Rapport Final : SOC Use Cases Basés sur MITRE ATT&CK

Realiser par :

CHATER AHMED

DAOUDA DAVID COULIBALY

Introduction

La sécurisation d'un environnement informatique passe par la détection proactive des comportements malveillants. Ce projet s'inscrit dans cette démarche en utilisant le serveur Wazuh, une machine virtuelle Ubuntu, et une machine fixe Windows comme agent, pour configurer et valider des règles de détection basées sur les TTPs (Tactics, Techniques, and Procedures) décrits dans le framework MITRE ATT&CK.

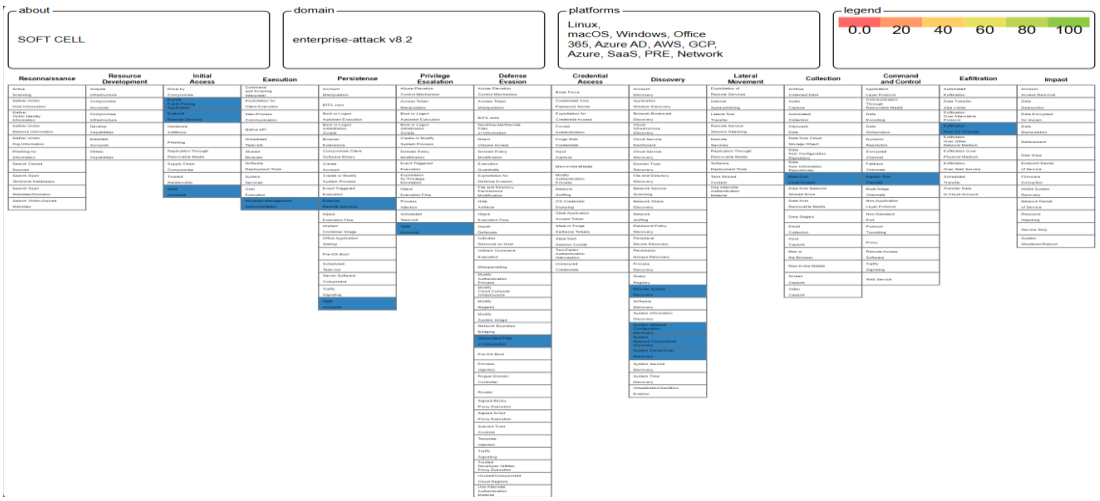
L'objectif principal est d'améliorer les capacités de détection et de réaction d'un SOC, en intégrant des règles adaptées à des scénarios réels d'attaques, notamment ceux observés dans l'opération *Soft Cell*.

---

1. Identification et Mapping des TTPs

Les TTPs analysés proviennent du rapport de l'opération *Soft Cell* et du cadre MITRE ATT&CK. Ils couvrent les phases d'attaque suivantes :

1. **Initial Access** : Techniques permettant aux attaquants de pénétrer dans le système.
2. **Persistence** : Méthodes pour maintenir un accès prolongé.
3. **Credential Dumping** : Extraction d'informations d'identification.
4. **Lateral Movement** : Déplacement vers d'autres systèmes.
5. **Exfiltration** : Transfert des données volées.



TTP	ID MITRE ATT&CK	OBJECTIF DE DETECTION	METHODE DE DETECTION
Web Shell	T1505.003	Identifier l'utilisation de Web Shells	Rechercher des logs IIS anormaux ou des commandes exécutées par `w3wp.exe`.
Archive Collected Data: Archive via Utility	T1560.001	Détecter la compression et l'archivage de données volées	Surveiller l'utilisation de WinRAR ou d'autres outils similaires dans les logs système.
Command and Scripting Interpreter: PowerShell	T1059.001	Identifier les scripts PowerShell suspects	Détecter des commandes PowerShell encodées ou des schémas d'exécution inhabituels.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Surveiller les commandes exécutées via le shell Windows	Analyser les commandes dans les journaux Windows Event ID 4688.
Create Account: Domain Account	T1136.002	Détecter la création de comptes de domaine non autorisés	Surveiller les événements Windows Event ID 4720 et 4724.
Data from Local System	T1005	Identifier la collecte de données locales	Détecter les accès répétés au registre et aux fichiers sensibles.
Data Staged: Local Data Staging	T1074.001	Surveiller les fichiers compressés ou archivés avant exfiltration	Détecter l'utilisation inhabituelle de la Corbeille pour stocker des fichiers compressés.
Exfiltration Over C2 Channel	T1041	Identifier les communications malveillantes avec les serveurs C2	Surveiller les connexions sortantes vers des adresses IP ou des noms DNS suspects.
Exploit Public-Facing Application	T1190	Détecter l'exploitation des applications publiques	Surveiller les requêtes inhabituelles dans les journaux des serveurs Web.
External Remote Services	T1133	Détecter les connexions VPN suspectes	Surveiller les connexions VPN non autorisées ou anormales.
Hijack Execution Flow: DLL SideLoading	T1574.002	Identifier l'utilisation de DLL pour l'exécution	Surveiller les chargements DLL inhabituels via les journaux système.
Ingress Tool Transfer	T1105	Détecter le transfert d'outils malveillants	Surveiller les fichiers téléchargés ou transférés via FTP, SMB, ou HTTP.
Masquerading: Rename System Utilities	T1036.003	Détecter les utilitaires système renommés	Identifier des fichiers comme `cmd.exe` avec des noms non standards dans les logs.

Obfuscated Files or Information	T1027	Identifier les fichiers ou scripts obfusqués	Détecter des chaînes encodées ou compressées dans les fichiers exécutés.
Software Packing	T1027.002	Identifier les payloads packés	Analyser les binaires exécutés avec des signatures de packers connus.
OS Credential Dumping: LSASS Memory	T1003.001	Identifier le dumping de la mémoire LSASS	Surveiller les accès à `lsass.exe` ou les appels à `MiniDump` dans les logs système.
Proxy: External Proxy	T1090.002	Détecter les redirections de connexion via proxy	Surveiller les outils comme HTRAN ou les connexions réseau suspectes.
Remote System Discovery	T1018	Identifier les scans réseau	Surveiller l'utilisation de `nbtscan` ou `ping` dans les journaux réseau.
Scheduled Task/Job: Scheduled Task	T1053.005	Détecter la création de tâches planifiées	Analyser les événements Windows liés aux tâches planifiées (Event ID 4698).
System Network Configuration Discovery	T1016	Surveiller la collecte d'informations réseau	Identifier des commandes comme `ipconfig /all` dans les journaux système.
System Network Connections Discovery	T1049	Détecter les analyses des connexions réseau	Surveiller l'utilisation de commandes comme `netstat oan`.
System Owner/User Discovery	T1033	Identifier la collecte d'informations sur les utilisateurs	Surveiller les commandes comme `whoami` ou `query user`.
Use Alternate Authentication Material: Pass the Hash	T1550.002	Détecter les authentifications Pass the Hash	Identifier des tentatives d'authentification avec des hachages dans les journaux.
Valid Accounts	T1078	Identifier l'utilisation de comptes légitimes compromis	Surveiller les connexions via des comptes existants avec des schémas inhabituels.
Windows Management Instrumentation	T1047	Identifier les exécutions ou installations via WMI	Surveiller les événements liés à `wmic.exe` ou aux requêtes WMI dans les journaux.

2. Définition et Configuration des Use Cases

2.1. Use Cases et Objectifs

Les use cases définissent les scénarios spécifiques de détection. Ils incluent les TTPs identifiés, leurs objectifs, et les critères pour générer des alertes.

TTP	ID MITRE ATT&CK	OBJECTIF DE DETECTION	USE CASE
Web Shell	T1505.003	Identifier l'utilisation de Web Shells	**Détection de Web Shells**
Archive Collected Data: Archive via Utility	T1560.001	Détecter la compression et l'archivage de données volées	**Compression de Données Volées**
Command and Scripting Interpreter: PowerShell	T1059.001	Identifier les scripts PowerShell suspects	**Exécution de Scripts PowerShell**
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Surveiller les commandes exécutées via le shell Windows	**Utilisation de la Console de Commandes**
Create Account: Domain Account	T1136.002	Détecter la création de comptes de domaine non autorisés	**Création de Comptes Suspects**
Data from Local System	T1005	Identifier la collecte de données locales	**Dumping de Crédentiels**
Data Staged: Local Data Staging	T1074.001	Surveiller les fichiers compressés ou archivés avant exfiltration	**Déplacement Latéral**
Exfiltration Over C2 Channel	T1041	Identifier les communications malveillantes avec les serveurs C2	**Exfiltration via Serveur C2**
Exploit Public-Facing Application	T1190	Détecter l'exploitation des applications publiques	**Exécution de DLL via Side-Loading**
External Remote Services	T1133	Détecter les connexions VPN suspectes	**Accès VPN Non Autorisé**
Hijack Execution Flow: DLL Side-Loading	T1574.002	Identifier l'utilisation de DLL pour l'exécution	**DLL Side-Loading pour PoisonIvy**
Ingress Tool Transfer	T1105	Détecter le transfert d'outils malveillants	**Transfert d'Outils**

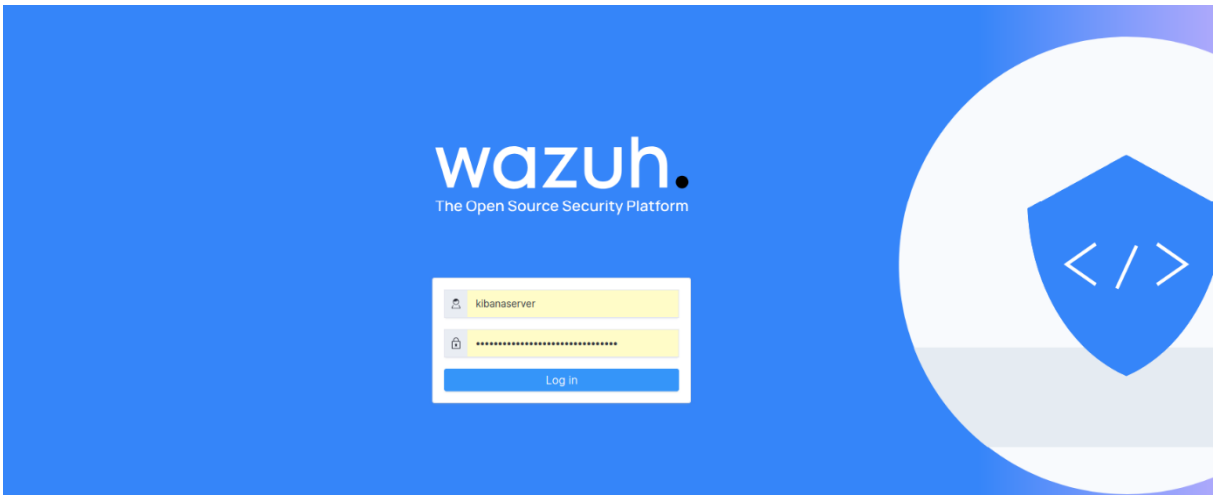
Masquerading: Rename System Utilities	T1036.003	Détecter les utilitaires système renommés	**Renommage d'Utilitaires Système**
Obfuscated Files or Information	T1027	Identifier les fichiers ou scripts obfusqués	**Fichiers Obfusqués**
Software Packing	T1027.002	Identifier les payloads packés	**Payloads Packés ou Modifiés**
OS Credential Dumping: LSASS Memory	T1003.001	Identifier le dumping de la mémoire LSASS	**Dumping de Crédentiels**
Proxy: External Proxy	T1090.002	Détecter les redirections de connexion via proxy	**Utilisation de HTRAN**
Remote System Discovery	T1018	Identifier les scans réseau	**Déplacement Latéral**
Scheduled Task/Job: Scheduled Task	T1053.005	Détecter la création de tâches planifiées	**Détection de Tâches Planifiées Suspectes**
System Network Configuration Discovery	T1016	Surveiller la collecte d'informations réseau	**Découverte de la Configuration Réseau**
System Network Connections Discovery	T1049	Détecter les analyses des connexions réseau	**Analyse des Connexions Réseau**
System Owner/User Discovery	T1033	Identifier la collecte d'informations sur les utilisateurs	**Découverte des Comptes Utilisateurs**
Use Alternate Authentication Material: Pass the Hash	T1550.002	Détecter les authentifications Pass the Hash	**Pass the Hash pour Mouvement Latéral**
Valid Accounts	T1078	Identifier l'utilisation de comptes légitimes compromis	**Utilisation de Comptes Valides**
Windows Management Instrumentation	T1047	Identifier les exécutions ou installations via WMI	**Exécution via WMI**

wazuh.

Loading ...

Configuration de Wazuh

1. **Préparation de l'Infrastructure**



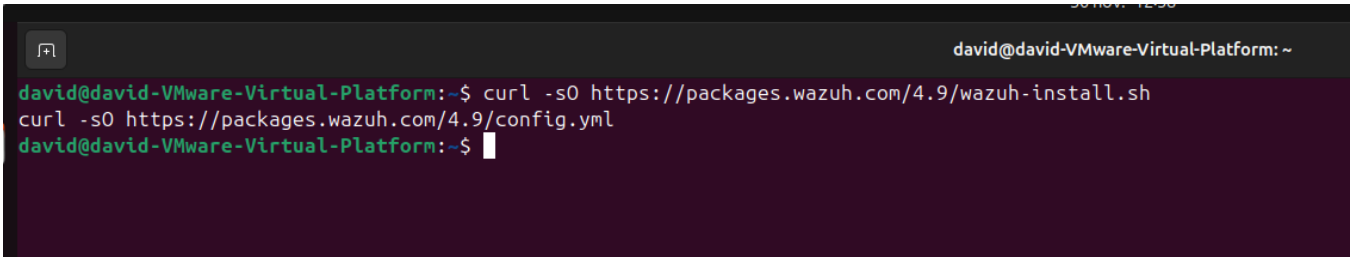
L'environnement se compose de :

- **Serveur Wazuh** : Hébergé sur une machine virtuelle Ubuntu.
- **Agent Windows** : Machine fixe configurée pour envoyer des logs au serveur Wazuh.

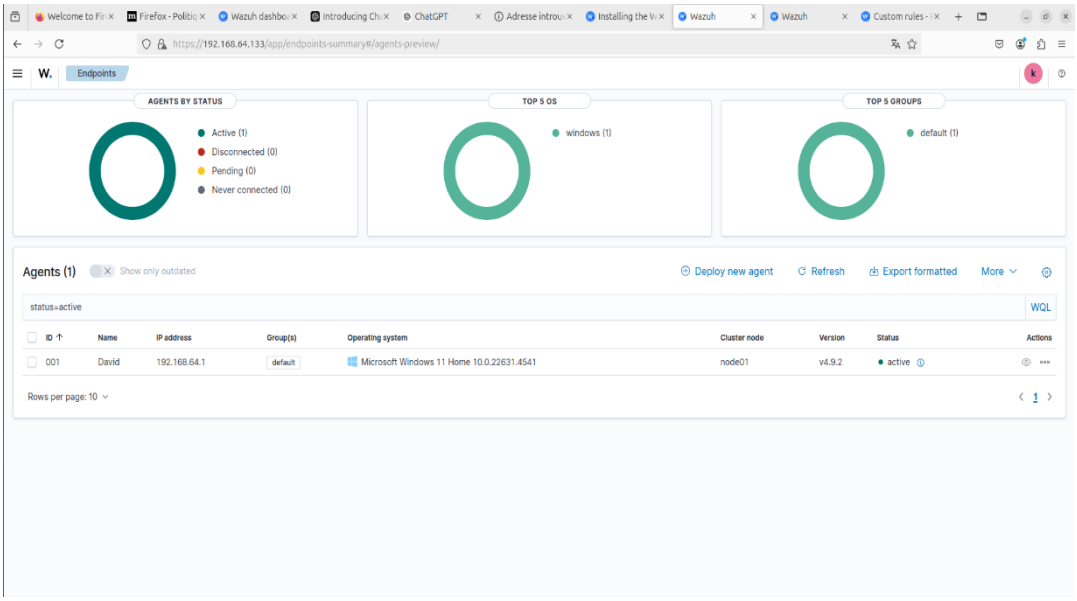
---

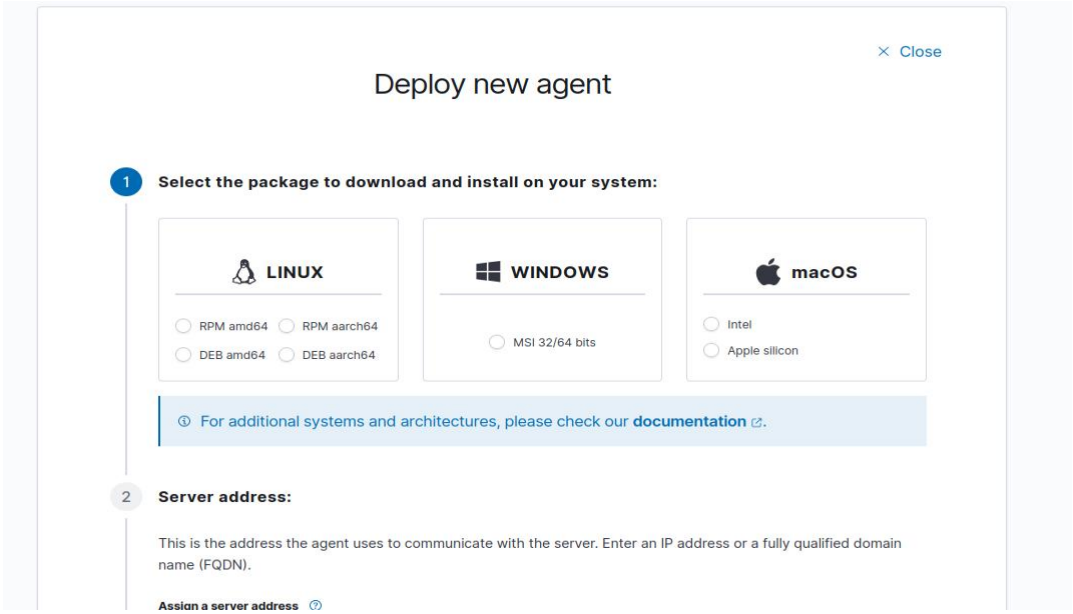
2. Installation et Configuration de Wazuh

2.1. Installation de Wazuh Manager sur Ubuntu



2.2. Installation de Wazuh Agent sur Windows





4 **Run the following commands to download and install the agent:**

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.2-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.64.133'
WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='David'
```

Requirements

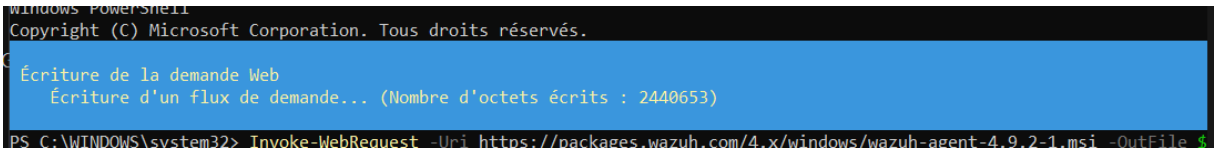
- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

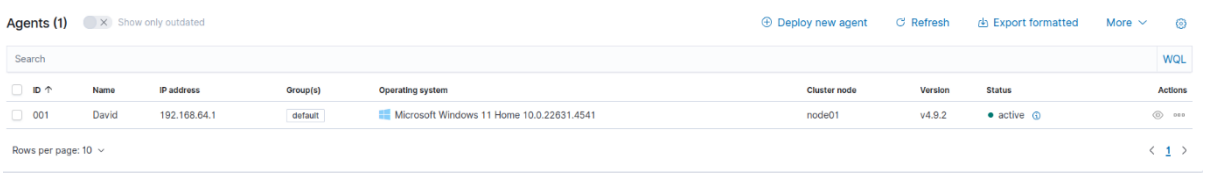
Keep in mind you need to run this command in a Windows PowerShell terminal.

5 **Start the agent:**

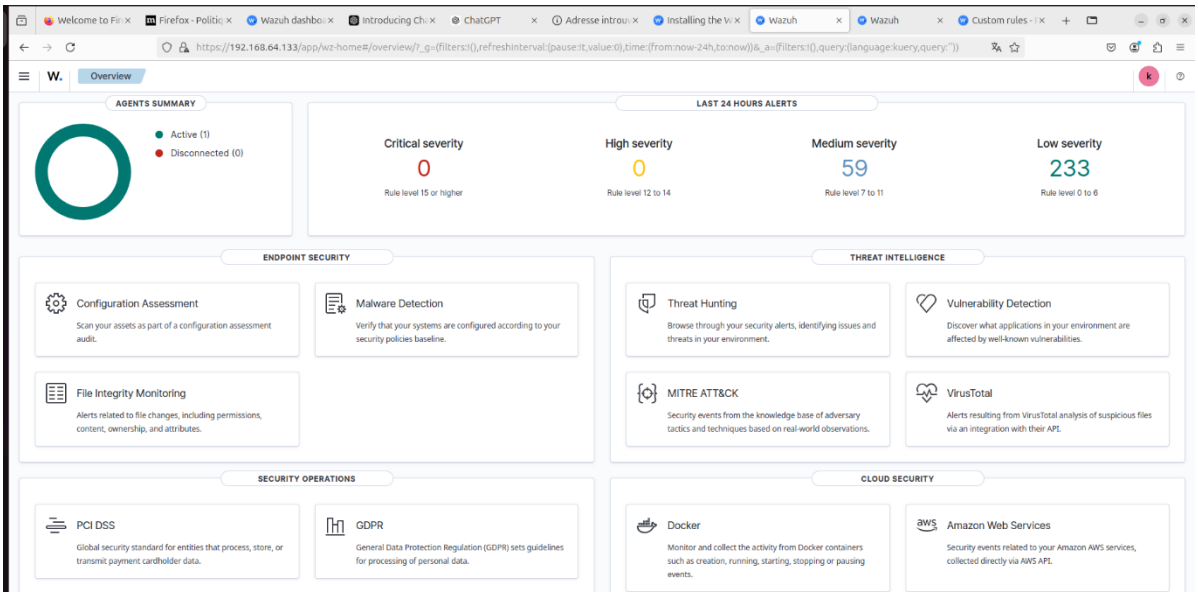
```
NET START WazuhSvc
```

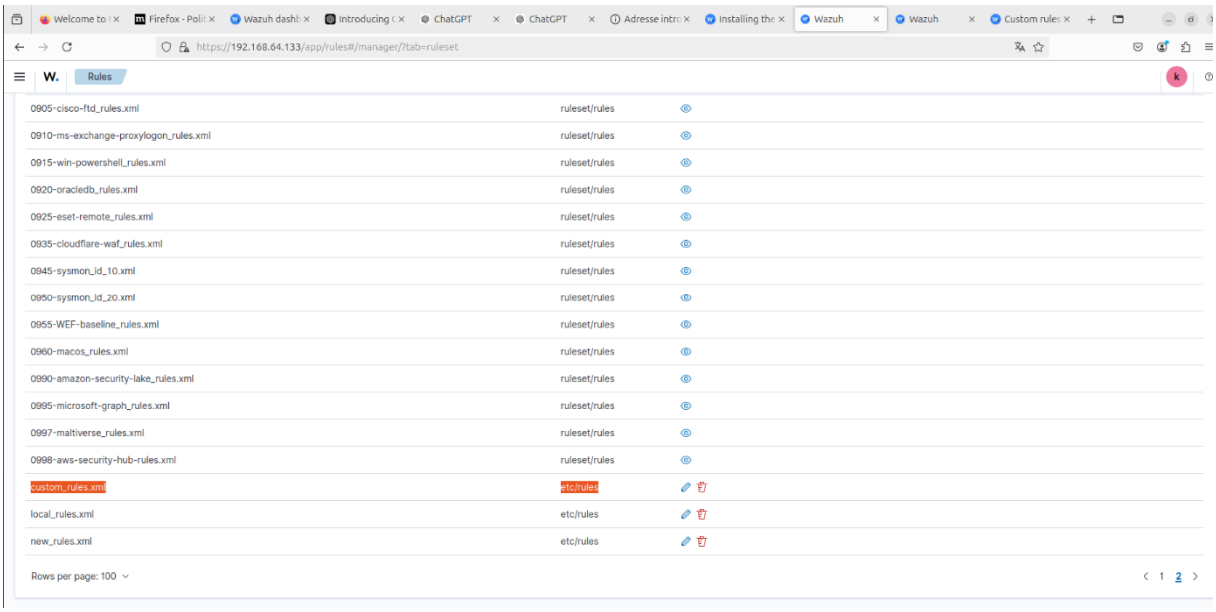
Close





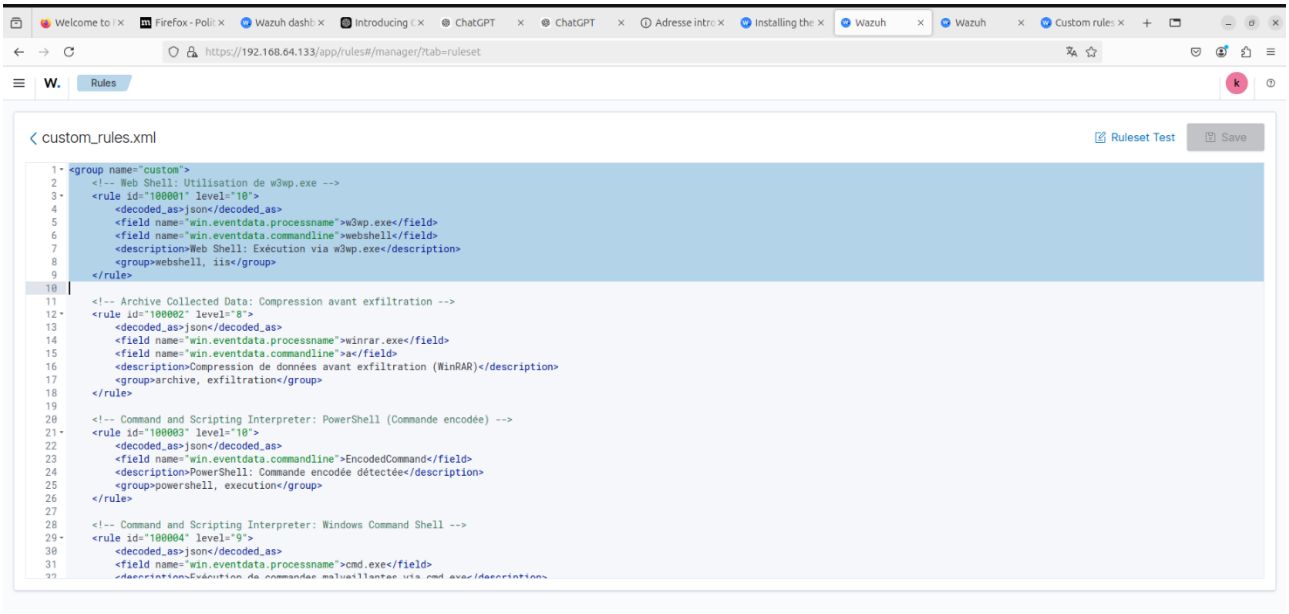
- **Les étapes suivantes décrivent la configuration détaillée de Wazuh.**





2.2. Règles dans Wazuh

Chaque use case est implémenté sous forme de règle dans Wazuh, avec un niveau de criticité adapté. Voici un exemple de configuration pour détecter des scripts PowerShell encodés :




```
<group name="custom">
  <!-- Web Shell: Utilisation de w3wp.exe -->
  <rule id="100001" level="10">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.processname">w3wp.exe</field>
    <field name="win.eventdata.commandline">webshell</field>
    <description>Web Shell: Exécution via w3wp.exe</description>
    <group>webshell, iis</group>
  </rule>

  <!-- Archive Collected Data: Compression avant exfiltration -->
  <rule id="100002" level="8">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.processname">winrar.exe</field>
    <field name="win.eventdata.commandline">a</field>
    <description>Compression de données avant exfiltration (WinRAR)</description>
    <group>archive, exfiltration</group>
  </rule>

  <!-- Command and Scripting Interpreter: PowerShell (Commande encodée) -->
  <rule id="100003" level="10">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.commandline">EncodedCommand</field>
    <description>PowerShell: Commande encodée détectée</description>
    <group>powershell, execution</group>
  </rule>

  <!-- Command and Scripting Interpreter: Windows Command Shell -->
  <rule id="100004" level="9">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.processname">cmd.exe</field>
    <description>Exécution de commandes malveillantes via cmd.exe</description>
    <group>cmd, execution</group>
  </rule>

  <!-- Create Account: Domain Account -->
  <rule id="100005" level="10">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.eventid">4720</field>
    <description>Création de compte de domaine non autorisé</description>
    <group>create_account, domain</group>
  </rule>
```

```
  <!-- Data from Local System: Extraction de données sensibles -->
  <rule id="100006" level="9">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.targetobject">SAM</field>
    <description>Extraction de données sensibles (SAM)</description>
    <group>data_exfiltration, local_system</group>
  </rule>

  <!-- Data Staged: Local Data Staging -->
  <rule id="100007" level="8">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.processname">winrar.exe</field>
    <field name="win.eventdata.commandline">*.* /c</field>
    <description>Préparation de données pour exfiltration (Compression suspecte)</description>
    <group>data_staging, exfiltration</group>
  </rule>

  <!-- Exfiltration Over C2 Channel -->
  <rule id="100008" level="10">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.destinationip">*.*</field>
    <description>Exfiltration de données via canal C2</description>
    <group>c2, exfiltration</group>
  </rule>

  <!-- Exploit Public-Facing Application -->
  <rule id="100009" level="9">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.query">*SQL*</field>
    <description>Exploitation d'application publique (Injection SQL)</description>
    <group>sql_injection, exploit</group>
  </rule>

  <!-- External Remote Services: Connexion VPN suspecte -->
  <rule id="100010" level="9">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.sourceip">*.*</field>
    <field name="win.eventdata.sourceremote">VPN</field>
    <description>Connexion VPN non autorisée depuis une source externe</description>
    <group>vpn, external</group>
  </rule>

  <!-- DLL Side-Loading -->
  <rule id="100011" level="8">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.processname">explorer.exe</field>
    <field name="win.eventdata.commandline">*dll*</field>
    <description>Chargement de DLL non autorisées</description>
    <group>dll_side_loading, exploitation</group>
  </rule>

  <!-- Ingress Tool Transfer -->
  <rule id="100012" level="8">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.processname">wget</field>
    <description>Transfert d'outils non autorisés via wget</description>
    <group>ingress_tool_transfer, tool_transfer</group>
  </rule>

  <!-- Rename System Utilities -->
  <rule id="100013" level="9">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.oldname">cmd.exe</field>
    <field name="win.eventdata.newname">notepad.exe</field>
    <description>Renommage suspect de cmd.exe (utilitaire système)</description>
    <group>rename_system_utilities, evasion</group>
  </rule>

  <!-- Obfuscated Files or Information -->
  <rule id="100014" level="9">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.filename">*.*</field>
    <description>Fichiers exécutables obfusqués détectés</description>
    <group>obfuscation, evasion</group>
  </rule>
```

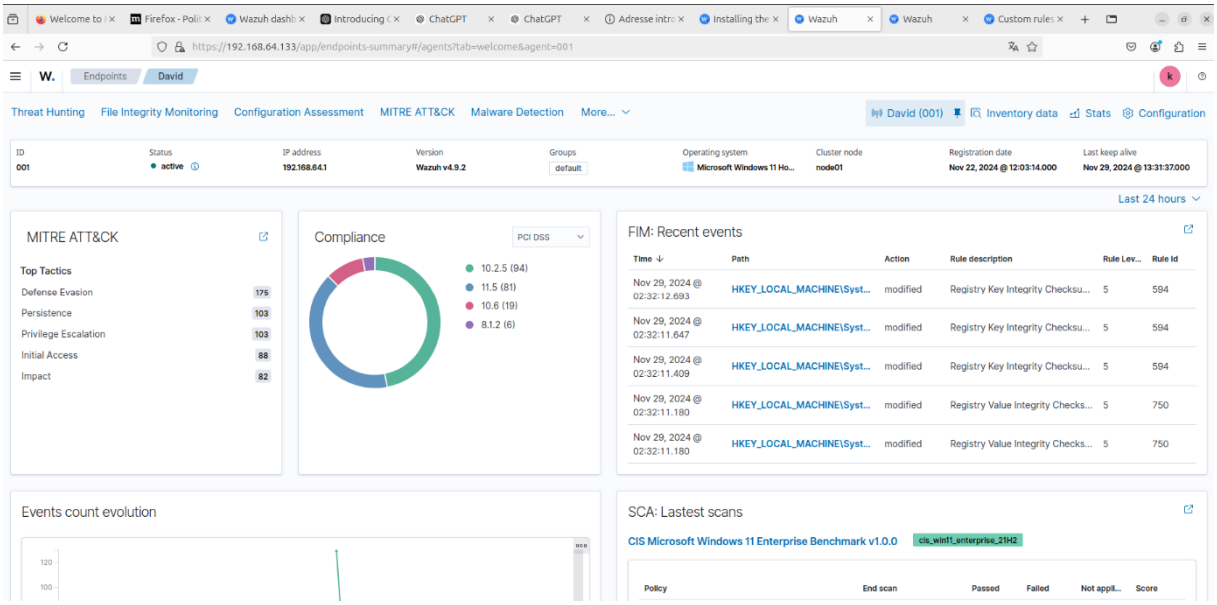
```
  <!-- OS Credential Dumping: SAM -->
  <rule id="100015" level="10">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.targetobject">SAM</field>
    <description>Dumping du SAM (Security Account Manager)</description>
    <group>credential_dumping, os_dump</group>
  </rule>

  <!-- Spearphishing via Service: Email -->
  <rule id="100016" level="9">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.subject">*phishing*</field>
    <description>Spearphishing via Service: Email suspect</description>
    <group>spearphishing, phishing</group>
  </rule>

  <!-- Remote File Copy -->
  <rule id="100017" level="8">
    <decoded_as>json</decoded_as>
    <field name="win.eventdata.processname">robocopy</field>
    <description>Copie de fichiers distante via robocopy</description>
    <group>file_transfer, remote_copy</group>
  </rule>
</group>
```

3. Simulation et Résultats

3.1. Scénarios de Simulation



Les simulations ont été effectuées en générant des activités suspectes depuis la machine Windows (agent) :

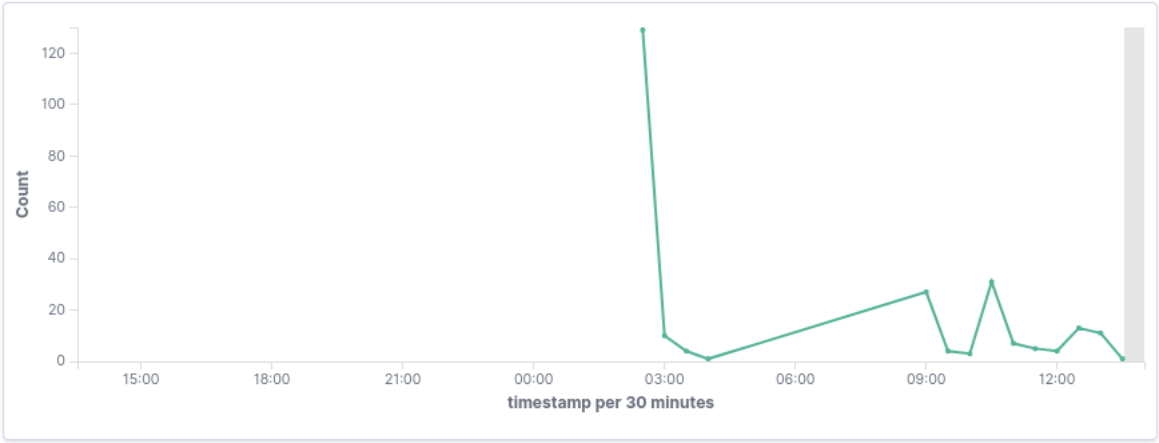
- Exécution de scripts PowerShell encodés.
- Création de comptes non autorisés.
- Tentatives de connexions suspectes via VPN.

3.2. Tableau des Résultats

FIM: Recent events

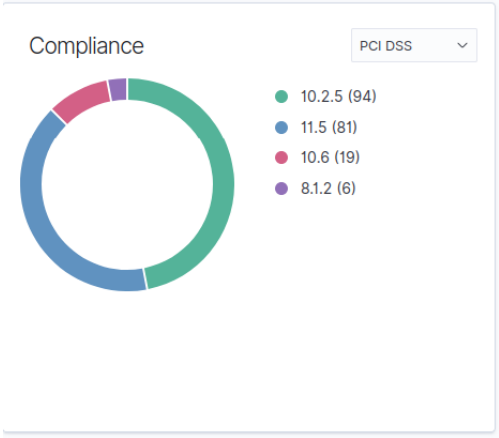
Time ↓	Path	Action	Rule description	Rule Lev...	Rule Id
Nov 29, 2024 @ 02:32:12.693	HKEY_LOCAL_MACHINE\Syst...	modified	Registry Key Integrity Checksu...	5	594
Nov 29, 2024 @ 02:32:11.647	HKEY_LOCAL_MACHINE\Syst...	modified	Registry Key Integrity Checksu...	5	594
Nov 29, 2024 @ 02:32:11.409	HKEY_LOCAL_MACHINE\Syst...	modified	Registry Key Integrity Checksu...	5	594
Nov 29, 2024 @ 02:32:11.180	HKEY_LOCAL_MACHINE\Syst...	modified	Registry Value Integrity Checks...	5	750
Nov 29, 2024 @ 02:32:11.180	HKEY_LOCAL_MACHINE\Syst...	modified	Registry Value Integrity Checks...	5	750

Events count evolution



4. Analyse des Résultats

Les simulations ont confirmé que la majorité des règles fonctionnaient comme prévu, détectant efficacement les activités malveillantes. Cependant, certains faux positifs ont été observés, nécessitant un ajustement des paramètres ou des seuils de détection.



---

5. Conclusion et Recommandations

5.1. Conclusion

Le projet a démontré la pertinence de l'utilisation de Wazuh pour détecter les TTPs associés à des attaques réelles. Les règles configurées offrent une couverture significative des phases critiques d'une cyberattaque.

5.2. Recommandations

1. **Élargissement des Règles** : Ajouter des règles pour couvrir les techniques non encore implémentées, telles que T1036.003 (Renommage d'utilitaires système).
2. **Automatisation** : Intégrer des mécanismes de réponse automatique pour accélérer les actions correctives.
3. **Tests Périodiques** : Effectuer des simulations régulières pour vérifier l'efficacité des règles en conditions réelles.