Université Grenoble Alpes

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

Par Frédéric Girousse et Luisa Bouteille

Sommaire

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 télémétrie

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

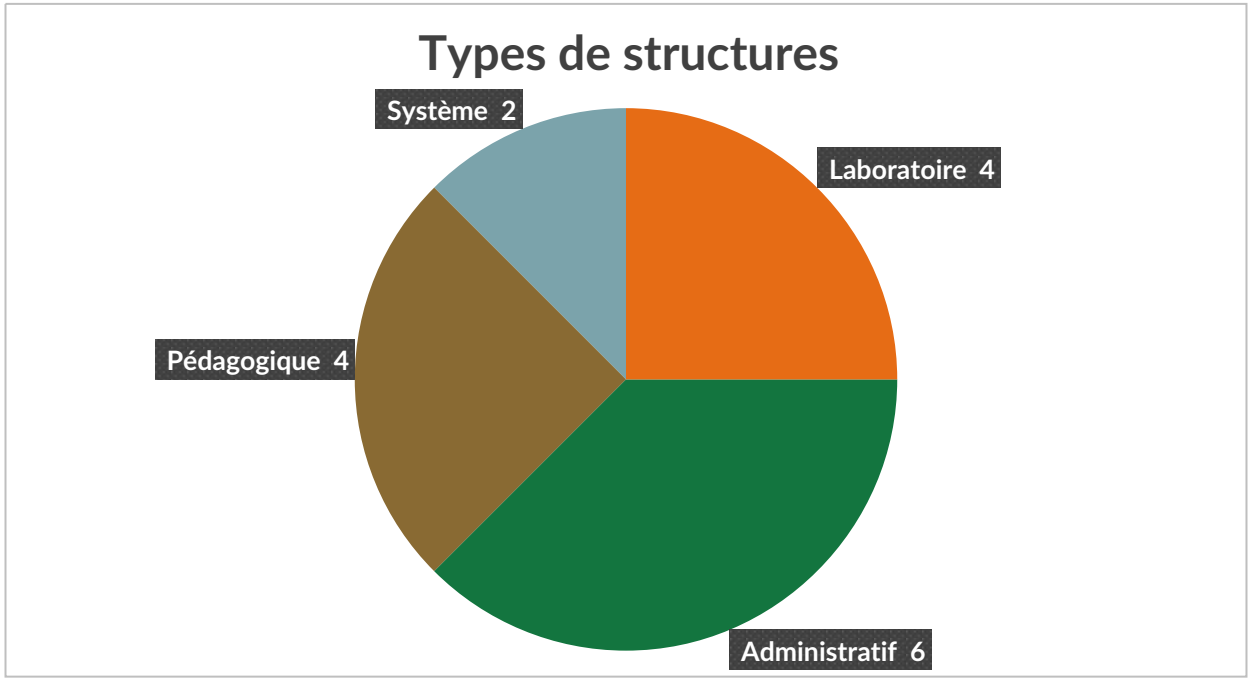
détection failles sécurités sur drivers

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

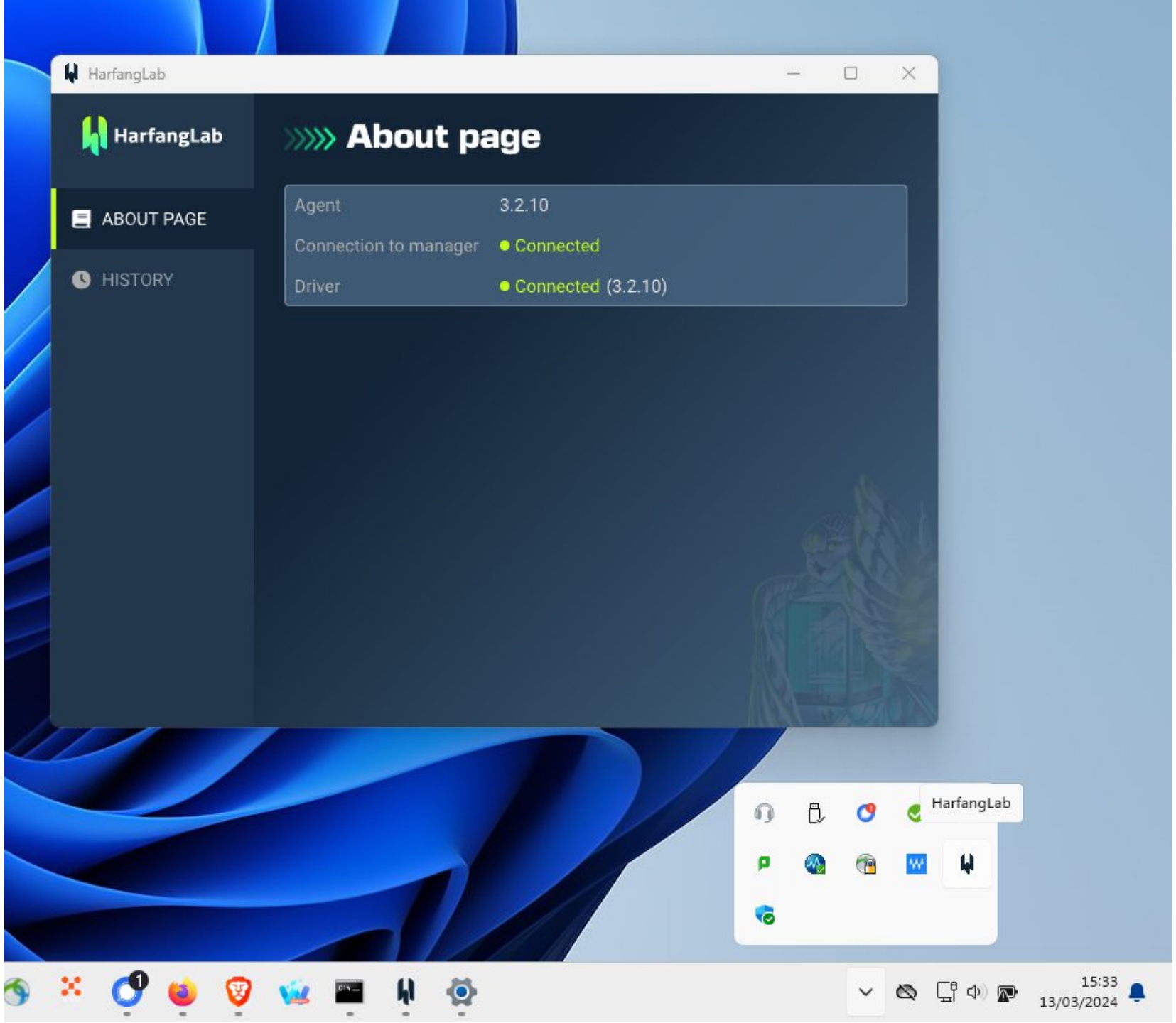
Déploiement simple et silencieux
via notre outil PDQ
ou tout autre moyen

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
ABOUT PAGE
HISTORY
Agent
3.2.10
Connection to manager
Connected
Driver
Connected (3.2.10)
HarfangLab
15:33
13/03/2024

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

Affectation de **Policies** selon les groupes

Création de 64 groupes

Création de 8 policies 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 : whitelistage

PROTECT

inventaire

remontée
de détection

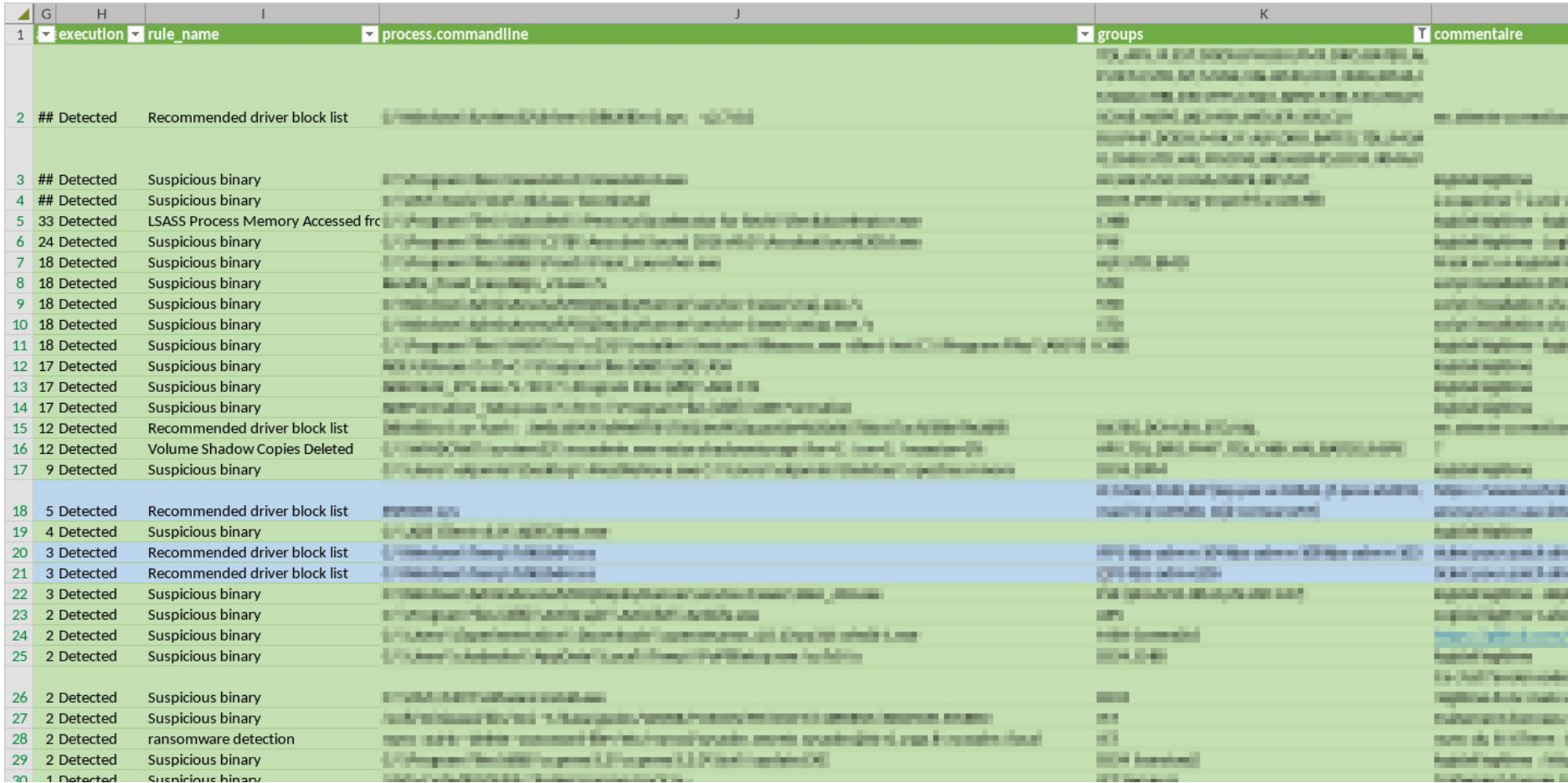
blocage automatique
des processus
malicieux

Whitelistage

6 passes de Whitelistage

200 détections « critiques » auditées

découvertes de failles de sécurités « drivers »



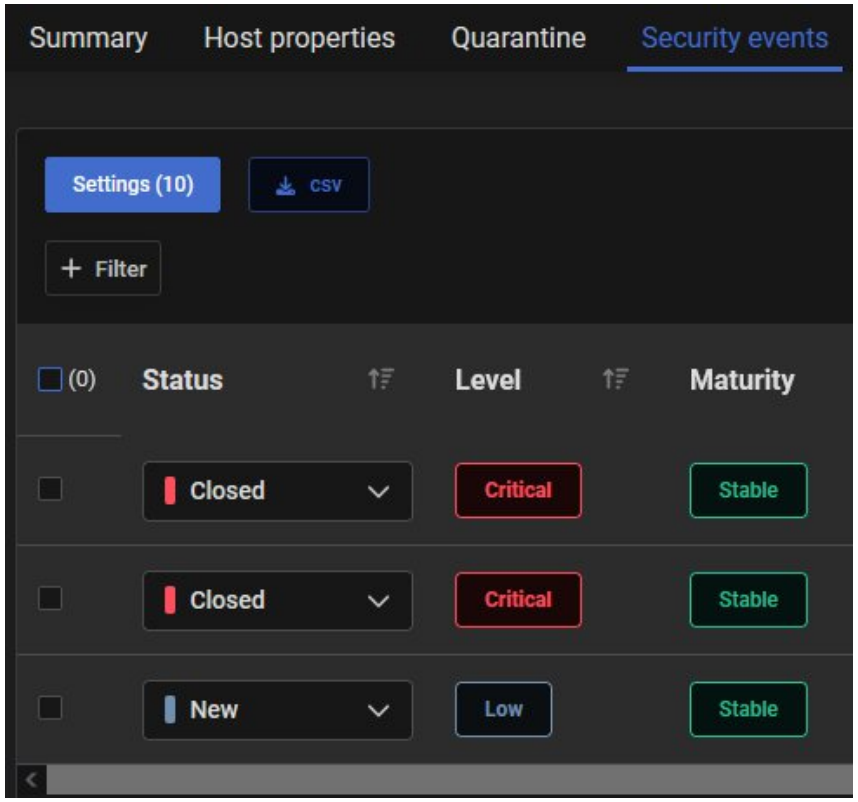
	G	H	I	J	K	
1		execution	rule_name	process.commandline	groups	commentaire
2		## Detected	Recommended driver block list			
3		## Detected	Suspicious binary			
4		## Detected	Suspicious binary			
5		33 Detected	LSASS Process Memory Accessed fro			
6		24 Detected	Suspicious binary			
7		18 Detected	Suspicious binary			
8		18 Detected	Suspicious binary			
9		18 Detected	Suspicious binary			
10		18 Detected	Suspicious binary			
11		18 Detected	Suspicious binary			
12		17 Detected	Suspicious binary			
13		17 Detected	Suspicious binary			
14		17 Detected	Suspicious binary			
15		12 Detected	Recommended driver block list			
16		12 Detected	Volume Shadow Copies Deleted			
17		9 Detected	Suspicious binary			
18		5 Detected	Recommended driver block list			
19		4 Detected	Suspicious binary			
20		3 Detected	Recommended driver block list			
21		3 Detected	Recommended driver block list			
22		3 Detected	Suspicious binary			
23		2 Detected	Suspicious binary			
24		2 Detected	Suspicious binary			
25		2 Detected	Suspicious binary			
26		2 Detected	Suspicious binary			
27		2 Detected	Suspicious binary			
28		2 Detected	ransomware detection			
29		2 Detected	Suspicious binary			
30		1 Detected	Suspicious binary			

Investigation

Investigation

Blocage processus AUTOMATIQUE

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

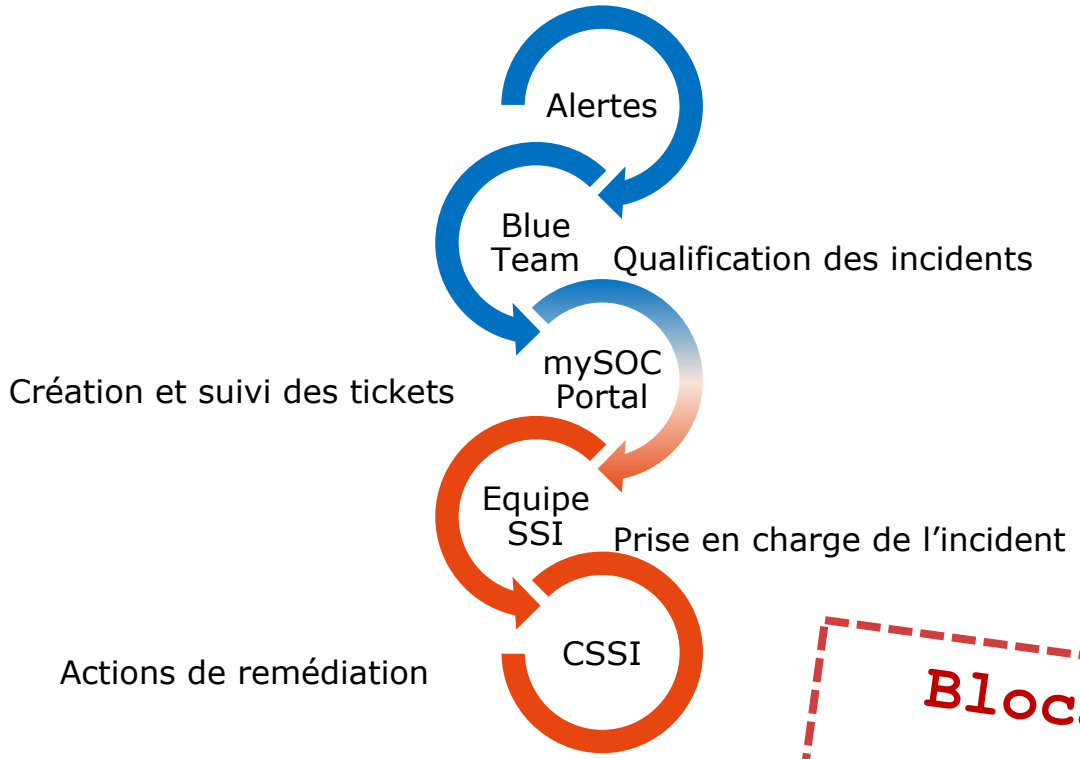


Investigation via **télémétrie** en temps réelle

- 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



Blocage flux reseau MANUEL

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 :

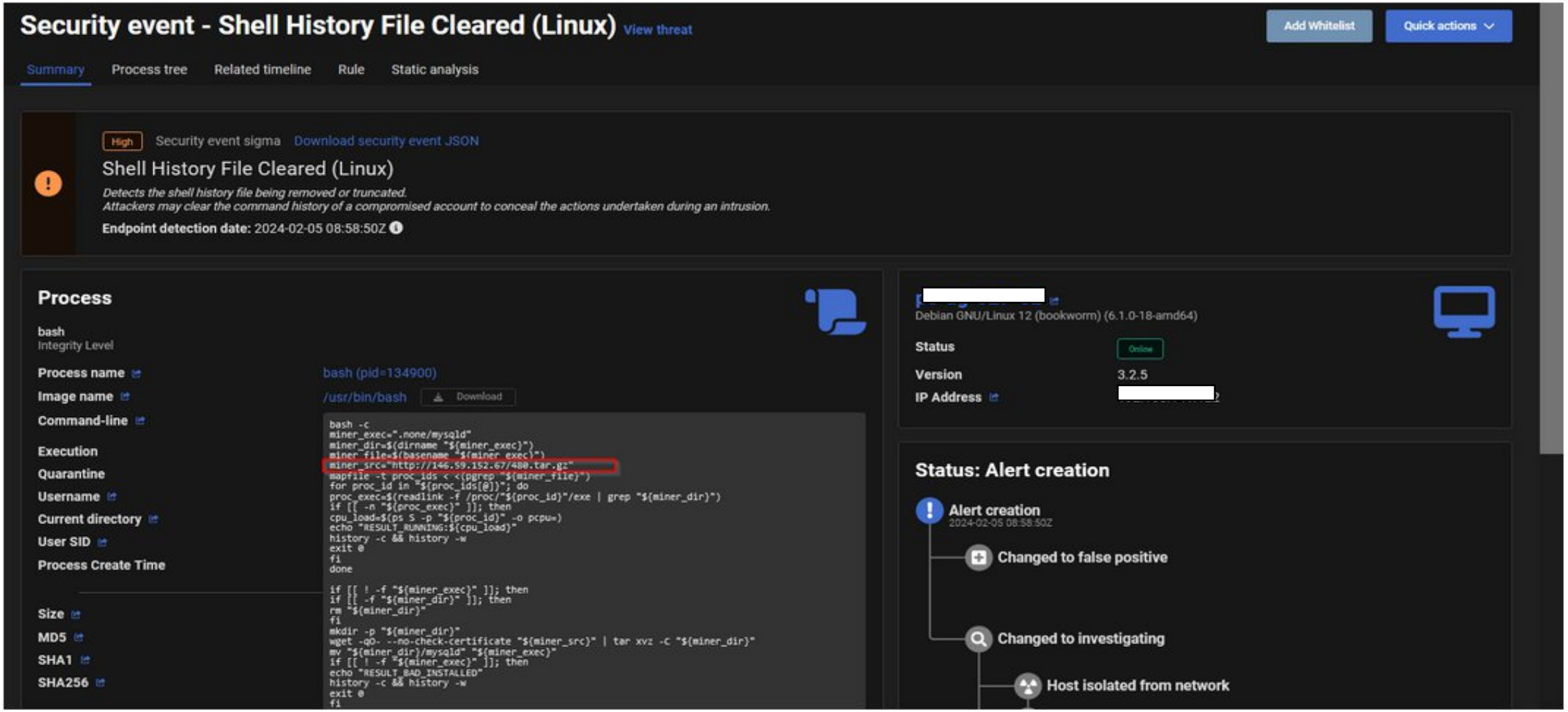
- Detect

Lien EDR :

- [redacted]/security-event/J0F_eI0ByRNByqfXkeQr/summary
- [redacted]/telemetry/processes?limit=25&offset=0&image_name__wildcard=.none/mysqld&ordering=-event_create_date

Analyse | Pièces jointes | Historique

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"

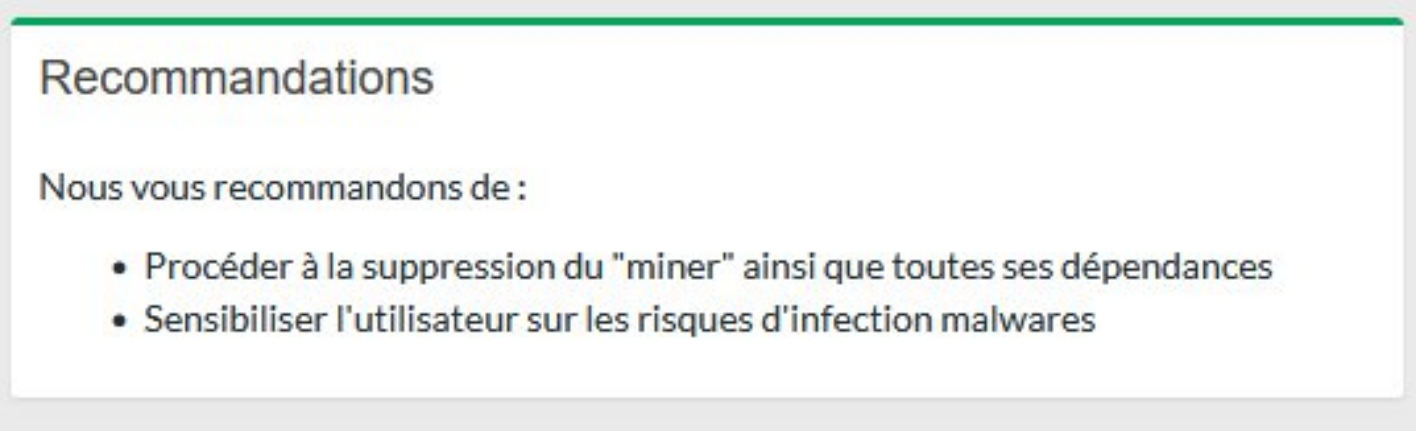


L'exécution du miner s'est faite sous le nom de ".none/mysqld ". Nous constatons d'ailleurs que ce processus (.none/mysqld) a été vu sur une autre machine : "[redacted]":

https://[redacted]/telemetry/processes?limit=25&offset=0&image_name__wildcard=.none/mysqld&ordering=-event_create_date

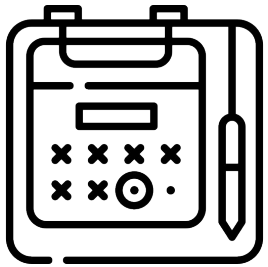
Investigation

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



Bilan

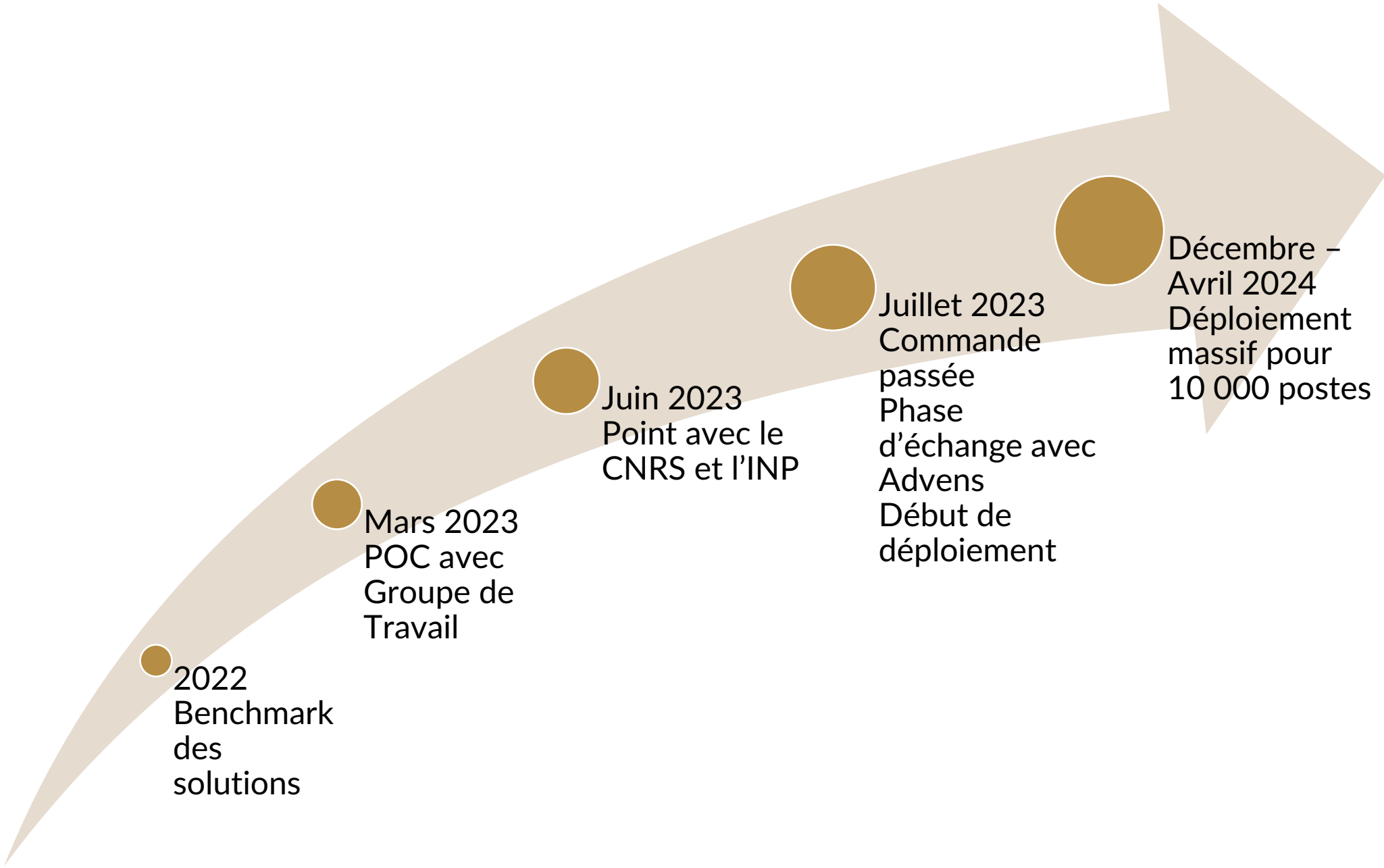
Bilan



Où en sommes nous dans ce projet ?

Retour
d ‘expérience

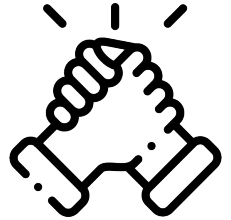
Bilan
produit


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