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

Projet de Fin Module

Implémentation du Atelier_Sécurité

Projet de Atelier_Sécurité des endpoints et supervision SIEM

Réalisé par :
Rhayour Abdelbarie

Encadré par :
Prof. Azeddine KHIAT

Année universitaire : 2025/2026

1 Introduction

Ce laboratoire a pour objectif de déployer une infrastructure de sécurité complète basée sur la solution Wazuh dans un environnement Cloud AWS. L'architecture met en œuvre une approche combinée SIEM (Security Information and Event Management) et EDR (Endpoint Detection and Response) pour superviser un parc hétérogène composé de serveurs Linux et Windows.
L'objectif est de démontrer la capacité de la plateforme à centraliser les journaux, détecter les tentatives d'intrusion (brute-force) et surveiller l'intégrité des systèmes (création
d'utilisateurs, élévation de privilèges).

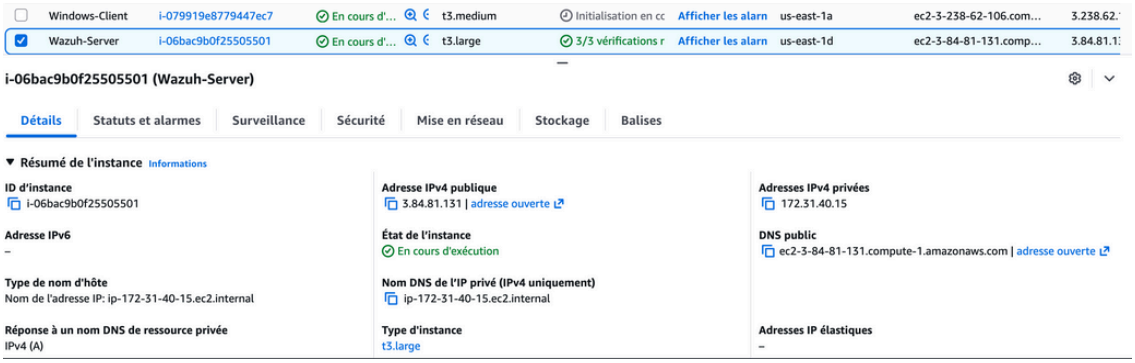
2 Architecture et Mise en place de l'environnement

2.1 Déploiement des Instances AWS

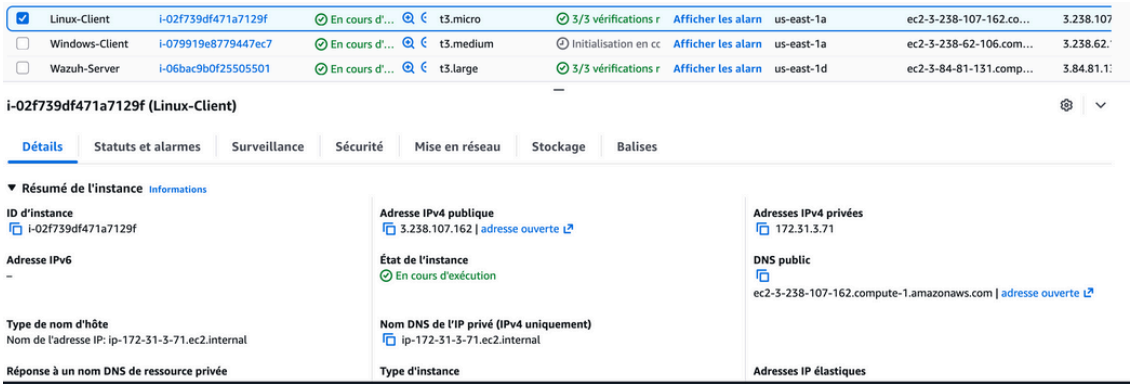
Préparation AWS Learner Lab

Créer les instances EC2

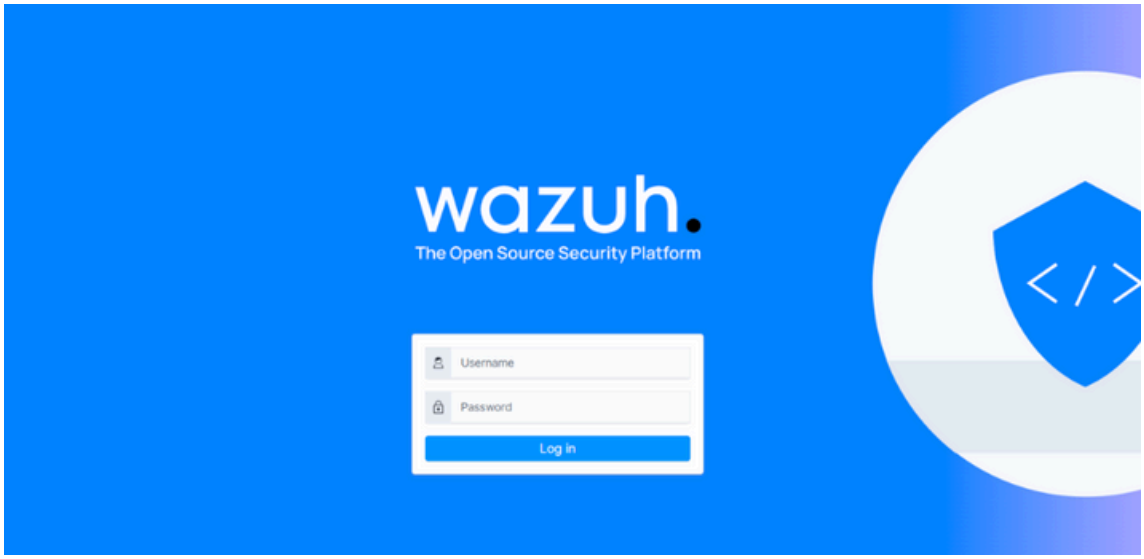
EC2-1 : Wazuh Server

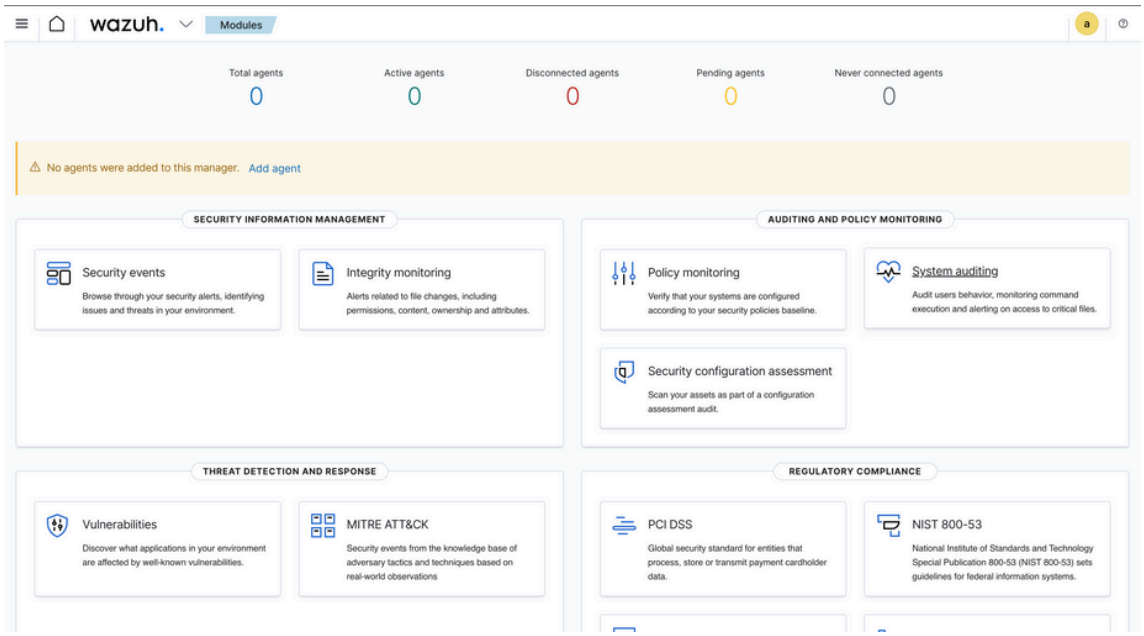


EC2-2 : Linux Client

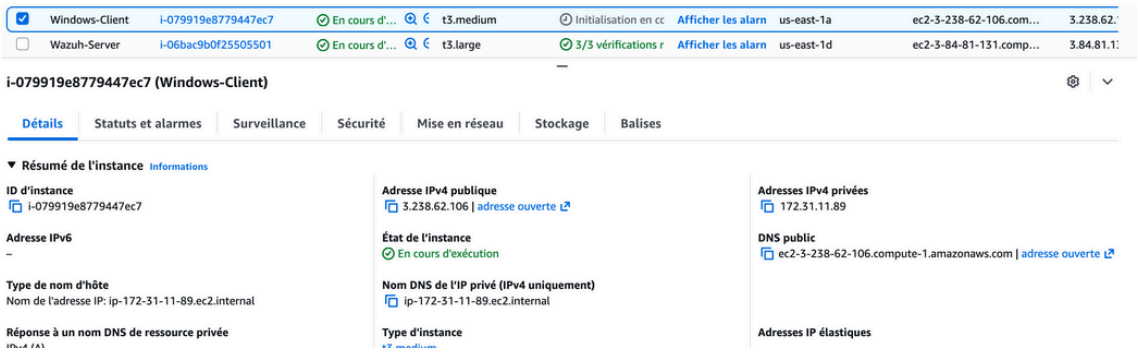


L’installation "All-in-One" a été réalisée via le script automatisé fourni par Wazuh sur l’instance Ubuntu server. Une fois l’installation terminée, nous avons récupéré les identifiants administrateur pour accéder à l’interface web.





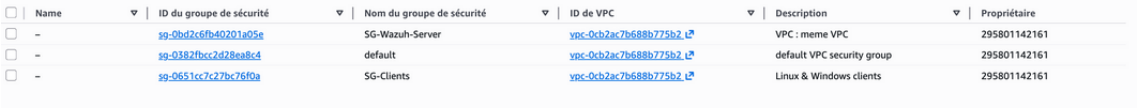
EC2-3 : Windows Client



2.2 Configuration Réseau et Sécurité (Security Groups)

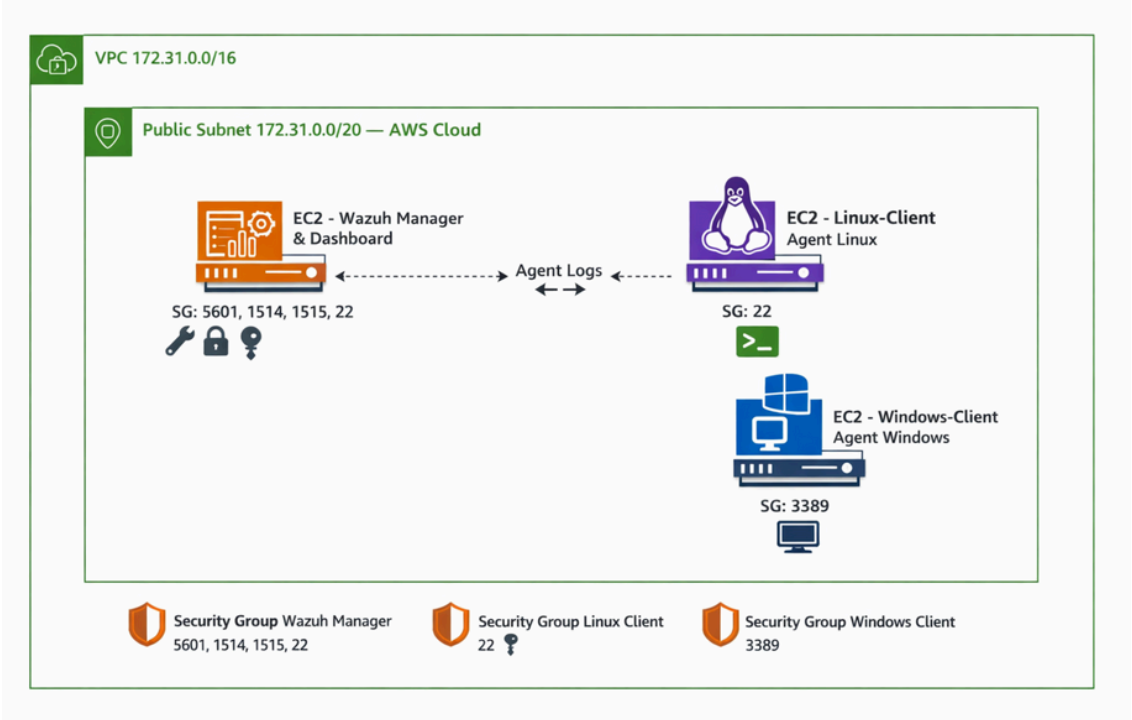
Pour assurer la communication sécurisée entre les agents et le serveur, ainsi que l'accès au tableau de bord, nous avons configuré les groupes de sécurité (SG) pour autoriser les flux suivants :

- **TCP 1514 :** Communication des agents vers le serveur Wazuh.
- **TCP 1515 :** Service d'enrôlement automatique des agents.
- **TCP 443 :** Accès HTTPS au Dashboard Wazuh.
- **TCP 22 & 3389 :** Accès SSH et RDP pour l'administration des serveurs.



Name	ID du groupe de sécurité	Nom du groupe de sécurité	ID de VPC	Description	Propriétaire
–	sg-0bd2c6fb40201a05e	SG-Wazuh-Server	vpc-0cb2ac7b688b775b2	VPC : meme VPC	295801142161
–	sg-0382fbcc2d28ea8c4	default	vpc-0cb2ac7b688b775b2	default VPC security group	295801142161
–	sg-0651cc7c27bc76f0a	SG-Clients	vpc-0cb2ac7b688b775b2	Linux & Windows clients	295801142161

2.3 Architecture



3 Installation et Déploiement de Wazuh

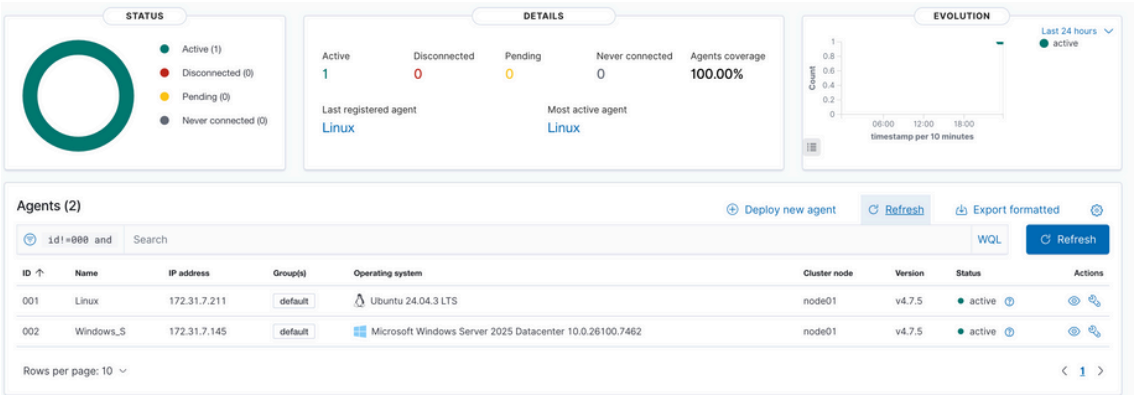
3.1 Installation du Serveur Wazuh

```
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu@ip-172-31-44-110:~$ curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
sudo bash wazuh-install.sh -a
```

Vérifier les services:

- sudo systemctl status wazuh-manager
- sudo systemctl status wazuh-indexer
- sudo systemctl status wazuh-dashboard

LES DEUX AGENTS SONT CORRECTEMENT CONNECTÉS ET APPARAISSENT COMME "ACTIVE" DANS LE TABLEAU DE BORD.



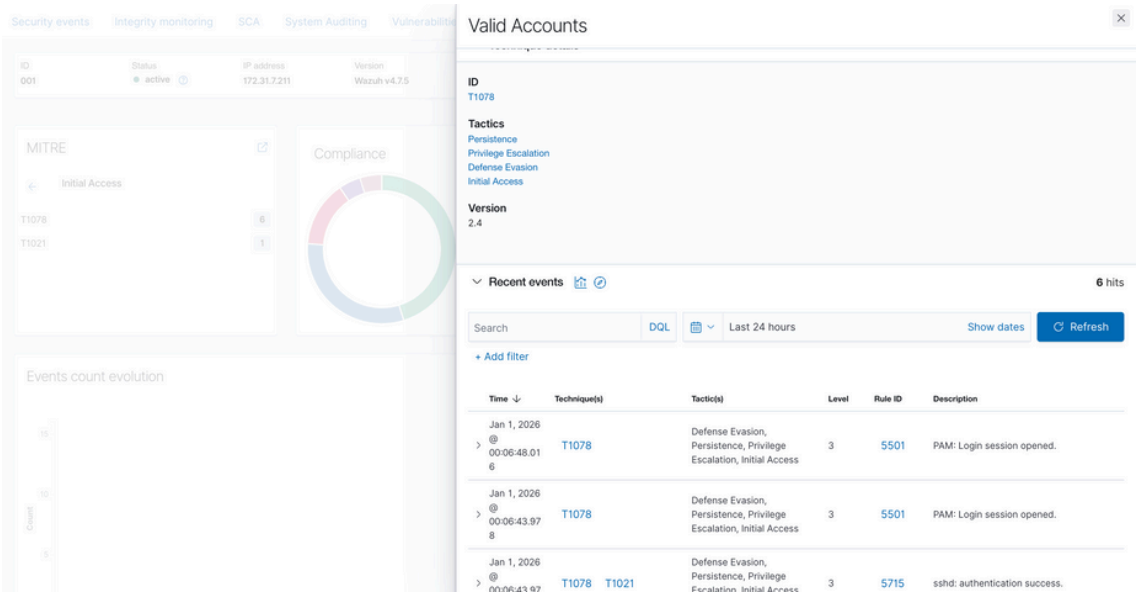
4 Scénarios de Sécurité et Analyse SIEM

4.1 Scénario Linux : Attaques SSH et Élévation de privilèges

Scénario 1 — Tentatives SSH échouées (bruteforce simulé)

Nous avons simulé une attaque par force brute sur le service SSH du client Linux en utilisant un utilisateur inexistant (fakeuser).
Observations : Wazuh a corrélé les échecs d'authentification et généré une alerte de sécurité de niveau élevé :
• Règle ID 5710 : "sshd : Attempt to login using a non-existent user".

```
fakeuser@172.31.24.132: Permission denied (publickey).
ubuntu@ip-172-31-24-132:~$ ssh fakeuser@172.31.24.132
fakeuser@172.31.24.132: Permission denied (publickey).
ubuntu@ip-172-31-24-132:~$ ssh fakeuser@172.31.24.132
fakeuser@172.31.24.132: Permission denied (publickey).
ubuntu@ip-172-31-24-132:~$ ssh fakeuser@172.31.24.132
fakeuser@172.31.24.132: Permission denied (publickey).
ubuntu@ip-172-31-24-132:~$ ssh fakeuser@172.31.24.132
fakeuser@172.31.24.132: Permission denied (publickey).
ubuntu@ip-172-31-24-132:~$
```

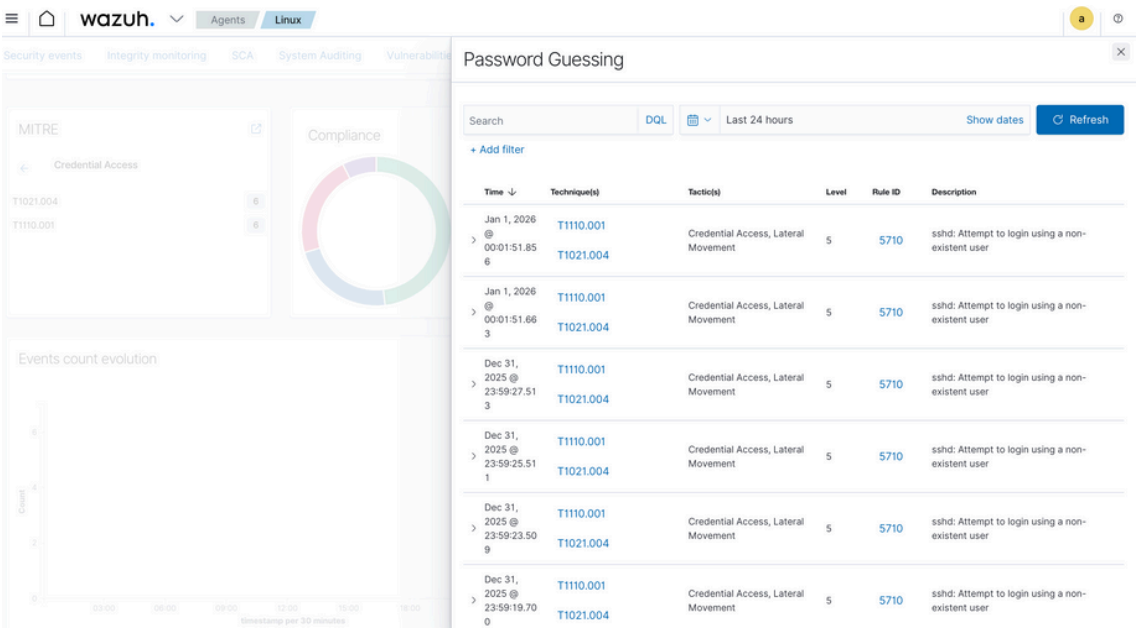


Scénario 2 — Élévation de privilèges (sudo)

Ensuite, nous avons effectué une élévation de privilèges légitime mais critique via la commande sudo su pour passer en root.
Observations:Wazuhadétectél'ouverturedesessionprivilégiéeviaPAM(Pluggable Authentication Modules) :

• Règle ID 5501 : "PAM : Login session opened".
• Technique MITRE : T1078 (Valid Accounts).
Ce type d'événement est essentiel pour le SOC afin de surveiller l'activité des administrateurs.

```
ubuntu@ip-172-31-24-132:~$ sudo su
root@ip-172-31-24-132:/home/ubuntu# /var/log/auth.log
bash: /var/log/auth.log: Permission denied
root@ip-172-31-24-132:/home/ubuntu# /var/log/auth.log
bash: /var/log/auth.log: Permission denied
root@ip-172-31-24-132:/home/ubuntu#
```

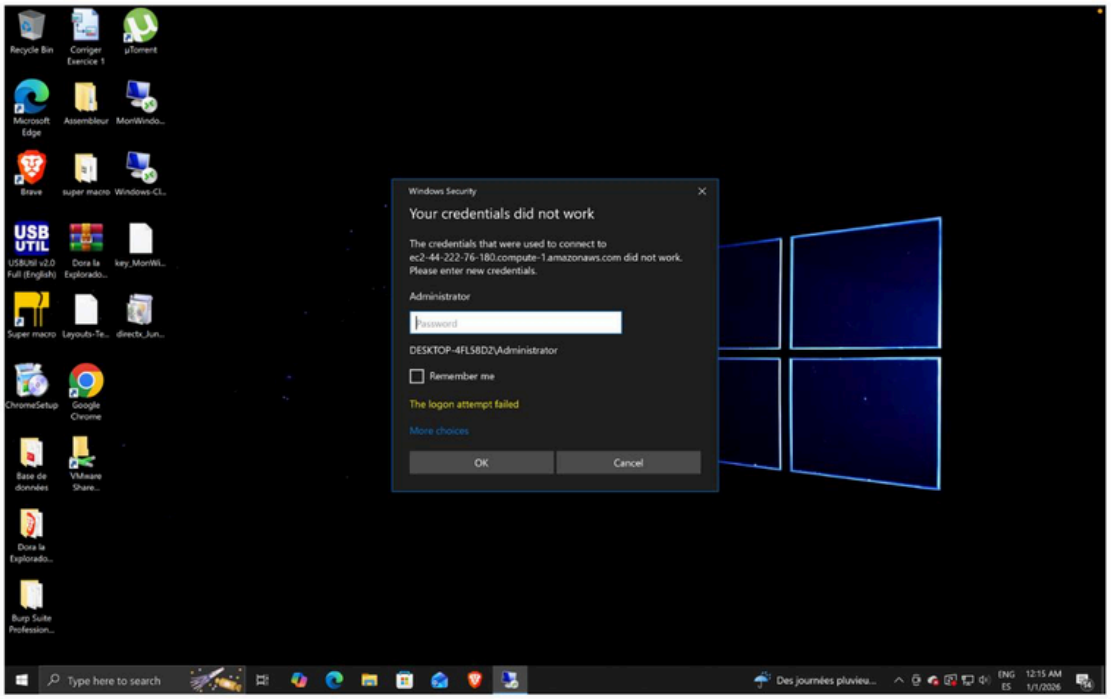


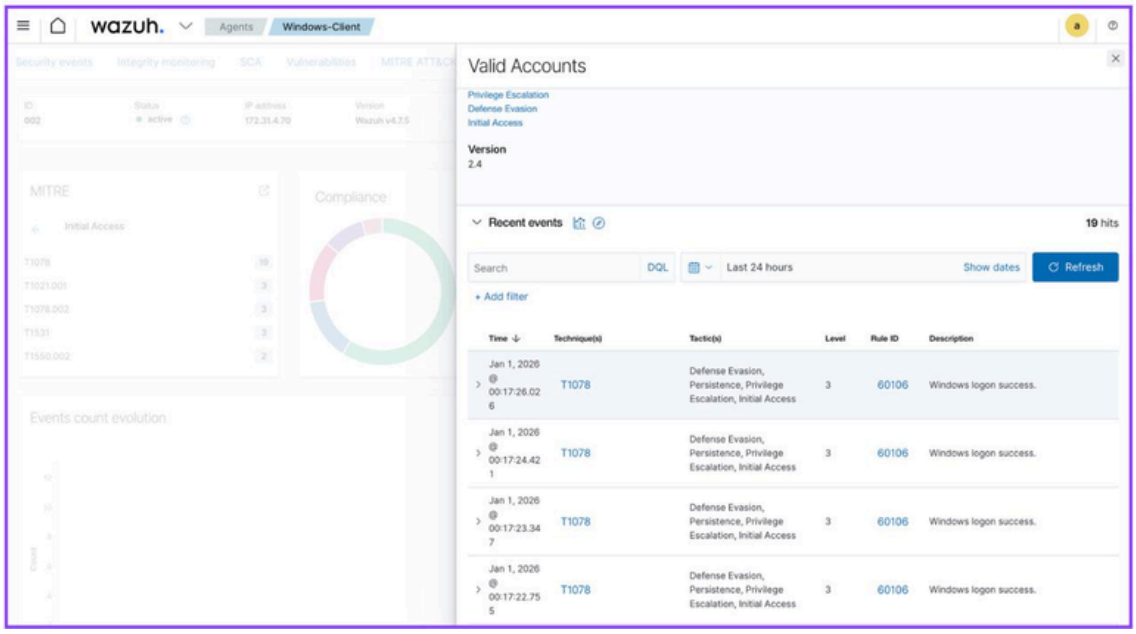
4.2 Scénario Windows : Gestion des utilisateurs et Groupes et Échecs de login :

Scénario 1 — Échecs de login

Objectif : Montrer la détection d'échecs de connexion sur un poste Windows via RDP

- Chaque échec est loggé avec Event ID 4625.
- Le système peut générer alertes dans un SIEM si configuré (ex : corrélation avec tentatives multiples pour détecter une attaque brute force).
- Permet de tester et démontrer la surveillance des tentatives de connexion échouées dans un contexte réel.





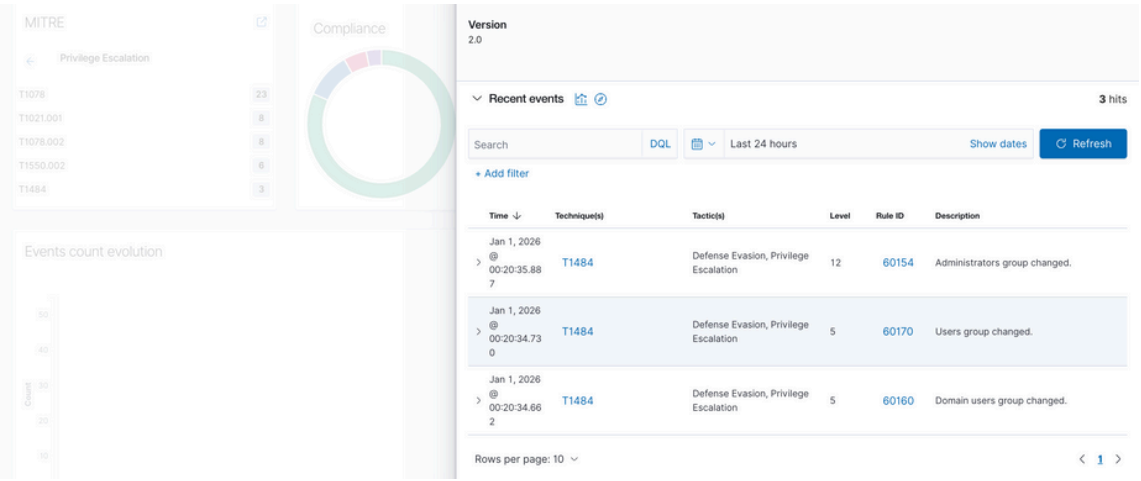
Scénario 2 — Création d'un utilisateur local

Sur le serveur Windows, nous avons créé un utilisateur local (labuser) et l'avons ajouté au groupe des administrateurs via PowerShell.
Observations : L'EDR a détecté les modifications critiques du système (création de compte et modification de groupe de sécurité) :
• Règle ID 60154 : "Administrators group changed".
• Règle ID 60170 : "Users group changed".
Ces alertes sont cruciales pour détecter la persistance d'un attaquant qui tenterait de se créer une porte dérobée avec des droits admin.

```
PS C:\Windows\system32> net user labuser P@ssw0rd! /add
The command completed successfully.

PS C:\Windows\system32> net localgroup administrators labuser /add
The command completed successfully.

PS C:\Windows\system32>
```



5 Security Monitoring et Threat Detection

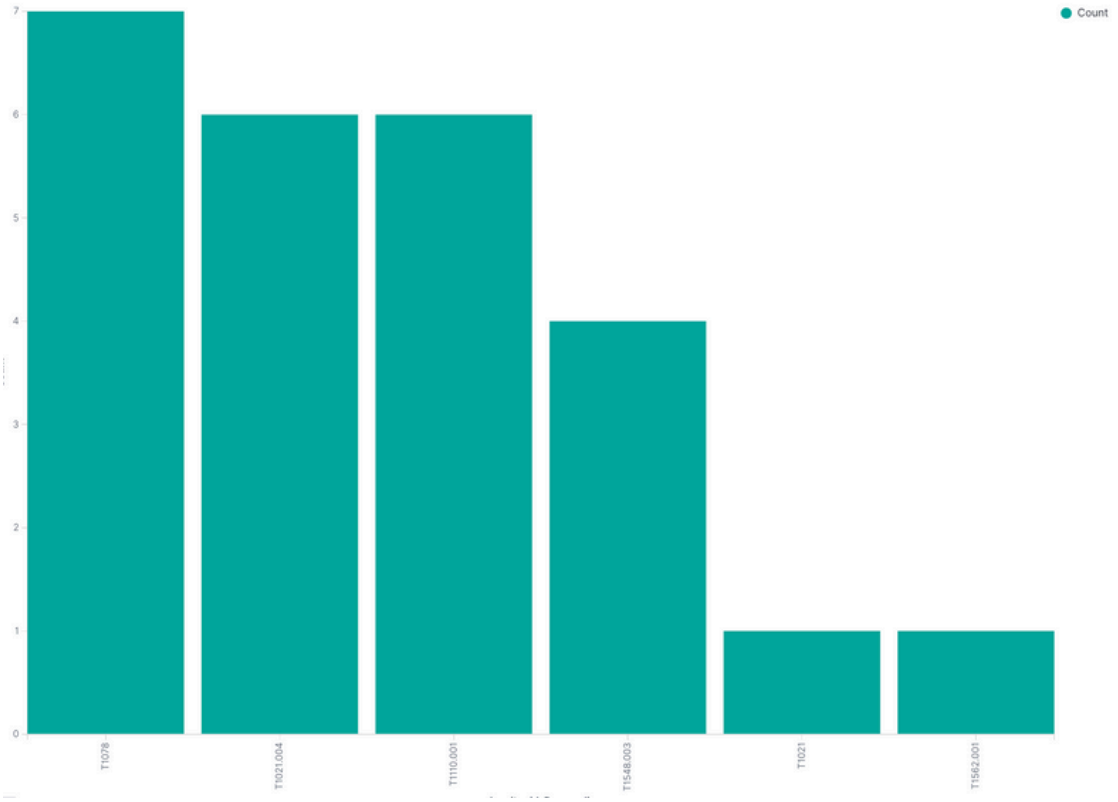
Threat Detection 1

1 Graphique des événements

- Il affiche le nombre d'alertes classées par technique MITRE ATT&CK.
- Techniques les plus fréquentes

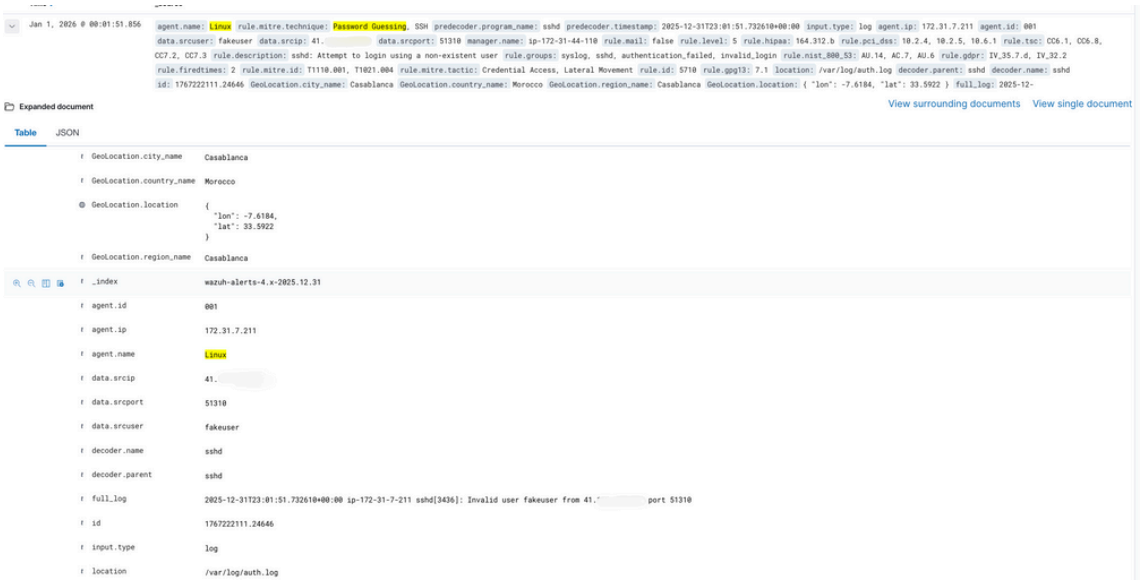
1. T1028 → ~7 événements (la plus élevée)
2. T1020.004 et T1100.001 → ~6 événements chacun
3. T1546.003 → ~4 événements
4. T1021 et T1569.001 → ~1 événement chacun

Ces techniques sont généralement liées à l'accès distant, l'exécution de code, la persistance ou le mouvement latéral dans un réseau.



2. Détail d'une alerte

Type d'alerte : tentative de connexion SSH avec un utilisateur invalide ("Invalid user ... from ...").
Règle Wazuh déclenchée : ID 5719 (brute-force ou scan SSH classique).
IP source : 172.31.7.211 (adresse privée, donc probablement interne à un réseau/VPC).
Machine cible : serveur Linux (agent Wazuh ID 001, IP publique 41.x.x.x).
Géolocalisation de la machine cible : Casablanca, Maroc.
Date de l'événement : début décembre 2025.

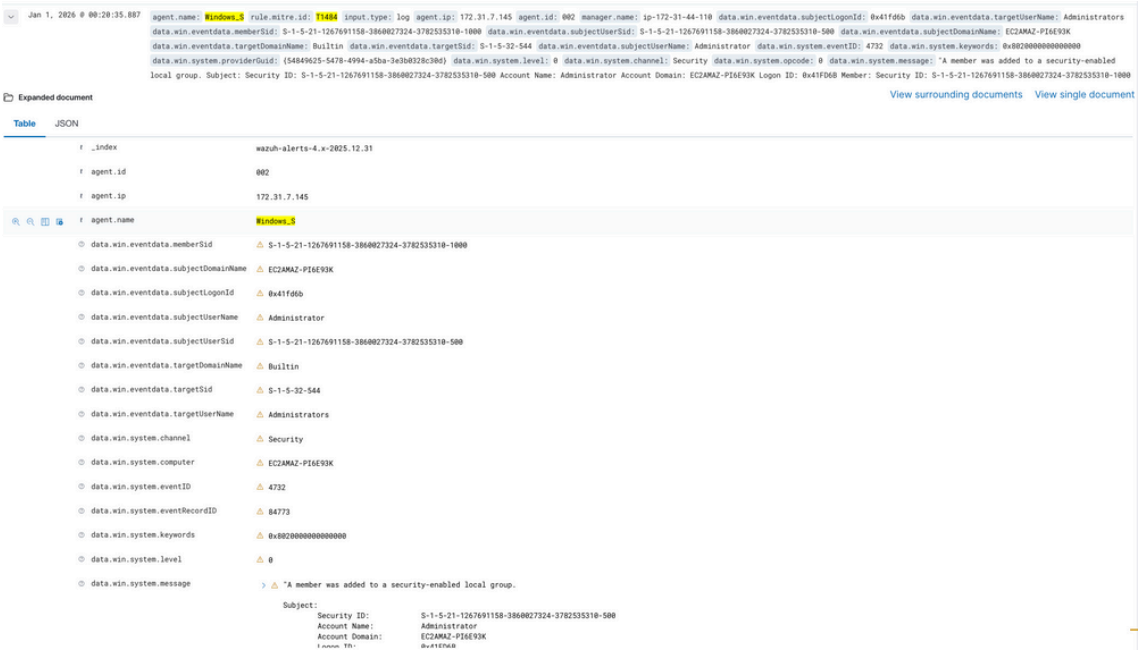


L’ensemble indique très probablement une tentative de brute-force SSH ou un scan automatisé visant ce serveur

Threat Detection 2

une alerte de sécurité élevée dans Wazuh concernant une modification du groupe local "Administrators" sur une machine Windows. Cela correspond à l'ajout d'un membre à ce groupe privilégié

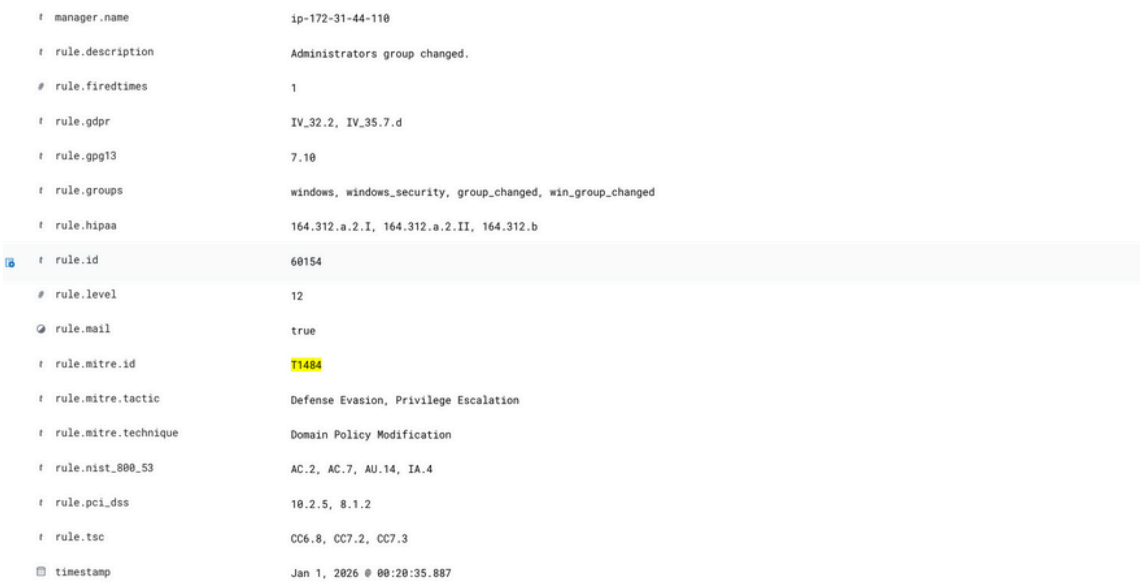
Détail de l’alerte



- Machine concernée : Agent Wazuh ID 002, nom "Windows_S", IP 172.31.7.145 (IP privée).
- Événement Windows : ID 4732 → "A member was added to a security-enabled local group".
- Groupe modifié : "Administrators" (groupe local Builtin des administrateurs).
- Compte ajouté : SID S-... (typiquement le compte Administrator du domaine).
- Compte qui a effectué l'action : Le même compte Administrator.

Technique MITRE ATT&CK

- ID : T1484
- Nom officiel (query name) : Domain or Tenant Policy Modification
- Sous-techniques possibles : T1484.001 (Group Policy Modification)
- Tactiques : Defense Evasion, Privilege Escalation



t	manager.name	ip-172-31-44-110
t	rule.description	Administrators group changed.
#	rule.firedtimes	1
t	rule.gdpr	IV_32.2, IV_35.7.d
t	rule.gpg13	7.10
t	rule.groups	windows, windows_security, group_changed, win_group_changed
t	rule.hipaa	164.312.a.2.I, 164.312.a.2.II, 164.312.b
t	rule.id	60154
#	rule.level	12
◕	rule.mail	true
t	rule.mitre.id	T1484
t	rule.mitre.tactic	Defense Evasion, Privilege Escalation
t	rule.mitre.technique	Domain Policy Modification
t	rule.nist_800_53	AC.2, AC.7, AU.14, IA.4
t	rule.pci_dss	10.2.5, 8.1.2
t	rule.tsc	CC6.8, CC7.2, CC7.3
🗓	timestamp	Jan 1, 2026 @ 00:20:35.887

- Règle Wazuh : ID 60154, niveau 12 (élevé).
- Description : "Administrators group changed."

Technique MITRE ATT&CK (confirmée)

ID : T1484
Nom officiel : Domain or Tenant Policy Modification
Tactique : Defense Evasion, Privilege Escalation
Technique détaillée : Domain Policy Modification (souvent via modification de Group Policy Objects - GPO).

Threat Detection 3

lertes sur une machine Windows cliente ("Windows-Client") indiquant une utilisation de comptes valides pour un mouvement latéral (probablement via RDP), combinée à une manipulation de compte et une authentification alternative (Pass the Hash). Cela s'inscrit dans une chaîne d'attaque potentielle

Requête de recherche

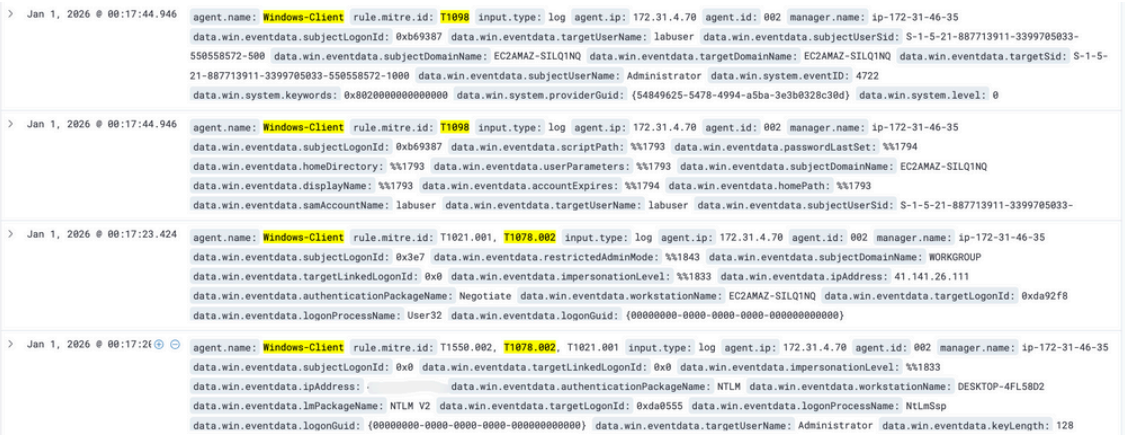
- Filtre appliqué : Agent nommé "Windows-Client" ET techniques MITRE T1098 OU T1078.002.
- Période : Dernières 24 heures.
- Cela cible spécifiquement les événements liés à la manipulation de comptes ou à l'abus de comptes de domaine.

Détails des alertes

Machine concernée :

Agent Wazuh ID 002, nom "Windows-Client", IP privée 172.31.4.70 (même sous-réseau 172.31.x.x que les alertes précédentes, typique d'un environnement lab/cloud)

Événements observés



1 Technique MITRE T1098 (deux alertes)

- Nom officiel : Account Manipulation
- Événement Windows ID 4722 : "A user account was enabled" (un compte utilisateur a été activé).
- Détails : Activation du compte local "labuser" par l'Administrator du domaine (EC2AMAZ-SIL01NQ).
- Paramètres suspects : home directory, script path, etc., définis avec des valeurs comme %1793 (potentiellement pour persistance ou backdoor).

2 Techniques MITRE T1021.001 + T1078.002

- T1021.001 : Remote Services: Remote Desktop Protocol
- T1078.002 : Valid Accounts: Domain Accounts
- Connexion RDP en Restricted Admin Mode (impersonation activée) depuis l'IP 41.x.x.x vers la machine cible

5 Conclusion

Ce laboratoire a permis de déployer une solution de supervision de la sécurité basée sur Wazuh, combinant efficacement les capacités SIEM et EDR au sein d'un environnement Cloud AWS multi-OS (Linux et Windows).

Le SIEM a assuré la collecte, la normalisation et la corrélation centralisée des journaux de sécurité, permettant la détection d'événements critiques tels que les tentatives d'authentification échouées et les accès non autorisés. En parallèle, l'EDR a fourni une visibilité approfondie au niveau des endpoints, notamment sur les élévations de privilèges, la création de comptes et les modifications des groupes à privilèges.

L'intégration des événements liés à l'IAM/PAM a mis en évidence l'importance du contrôle et de la traçabilité des identités et des accès à privilèges, éléments clés pour la détection d'abus internes et de phases de post-exploitation. La complémentarité entre SIEM, EDR et IAM/PAM constitue ainsi un socle essentiel pour renforcer la capacité de détection, d'analyse et de réponse aux incidents au sein d'un SOC moderne.