DATABASE DONNÉES

TABLE AGENTS:

agent_code : Eclair
name : Sebastien DEMEY
password : arcraiddersGEEKos
team_id : 1
contact : +33 3 46 70 98 02

agent_code : Elmusico
name : Alexandre ESTRABAUD
password : rammstein4ever
team_id : 3
contact : +33 3 12 05 92 07

agent_code : QWERTY4GNS
name : Axel GINEPRO
password : jaimelalingerie
team_id : 2
contact : +33 3 10 04 82 04

agent_code : WaffleMan
name : Valentin SCHELLENS
password : brusselsansX
team_id : 1
contact : +32 1 17 55 42 97

agent_code : Soldelavie
name : Solène BRANLY
password : cestchaudlahaut
team_id : 2
contact : +33 2 87 50 29 19

agent_code : NoFitness
name : Audrey FERRERE
password : Vivelamuscu
team_id : 3
contact : +32 5 27 85 12 97

TABLE CLIENTS:

client code : 01
name : Maria Dubois
contact : +33 5 40 98 78 50

client code : 02
name : Nicolas Frank Strudel
contact : nfstrudel@gmail.com

client code : 03
name : Geral Nolan Smith
contact : gnsmith3@gmail.com

TABLE INVESTIGATIONS:

title : Vol de pâtisserie
investigation_code : 001
description : Monsieur S, propriétaire d'une pâtisserie, se fait voler régulièrement des éclairs au chocolat.
status : Opened
creation_date : 20240810
client_id : 02
team_id: 1

title : La conception secrète
investigation_code : 002
description : Madame D pense qu'une entreprise de lingerie concurrente à la sienne a volé le patron de l'ensemble principal de sa nouvelle collection en peau d'alligator nourri au grain végétal.
status : Freezed
creation_date : 20201029
client_id : 01
team_id: 2

title : Le divorce à 1 million
investigation_code : 003
description : Monsieur S souhaite trouver des preuves compromettantes sur sa femme afin de pouvoir divorcer et récupérer tout le capital financier.
status : Closed
creation_date : 20260103
client_id : 03
team_id: 3

REGLES WAZUH:

Emplacement du fichier recommandé :
`/var/ossec/etc/rules/local_rules.xml`

AD :

-CRITIQUE:

Objectifs : Détecter **Golden Ticket, DCSync,** Création de comptes admins, Désactivation sécurité

```
<group name="windows,ad,security">

  <!-- Ajout à Domain Admins -->
  <rule id="100100" level="15">
    <if_sid>60103</if_sid>
    <field name="win.eventdata.TargetUserName">Domain Admins</field>
    <description>CRITICAL - User added to Domain Admins</description>
    <mitre>T1098</mitre>
  </rule>

  <!-- DCSync -->
  <rule id="100101" level="15">
    <if_sid>60102</if_sid>
    <match>Replicating Directory Changes</match>
    <description>CRITICAL - Possible DCSync attack</description>
    <mitre>T1003</mitre>
  </rule>

  <!-- Désactivation audit / logs -->
  <rule id="100102" level="14">
    <match>audit policy change</match>
    <description>HIGH - Audit policy modified on Domain Controller</description>
    <mitre>T1562</mitre>
  </rule>

</group>
```

-tentative de suppression des logs

-MEDIUM:

creation compte utilisateur, groupes

DB:

-Tentatives de Brute Force SQL : Détecter plus de 5 échecs de connexion en moins de 2 minutes sur le port 3306.

<rule id="100401" level="10" frequency="5" timeframe="120">

<if_matched_sid>501</if_matched_sid> <description>Detechtive: Brute force attack on Database detected</description>

<mitre>T1110</mitre>

</rule>

-Accès depuis un VLAN non autorisé : Alerte si une connexion à la DB provient d'un autre réseau que celui des serveurs (VLAN 10) ou du poste d'administration.

-Modification des privilèges : Surveiller les logs MariaDB/MySQL pour toute commande `GRANT` ou modification de la table `user`.

<group name="database,security">

<!-- Dump SQL -->
<rule id="100400" level="14">
<match>mysqldump|pg_dump|BACKUP DATABASE</match>
<description>HIGH - Database dump detected</description>
<mitre>T1005</mitre>
</rule>

</group>

Astuce : combiner avec **FIM sur les fichiers .bak / .sql**

GENERAL

-Tentative d'accès par un VLAN non autorisé, mouvement-latéral
<group name="network,lateral_movement">

<!-- Scan réseau -->
<rule id="100600" level="13">
<match>nmap|masscan</match>

```
    <description>HIGH - Network scanning detected</description>
    <mitre>T1046</mitre>
  </rule>

</group>
```

-detection de scan nmap

-Utilisation d'outils de hacking : Wazuh possède des signatures pour détecter l'exécution de `mimikatz`, `powersploit` ou `hydra` sur les machines cibles.

-Anomalies PfSense : Corréler les logs de ton PfSense (192.168.10.1) avec Wazuh pour détecter si une IP tente de franchir les règles de pare-feu entre le VLAN 30 (Monitoring) et le VLAN 10 (Serveurs).

WORKSTATION

-Tentative de Connexion / Accès Workstations
Objectifs : LSASS dump, Pass-the-hash, Outils offensifs.

```
<group name="windows,workstation,attack">

  <!-- Dump LSASS -->
  <rule id="100200" level="15">
    <match>lsass.exe</match>
    <description>CRITICAL - LSASS access detected</description>
    <mitre>T1003</mitre>
  </rule>

  <!-- Outils hacking -->
  <rule id="100201" level="14">
    <match>mimikatz|rubeus|psexec|secretsdump</match>
    <description>HIGH - Credential dumping tool detected</description>
    <mitre>T1003</mitre>
  </rule>

</group>
```

FILESERVER :

Objectif : Détection chiffrement massif, Suppression VSS, Accès anormal/surveillance

```
<group name="windows,fileserver,ransomware">

  <!-- Suppression shadow copies -->
  <rule id="100300" level="15">
    <match>vssadmin delete shadows</match>
    <description>CRITICAL - Shadow copies deleted (ransomware behavior)</description>
    <mitre>T1490</mitre>
  </rule>

  <!-- Suppression massive -->
  <rule id="100301" level="13">
    <match>del /s|Remove-Item -Recurse</match>
    <description>HIGH - Mass file deletion detected</description>
    <mitre>T1485</mitre>
  </rule>

</group>
```

WEBSERVER:

Objectifs : Webshell; SQLi / RCE; Upload malveillant

```
<group name="web,attack">

  <!-- Webshell -->
  <rule id="100500" level="15">
    <match>cmd.exe|powershell.exe</match>
    <description>CRITICAL - Possible webshell execution</description>
    <mitre>T1505</mitre>
  </rule>

  <!-- SQL Injection -->
  <rule id="100501" level="12">
    <match>union select|or 1=1|sleep\(|benchmark\(|xp_cmdshell</match>
    <description>MEDIUM - Possible SQL Injection attempt</description>
    <mitre>T1190</mitre>
  </rule>

</group>
```

FIM (Files Integrity Monitoring)

```
<syscheck>
  <directories realtime="yes">C:\Windows\System32</directories>
</syscheck>
```

VERSION CORRIGEE

Catégorie	ID de règle	Niveau	Menace ciblée
Active Directory	**100100**	**15**	**Ajout d'un membre dans "Domain Admins"**
Active Directory	**100101**	**15**	**Attaque DCSync (Réplication suspecte)**
Active Directory	**100102**	**15**	**Ajout d'utilisateur dans un groupe Admin**
Sécurité Système	**100200**	**15**	**Dump de mémoire LSASS (via Sysmon)**
Sécurité Système	**100201**	**15**	**Exécution de commande via LSASS**
Ransomware	**100300**	**15**	**Suppression des Shadow Copies (sauvegardes)**

Ransomware	**100301**	**13**	**Suppression massive de fichiers sur FileServer**
Database	**100400**	**14**	**Dump de base de données (extraction)**
Database	**100401**	**12**	**Brute Force SQL (Fréquence de 5 échecs)**
Web Server	**100500**	**15**	**Exécution de Webshell (cmd.exe, bash)**
Web Server	**100501**	**12**	**Tentative d'Injection SQL**
Reconnaissance	**100600**	**13**	**Détection d'outils de scan (Nmap, Masscan)**
Mouvement Latéral	**100601**	**12**	**Blocage Firewall PfSense entre VLANs**
Mouvement Latéral	**100602**	**10**	**Scan de ports**
Brute force sur pfsense	**100700**	**12**	**Détecter les échecs de connexion répétés sur l'interface web de PfSense.**

Configuration des Règles (/var/ossec/etc/rules/local_rules.xml)

1. Active Directory & Windows (Priorité Critique)

L'objectif est de surveiller les modifications de privilèges et les attaques sur la mémoire (LSASS).

XML

```
<group name="windows,ad,security">

  <rule id="100100" level="15">
    <if_sid>60103</if_sid>
    <field name="win.eventdata.TargetUserName">Domain Admins</field>
    <description>CRITICAL - Utilisateur ajouté au groupe Domain
Admins</description>
    <mitre>T1098</mitre>
  </rule>

  <rule id="100101" level="15">
    <if_sid>60102</if_sid>
    <match>Replicating Directory Changes</match>
    <description>CRITICAL - Tentative d'attaque DCSync (Réplication AD non
autorisée)</description>
    <mitre>T1003</mitre>
  </rule>

<rule id="100102" level="15">
  <if_sid>60103</if_sid>
  <regex type="pcre2">TargetUserName=(Administrators)</regex>
  <description>CRITICAL - Utilisateur ajouté à un groupe AD sensible</description>
  <mitre>T1098</mitre>
</rule>

  <rule id="100200" level="15">
    <if_sid>61612</if_sid> <field
name="win.eventdata.TargetImage">C:\\Windows\\System32\\lsass.exe</field>
    <description>CRITICAL - Accès suspect au processus LSASS (Tentative de
Dump)</description>
    <mitre>T1003</mitre>
  </rule>
```

```
<rule id="100201" level="15">
  <if_sid>61612</if_sid>
  <field name="win.eventdata.TargetImage">C:\\Windows\\System32\\lsass.exe</field>
  <regex
type="pcre2">ParentImage=(?:.*\\cmd\.exe|.*\\powershell\.exe|.*\\wscript\.exe)</regex>
  <description>CRITICAL - Accès suspect à LSASS depuis un processus parent
inhabituel</description>
  <mitre>T1003</mitre>
</rule>
```

2. Base de Données (MariaDB/MySQL)

On surveille ici l'extraction de données et les accès réseaux suspects.

XML

```
<group name="database,security">

  <rule id="100400" level="14">
    <match>mysqldump|pg_dump|BACKUP DATABASE</match>
    <description>HIGH - Export de la base de données détecté (Dump)</description>
    <mitre>T1005</mitre>
  </rule>

  <rule id="100401" level="12" frequency="5" timeframe="120">
    <if_matched_sid>501</if_matched_sid> <description>HIGH - Attaque Brute Force
sur la Database</description>
    <mitre>T1110</mitre>
  </rule>

</group>

<rule id="100403" level="14">
  <match>LOAD_FILE|INTO OUTFILE|INTO DUMPFILE|UNION SELECT</match>
  <description>HIGH - Requête SQL dangereuse détectée (exfiltration
possible)</description>
  <mitre>T1190</mitre>
</rule>
```

3. File Server & Ransomware

Surveillance de la destruction des sauvegardes (Shadow Copies) et du sabotage de fichiers.

XML

```
<group name="windows,fileserver,ransomware">
```

```
  <rule id="100300" level="15">
    <match>vssadmin delete shadows|wmic shadowcopy delete</match>
    <description>CRITICAL - Suppression des Shadow Copies (Comportement
Ransomware)</description>
    <mitre>T1490</mitre>
  </rule>

  <rule id="100301" level="13" frequency="10" timeframe="60">
    <match>del /s|Remove-Item</match>
    <description>HIGH - Suppression massive de fichiers détectée</description>
    <mitre>T1485</mitre>
  </rule>

</group>
```

4. Web Server & Attaques Applicatives

Détection des injections SQL et des portes dérobées (Webshells).

XML

```
<group name="web,attack">

  <rule id="100500" level="15">
    <match>cmd.exe|powershell.exe|/bin/bash|/bin/sh</match>
    <description>CRITICAL - Webshell suspect détecté sur le serveur
Web</description>
    <mitre>T1505</mitre>
  </rule>

  <rule id="100501" level="12">
    <match>union select|or 1=1|sleep\(|xp_cmdshell</match>
    <description>HIGH - Tentative d'Injection SQL détectée</description>
    <mitre>T1190</mitre>
  </rule>

</group>
```

Analyse réseau PfSense

Pour que les alertes "VLAN non autorisé" fonctionnent, tu dois configurer ton PfSense pour envoyer ses logs de blocage à Wazuh (via Syslog).

```
<rule id="100601" level="12">
  <if_sid>60000</if_sid>
  <match>BLOCK</match>
  <field name="source.ip">IP_KALI</field>
```

```
  <field name="destination.vlan">10</field>
  <description>HIGH - Trafic bloqué de Kali vers le VLAN Serveurs (VLAN 10)</description>
  <mitre>T1048</mitre>
</rule>

<rule id="100602" level="10" frequency="20" timeframe="60">
  <match>portscan|SYN Scan|Nmap</match>
  <description>MEDIUM - Scan de ports détecté sur le réseau</description>
  <mitre>T1046</mitre>
</rule>



  <rule id="100700" level="12" frequency="5" timeframe="120">

    <if_matched_sid>5402</if_matched_sid> <match>webConfigurator authentication
error</match>

    <description>Detechtive : Tentative de Brute Force détectée sur l'interface de gestion
PfSense</description>

    <mitre>

      <id>T1110</id>

    </mitre>

  </rule>
```

Configuration FIM (Cible Précise)

Ne surveille pas tout `System32`, cela ferait ramer ta machine. Préfère ces dossiers :

XML

```
<syscheck>
  <directories realtime="yes"
check_all="yes">C:\Windows\System32\drivers\etc</directories>
  <directories realtime="yes"
check_all="yes">C:\Windows\System32\config\</directories>
  <directories realtime="yes" check_all="yes">C:\inetpub\</directories>
  <ignore type="sregex">\.tmp$|\.log$|\.bak$</ignore>
</syscheck>
```

Blocage

1. **Bloquer une ip après 5 essais de connexion en ssh**

```
<group name="sshd,authentication,">
  <rule id="100700" level="10" frequency="5" timeframe="60">
    <if_matched_sid>5716</if_matched_sid> <!-- ID de l'alerte SSH failed login -->
    <same_source_ip />
    <description>HIGH - 5 échecs de connexion SSH depuis la même IP (possible brute
force)</description>
    <mitre>T1110</mitre>
  </rule>
</group>
```

- **puis dans Pfsense**

```
#!/bin/bash
LOCAL=`dirname $0`
IP=$1

# Envoi d'une commande à PfSense pour bloquer l'IP (exemple avec SSH)
ssh admin@IP_PFSENSE "pfctl -t blocked_ips -T add $IP"
logger -t wazuh "IP bloquée : $IP"
```

- **et dans var/ossec/etc/ossec.conf**

```
<ossec_config>
  <command>
    <name>block_ip</name>
    <executable>/var/ossec/active-response/bin/block_ip.sh</executable>
    <timeout_allowed>yes</timeout_allowed>
  </command>

  <active-response>
    <command>block_ip</command>
    <location>local</location>
    <rules_id>100700</rules_id> <!-- ID de la règle déclenchante -->
    <timeout>600</timeout> <!-- Durée du blocage (en secondes) -->
  </active-response>
</ossec_config>
```

Bloquer une ip après brute force sur la DB

```
<rule id="100701" level="12" frequency="5" timeframe="120">
  <if_matched_sid>501</if_matched_sid> <!-- ID de l'alerte de connexion échouée -->
  <same_source_ip />
  <description>HIGH - 5 échecs de connexion à la base de données depuis la même
IP</description>
  <mitre>T1110</mitre>
</rule>
```

- dans ossec.conf

```
<active-response>
  <command>block_ip</command>
  <location>local</location>
  <rules_id>100701</rules_id>
  <timeout>1800</timeout> <!-- 30 minutes -->
</active-response>
```

Bloquer une ip après randsomewar

```
<rule id="100702" level="15" frequency="3" timeframe="30">
  <if_matched_sid>100301</if_matched_sid> <!-- ID de la règle de suppression massive -->
  <same_source_ip />
  <description>CRITICAL - Suppression massive de fichiers répétée
(ransomware)</description>
  <mitre>T1485</mitre>
</rule>
```

- dans ossec.conf

```
<active-response>
  <command>block_ip</command>
  <location>local</location>
  <rules_id>100702</rules_id>
  <timeout>3600</timeout> <!-- 1 heure -->
</active-response>
```

Bloquer l'accès après un Scan de Ports (Reconnaissance)

Avant d'attaquer la DB ou l'AD, votre Kali va forcément scanner le réseau. Si vous bloquez l'IP dès le scan, l'attaque s'arrête avant même d'avoir commencé.

La Règle (ID 100703) :
XML

```
<rule id="100703" level="10" frequency="15" timeframe="30">
  <if_matched_sid>100602</if_matched_sid> <same_source_ip />
  <description>ATTACK - Scan de ports intensif détecté : Blocage immédiat</description>
</rule>
```

Action : Ajoutez cette règle dans votre `ossec.conf` avec un timeout de **3600** (1 heure). C'est radical contre la phase de reconnaissance.

Isoler une machine après un vol de mot de passe (LSASS)

Si la règle **100200** (accès à LSASS) se déclenche sur une Workstation ou l'AD, il ne faut pas seulement bloquer une IP, il faut **isoler la machine** du réseau.

Active Response (ossec.conf) :
XML
<active-response>
  <command>block_ip</command>
  <location>local</location>
  <rules_id>100200</rules_id> <timeout>0</timeout> </active-response>

Bloquer les Webshells (Web-server):

Si larègle **100500** détecte un Webshell (utilisation de `cmd.exe` par le serveur web), l'attaquant a déjà un pied dans la place.

La Règle (ID 100704) :
XML
<rule id="100704" level="15">
  <if_sid>100500</if_sid>
  <description>CRITICAL - Exécution de Webshell : Blocage de l'IP source</description>
</rule>