mgmt0* du GCenter.
Le message d'erreur renvoyé par le GCap lors du pairing est `Can't connect to \<Gcenter IP\>`.
Cela se produit même si le GCap et le GCenter sont dans le même sous-réseau et qu'aucune passerelle par défaut ne devrait être nécessaire.

Ce problème est corrigé en V2.5.3.102.

3.3 Appairage à un GCap impossible après changement de la configuration réseau du GCenter

Suite à une reconfiguration des paramètres réseau de l'interface VPN du GCenter (ex : IP, subnet, FQDN), il est possible que le ré-appairage avec un GCap précédemment appairé ne fonctionne plus.
Lors de l'appairage, le GCap indique le message d'erreur suivant : `pairing not established`.

Ce problème est corrigé en V2.5.3.102.

3.4 Règles LastInfoSec

Incohérence entre les règles LIS et le fichier généré, il manque les règles avec les hashs.

Ce problème est corrigé en V2.5.3.102.

3.5 Moteur Machine Learning et édition CIE

Les tableaux GATEWATCHER du moteur de Machine Learning ne prennent pas en compte la restriction de licence lorsque le GCenter est une édition CIE.

Ce problème est corrigé en V2.5.3.102.

3.6 Export Netdata - Incompatibilité avec des versions Netdata supérieures à 1.19

L'export des statistiques de monitoring GCap/GCenter vers un Netdata externe n'est compatible qu'avec un serveur Netdata dont la version est égale ou inférieure à 1.19.
Dans les versions supérieures, les données sont bien exportées et requêtables au sein du Netdata externe, mais une erreur au niveau de l'interface graphique se produit et il est impossible de visualiser les données.
Cela n'impacte pas le GCenter, seulement le serveur Netdata externe.

Ce problème est corrigé en V2.5.3.102.

3.7 GScan - Edition *Critical Infrastructure Edition* (CIE)

La fonctionnalité GScan ne prend pas en compte la restriction de licence lorsque le GCenter est une édition CIE.

Ce problème est corrigé en V2.5.3.102.

3.8 DGA - Champ non présent

L'absence du champ `dga_probability` dans les events se fera si les conditions suivantes sont réunies :

- l'activation du logging sur les event-type DNS
- l'activation du module de Machine Learning DGA Detection
- une charge réseau DNS importante

Ce problème n'est plus visible car en V2.5.3.102 il existe des évènements dédiés pour le DGA.

3.9 Third Party - Intelligence

La configuration d'interconnexion avec intelligence lève une erreur 500 si le token est erroné.

Ce problème est corrigé en V2.5.3.102.

3.10 Kibana - Tableaux inaccessibles

Les tableaux KIBANA peuvent ne pas s'afficher suite à un redémarrage sur GCenter et/ou de l'interface WEB.
Le message d'erreur affiché est `Elastic dit not load properly. Check the server output for more information`.

Ce problème est corrigé en V2.5.3.102.

3.11 Kibana - « Not ready yet »

Dans certains cas particuliers, une défaillance du système de rotation des logs peut entraîner la saturation de la partition /var/log/.
Cela se traduit au niveau de Kibana par un message d'erreur de type `not ready yet`.

Ce problème est corrigé en V2.5.3.102.

3.12 Malcore Management - GScan Profile

L'option `Number of files` du profil GScan de Malcore Management permet de retourner une alerte en fonction du nombre de fichier présent dans l'archive.
Cette fonctionnalité n'est pas opérationnelle.

Ce problème est corrigé en V2.5.3.102.

3.13 Malcore - Status healtcheck erroné en licence *Critical Infrastructure Edition* (CIE)

L'état de santé du moteur Malcore peut être affiché de manière erronée au niveau de la page d'accueil, dans global **status/healthcheck**.
Cela peut se produire lorsque le GCenter fonctionne avec la licence **CIE** : le healtcheck peut alors afficher `Malware Analysis engine has one or more issue`, même si le moteur est fonctionnel.

Ce problème est corrigé en V2.5.3.102.

3.14 Malcore - Absence de flow_id

Dans de rares cas, le champ `flow_id` d'une alerte Malcore peut ne pas apparaître.
La corrélation avec les métadata relatives à cet événement Malcore peut être faite à l'aide des SHA256 et `timestamp_detected` de l'alerte Malcore.
A partir de la version 2.5.3.101-HF2 si le `flow_id` est absent, celui-ci est définis à 0, permettant l'export des alertes.

Ce problème est corrigé en V2.5.3.102.

3.15 Malcore - Doublon d'analyse

Des doublons d'analyse Malcore peuvent apparaître lors des opérations de shrinking de la base de données elasticsearch.
Ces opérations ont lieu tous les jours à 02:00 UTC et visent à optimiser la consommation mémoire d'elasticsearch en réduisant le nombre de shards par index.

Ce problème est corrigé en V2.5.3.102.

3.16 Malcore - Crash du moteur suite à une surcharge

Le moteur Malcore peut devenir instable s'il est soumis à une charge extrême et que des centaines de milliers de fichiers sont en attente de traitement.
Cela se traduit par un blocage total du moteur (plus d'analyse) ou une réduction très importante du nombre d'analyses produites.

Ce problème est corrigé en V2.5.3.102.

3.17 Malcore - Saturation des moteurs d'analyse

Si la vitesse de reconstruction des fichiers sur le GCap est supérieure à la vitesse d'analyse de Malcore, une file d'attente se créée au niveau du GCenter, provoquant un phénomène de saturation des moteurs et de perte du temps réel dans les alertes Malcore.

Ce problème est corrigé en V2.5.3.102.

3.18 Malcore - Arrêt du service pour cause de saturation

Dans de rares cas, lorsque la file d'attente des analyses Malcore comporte plusieurs milliers de fichiers de taille importante, un ralentissement ou un arrêt du service peut être observé.

Ce problème est corrigé en V2.5.3.102.

3.19 Malcore - Désactivation d'un moteur antivirus

La solution Malcore est composée de 16 moteurs de détection.
L'un des moteurs provoque des dysfonctionnements. Il a été désactivé en version 2.5.3.101-HF2.
Cela est visible au niveau du champ `total_found` des logs Malcore qui est de XX/15.

Ce moteur a été réactivé en V2.5.3.102 et cela est visible au niveau du champ total_found des logs Malcore qui est de XX/16.

3.20 Malcore - Export des logs avec flow_id=0

Dans de rares cas, le champ `flow_id` des logs Malcore n'est pas défini, ce qui empêche l'export de ceux-ci.

Ce problème est corrigé en V2.5.3.102.

3.21 Malcore - Incohérence healthcheck webui et statut des updates

Sur la page d'accueil du GCenter pour les administrateurs, il existe une incohérence graphique entre le `Updates Status` du panneau `Global Status` et le panneau `Malcore Update Status`.
Ces deux panneaux alertent l'utilisateur lorsque les mises à jour sont plus vieilles de 7 jours ;

- le premier le fait au bout d'une durée strictement supérieure à 7 jours
- tandis que le second le fait pour une durée supérieure ou égale à 7 jours

Ce problème est corrigé en V2.5.3.102 avec la refonte complète de la page de healthcheck.

3.22 Erreur d'enrichissement de Malcore sur le champ app_proto

Dans les logs Malcore, le champ `app_proto` indique le protocole par lequel un fichier analysé a été transporté.
Si un même fichier est transporté par deux protocoles différents (par exemple HTTP puis SMTP) pendant la durée du file_resend_interval (configurable dans `Operator > Gcap profiles > Base variables > File resend interval`) :

- un premier log replica=false avec app_proto=HTTP sera produit
- puis un deuxième log avec replica=true sera produit. Le champ `app_proto` vaudra HTTP, alors qu'il aurait du valoir SMTP

Ce problème est corrigé en V2.5.3.102.

3.23 Incohérence dans les alertes Malcore sur le champ `total_found`

Dans les alertes Malcore, dans certains cas, le champ `total_found` et le nombre d'`engine_id` ne sont pas identiques.

Ce problème est corrigé en V2.5.3.102.

3.24 API - Paramètre authentification

Les requêtes destinées à l'API du GCenter utilisent le mot-clé `API-KEY` pour fournir le token d'authentification en paramètre.
Dans swagger (https://HOSTNAME-GCENTER/docs/swagger/) les exemples de requêtes générées utilisent le mot-clé `apikey`.

Ce problème est corrigé en V2.5.3.102.

3.25 API - endpoint */api/alerts* non-fonctionnel

Le endpoint */api/alerts* de l'API du GCenter n'est pas fonctionnel :

- lors de l'utilisation du classement par date de manière décroissante, on obtient une erreur 500 si le paramètre `page` n'est pas défini ou égal 1
- le paramètre `page` détermine le nombre de résultats renvoyés au lieu de renvoyer la page spécifiée
- le paramètre `page_size` n'est pas pris en compte

Ce problème est corrigé en V2.5.3.102.

3.26 Proxy - Error 500 en cas de résolution de nom impossible

Si le proxy renseigné dans `Configuration/Proxy Configuration` ne peut pas être résolu par le serveur DNS configuré pour le GCenter, cela produit deux erreurs :

- une erreur 500 au niveau de la page de configuration du proxy (/configuration/proxy_settings/)
- une erreur dans le menu de configuration de GUM (/gum/configuration)

Ce problème est corrigé en V2.5.3.102.

3.27 Gcenter-setup - message d'erreur

Lors du lancement de *gcenter-setup*, le message d'erreur suivant peut être visible :

```
`Could not chdir to home directory /nonexistant: No such file or directory`.
```

Cela n'affecte en rien le fonctionnement du GCenter.

Ce problème est corrigé en V2.5.3.102.

3.28 LDAP Configuration - TLS

La gestion des utilisateurs peut être assurée via la connexion du GCenter à un Active Directory ou tout autre solution utilisant LDAP via le menu `Accounts/LDAP configuration`.
Lorsqu'un serveur LDAP est utilisé avec des paramètres TLS, le statut visible dans le panneau de configuration `LDAP interconnection status` peut indiquer une erreur bien que la configuration soit fonctionnelle.
L'erreur affichée est alors la suivante :

```
`Cannot connect to LDAP with current settings: {'desc': "Can't contact LDAP server",
↪'errno': 115, 'info': '(unknown error code)'}`.
```

Ce problème est corrigé en V2.5.3.102.

3.29 LDAP avec SSL ou STARTTLS

Si LDAP est configuré avec SSL ou STARTTLS et utilise un certificat pour valider le serveur, il peut disparaître lors d'un changement de configuration via la WebUI du GCenter.
Il est cependant bien conservé et utilisé.

Ce problème est corrigé en V2.5.3.102.

3.30 Export syslog : absence des analyses Malcore des fichiers « unknown »

Un bug affectant le moteur Suricata dans des conditions extrêmement précises peut aboutir à l'apparition de fichiers dits *unknown* c'est-à-dire dont les métadata n'ont pas pu être récupérées par Suricata.
Voir la description détaillée des conditions ici.
Les analyses Malcore relatives à ces fichiers sont consultables dans Kibana mais ne sont pas exportées via syslog.

Ce problème est corrigé en V2.5.3.102.

3.31 Export syslog : comportement lors des saturations

Si le débit des logs à exporter est tel qu'il sature l'export syslog, le GCenter commencera par traiter les evènements de type métadata en *best-effort* (pertes possibles) afin de préserver l'export des alertes sigflow, Malcore et codebreaker.

Ce problème est corrigé en V2.5.3.102.

3.32 Export syslog - Exceptions dans les formats de logs

Des incohérences mineures peuvent exister dans les logs de type Malcore (index malware) lors de leur export.
Les champs suivants peuvent être de type entier (sans guillemet autour de la valeur du champ) ou de type chaîne de caractères (avec guillemets) :

- *src_port*
- *dest_port*
- *detail_scan_time*

Par exemple :

- « src_port » : « 25 »
- ou « src_port » : « 25 ».

Ce problème est corrigé en V2.5.3.102.

3.33 Export syslog - alertes sigflow en double

Dans l'export syslog, les logs de type « alerte sigflow » (type=suricata AND event_type=alert) sont envoyés en double.

Ce problème est corrigé en V2.5.3.102.

3.34 Redirection Trackwatch Logs vers le dashboard Syslog

Lorsque l'on clique sur `Administrator > Gcenter > Trackwatch logs`, l'utilisateur est redirigé vers le dashboard `Tactical` à la place du dashboard `Syslog`.

Ce problème est corrigé en V2.5.3.102.

3.35 Réactivation des comptes par défaut

Lors de la configuration d'un GCenter, les comptes par défaut *administrator* et *operator* doivent être désactivés/ou le mot de passe changé.
Lorsque l'on procède à un upgrade, les valeurs de ces comptes sont réinitialisées à celles par défaut et ces derniers sont réactivés.

Ce problème est corrigé en V2.5.3.102.

3.36 Activation par défaut du protocole CIP/ENIP

Le parsing du protocole CIP/ENIP est activé par défaut et ne peut pas être désactivé dans l'interface du GCenter.

Ce problème est corrigé en V2.5.3.102.

3.37 Bug d'affichage pour ajouter des IP dans la partie external_net

Dans `Operator > Gcap profiles > Netvariables`, si l'on essaye d'ajouter un EXTERNAL_NET de type list avec un masque différent de /24, un bug d'affichage empêche d'ajouter le réseau.

Ce problème est corrigé en V2.5.3.102.

Chapter 4

Problèmes connus et limitations

4.1 Export Netdata - Absence temporaire d'informations

Lors de l'activation/désactivation répétée de l'export netdata, les informations de monitoring liées aux sondes de détections peuvent devenir momentanément indisponibles, pour une durée de 5 à 20 minutes.

Solution de contournement : pas de solution.

4.2 Sauvegarde/Restauration GCenter - Gestion des erreurs

Si une erreur a été commise par l'utilisateur en appliquant la procédure de restauration, la barre de progression du menu (écran `Admin-Backup/Restore - Backup operations`) reste bloqué et aucun message d'erreur n'est visible au niveau de la WebUI.

Solution de contournement : pas de solution.

4.3 Sauvegarde/Restauration GCenter - appairage du GCap

Suite à une sauvegarde du GCenter, si l'appairage du GCap est supprimé alors la restauration de la sauvegarde ne permettra pas de restaurer la connexion avec le GCap préalablement supprimée.

Solution de contournement : refaire l'appairage.

4.4 Désactivation d'une configuration LDAP avec un serveur LDAP éteint

La désactivation d'une configuration LDAP génère une erreur si le serveur LDAP est inaccessible.

Solution de contournement : faire une configuration LDAP valide avec le serveur LDAP accessible pour pouvoir désactiver la configuration souhaitée.

4.5 Etat GCap erroné suite à la mise à jour du GCenter

L'état du GCap peut être erroné suite à la mise à jour du GCenter (Last update = unknown / State: Online but update outdated)

Solution de contournement : ré appliquer la configuration du ruleset au niveau du GCap.

4.6 Kibana - cartes GeoIP

La visualisation des informations de GeoIP au sein des tableaux de bord Kibana est dépréciée.

Solution de contournement : pas de solution.

4.7 Sigflow Manager - Transform Category

L'application d'un Transform category lève une erreur 500 si aucun ruleset n'est présent sur le GCenter.

Solution de contournement : créer un ruleset.

4.8 Sigflow Manager - Erreur 500 lors de l'ajout d'une règle dans une source personnalisée

L'ajout d'une règle lève une erreur 500 si les conditions suivantes sont réunies :

- l'ajout se fait en éditant une custom source
- la règle existe déjà dans une autre source personnalisée (même SID)

Solution de contournement : changer le SID de la règle que l'on souhaite ajouter afin d'éviter le conflit de SID.

4.9 Sigflow Manager - Incohérence dans l'affichage du nombre de catégories et de règles d'une catégorie

La page d'accueil de `Sigflow > Sources` présente le nombre de catégories et de règles contenues dans chaque source.
Il est possible que les informations présentées soient incohérentes avec le contenu réel des sources.
Ce cas peut se produire après l'édition d'une custom source ou d'une mise à jour.

Solution de contournement : pas de solution.

4.10 Migration - configuration LDAP faite en v.2.5.3.100 et jamais modifiée depuis génère une erreur

La configuration LDAP faite en v.2.5.3.100 et jamais modifiée depuis, engendre un problème lors de la migration en version v2.5.3.102.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.
En cas de doute, veuillez contacter le support technique de Gatewatcher.

4.11 Configuration Sigflow - nom d'un source personnalisée ne peut contenir d'espace

Dans l'écran Config - Sigflow/sources de la legacy web UI, il est possible de définir une source personnalisée des signatures pour le moteur de détection Sigflow.
Lors de la procédure d'ajout, le nom de la source doit être saisie.
Ce nom ne doit pas contenir d'espace sinon cela génère une erreur.

Solution de contournement : modifier le nom en enlevant les espaces.

4.12 Limitation du stockage des données indexées dans ElasticSearch

Dans la version v2.5.3.102, les index ES ont été migré vers le stockage le plus performant du GCenter ce qui limite le volume disponible pour la conservation des ces données.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.
Pour cela, se référer à la procédure de migration du support de stockage présent dans la partie Hotfix de cette note de version.
En cas de doute, veuillez contacter le support technique de Gatewatcher.

4.13 Crash d'un composant lors de la réception d'un evelog vide

Dans la version v2.5.3.102, l'envoi d'un evelog vide provoque le crash d'un composant du GCenter.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.14 ActiveHunt - Problème de duplication de SID

Dans la version v2.5.3.102, il est possible que ActiveHunt génère des règles Sigflow avec un SID dupliqué.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.15 LDAP - Problème dans l'activation du module LDAP

Dans la version v2.5.3.102, il est impossible, dans certains cas, d'activer le module LDAP.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.16 Sauvegarde/Restauration GCenter - Problèmes sur les tableaux de bords NDR

Dans la version v2.5.3.102, lors de la restauration d'une sauvegarde, les tableaux de bord NDR ne sont plus fonctionnels.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.17 Sauvegarde/Restauration GCenter - configuration réseau

Dans la version v2.5.3.102, lors de la restauration d'une sauvegarde, la configuration IP de l'interface MGMT0 est restaurée ce qui peut engendrer certains problèmes.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.18 Sauvegarde/Restauration GCenter - erreur dans le FQDN

Dans la version v2.5.3.102, lors de la restauration d'une sauvegarde, si le FQDN du GCenter cible est différent alors une erreur est générée.

Solution de contournement : il faut changer le FQDN du GCenter cible et procéder à un redémarrage.

4.19 Sauvegarde/Restauration GCenter - numéro de version

Dans la version v2.5.3.102, il est impossible d'identifier le numéro de version d'un fichier de sauvegarde.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.20 NDR- Suppression des données

Dans la version v2.5.3.102, lors de l'utilisation de la fonction disponible dans le menu `Data Management > Data Deletion`, la suppression de certaines données de l'interface NDR ne s'effectue pas correctement.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.21 WebUI - Problème d'accès lors de la modification de la MTU

Dans la version v2.5.3.102, dans certains cas, la modification de la MTU de l'interface MGMT0 empêche l'accès à la WebUI.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.22 Migration - problème avec les compteurs des fichiers en attente d'analyse

Suite à la migration en v2.5.3.102, dans certains cas, les compteurs des fichiers en attente ne changent plus et affichent une valeur erronée.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.23 Migration - problème dans l'analyse des payloads de Codebreaker

Suite à la migration en v2.5.3.102, dans certains cas, les payloads devant être analysés par Codebreaker peuvent être bloqués.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1. Un problème peut cependant persisté avec les compteurs de fichiers en attente.
En cas de doute veuillez contacter le support technique de Gatewatcher.

4.24 Migration - problème avec l'export Syslog avec l'option TLS activée

Suite à la migration en v2.5.3.102, l'export Syslog avec l'option TLS activée n'est plus fonctionnel.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.25 Migration - problème de communication entre certains composants

Suite à la migration en v2.5.3.102, la communication entre certains composants n'est plus fonctionnelle.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.26 WebUI - problème lors d'une recherche sur une période de temps

Au niveau de la WebUI, dans les différents tableaux de bord NDR, la recherche sur une période de temps est faite en UTC tandis que l'affichage des résultats s'effectue en UTC+1.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.27 WebUI - problème de changement de mot de passe et d'édition de profil

Les utilisateurs appartenant au groupe Administrator ne peuvent pas changer leur mot de passe ou éditer leur profil au-travers de la WebUI.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.28 WebUI - problème d'affichage lorsque certains protocoles sont activés

Lorsque certains protocoles sont activés, cela peut provoquer des erreurs au niveau de certains tableaux de bord NDR.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

4.29 Kibana - Erreur 500 suite au changement de support de stockage pour les données d'ES

Suite au changement de support de stockage des données ES, une erreur 500 temporaire peut apparaître lors de l'accès à Kibana.

Solution de contournement : attendre quelques minutes.

4.30 Kibana - problème avec les raccourcis générés via l'interface NDR

Lors de l'utilisation de la fonction `Go hunting` au niveau du tableau de bord NDR des alertes, un problème d'heure est présent dans la redirection vers Kibana.

Solution de contournement : ce problème est corrigé en v2.5.3.102-HF1.

Chapter 5

Compatibilité logicielle

5.1 Compatibilité avec le GCap

Version du GCenter	Version du GCap	Compatibilité
2.5.3.102	2.5.3.104	Configuration non supportée : GCap à migrer en amont de la mise à jour du GCenter
2.5.3.102	2.5.3.105 (ou +)	Configuration ok

Chapter 6

Comptabilité matérielle

La version 2.5.3.102 est compatible avec toutes les versions matérielles des GCenter.

Référence GCENTER	Stockage local	Autre stockage	Interface réseau	Alimentation éléctrique
GCENT8100r2	2 x 960GB RAID1	2 x 2 TB RAID1	4 x RJ45	2 x 750W
GCENT9100r2	4 x 480GB RAID5	2 x 2 TB RAID1	4 x RJ45	2 x 750W
GCENT9900r2	10 x 480GB RAID5	4 x 2 TB RAID5	4 x RJ45	2 x 1100W
GCENT10500r2	12 x 480GB RAID5	4 x 2 TB RAID5	4 x RJ45	2 x 1100W

Chapter 7

Hotfix

7.1 Package 1

Package 1 - Hotfix (HF1 / SHA256)
Package 1 - Mise à jour/Installation (HF1 / SHA256)

Le hotfix n°1 s'applique sur les versions suivantes :

- version 2.5.3.101-HF4
- version 2.5.3.102

Si vous souhaitez mettre à jour un GCenter v2.5.3.102, appliquer le **Package 1 - Hotfix** via le menu `GUM > Software Update`.
Si vous souhaitez mettre à jour un GCenter v2.5.3.101, appliquer le **Package 1 - Mise à jour/Installation** via le menu `GUM > Upgrade`.

Le hotfix n°1 permet de corriger les problèmes suivants :

- *Migration - Configuration LDAP faite en v.2.5.3.100 et jamais modifiée depuis génère une erreur*
- *Limitation du stockage des données indexées dans ElasticSearch*
- *Crash d'un composant lors de la réception d'un evelog vide*
- *ActiveHunt - Problème de duplication de SID*
- *LDAP - Problème dans l'activation du module LDAP*
- *Sauvegarde/Restauration GCenter - Problèmes sur les tableaux de bords NDR*
- *Sauvegarde/Restauration GCenter - configuration réseau*
- *Sauvegarde/Restauration GCenter - numéro de version*
- *NDR - Suppression des données*
- *WebUI - Problème d'accès lors de la modification de la MTU*
- *Migration - Pproblème avec les compteurs des fichiers en attente*
- *Migration - Problème dans l'analyse des payloads de Codebreakers*
- *Migration - Problème avec l'export Syslog en TLS*
- *Migration - Problème de communication entre certains composants*
- *WebUI - Problème lors d'une recherche sur une période de temps*
- *WebUI - Problème de changement de mot de passe et d'édition de profil*
- *WebUI - Problème d'affichage lorsque certains protocoles sont activés*
- *Kibana - Problème avec les raccourcis générés via l'interface NDR*

7.2 Procédure de migration du support de stockage

Le Hotfix 1 a ajouté une commande supplémentaires dans le menu de configuration : `Elasticsearch storage mode`.
Cette commande permet de déplacer les index ES :

- le déplacement peut être fait depuis les disques HDD vers les disques SSD
- le déplacement peut être fait depuis les disques SSD vers les disques HDD

Dans le cadre de l'installation du HF1, les index ES ont été migré vers le stockage le plus performant du GCenter (les SSD) ce qui limite le volume disponible pour la conservation des ces données.
Si la taille réservée aux index ES est devenue trop basse, il est possible de transférer les index ES vers les disques HDD (espace disque sera plus grand mais le temps d'accès plus long).

Pour effectuer ce transfert depuis les disques SSD vers les disques HDD, effectuer les procédures suivantes :

7.2.1 Procédure de vérification

- Accéder au menu de configuration en SSH avec le compte setup.
- Utiliser la commande `Elasticsearch storage mode`.
  Dans la fenêtre `Elastic storage mode`, la ligne `Current storage type :` indique la configuration courante.
  - si le paramètre est `slow`, cela signifie que les index ES sont déjà localisés sur les disques HDD
  - si le paramètre est `fast`, cela signifie que les index ES sont localisés sur les disques SSD: effectuer la procédure suivante
- Dans la fenêtre `Elastic storage mode`, les informations suivantes sont affichées (les valeurs données ici sont un exemple):

```
Current storage type : fast
Maximum size on fast storage for elasticsearch : 411G
Maximum size on slow storage for elasticsearch : 1.8T
Current space used by elasticsearch : 273G
```

- Dans cet exemple :
  - les index ES sont localisés sur les disques SSD
  - la taille courante est de 273G
  - la taille maximum est de 411G sur les disques SSD
  - la taille maximum sera de 1.8T sur les disques HDD si les index ES sont transférés

---

7.2.2 Procédure de transfert

- Dans la fenêtre `Elastic storage mode`, cliquer sur le bouton `Switch storage type`.
  La fenêtre suivante donne des informations sur :
  - la préservation des données
  - la durée de l'opération
  - la taille maximum disponible sur les disques HDD
  - la taille choisie de l'espace réservé aux index ES après transfert : cette valeur pourra être modifiée via la WEB UI
  - la taille courante des index ES

- Cliquer sur le bouton `Switch storage type and launch data migration`.
  La fenêtre suivante donne des informations sur :
  - la préparation de la configuration : quand le paramètre est `Done` alors le transfert commence
  - la progression du transfert : valeur transférée / valeur totale
  - la reconfiguration du mode de stockage
- Attendre que la progression affiche les mêmes valeurs et cliquer sur le bouton `Refresh`.
  La procédure est terminée.
  On revient sur la fenêtre initiale mais la ligne ``Current storage type`` est maintenant à `slow`.

Chapter 8

Procédure de montée de version de V101 à V102

8.1 Prérequis

Pour déployer la mise à jour **V2.5.3.102** :

- le GCenter devra être en version **V2.5.3.101-HF3** ou supérieur
- le GCap devra être en version **V2.5.3.105** ou supérieure
- si une configuration LDAP existe en **v2.5.3.101**, refaire cette configuration en **v2.5.3.101** avant la migration vers la **V2.5.3.102**

  Important:

  Pour la mise à jour vers la V2.5.3.102, il est impératif d'utiliser le package suivant afin d'éviter certains problèmes de migration: https://update.gatewatcher.com/upgrade/2.5.3.102/gcenter/gcenter_2.5.3.102-8541~prod-hf1.gwp

- si des questions se posent sur ces éléments, veuillez contacter le support technique de Gatewatcher.

Important:

Il est fortement recommandé d'avoir une connexion de type iDRAC afin de pouvoir se connecter post-mise à jour si un problème survient pendant le processus.

Important:

Avant de procéder à la mise à jour, il est fortement recommandé de procéder à une sauvegarde de la configuration du GCenter dans le menu `Administrators > Backup / Restore > Operations` et de sauvegarder le fichier sur un serveur externe dans un répertoire indiquant la version actuelle du GCenter (exemple: 2.5.3.102-XXXX-HFX).

8.2 Données conservées

L'ensemble de la configuration du GCenter est conservée.
Les données (métadata et alertes) devront être migrées au préalable avec un hotfix spécifique (se référer à la procédure d'installation avec conservation des données ci-dessous).

Important:

Une fois migrées, les données seront uniquement disponibles au-travers du menu `Discover` de l'interface Kibana (Hunting).

8.3 Procédure d'installation avec conservation des données

1. Vérifier que les sondes GCap sont en version **V2.5.3.105** ou supérieur sinon se référer à la procédure de mise à jour suivante: https://releases.gatewatcher.com/fr/gcap/2.5.3/105/8_upgrade_procedure.html
2. Télécharger la nouvelle version du GCenter disponible et le sha256 associé sur la plate-forme https://update.gatewatcher.com/upgrade/ (répertoire 2.5.3.102).
3. Faire la vérification de l'image avec le sha256 associé.
4. Télécharger le hotfix permettant de préparer les données avant migration: https://update.gatewatcher.com/hotfix/2.5.3.101/gcenter/gcenter_2.5.3.101_hf_data-preparation-for-2.5.3.102.gwp et le sha256 associé.
5. Faire la vérification de l'image avec le sha256 associé.
6. Se connecter à la WebUI du GCenter et aller dans le menu `Administrators > GUM > Hotfix`.
7. Dans la section `Uploading a new hotfix package`, cliquer sur le bouton `Choisir un fichier`, sélectionner le hotfix précédemment téléchargé puis cliquer sur `Send hotfix`.
8. Toujours dans la WebUI du GCenter, aller dans le menu `Administrators > GUM > Upgrade`.
9. Dans la section `Upload an upgrade`, cliquer sur le bouton `Choisir un fichier`, sélectionner la nouvelle version du GCenter précédemment téléchargée puis cliquer sur `Submit`.
10. Se connecter en SSH sur le GCap avec le compte **setup**.
11. Stopper le moteur de détection avec la commande suivante : `monitoring-engine stop`.
12. Modifier le mode de compatibilité avec la commande suivante : `set compatibility-mode 2.5.3.102+`.
13. Démarrer le moteur de détection avec la commande suivante : `monitoring-engine start`.
14. Retourner dans la WebUI du GCenter, dans le menu `Administrators > GUM > Hotfix`.
15. Dans la section `Saved package list`, au niveau du hotfix précédemment envoyé, cliquer sur le bouton `Apply`.
16. Une fois appliqué, se connecter en SSH sur le GCenter avec le compte **setup**.
17. Aller dans le nouveau menu disponible `data persistence`.
18. Dans le menu `Warning data preparation` lire attentivement l'avertissement puis cliquer sur `Continue (reversible)` pour continuer.

    Le menu suivant offre la possibilité de supprimer les données (index) les plus anciennes afin d'accélérer le processus de migration et que les données migrées puissent être stockées dans la nouvelle architecture.

Important:

Il se peut que certaines données présentes soient plus anciennes que la durée de rétention configurée.

Ces données seront donc automatiquement supprimées une fois la mise à jour en V2.5.3.102 effectuée.

Il est donc important de supprimer manuellement ces données à cette étape.

Pour vérifier la durée de conservation configurée, il faut se connecter à la WebUI du GCenter et aller dans le menu `Administrators > GCenter > Configuration > Gloabl settings`.

La configuration se situe au niveau de l'entrée `Data retention (in days):`

Important:

Les changements d'architecture opérés en V2.5.3.102 impliquent une limitation dans le volume de données conservées qui s'étend à 95% de la partition /es.

La partition de backup n'est donc plus utilisée pour le stockage des données relatives à Elastic Search.

Ce comportement sera modifiable dans le prochain hotfix.

19. Pour supprimer les index, sélectionner ceux qui ne doivent pas être conservés puis cliquer sur `Delete selected indices (irreversible)`.
20. Une fois l'opération effectuée, cliquer sur `Continue (reversible)`.
21. Le menu suivant présente les différentes phases de la migration et leur statut, cliquer sur `Continue (reversible)`.
22. La dernière fenêtre permet de lancer la migration qui sera alors irréversible, cliquer sur `Launch data preparation (irreversible)`.

Important:

Le temps de migration dépend du matériel et du volume de données à migrer. Il faut compter en moyenne 1h pour 100Go.

23. Le menu suivant présente les différentes phases de la migration et leur statut, cliquer ponctuellement sur `Refresh` pour voir la progression de l'opération.

    A la fin de l'opération, si toutes les étapes sont en vert **true**, cela signifie que la migration s'est correctement effectuée, dans le cas contraire veuillez contacter le support technique Gatewatcher.
24. Quitter le menu **setup**, se connecter la WebUI du GCenter, aller dans le menu `Administrators > GUM > Upgrade`.
25. Dans la section `Saved package list`, au niveau de la mise à jour précédemment envoyée, cliquer sur le bouton `Apply`.
26. Une fois l'opération terminée, redémarrer le GCenter en se connectant en SSH avec le compte **setup** puis en allant dans le menu `Restart`.
27. Une fois le GCenter redémarré, se connecter à la WebUI et vérifier que des nouveaux évènements apparaissent dans la partie `Hunting` (interface Kibana).

8.4 Procédure d'installation sans conservation des données

1. Vérifier que les sondes GCap sont en version **V2.5.3.105** ou supérieur sinon se référer à la procédure de mise à jour suivante : https://releases.gatewatcher.com/fr/gcap/2.5.3/105/8_upgrade_procedure.html
2. Télécharger la nouvelle version du GCenter disponible et le sha256 associé sur la plate-forme https://update.gatewatcher.com/upgrade/ (répertoire 2.5.3.102).
3. Faire la vérification de l'image avec le sha256 associé.
4. Se connecter en SSH sur le GCap avec le compte **setup**.
5. Stopper le moteur de détection avec la commande suivante: `monitoring-engine stop`.
6. Modifier le mode de compatibilité avec la commande suivante: `set compatibility-mode 2.5.3.102+`.
7. Démarrer le moteur de détection avec la commande suivante: `monitoring-engine start`.
8. Se connecter à la WebUI du GCenter, aller dans le menu `Administrators > GUM > Upgrade`.
9. Dans la section `Upload an upgrade`, cliquer sur le bouton `Choisir un fichier`, sélectionner la nouvelle version du GCenter précédemment téléchargée puis cliquer sur `Submit`.
10. Dans la section `Saved package list`, au niveau de la mise à jour précédemment envoyée cliquer sur le bouton `Apply`.
11. Une fois l'opération terminée, redémarrer le GCenter en se connectant en SSH avec le compte **setup** puis en allant dans le menu `Restart`.
12. Une fois le GCenter redémarré, se connecter à la WebUI et vérifier que des nouveaux évènements apparaissent dans la partie `Hunting` (interface Kibana).

`PDF Release Note`