TP SOC/SIEM

SOC - Security Operation Center

What ?

- Détecter les attaques en cours dés que possible
- Réagir efficacement et de manière coordonnée
- Fournir un retour d'expérience (retex) après chaque incident
- Faire de la veille
- Automatiser et réaliser des procédures

Who ?

- Cellule spécialisée dans la détection, l'analyse, la réponse aux incidents de sécurité d'un système d'information.Il s'agit d'une équipe centralisée composée d'analystes SOC et de leurs outils. Cette équipe opère souvent en continue (24h/24 & 7j/7)

Analyste N1

- Triage et de la surveillance

Analyste N2

- Analyste seniors ou incidents responders

Analyste N3

- Threat Hunters, experts forensics, reverse engineers
- SOC Managers
- Supervise la cellule et interagit avec le RSSI et la direction

How ?

- Surveillance en continue des logs

- Corrélation des événements
- Gestion des alerts et des incidents de sécurité
- Investigations et forensics
- Réponse aux incidents
- Rédaction de rapports
- Veille et anticipation

SIEM - Security Informations and Event Management

Collecte des logs

- Firewalls
- Endpoints
- Solutions tierces
- Normalisation des champs : source_ip, ip_src ou ipv4_source ?
- Proposition de solution : OSSEM project
- Les backends doivent toujours être accessible

Log Analysis

- Analyser les logs reçus depuis les endpoints
- Déterminer la sévérité des logs reçus via l'analyse de logs
- Création de jeu de règles
- Faire le tri entre les alertes sans intérêts (ce que l'on appelle le bruit)

Log Storage

- Stockage des logs
- Besoin de pouvoir interroger les logs de manière claire et rapide
- Log Visualisation
- Voir les logs via des widgets et des dashboards
- Avoir un dashboard qui agrège les sources de manière intelligente

Log Intelligence Enrichment

- Enrichissement des données reçues par plusieurs sources de CTI
- Stockage et parsing des logs pour ne stocker que les données importantes
- Automatiser pour que les analystes SOC n'aient pas à enrichir manuellement les logs
- Log Case Management
- Besoin d'une plateforme pour identifier clairement les événements critiques
- Permettre la collaboration entre les membres du SOC
- Permettre des actions de réponse pour que les analystes puissent déclencher des actions sur les endpoints

Log Investigation

- Les analystes SOC doivent pouvoir intervenir sur les endpoints
- Mise en quarantaine d'un device
- Pouvoir collecter les données des endpoints pour du forensic

Identifiants Proxmox

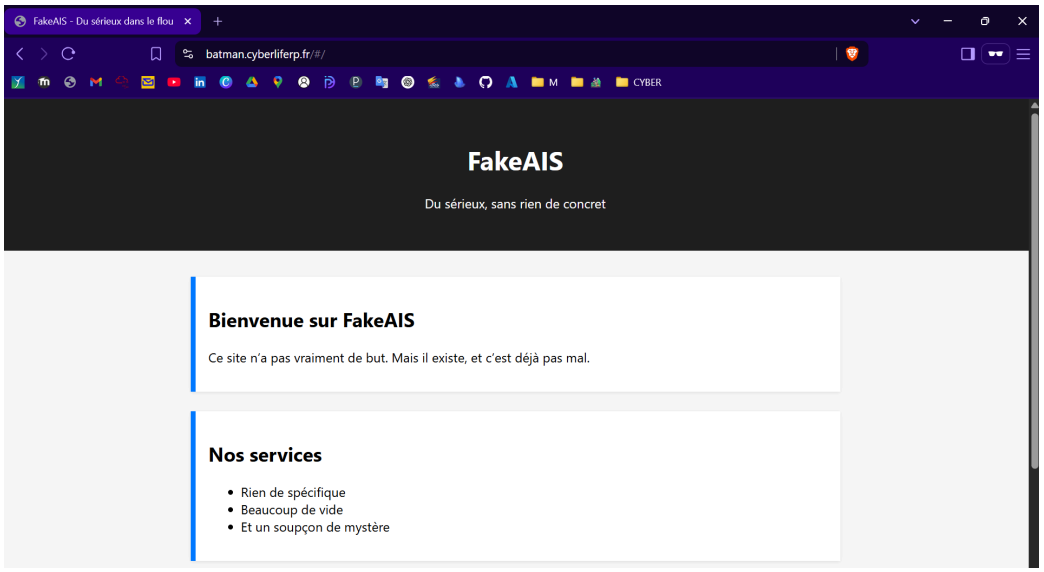
Identifiant : root

Mot de passe : Kirikou2209!

Environnement

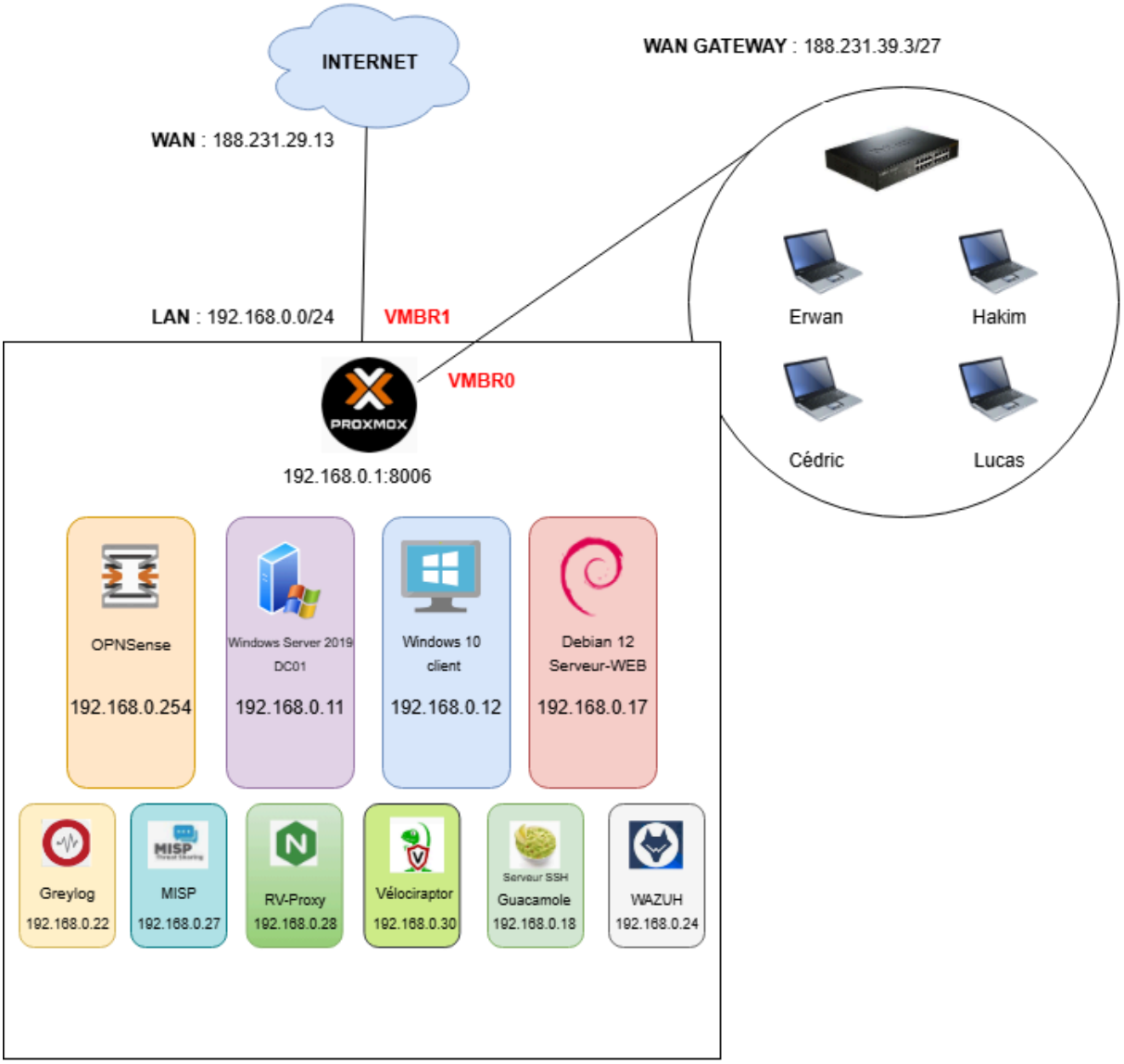
- 1 firewall physique OPNSense avec - id : root ; mdp : opnsense
  - IPv4 publique
  - Nom de domaine
  - interface WAN / LAN
- Un serveur "cube" Proxmox avec
  - Microsoft Windows
    - Contrôleur de domaine ADDS DC-01 : simple forêt et simple domaine id : Administrateur / Kirikou202209!
    - Machine(s) Microsoft Windows 10 ou 11 - id: erwan.dussaux /Kirikou202209!
  - GNU / Linux

- Serveur WEB id: fakeais/Kirikou2209!
  - Page web bidon
  - Certbot



- Serveur SSH - id : fakeais/Kirikou2209!
  - Rebond SSH

Schéma à Faire :

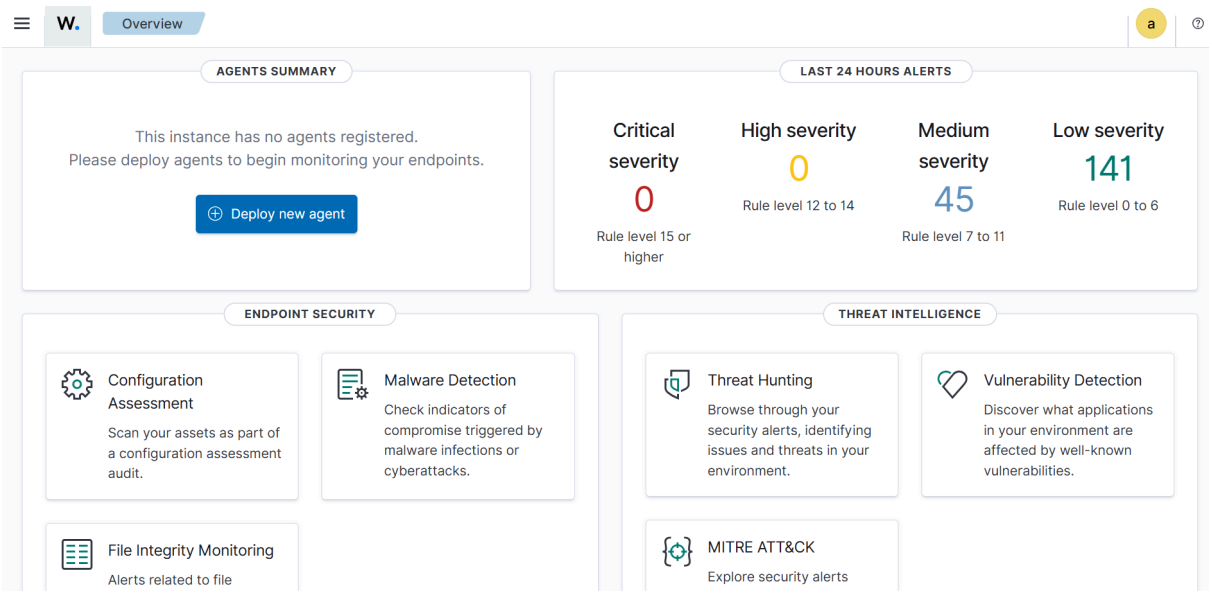


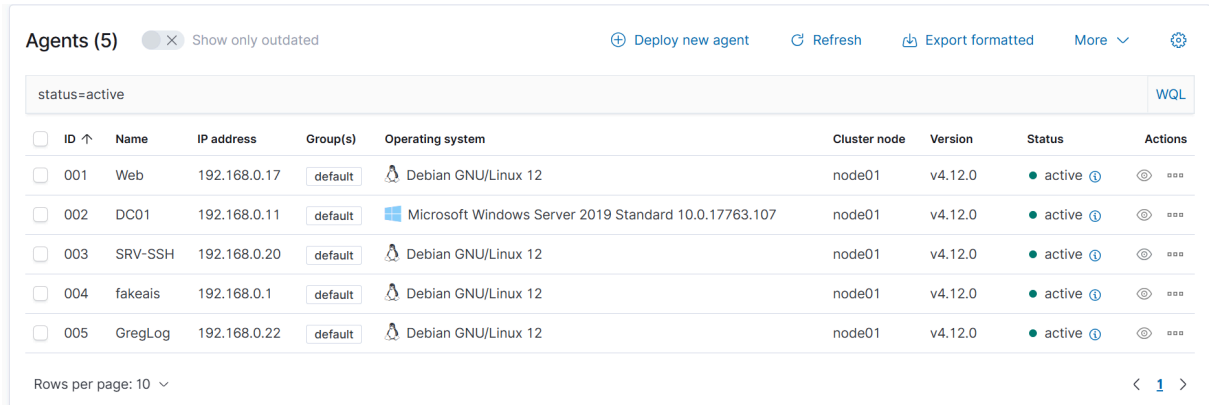

```
root@web:/home/fakeais# curl xvideo.com
<script>
    (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
        (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
          m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
        })(window,document,'script','//www.google-analytics.com/analytics.js','ga');

  ga('create', 'UA-39784601-1', 'xvideo.com');
  ga('send', 'pageview');


setTimeout(OpenSite, 400);
function OpenSite()
{
  document.location = 'https://share.myfreecams.com/?cam=30603';
}
```

Wazuh

https://documentation.wazuh.com/current/deployment-options/docker/wazuh-container.html

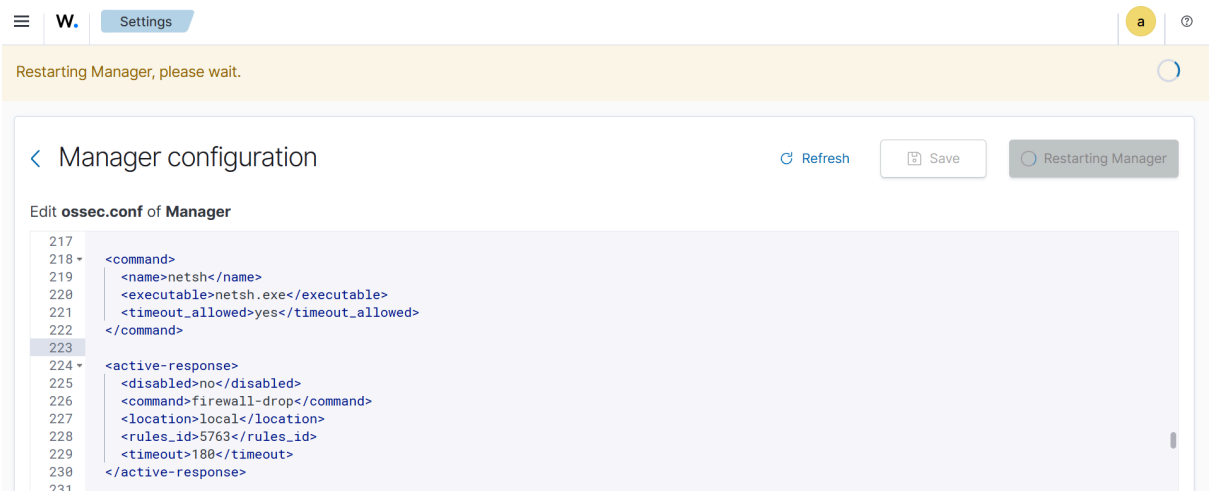
https://192.168.0.24/app/login admin/SecretPassword





Active response blocking SSH Bruteforce

Doc



Il faut ajouter sur chaque vm contenant l'agent wazuh, l'outil iptables et occtroyer les permissions nécessaires pour l'utilisateur Wazuh :

- En éditant le fichier /etc/sudoers et insérant ceci

```
wazuh ALL=(ALL) NOPASSWD: /sbin/iptables
```

- Ensuite redémarrer l'agent sur chaque vm concerner

```
sudo systemct restart wazuh-agent
```

Test :

```
└─$ ping 192.168.0.17
PING 192.168.0.17 (192.168.0.17) 56(84) bytes of data.
64 bytes from 192.168.0.17: icmp_seq=1 ttl=63 time=1.12 ms
64 bytes from 192.168.0.17: icmp_seq=2 ttl=63 time=1.26 ms
64 bytes from 192.168.0.17: icmp_seq=3 ttl=63 time=1.31 ms
64 bytes from 192.168.0.17: icmp_seq=4 ttl=63 time=1.19 ms
64 bytes from 192.168.0.17: icmp_seq=5 ttl=63 time=1.38 ms
64 bytes from 192.168.0.17: icmp_seq=6 ttl=63 time=1.73 ms
^C
--- 192.168.0.17 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 1.124/1.330/1.728/0.195 ms

┌──(lucas㉿Lap)-[~]
└─$ sudo hydra -t 4 -l fakeais -P /usr/share/wordlists/rockyou.txt 192.168.0.17 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 09:49:40
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, t
o prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.0.17:22/
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 14344367 to do in 7471:02h, 4 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(lucas㉿Lap)-[~]
└─$ ping 192.168.0.17
PING 192.168.0.17 (192.168.0.17) 56(84) bytes of data.
```

	↓ timestamp	agent.name	rule.description	rule.level	rule.id
	Jun 4, 2025 @ 09:50:13.240	Web	sshd: authentication failed.	5	5760
	Jun 4, 2025 @ 09:50:13.231	Web	sshd: authentication failed.	5	5760
	Jun 4, 2025 @ 09:50:13.223	Web	sshd: authentication failed.	5	5760
	Jun 4, 2025 @ 09:50:13.219	Web	sshd: authentication failed.	5	5760
	Jun 4, 2025 @ 09:50:11.284	Web	PAM: User login failed.	5	5503
	Jun 4, 2025 @ 09:50:11.284	Web	PAM: Multiple failed logins in a small period of time.	10	5551
	Jun 4, 2025 @ 09:50:11.284	Web	PAM: User login failed.	5	5503
	Jun 4, 2025 @ 09:50:11.284	Web	Multiple authentication failures.	10	40111
	Jun 4, 2025 @ 09:50:11.284	Web	PAM: User login failed.	5	5503
	Jun 4, 2025 @ 09:50:11.242	Web	syslog: User authentication failure.	5	2501
	Jun 4, 2025 @ 09:50:11.240	Web	Maximum authentication attempts exceeded.	8	5758
	Jun 4, 2025 @ 09:50:11.236	Web	syslog: User missed the password more than one time	10	2502
	Jun 4, 2025 @ 09:50:11.236	Web	syslog: User authentication failure.	5	2501
	Jun 4, 2025 @ 09:50:11.236	Web	syslog: User authentication failure.	5	2501
	Jun 4, 2025 @ 09:50:11.236	Web	syslog: User missed the password more than one time	10	2502

```
root@web:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.0.15         anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.0.15         anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Detecting Cobalt Strike beacons using Wazuh

Ajout de règle dans local_rules.xml depuis le dashboard Wazuh :


```
<group name="local,cobalt_strike,beaconing,">

  <rule id="100002" level="3">
    <if_sid>61600</if_sid>
    <field name="win.system.eventID">^17$</field>
    <description>A pipe was created. Possible Cobalt Strike activity.</descripti
    <mitre>
      <id>T1071</id>
    </mitre>
  </rule>
```

```
  <rule id="100003" level="14">
    <if_sid>100002</if_sid>
    <field name="win.eventdata.pipeName" type="pcre2">(?i)MSSE-[0-9]{4}-s
    <description>A named pipe $(win.eventdata.pipeName) associated with Co
    <mitre>
      <id>T1071</id>
    </mitre>
  </rule>

  <rule id="100004" level="14">
    <if_sid>100003</if_sid>
    <field name="win.eventdata.pipeName" type="pcre2">(?i)msagent_[0-9a-f
    <description>A named pipe $(win.eventdata.pipeName) associated with Co
    <mitre>
      <id>T1071</id>
      <id>T1572</id>
    </mitre>
  </rule>

  <rule id="100005" level="14">
    <if_sid>100003</if_sid>
    <field name="win.eventdata.pipeName" type="pcre2">(?i)postex_ssh_[0-9
    <description>A named pipe $(win.eventdata.pipeName) associated with Co
    <mitre>
      <id>T1071</id>
      <id>T1572</id>
    </mitre>
  </rule>

</group>
```

Detecting and removing malware using VirusTotal integration

Agent Linux

Voici les étapes pour configurer Wazuh afin de surveiller en **quasi temps réel** les changements dans le répertoire `/root` sur un système Ubuntu. Elles s'appliquent également à d'autres distributions Linux.

1. Activer la surveillance des fichiers sur l'agent Wazuh

Dans le fichier de configuration de l'agent Wazuh `/var/ossec/etc/ossec.conf`, recherchez le bloc `<syscheck>` et assurez-vous que `<disabled>` est défini à `no`.

Ajoutez ensuite la ligne suivante à ce bloc pour surveiller le répertoire `/root` :

```
<directories realtime="yes">/root</directories>
```

---

2. Installer `jq` (outil pour traiter le JSON)

```
sudo apt update
sudo apt -y install jq
```

---

3. Créer le script de réponse active `remove-threat.sh`

Fichier : `/var/ossec/active-response/bin/remove-threat.sh`

```
#!/bin/bash

LOCAL=`dirname $0`;
cd $LOCAL
cd ../

PWD=`pwd`

read INPUT_JSON
FILENAME=$(echo $INPUT_JSON | jq -r .parameters.alert.data.virustotal.source.file)
COMMAND=$(echo $INPUT_JSON | jq -r .command)
LOG_FILE="${PWD}/../logs/active-responses.log"

#------------------------ Analyse de la commande ------------------------#
if [ ${COMMAND} = "add" ]
```

```
then
 printf '{"version":1,"origin":{"name":"remove-threat","module":"active-resp
onse"},"command":"check_keys", "parameters":{"keys":[]}}\n'
 read RESPONSE
 COMMAND2=$(echo $RESPONSE | jq -r .command)
 if [ ${COMMAND2} != "continue" ]
 then
  echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Réponse acti
ve annulée" >> ${LOG_FILE}
  exit 0;
 fi
fi

# Suppression du fichier
rm -f $FILENAME
if [ $? -eq 0 ]; then
 echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Fichier malveil
lant supprimé avec succès" >> ${LOG_FILE}
else
 echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Erreur lors de
la suppression du fichier" >> ${LOG_FILE}
fi

exit 0;
```

Modifiez les droits et la propriété du script :

```
sudo chmod 750 /var/ossec/active-response/bin/remove-threat.sh
sudo chown root:wazuh /var/ossec/active-response/bin/remove-threat.sh
```

Redémarrez l'agent Wazuh :

```
sudo systemctl restart wazuh-agent
```

Wazuh Manager

1. Ajouter des règles locales pour détecter des modifications dans `/root`

Fichier : `/var/ossec/etc/rules/local_rules.xml`

```
<group name="syscheck,pci_dss_11.5,nist_800_53_SI.7,">
  <rule id="100200" level="7">
    <if_sid>550</if_sid>
    <field name="file">/root</field>
    <description>Fichier modifié dans le répertoire /root.</description>
  </rule>
  <rule id="100201" level="7">
    <if_sid>554</if_sid>
    <field name="file">/root</field>
    <description>Fichier ajouté au répertoire /root.</description>
  </rule>
</group>
```

2. Activer l'intégration VirusTotal

Ajoutez dans `/var/ossec/etc/ossec.conf` :

```
<ossec_config>
  <integration>
    <name>virustotal</name>
    <api_key><VOTRE_CLÉ_API_VIRUSTOTAL></api_key> <!-- Remplacez c
eci -->
    <rule_id>100200,100201</rule_id>
    <alert_format>json</alert_format>
  </integration>
</ossec_config>
```

ℹ️ **Remarque :** La version gratuite de l'API VirusTotal est limitée à **4 requêtes par minute**. Si vous disposez d'une clé premium, vous pouvez ajouter davantage de règles ou surveiller plus de répertoires.

---

3. Activer la réponse active et appeler le script `remove-threat.sh`

Ajoutez ceci à `ossec.conf` :

```
<ossec_config>
  <command>
```

```
    <name>remove-threat</name>
    <executable>remove-threat.sh</executable>
    <timeout_allowed>no</timeout_allowed>
  </command>

  <active-response>
    <disabled>no</disabled>
    <command>remove-threat</command>
    <location>local</location>
    <rules_id>87105</rules_id>
  </active-response>
</ossec_config>
```

4. Ajouter des règles pour suivre les résultats des réponses actives

Ajoutez ces règles à `local_rules.xml` :

```
<group name="virustotal,">
  <rule id="100092" level="12">
    <if_sid>657</if_sid>
    <match>Successfully removed threat</match>
    <description>$(parameters.program) a supprimé la menace située à $(p
arameters.alert.data.virustotal.source.file)</description>
  </rule>

  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Erreur lors de la suppression de la menace située à $(para
meters.alert.data.virustotal.source.file)</description>
  </rule>
</group>
```

5. Redémarrer le gestionnaire Wazuh

```
sudo systemctl restart wazuh-manager
```

Test de l’attaque

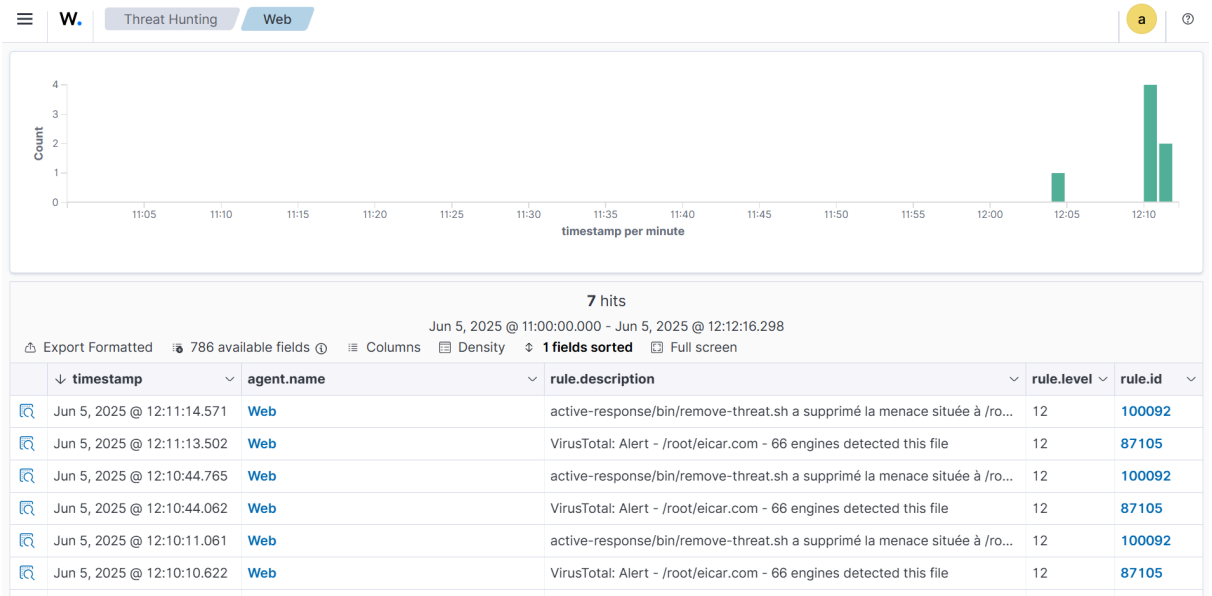
Sur l’agent :

```
sudo curl -Lo /root/eicar.com https://secure.eicar.org/eicar.com && sudo ls -la
```

Résultat attendu

1. Le fichier est détecté par Wazuh via FIM (surveillance du fichier `/root`).
2. La règle déclenche une requête vers l’API VirusTotal.
3. VirusTotal identifie le fichier comme malveillant (car EICAR est une signature de test).
4. Wazuh exécute automatiquement le script `remove-threat.sh`.
5. Le fichier est supprimé, et un journal de succès ou d’échec est généré.

Résultat sur notre infra les alertes remontent bien et le virus est bien supprimé sur l’agent ✅ :



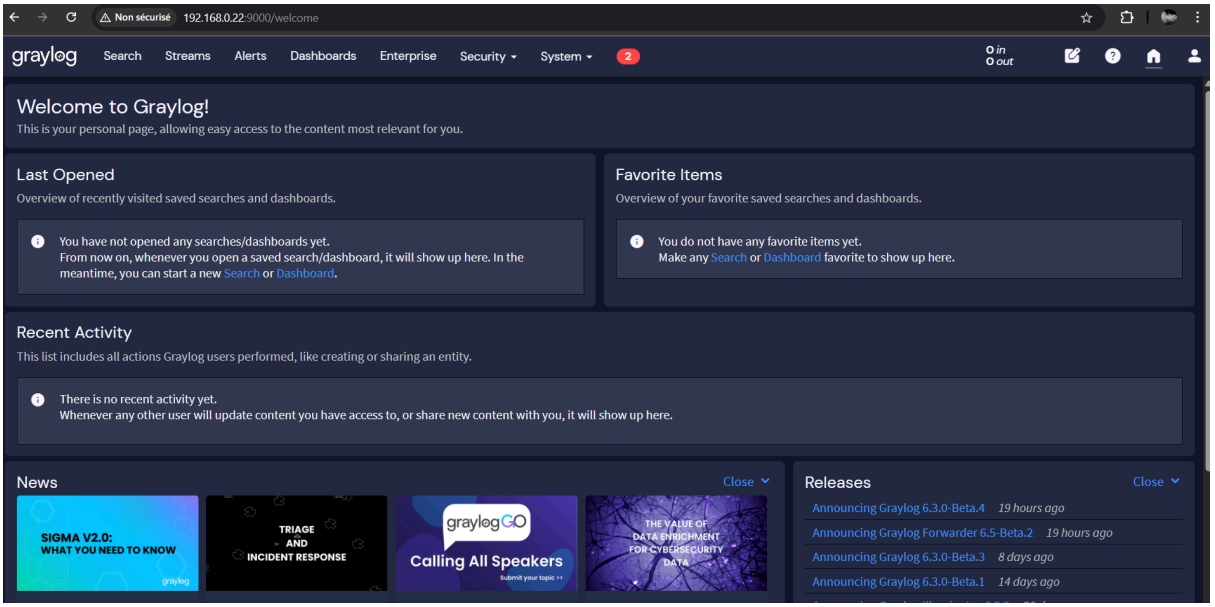
timestamp	agent.name	rule.description	rule.level	rule.id
Jun 5, 2025 @ 12:11:14.571	Web	active-response/bin/remove-threat.sh a supprimé la menace située à /ro...	12	100092
Jun 5, 2025 @ 12:11:13.502	Web	VirusTotal: Alert - /root/eicar.com - 66 engines detected this file	12	87105
Jun 5, 2025 @ 12:10:44.765	Web	active-response/bin/remove-threat.sh a supprimé la menace située à /ro...	12	100092
Jun 5, 2025 @ 12:10:44.062	Web	VirusTotal: Alert - /root/eicar.com - 66 engines detected this file	12	87105
Jun 5, 2025 @ 12:10:11.061	Web	active-response/bin/remove-threat.sh a supprimé la menace située à /ro...	12	100092
Jun 5, 2025 @ 12:10:10.622	Web	VirusTotal: Alert - /root/eicar.com - 66 engines detected this file	12	87105

GregLog

doc: https://www.it-connect.fr/tuto-graylog-sur-debian-centraliser-et-analyser-logs/

doc mango: https://www.mongodb.com/docs/manual/installation/

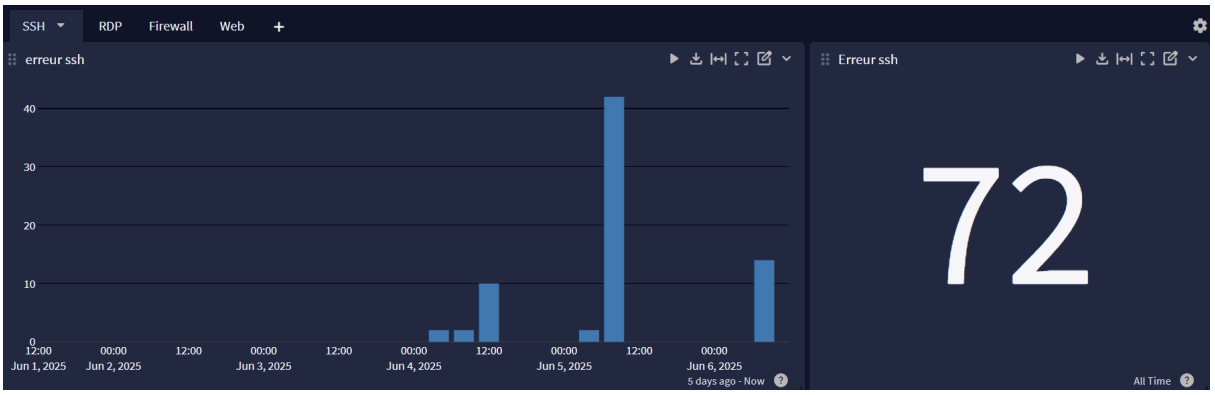
http://192.168.0.22:9000 admin/Kirikou2209!



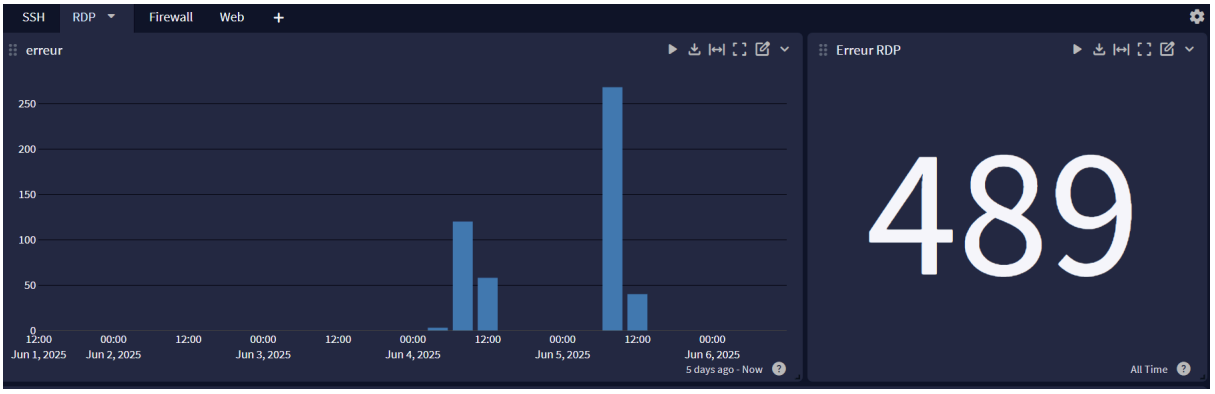
tcp sur port 10514

```
root@Greylog:/home/ais# ss -tnp | grep 10514
ESTAB 0      0      [::ffff:192.168.0.22]:10514 [::ffff:192.168.0.17]:57190 users:(("java",pid=634,fd=355))
```

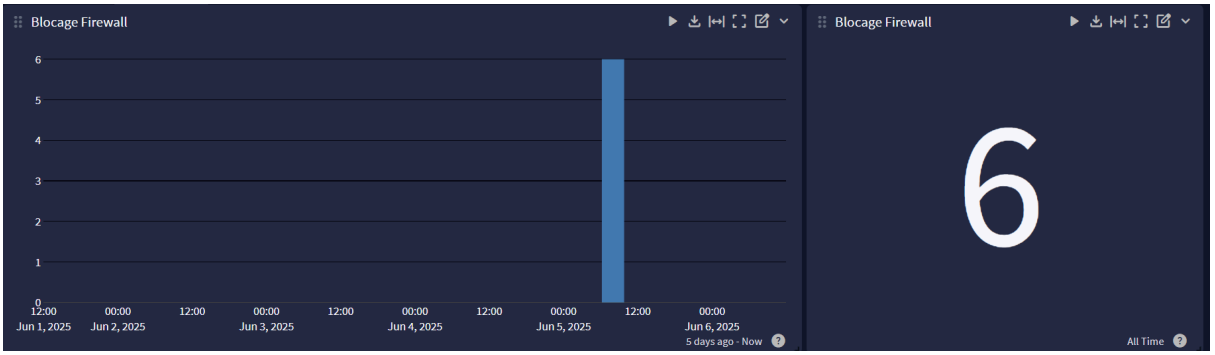
filtre pour voir les connexion ssh echoué: message:Failed password AND application_name:sshd



requête rdp: RDP



filtre pour voir les connexion bloquer par le firewall: message:"BLOCK" OR message:"DENY”



Guacamole

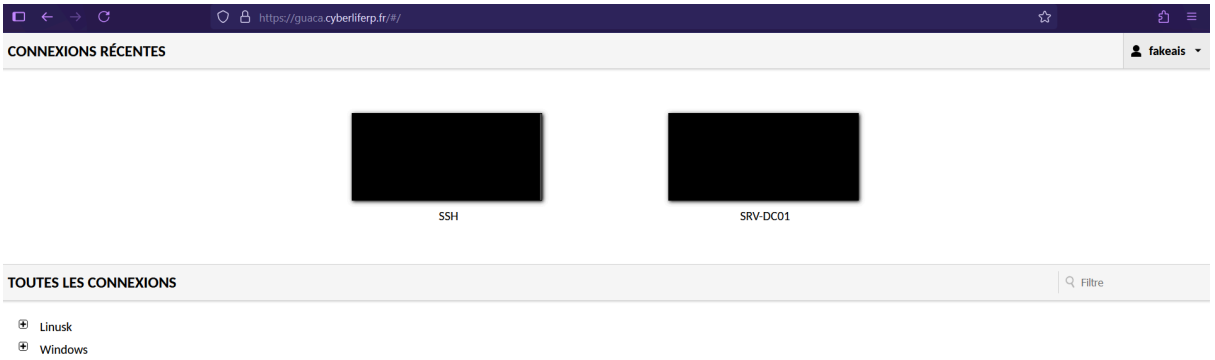
Accès :

User : fakeais

MDP : Kirikou2209!

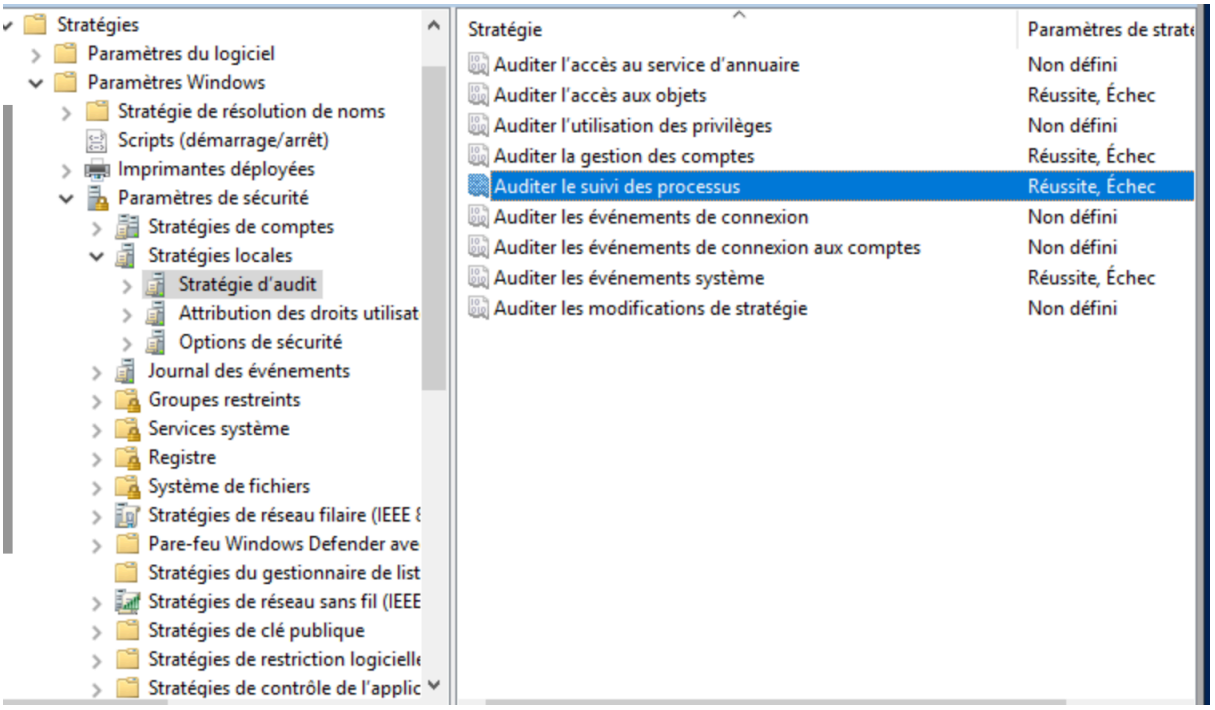
guaca.cyberliferp.fr

https://guaca.cyberliferp.fr/



WINDOWS

Stratégie d'audit Windows Server GPO :



Installation Sysmon via Powershell

Sysmon (System Monitor) est un outil de Microsoft qui enregistre en détail l'activité du système (processus, connexions réseau, modifications de fichiers, etc.) dans les logs Windows. Il sert à la détection des comportements suspects pour les analystes en cybersécurité.

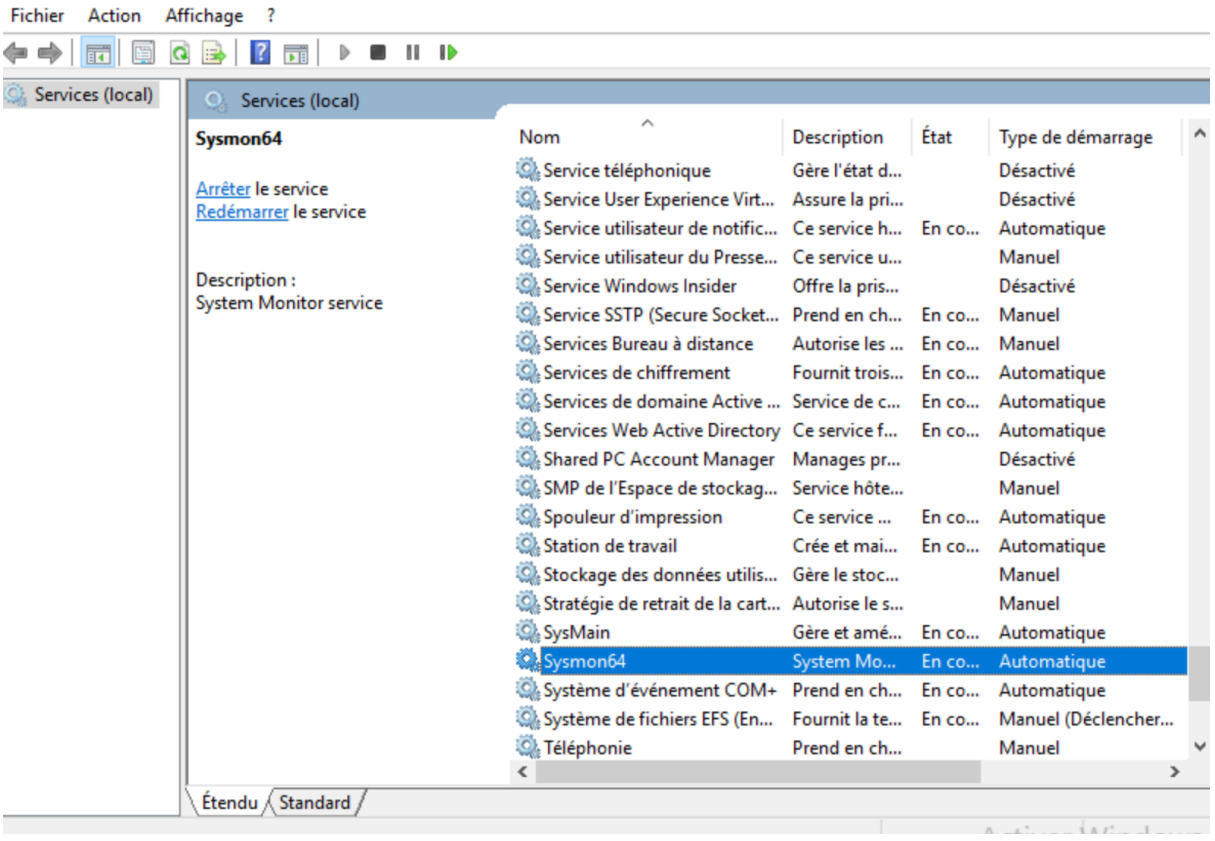
Il s'agit d'un modèle de fichier de configuration Microsoft Sysinternals Sysmon avec un suivi d'événements de haute qualité par défaut.

Le fichier doit constituer un excellent point de départ pour la surveillance des modifications du système dans un package autonome et accessible. Cette

configuration et ces résultats devraient vous donner une bonne idée de ce qui est possible pour Sysmon. Notez que cela ne suit pas des éléments tels que l'authentification et d'autres événements Windows qui sont également essentiels pour l'enquête sur les incidents.

Fichier à télécharger : GitHub - SwiftOnSecurity/sysmon-config : modèle de fichier de configuration Sysmon avec suivi des événements de haute qualité par défaut

```
PS C:\Users\Administrateur\downloads\sysmon> sysmon64.exe -accepteula -i sysmonconfig-export.xml

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\Administrateur\downloads\sysmon>
```

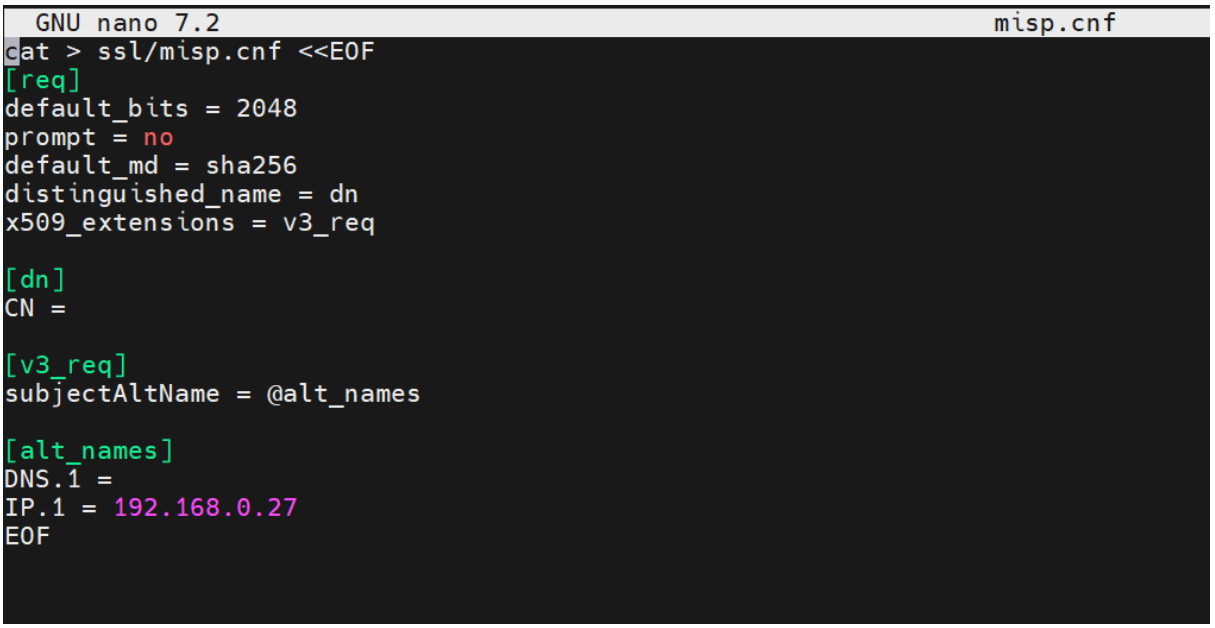


MISP

`git clone https://github.com/MISP/misp-docker`

`mkdir -p ~/misp-docker/ssl && cd ~/misp-docker`

`cat > ssl/misp.cnf <<EOF`

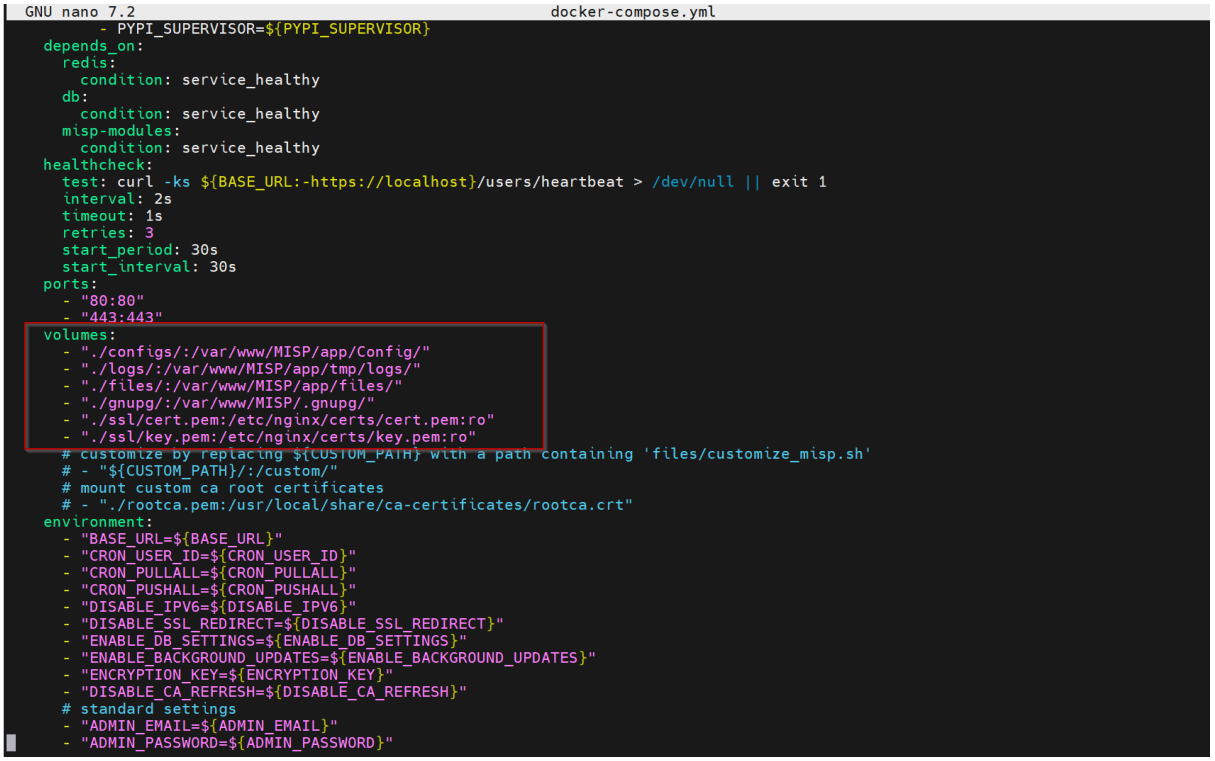



```
openssl req -x509 -nodes -days 365 \
  -newkey rsa:4096 \
  -keyout ssl/key.pem \
  -out ssl/cert.pem \
  -config ssl/misp.cnf
```

On ajoute le FQDN dans le fichier template.env :

`BASE_URL= https://misp.doma.in`

Dans le fichier docker-compose.yml, on ajoute les lignes suivantes : *

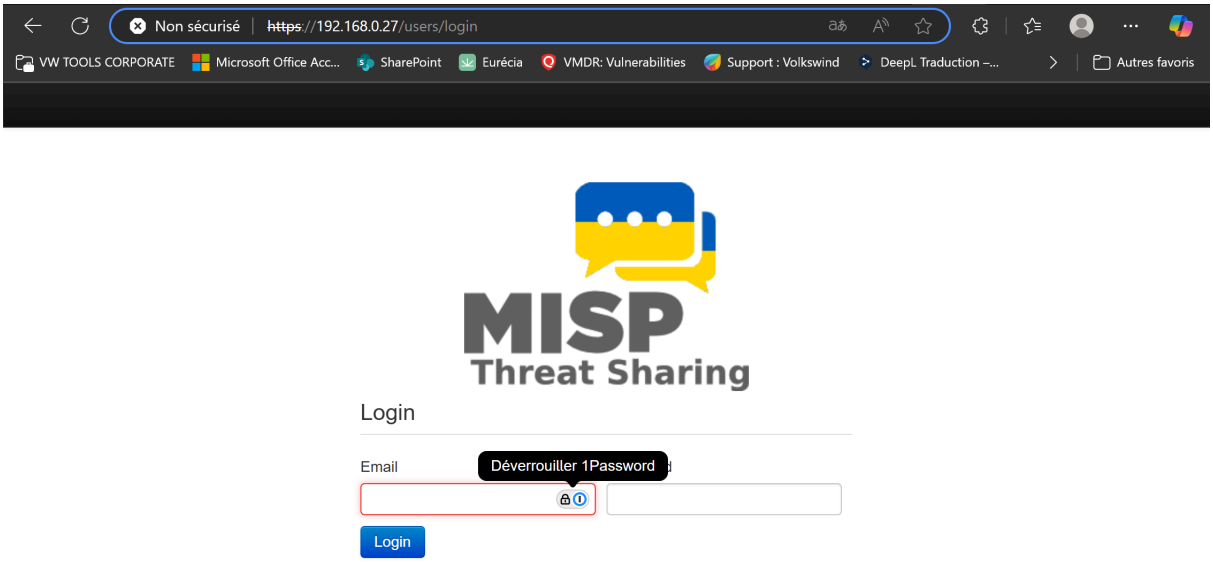


Rebuild complet :

docker compose down
docker compose build
docker compose up -d

Interface MISP:

Email : admin@admin.test
Mot de passe : admin



Autosigné avec misp.doma.in

Émis pour

Nom commun (CN)	misp.doma.in
Organisation (O)	<Ne fait pas partie du certificat>
Unité d'organisation (UO)	<Ne fait pas partie du certificat>

Émis par

Nom commun (CN)	misp.doma.in
Organisation (O)	<Ne fait pas partie du certificat>
Unité d'organisation (UO)	<Ne fait pas partie du certificat>

Période de validité

Date d'émission	jeudi 5 juin 2025 à 13:44:28
Date d'expiration	vendredi 5 juin 2026 à 13:44:28

Empreintes digitales SHA-256

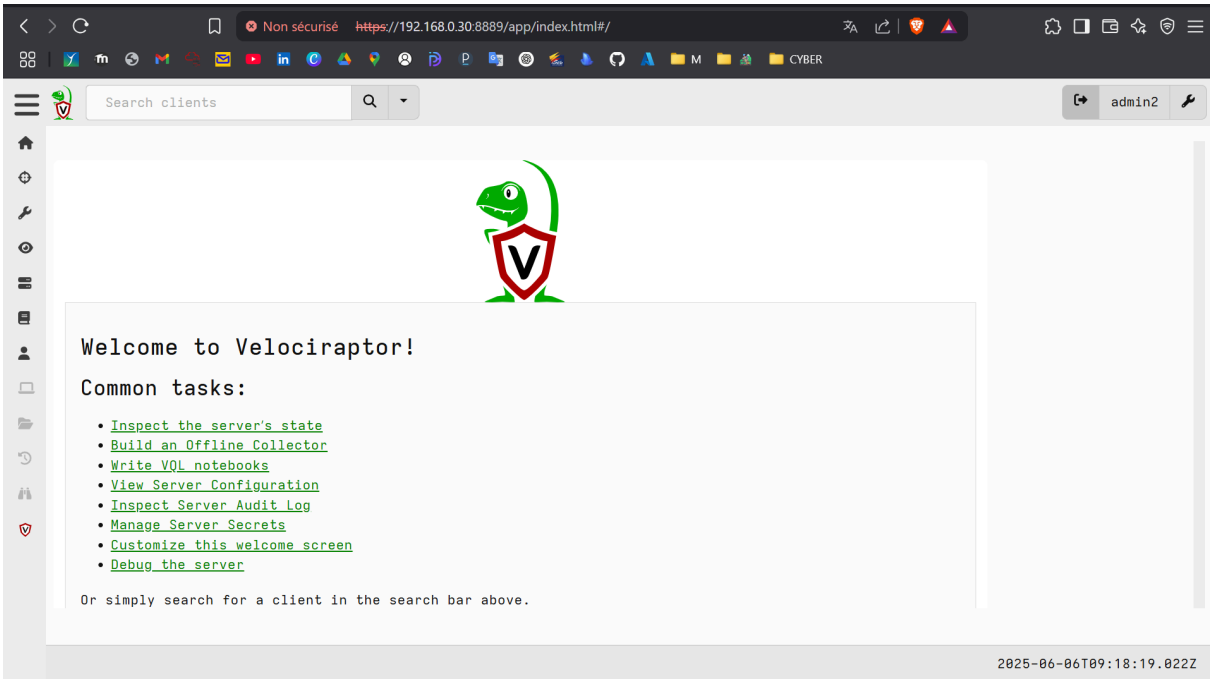
Certificat	06fd7bbc8d0b593f38c20b423d8c5ced634974415a899f5089ff635c96c1a97f
Clé publique	628e417e8dd341b6faa032548aeb46b43a205497755bdc66868572159d121dd7

Velociraptor

Velociraptor est un outil avancé de forensic et de réponse aux incidents avec visibilité sur les endpoints.

https://192.168.0.30:8889/app/index.html admin2/Kirikou2209!

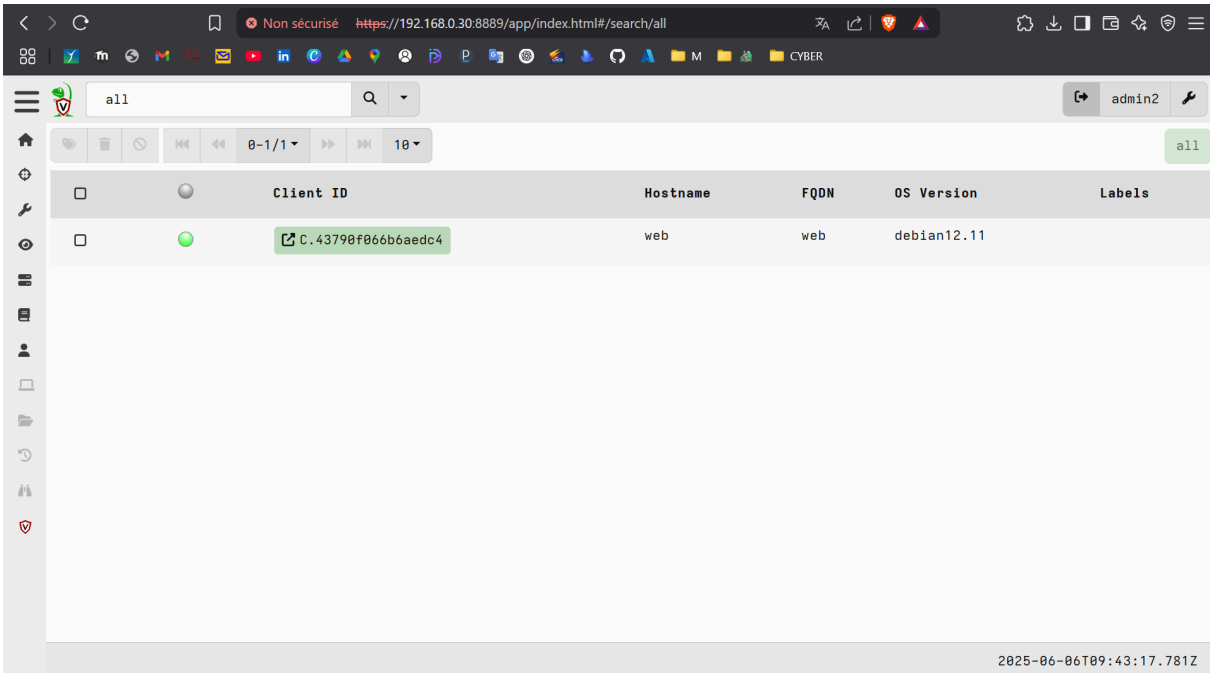
Pour déploiement du serveur : https://docs.velociraptor.app/docs/deployment/



Clients

Pour déploiement des clients : https://docs.velociraptor.app/docs/deployment/clients/

Les agents remontent :


Non sécurisé
https://192.168.0.30:8889/app/index.html#/search/all
CYBER
all
admin2
0-1/1
10
all
Client ID
Hostname
FQDN
OS Version
Labels
C.43790f066b6aedc4
web
web
debian12.11
2025-06-06T09:43:17.781Z