Note de version
GCenter Version 2.5.3.103

Version de la note : V1

Date de création : Janvier, 2025

Dernière mise à jour : Janvier, 2025

Contents

Contents 1

1 Présentation de la version 2.5.3.103 du GCenter 3

2 Nouvelles fonctionnalités et améliorations 4
2.1 Moteurs et fonctionnalités de détection . . . 4
2.1.1 Moteur de détection DGA . . . 4
2.1.2 Moteur de détection Malcore . . . 4
2.1.3 Moteur de détection Beacon detect . . . 4
2.1.4 Moteur de détection Ransomware detect . . . 4
2.1.5 Moteur de détection GScan . . . 5
2.1.6 Fonctionnalité d'auto-threshold . . . 5
2.1.7 Fonctionnalité de multitenant pour les variables réseaux . . . 5
2.2 Analystes : WebUI et fonctionnalités . . . 5
2.2.1 Amélioration de la page d'accueil . . . 5
2.2.2 Amélioration de la gestion des alertes . . . 5
2.2.3 Filtrage des assets et des users . . . 6
2.2.4 Menu Malcore . . . 6
2.2.5 Menu Powershell et Shellcode detect . . . 6
2.2.6 Menu YARA . . . 6
2.2.7 Menu Active CTI . . . 6
2.2.8 Menu Sigflow manager . . . 6
2.3 Administration : WebUI et fonctionnalités . . . 6
2.3.1 Nouveau système de notifications . . . 6
2.3.2 Historisation des actes d'administration . . . 7
2.3.3 Standardisation du format des évènements . . . 7
2.3.4 Amélioration de l'export des données . . . 7
2.3.5 Menu GCap pairing . . . 7
2.3.6 Menu Software update . . . 7
2.3.7 Menu Threat DB update . . . 8
2.3.8 Menu Retention policy . . . 8
2.3.9 Menu Network settings . . . 8
2.3.10 Menu Licensing . . . 8
2.3.11 Menu Diagnostics . . . 8
2.4 WebUI – Tableaux de bord Kibana . . . 8
2.4.1 Améliorations des tableaux de bord existants . . . 8
2.4.2 Nouveau tableau de bord Beacon detect . . . 9
2.4.3 Nouveau tableau de bord Ransomware detect . . . 9
2.4.4 Nouveau tableau de bord Relations . . . 9
2.4.5 Nouveau tableau de bord Administration . . . 9
2.5 Système . . . 9
2.5.1 Mise à jour du système d'exploitation . . . 9
2.5.2 Mise à jour du noyau . . . 9

2.5.3 Mise à jour des composants . . . 9
2.5.4 Virtualisation . . . 9
2.5.5 Certificats ECDSA . . . 10
2.5.6 Outil de configuration du GCenter . . . 10
2.6 Autres améliorations . . . 10
2.6.1 Aide contextuelle . . . 10
2.6.2 Interopérabilité Reflex . . . 10
2.6.3 Amélioration de l'API . . . 10
2.6.4 Conformité PCI-DSS . . . 10
2.6.5 Authentification LDAP . . . 10
2.7 Autres changements . . . 10
2.7.1 Renommage `active-hunt` en `active-cti` . . . 10
2.7.2 Retrait d'interopérabilité . . . 11
2.7.3 Format IDMEF . . . 11

3 Correctifs **12**

4 Problèmes connus et limitations **13**
4.1 Active-CTI / RetroHunt - Problème post mise à jour . . . 13
4.2 Sauvegarde/Restauration GCenter - Gestion des erreurs . . . 13
4.3 Sauvegarde/Restauration GCenter - appairage du GCap . . . 13
4.4 État du GCap erroné suite à la mise à jour du GCenter . . . 13
4.5 Sigflow Manager - Transform Category . . . 14
4.6 Sigflow Manager - Erreur 500 lors de l'ajout d'une règle dans une source personnalisée . . . 14
4.7 Sigflow Manager - Incohérence dans l'affichage du nombre de catégories et de règles d'une catégorie 14
4.8 Configuration Sigflow - nom d'une source personnalisée ne peut contenir d'espace . . . 14
4.9 Sauvegarde/Restauration GCenter - erreur dans le FQDN . . . 15
4.10 Kibana - Erreur 500 suite au changement de support de stockage pour les données d'ES . . . 15

5 Compatibilité logicielle **16**
5.1 Compatibilité avec le GCap . . . 16

6 Compatibilité matérielle **17**

7 Hotfix **18**

8 Procédure de montée de version de V102 à V103 **19**
8.1 Prérequis . . . 19
8.2 Données conservées . . . 19
8.3 Procédure d'installation avec conservation des données . . . 20

Chapter 1

Présentation de la version 2.5.3.103 du GCenter

Cette note de version décrit :

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

Chapter 2

Nouvelles fonctionnalités et améliorations

2.1 Moteurs et fonctionnalités de détection

2.1.1 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
- la possibilité de gérer la sensibilité du moteur avec six niveaux différents
- un système qui aide les analystes dans la configuration de la liste des domaines devant être ignorés

---

2.1.2 Moteur de détection Malcore

Une nouvelle version du moteur Malcore est disponible améliorant ses performances et sa stabilité.

2.1.3 Moteur de détection Beacon detect

Un moteur de détection des balises relatives aux infrastructures de commande et de contrôle (C&C) est maintenant disponible afin de détecter les communications chiffrées entre un hôte infecté et un serveur C&C.
Un système est présent pour aider les analystes dans la configuration de la liste des adresses IP devant être ignorées.

2.1.4 Moteur de détection Ransomware detect

Un moteur de détection des rançongiciels est maintenant disponible afin de détecter les activités de ce type de logiciel malveillant sur le protocole SMB.
Il est possible :

- de gérer la sensibilité du moteur avec 6 niveaux différents
- d'investiguer en se basant sur l'identifiant d'une session SMB
- d'ajouter des adresses IP dans une liste blanche

2.1.5 Moteur de détection GScan

L'interface du moteur GScan a été améliorée pour donner plus de détails sur les fichiers analysés sur demande.

2.1.6 Fonctionnalité d'auto-threshold

Une nouvelle fonctionnalité `auto-threshold` est disponible pour limiter le nombre d'alertes générées par le moteur Sigflow.
Cette fonctionnalité est basée sur des règles de threshold qui seront directement appliquées au moteur Sigflow.
Un analyste pourra utiliser l'un des sept profils de configuration existants ou configurer un profil personnalisé.

2.1.7 Fonctionnalité de multitenant pour les variables réseaux

Une nouvelle fonctionnalité permettant d'améliorer le support des architectures de type `multitenant` est disponible pour le moteur Sigflow.
Cette fonctionnalité offre la possibilité de déclarer :

- une variable ayant une configuration différente par tenant
- une variable de type `adresse réseau` personnalisée
- une variable de type `port réseau` personnalisée

2.2 Analystes : WebUI et fonctionnalités

2.2.1 Amélioration de la page d'accueil

La page d'accueil a été améliorée afin de visualiser rapidement les informations importantes pour les analystes et les administrateurs.

2.2.2 Amélioration de la gestion des alertes

Le système de gestion des alertes a été amélioré permettant :

- d'acquitter les alertes
- de rendre les alertes silencieuses
- de trier les alertes selon différents critères (niveau de risque, nom, date, nombre d'occurrences)
- de gérer les alertes en masse

Les alertes qui ont été acquittées sont exclues du calcul du niveau de risque.

2.2.3 Filtrage des assets et des users

Dans la barre de recherche, il est maintenant possible de filtrer les assets et les users suivant un niveau de risque (`risk_min` et `risk_max`).

2.2.4 Menu Malcore

Une nouvelle interface est disponible pour la gestion du moteur Malcore.
Deux options ont été ajoutées pour ignorer les alertes en se basant sur un nom de fichier ou celles générées par un moteur spécifique.

2.2.5 Menu Powershell et Shellcode detect

Une nouvelle interface est disponible pour la gestion du moteur Powershell et Shellcode detect.

2.2.6 Menu YARA

Une nouvelle interface est disponible pour la gestion des règles YARA.

2.2.7 Menu Active CTI

Une nouvelle interface est disponible pour la gestion de la CTI.

2.2.8 Menu Sigflow manager

Le bouton `generate rule file` a été remplacé par un bouton `save` qui se situe en haut à droite du menu de configuration d'un `ruleset` afin de sauvegarder les modifications apportées à la politique appliquée au moteur Sigflow.

2.3 Administration : WebUI et fonctionnalités

2.3.1 Nouveau système de notifications

Un nouveau système de notification présent dans le menu `Health` est disponible pour avertir les utilisateurs des dysfonctionnements de certains composants de la solution.
Une notification peut être déclenchée dans de nombreuses situations :

- problèmes de mise à jour des moteurs
- problèmes de configuration

- problèmes de connexion entre le GCap et le GCenter
- problèmes de compatibilité
- problèmes de performances...

Il est possible de rendre silencieuses ces notifications ou bien encore de les acquitter.

2.3.2 Historisation des actes d'administration

Une nouvelle fonctionnalité a été développée pour historiser les actions des utilisateurs.
Les évènements qui sont générés peuvent être exportés vers un serveur Syslog.

2.3.3 Standardisation du format des évènements

Un nouveau format des évènements, ECS (Elastic Common Schema), est disponible pour les alertes, les metadata ainsi que les évènements d'administration.
Un mode de compatibilité existe, pour l'export de données, permettant de conserver l'ancien format qui sera retiré lors de la prochaine version majeure.

2.3.4 Amélioration de l'export des données

La fonctionnalité d'export de données permet maintenant :

- de filtrer les alertes par moteur
- d'exporter les évènements systèmes

2.3.5 Menu GCap pairing

Une nouvelle interface est disponible pour la gestion de l'appairage du GCap au GCenter.
Un menu d'assistance a été ajouté pour faciliter la configuration.

2.3.6 Menu Software update

Une nouvelle interface est disponible pour la gestion des mises à jour système.

2.3.7 Menu Threat DB update

Une nouvelle interface est disponible pour la gestion des mises à jour des moteurs de détection.
Plusieurs options ont été ajoutées :

- la gestion de la fréquence des mises à jour du GCap
- la possibilité de télécharger les mises à jour en plusieurs parties
- la possibilité d'utiliser un serveur local en HTTPS

2.3.8 Menu Retention policy

Une nouvelle interface est disponible pour la gestion de la rétention des données stockées dans Elastic Search.
Il est maintenant possible de gérer l'espace alloué pour les alertes, les metadata et les évènements d'administration.

2.3.9 Menu Network settings

Une nouvelle interface est disponible pour visualiser les paramètres de configuration du réseau.

2.3.10 Menu Licensing

Une nouvelle interface est disponible pour la gestion des licences.

2.3.11 Menu Diagnostics

Une nouvelle interface est disponible pour la génération des journaux systèmes et du tech support.

2.4 WebUI – Tableaux de bord Kibana

2.4.1 Améliorations des tableaux de bord existants

Les tableaux de bord existants ont été restructurés afin d'avoir une meilleure visibilité et faciliter l'investigation.

2.4.2 Nouveau tableau de bord Beacon detect

Un nouveau tableau de bord est disponible pour pouvoir consulter les évènements du moteur Beacon detect.

2.4.3 Nouveau tableau de bord Ransomware detect

Un nouveau tableau de bord est disponible pour pouvoir consulter les évènements du moteur Ransomware detect.

2.4.4 Nouveau tableau de bord Relations

Un tableau de bord pour les relations entre les différentes adresses IP remontées dans la solution est disponible dans le menu `Hunting > Network Metadata > Relations`.

2.4.5 Nouveau tableau de bord Administration

Un nouveau tableau de bord est présent pour pouvoir consulter les évènements d'administration.

2.5 Système

2.5.1 Mise à jour du système d'exploitation

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

2.5.2 Mise à jour du noyau

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

2.5.3 Mise à jour des composants

Les différents composants du système d'exploitation ont été mis à jour.

2.5.4 Virtualisation

Le GCenter est officiellement supporté sur les hyperviseurs ESXi de VMware.

2.5.5 Certificats ECDSA

Les certificats ECDSA sont supportés pour la sécurisation de l'accès à l'interface web du GCenter.

2.5.6 Outil de configuration du GCenter

L'outil de configuration du GCenter a été amélioré pour faciliter la configuration du réseau et pour ajouter des clés SSH à l'utilisateur `setup`.

2.6 Autres améliorations

2.6.1 Aide contextuelle

Une aide contextuelle est disponible au niveau de l'interface web du GCenter.

2.6.2 Interopérabilité Reflex

Un nouveau menu est disponible pour s'interconnecter avec la solution Reflex.

2.6.3 Amélioration de l'API

De nouveaux point d'API ont été ajoutés pour permettre d'automatiser certaines actions.

2.6.4 Conformité PCI-DSS

Une nouvelle option a été ajoutée pour remplacer les numéros de carte de crédit par un mot clé spécifique.

2.6.5 Authentification LDAP

Lors de la connexion utilisant un serveur LDAP pour l'authentification, si le compte utilisé est présent dans la base locale du GCenter, il est alors désactivé pour éviter les conflits.

2.7 Autres changements

2.7.1 Renommage `active-hunt` en `active-cti`

Le classtype des règles suricata générées par active CTI est renommé en `active-cti`.

2.7.2 Retrait d'interopérabilité

Les interconnexions avec les solutions suivantes ont été retirées :

- Intelligence
- Hurukai

2.7.3 Format IDMEF

Le format IDMEF n'est plus supporté lors de l'export des évènements vers un serveur Syslog.

Chapter 3

Correctifs

Section laissée vide intentionnellement

Chapter 4

Problèmes connus et limitations

4.1 Active-CTI / RetroHunt - Problème post mise à jour

Dans certains cas, Active-CTI et RetroHunt (disponible avec la licence LIS) pourraient ne pas fonctionner de manière optimale.

Solution de contournement : contacter le support technique de Gatewatcher.

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 bloquée 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 État du 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.

4.5 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.

4.6 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.

4.7 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.

4.8 Configuration Sigflow - nom d'une 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.

4.9 Sauvegarde/Restauration GCenter - erreur dans le FQDN

Dans la version v2.5.3.103, 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.

4.10 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.

Chapter 5

Compatibilité logicielle

5.1 Compatibilité avec le GCap

Version du GCenter	Version du GCap	Compatibilité
2.5.3.103	2.5.3.105	Configuration non supportée : GCap à migrer en amont de la mise à jour du GCenter
2.5.3.103	2.5.4.0 (ou +)	Configuration ok

Chapter 6

Compatibilité matérielle

La version 2.5.3.103 est compatible avec toutes les versions matérielles des GCenter.

Référence GCENTER	Stockage local	Autre stockage	Interface réseau	Alimentation électrique
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

Section laissée vide intentionnellement

Chapter 8

Procédure de montée de version de V102 à V103

8.1 Prérequis

Pour déployer la mise à jour **V2.5.3.103** :

- le GCenter devra être en version **V2.5.3.102-HF3** ou supérieure
- le GCap devra être en version **V2.5.4.0** ou supérieure
- 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. Dans le cas contraire, il faudra avoir un accès physique à l'équipement (écran, clavier).

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 et des données du GCenter sont conservées.

8.3 Procédure d'installation avec conservation des données

1. Vérifier que les sondes GCap sont en version **V2.5.4.0** ou supérieure, sinon se référer à la procédure de mise à jour suivante: https://releases.gatewatcher.com/fr/gcap/2.5.4/V0/8_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 2.5.3.103).
3. Faire la vérification de l'image avec le sha256 associé.
4. Se connecter à la WebUI du GCenter et aller dans le menu `Admin > GUM > Software update`.
5. Dans la section `Uploading a new software update`, cliquer sur le bouton `Choisir un fichier`, sélectionner la nouvelle version du GCenter précédemment téléchargée puis cliquer sur `Submit`.
6. Se connecter en SSH sur le GCap avec le compte **setup**.
7. Stopper le moteur de détection avec la commande suivante : `monitoring-engine stop`.
8. Modifier le mode de compatibilité avec la commande suivante : `set compatibility-mode 2.5.3.103`.
9. Démarrer le moteur de détection avec la commande suivante : `monitoring-engine start`.
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 Note de version`