

# EDR HarfangLab

---

Réunion CAPITOUL

26/04/2024



- 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

- « 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

- 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...)

- 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 événements permettant de détecter les schémas d'attaque
- Automatisation et intégration: API, actions via les agents...

- 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>

- 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

- 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 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

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
```

- 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

- 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

- 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'intégralité 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 à s'occuper de (faire) mettre en liste les faux positifs avant de passer en mode remédiation
  - Prévenir les responsables des systèmes passés en remédiation pour remonter le plus rapidement possible un blocage non désiré et non détecté en amont

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

- 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

- 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 relancer après la mise a jour.



## Dashboard

2024-04-11 13:01:37Z To 2024-04-25 13:01:37Z

### Progress of Investigation

11181

490

New security events

Threats...

Security events to investigate  
**11181**

Potential Malware  
**0**

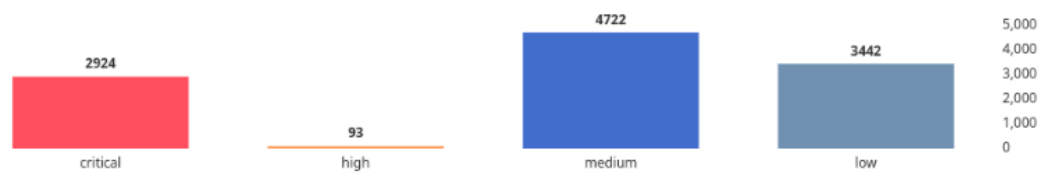
Agents at risk  
**10**

Online Agents  
**419**

Isolated Agents  
**0**

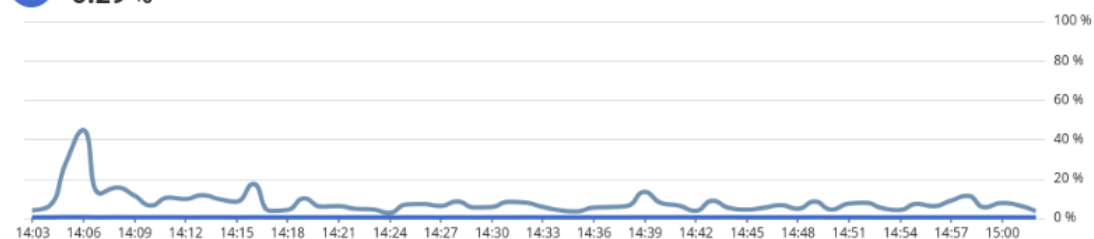
Total Agents  
**619**

### Security events by severity

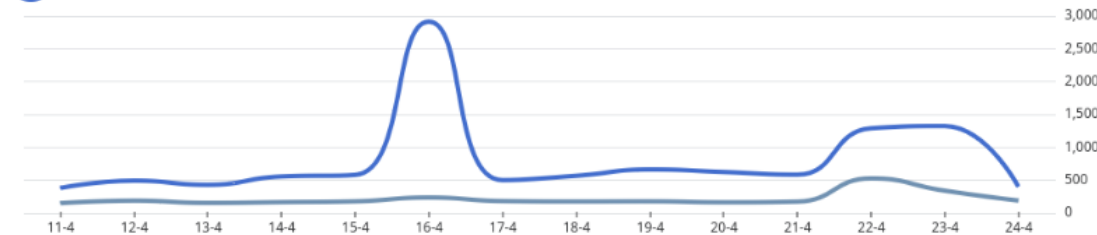


### CPU used by online agents over the last hour

**0.29 %**

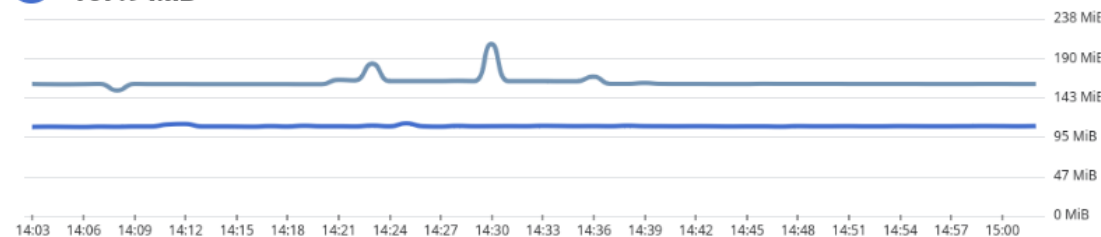


Daily security events  
**11181**



### RAM used by online agents over the last hour

**107.9 MiB**



## Security events

2024-04-10 00:00:00Z To 2024-04-24 23:59:59Z

### Analytics

Aggregate by: Rule name

- suspicious binary : 2115
- powershell invoke-command executed on remote host : 1399
- windows event logs cleared : 1268
- netstat execution (linux) : 1177
- archiver tool started with suspicious parameters : 1173
- recommended driver block list : 970
- prefetch file deleted : 576
- windows application logs cleared : 502
- job creation scheduled via at : 464
- whoami execution (linux) : 396

### MITRE ATT&CK® Matrix

initial-access	execution	persistence	privilege-escalation	defense-evasion	credential-access	discovery	lateral-movement	collection	command-and-control	exfiltration	impact	reconnaissance
Valid Accounts	Windows Management Instrumentation	Boot or Logon Initialization Scripts	Domain or Tenant Policy Modification	Rootkit	OS Credential Dumping: LSASS Memory	System Service Discovery	Remote Services	Automated Collection	Proxy	Automated Exfiltration: Traffic Duplication	Service Drop	Gather Victim Host Information: Clear Configurations
Exploit Public Facing Application	Scheduled Task/Job: At	Boot or Logon Initialization Scripts: RC Scripts	Abuse Elevation Control Mechanism: Setuid and Setgid	Obfuscated Files or Information	OS Credential Dumping: /etc/passwd and /etc/shadow	System Network Configuration Discovery	Remote Services: SSH	Archive Collected Data	Non-Application Layer Protocol		Inhibit System Recovery	
	Scheduled Task/Job: Cron	Account Manipulation: SSH Authorized Keys		Masquerading: Masquerade Task or Service	Unsecured Credentials: Bash History	Remote System Discovery	Remote Services: Windows Remote Management	Archive Collected Data: Archive via Utility	Multi-Stage Channels			
	Command and Scripting Interpreter: PowerShell	Create Account: Local Account		Masquerading: Match Legitimate Name or Location	Unsecured Credentials: Private Keys	System Owner/User Discovery	Remote Service Session Hijacking: SSH Hijacking		Ingress Tool Transfer			
	Command and Scripting Interpreter: AppleScript	Traffic Signaling: Port Knocking		Indicator Removal: Clear Windows Event Logs	Unsecured Credentials: Password Stores	Network Service Discovery			Data Exfiltration: Standard Encoding			
	Command and Scripting Interpreter: AppleScript	Server Software Component: Web Shell		Indicator Removal: Clear Linux or Mac System Logs		System Network Connections Discovery			Non-Standard Port			
	Command and Scripting Interpreter: PowerShell	Create or Modify System Process		Indicator Removal: Clear ...		System Information						

Settings (8) [CSV](#) Update status  11 813 Security events

Status is New Investigating Level is Low Medium High Critical

<input type="checkbox"/> (0)	Status	Level	Maturity	Type	Date	Execution	Rule name	Image name
<input type="checkbox"/>	New	Critical	Stable	driver	2024-04-24 13:03:46Z	Detected	Recommended driver block list	C:\Windows\System32\drivers\DBUtilDrv2.sys
<input type="checkbox"/>	New	Low	Stable	sigma	2024-04-24 13:01:02Z	Detected	PowerShell Invoke-Command Executed on Remote Host	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
<input type="checkbox"/>	New	Critical	Stable	driver	2024-04-24 12:47:58Z	Startup blocked	Recommended driver block list	C:\Windows\System32\drivers\DBUtilDrv2.sys

## Security event - Suspicious binary [View threat](#)

[Add Whitelist](#)
[Quick actions](#)
[Summary](#) [Process tree](#) [Related timeline](#) [Rule](#) [Static analysis](#)

**Critical** AI security event [Download security event JSON](#)

### Suspicious binary

*Binary was found potentially malicious by the AI module.*

Endpoint detection date: 2024-04-24 12:40:19Z

### Process

mfsort  
Integrity Level

**Process name** [mfsort \(pid=2329491\)](#)

**Image name** [/data/distrib/microfocus/cobol/bin/cobdriver](#) [Download](#)

**Command-line** [mfsort take /data/distrib/hzp1804/txt/tmp/NR8388.2328821](#)

**Execution** Detected

**Quarantine** No action

**Username** [hrpl804](#)

**Current directory** [/data/exploit/log/hrpl804/txt/tmp/](#)

**User SID**

**Process Create Time** 2024-04-24 12:40:18Z

---

**Size** [15184 \(14.83 KiB\)](#)

**MD5** [e0bac0918461c6265a8e8cc25d2118f1](#)

**SHA1** [306952000b9ba97c1faf241e816465fc71c9c388](#)

**SHA256** [9bcc9b93b138e8dca4721508d53f9c5a3cb535e32aae1355161b85b92e4bc503](#) (see on VirusTotal)

**IMPHASH**

**PE timestamp**

---

**Signed** [Signed](#) ●

[Click to reduce](#)



### ut2j-siham-prod

Red Hat Enterprise Linux 8.6 (Ootpa) (4.18.0-372.32.1.el8\_6.x86\_64)

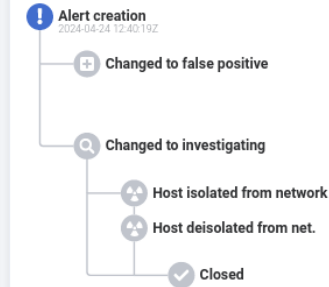
**Status** Online

**Version** 3.7.3

**IP Address** [10.3.220.68](#)



### Status: Alert creation



### Binary classifier information

**Imported functions**

- [INFO](#) Can create a process
- [INFO](#) Can write files
- [INFO](#) Can read files



## Quick Whitelist

Click on the desired value to add them as a criterion to the whitelist. You can change each criterion's value.

### Configuration

#### Agent

+ Hostname `ut2j-siham-prod`

#### Process

+ Process Name `mfsort`  
 + Image Name `/data/distrib/microfocus/cobol/bin/cobdriver`  
 + Command-line `mfsort take /data/distrib/hrpl804/txt/tmp/NRB308.2328821`  
 + SHA256 `9bcd9b93b138e8dca4721508d53f9c5a3cb535e32aae1355161b85b92e4bc503`  
 + Ancestors `/usr/bin/bash|usr/lib/jvm/java-17-openjdk-17.0.5.0.8-2.el8_6.x86_64/bin/java|usr/lib/systemd/systemd`

#### Parent Process

+ Parent image `/usr/bin/bash`  
 + Parent command-line `sh /distrib/PL804/scripts/hraccess/solution/nrb/bin/subnrbSiham_BDP.ksh -p AS611 -f /data/exploit/log/hrpl804/txt/tmp/ZE2E-2024424-14407-DJESSON.bdx -i 1567`

#### Grandparent Process

+ Grandparent image `/usr/lib/jvm/java-17-openjdk-17.0.5.0.8-2.el8_6.x86_64/bin/java`  
 + Grandparent command-line `/usr/lib/jvm/jre-17-openjdk/bin/java -Djava.util.logging.config.file=/data/distrib/hrpl804/web1/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Xms1024M -Xmx6144M -Xss256M -XX:CompileCo...`

#### Criteria

`process.hashes.sha256` Equals `9bcd9b93b138e8dca4721508d53f9c5a3cb535e32aae1355161b85b92e4bc503`

+ Add criterion

#### Comment

Description of the whitelist

#### Expiration date

You can optionally set an expiration date for your whitelist. It is automatically disabled on expiration.

#### Retroactive application

Retroactively whitelist security events

Applying this whitelist retroactively will update the security events statuses from:  To

### Quick Whitelist

Click on the desired value to add them as a criterion to the whitelist. You can change each criterion's value.

#### Configuration

**Agent**

- + Hostname: ut2j-siham-prod

**Process**

- + Process Name: mfsort
- + Image Name: /data/distrib/microfocus/cobol/bin/cobdriver
- + Command-line: mfsort take /data/distrib/hrpl804/txt/tmp/NRB308.2328821
- + SHA256: 9bcd9b93b138e8dca4721508d53f9c5a3cb535e32aae1355161b85b92e4bc503
- + Ancestors: /usr/bin/bash|usr/lib/jvm/java-17-openjdk-17.0.5.0.8-2.el8\_6.x86\_64/bin/java|usr/lib/systemd/systemd

**Parent Process**

- + Parent image: /usr/bin/bash
- + Parent command-line: sh /distrib/PL804/scripts/hraccess/solution/nrb/bin/subnrbSiham\_BDP.ksh -p AS611 -f /data/exploit/log/hrpl804/txt/tmp/ZE2E-2024424-14407-DJESSON.bdx -i 1567

**Grandparent Process**

- + Grandparent image: /usr/lib/jvm/java-17-openjdk-17.0.5.0.8-2.el8\_6.x86\_64/bin/java
- + Grandparent command-line: /usr/lib/jvm/jre-17-openjdk/bin/java -Djava.util.logging.config.file=/data/distrib/hrpl804/web1/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Xms1024M -Xmx6144M -Xss256M -XX:CompileCo...

#### Criteria

process.hashes.sha256	Equals	9bcd9b93b138e8dca4721508d53f9c5a3cb535e32aae1355161b85b92e4bc503	<input type="checkbox"/> Aa
process.process_name	Equals	mfsort	<input type="checkbox"/> Aa
process.image_name	Equals	/data/distrib/microfocus/cobol/bin/cobdriver	<input type="checkbox"/> Aa

[+ Add criterion](#)

**Comment**

Description of the whitelist

---

**Expiration date**

You can optionally set an expiration date for your whitelist. It is automatically disabled on expiration.

---

**Retroactive application**

Retroactively whitelist security events

Applying this whitelist retroactively will update the security events statuses from:  To:

**10 000+ security events** will be impacted according to the criteria listed above.

## Threats

To

Settings (5)		Select actions		1 777 351 Threats		Search	
<span>General -&gt; Status is</span> <span>New</span> <span>Investigating</span> <span>✕</span> <span>+</span>							
General	Dates	Rules	Agents	Summary			
<input type="checkbox"/> <p>Level: <span>Low</span></p> <p>Status: <span>New</span></p> <p>Threat ID: TH-2024-177596</p>	<p>2024-01-23 13:16:00Z</p> <p>2024-04-24 13:16:00Z</p> <p>Duration: 92d 00h 00m 00s</p>	<p><span>L</span> PowerShell Invoke-Command Execute... 8 K</p> <p>Show rule details</p>	<p>gest-ut2j</p> <p>Show endpoint details</p>	<p>8 K</p> <p>Security events</p> <p>User</p> <p>MITRE ATT&amp;CK tactics</p>	<p>8857</p> <p>UTM\</p> <p>Administrateur</p>	<input type="checkbox"/> <span>i</span>	
<input type="checkbox"/> <p>Level: <span>Critical</span></p> <p>Status: <span>New</span></p> <p>Threat ID: TH-2024-177585</p>	<p>2024-01-14 14:25:00Z</p> <p>2024-04-24 13:11:00Z</p> <p>Duration: 100d 22h 46m 00s</p>	<p><span>C</span> Recommended driver block list 5 K</p> <p><span>H</span> Suspicious Change in UAC Registry Con... 1</p> <p><span>M</span> Archiver Tool Started with Suspicious ... 93</p> <p>7 other rules 133</p> <p>Show rule details</p>	<p>DAR00-A-figueroa</p> <p>DAR00-A-enjhalbert</p> <p>DAR00-A-KACHOUCHE</p> <p>118 other endpoints</p> <p>Show endpoint details</p>	<p>422</p> <p>294</p> <p>159</p> <p>4 K</p> <p>Security events</p> <p>Users</p> <p>MITRE ATT&amp;CK tactics</p>	<p>5352</p> <p>15</p>	<input type="checkbox"/> <span>i</span>	
<input type="checkbox"/> <p>Level: <span>Medium</span></p> <p>Status: <span>New</span></p> <p>Threat ID: TH-2024-177760</p>	<p>2024-04-24 13:05:00Z</p> <p>2024-04-24 13:05:00Z</p> <p>Duration: 0d 00h 00m 00s</p>	<p><span>M</span> Archiver Tool Started with Suspicious P... 3</p> <p>Show rule details</p>	<p>DRHGC-AP-PETI01</p> <p>Show endpoint details</p>	<p>3</p> <p>Security events</p> <p>User</p> <p>MITRE ATT&amp;CK tactics</p>	<p>3</p> <p>UTM\</p> <p>virginie.petitpain</p>	<input type="checkbox"/> <span>i</span>	
<input type="checkbox"/> <p>Level: <span>Critical</span></p> <p>Status: <span>New</span></p> <p>Threat ID: TH-2024-177661</p>	<p>2024-03-03 14:32:00Z</p> <p>2024-04-24 12:40:00Z</p> <p>Duration: 51d 22h 08m 00s</p>	<p><span>C</span> Suspicious binary 10 K</p> <p><span>H</span> SetGID Access Flag Set via chmod/setc... 8</p> <p><span>H</span> File /etc/shadow Read 4</p> <p>22 other rules 9 K</p> <p>Show rule details</p>	<p>ut2j-siham-prod</p> <p>ut2j-siham-tools-test</p> <p>ut2j-siham-pale</p> <p>9 other endpoints</p> <p>Show endpoint details</p>	<p>10 K</p> <p>2 K</p> <p>2 K</p> <p>3 K</p> <p>Security events</p> <p>Users</p> <p>MITRE ATT&amp;CK tactics</p>	<p>19310</p> <p>15</p>	<input type="checkbox"/> <span>i</span>	
<input type="checkbox"/> <p>Level: <span>Medium</span></p> <p>Status: <span>New</span></p> <p>Threat ID: TH-2024-177665</p>	<p>2024-03-05 08:29:00Z</p> <p>2024-04-24 12:15:00Z</p> <p>Duration: 50d 03h 46m 00s</p>	<p><span>M</span> SystemD Service Started 118</p> <p>Show rule details</p>	<p>ruhnu</p> <p>Show endpoint details</p>	<p>119</p> <p>Security events</p> <p>User</p> <p>MITRE ATT&amp;CK tactics</p>	<p>119</p> <p>dockeruser</p>	<input type="checkbox"/> <span>i</span>	

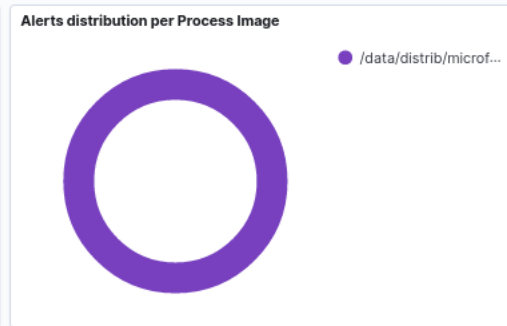
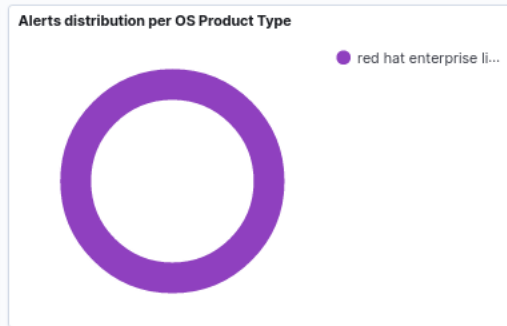
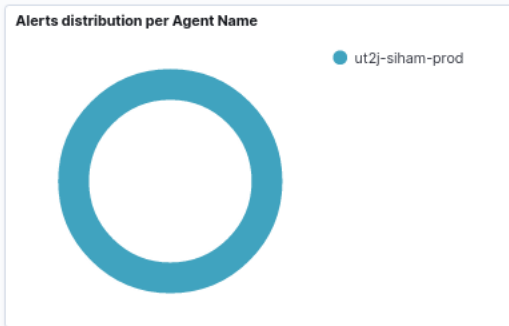
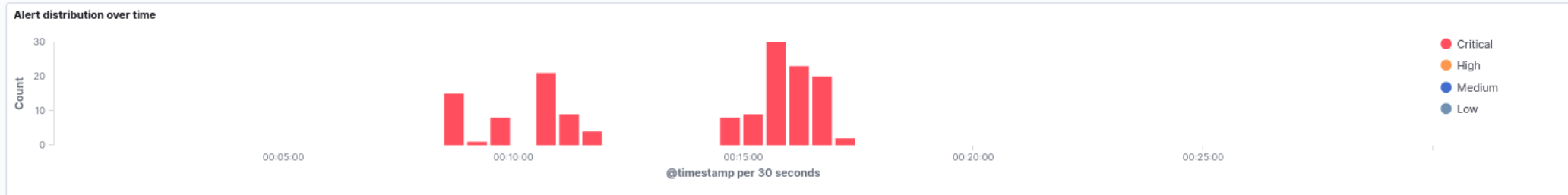
## Data Visualization

Data visualization

Alerts Audit logs Connections Event logs Processes

Search KQL Apr 24, 2024 @ 00:00:00.0 → Apr 24, 2024 @ 00:30:00.0 Refresh

Critical × + Add filter



**Alert list** 1-50 of 150

Time	level	alert_type	alert_subtype	agent.hostname	process.commandline	process.image_name	rule_name
> Apr 24, 2024 @ 00:17:00.459	critical	hlai	process	ut2j-siham-prod	mfsort take /data/distrib/hrpl804/txt/tmp/NRB306.1965713	/data/distrib/microfocus/cobol/bin/cobdriver	Suspicious binary
> Apr 24, 2024 @ 00:17:00.034	critical	hlai	process	ut2j-siham-prod	mfsort take /data/distrib/hrpl804/txt/tmp/NRB302.1965713	/data/distrib/microfocus/cobol/bin/cobdriver	Suspicious binary

## Agents

Settings (10) [CSV](#) Select actions **619 Agents**

[+ Filter](#)

<input type="checkbox"/> (0)	Status	Groups	Hostname	Dom...	Policy name	OS type	OS product type	Last seen	Version	
<input type="checkbox"/>	Online	UT2-SLM-USERS	DEEP0-AP-CORT11	UTM	Politique de Bloc age	Windows	Windows 10 Pro	2024-04-24 13:25:55Z	3.7.3	<a href="#">i</a> <a href="#">x</a>
<input type="checkbox"/>	Online	UT2-SLM-USERS	SHS-PC-Garde2	UTM	Politique de Bloc age	Windows	Windows 10 Pro	2024-04-24 13:25:55Z	3.7.3	<a href="#">i</a> <a href="#">x</a>
<input type="checkbox"/>	Online		TARTH	UTM	default	Windows	Windows Server 2012 Standard	2024-04-24 13:25:55Z	3.7.3	<a href="#">i</a> <a href="#">x</a>



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 5

[+ Add a description](#)

### Details

Hostname	DEEP0-AP-CORTI1	IP address	172.31.6.128 / 255.255.255.0
Domain name	i-univ-tlse2.fr / UTM	Unique ID	00b2e09b-b98a-4cd6-adce-aa52f20932c4
CPU	8 cores, 1800 Mhz	Version	3.7.3
Memory	16231.09 MiB	Additional info	<a href="#">Edit</a>
Machine serial	Z2RLX33		

### 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-AADEM
Product type	workstation

### Policy

Policy	Politique de Blocage <a href="#">Edit</a>
Sleep time	60 (s) +/- 10%
Log level	ERROR
Driver	Enabled / Loaded <a href="#">Edit</a>
Telemetry	Enabled <a href="#">Edit</a>

### Antivirus profile !

Profile	No Profile Configured <a href="#">Edit</a>
Antivirus	Antivirus Trend Micro Apex One

### Groups (1)

- UT2-SLM-USERS [Edit](#)

### Quarantined files

Last update (10 minutes ago): 2024-04-24 13:16:52Z [Refresh](#)

Total: 0 files

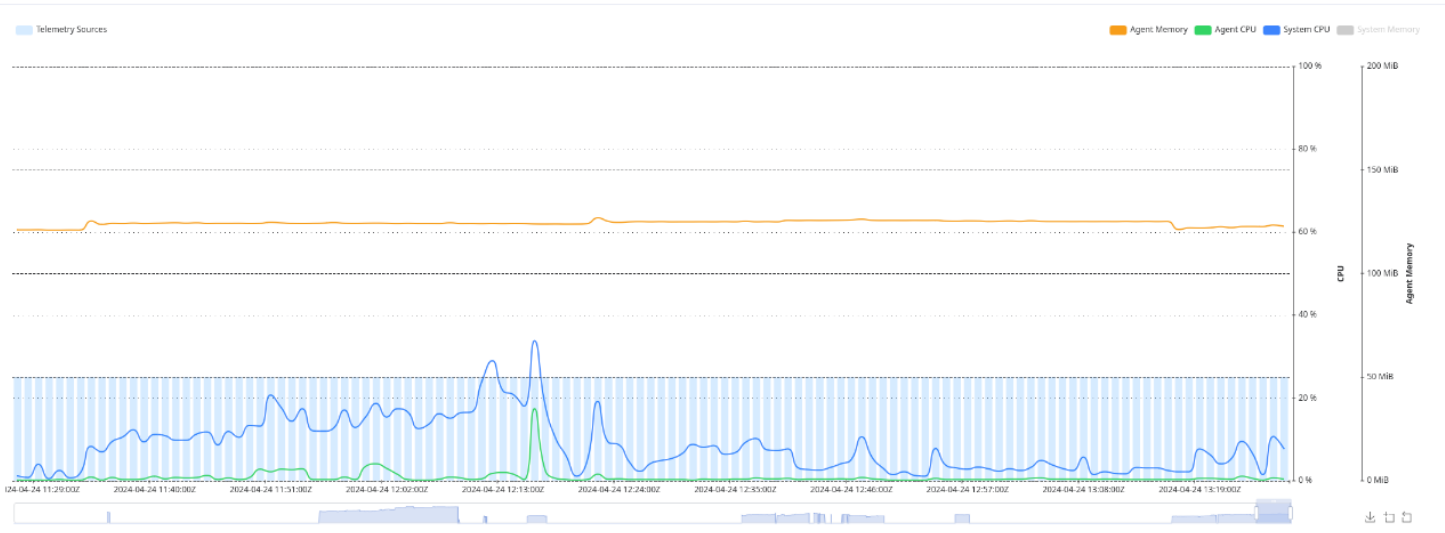
### Host Properties

Last update (10 minutes ago): 2024-04-24 13:16:52Z [Refresh](#)

- Users: 5
- Admins: 2
- Groups: 19
- Network interfaces: 8
- Applications: 65
- Disks: 1

### Resources used by Agent & System

[Auto refresh](#)



## Groups

[+ Create group](#)
[Settings \(4\)](#)
[csv](#)
16 Groups

[+ Filter](#)

Name	Description	Agents	Roles
UT2-INSPE-DSI-PROXR-USERS	Personnels de la DSI-ProxR	8	<a href="#">edit</a> <a href="#">info</a> <a href="#">delete</a>
UT2-INSPE-DSI-SRV	Serveurs INSPE (hors AD)	33	<a href="#">edit</a> <a href="#">info</a> <a href="#">delete</a>
UT2-INSPE-DSI-SRV-AD	Serveurs AD INSPE	12	<a href="#">edit</a> <a href="#">info</a> <a href="#">delete</a>
UT2-INSPE-USERS	Utilisateurs de l'INSPE	65	<a href="#">edit</a> <a href="#">info</a> <a href="#">delete</a>

**Edit YARA file** ✕

\* Name

Enabled

Maturity

\* Content

```

1 rule cobalt_strike_invoke_assembly
2 {
3     meta:
4         title = "Cobalt Strike Invoke Assembly DLL - generic"
5         id = "1bf15ffa-4d4a-4543-9308-4ed3d6269433"
6         description = "Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as adversary simula
7         references = "https://attack.mitre.org/software/S0154/"
8         date = "2020-12-15"
9         modified = "2020-12-15"
10        author = "HarfangLab"
11        tags = "attack.s0154;attack.defense_evasion;attack.t1569.002;attack.t1218;attack.t1055.012;attack.t1027.005;attack.t1
12        classification = "Windows.Framework.CobaltStrike"
13        os = "Windows"
14        score = 60
15
16    strings:
17        $s1 = "[ - ] No .NET runtime found. :(" ascii
18        $s2 = "[ - ] get_EntryPoint failed." ascii
19        $s3 = "[ - ] GetParameters failed." ascii
20        $s4 = "[ - ] Invoke_3 on EntryPoint failed" ascii
21        $s5 = "[ - ] Failed to create the runtime host" ascii
22        $s6 = "[ - ] CLR failed to start w/hr 0x%08lx" ascii
23        $s7 = "[ - ] ICorRuntimeHost::GetDefaultDomain failed w/hr 0x%08lx" ascii
24        $s8 = "[ - ] Failed to get default AppDomain w/hr 0x%08lx" ascii
25        $s9 = "[ - ] Failed to load the assembly w/hr 0x%08lx" ascii
26        $s10 = "ICLRMetaHost::GetRuntime (%S) failed w/hr 0x%08lx" ascii
27
28    condition:
29        5 of them
30 }
31

```

### Edit Sigma rule

\* Name

Enabled

Maturity

Level override

Content

```
1 title: Suspicious Binary Signed with ANYDESK stolen certificate
2 id: f814fbb3-3572-4d00-a82b-7897523bbccd
3 description: Detects the execution of suspicious binaries signed with Anydesk stolen certificate.
4 references:
5   - https://github.com/Neo23x0/signature-base/blob/master/yara/gen_anydesk_compromised_cert_feb23.yar
6 date: 2024/02/06
7 status: stable
8 author: FA_CM
9 tags:
10  - attack.defense_evasion
11  - attack.t1553.002
12 logsource:
13   product: windows
14   category: process_creation
15 detection:
16   selection_displayname:
17     ProcessSignatureSignerIssuerName: 'DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1'
18   selection_serial:
19     ProcessSignatureSignerSerialNumber: '0dbf152deaf0b981a8a938d53f769db8'
20   condition: all of selection_*
21 level: critical
```

**Threat Intelligence**

YARA Sigma IOC Driver block list Rulesets Whitelists

The recommended driver block list is an HarfangLab-maintained list containing driver indicators that are considered dangerous from a security standpoint. Drivers can also be blocked or detected through other engines, such as Sigma, YARA or IOC.

Settings (5) [Download CSV](#) 1 845 Driver indicators

[+ Filter](#)

Type	Value	Enabled	Maturity	Comment
Hash	d9a73df5ac5c68ef5b37a67e5e649332da0f649c3bb6828f70b65c0a2e7d3a23	✓	Stable	Vulnerable Kernel Driver (aka ComputerZ.Sys) [https://blogs.vmware.com/security/2023/10/hunting-vulnerable-kernel-drivers.html]
Hash	8047859a7a886bcf4e666494bd03a6be9ce18e20dc72df0e5b418d180efef250	✓	Stable	Vulnerable Kernel Driver (aka ComputerZ.Sys) [https://blogs.vmware.com/security/2023/10/hunting-vulnerable-kernel-drivers.html]
Hash	342cf884840fc2b48c96398f690a1801ed8ac1ea59305af9e3d070d13ef85601	✓	Stable	Vulnerable Kernel Driver (aka mhyprot2.sys) [https://www.loldrivers.io/drivers/57354c82-ff9c-4a54-8377-d195e4ff0a26/]
Hash	94ba4bcdb55d6faf9f33642d0072109510f5c57e8c963d1a3eb4f9111f30112	✓	Stable	Malicious Kernel Driver (aka mimidrv.sys) [https://www.loldrivers.io/drivers/87752fb8-e9f6-4235-91e2-c4343677d817/]
Hash	b95b2d9b29bd25659f1c7ba5a187f8d23cde01162d9b5b1a2c4aea8f64b38441	✓	Stable	American Megatrends vulnerable BIOS flash tool (aka UCOREW64.SYS and amifldr64.sys) [https://www.loldrivers.io/drivers/a338a9fc-9fe3-400c-9fe4-69bb7892602d/]
Hash	238046cfe126a1f8ab96d8b62f6aa5ec97bab830e2bae5b1b6ab2d31894c79e4	✓	Stable	Elaborate Bytes vulnerable driver (aka ElbyCDIO.sys) [CVE-2009-0824] [https://www.loldrivers.io/drivers/855ade1f-8a9e-4c9d-ab8e-d7e409609852/]
Hash	cff9aa9046bdf781d34f607d901a431a51bb7e5f48f4f681cc743b2cdedc98c	✓	Stable	Intel Ethernet diagnostics vulnerable driver (aka IQVW64.sys) [CVE-2015-2291] [https://www.loldrivers.io/drivers/1d2cdef1-de44-4849-80e5-e2fa288df681/]
Hash	77950e2a40ac0447ae7ee1ee3ef1242ce22796a157074e6f04e345b1956e143c	✓	Stable	Process Explorer driver (aka PROCEXP.SYS and PROCEXP152.SYS) [https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer]
Hash	ff1cce7374a1a5054a6f4437e3e0504b14ed76e17090cc6b1a4ec0e2da427a5	✓	Stable	Vulnerable Kernel Driver (aka HWINFO32.SYS) [https://www.loldrivers.io/drivers/2225128d-a23f-434a-aaee-69a88ea64fbd/]
Hash	4710acc9c4a61e2fcd6aafb09d72e11b603ef8cd732e12a84274ea9ad6d43be	✓	Stable	NVIDIA vulnerable flash tool (aka nvflash.sys nd nvflsh64.sys) [CVE-2019-5688] [https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules]
Hash	ac26150bc98ee0419a8b23e4cda3566e0eba94718ba8059346a9696401e9793d	✓	Stable	Vulnerable Kernel Driver (aka capcom.sys) [https://www.loldrivers.io/drivers/b51c441a-12c7-407d-9517-559cc0030cf6/]

## Threat Intelligence

YARA Sigma IOC Driver block list Rulesets Whitelists

+ Add whitelist

csv

Show provided by HarfangLab

+ Filter

Last update



Creation date



From



To

Search by field, value, rule, comment...

HL-AI	process.hashes.sha256	eq	9bcd9b93b138e8dca4721508d53f9c5a3cb535e32aa...	Applies only on HL-AI engine	
	process.process_name	eq	mfsort	pascal.bassoua	2024/04/24 13:16 0
	process.image_name	eq	/data/distrib/microfocus/cobol/bin/cobdriver		
YARA	process.pe_info.original_...	eq	update_task.exe	Applies only on YARA engine	Whitelist provided by HarfangLab
	process.signed	eq	true	HarfangLab	2024/04/22 16:15 178225
	process.signature_info.si...	eq	Fortinet Technologies (Canada) ULC		
YARA	process.pe_info.original_...	eq	AVGSvc.exe	Applies only on YARA engine	Whitelist provided by HarfangLab
	process.signed	eq	true	HarfangLab	2024/04/18 08:56 0
	process.signature_info.si...	eq	AVG Technologies USA, LLC		
<a href="#">Show 2 more items</a>					
YARA	process.pe_info.original_...	eq	ShShell.exe	Applies only on YARA engine	Whitelist provided by HarfangLab
	process.signed	eq	true	HarfangLab	2024/04/15 09:53 0
	process.signature_info.si...	eq	EnigmaSoft Limited		
YARA	process.image_name	contains	\\FIP-FS\Bin\scanningprocess.exe	Applies only on YARA engine	Whitelist provided by HarfangLab
	process.integrity_level	eq	System	HarfangLab	2024/03/29 14:23 0
	process.signature_info.si...	eq	Microsoft Corporation		
<a href="#">Show 1 more items</a>					

## Security event - IP Route Execution (Linux) [View threat](#)

Add Whitelist

Quick actions

Summary Process tree Related timeline Rule Static analysis

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



### IP Route Execution (Linux)

Detects the execution of the IP route utility to display the routing table management. Attackers may use it during discovery phase to discover remote systems.

Endpoint detection date: 2024/04/24 07:20:05Z

### Process

ip  
Integrity Level

**Process name** ip (pid=1576851)  
**Image name** /usr/bin/ip [Download](#)  
**Command-line** ip -6 r  
**Execution** Detected  
**Quarantine** No action  
**Username** root  
**Current directory** /usr/lib/check\_mk\_agent/plugins/  
**User SID**  
**Process Create Time** 2024/04/24 07:20:05Z

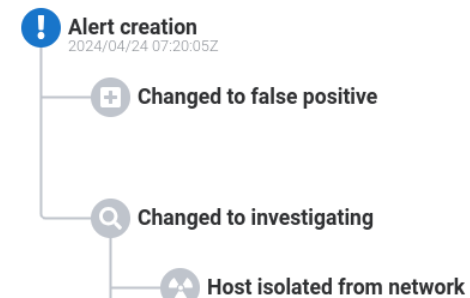
**Size** 632632 (617.80 KiB)  
**MD5** 5bbec30e69f4fd4dba735fd6a45ad643  
**SHA1** 3c954614f2c9af7181e4d00e00ab4485e4a9c33f  
**SHA256** 1cadbfa239fdacf0b4f2472a071a3dd69ae8011ca3fe9ee5cff16c937b945fe(see on VirusTotal)

### vega-h

Debian GNU/Linux 11 (bullseye) (5.15.143-1-pve)

**Status** Online  
**Version** 3.7.3  
**IP Address** 172.16.2.150

### Status: Alert creation



## Security event - IP Route Execution (Linux) [View threat](#)

Add Whitelist

Quick actions

Summary **Process tree** Related timeline Rule Static analysis

[Recenter process graph](#)
[Show legend](#)
[Enter fullscreen](#)
 Show Remote Threads
  Show Process Access



### Process

**Process name** [ip](#)  
**Size** 617.80 KiB (632632 B)  
**Image name** [/usr/bin/ip](#)  
**Command-line** [ip -6 r](#)  
**Username** [root](#)  
**Current directory** [/usr/lib/check\\_mk\\_agent/plugins/](#)  
**Integrity level**  
**Started at** 2024/04/24 07:20:05Z  
**PID** [1576851](#)  
**Unique ID** [aef3d195-f01a-499c-5911-2d23d55ca4fd](#)  
**Parent image name** [/usr/bin/dash](#)  
**PPID** [aef3d195-f01a-499c-1afd-c640d4b182a5](#)

### Signature

**Signed** ✘

### Hashes

**MD5** [5bbec30e69f4fd4dba735fd6a45ad643](#)

### Security events

Settings (8)

Update status

Search



## Security event - IP Route Execution (Linux) [View threat](#)

Add Whitelist

Quick actions

Summary Process tree Related timeline **Rule** Static analysis

### Rule definition

```

1 title: "IP Route Execution (Linux)"
2 id: b7865333-71e3-4f99-be6c-df2db775b39d
3 description: "Detects the execution of the IP route utility to display the routing table.
4 Attackers may use it during discovery phase to discover remote systems."
5 references:
6   - https://man7.org/linux/man-pages/man8/ip-route.8.html
7   - https://attack.mitre.org/techniques/T1018/
8 status: stable
9 date: 2022/12/23
10 modified: 2024/04/22
11 author: HarfangLab
12 tags:
13   - attack.discovery
14   - attack.t1018
15 logsource:
16   category: process_creation
17   product: linux
18 detection:
19   selection:
20     Image|endswith: '/ip'
21     CommandLine|contains: 'r' # route
22     ParentImage|startswith: '/' # Filter-out missing parents
23
24   exclusion_not_show:
25     CommandLine|contains:
26       - 'add'
27       - 'change'
28       - 'replace'
29       - 'delete'
30       - 'flush'
31       - 'get'
32       - 'restore'
33       - 'rule'
34
35   exclusion_rule:

```

### Configuration

#### Enabled

Enable or disable the detection of this rule on the endpoints

enabled

#### Block on endpoint

Enabling this option will block all processes that trigger this rule, if the endpoint's policy is configured accordingly

disabled

### Maturity

#### Rule maturity

Update rule maturity

Stable

### Level override

#### Rule level override

Update rule level override

No override

## Security event - IP Route Execution (Linux) [View threat](#)

Add Whitelist Quick actions

### Rule definition

```

66 exclusion_sosreport:
67   - GrandparentCommandLine: '/usr/bin/python /usr/sbin/sosreport'
68   - GrandparentCommandLine|startswith: '/usr/bin/python /usr/sbin/sosreport '
69
70 exclusion_ocsinventory1:
71   ParentCommandLine|startswith:
72     # /usr/bin/perl /usr/bin/ocsinventory-agent --force
73     # /usr/bin/perl /usr/sbin/ocsinventory-agent --wait 100
74     - '/usr/bin/perl /usr/bin/ocsinventory-agent'
75     - '/usr/bin/perl /usr/sbin/ocsinventory-agent'
76     - '/usr/bin/perl /usr/local/bin/ocsinventory-agent'
77 exclusion_ocsinventory2:
78   GrandparentCommandLine|startswith:
79     # /usr/bin/perl /usr/bin/ocsinventory-agent --force
80     # /usr/bin/perl /usr/sbin/ocsinventory-agent --wait 100
81     - '/usr/bin/perl /usr/bin/ocsinventory-agent'
82     - '/usr/bin/perl /usr/sbin/ocsinventory-agent'
83     - '/usr/bin/perl /usr/local/bin/ocsinventory-agent'
84
85 exclusion_hyperv:
86   GrandparentImage:
87     - '/usr/sbin/hypervkvpd'
88     - '/usr/sbin/hv_kvp_daemon'
89
90 exclusion_qualys:
91   GrandparentImage:
92     - '/usr/local/qualys/cloud-agent/bin/qualys-scan-util'
93     - '/usr/local/qualys/cloud-agent/bin/qualys-cloud-agent'
94
95 exclusion_gitlab:
96   - ParentCommandLine|contains: '/opt/gitlab/embedded/bin/ruby /opt/gitlab/embedded'
97   - GrandparentCommandLine: '/bin/bash /opt/gitlab/bin/gitlab-ctl reconfigure'
98   - GrandparentImage|startswith: '/opt/gitlab/embedded/bin/'
99
100 exclusion_udscan:
  
```

### Configuration

**Enabled**  enabled  
Enable or disable the detection of this rule on the endpoints

**Block on endpoint**  disabled  
Enabling this option will block all processes that trigger this rule, if the endpoint's policy is configured accordingly

### Maturity

**Rule maturity** Stable  
Update rule maturity

### Level override

**Rule level override** No override  
Update rule level override

+ Add whitelist csv

Show provided by HarfangLab

HarfangLab
✕

**Quick Whitelist**

Click on the desired value to add them as a criterion to the whitelist. You can change each criterion's value.

**Configuration**

**Agent**

- + Hostname vega-h

**Process**

- + Process Name ip
- + Image Name /usr/bin/ip
- + Command-line ip -6 r
- + SHA256 1cadbfa239fdacf0b4f2472a071a3dd69ae8011ca3fe9ee5cff16c937b945fe
- + Ancestors /usr/bin/dash|usr/bin/bash|usr/lib/systemd/systemd

**Parent Process**

- + Parent image /usr/bin/dash
- + Parent command-line /bin/sh ./mk\_inventory linux

**Grandparent Process**

- + Grandparent image /usr/bin/dash
- + Grandparent command-line /bin/sh ./mk\_inventory linux

**Criteria**

Aa

Please fill all the fields