ECOLE NORMALE SUPÉRIEURE DE L'ENSEIGNEMENT
TECHNIQUE DE MOHAMMEDIA
UNIVERSITÉ HASSAN II DE CASABLANCA

Fillière: CCN

Projet Fin de Module:

Sécurité des endpoints et supervision SIEM:

étude de cas multi-OS (Linux & Windows)

Présenté par: OUAHABI Issam

Encadré par: Prof. Azeddine KHIAT

Année universitaire : 2025/2026

1- Introduction

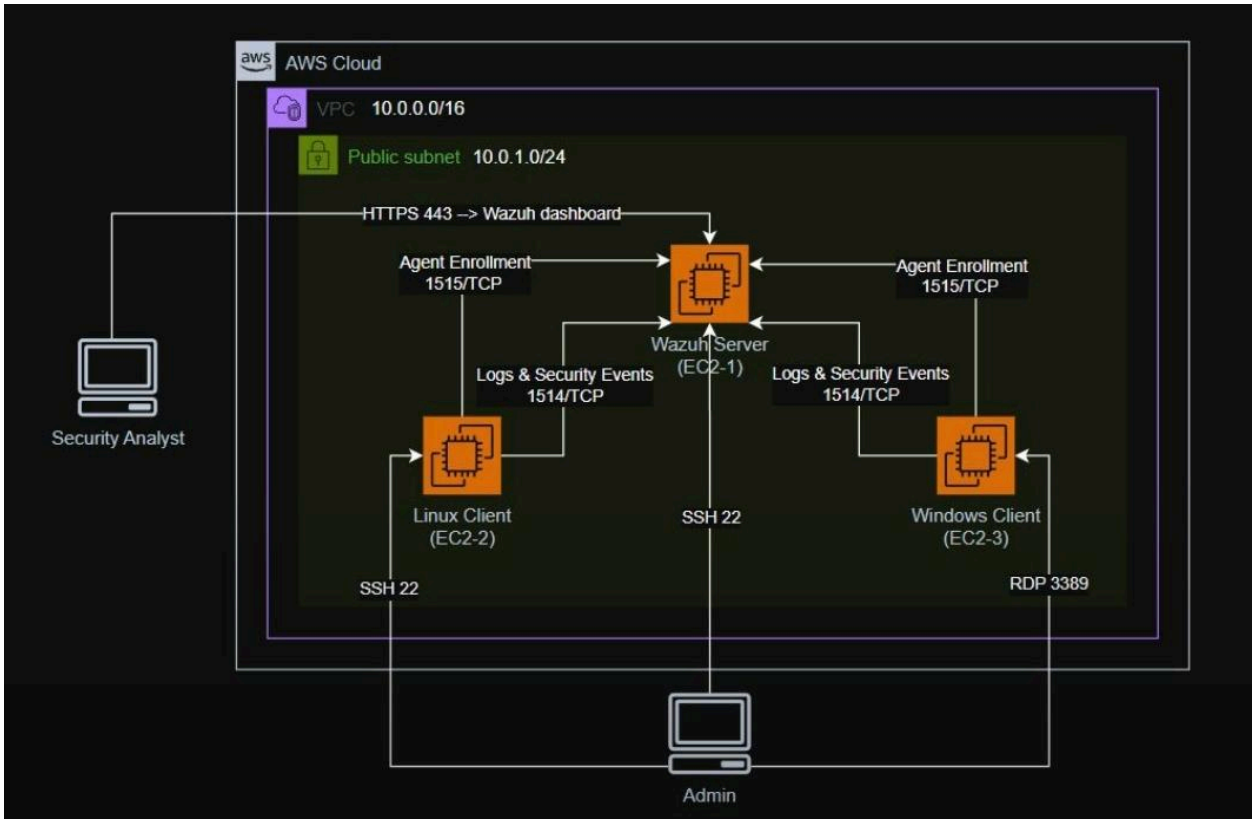
L'objectif de ce projet est de mettre en place une plateforme de **supervision et de détection de sécurité** basée sur une approche **SIEM et EDR**, déployée dans un environnement Cloud. Cette plateforme vise à centraliser, analyser et corréler des événements de sécurité provenant de plusieurs systèmes afin d'identifier des comportements suspects et des incidents potentiels.

Le lab s'appuie sur la solution **Wazuh**, utilisée comme composant central d'un **SOC moderne**, permettant la collecte et l'analyse des journaux de sécurité, ainsi que la surveillance des endpoints. Deux types de systèmes sont supervisés : un **client Linux** et un **client Windows**, représentant des environnements couramment rencontrés en entreprise.

À travers des scénarios réalistes (tentatives d'authentification échouées, élévation de privilèges, création d'utilisateurs, événements système), ce projet démontre la capacité de la plateforme à **détecter des événements de sécurité réels**, à les centraliser dans un tableau de bord unique et à fournir une visibilité claire sur l'état de sécurité des systèmes.

Ce travail permet ainsi d'illustrer le fonctionnement opérationnel d'un **SOC**, en montrant comment les solutions SIEM et EDR peuvent être utilisées conjointement pour améliorer la détection, l'analyse et la compréhension des menaces dans un environnement Cloud.

2- Architecture du lab



L'architecture du projet est déployée dans un **environnement AWS Cloud**, au sein d'un **VPC dédié (10.0.0.0/16)** comprenant un **subnet public (10.0.1.0/24)**. Cette architecture vise à simuler un environnement d'entreprise supervisé par un **SOC centralisé**.

Serveur Wazuh (EC2-1)

Le cœur de l'architecture repose sur une instance **EC2 Ubuntu** jouant le rôle de **serveur Wazuh All-in-One**. Cette instance regroupe :

- le **Wazuh Manager** (analyse et corrélation des événements),
- l'**Indexer** (stockage et recherche),
- le **Dashboard** (visualisation SIEM).

Le serveur Wazuh est accessible par l'analyste sécurité via le **port HTTPS 443**, permettant l'accès au tableau de bord de supervision.

Clients supervisés

Deux endpoints sont intégrés à la plateforme :

- **Client Linux (EC2-2)**
  Une instance Ubuntu équipée de l'**agent Wazuh**, représentant un serveur Linux d'entreprise.
  L'administration se fait via **SSH (port 22)**.

- **Client Windows (EC2-3)**
  Une instance Windows Server équipée de l'**agent Wazuh**, représentant un poste ou serveur Windows en environnement professionnel.
  L'accès administrateur se fait via **RDP (port 3389)**.

Communication et flux réseau

Les communications entre les agents et le serveur Wazuh reposent sur des ports dédiés :

- **1515/TCP** : utilisé pour l'**enrôlement des agents** (Linux et Windows) vers le serveur Wazuh.

- **1514/TCP** : utilisé pour la **transmission des logs et événements de sécurité** des agents vers le serveur.

- **443/TCP** : accès au **dashboard Wazuh** pour l'analyste sécurité.

Ces flux permettent la centralisation des journaux, la corrélation des événements et la détection d'activités suspectes en temps réel.

Rôles des utilisateurs

- **Administrateur** : accède aux instances via SSH et RDP pour la configuration et la génération d'événements.

- **Analyste sécurité** : accède uniquement au dashboard Wazuh pour analyser les alertes et mener des activités de threat hunting.

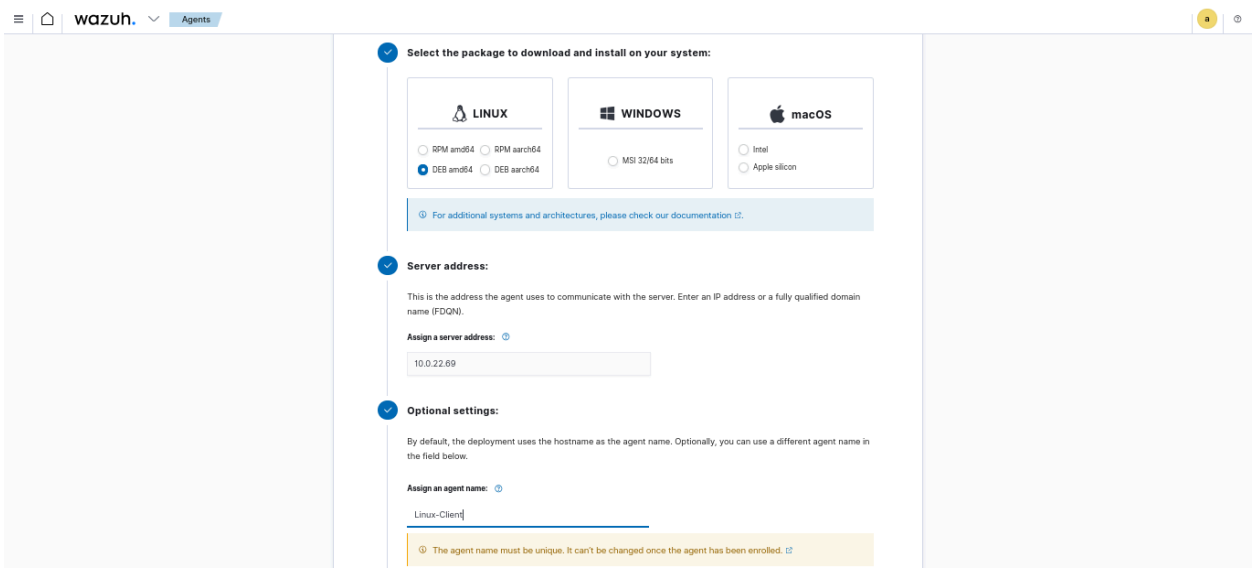
3- Mise en place technique

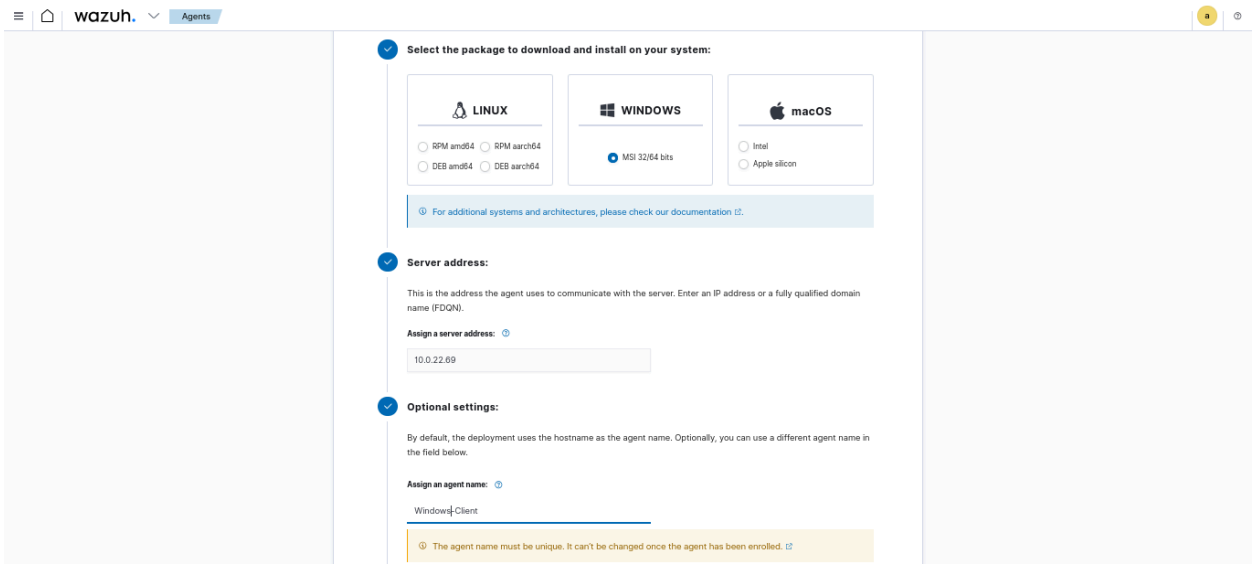
Installation de Wazuh sur le serveur

```
┌──(kali㉿kali)-[~/Downloads]
└─$ chmod 400 wazuh-lab-key.pem

┌──(kali㉿kali)-[~/Downloads]
└─$ ssh -i wazuh-lab-key.pem ubuntu@34.228.40.89
The authenticity of host '34.228.40.89 (34.228.40.89)' can't be established.
ED25519 key fingerprint is: SHA256:SR+NWf0ZsyMLgpmlRf6PHOpwpnrsUSoDFFT3gPf90HY
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '34.228.40.89' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-1040-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu Jan  8 18:25:03 UTC 2026

  System load:  0.23              Processes:             116
  Usage of /:   6.0% of 28.89GB   Users logged in:       0
  Memory usage: 3%                IPv4 address for ens5: 10.0.22.69
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

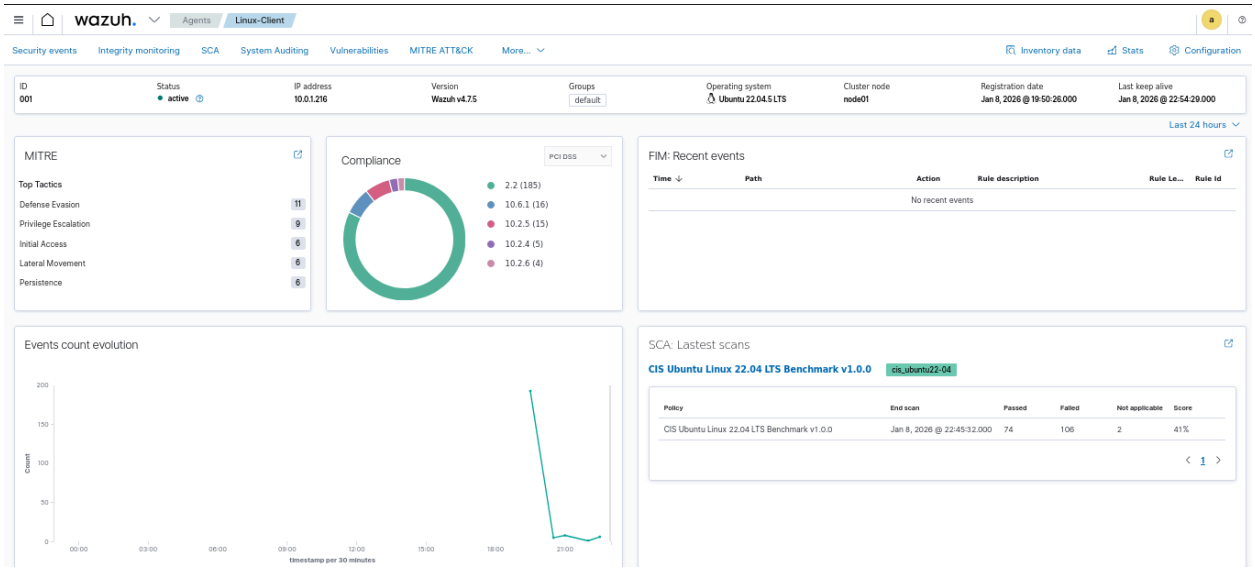
```
ubuntu@ip-10-0-22-69:~$ sudo apt update && sudo apt -y upgrade
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
sudo bash wazuh-install.sh -a
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [3162 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [485 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [19.1 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [5043 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [944 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [644 B]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1245 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [310 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [30.0 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [57.6 kB]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [13.2 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [600 B]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [69.4 kB]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [11.5 kB]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [412 B]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 B]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [31.7 kB]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [16.9 kB]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [672 B]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [2902 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [417 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [14.0 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [4883 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [917 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [652 B]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [1008 kB]
```

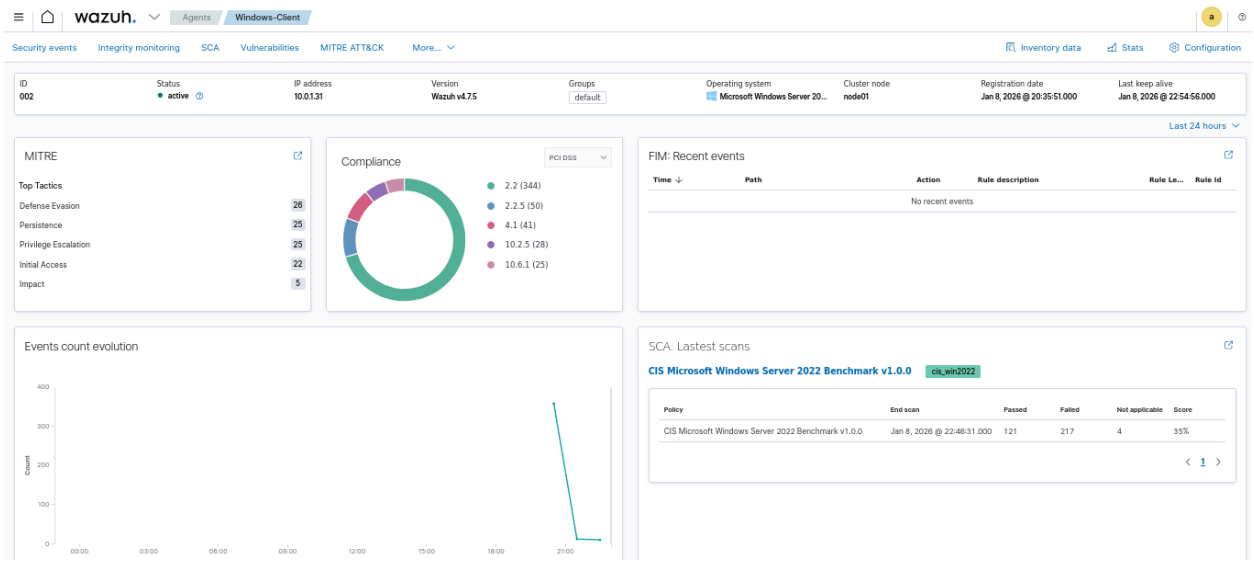
Création des agents Linux et Windows





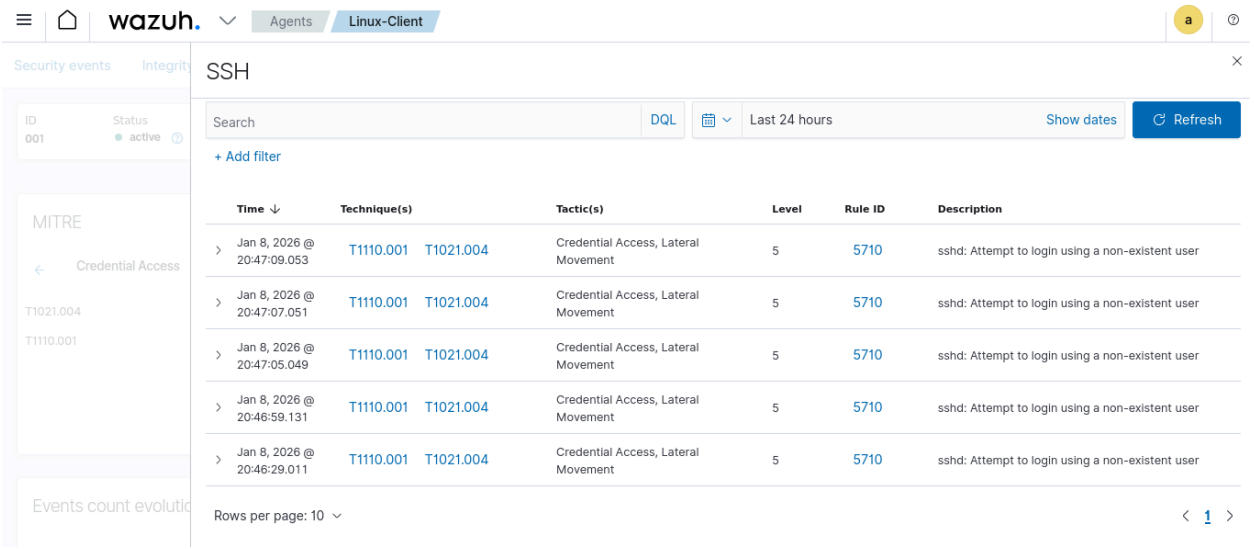
Visualisation des agents Linux et Windows

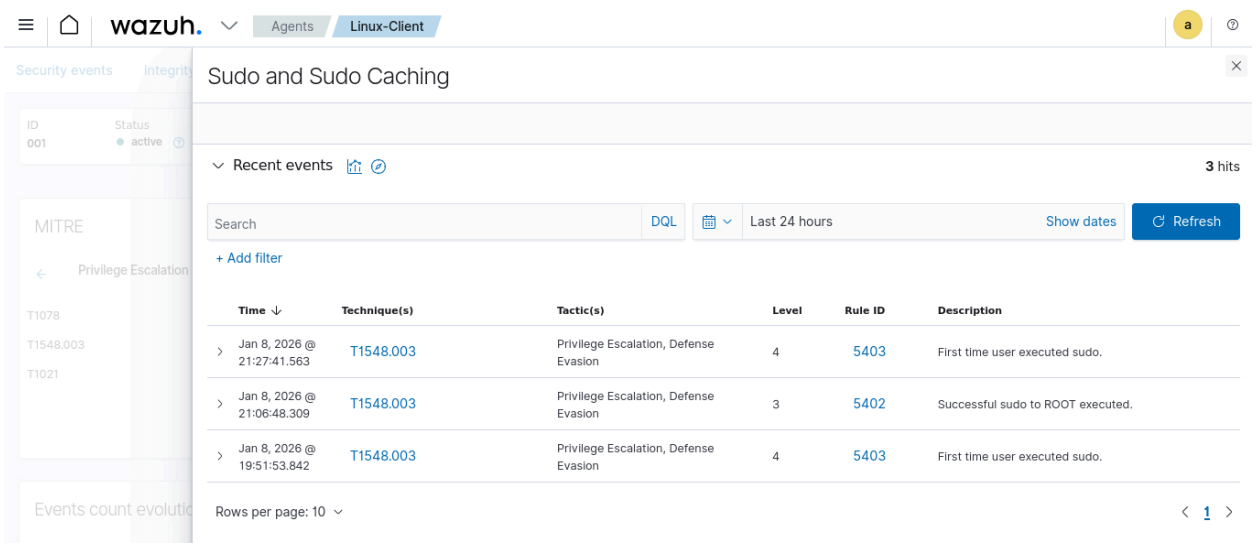


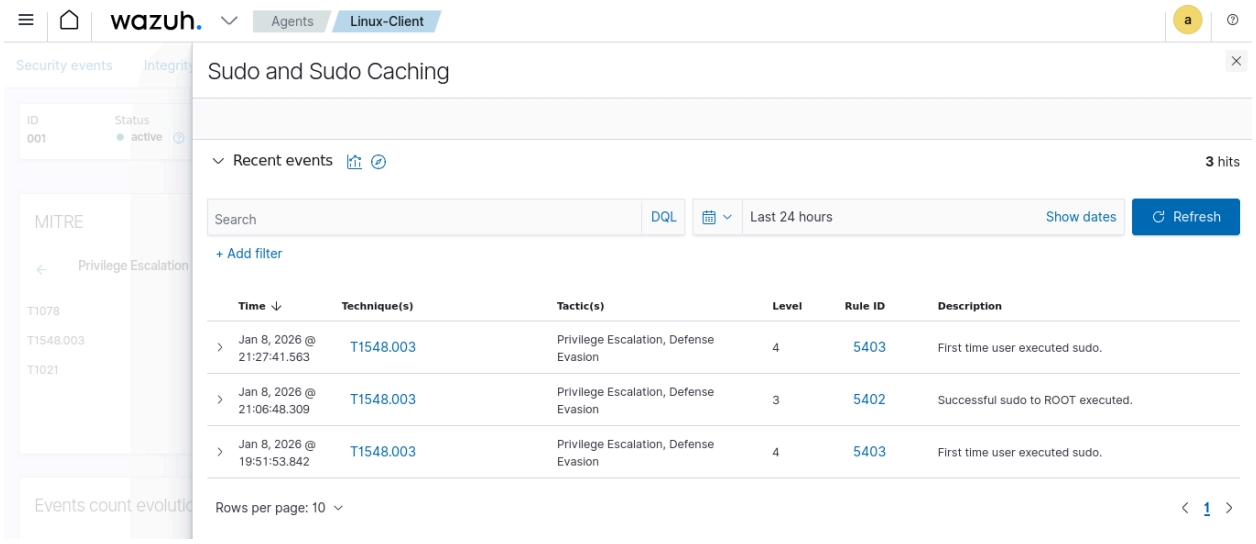

wazuh.
Agents
Windows-Client
Security events
Integrity monitoring
SCA
Vulnerabilities
MITRE ATT&CK
More...
Inventory data
Stats
Configuration
ID
002
Status
active
IP address
10.0.1.31
Version
Wazuh v4.7.5
Groups
default
Operating system
Microsoft Windows Server 20...
Cluster node
node01
Registration date
Jan 8, 2026 @ 20:35:51.000
Last keep alive
Jan 8, 2026 @ 22:54:56.000
Last 24 hours
MITRE
Top Tactics
Defense Evasion 26
Persistence 25
Privilege Escalation 25
Initial Access 22
Impact 5
Compliance
PCI DSS
2.2 (344)
2.2.5 (50)
4.1 (41)
10.2.5 (28)
10.6.1 (25)
FIM: Recent events
Time
Path
Action
Rule description
Rule Le...
Rule Id
No recent events
Events count evolution
Count
400
300
200
100
0
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
SCA: Lastest scans
CIS Microsoft Windows Server 2022 Benchmark v1.0.0
cis_win2022
Policy
End scan
Passed
Failed
Not applicable
Score
CIS Microsoft Windows Server 2022 Benchmark v1.0.0
Jan 8, 2026 @ 22:46:31.000
121
217
4
35%
1

4- Démonstrations de détection

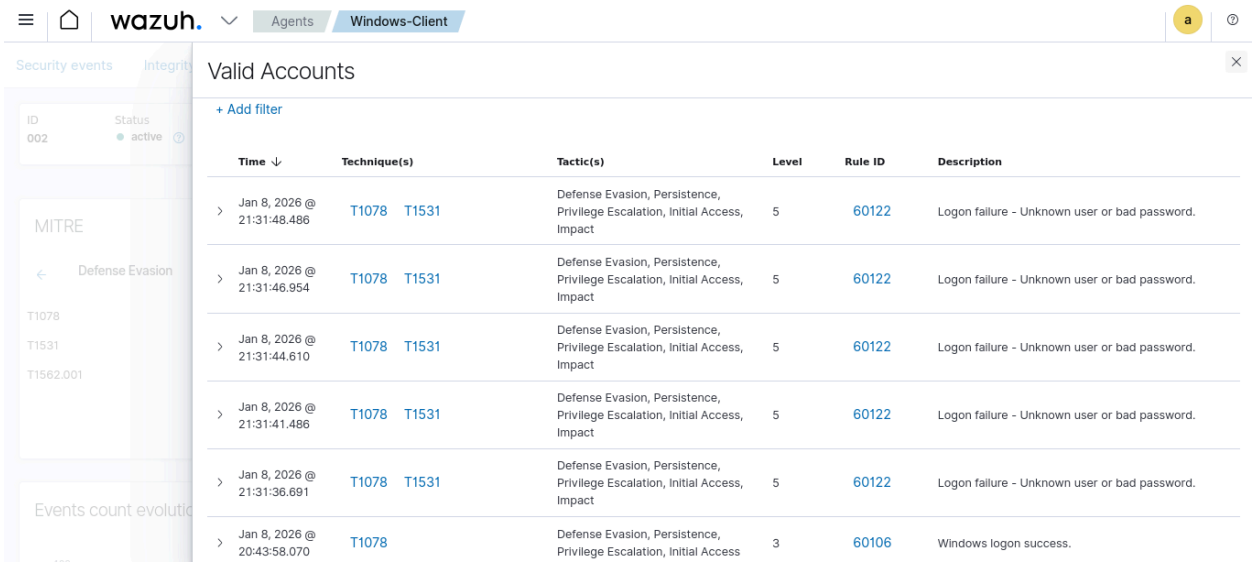
4.1 Détection SIEM côté Linux

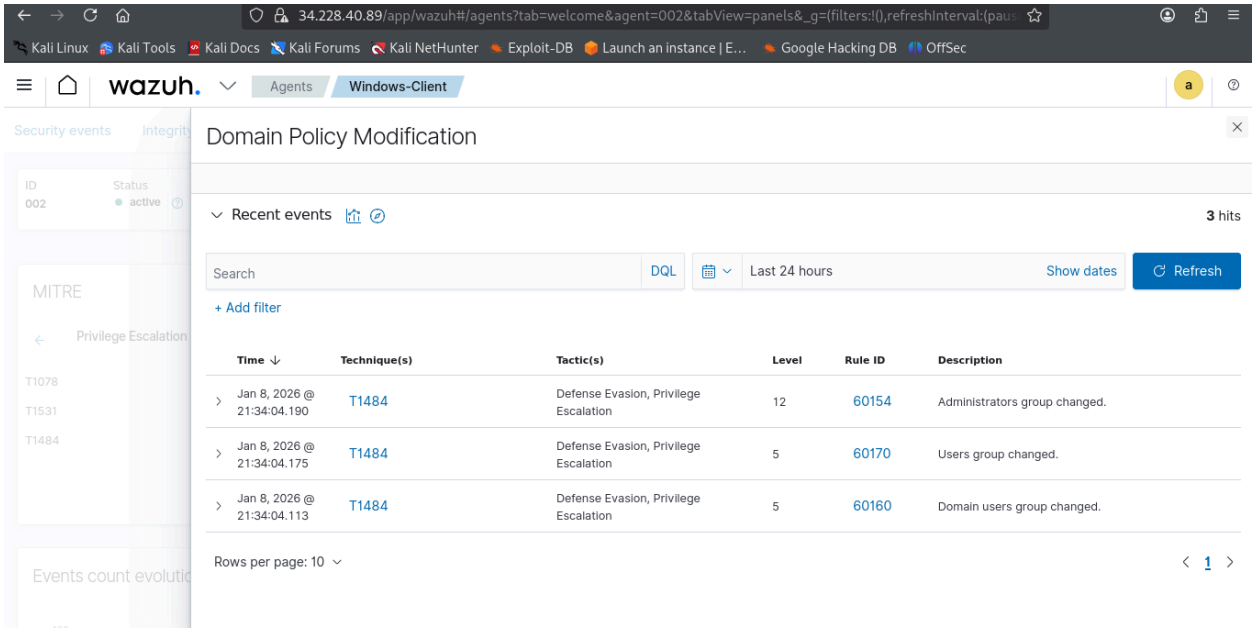


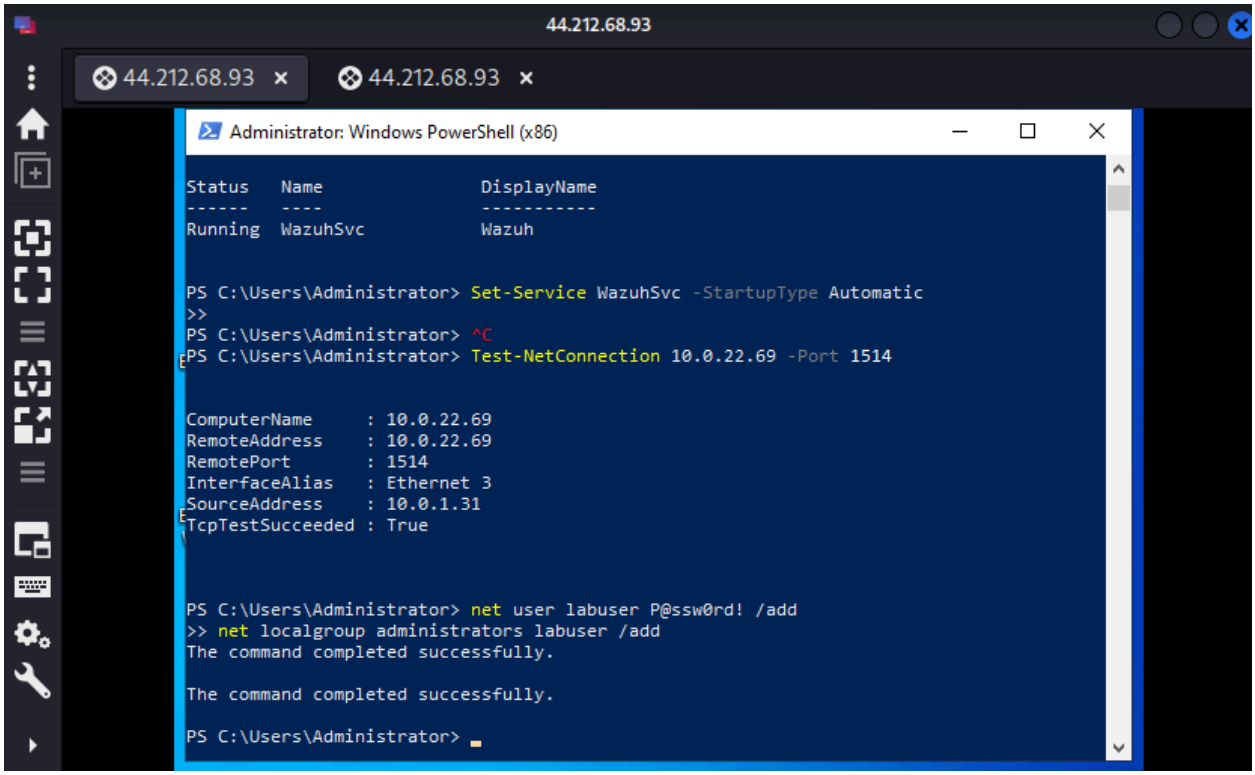


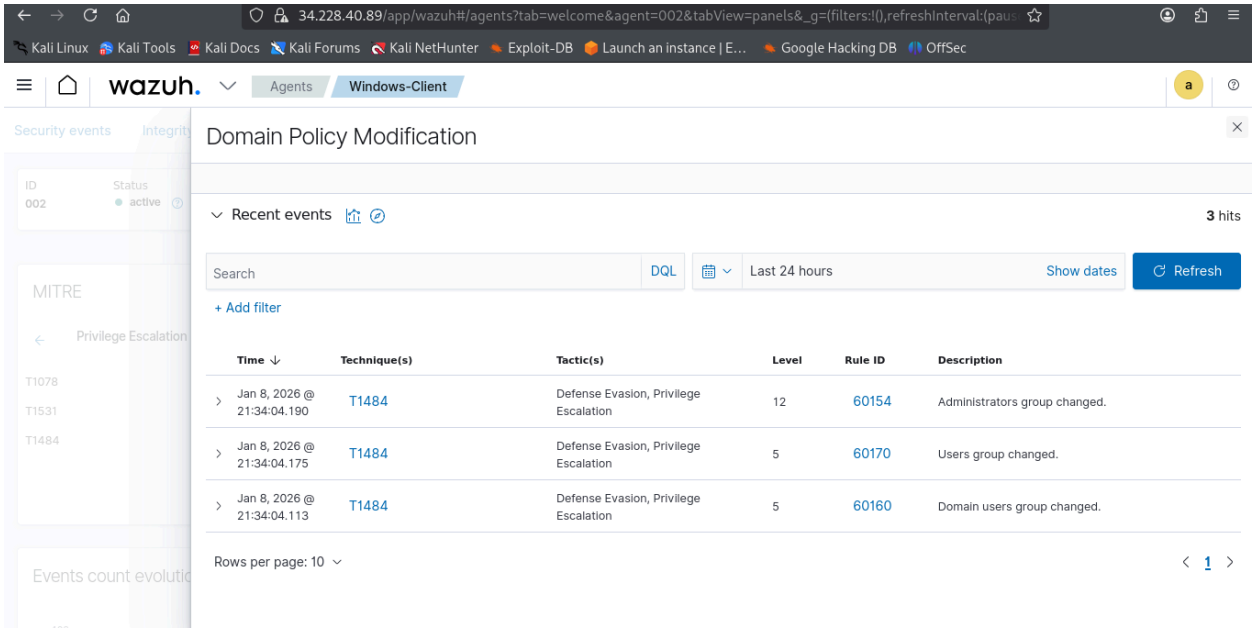


4.2 Détection SIEM / EDR côté Windows


wazuh.
Agents
Windows-Client
a
Security events
Integrity
ID
002
Status
active
MITRE
Defense Evasion
T1078
T1531
T1562.001
Events count evolutio
Valid Accounts
+ Add filter
Time
Technique(s)
Tactic(s)
Level
Rule ID
Description
Jan 8, 2026 @ 21:31:48.486
T1078 T1531
Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact
5
60122
Logon failure - Unknown user or bad password.
Jan 8, 2026 @ 21:31:46.954
T1078 T1531
Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact
5
60122
Logon failure - Unknown user or bad password.
Jan 8, 2026 @ 21:31:44.610
T1078 T1531
Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact
5
60122
Logon failure - Unknown user or bad password.
Jan 8, 2026 @ 21:31:41.486
T1078 T1531
Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact
5
60122
Logon failure - Unknown user or bad password.
Jan 8, 2026 @ 21:31:36.691
T1078 T1531
Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact
5
60122
Logon failure - Unknown user or bad password.
Jan 8, 2026 @ 20:43:58.070
T1078
Defense Evasion, Persistence, Privilege Escalation, Initial Access
3
60106
Windows logon success.


34.228.40.89/app/wazuh#/agents?tab=welcome&agent=002&tabView=panels&_g=(filters:!(),refreshInterval:(paus
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Launch an instance | E...
Google Hacking DB
OffSec
wazuh.
Agents
Windows-Client
Domain Policy Modification
Recent events
3 hits
Search
DQL
Last 24 hours
Show dates
Refresh
+ Add filter
Time
Technique(s)
Tactic(s)
Level
Rule ID
Description
Jan 8, 2026 @ 21:34:04.190
T1484
Defense Evasion, Privilege Escalation
12
60154
Administrators group changed.
Jan 8, 2026 @ 21:34:04.175
T1484
Defense Evasion, Privilege Escalation
5
60170
Users group changed.
Jan 8, 2026 @ 21:34:04.113
T1484
Defense Evasion, Privilege Escalation
5
60160
Domain users group changed.
Rows per page: 10
1


44.212.68.93
44.212.68.93
44.212.68.93
Administrator: Windows PowerShell (x86)
Status Name DisplayName
Running WazuhSvc Wazuh
PS C:\Users\Administrator> Set-Service WazuhSvc -StartupType Automatic
>>
PS C:\Users\Administrator> ^C
PS C:\Users\Administrator> Test-NetConnection 10.0.22.69 -Port 1514
ComputerName : 10.0.22.69
RemoteAddress : 10.0.22.69
RemotePort : 1514
InterfaceAlias : Ethernet 3
SourceAddress : 10.0.1.31
TcpTestSucceeded : True
PS C:\Users\Administrator> net user labuser P@ssw0rd! /add
>> net localgroup administrators labuser /add
The command completed successfully.
The command completed successfully.
PS C:\Users\Administrator>



5- SIEM vs EDR

Ce tableau montre les différences entre SIEM et EDR

SIEM	EDR
Centralisation des logs	Surveillance des endpoints
Corrélation d'événements	Activité processus
Vision globale	Vision locale approfondie

6- IAM / PAM

La gestion des identités et des accès (**IAM – Identity and Access Management**) constitue un élément central de la sécurité des systèmes d'information. Elle permet de contrôler **qui peut accéder aux ressources**, **avec quels droits** et **dans quelles conditions**. Dans ce projet, plusieurs événements détectés par Wazuh illustrent directement les enjeux liés à l'IAM et au **PAM (Privileged Access Management)**.

Création d'un utilisateur local

La création d'un nouvel utilisateur sur un système est considérée comme un **événement critique**, car elle peut indiquer :

- l'arrivée d'un nouvel utilisateur légitime,
- ou une **action malveillante** visant à établir une persistance sur le système.

Un attaquant qui crée un compte local peut réutiliser cet accès ultérieurement sans exploiter à nouveau une vulnérabilité. La détection de cet événement permet donc d'identifier rapidement une tentative de compromission ou une mauvaise gestion des accès.

Ajout au groupe Administrators

L'ajout d'un utilisateur au groupe **Administrators** représente une **élévation de privilèges**. Cet événement est particulièrement sensible, car un compte administrateur dispose de droits étendus :

- modification de la configuration système,
- installation de logiciels,
- désactivation des mécanismes de sécurité,
- accès à des données sensibles.

Dans un contexte de sécurité, ce type de changement peut révéler une **escalade de privilèges non autorisée**, souvent associée à une attaque post-compromission.

Lien avec IAM et PAM

Ces événements illustrent concrètement les principes de l'IAM et du PAM :

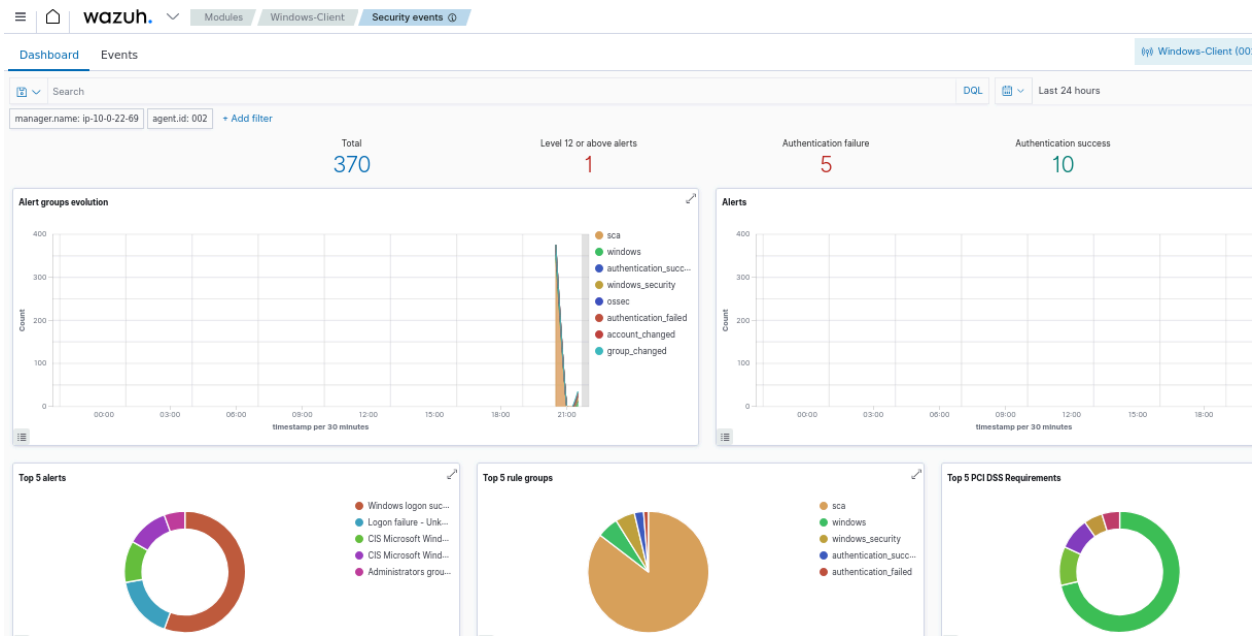
- **IAM** : contrôle de l’identité des utilisateurs et de leurs droits d’accès.

- **PAM** : surveillance et limitation des comptes à privilèges élevés afin de réduire les risques liés à leur abus.

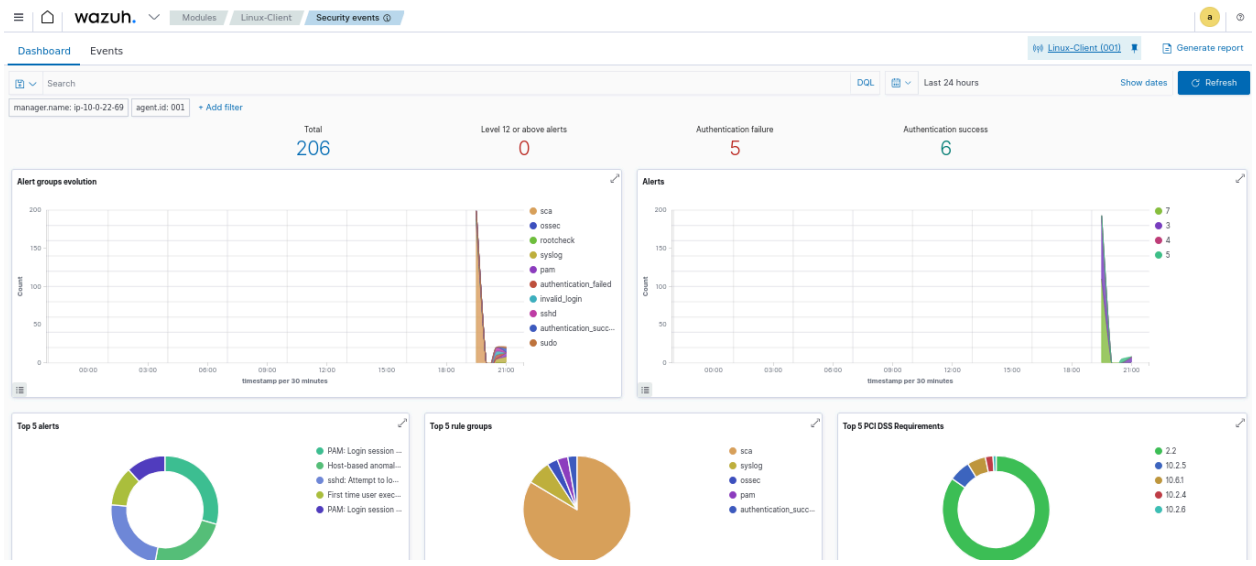
Grâce à Wazuh, ces actions sont détectées, centralisées et analysées, permettant au SOC d’identifier rapidement des comportements à risque et de réagir avant qu’un incident majeur ne se produise.

7- Threat Hunting

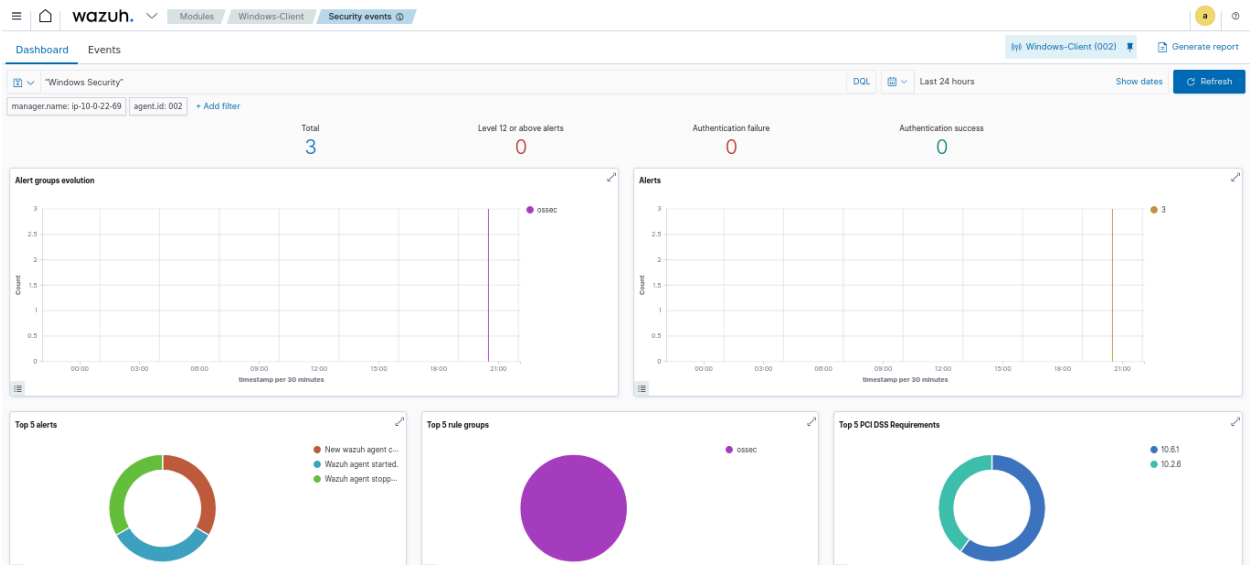
Filtrer seulement Windows client



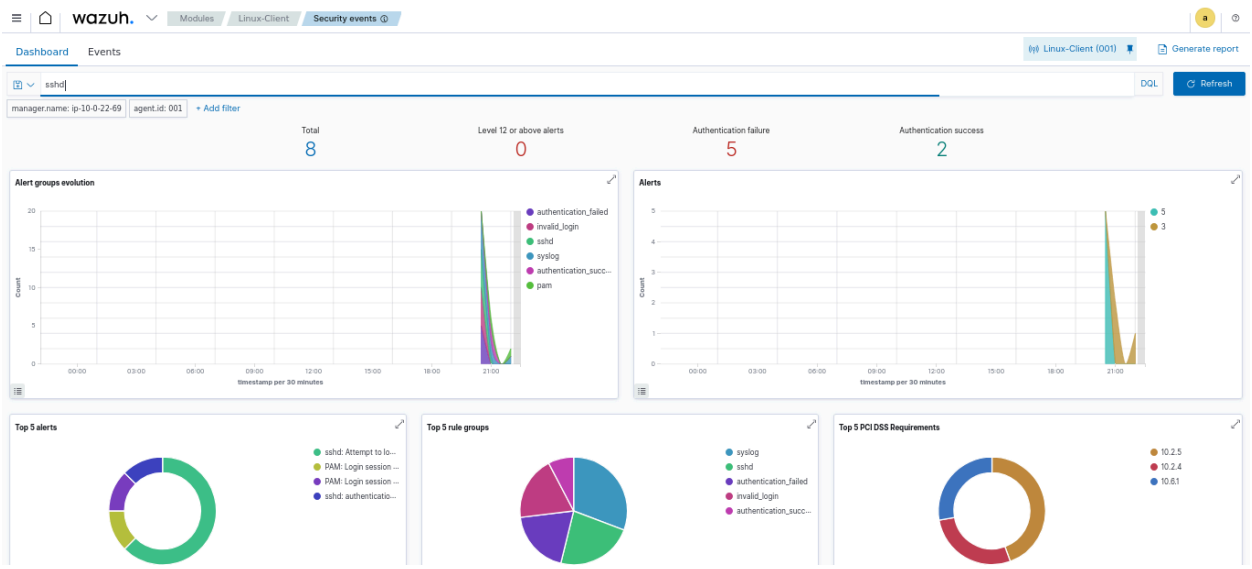
Filtrer seulement Linux client



Dans Windows, chercher pour les alertes “Windows Security” seulement



Dans Linux, chercher pour les alertes “SSHD” seulement



Conclusion

Ce lab a permis de démontrer la mise en œuvre concrète d'une plateforme de **supervision et de détection de sécurité** basée sur une approche **SIEM et EDR**, déployée dans un environnement Cloud. À travers la supervision de systèmes **Linux et Windows**, la solution Wazuh a montré sa capacité à centraliser les journaux, détecter des événements de sécurité réels et fournir une visibilité unifiée sur l'état de sécurité des endpoints.

L'association du **SIEM** (corrélation et analyse centralisée des événements) et de l'**EDR** (surveillance détaillée des activités des endpoints) constitue un atout majeur dans le Cloud, où les environnements sont dynamiques et distribués. Cette complémentarité permet une détection plus efficace des attaques, une meilleure compréhension des incidents et une réaction plus rapide face aux menaces.

Cependant, ce projet reste un **lab pédagogique**. Les scénarios de détection sont limités et ne couvrent pas l'ensemble des attaques possibles en environnement réel. De plus, l'architecture mise en place ne prend pas en compte certains aspects avancés tels que la haute disponibilité, la scalabilité ou l'automatisation complète des réponses. Malgré ces limites, ce travail offre une base solide pour comprendre le fonctionnement opérationnel d'un SOC moderne et l'intérêt des solutions SIEM et EDR dans un contexte Cloud.

LIEN GITHUB:
https://github.com/issamouahabi/Atelier_Securite-des-endpoints-et-supervision-SIEM-tude-de-cas-multi-OS-Linux-et-Windows