EDR HarfangLab

Réunion CAPITOUL

26/04/2024

Plan

- Contexte (UT2)
- EDR, fonctionnement et avantages
- Pourquoi HarfangLab (UT2)
- Fonctionnement de l'EDR HarfangLab
- Le POC (UT2)
- La PROD (UT2)
- (Tout petit) bilan à UT2
- HarfangLab à l'IMT Albi
- RETEX IMT Saint-Etienne
- (Effet) Démo

Contexte UT2

- « Sensibilisation » particulièrement efficace des équipes de direction de l'UT2 sur les risques cyber et leurs impacts en mai 2021 puis en septembre 2022
  - Campagne « perpétuelle » de phishing pédagogique (avant de cliquer) pour « travailler » sur le maillon faible des systèmes d'information
  - Mise en place d'un EDR pour faire face à l'augmentation des risques d'incidents de sécurité de nos systèmes d'information

Fonctionnement d’un EDR

- L’EDR (Endpoint Detection and Response) est une catégorie de solutions capable de détecter et contrer des activités suspectes sur les terminaux (utilisateurs et serveurs):
  - Collecte des données télémétriques issues des terminaux (agent sur le poste)
  - Envoi des données collectées à la plateforme EDR centrale (généralement, cloud)
  - Analyse des données pour détecter et apporter une réponse rapide aux activités suspectes (IA)
  - Rétention des données en vue de leur réutilisation (Tableaux de bord…)

Avantage d’un EDR

- Visibilité approfondie et élargie: vision d’un terminal et de l’ensemble des terminaux permettant la détection de répétition de schémas sur les terminaux (attaque massive)
- Détection des menaces avancées: « zero-day », menaces internes (latéralisation), hacking sophistiqué (sur mesure)
- Simplification de la réponse aux incidents: les EDR sont conçus pour ça: centralisation et corrélation des évènements permettant de détecter les schémas d’attaque
- Automatisation et intégration: API, actions via les agents…

Pourquoi HarfangLab à l'UT2

- Produit français https://www.harfanglab.io/
- Pas de blocage RGPD (IA et données chez OVH)
- Agent EDR **Hurukai** (version 2.0.1 de 2021) certifié CSPN par l'ANSSI
- Disponible au travers des marchés auxquels adhère l'université (CAIH)
- Manque de main d'œuvre / compétences pour gérer les problèmes, besoin d'automatiser la détection mais aussi les réponses: Délégation de la partie exploitation à un prestataire Advens https://www.advens.fr

Fonctionnement de HarfangLag

- Déploiement d'un agent sur les terminaux chargé de :
  - collecter et renvoyer les éléments de télémétrie vers la console centralisée EDR
  - Appliquer les actions de remédiation (peut donc aussi servir de vecteur d'attaque)
- Analyse des éléments de télémétrie:
  - Moteur basé sur des indicateurs de compromission (IOC)
  - Moteur de détection basé sur des « signatures »
    - Règles Yara
    - Règles Sigma
    - Liste de drivers vulnérables
  - Moteur IA (En fait, des modèles mathématiques)
    - Modèle Hibou (calcul de probabilité qu'un fichier soit malveillant)
    - Modèle Chocard (détection de script PowerShell malveillants)
    - Modèle Condor (détection d'exécutables malveillants)
  - Moteur comportemental
  - Moteur ramsonguard

Instance d ’évaluation à l’UT2

- Instanciation d’une instance de test avec HarfangLab pour environ 150 machines:
- 80 serveurs (dont les AD et serveurs de fichiers Windows)
- Les postes des agents la DSI
- Les postes de personnels hors DSI disposants d’accès avancés au SI

Déploiement de l’Agent

- Déploiement des postes et serveurs Windows via GPO si machines dans un des domaines de l’UT2
- Déploiement manuel des serveurs Windows hors domaines
- Déploiement des serveurs Linux via Ansible
- Déploiement des postes utilisateurs Linux / Mac manuellement

Déploiement par Ansible

Création d'un module spécifique dans notre script de mise en conformité, utilisé pour tout nouveau serveur

On utilise un tag spécifique de façon à pouvoir lancer uniquement le déploiement de l'agent

2 étapes:

- Transfert du binaire (pour débian ou redhat)
- Installation de l'agent en spécifiant les variables d'environnement nécessaires (via apt ou yum en fonction du système)

```
- name: EDR - upload binary - debian
  copy:
    dest: /tmp/agent.deb
    src: agent-2.29.7_x64.deb
  when: ansible_facts['os_family'] == "Debian"
  tags: EDR

- name: EDR - upload binary - redhat
  copy:
    dest: /tmp/agent.rpm
    src: agent-2.29.7_x64.rpm
  when: ansible_facts['os_family'] == "RedHat"
  tags: EDR

- name: EDR - Install agent - debian
  apt:
    deb: /tmp/agent.deb
  environment:
    HURUKAI_HOST: 283a6b91402314ca.hurukai.io
    HURUKAI_PORT: 443
    HURUKAI_PROTOCOL: https
    HURUKAI_KEY: <clé de licence>
    DEBIAN_FRONTEND: noninteractive
  when: ansible_facts['os_family'] == "Debian"
  tags: EDR

- name: EDR - Install agent - RedHat
  yum:
    name: /tmp/agent.rpm
    state: present
    disable_gpg_check: true
  environment:
    HURUKAI_HOST: 283a6b91402314ca.hurukai.io
    HURUKAI_PORT: 443
    HURUKAI_PROTOCOL: https
    HURUKAI_KEY: <clé de licence>
  when: ansible_facts['os_family'] == "RedHat"
  tags: EDR
```

Bilan du POC

- HarfangLab réactif pour la mise en place et l'accompagnement sur le POC
- Déploiement des agents facile sur les OS Windows et Linux maintenus
- Peu de ressources nécessaires pour l'agent (entre 130 et 180MO, 0.5% CPU)
- Console web relativement intuitive (voir démo) et facile d'usage, quelques opérations pénibles (mise des machines dans les groupes) -> voir si possible d'automatiser via API ou option de ligne de commande à l'installation
- Beaucoup de faux positifs ! Chronophage pour le passage en liste blanche

=> Décision de passer en production et de contractualiser avec Advens pour déléguer l'exploitation

La mise place de la délégation

- Réunion de cadrage avec Advens et mise en place des services managés mySOC:
  - Un fichier Excel à compléter avec les modes de communication et les interlocuteurs
  - Une lettre de délégation définissant le périmètre de délégation des actions qu' Advens peut effectuer à notre place
- Passage par le gestionnaire de ticket d'Advens pour les demandes d'intervention et le suivi des actions

Le passage en production

- Cible 2024: environ 1000 postes
  - Intégralité des serveurs sur lesquels l'agent est déployable
  - Les postes des personnels ayant un accès au SI
- Cible 2025: environ 2000 postes
  - Passage à l'ntégralité des postes des personnels
- Déploiement d'un nombre d'agents suffisamment significatif (>600) avant de passer en remédiation
- Passage des machines en mode remédiation:
  - Petit à petit (groupe par groupe) => attention a s'occuper de (faire) mettre en liste les faux positif avant de passer en mode remédiation
  - Prévenir les responsables des systèmes passé en remédiation pour remonter le plus rapidement possible un blocage non désiré et non détecté en amont

Petit bilan sur le passage en production

- Plein de choses à regarder / affiner:
  - La phase « passage en liste blanche » va générer beaucoup de travail
  - Travail à venir sur les critères de déclanchement de la remédiation
- Passage pour l'instant en mode remédiation uniquement pour les postes utilisateurs, les serveurs restent en observation jusqu'à épurage des faux positif.
  - Dès le premier jours (22/04/2024), blocage de drivers présentant une vulnérabilité (Dell) sur les postes utilisateurs

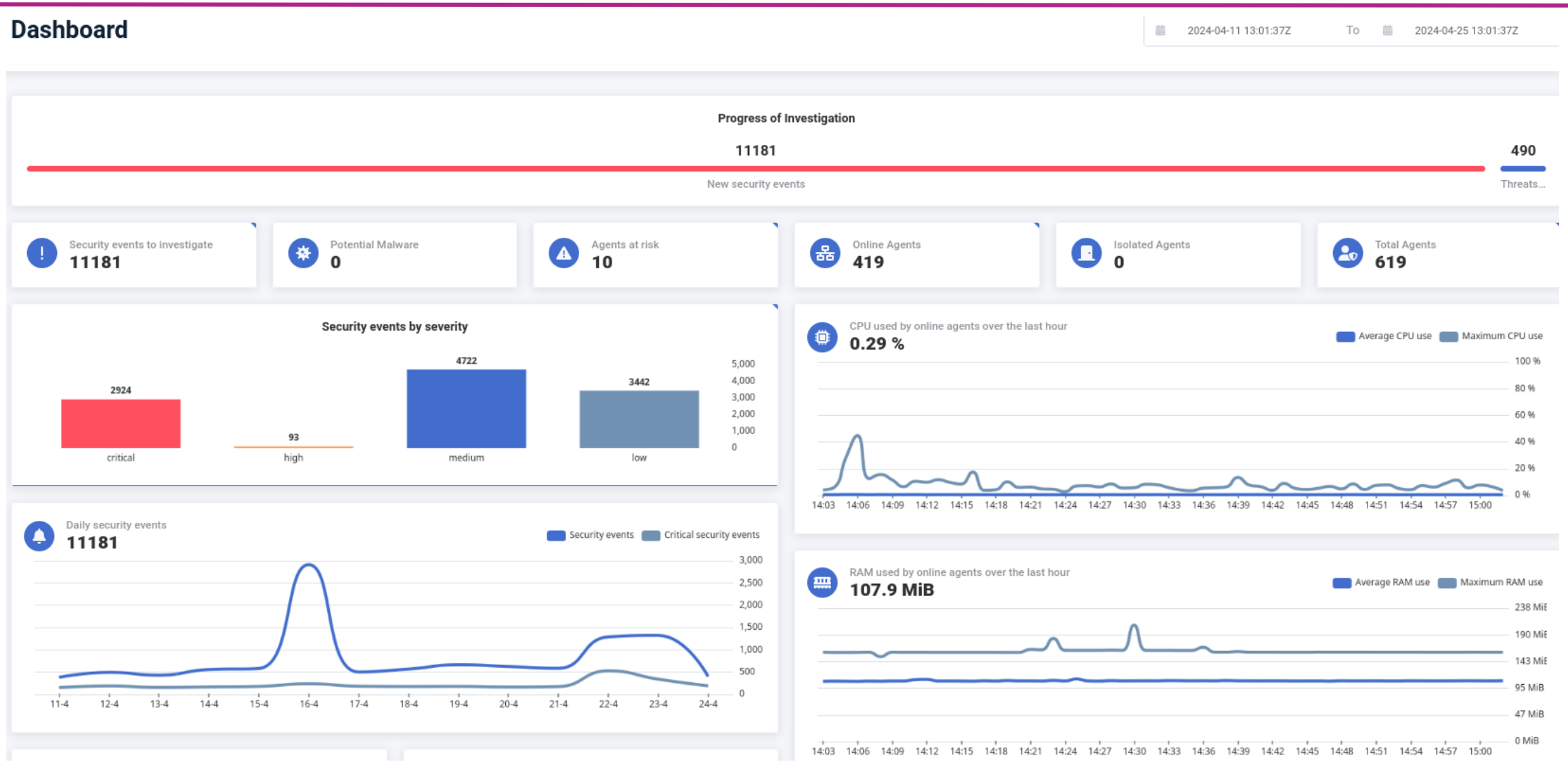
HarfangLab à l’ IMT Albi

- PoC avec Harfanglab en mars 2024 sur 10 machines "blanches"
- Achat SOC Exaprobe groupe logiciel antivirus par l'Institut Mines Telecom 1000 agents/école prévu courant mai 2024

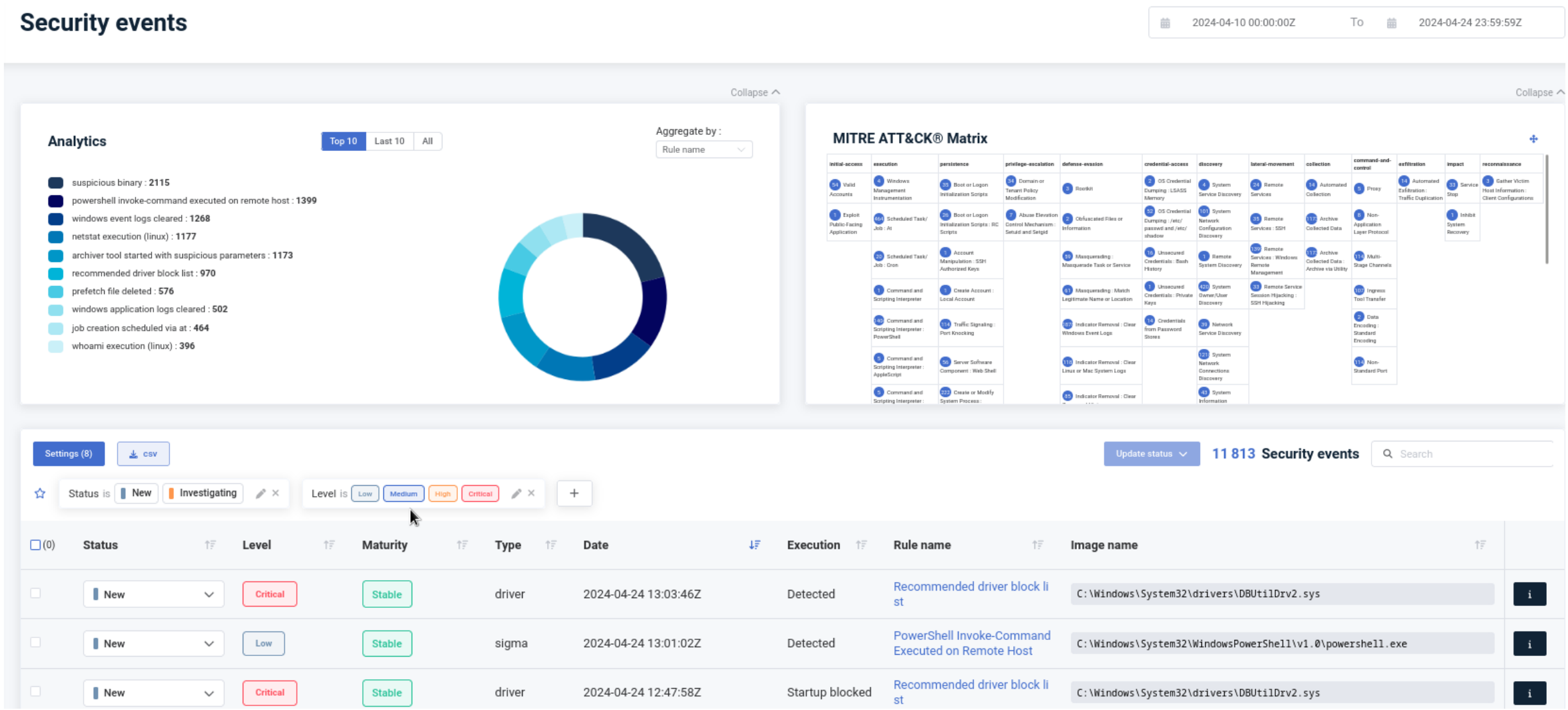
Retex IMT Mines Saint-Etiennes

- Achat SOC Exaprobe groupe logiciel antivirus en décembre 2023
- Déploiement fait sur 600 poste de travail et serveurs (hyperviseur proxmox + VM), reste a faire salles TP, prévu d'ici septembre
- 3 mois d'apprentissage
- approximativement 200 règles white list
- règles sigma alertes seulement, niveau critical et high (le reste est du bruit) règles yara et IA en remédiation
- Note : avant les mises a jour de serveur la procédure est de stopper le service hurukai-agent pour éviter de bloquer les scripts apt/deb puis de relacer après la mise a jour.

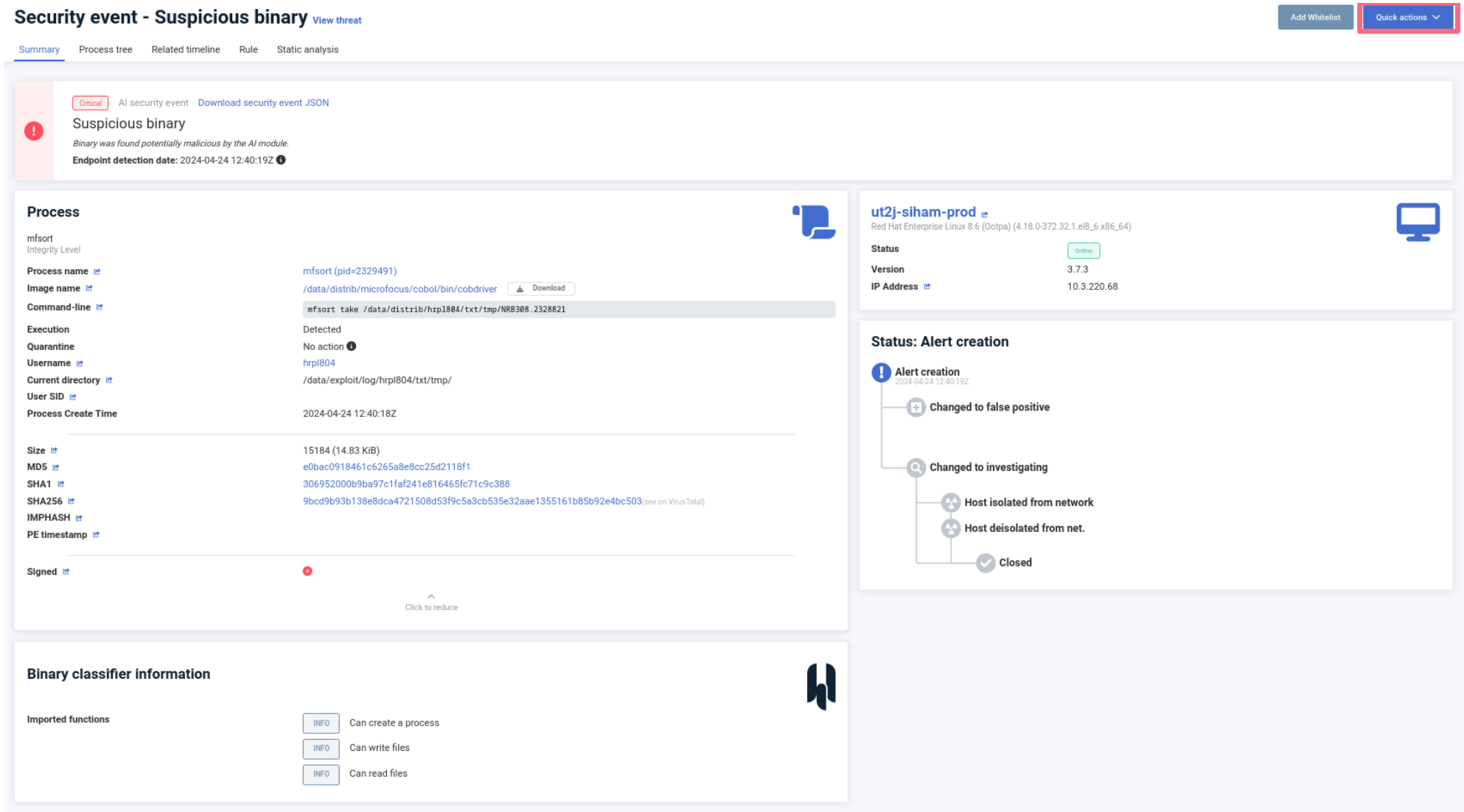
Démo - Dashboard



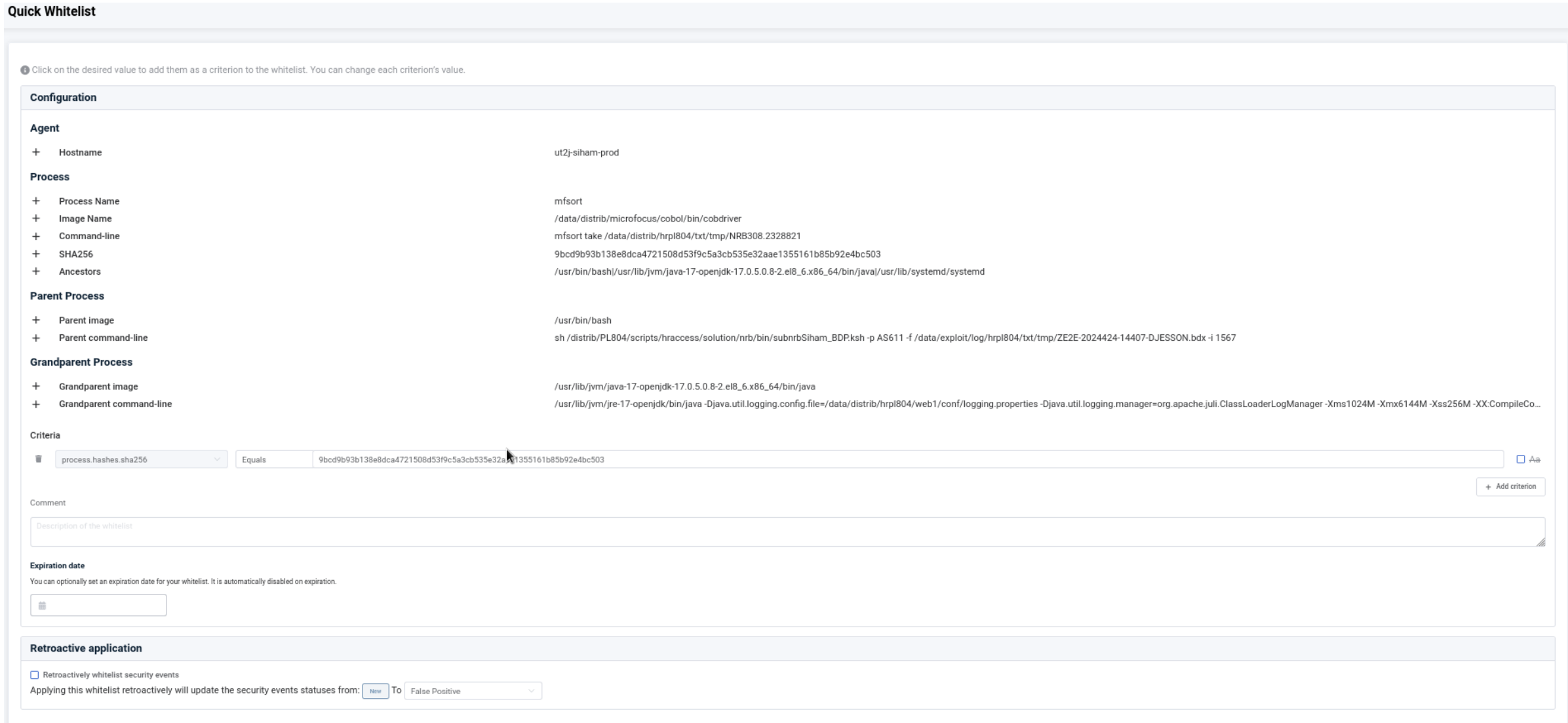
Démo – Evènements de sécurité



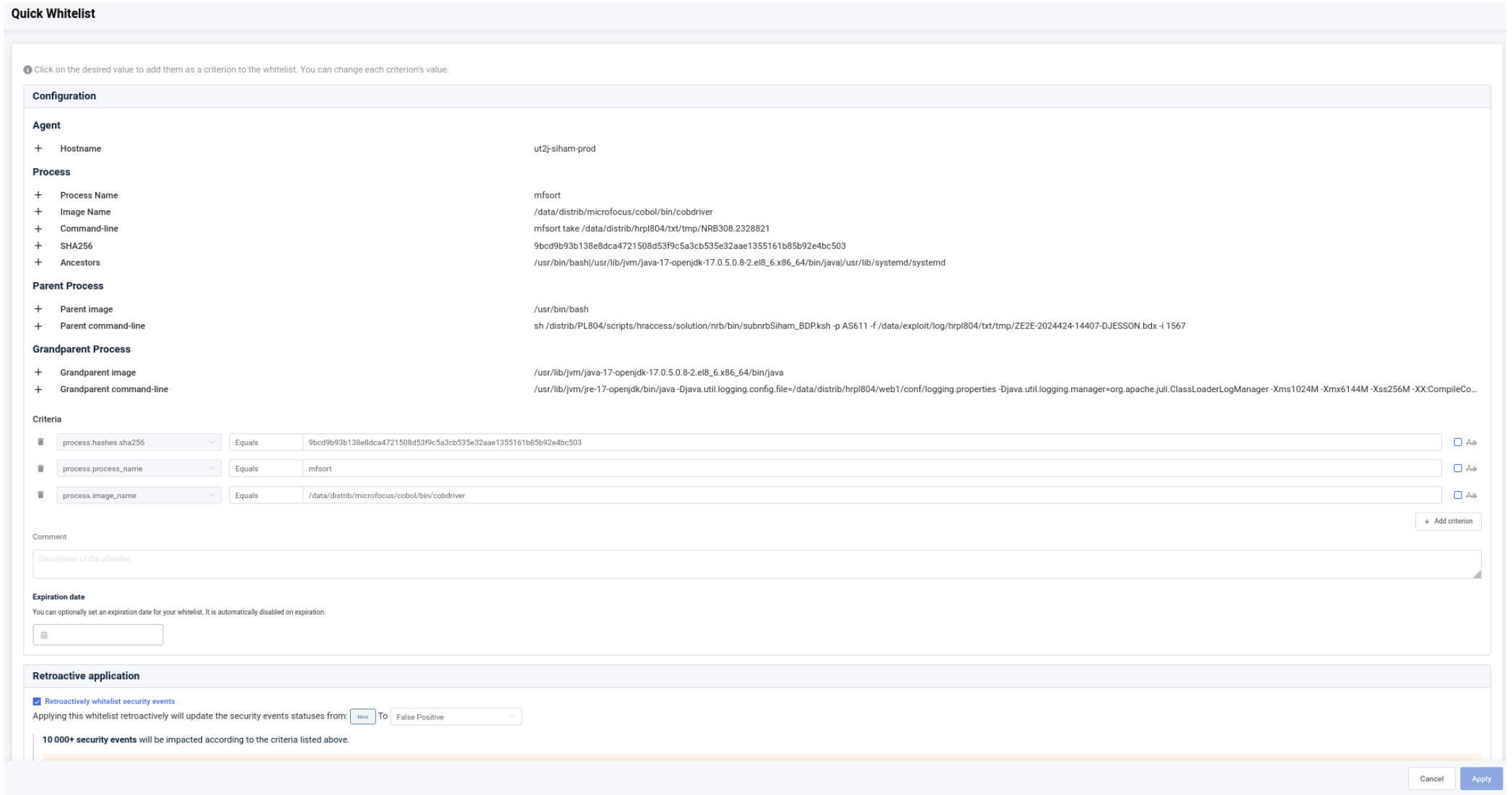
Démo – Un faux positif



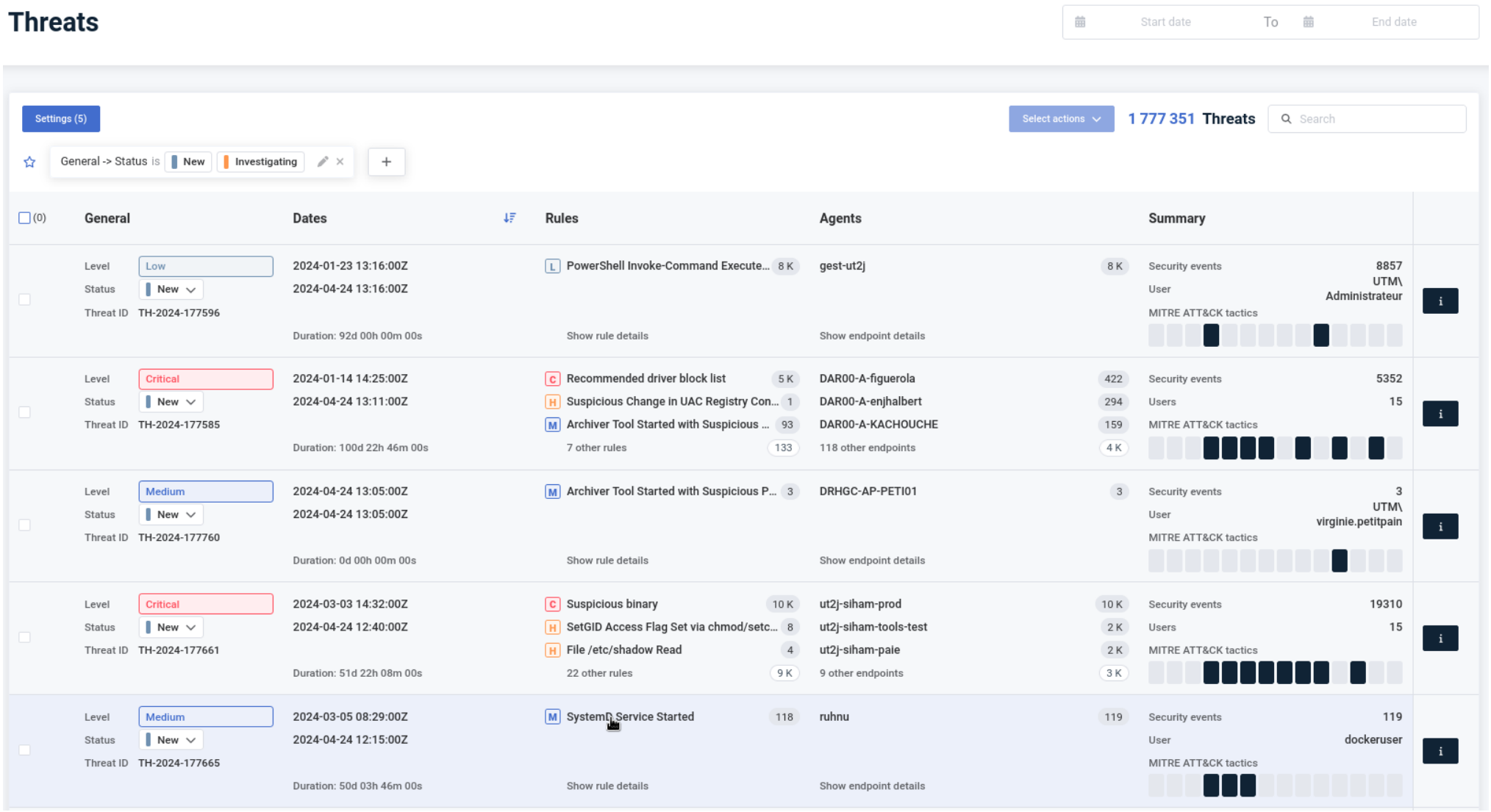
Démo – Mettre en liste blanche



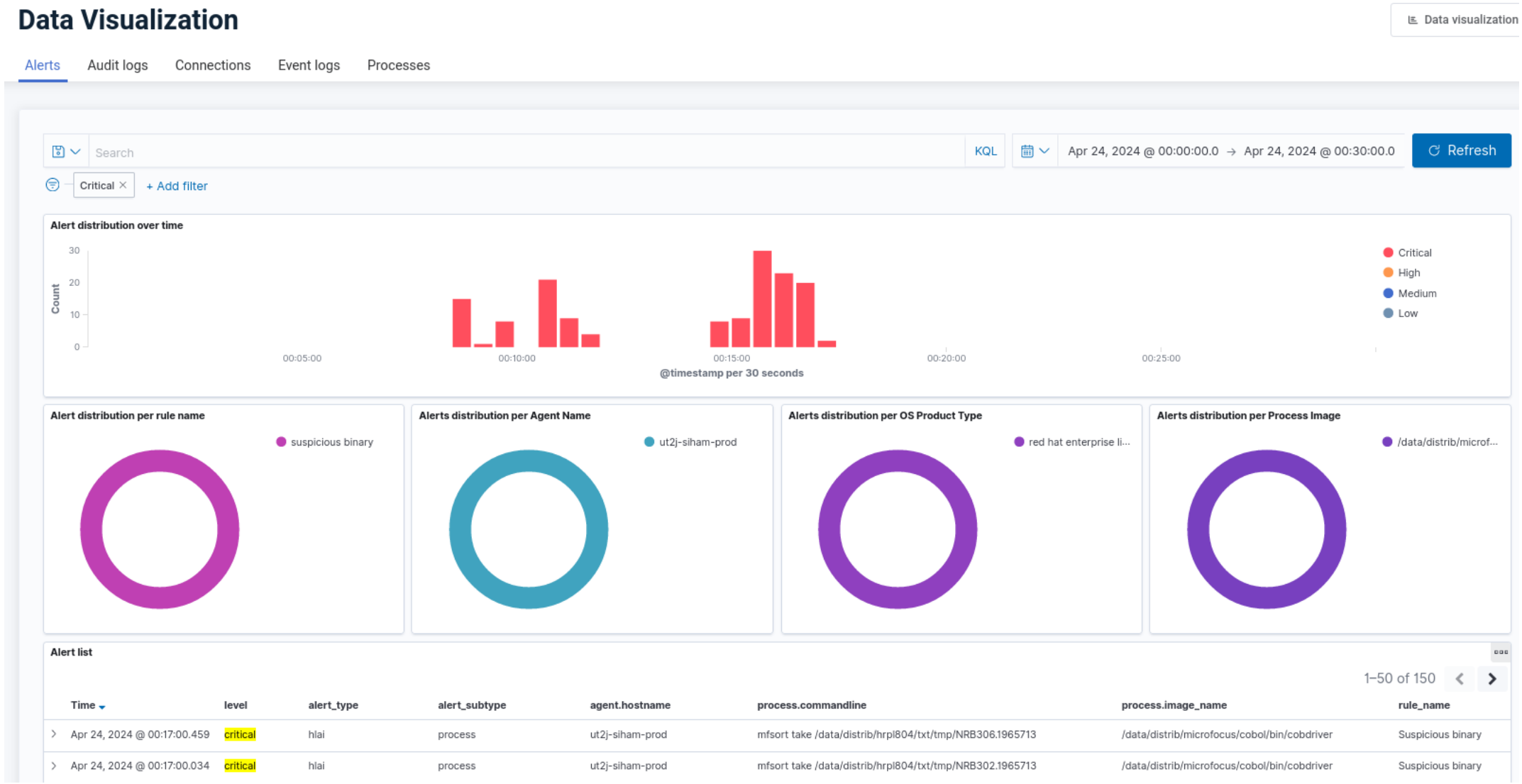
Démo – Mettre en liste blanche: les critères



Démo – Menaces détectées

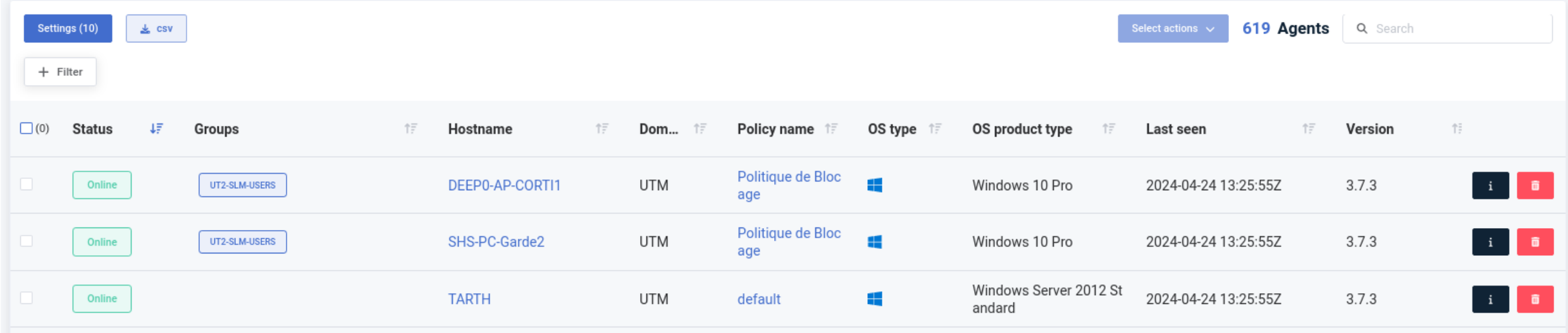


Démo – Visualisation des données (elastic)

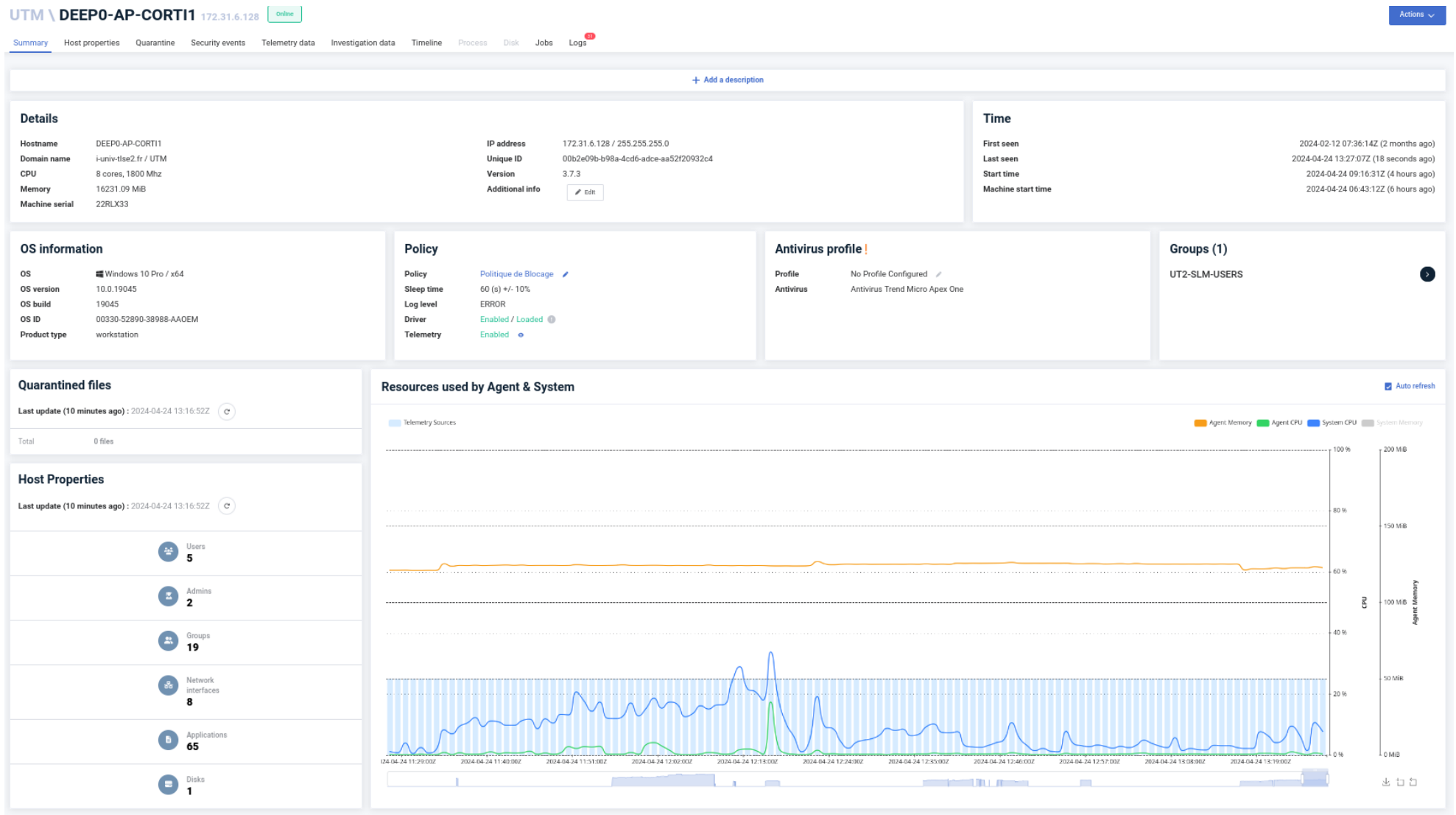


Démo - Agents

Agents

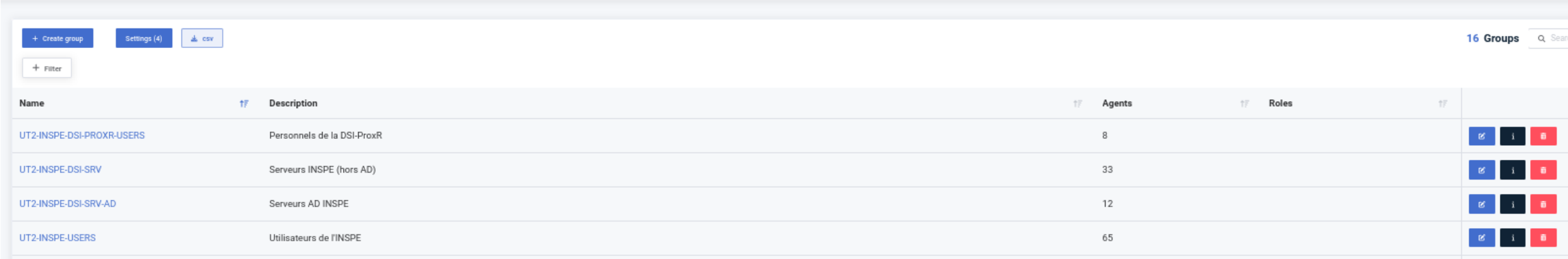


Démo - Agent

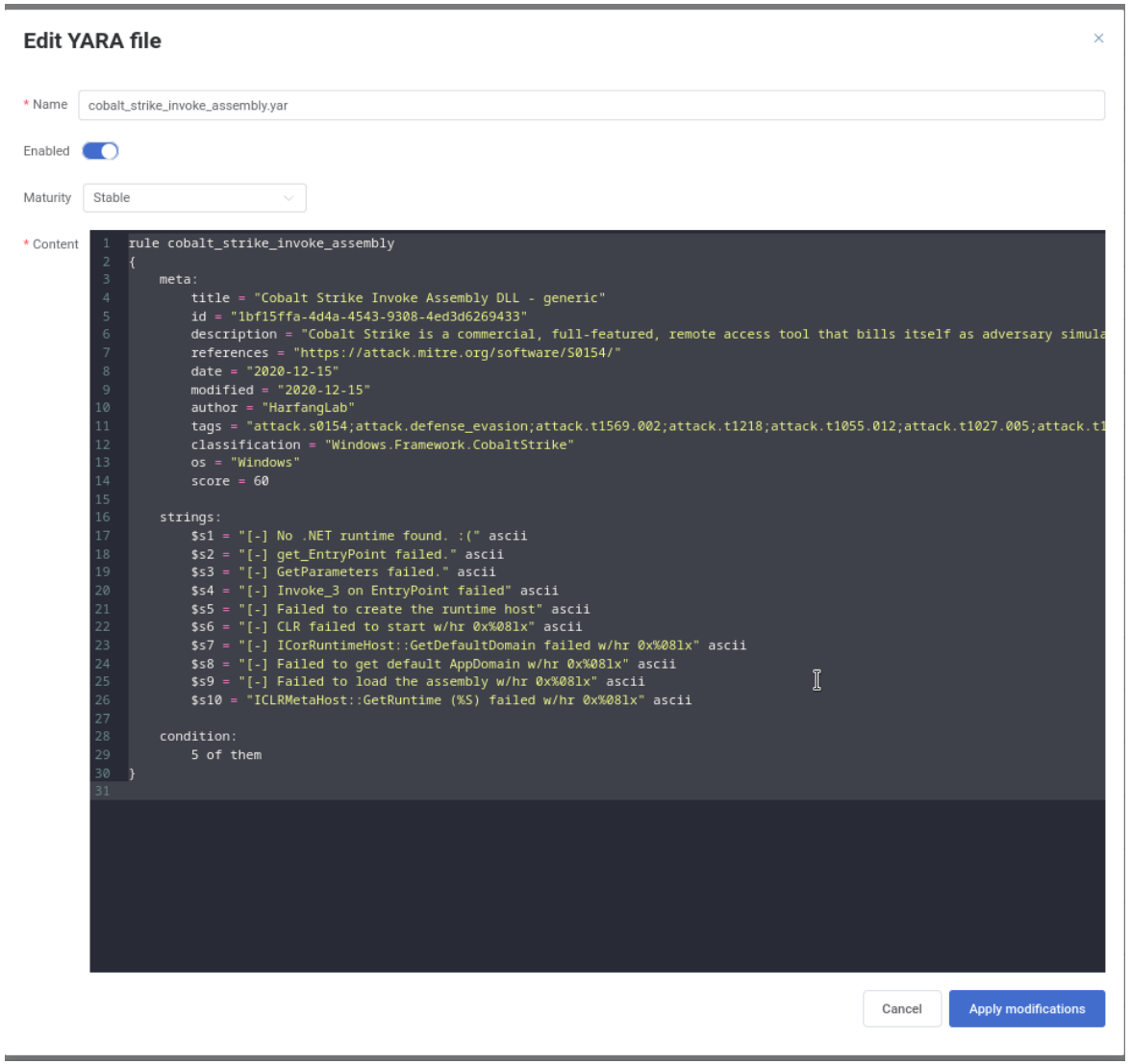

UTM \ DEEP0-AP-CORTI1 172.31.6.128
Online
Actions
Summary
Host properties
Quarantine
Security events
Telemetry data
Investigation data
Timeline
Process
Disk
Jobs
Logs
Add a description
Details
Hostname DEEP0-AP-CORTI1
Domain name i-univ-tlse2.fr / UTM
CPU 8 cores, 1800 Mhz
Memory 16231.09 MiB
Machine serial 22RLX33
IP address 172.31.6.128 / 255.255.255.0
Unique ID 00b2e09b-b98a-4cd6-adce-aa52f20932c4
Version 3.7.3
Additional info
Edit
Time
First seen 2024-02-12 07:36:14Z (2 months ago)
Last seen 2024-04-24 13:27:07Z (18 seconds ago)
Start time 2024-04-24 09:16:31Z (4 hours ago)
Machine start time 2024-04-24 06:43:12Z (6 hours ago)
OS information
OS Windows 10 Pro / x64
OS version 10.0.19045
OS build 19045
OS ID 00330-52890-38988-AAOEM
Product type workstation
Policy
Policy Politique de Blocage
Sleep time 60 (s) +/- 10%
Log level ERROR
Driver Enabled / Loaded
Telemetry Enabled
Antivirus profile
Profile No Profile Configured
Antivirus Antivirus Trend Micro Apex One
Groups (1)
UT2-SLM-USERS
Quarantined files
Last update (10 minutes ago) : 2024-04-24 13:16:52Z
Total 0 files
Host Properties
Last update (10 minutes ago) : 2024-04-24 13:16:52Z
Users 5
Admins 2
Groups 19
Network interfaces 8
Applications 65
Disks 1
Resources used by Agent & System
Auto refresh
Telemetry Sources
Agent Memory
Agent CPU
System CPU
System Memory
100 %
80 %
60 %
40 %
20 %
0 %
200 MiB
150 MiB
100 MiB
50 MiB
0 MiB
CPU
Agent Memory

Démo - Groupes

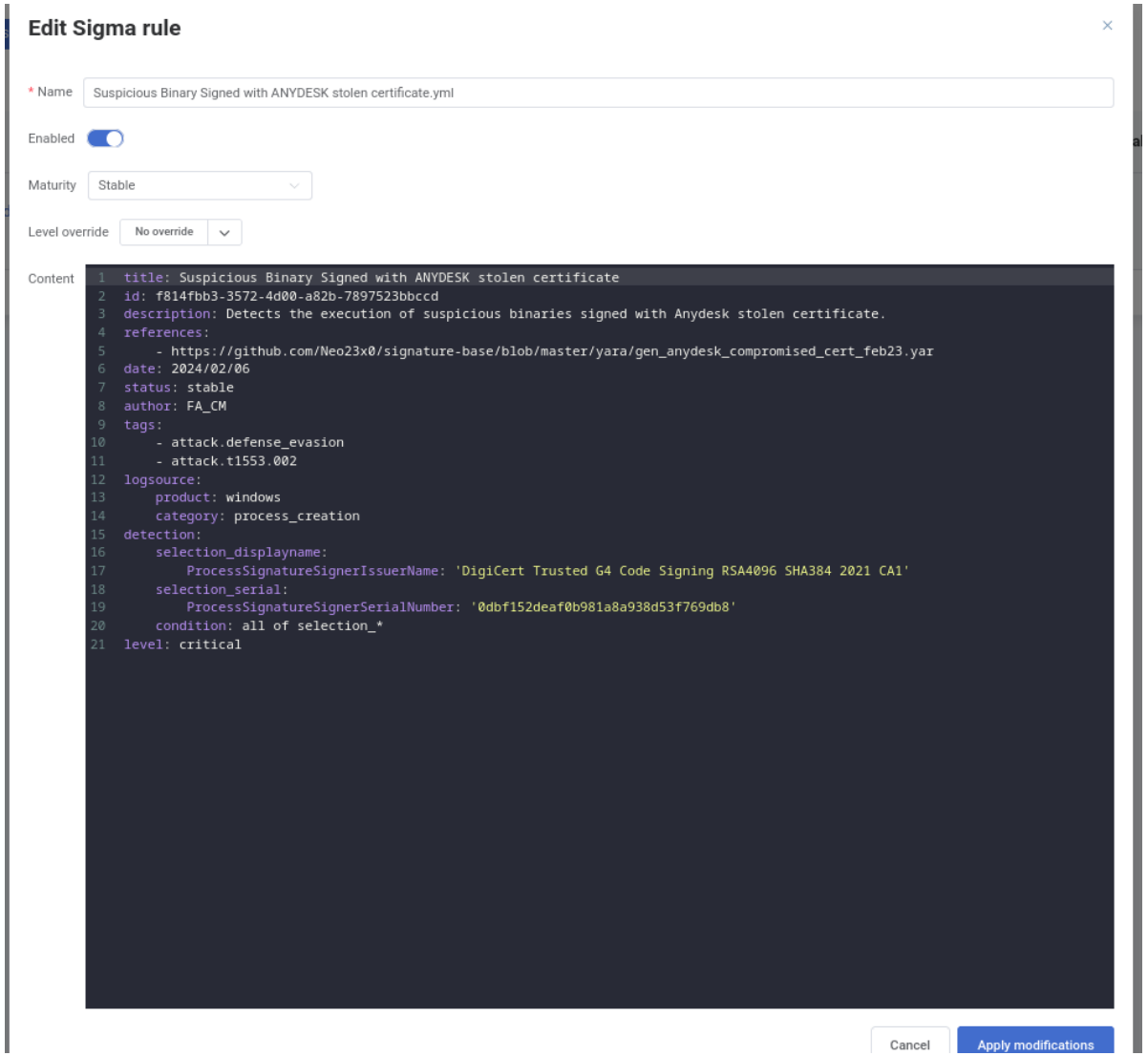
Groups



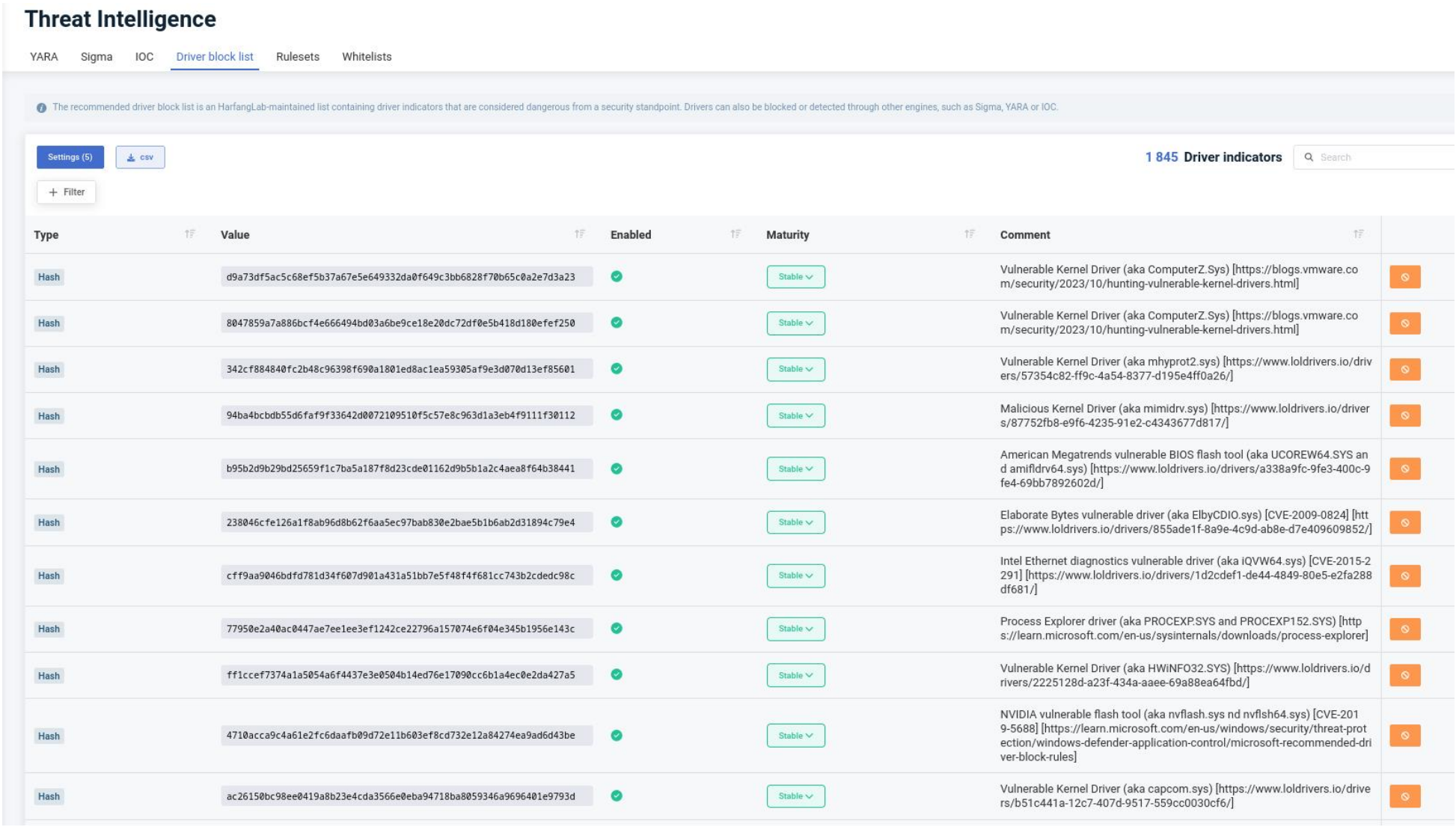
Démo – Règles Yara



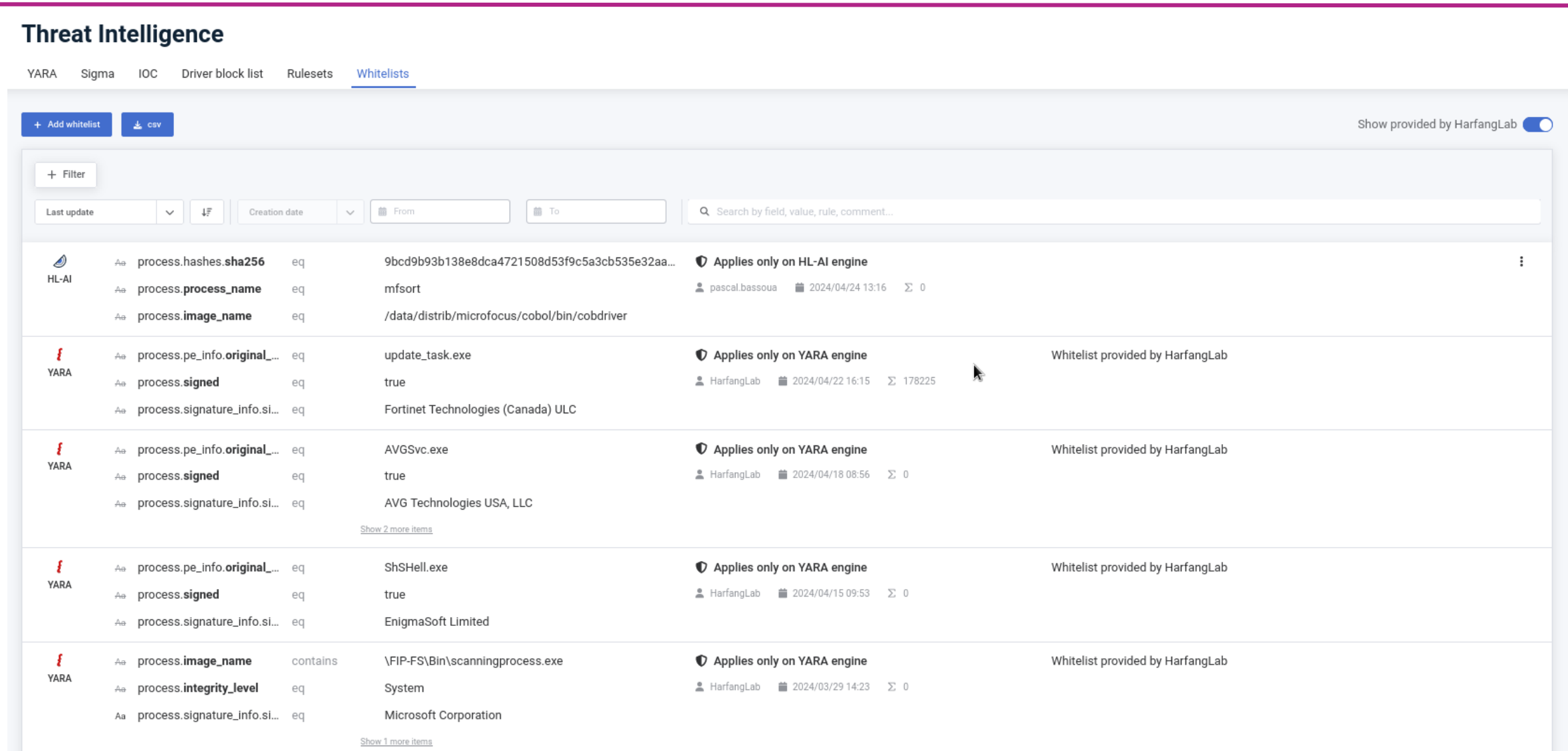
Démo – Règles Sigma



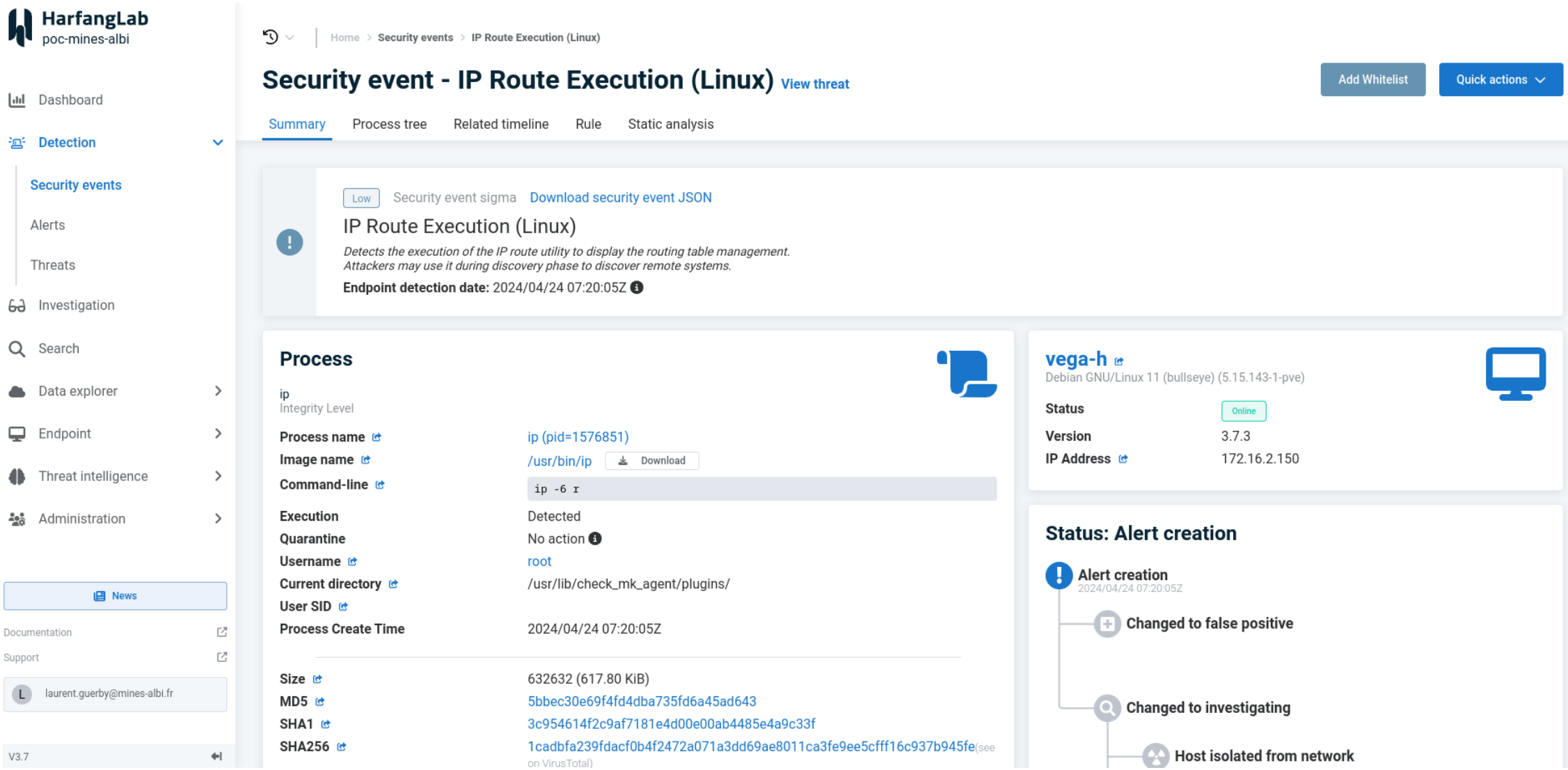
Démo – Liste de drivers à bloquer



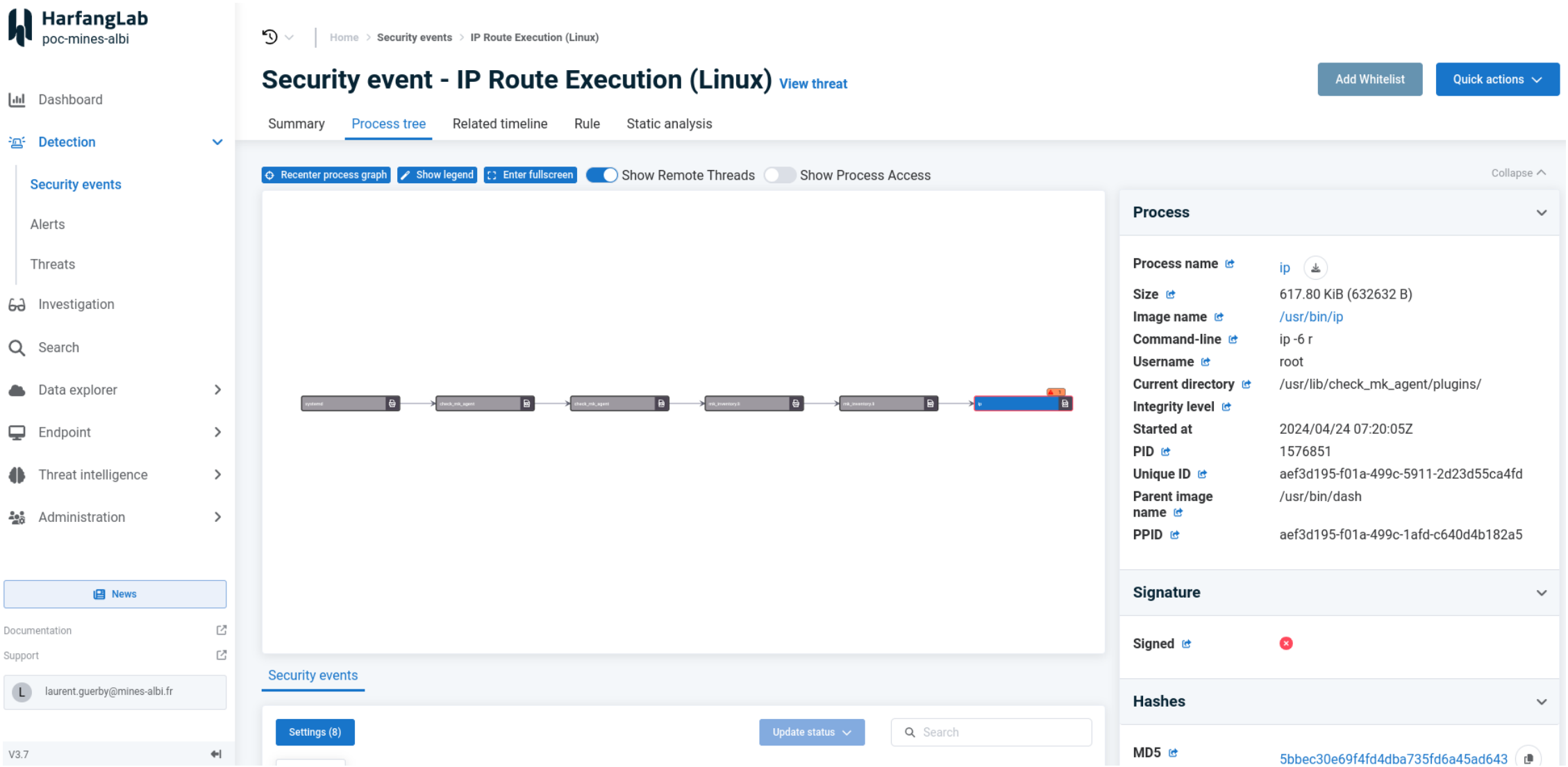
Démo – Listes blanches



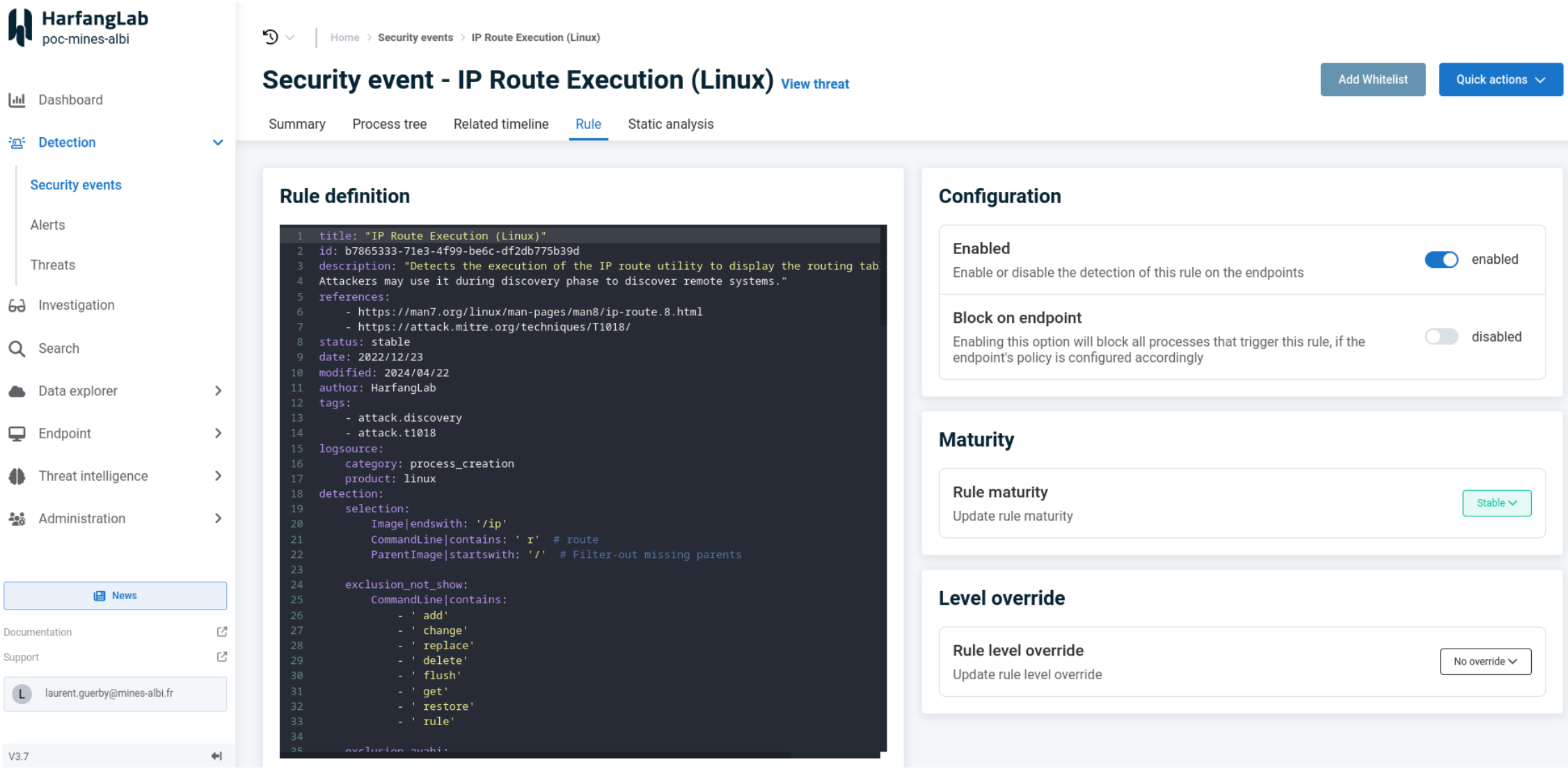
IMT Albi – Mise en liste blanche



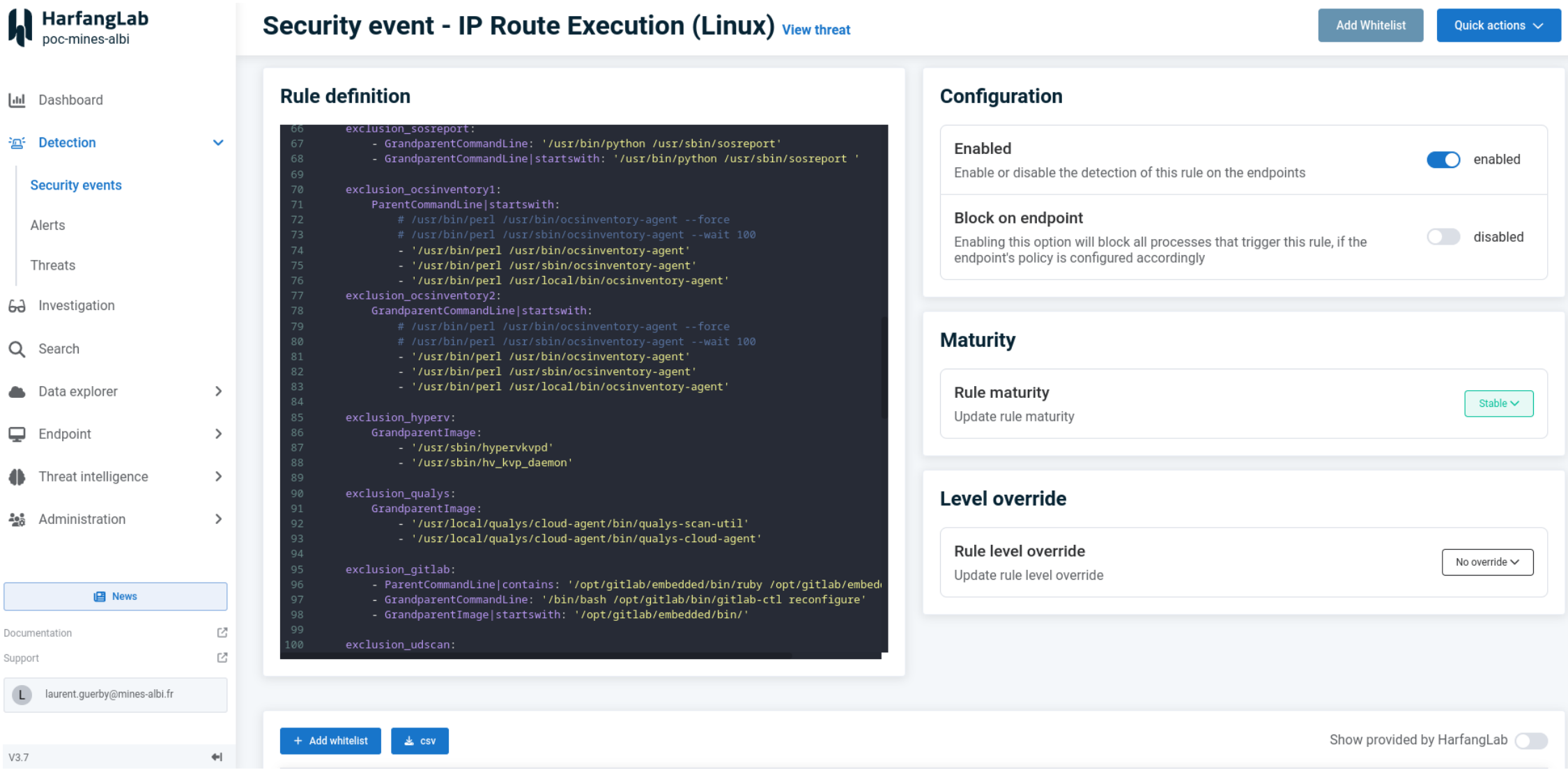
IMT Albi – Mise en liste blanche



IMT Albi – Mise en liste blanche



IMT Albi – Mise en liste blanche



IMT Albi – Mise en liste blanche