Note de Version GCENTER 2.5.3.100

Gatewatcher

Created on : December, 2020

Last updated : November, 2022

Contents

Contents i

1 Note de Version GCENTER 2.5.3.100 2

2 Nouvelles fonctionnalités 3
2.1 Gatewatcher Licensing Center . . . 3
2.2 Gatewatcher Update Manager . . . 3
2.3 Connecteur Endpoint Detection and Response (expérimental) . . . 4
2.4 Sauvegarde et restauration . . . 4
2.5 Connecteur MISP : Malware Information Sharing Platform . . . 4
2.6 Interconnexion GBox . . . 4
2.7 Paramètres avancés Sigflow . . . 4
2.8 Rulesets par interface physique . . . 4
2.9 Conteneurs . . . 5
2.10 Python 3.6 ou supérieur . . . 5
2.11 API GCenter . . . 5
2.12 Simplification du script de configuration . . . 5
2.13 Démmarage des services GCenter . . . 5
2.14 Urls GCenter . . . 5
2.15 Heartbeat . . . 5
2.16 ElasticSearch (ES) et Cycles de Vie des Index (ILM) . . . 5
2.17 Demon d'orchestration . . . 6
2.18 Machine Learning et "Domain Generation Algorithm" . . . 6
2.19 Détection de powershell malicieux basé sur du Machine Learning . . . 6
2.20 Shellcodes vizualisation . . . 6
2.21 Tableaux KIBANA - NETDATA . . . 6
2.22 LastInfoSec / Sigflow . . . 6
2.23 Analyse Malcore . . . 7
2.24 Multi-tenant . . . 7
2.25 Personnalisation de la durée de session . . . 7
2.26 Authentification centralisée LDAPS / AD . . . 7
2.27 KAFKA . . . 7
2.28 API Publique . . . 7

3 Correctifs 8
3.1 Double Authentification . . . 8
3.2 Certificat Personnalisé du GCenter . . . 8
3.3 SWAP . . . 8
3.4 Partition chiffrée de sauvegarde . . . 8
3.5 Activation de la configuration spécifique à la Loi de Programmation Militaire (LPM) . . . 9
3.6 Affichage page d'accueil . . . 9
3.7 Configuration avancée de Malcore . . . 9
3.8 Profils d'analyse . . . 9

3.9 Expiration session web . . . 9
3.10 Champs ElasticSearch . . . 9
3.11 Gestion des cookies . . . 9
3.12 Edition des tableaux KIBANA . . . 10
3.13 Historique des authentifications . . . 10
3.14 Historique des adresses IP de connexion . . . 10
3.15 Création/Edition d'un utilisateur . . . 10
3.16 Règles Sigflow . . . 10
3.17 Rapport PDF . . . 10
3.18 BlackList/WhiteList Malcore . . . 10
3.19 Sigflow Manager . . . 10
3.20 Nombre d'alertes dans les tableaux GATEWATCHER . . . 11
3.21 Export des diagnostiques . . . 11
3.22 Champ mot de passe des archives . . . 11
3.23 Healtcheck . . . 11
3.24 Utilisateurs non-authentifiés . . . 11
3.25 Utilisateurs authentifiés . . . 11
3.26 Authentification LDAP . . . 12

4 Problèmes connus **13**
4.1 Export SYSLOG . . . 13
4.2 Statut des last updates . . . 13
4.3 Règles LastInfoSec . . . 13
4.4 Gestion des erreurs GUM mode Local ou Online . . . 13
4.5 LDAP avec SSL ou STARTTLS . . . 13
4.6 Double amorçage . . . 14
4.7 Moteur Machine Learning et édition CIE . . . 14
4.8 Certificat autosigné . . . 14
4.9 Alerte Malcore . . . 14
4.10 Configuration serveur mandataire (proxy) . . . 14
4.11 Configuration interface SUP0 . . . 14
4.12 Ruleset . . . 15
4.13 Threshold rule . . . 15
4.14 Export syslog . . . 15
4.15 Sigflow Manager - Transform Category . . . 15
4.16 Sigflow Manager - Erreur 500 lors de l'ajout d'une règle dans une source personnalisée . . . 15
4.17 Sigflow Manager - Incohérence dans l'affichage du nombre de catégories et de règles d'une catégorie 15
4.18 LDAP COnfiguration - TLS . . . 16
4.19 Backup Restore . . . 16
4.20 FQDN du GCap (Pairing/Status) . . . 16
4.21 Kernel - Instabilité du module IPSEC . . . 16
4.22 Malcore - Mauvaise association de fichiers dans le cas de replicas . . . 16
4.23 Malcore - Accumulation de fichiers dans /tmp . . . 17
4.24 Malcore - Profiles non préservés post upgrade . . . 17
4.25 Malcore - Désactivation d'un moteur antivirus . . . 17
4.26 Malcore Management - GScan Profile . . . 17
4.27 Malcore - Analyse de fichier . . . 17
4.28 Malcore - Absence de flow_id . . . 18
4.29 Malcore - Configuration et application d'une Black/White list . . . 18
4.30 Malcore - Doublon d'analyse . . . 18
4.31 Malcore - Crash du moteur suite à une surcharge . . . 18

5 Hotfix **19**
5.1 Package 1 (HF1 / SHA256) . . . 19
5.2 Package 2 (HF2 / SHA256) . . . 19
5.3 Package 3 (HF3 / SHA256) . . . 20
5.4 Package 4 (HF4 / SHA256) . . . 20
5.5 Package 5 (HF5 / SHA256) . . . 21

5.6 Package 6 (HF6 / SHA256) 21
5.7 Package 7 (HF7 (mode upgrade) / SHA256 // HF7 (mode hotfix) / SHA256) 22

6 Note de version hors-ligne **23**

Chapter 1

Note de Version GCENTER 2.5.3.100

Vous trouverez :

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

Chapter 2

Nouvelles fonctionnalités

2.1 Gatewatcher Licensing Center

A partir de la version 2.5.3.100, les serveurs de management (GCenter) utilisent le nouveau system de licence GATEWATCHER LICENSING CENTER (GLC).

La licence se compose au minimum d'une licence GWAPI perpétuelle associée à un GCenter.

L'administrateur doit ajouter une licence afin de configurer l'équipement.

L'opérateur, peut quant à lui, accéder aux données du GCenter.

Pour obtenir une licence version 2.5.3.100, merci de vous rapprocher de votre ingénieur d'affaire Gatewatcher ou contacter commerciaux@gatewatcher.com.

2.2 Gatewatcher Update Manager

A partir de la version 2.5.3.100, les GCenters se basent sur un nouvel outil de mise à jour unifié GATEWATCHER Update Manager (GUM).

Il permet la gestion des différents types de mises à jour : update, upgrade, hotfix.

Un statut en temps réel est visible depuis l'interface WEB du GCenter.

Les updates sont désormais unifiées en un seul package avec les moteurs souhaités (Codebreaker, Sigflow, Malcore) et peuvent se faire :

- En ligne via https://update.gatewatcher.com/update/ et https://gupdate.gatewatcher pour Malcore. Ceci requiert un compte intelligence.
- Localement, en définissant un répertoire par défaut.

La mise à jour de Malcore en ligne est différentielle et chiffrée.

La personnalisation de l'horaire souhaité est possible via l'interface WEB du GCenter.

Les hotfix permettent d'injecter un correctif sans qu'un redémarrage du GCenter soit nécessaire.

Il est possible de conserver jusqu'à trois paquets d'upgrade GCenter et/ou de la sonde de détection (GCap).

La configuration de GUM est possible via un serveur mandataire (PROXY).

2.3 Connecteur Endpoint Detection and Response (expérimental)

Il est possible d'ajouter un connecteur HarfangLab Hurukai (EDR) au GCenter. La configuration de cette fonctionnalité est possible via un serveur mandataire (PROXY).

2.4 Sauvegarde et restauration

Il est désormais possible d'effectuer une sauvegarde chiffrée de la configuration du GCenter (licence incluse) et du GCap pour restauration.

Celle-ci peut être exportée localement, en SCP ou FTP via l'interface WEB du GCenter

Il est possible de planifier une sauvegarde ainsi que son export via l'interface WEB du GCenter.

2.5 Connecteur MISP : Malware Information Sharing Platform

Il est possible d'ajouter un connecteur MISP au GCenter afin de convertir des IOC en signatures Sigflow. La configuration de cette fonctionnalité est possible via un serveur mandataire (Proxy).

2.6 Interconnexion GBox

Il est désormais possible d'interconnecter une GBox au GCenter et d'envoyer automatiquement des malwares vers cette dernière.

La configuration de la GBox est possible via un serveur mandataire (PROXY).

2.7 Paramètres avancés Sigflow

Il est possible de configurer les options avancées de Sigflow pour tous les GCaps via la WebUI du GCenter.

Il est donc désormais possible de configurer de nombreux paramètres tels que :

- Les variables d'environnement.
- Les variables réseaux.
- Les timeout protocolaires.
- Les reconstructions de fichiers.
- Le filtrage local des GCap (XDP Filter).

Le conteneur Sigflow Manager a été unifié au travers de celui de la WebUI du GCenter.

2.8 Rulesets par interface physique

La configuration via l'interface WEB du GCenter d'un ruleset global ou par interface physique avec un GCap compatible avec la version 2.5.3.100 du GCenter est désormais possible.

2.9 Conteneurs

L'ensemble des conteneurs présents dans le GCenter reposent maintenant sur une distribution linux Debian 10 (Buster).

2.10 Python 3.6 ou supérieur

L'intégralité du code Python du GCenter est en Python 3.6 ou supérieur.

2.11 API GCenter

L'API interne du GCenter agrège la quasi-totalité des modèles de configuration des applications de la machine hôte et/ou de ces conteneurs.

2.12 Simplification du script de configuration

Il est désormais possible d'utiliser une ligne de commande python avec arguments pour effectuer la configuration du GCenter.

2.13 Démmarage des services GCenter

Au démarrage du GCenter, un contrôle de chaque service est effectué afin de vérifier le bon lancement de celui-ci.

2.14 Urls GCenter

Dans une démarche de simplification et d'organisation, l'ensemble des URLs de la WebUI du GCenter a été unifié.

2.15 Heartbeat

Le GCenter est désormais capable de détecter l'absence ou la perte d'un GCap en utilisant un demon de Heartbeat.

2.16 ElasticSearch (ES) et Cycles de Vie des Index (ILM)

Depuis la version 2.5.3.100, le GCenter intègre la version 6.8 de la suite ELK.

Elle permet un renforcement de la sécurité des clusters.

Les tableaux KIBANA ont entièrement été revus.

Le Cycles de Vie des index (ILM) permet d'augmenter la capacité de rétention des alertes et des meta données en utilisant ces fonctionnalités :

- Utilisation de données chaudes sur un media de type SSD.
- Utilisation de données froides sur un media de type HDD.

L'ILM permet de conserver les données des dernières 24H en zone chaude, au-delà de ce délai, les données sont archivées en zone froide.

N.B: Lors de la mise à jour de la version 2.5.3.10 vers la 2.5.3.100, pour des raisons de performances et de temps, seuls les index 'logstash-*' et 'malwares-*' sont conservés. Dans la version 2.5.3.100, la nomenclature des index 'logstash-*' est modifiée en 'suricata-*'.

2.17 Demon d'orchestration

Afin d'assurer la continuité des services du GCenter, un demon d'orchestration a été ajouté.

2.18 Machine Learning et "Domain Generation Algorithm"

A partir de la version 2.5.3.100, le GCenter embarque l'intelligence artificielle grâce à du Machine Learning basé sur du 'deep-learning' à la recherche de 'Domain Generation Algorithm' (DGA).

Cette nouvelle fonctionnalité permet la détection de DGA pouvant être reliés à des serveurs de 'Commande and Control' (C&C) utilisés par des malwares.

Le seuil de déclenchement d'une alerte est configurable via la WebUI du GCenter.

2.19 Détection de powershell malicieux basé sur du Machine Learning

Depuis la version 2.5.3.100, nous sommes désormais capable d'auto apprendre et d'analyser les scripts powershell afin de pourvoir détecter le caractère malicieux de ceux-ci. Uniquement disponible avec un GCap compatible.

2.20 Shellcodes vizualisation

Afin de simplifier la compréhension d'une attaque par Shellcode, il est possible de visualiser une cinématique graphique via la WebUI du GCenter.

2.21 Tableaux KIBANA - NETDATA

L'implémentation de la nouvelle version de KIBANA et de la partition ES permet de créer des tableaux pour afficher les logs du GCap via le 'GCenter/Trackwatch Logs'. A terme, les tableaux KIBANA centraliseront les logs de l'ensemble des équipements.

2.22 LastInfoSec / Sigflow

Sigflow intègre désormais les sources externe 'LastInfoSec'(CTI Française). Cette fonctionnalité est expérimentale.

2.23 Analyse Malcore

La version 2.5.3.100 permet la corrélation des fichiers analysés par Malcore et un flux de données basé sur un 'flow_id'.

2.24 Multi-tenant

Il est possible d'activer le support multi-tenant via la WebUI du GCenter. Uniquement avec un GCap compatible.

2.25 Personnalisation de la durée de session

Depuis la version 2.5.3.100, il est possible de personnaliser la durée de session WEB par utilisateur.

2.26 Authentification centralisée LDAPS / AD

LDAP ne requiert plus de créer des groupes spécifiques dans l'annuaire. Il utilise désormais les mappings.

Son utilisation via SSL ou STARTTLS est maintenant possible.

L'authentification par LDAP peut se faire de manière anonyme ou en utilisant un compte dédié.

La validation des certificats serveurs auto-signés est possible et optionnelle.

2.27 KAFKA

Depuis la version 2.5.3.100, l'export KAFKA n'existe plus.

2.28 API Publique

La version 2.5.3.100 introduit le développement d'une API publique et sa documentation. Celle-ci se repose sur l'outil open source SWAGGER.

Chapter 3

Correctifs

3.1 Double Authentification

L'activation de la double authentification par certificat rendait la WebUI inaccessible et nécessitait une réinitialisation de sa configuration.

Cette fonctionnalité est désormais corrigée et permet d'ajouter une autorité de certification (CA) et une liste de révocation (optionnelle) afin de valider les certificats clients.

Il est possible de l'activer/désactiver via l'interface de la WebUI du GCenter.

3.2 Certificat Personnalisé du GCenter

La fonctionnalité d'ajout de certificat pour la WebUI du GCenter est corrigé. Il est désormais possible de l'activer ou de la désactiver.

3.3 SWAP

Lors du démarrage du GCenter, l'initialisation de la partition de SWAP chiffrée s'effectue désormais correctement.

3.4 Partition chiffrée de sauvegarde

Dans certains cas, au moment du démarrage des services, les disques de sauvegarde ne montaient pas correctement.

Désormais, lorsque leur déchiffrement est effectué, le service vérifie que le disque est accessible et sa partition bien présente.

3.5 Activation de la configuration spécifique à la Loi de Programmation Militaire (LPM)

L'application du renforcement LPM du GCenter lorsque celui-ci est sélectionné est fonctionnelle. L'API interne du GCenter résout ce problème.

3.6 Affichage page d'accueil

Les informations affichées sur la page d'accueil de l'interface WEB du GCenter étaient erronées et manquaient de cohérence.

Les statuts sont maintenant cohérents avec les alertes en cours.

Les indicateurs de fichiers en attente affichent désormais des valeurs justes pour chacun des moteurs.

Les informations liées aux partitions ElasticSearch sont cohérentes.

3.7 Configuration avancée de Malcore

Dans certains cas d'utilisation ou lors de fortes charges, les profils de Malcore se désynchronisaient. Cela avait pour conséquence une surcharge des CPU et de la RAM, ce qui entrainait une accumulation de fichier à analyser.

3.8 Profils d'analyse

La synchronisation des profils d'analyse est opérationnelle entre l'interface WEB du GCenter et Malcore à la suite d'un redémarrage inopiné.

3.9 Expiration session web

La configuration du backend de la WebUI du GCenter était incohérente et entrainait des déconnexions inopinées des utilisateurs.

3.10 Champs ElasticSearch

Dans les versions précédentes de la 2.5.3.100, les incohérences des champs ElasticSearch empêchaient d'utiliser de manière optimale les meta données envoyés à un SIEM.

L'unification et la ré-organisation de ceux-ci ('src_ip','dest_ip') ont permis de résoudre ce problème.

3.11 Gestion des cookies

La configuration des cookies de sessions sur le GCenter était basée sur une gestion côté client. Cela permettait de les réutiliser.

La gestion des cookies est désormais faite côté serveur ce qui empêche toute réutilisation non désirée.

3.12 Edition des tableaux KIBANA

La version précédente de KIBANA ne permettait pas la création, l'édition ou la duplication des tableaux. Ce problème est corrigé suite à la mise à jour de KIBANA.

3.13 Historique des authentifications

La pagination de l'historique des authentifications sur l'interface Web du GCenter n'était pas correct. Elle est désormais fonctionnelle.

3.14 Historique des adresses IP de connexion

L'utilisation de docker entraînait l'affichage d'une adresse IP unique et interne au GCenter.

Désormais l'adresse IP réelle de l'utilisateur qui s'est connecté à la WebUI du GCenter est correctement affichée.

3.15 Création/Edition d'un utilisateur

Il était possible de créer un utilisateur avec un nom contenant plus de 256 caractères ce qui entrainait une erreur d'affichage et retournait un code d'erreur HTTP 500. La taille maximale des champs est désormais de 256 caractères.

3.16 Règles Sigflow

Dans les versions précédentes, les règles Sigflows générées pour les différents GCaps étaient accessibles de manière globale.

Désormais ces règles son cloisonnées et accessibles par le GCap concerné.

3.17 Rapport PDF

La mise en forme des rapports PDF générés par le GCenter était incorrecte. Elle est désormais corrigée.

3.18 BlackList/WhiteList Malcore

L'utilisation du système de 'Black/White list' pour l'analyse n'avait aucun effet. Elle est désormais corrigée.

3.19 Sigflow Manager

L'utilisation de Sigflow Manager était indépendante de la WebUI du GCenter. Désormais Sigflow Manager fait partie intégrante de l'interface Web du GCenter.

3.20 Nombre d'alertes dans les tableaux GATEWATCHER

La configuration du nombre d'alertes dans les tableaux Gatewatcher utilise JavaScript.

La sélection d'un trop grand nombre d'alertes entrainait une surcharge du navigateur et rendait l'exploitation des données impossible.

La limitation à 5000 alertes autorisées et 500 par défaut corrige ce problème.

3.21 Export des diagnostiques

Le nom du fichier lors de l'export des diagnostiques était erroné, cela empêchait l'opération.

La nouvelle nomenclature du fichier est sous la forme <DATE_UTC>_GCap_diagnostics.csv. Cela corrige le problème.

3.22 Champ mot de passe des archives

La configuration du mot de passe pour l'extraction ou la génération d'archives par le GCenter était affichée en clair.

Il est désormais masqué par défaut avec une possibilité de le visualiser.

3.23 Healtcheck

Il n'y avait pas de gestion de services des conteneurs.

Grâce à la mise en place d'un Healtcheck, les services des conteneurs sont contrôlés et redémarrés si besoin.

3.24 Utilisateurs non-authentifiés

Dans les versions précédentes, un utilisateur non authentifié pouvait accéder librement aux pages d'erreurs correspondant aux différents code http (4XX,5XX). Cela n'est désormais plus possible. Tant que l'utilisateur n'est pas authentifié il est redirigé automatiquement vers la page d'authentification.

3.25 Utilisateurs authentifiés

Après authentification, l'utilisateur est redirigé vers la page demandée et non plus vers la page d'accueil.

Dans les versions précédentes, la redirection après authentification n'était pas fonctionnelle.

Désormais, l'utilisateur authentifié sera redirigé vers la page demandée. Si elle n'existe pas, l'utilisateur sera redirigé vers une page de code erreur.

Si la requête est sous forme POST et qu'une authentification est requise, elle sera modifiée sous forme GET.

3.26 Authentification LDAP

L'authentification LDAP n'était pas fonctionnelle. La correction de celle-ci est consultable dans les nouvelles fonctionnalités (1.26).

Chapter 4

Problèmes connus

4.1 Export SYSLOG

L'export Syslog UDP tronque les alertes lorsqu'il y a plus de 65635 Octets.

Solution de contournement: privilégier l'utilisation de TCP.

4.2 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.

4.3 Règles LastInfoSec

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

Solution de contournement: Pas de solution.

4.4 Gestion des erreurs GUM mode Local ou Online

Pour les mises à jour GUM (local ou online) aucune information liée à l'erreur n'est disponible via la WebUI du GCenter.

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

4.5 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.

4.6 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 autosigné

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

Solution de contournement: Pas de solution.

4.9 Alerte Malcore

Dans certains cas, une incohérence peut survenir entre les champs "total_found" et "engine_id".

Solution de contournement: Pas de solution.

4.10 Configuration serveur mandataire (proxy)

Après une mise à jour d'une version 2.5.3.10 vers 2.5.3.100 du GCenter, la configuration du serveur mandataire n'est plus effective.

Solution de contournement: Il faut ré-éditer la configuration de celui-ci. Corrigé en version 2.5.3.100-hf5.

4.11 Configuration interface SUP0

Après une mise à jour d'une version 2.5.3.10 vers 2.5.3.100 du GCenter, la configuration de l'interface SUP0 n'est plus effective. Cela entraîne des problèmes d'export vers le serveur SYSLOG en empruntant par défaut l'interface MGMT0.

Solution de contournement: Il faut ré-éditer la configuration de celle-ci. Corrigé en version 2.5.3.100-hf5.

4.12 Ruleset

Lorsque nous désactivons une règle dans plusieurs rulesets, la réactivation de celle-ci dans un seul ruleset ne fonctionne pas.

Solution de contournement: Il faut activer la règle pour tous les rulesets.

4.13 Threshold rule

Lorsque nous éditons une règle pour activer un Threshold rule, le generate rules file ne met pas à jour cette nouvelle configuration.

Solution de contournement: Il faut effectuer un generate rules file deux fois. Corrigé à partir du HF5.

4.14 Export syslog

L'export des logs vers le serveur syslog ne s'effectue pas sur une version 2.5.3.100-hf4.

Solution de contournement: Il faut effectuer un redémarrage de logstash. Correctif présent dans le package 5.

4.15 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: Création d'un ruleset.

4.16 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.

4.17 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.

4.18 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.

4.19 Backup Restore

Dans le cadre d'une réinstallation de la version du GCenter qui a suivi un chemin d'upgrade particulier, la restauration de la sauvegarde ne fonctionnera pas.

Solution de contournement: il faut procéder à la mise à jour des versions en respectant le chemin initialement fait pour que la sauvegarde puisse être appliquée.

Exemple : Le GCenter a été installé en version XXX, les hotfix X, Y et Z ont été appliquées.

Pour effectuer une restauration :

- *Installer le gcenter avec la version XX,*
- *puis appliquer respectivement les hotfix X, Y et Z avant de procéder à la restauration.*

4.20 FQDN du GCap (Pairing/Status)

Des majuscules au niveau du FQDN du GCap provoqueront des erreurs d'associations lors de l'initiation du tunnel IPsec avec le GCenter,

Solution de contournement: il faut que le FQDN du GCap dans le champ Pairing/Status soit composé uniquement de minuscule.

4.21 Kernel - Instabilité du module IPSEC

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

Solution de contournement: Corrigé en version 2.5.3.100-hf6.

4.22 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.

Solution de contournement: Pas de solution.

4.23 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.

Solution de contournement: Corrigé en version 2.5.3.100-hf6.

4.24 Malcore - Profiles non préservés post upgrade

Lors de l'application du HF6, 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 avant upgrade, 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**.

4.25 Malcore - Désactivation d'un moteur antivirus

Avec malcore v4 (à partir de l'application du HF6), un des moteurs antivirus connaît des instabilités dangereuses pour la stabilité globale de Malcore. Celui-ci a été désactivé. En conséquence, malcore fonctionne avec 15 moteurs antiviraux, et le champ *total_found* des logs malcore vaut *XX/15* et non *XX/16*.

Solution de contournement : Pas de solution de contournement.

4.26 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.

4.27 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).

Après l'application du HF6, 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*).

4.28 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 SHA256 et timestamp_detected de l'alerte malcore.

Solution de contournement: Pas de solution.

4.29 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.

4.30 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.

4.31 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.

Chapter 5

Hotfix

5.1 Package 1 (HF1 / SHA256)

Le système de correctif à chaud de GUM du GCenter a été amélioré.

5.2 Package 2 (HF2 / SHA256)

Le fonctionnement actuel qui préserve la santé du GCenter (Emergency Mode) lors d'un pic de charge a été optimisé et amélioré.

Les journaux de la WebUI du GCenter embarquent désormais plus d'informations.

L'analyse d'un script Powershell pouvait être faite en boucle si la donnée envoyée par la sonde de détection venait à être corrompue. Une meilleure gestion des erreurs a corrigé ce problème.

Il n'est plus nécessaire d'entrer une authentification lors de la première configuration de GUM avec un miroir local.

La barre de progression de GUM lors de diverses opérations ne reste plus bloquée.

La configuration des tâches planifiées dans GUM a été améliorée.

Le suivi des versions de Hotfix a été implémenté à la WebUI du GCenter.

L'affichage des unités de mesure Netdata a été corrigé, il se fait désormais en Mégabits.

La visibilité des interfaces depuis la WebUI du GCenter a été améliorée, le nom de celles-ci est associé à son adresse IP.

L'indicateur "Suspicious (archived)" dans le tableau "Live Critical Indicators" a été corrigé, il affiche désormais une information cohérente

Le monitoring Netdata des partitions /es et /backups a été ajouté.

L'activation du calcul du hash des fichiers reconstruits dans le profil du GCap ne reflétait pas la configuration réelle. L'affichage indique désormais la configuration effective.

Après plusieurs jours d'utilisation, il était impossible d'exporter les logs de l'appliance. La partition temporaire de 10Go utilisée par l'API du GCenter était à l'origine de ce problème. L'emplacement de celle-ci a été modifié, elle intègre désormais un plus grand espace de stockage permettant ainsi à l'API d'effectuer la préparation de l'archive chiffrée destinée à l'exportation des journaux du GCenter. Lors d'une restauration, les dossiers des GCaps concernant les analyses et la configuration étaient manquants. Au démarrage, le GCenter vérifie désormais la présence de ces dossiers.

La configuration d'une passerelle par défaut pour les interfaces n'est plus nécessaire.

Attention : l'application de ce correctif génère un redémarrage automatique de la WebUI du GCenter. Un rafraîchissement manuel de page est nécessaire.

5.3 Package 3 (HF3 / SHA256)

Dans le cas d'un export des alertes avec syslog et l'utilisation du protocole TCP, lorsqu'une interruption de service survenait entre le GCenter et le serveur syslog, la publication des alertes dans la base ElasticSearch était elle aussi interrompue.

Pour bénéficier des correctifs de sécurité et de stabilité, la version d'ELK a été mise à jour en version 6.8.11. (Lien)

Lorsqu'un utilisateur configurait la fonctionnalité SMTP Privacy sur le GCenter, celle-ci n'était pas prise en compte, elle est désormais fonctionnelle.

L'export des journaux du GCenter embarque désormais plus d'informations concernant les messages système.

Une corruption des données lors de l'export des journaux du GCenter pouvait survenir. Ce problème a été corrigé.

Une fuite de mémoire pouvait survenir sur le GCenter suite à l'application d'une mise à jour GUM planifiée à intervalle très réduite. Ce problème a été corrigé.

Dans certains cas la mise à jour des moteurs d'analyse via GUM peut échouer et atteindre le délai d'attente maximum. L'allongement de ce délai permet au GCenter d'effectuer l'ensemble des mises à jour nécessaires.

L'Emergency Mode a été optimisé en intégrant une meilleure itération des fichiers présents dans les différents répertoires et une meilleure gestion des erreurs lié à MALCORE.

Les événements powershell remontés par CODEBREAKER contenaient une valeur en SHA256 dans le champ MD5. L'information a été rectifié. Les événements powershell et shellcode remontés ont désormais les champs SHA256 et MD5. **Remarque** : Cette correction ne s'applique pas sur les anciens événements.

Lors d'une authentification avec un serveur LDAP (OpenLDAP uniquement) en TLS et avec un certificat autosigné au GCenter, les utilisateurs ne pouvaient pas s'authentifier. Ce problème a été corrigé.

L'indexation des documents provenant d'un événement de type "flow" contenant une valeur supérieure à 256 caractères dans le champ "flow.age" était impossible. La configuration ElasticSearch a été modifiée pour corriger ce problème.

Dans la configuration avancée d'un GCAP, si aucun ruleset n'était présent lors d'un "Save and Apply" une erreur 500 apparaissait sur la WebUI du GCenter . Ce problème est maintenant corrigé.

La suppression ainsi que l'édition des rulesets mis à jour depuis la version 2.5.3.10 vers la version 2.5.3.100 ne pouvaient être fait. Ce problème est maintenant corrigé.

5.4 Package 4 (HF4 / SHA256)

Codebreaker : Amélioration de la détection des scripts Powershell et réduction du taux de faux positifs.

Licensing : Ajout des CGU Gatewatcher - après l'application du hotfix, ces dernières sont automatiquement acceptées.

Configuration du proxy / Configuration du monitoring externe : la saisie d'une adresse incorrecte entraînait une erreur 500 . L'erreur est maintenant prise en charge et affiche un message d'erreur.

GUM - Updates : La mise à jour d'un ruleset ne s'effectuait pas correctement. Le ruleset original devait être régénéré afin de prendre en compte les nouvelles règles incluses dans la mise à jour. La mise à jour est maintenant automatique.

GUM - Updates : Si une nouvelle catégorie était ajoutée à une source, l'activation de celle-ci dans une règle liée n'était pas automatique. Ce défaut de mise à jour à été corrigé.

Sigflow Manager : Si une règle était liée à une autre, la désactivation de celle-ci retournait une erreur 500. Il est désormais possible de désactiver des règles liées entre elles sans produire d'erreur.

L'installation du GCenter en version 2.5.3.100-hf3 ou la mise à jour d'une version 2.5.3.10 vers une version 2.5.3.100-hf3 ne permettait pas la reconstitution des flow_id ainsi que l'indexation des fichiers dédupliqués par le GCap. Ce problème est maintenant résolu. Il est par ailleurs recommandé d'effectuer une installation en version 2.5.3.100-hf4.

Amélioration de la gestion des events: Logstash et Filebeat ont été mis à jour en version 7.9 pour améliorer la gestion du traitement des messages (Cf. release note Logstash et release note Filebeat)

L'orchestrateur interne du GCenter supervise désormais Logstash, permettant la gestion et la reprise sur erreur.

5.5 Package 5 (HF5 / SHA256)

GUM - Hotfix : À partir du package 5, tout correctif appliqué est automatiquement supprimé de la liste dès qu'il est appliqué. En mode LPM, l'application d'un correctif est impossible.

Export Syslog : Le gestionnaire de pipeline rencontrait un problème de redémarrage suite à l'installation d'un GCenter en version 2.5.3.100-hf4, la reprise de celui-ci est désormais opérationnelle. Des champs étaient manquants sur les index « malware », ils ont été réappliqués. Un champ « uuid » a été ajouté à tous les événements remontés.

Ruleset - Threshold : L'édition d'un Threshold rule nécessitait une double génération pour pouvoir fonctionner correctement. Désormais le Threshold rule est mis à jour dès la première génération du ruleset.

GCenter - logs : L'export des journaux du GCenter supérieur à 10GO pouvait rencontrer un problème. Celui-ci a été corrigé.

CODEBREAKER - Alerts : La remontée des alertes powershell dans les tableaux KIBANA pouvait être interrompue à cause de valeurs non prises en charges. La prise en charge de ces valeurs a été ajoutée.

SYSLOG -IDMEF : Lors d'un export syslog au format idmef, les journaux Heartbeats étaient manquants. Les éléments sont désormais présents, il faut néanmoins réappliquer la configuration syslog pour que le correctif soit appliqué.

GSCAN - PowerShell : L'analyse via GSCAN des PowerShell retournait systématiquement un message d'erreur en version 2.5.3.100-hf4. Les analyses se déroulent désormais correctement.

GSCAN -LPM : Lorsque la fonctionnalité LPM est activée, GSCAN est désactivé automatiquement par le GCenter. L'activation du GSCAN n'est pas possible tant que cette fonctionnalité est active.

Alertes : Aucune remontée d'alertes shellcode ou malware dans les tableaux Gatewatcher en version 2.5.3.100-hf4. Le problème a été corrigé.

Sigflow - Custom Source : l'édition d'une source personnalisée retournait une erreur. Il est désormais possible d'éditer une *custom source*.

Malcore - Alertes : Une incohérence entre les champs « engine_id » et « total_found » était présente. Celle-ci a été rectifiée.

5.6 Package 6 (HF6 / SHA256)

Important:

Ce HF doit être appliqué **comme une 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 pas être appliqué à chaud.

Important: Le HF6 ne peut être appliqué que sur un GCenter en v100 HF5. Les autres chemins d'upgrade ne sont pas supportés.

Avertissement: Après l'upgrade, le moteur malcore doit être mis à jour. Si vous êtes en mode online (voir Administrator > GUM > Config), cela peut prendre jusqu'à 15 minutes. En mode offline, vous devrez appliquer une mise à jour manuelle pour que malcore devienne fonctionnel.

Avertissement: Les fichiers à utiliser pour mettre à jour les moteurs sigflow et malcore ne sont plus les mêmes.

Le téléchargement manuel des mises à jour s'effectue depuis https://update.gatewatcher.com/update/2.5.3.100/gcenter/ :

- latest_sigflow_v3.gwp correspond à la mise à jour des règles sigflow.
- latest_malcore_v3.gwp correspond à la mise à jour du moteur malcore.
- latest_full_v3.gwp correspond aux mises à jour de malcore et sigflow combinées.

Avertissement: Lors du passage en HF6, le bug *profil malcore non préservé* peut se produire. De plus, *seuls 15 moteurs antiviraux seront disponibles*

Kernel - Instabilité du module IPSEC : Le noyau linux possédait un module relatif à ipsec susceptible d'entraîner des erreurs kernel (kernel oops). Le problème a été corrigé. (cf. *known bug*)

Mise à jour Malcore : Malcore a été upgradé en version 4, permettant une meilleure stabilité et corrigeant de nombreux problèmes. (cf. *accumulation de fichiers*, *association de fichiers*, *absence de flow_id*)

Mapping des champs malcore : Le mapping des champs des logs produits par malcore est désormais identique à celui de la version 2.5.3.101 documenté ici : https://docs.gatewatcher.com/fr/gcenter/2.5.3/101/definition_des_alertes/definition_des_alertes.html#malcore

Amélioration de la stabilité du moteur GOASM : le moteur d'analyse des shellcode a été revu afin d'accroître sa stabilité.

Amélioration de la sécurité de l'interface web : des vulnérabilités de type CSRF ont été corrigées.

Mise à jour des composants internes : les composants internes du Gcenter comme le moteur du serveur web ont été mis à jour.

5.7 Package 7 (HF7 (mode upgrade) / SHA256 // HF7 (mode hotfix) / SHA256)

Le HF7 corrige une mise à jour de licence interne au produit GCENTER et doit être appliqué impérativement avant le 31/12/2021. Ce hotfix ne s'applique que sur un GCENTER en version 100-HF6 (en mode upgrade ou hotfix).

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