Note de Version
GCenter Version 2.5.3.101

Version de la note : V1

Date de création : Octobre, 2022

Last updated : November, 2022

Contents

Chapter 1

Note de Version GCENTER 2.5.3.101

Avertissement:

Si la version de votre GCENTER est 2.5.3.100-HF6 ou supérieure vous devez utiliser l'archive suivante pour un upgrade :

- https://update.gatewatcher.com/upgrade/2.5.3.101/gcenter/gcenter-2.5.3.101-7126~prod.gwp

Si la version de votre GCENTER est 2.5.3.100-HF5 vous devez utiliser l'archive suivante pour un upgrade :

- https://update.gatewatcher.com/upgrade/2.5.3.101/gcenter/from_2.5.3.101-HF5/gcenter-2.5.3.101-7126~prod-gv2.gwp

Si la version de votre GCENTER est 2.5.3.100-HF4 ou inférieure, vous ne pouvez pas appliquer une upgrade en version 2.5.3.101. Il faut alors appliquer des upgrades intermédiaires.

Avertissement:

Avant d'effectuer la mise à jour, veuillez prendre connaissance des informations suivantes :

- https://docs.gatewatcher.com/fr/gcenter/2.5.3/101/upgrade_253101.html

Vous trouverez :

- Nouvelles Fonctionnalités.
- Les correctifs.
- Les problèmes connus.

1.1 Mise à jour en vidéo

1. Téléchargez le paquet de mise à jour v101 ici : https://update.gatewatcher.com/upgrade/2.5.3.101/gcenter Vous pouvez également télécharger les signatures Sigflow/Malcore ici : https://update.gatewatcher.com/update/2.5.3.101/gcenter
2. Une fois le téléchargement terminé, téléchargez le paquet de mise à jour dans le menu GUM/Upgrade. Cette opération peut prendre plusieurs minutes et dépend de votre bande passante.
3. Une fois le téléchargement terminé (affichage du message « Opération GUM en cours »), veuillez rafraîchir votre navigateur après quelques minutes
4. Cliquez sur « Upgrade » pour lancer l'opération.
5. Pour finaliser le processus de mise à niveau, connectez-vous en ssh/setup sur le GCenter et redémarrez l'appliance. Le redémarrage peut prendre une douzaine de minutes.
6. Lorsque la WebUI du GCenter est disponible, connectez-vous et vérifiez que la version est v2.5.3.101.
7. Pour installer le module MalcoreV4, allez dans le menu GUM/Updates et téléchargez le paquet « latest_full_v3.gwp ».

Chapter 2

Nouvelles fonctionnalités

2.1 Mise à jour ELK

La suite ELK a été mise à jour en version 7, permettant une optimisation de ces services ainsi qu'une meilleure stabilité.

2.2 Mise à jour tableaux KIBANA

Les tableaux KIBANA intègrent les nouveaux protocoles supportés par une sonde de détection (GCap) d'une version 2.5.3.103 ou supérieure.

Une refonte du menu de navigation a été effectuée, ayant un thème DARK par défaut.

La fonctionnalité Kibana Maps a été intégrée.

2.3 Mise à jour Malcore

Malcore a été upgradé en version 4, permettant une meilleure stabilité.

2.4 Bannière SSH préauthentification

Une bannière SSH de préauthentification est configurable pour l'ensemble des GCaps appairés ainsi que le GCenter depuis la WebUI de celui-ci.

Les GCaps s'appairant au GCenter bénéficieront automatiquement de celle-ci, si elle a été au préalable configurée.

2.5 Support des règles de détection par interfaces de monitoring et par VLAN (multi-tenancy)

La configuration de jeux de règles de détection peut être appliquée à des interfaces de monitoring (jusqu'à 8) ou a des VLAN spécifiques. Elle s'effectue depuis l'interface Web du GCenter.

2.6 Export des logs

Il est désormais possible de configurer deux serveurs syslog pour l'export des journaux d'événements.

L'interface graphique a totalement été revue afin de la rendre fluide et dynamique.

L'export prend en charge le RFC 3164 ou RFC 5424. Les filtres avancés permettent de cibler :

- Les différents protocoles pris en charge par la ou les sondes de détections appairées.
- IPV4 ou IPV6.
- La liste des GCaps appairés au GCenter.

L'intégration du protocole TLS permet d'avoir des échanges sécurisés entre le GCenter et le serveur syslog. Un certificat est nécessaire pour l'activation de celui-ci.

2.7 API

Le GCenter dispose maintenant d'une API permettant d'automatiser certaines actions ou requêtes via des scripts ou un SOAR. La documentation swagger est accessible directement sur le GCenter ; un package python et un manuel d'utilisation sont disponibles dans la documentation.

2.8 GUM - Hotfix cumulatif

Les différentes corrections à chaud mises à disposition pourront être appliquées via un package unique.

2.9 Deep Scan Shellcode

Un mode « Deep Scan » a été ajouté à la fonctionnalité GScan des shellcodes.

Il permet d'améliorer la détection de pattern ou de méthode d'obfuscation inconnue. Cette méthode demandant un coût temporel plus grand, peut être "activé/désactivé" depuis l'interface Web du GCenter. Une durée maximale peut aussi être configurée.

2.10 Moteur shellcode et powershell

Les moteurs de détection de shellcode (GOASM) et de powershell (GPS) ont été améliorés pour une meilleure stabilité.

2.11 Support de nouveau protocole

Le GCenter permet la configuration de nouveaux protocoles pris en charge par un GCap d'une version 2.5.3.103 et supérieur.

2.12 Service de supervision sécurisé

Il est désormais possible de configurer l'export Netdata de manière sécurisé via TLS et un certificat.

L'interface Web de configuration a été revue améliorant l'interactivité.

2.13 Évolution interface WebUI

Les tableaux Gatewatcher ont évolué dans un nouveau menu **INSPECTRA** accessible depuis l'interface web du GCenter. Ils ne concernent plus que les moteurs **MALCORE** et **CODEBREAKER**. Les alertes remontées restent accessibles depuis les tableaux Kibana dans le menu **Dashboards**.

La fonctionnalité .

Les fonctionnalités suivantes ont été supprimées : * **ICAP**, * **Reporting**, * lors de l'édition d'une règle *Delete generated alerts*, * et **All In One** ont été supprimées.

Les vues **Global Status** et **Malcore Update Status** évoluent indiquant plus de détails lors d'une défaillance sur un des équipements ou sur les mises à jour des moteurs antiviraux.

Le menu **Malcore Management/Global Setting** a été revu intégralement.

2.14 Profil GCap

Il est possible pour un *Operator* de configurer le profil d'un GCap via le menu **Sigflow** de la WebUI.

Le template par défaut proposé à l'opérateur est entièrement configurable par un *administrateur*.

L'administrateur peut choisir parmi cinq templates que nous mettons à sa disposition :

- **Default** : la configuration la plus optimisée.
- **Minimal** : rien n'est activé.
- **LPM** : Les paramètres nécessaires au mode LPM.
- **Intuitio** : Les prérequis pour le Network Detection and Response (NDR).
- **Paranoid** : Tout est activé.

Une fois le template par défaut appliqué par l'opérateur, la configuration du profil GCap reste entièrement personnalisable par celui-ci.

2.15 Tech Support

Il est possible de lancer un diagnostic rapide et complet du GCenter depuis le *gcenter-setup* via le menu **Tech Support**. Le résultat du diagnostic se fait directement depuis le terminal.

2.16 GApps Management - Restart GApp

Le menu **GApps Management/Restart a GApp** via *gcenter-setup* propose le redémarrage des services internes au GCenter suivants :

- Malware Analysis Engine.
- WebUI Service 1/2.
- Database Service.
- Threat Analysis and Retroactive Orchestrator.
- Connections Manager.
- DGA Engine.
- Kibana Service.

- Monitoring Service.
- Gcap Upgrade Provider Service.
- WebUI Service 2/2.
- Ephemeral Data Service.
- Threat Logger Service.
- Master ES Service.
- Hot Data ES Service.
- Cold Data ES Service.
- PowerShell Analyser Engine.
- Exploit Analyser Engine .

Chapter 3

Correctifs

3.1 Kernel - Instabilité du module IPSEC

Le noyau linux possédait un module relatif à ipsec susceptible d'entrainer des erreurs kernel (kernel oops).

Le problème a été corrigé.

3.2 Malcore - Mauvaise association de fichiers dans le cas de replicas

Dans les logs de type malcore, le champ « filename » pouvait être inexact quand plusieurs fichiers possédaient le même hash mais des noms différents.

Le problème a été corrigé.

3.3 Malcore - Accumulation de fichiers dans /tmp

Dans certains cas, malcore pouvait rater des analyses, et des fichiers en attente restaient indéfiniment dans un répertoire réservé aux fichiers temporaires.

Le problème a été corrigé.

3.4 Malcore - Absence de flow_id

Le champ flow_id n'était pas systématiquement présent dans les alertes malcore.

Le problème a été corrigé.

3.5 Sigflow - Threshold rule

Lorsque l'on éditait une règle pour activer un Threshold rule, le *generate rules file* ne mettait pas à jour cette nouvelle configuration.

Le problème a été corrigé.

Chapter 4

Problèmes connus

4.1 Statut des last updates

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

Solution de contournement : Régénérer le fichier de règles dans Sigflow Manager.

4.2 Pairing à un GCAP impossible si aucune gateway n'est renseignée pour l'interface VPN

Le pairing 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.

Solution de contournement: Renseigner une passerelle par défaut, quelle qu'elle soit.

4.3 Pairing 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 du pairing, le GCap indique le message d'erreur suivant : « pairing not established ».

Solution de contournement: Contacter le support Gatewatcher.

4.4 Règles LastInfoSec

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

Solution de contournement: Pas de solution.

4.5 Gestion des erreurs GUM mode Local ou Online

La webui du GCenter ne dispose pas d'un affichage des erreurs relatives à un dysfonctionnement du module GUM (gestion des mises à jour).

Solution de contournement : Message d'erreur disponible dans les logs du GCenter.

4.6 Double amorçage

À partir de la version 2.5.3.100, le double amorçage n'est plus supporté.

Solution de contournement: Pas de solution.

4.7 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.

Solution de contournement: Pas de solution.

4.8 Certificat auto-signé

Une erreur peut apparaître depuis la WebUI du GCenter lors de l'application de certificats auto-signés. Cela n'impacte pas le bon fonctionnement de l'authentification chiffrée.

Solution de contournement: Pas de solution.

4.9 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.

4.10 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 requêtable 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.

Solution de contournement : Utiliser un Netdata externe avec une version 1.19.

4.11 GUM - Configuration Frequency non préservée post upgrade

Lors d'un upgrade d'une version **2.5.3.100** vers **2.5.3.101**, le panneau de configuration des mises à jour via GUM présente un problème d'affichage lorsqu'on le consulte pour la première fois.

Solution de contournement: Rafraîchir la page.

4.12 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.

Solution de contournement: Pas de solution.

4.13 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.

4.14 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.

4.15 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 de contournement.

4.16 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.

Solution de contournement: Pas de solution.

4.17 Third Party - Intelligence

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

Solution de contournement : Appliquer un token valide.

4.18 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 ».

Important:

Ce problème a une plus forte probabilité de se produire lors du premier démarrage du GCenter après une upgrade.

Solution de contournement : Le bug est résolu avec la manipulation suivante : Dans la console, via *gcenter-setup* : GApps Management > Restart a GApp > WebUI Service #2

4.19 Kibana - incohérence entre champs de type timestamp

Dans Kibana, les logs de type malware possèdent trois timestamp :

- *timestamp_detected* : moment où le fichier a été capturé par le GCap,
- *timestamp_analysis* : moment où le fichier est traité par le GCenter,
- et *timestamp_last_malcore_analysis* : dans le cas où le fichier avait déjà été analysé, moment de sa dernière analyse.

Il existe une incohérence de format au niveau de Kibana dans l'affichage de ces champs, faisant que les deux premiers timestamp sont rapportés à l'heure locale configurée dans Kibana, tandis que le troisième est affiché en UTC.

Cela peut donner l'impression que *timestamp_last_malcore_analysis* est incohérent avec les autres timestamp.

Par défaut, Kibana utilise le fuseau horaire du navigateur utilisé pour la consultation, la différence observée sera donc égale au décalage entre le fuseau horaire du navigateur et l'heure UTC.

Solution de contournement: En tant qu'administrateur, aller dans *Kibana > Stack management > Index pattern > malware* > refresh field list > refresh (en haut à droite).* Cela fera disparaître le problème.

4.20 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 ».

Solution de contournement: Se connecter en SSH sur le GCenter et aller dans le menu GApps Management > Restart a GApp. Procéder ensuite au redémarrage (dans cet ordre) des GApps : - Threat analysis and retroactive orchestrator Service - DGA engine - Kibana Service Si cette manipulation de ne fonctionne pas, contactez le support Gatewatcher.

4.21 Kibana - Maps GeoIP

La visualisation des informations de GeoIP au sein des dashboards Kibana nécessite un accès à internet pour que les fonds de carte puissent être téléchargés.

Solution de contournement: Pas de solution.

4.22 Kibana - UPGRADE

Lors d'un upgrade de version 2.5.3.100 vers une version 2.5.3.101, une corruption des index *.kibana* peut survenir rendant inaccessible les dashboarding KIBANA en affichant le message d'erreur suivant : « *Kibana server is not ready yet* ».

Solution de contournement: Appliquer l'upgrade HF2 de la version 101 du GCenter.

Si le problème survenait de nouveau, le menu GCenter-Setup peut être utilisé pour nettoyer l'index *.kibana*. Pour cela dans la GUI du Gcenter (via SSH ou en console), *GApps Management > Reset a GApp > Wipe Elasticsearch index*. L'utilisation de ce menu supprimera tous les dashboards Kibana personnalisés, mais préservera les données métier.

4.23 Malcore - Profiles non préservés post upgrade

Lors d'un upgrade d'une version **2.5.3.100-hfx** vers **2.5.3.101**, la configuration des profiles via **Malcore Management** n'est pas maintenue.

Notamment, le paramètre concernant la taille maximale des fichiers analysés par **malcore**, s'il était à sa valeur par défaut en v100, il sera ramené à 2Mo.

Potentiellement, des fichiers reconstruits par les GCap ne seraient alors plus analysés : cela se traduirait par la valeur *File size exceeded* dans le champ *total_found* des logs **malcore**.

Solution de contournement: Réappliquer la configuration des profiles de **Malcore Management** et appliquer la valeur recommandée de *100* pour le paramètre *Maximum size of scanned files (in MB)* dans le profile *Default* accessible depuis le menu **Administrator/Malcore Management/Profile/Default**.

4.24 Malcore - non fonctionnel après une mise à jour de version

Les mises à jour peuvent être configurées pour être réalisées de manière automatique via **GUM**, accessible depuis **Administrator/GUM/Config/Enabled**.

Si les mises à jours automatiques sont activées et que l'on procède à une upgrade d'une version 2.5.3.100 à une versions 2.5.3.101, **Malcore** ne sera pas opérationnel.

Solution de contournement: Depuis **Administrator/GCenter/Configuration/Proxy settings**, il faut activer/désactiver le proxy via le paramètre *Enable web proxy*, puis le remettre dans son état d'origine. C'est-à-dire que s'il était activé, désactivez-le (décochez, puis *save*) et réactivez-le (cocher puis *save*). Inversement s'il était désactivé, activez-le avec n'importe quelle configuration puis désactivez-le.

Important:

Le serveur mandataire souffre du bug *Proxy - Error 500 en cas de résolution de nom impossible* : aussi, si vous devez mettre une configuration temporaire pour activer/désactiver le proxy, utilisez une IP ou un nom de domaine joignable par le GCenter. (Vous pouvez utiliser l'adresse IP du GCenter lui-même ou *127.0.0.1* par exemple).

4.25 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.

Solution de contournement : Pas de solution de contournement.

4.26 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.

Solution de contournement: Pas de solution.

4.27 Malcore - Analyse indisponible durant l'upgrade

Pendant l'upgrade de v100 à v101, Malcore peut rater des analyses. Cela se traduit par des logs **malcore** (index malware) où le champ *detail_threat_found* vaudra *Unknown*, *Not Scanned* ou *Could not open pipe. Error: 2.*

Solution de contournement: Stopper l'envoi des fichiers du GCap vers le GCenter durant le temps de la mise à jour. Dans gcap-setup > Service Management > Stop sending files (but keep on extracting them).

4.28 Malcore - Analyse de fichier

Lorsque malcore analyse un fichier une première fois, il génère un log possédant un champ *replica=false*.

Si ce fichier est à nouveau vu avant la fin de la période de *file_resend_interval*, malcore ne réanalyse pas le fichier et crée un log possédant un champ *replica=true*. Ces analyses de fichiers déjà observés sont appelées des **replica**. (Le *file_resend_interval* est configurable au niveau des paramètres **Sigflow/GCap Profiles** du GCap dans **Base variables** et sa valeur par défaut est de 24h).

Malcore garantit que chaque fichier est analysé au moins une fois. Dans de rares cas, et quand un grand nombre de replicas sont observés, il est possible que certains logs d'analyse *replica=true* ne soient pas générés, ou au contraire soient observés en plusieurs exemplaires (dans ce dernier cas, on observe que le champ *try_count* -qui est interne au fonctionnement du GCenter- est incrémenté entre chaque exemplaire).

Solution de contournement: Si l'on souhaite retrouver de manière certaine l'ensemble des apparitions d'un fichier ayant généré un grand nombre de *replica=true*:

- trouver le SHA256 du fichier en question dans les données produites par **malcore** (champ *SHA256*),
- filtrer les métadonnées file reconstruction de **sigflow** avec ce SHA (champ *fileinfo.sha256*).

4.29 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 métadonnées relatives à cet évènement malcore peut être faite à l'aide des SHA257 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.

Solution de contournement: Pas de solution.

4.30 Malcore - Configuration et application d'une Black/White list

Il est possible d'ajouter des White/Black list de fichiers que malcore ne doit pas analyser.

La configuration de cette fonctionnalité se trouve dans **Gcenter/Malcore Management/Whitelist(Blacklist)**.

Le white/blacklisting d'un fichier n'est pas immédiatement effectif, et prend effet après une période inférieure ou égale au *file_resend_interval* configuré sur le GCap qui observe le fichier. (Le *file_resend_interval* est configurable au niveau des paramètres **Sigflow/GCap Profiles** du GCap dans **Base variables** et sa valeur par défaut est de 24h).

Solution de contournement: Pas de solution.

4.31 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.

Solution de contournement: Pas de solution.

4.32 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.

Solution de contournement: Dans Gcenter-setup : Gapps Management > Reset a GApp > Reset Malcore Engine.

4.33 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 crée au niveau du GCenter, provoquant un phénomène de saturation des moteurs et de perte du temps réel dans les alertes malcore.

Solution de contournement :

- Réduire la quantité de fichiers reconstruits et analysés par malcore, grâce à la configuration de Operators > Sigflow > GCAP Profiles > Files rules management.
- Vérifier que le file_resend_interval est d'au moins 24h (valeur par défaut) dans Operators > Sigflow > GCAP Profiles.
- Upgrader en version 2.5.3.101 Hotfix 2, qui apporte un gain de performance significatif.

4.34 Malcore - Arrêt du service pour cause de saturation

Dans de rare 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.

Solution de contournement: Appliquer l'upgrade HF2 pour la version 101 du GCenter.

4.35 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 au lieu de XX/16.

Solution de contournement: Appliquer l'upgrade HF3 pour la version 101 du GCenter.

4.36 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.

Solution de contournement: Appliquer l'ugrade HF2 de la version 101 du GCenter. Les logs sans flow_id sont exportés avec la valeur flow_id=0.

4.37 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.

Solution de contournement: Pas de solution.

4.38 Malcore - Code d'erreur 3

Dans certains cas les fichiers ne sont pas analysés par Malcore et sont stockés dans */data/extraction/3*. Ce code d'erreur indique que le fichier n'a pas pu être analysé par Malcore.

Solution de contournement: Appliquer l'upgrade HF3 pour la version 101 du GCenter.

4.39 Malcore - Code d'erreur 10

Dans certains cas les fichiers ne sont pas analysés par Malcore et sont stockés dans */data/extraction/10*. Ce code d'erreur indique que lors de l'analyse d'un fichier, aucun moteur de détection n'avait de statu up. Ce cas arrive principalement lors des mises à jour Malcore en CIE ou un seul moteur est disponible.

Solution de contournement: Appliquer l'upgrade HF3 pour la version 101 du GCenter. Cet upgrade permet de limiter les fichiers non analysés et retournant le code d'erreur 10.

4.40 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.

Solution de contournement: Utiliser le flow_id pour effectuer un recoupement entre les alertes malcore et les métadonnées.

4.41 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*.

Solution de contournement: Dans les requêtes proposées par swagger, remplacer le mot-clé *apikey* par *API-KEY*.

4.42 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.

Solution de contournement: Consulter les alertes via l'API en utilisant :

- le endpoint `/api/alerts/clusters` : les alertes sont alors groupées par adresse IP et par période de temps,
- ou directement en effectuant une requête elasticsearch via le endpoint d'API *api/data/es/search*.

4.43 Options Payload et Payload printable - Drop d'events

Dans certains cas, et en raison d'une mauvaise gestion du format *JSON par suricata*, le GCap peut générer des logs d'alerte dont la taille dépasse 65 ko. Ces logs sont alors perdus, et peuvent entraîner la malformation du log subséquent, quel qu'il soit.

Cette anomalie peut se produire lorsque suricata insère une grande quantité de données dans les logs, notamment lorsque les options suivantes sont activées simultanément :

- *payload*,
- *payload_printable*,
- *packet*,
- *http_body*
- et *http_body_printable*.

Ces options sont paramétrables dans **Sigflow/GCap Profiles** du GCap dans **Base variables**.

Solution de contournement: Ne pas activer simultanément les options *payload*, *payload_printable*, *packet*, *http_body* et *http_body_printable*.

4.44 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).

Solution de contournement:

- utiliser un proxy qui peut être résolu par le DNS configuré,
- ou paramétrer directement l'adresse IP du serveur mandataire (auquel cas il n'y a plus besoin de résolution DNS).

4.45 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.

Solution de contournement: Pas de solution.

4.46 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)'}`.
```

Solution de contournement: Pas de solution.

4.47 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.

Solution de contournement: Pas de solution.

4.48 LDAP - le GCenter ne ferme pas les connections

Dans le cas de l'utilisation d'un serveur LDAP pour authentifier les utilisateurs, le GCenter ne ferme pas les connexions établies avec le serveur LDAP, et rouvre des connexions pour chaque utilisation.

Solution de contournement: Pas de solution.

4.49 API indisponible lors de l'utilisation du module LDAP

Lorsque le GCenter est configuré pour authentifier les utilisateurs via un serveur LDAP, l'API devient indisponible et renvoie une erreur 500 sur l'ensemble des endpoints.

Solution de contournement: Appliquer l'upgrade HF2 pour la version 101 du GCenter.

4.50 Export syslog - Enrichissement faux

Lorsque les alertes malcore sont exportées au niveau de syslog, un certain nombre d'enrichissements ont lieu au niveau des champs *http* et *smtp* :

- *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*.

Ces enrichissements se font entre le SHA256 du fichier analysé par **malcore**, et les métadonnées les plus récentes de **sigflow** relative au même SHA256.

Si le fichier a été vu un grand nombre de fois, et si les analyses produites par le GCenter se font avec une latence importante due à une charge élevée, il est possible que les métadonnées *les plus récentes* ne correspondent pas au fichier analysé en question. Dans ces conditions, l'enrichissement peut être faux.

Solution de contournement: Au niveau d'un **SIEM**, utiliser le champ *flow_id* pour réaliser des corrélations entre les alertes **malcore** et les métadonnées **sigflow**.

4.51 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 métadonnées 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.

Solution de contournement: En plus de la consultation via Kibana, il est possible d'effectuer une requête elasticsearch via l'API du GCenter.

4.52 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 metadonnées en *best-effort* (pertes possibles) afin de préserver l'export des alertes sigflow, malcore et codebreaker.

Solution de contournement: Appliquer l'upgrade HF2 de la version 101 du GCenter, qui assure le *at-least once delivery* de tous les messages exportés par syslog.

4.53 Export syslog - taille maximale des logs exportés

L'export syslog tronque les logs dont la taille dépasse 65 ko.

Solution de contournement: Pas de solution.

4.54 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.

Solution de contournement: Pas de solution.

4.55 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.

Solution de contournement: Appliquer le Hotfix 1. Pour les clients LPM (pas d'application de HF possible) une procédure peut vous être communiquée par le support gatewatcher.

4.56 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 ».

Solution de contournement: Pas de solution.

4.57 Exception causée par le driver megaraid

Un problème au niveau du driver megaraid intégré par l'OS peut entraîner un blocage du GCenter, et nécessiter son redémarrage.

Solution de contournement: Appliquer l'upgrade HF2 de la version 101 du GCenter.

4.58 Analyse Powershell bloquée

Le nombre d'analyse powershell en attente sur la page d'acceuil (*Live Critical Indicators*) peut apparaître élevé et croître de manière rapide, donnant ainsi l'impression que le moteur est bloqué.

En réalité, le moteur fonctionne et les analyses ont bien lieu. Il existe un problème de cohérence au niveau du compteur : certains fichiers ne pouvant être analysés par le module restent dans la file d'attente des fichiers à traiter.

Le problème n'est pas bloquant, les fichiers sont conservés pour la durée de rétention du GCenter (*Configuration/Global settings/Data retention (in days)*), ils sont ensuite purgés.

Solution de contournement: Appliquer l'upgrade HF3 de la version 101 du GCenter.

- Si vous êtes dans une version inférieure à la version 2.5.3.101-HF3 du GCenter, pour remettre le compteur Powershell de *Live Critical indicators* à 0, il est possible d'obtenir une procédure en contactant le support.

4.59 Exception dans la gestion des données chaudes ou froides

Les données indexées dans elasticsearch sont gérées suivant un schéma de données chaud/froid ; Les données récentes sont placées sur SSD, tandis que les plus anciennes sont déplacées sur des disques plus lents.

Cette gestion des données ne fonctionne pas correctement, entrainant la saturation possible de certains espaces de stockage, et le dysfonctionnement de plusieurs composants du Gcenter (indexation des logs, création des alertes malcore, etc.)

Solution de contournement: Consulter le taux d'occupation de la partition /es : cela peut se faire de deux manières :

- En tant qu'administrateur, sur la page d'accueil du GCenter, le taux d'occupation est donnée dans **Live Critical Indicators** à la ligne *Elasticsearch index size (used)*
- En tant qu'administrateur, dans Administrators > GCenter > Monitor > BASIC HOST STATS

Si le taux d'occupation de /es est inférieur à 65%:

- Upgrader en version 2.5.3.101 Hotfix 2, qui corrige le problème pour toutes les nouvelles données écrites.

Si le taux d'occupation de /es est supérieur à 65%:

- Le hotfix n'a pas d'effet rétroactif sur les données déjà écrites, et il est fortement recommandé de supprimer une partie des données avant de procéder à l'upgrade.
- Pour cela, aller dans Administrators > Gcenter > Data Management > Data deletion, et cocher les cases Malcore, Codebreaker, Sigflow et Syslog.
- Avec le selecteur de date, sélectionner les données les plus vieilles présentes sur le GCenter ; La durée de rétention par défaut est de 15 jours, et est configurable dans Administrators > Gcenter > Configuration > Global settings > Data retention in days. Dans le cas par défaut, commencer par supprimer les données de J-15. Puis de J-14, et ainsi de suite jusqu'à faire descendre le taux d'occupation de /es en dessous de 65%.
- Upgrader en version 2.5.3.101 Hotfix 2, qui corrige le problème pour toutes les nouvelles données écrites.

4.60 Instabilité de Filebeat

Lors de l'injection massive de données en provenance du GCap, Filebeat pouvait, dans certains cas, remonter des erreurs de traitement.

Solution de contournement: Appliquer l'upgrade HF3 de la version 101 du GCenter.

4.61 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 une upgrade les valeurs de ces comptes sont réinitialisées à celles par défaut et ces derniers sont réactivés.

Solution de contournement: Une désactivation/changement de mot de passe de ces comptes est de nouveau nécessaire.

4.62 GSCAN - Taille maximale des fichiers analysés

La taille maximale des fichiers analysés par GScan est de 10 Mo, même si l'on configure une valeur supérieure dans Administrators > Gcenter > Malcore management > Profiles > GScan profile settings > Maximum size of scanned files.

Solution de contournement: Pas de solution.

4.63 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.

Solution de contournement: pas de solution.

4.64 Bug d'affichage pour ajouter des ip dans la partie external_net

Dans Operators > Sigflow > Gcap profiles > Network variables, 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.

Solution de contournement: Rafraîchir la page.

4.65 IPsec - Impossible de monter le tunnel IPsec dans un réseau NAT

Les règles IPtables du GCenter empêchent l'établissement du tunnel IPSec entre le GCap et le GCenter si le réseau entre les deux appliances est en NAT.

Solution de contournement: Appliquer l'upgrade HF3 de la version 101 du GCenter.

Chapter 5

Hotfix

5.1 Package 1 (HF1 / SHA256)

Le hotfix n°1 permet de régler le problème de doublon des alertes sigflow dans l'export syslog (cf. *Export des alertes sigflow en double*)

5.2 Package 2 (HF2 / SHA256)

Avertissement:

Le HF2 contient une mise à jour de licence interne au produit GCenter et doit être appliquée impérativement avant le 31/12/2021.
Le package de mise à jour doit être appliqué via le menu *GUM* > *upgrade* (ce qui implique un redémarrage).
Il est impossible d'appliquer ce correctif comme un hotfix car il apporte - entre autre - un patch du kernel qui ne peut s'appliquer à chaud.

Le hotfix n°2 s'applique sur les versions suivantes :

- version 2.5.3.101
- version 2.5.3.101-HF1

Le hotfix n°2 permet de corriger les problèmes suivants :

- Exception causée par le driver Megaraid (cf. *Exception causée par le driver megaraid*)
- Amélioration de la fiabilité de malcore (cf. *Malcore - Arrêt du service pour cause de saturation*)
- Exception dans la gestion des données chaudes froides (cf. *Exception dans la gestion des données chaudes ou froides*)
- Malcore - Absence de flow_id (cf. *Malcore - Absence de flow_id*)
- Perte de données lors de l'export vers un syslog (cf. *Export syslog : comportement lors des saturations*)
- Amélioration significative des performances, vitesse de traitement des fichiers améliorée entre 50% et 100% (cf. *Malcore - saturation des moteurs d'analyse*)
- Problème de corruption dans dashboard kibana (cf. *Kibana - UPGRADE*)
- Erreur dans l'API (cf. *API indisponible lors de l'utilisation du module LDAP*)

Important:

Une attention particulière doit être portée sur les bugs suivants :

- Désactiver les comptes operator et administrator (cf. *Réactivation des comptes par défaut*)
- Vérifier manuellement la taille des index avant l'upgrade (cf. *Exception dans la gestion des données chaudes ou froides*)
- Retrait d'un moteur AV (cf. *Malcore - Désactivation d'un moteur antivirus*)
- Redémarrage manuel de Kibana (cf. *Kibana - tableaux inaccessibles*)

5.3 Package 3 (HF3 (mode upgrade) / SHA256 // HF3 (mode hotfix) / SHA256)

Le hotfix s'applique sur les versions suivantes :

- version 2.5.3.101-HF2

Le hotfix permet de corriger les problèmes suivants :

- IPsec - Impossible de monter le tunnel IPsec dans un réseau NAT (cf. *Impossible de monter le tunnel IPsec dans un réseau NAT*)
- Analyse Powershell bloquée (cf. *Analyse Powershell bloquée*)
- Instabilité de Filebeat (cf. *Instabilité de Filebeat*)
- Malcore code 3 (cf. *Malcore code 3*)
- Malcore code 10 (cf. *Malcore code 10*)
- Malcore - Réactivation d'un moteur antivirus (cf. *Malcore - Désactivation d'un moteur antivirus*)

Ce hotfix permet également de réintroduire l'application de hotfix pour les clients en LPM.

5.4 Package 4 (HF4 (mode hotfix) / SHA256)

Le hotfix s'applique sur les versions suivantes :

- version 2.5.3.101-HF3
- version 2.5.3.101-HF3 (LPM)

Le hotfix permet de :

- Corriger le problème relatif aux connexions LDAPs qui restent ouvertes. (cf. LDAP - le GCenter ne ferme pas les connexions).
- Corriger d'un problème au niveau de filebeat intervenant suite à l'application du HF3 en mode upgrade. (cf. *Instabilité de Filebeat*)
- Améliorer la stabilité du module Malcore avec la mise en place d'un orchestrateur.
- Améliorer les mises à jour en ligne du module Malcore.
- Désactiver un moteur antivirus qui est instable.
- Améliorer la gestion de certains services avec un redémarrage automatique en cas de dysfonctionnement.
- Améliorer la gestion des fichiers de logs du gcenter pour éviter la saturation de l'espace disque réservé à cet effet.

Chapter 6

Note de version hors-ligne

Note de version au format PDF

Note de version au format HTML

Note de version au format EPUB