GATEWATCHER

Release Notes

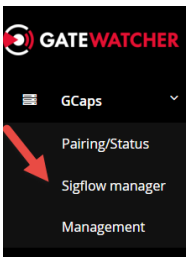
Version 2.5.0

15 Juillet 2017

➢ Nouvelles fonctionnalités :

1. Centralisation de la gestion des signatures / IOC

Désormais la gestion de SIGFLOW se fait en central sur le GCENTER. Vous pouvez appliquer un profil (ruleset) sur chaque sonde de manière simple et rapide.

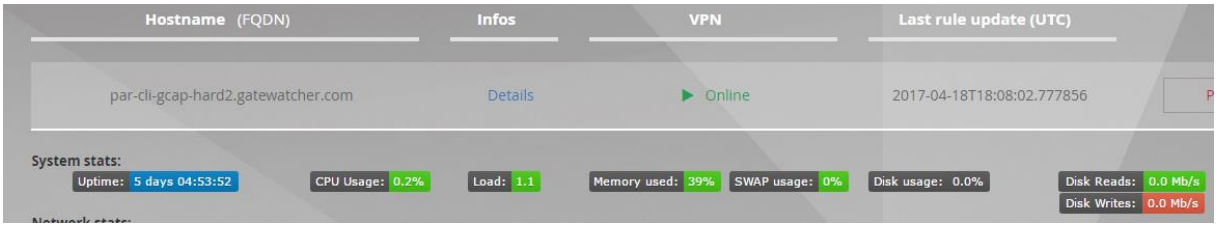


2. Maj des signatures en direct sur le statut :

La date de dernière MAJ des GCAP est affiché en temps réel pour savoir si le GCAP bénéficie des dernière MAJ présente sur le GCENTER.

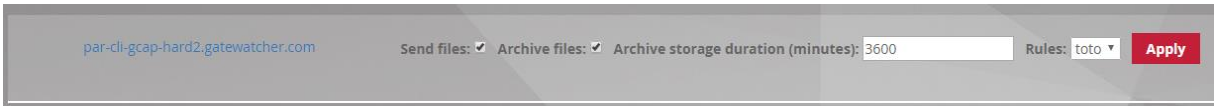
3. Supervision des GCAP en temps réel :

Le GCENTER centralise automatiquement l'ensemble des informations critiques du GCAP.



4. Paramétrage OIV directement depuis l'interface du GCENTER :

Les paramétrages relatifs à la LPM sont désormais disponibles directement de manière centralisée.



5. **Suppression totale du GVIEW :**

Le GVIEW était une Appliance supplémentaire obligatoire pour les PDIS. Après discussion avec l'ANSSI et obtention de leur accord, nous avons réussi à supprimer ce dernier et à proposer une fonctionnalité de remplacement directement sur le GCAP.

6. **GCAP KVM : disponible en VM jusqu'à 1GB**

7. **GCAP VMware : 10 GB disponible (16 vCPU minimum)**

8. **Split des interfaces d'administration et de tunnel IPSEC depuis l'interface du GCENTER**

9. **GCENTER-SETUP : disponible pour tous les paramétrages initiaux comme pour le GCAP**

10. **Dashboard SYSLOG :**

Permet de voir tous les messages d'erreur / warning / info des GCAP (pour diag avancé).

11. **Dashboard expérimental ALL IN ONE :**

Adapté pour les SOC il permet de voir en temps réel sur une même interface les attaques de tout type.

12. **Dashboard ICAP :**

Adapté pour consulter les logs de la partie Proxy / ICAP. A noter que ce dashboard est lié à l'évolution permettant de visualiser les logs provenant de ICAP.

13. **Configuration des certificats SSL :**

Upload des certificats de l'entreprise pour éviter l'utilisation d'un certificat auto généré.

14. **Dépôt local des MAJ :**

Permet de paramétrer les MAJ sur un repo local externe (obligatoire dans PDIS).

15. **Retroanalyse des fichiers sains :**

Option permettant de rétro analyser l'ensemble des fichiers sains (à utiliser sur des petits périmètres …).

16. **API GW :**

Ouverture à l'extérieur pour la partie GSCAN.

17. **GCAP 40 GB BETA TEST**

Grâce aux nouveaux drivers d'acquisition, le GCAP est désormais capable d'atteindre 40 GB.

[METTRE UN SCREENSHOT]

18. **Choix des méthodes d'acquisition réseau sur le GCAP**

Permet de sélectionner les différentes méthodes d'acquisition pour améliorer les performances.

➢ Améliorations fonctionnelles :

1. **Appairage simplifié et beaucoup plus rapide :**

Le processus d'appairage d'un GCAP avec un GCENTER se fait beaucoup plus rapidement. Vous pouvez le refaire à la volée via le bouton « Pair this gcap again »

2. **Upload des fichiers en central :**

Désormais la remonté des fichiers se fait de manière beaucoup plus rapide (20 à 30X selon nos tests)

3. **Dashboard TACTICAL 5.14**

4. **Paramétrage d'un mdp pour les malwares téléchargés**

5. **Utilisation de MALCORE avec ICAP (compatible WEBSENSE / BLUECOAT / SQUID)**

Paramétrage depuis l'interface du GCENTER.

6. **GCAP 10 GB Full RATE**

Elimination des derniers problèmes dus aux nombre de sessions http (> 200 000) à 10 GB.

7. **GSCAN possède des messages d'erreurs beaucoup plus spécifiques**

8. **SHELLCODES**

Décodage des shellcodes non encodés X86.

9. **Détection de Malware :**

Travail sur les nouvelles versions de VEIL FRAMEWORK (la future version possédera une fonction dédiée anti VEIL).

10. **Export KAFKA SIEM :**

Amélioration de l'export KAFKA depuis le GCENTER (avec l'utilisation de champs additionnels).

11. Export :

Possibilité de filtrer sur ce qui est envoyé vers le SIEM (alertes uniquement ou tous les messages).

12. MAJ offline :

Désormais le GCENTER indique l'avancement des MAJ OFFLINE (in Progress).

13. Malcore :

Elimination de beaucoup de faux positifs + taux de détection amélioré de 30 à 40 % minimum.

14. Alertes :

Création d'un ID unique pour toutes les alertes (pour favoriser le traitement dans un SIEM).

15. LDAP : intégration de LDAP pour l'authentification centralisée

Authentification centralisé intégré avec AD (Microsoft) / LDAP (v2 et v3).

16. Refonte des dashboards GATEWATCHER (timeline – visuel – recherches)

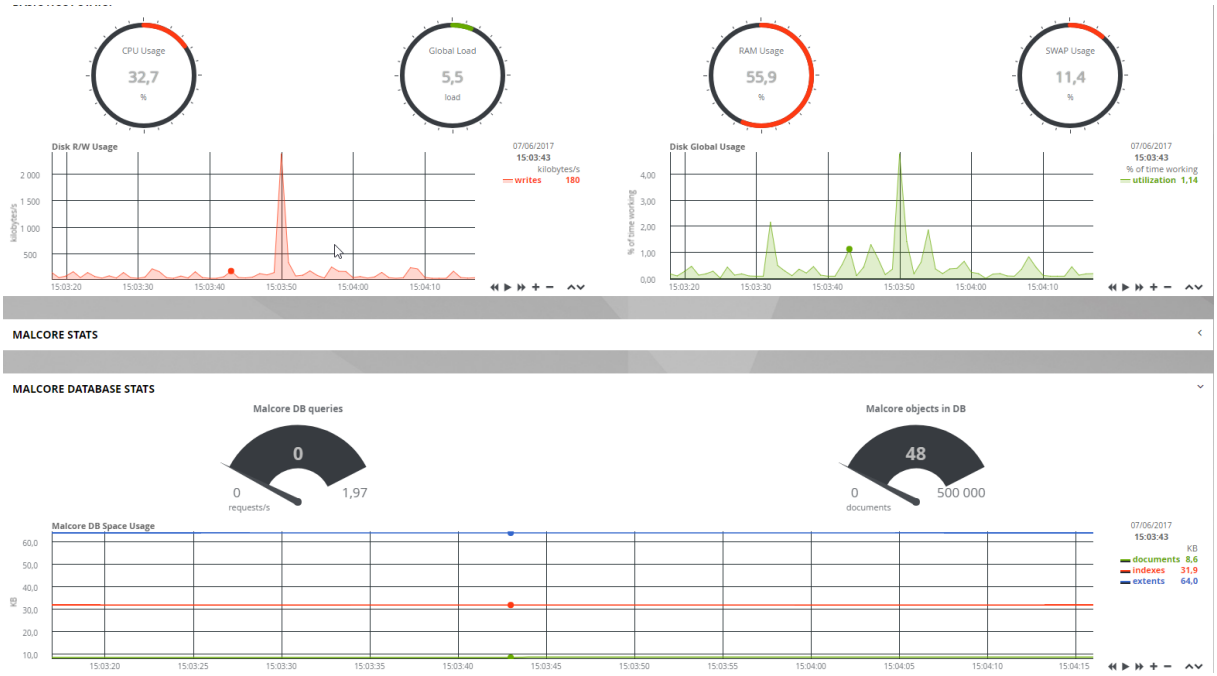
Les dashboards ont été complètement refondus afin de faciliter la recherche sur des périodes de temps spécifiques. Le visuel a été largement amélioré.

17. Emergency recover

Permet de supprimer automatiquement les données ES (les plus anciennes) si le disque arrive à saturation pour éviter les erreurs / corruption. Permet également de reprendre même si un crash hardware a provoqué des éventuelles erreurs.

18. **Supervision GCENTER**

Disponible en local de manière très précise avec de nouveaux indicateurs. Refonte totale niveau visuel



➢ Améliorations techniques :

1. Durcissement PAX renforcé
2. Réduction de la surface d'attaque du GCAP
3. Nouveaux outils de ligne de commande disponible sur le GCAP (principalement réseaux)
4. Meilleure gestion de NTP et des timestamps
5. Sécurisation du boot des GCAP
6. Suppression des fichiers tronqués
7. Message d'erreurs suricata vers un fichier dédié
8. Auto suppression des logs lorsque le disque arrive à saturation
9. Gcenter en mode « Gentoo » : le GCENTER a pour objectif d'être également qualifié par l'ANSSI. Le « Build » du GCAP est désormais le même pour le GCENTER. A terme le GCENTER sera autant durci que le GCAP (si possible)
10. SSO SIGFLOW Manager / Authentification GCENTER

➢ BugFixes :

CRITICAL :

1. Suricata crash par intermittence : résolution du memory leak et supervision avancée du démon avec redémarrage immédiat

2. Kernel panic / CPU SOFT LOCKUP sur certains matériel / processeur INTEL : le problème provenait des librairies de chiffrement optimisé par INTEL et l'utilisation de certains instructions CPU.

High priority :

1. Disparition des problèmes d'appairage de manière aléatoire. (error & timeout)

2. Fichiers « truncated » : les fichiers apparaissaient tronqués alors qu'ils ne l'étaient pas.

Low priority :

1. Correction des attachment SMTP qui n'apparaissaient pas dans les champs présents

2. Magic Bytes / MD5 non présent pour les fichiers analysés

3. Téléchargement des malwares parfois impossible

4. Fonts google qui tentaient de communiquer vers l'extérieur

5. Logs ICAP non disponible

6. Problème de droits au niveau du GCENTER avec la cible ANSSI

➢ Known bugs :

High priority :

1. Icap : blocage de certains fichiers sans raison sur le proxy au travers de la réponse ICAP

2. Débrayage syslog / kafka

Low priority :

1. Droits des utilisateurs spécifiques sur le GCENTER non fonctionnel

➢ BETA OUVERTE :

1. GATEWATCHER INTELLIGENCE : inscription sur https://intelligence.gatewatcher.com

2. Plateforme d'analyse avancée des menaces (Cloud)

3. Module Navigateur CHROME / FIREFOX : disponible en téléchargement sur GATEWATCHER INTELLIGENCE dans votre menu d'administration.

➢ COMING SOON :

1. ROP Detection V2

2. Cluster GCENTER

3. Supervision espace disque GCENTER

4. GCAP - GCENTER LIGHT LPM ONLY