RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CyberOPS cnes

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

BILAN DÉPLOIEMENT
EDR AU CNES

CAPITOUL

25/04/2024

SOMMAIRE

Pourquoi Harfanglab ?

L'architecture déployée

Politiques mises en œuvre

La « plaie » du white listing

Les premiers résultats

Ce qu'on aimerait voir arriver

ENDPOINT DETECTION AND RESPONSE

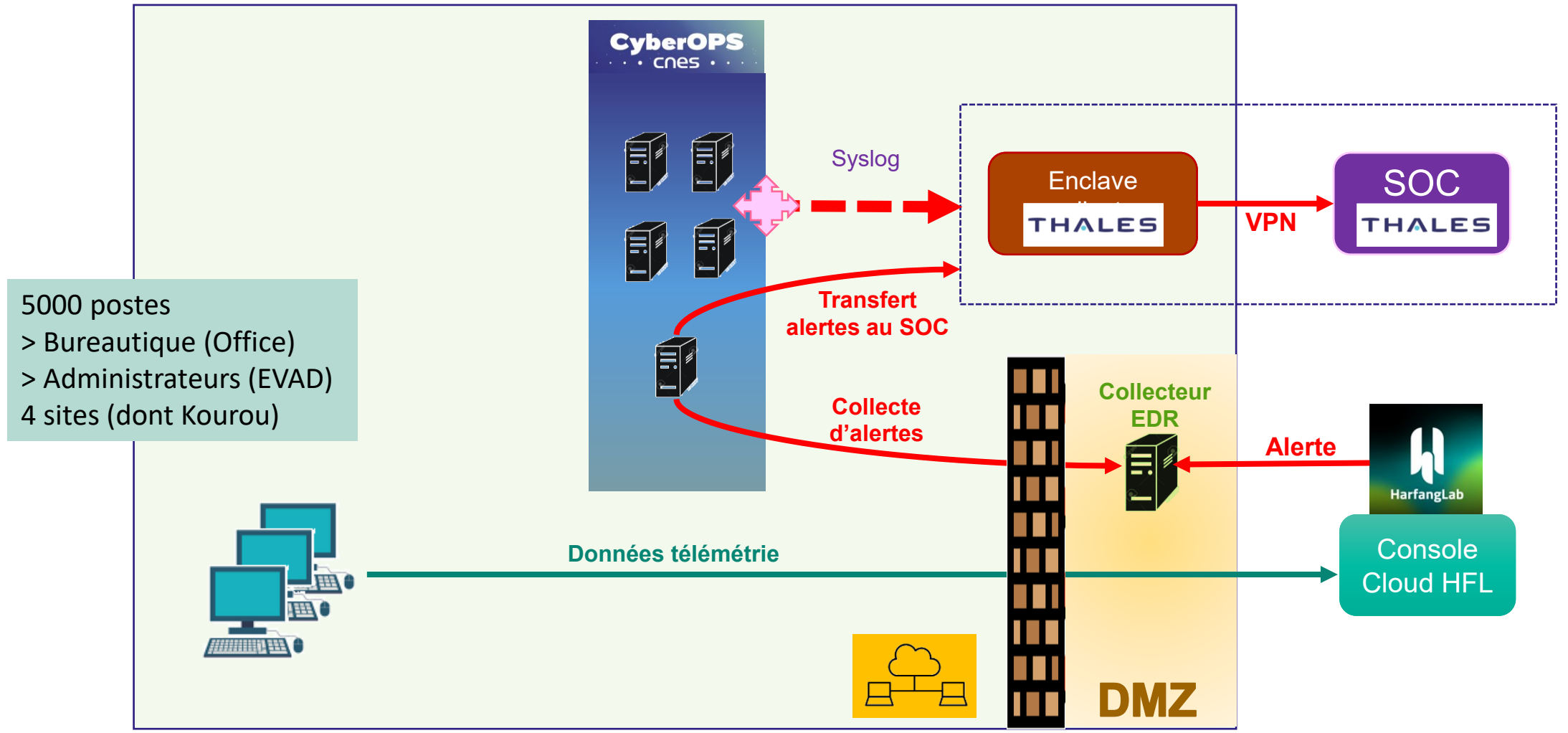
POURQUOI HARGANGLAB ?

Premier et seul EDR certifié par l'ANSSI et reconnu par le BSI en Allemagne.

*« **Une capacité de détection de haut-niveau :** reconnue lors des évaluations du MITRE 2023, tant dans la détection que dans la capacité d'analyse.*
Top 10 des EDR du marché & Top 3 des EDR européens.»

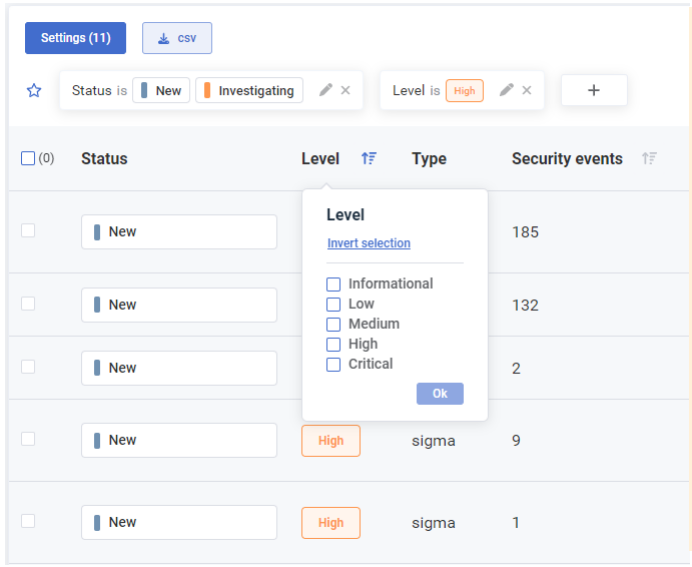
*« **Cinq moteurs de détection complémentaires, et des modèles IA au service de notre solution :** des modèles de machine learning et de deep learning déployés au sein de notre agent pour identifier finement les menaces et y répondre avec le moins de faux positifs du marché.»*

ARCHITECTURE LOGIQUE DE L'EDR AU CNES



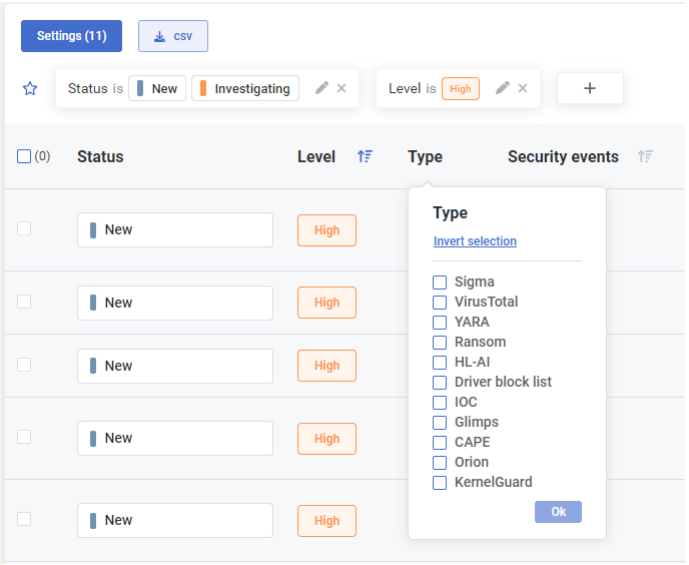
5000 postes
> Bureautique (Office)
> Administrateurs (EVAD)
4 sites (dont Kourou)

PK C'EST LONG DE WHITE LISTER CE QU'ON A RETENU AU CNES



Même si les postes sont issus d'un master, chaque poste n'est pas rigoureusement identique à son voisin, donc autant d'évènements différents à statuer.
A noter la « plaie » des devs « perso » : scripts en divers langages, macros diverses, …

Il a fallu ~2 mois à une personne , 2 jours / semaine avec les paramètres ci-dessous



TROP d'évènements générés si on coche tout !

Level : High et Critical only

Type : 5 seulement (driver block list, SIGMA, YARA, IOC, Ranson Guard)

A noter : obligé de désactiver HL-AI, générait trop d'alertes !

L'IA pas encore au point.

Sortie d'une nouvelle version imminente.

Level	Nombre alertes
Low + Medium	293 000
High	12 000
Critical	1802

LES PREMIERS RETOURS !

L'EDR a permis de détecter plusieurs comportements malveillants :

- Un certain nombre de personnes jouant à des jeux sur leur PC bureautique (1)
- La détections de scripts développés en internes et potentiellement malveillants/non conformes (exemple des scripts move_mouse que l'on a pu voir régulièrement). (2)
- L'utilisation de RAT (Remote Access Tools), comportement qui n'est pas autorisé sauf cas très exceptionnels. Une liste de RAT a été définie, et une règle de détection a été mise en place pour détecter et bloquer (grâce à une blocklist) l'exécution de tels outils.(3)
- Quelques autres exemples comme l'ajout de comptes au groupe admin, des exécutions suspectes de processus (par exemple avec des doubles extensions), des captures de trames réseaux...(4)

Des tests ont également pu être effectués pour :

- Créer des listes d'IOC pouvant se baser sur un nom de fichier, un chemin, un hash, une IP, un nom de domaine... avec la possibilité d'en bloquer l'accès/l'exécution.
- Créer de nouvelles règles de détection (Sigma/Yara).
- Récupération d'un fichier détecté comme malveillant (au format .bin, dans un zip protégé) pour analyse forensic.

1. ~ +/- 20
2. C'est quelques milliers d'évènements ici (non pas d'incidents créés), le cas a été légitimé et mis en whitelist.
3. ~ +/- 10
4. ~ +/- 50

CE QU'IL NOUS MANQUE

La récupération de binaire :

- Ne peut être bloquée par le « super admin »
- Ne peut être soumise à l'autorisation d'une tierce personne
- Ne peut être soumise à l'autorisation de l'utilisateur
- Se fait sans que l'utilisateur en soit informé

Nous avons développé une règle permettant de détecter :

- Les job de téléchargements de fichier directement sur une workstation

- Les téléchargements de binaires via un SecurtityEvents format .bin, dans un zip protégé) pour analyse forensic.

Le blocage de l'exécution d'un binaire

- Se fait sans que l'utilisateur en soit informé (que le binaire est bloqué pour raison ssi …)

Nous avons développé une règle de « détection d'un blocage par l'EDR »

- Nous avons des signatures EDR "*IOC alert : blacklist process activity*" qui sont pris en comptes dans les règles en production sur le SIEM.

MERCI

CyberOPS
cnes

Contact : louis.jimenez@cnes.fr