



# 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

# 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

	ID instance	Nom de l'instance	Etat	Type d'instance	Initialisation en cc	Afficher les alarm	Zone	URL	Version	
<input type="checkbox"/>	i-079919e8779447ec7	Windows-Client	En cours d'initialisation	t3.medium	Initialisation en cours	Afficher les alarmes	us-east-1a	ec2-3-238-62-106.com...	3.238.62.1	
<input checked="" type="checkbox"/>	i-06bac9b0f25505501	Wazuh-Server	En cours d'initialisation	t3.large	3/3 vérifications réussies	Afficher les alarmes	us-east-1d	ec2-3-84-81-131.compute-1.amazonaws.com...	3.84.81.1	
i-06bac9b0f25505501 (Wazuh-Server)										
<a href="#">Détails</a> <a href="#">Statuts et alarmes</a> <a href="#">Surveillance</a> <a href="#">Sécurité</a> <a href="#">Mise en réseau</a> <a href="#">Stockage</a> <a href="#">Balises</a>										
<b>Résumé de l'instance</b> <a href="#">Informations</a>										
ID d'instance <a href="#">i-06bac9b0f25505501</a>			Adresse IPv4 publique <a href="#">3.84.81.131   adresse ouverte</a>			Adresses IPv4 privées <a href="#">172.31.40.15</a>				
Adresse IPv6 -			État de l'instance <a href="#">En cours d'exécution</a>			DNS public <a href="#">ec2-3-84-81-131.compute-1.amazonaws.com   adresse ouverte</a>				
Type de nom d'hôte Nom de l'adresse IP: ip-172-31-40-15.ec2.internal			Nom DNS de l'IP privé (IPv4 uniquement) <a href="#">ip-172-31-40-15.ec2.internal</a>			Adresses IP élastiques -				
Réponse à un nom DNS de ressource privée IPv4 (A)			Type d'instance <a href="#">t3.large</a>			Adresses IP élastiques -				

##### EC2-2 : Linux Client

	ID instance	Nom de l'instance	Etat	Type d'instance	Initialisation en cc	Afficher les alarm	Zone	URL	Version	
<input checked="" type="checkbox"/>	i-02f739df471a7129f	Linux-Client	En cours d'initialisation	t3.micro	3/3 vérifications réussies	Afficher les alarmes	us-east-1a	ec2-3-238-107-162.com...	3.238.107	
<input type="checkbox"/>	i-079919e8779447ec7	Windows-Client	En cours d'initialisation	t3.medium	Initialisation en cours	Afficher les alarmes	us-east-1a	ec2-3-238-62-106.com...	3.238.62.1	
<input type="checkbox"/>	i-06bac9b0f25505501	Wazuh-Server	En cours d'initialisation	t3.large	3/3 vérifications réussies	Afficher les alarmes	us-east-1d	ec2-3-84-81-131.compute-1.amazonaws.com...	3.84.81.1	
i-02f739df471a7129f (Linux-Client)										
<a href="#">Détails</a> <a href="#">Statuts et alarmes</a> <a href="#">Surveillance</a> <a href="#">Sécurité</a> <a href="#">Mise en réseau</a> <a href="#">Stockage</a> <a href="#">Balises</a>										
<b>Résumé de l'instance</b> <a href="#">Informations</a>										
ID d'instance <a href="#">i-02f739df471a7129f</a>			Adresse IPv4 publique <a href="#">3.238.107.162   adresse ouverte</a>			Adresses IPv4 privées <a href="#">172.31.3.71</a>				
Adresse IPv6 -			État de l'instance <a href="#">En cours d'exécution</a>			DNS public <a href="#">ec2-3-238-107-162.compute-1.amazonaws.com   adresse ouverte</a>				
Type de nom d'hôte Nom de l'adresse IP: ip-172-31-3-71.ec2.internal			Nom DNS de l'IP privé (IPv4 uniquement) <a href="#">ip-172-31-3-71.ec2.internal</a>			Adresses IP élastiques -				
Réponse à un nom DNS de ressource privée IPv4 (A)			Type d'instance			Adresses IP élastiques -				

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.

The screenshot shows the Wazuh web interface. At the top, there is a large blue header with the Wazuh logo and tagline "The Open Source Security Platform". Below the header is a login form with fields for "Username" and "Password" and a "Log in" button. To the right of the login form is a large circular graphic featuring a blue hexagon with white code brackets "< / >" inside it. The main content area has a light gray background. At the top left, there is a navigation bar with icons for home, user profile, and search, followed by the text "wazuh." and a dropdown menu labeled "Modules". Below the navigation bar, there are five status indicators: "Total agents" (0), "Active agents" (0), "Disconnected agents" (0), "Pending agents" (0), and "Never connected agents" (0). A yellow banner below these indicators states "⚠️ No agents were added to this manager. [Add agent](#)". The interface is divided into several sections: "SECURITY INFORMATION MANAGEMENT" (Security events, Integrity monitoring), "AUDITING AND POLICY MONITORING" (Policy monitoring, System auditing, Security configuration assessment), "THREAT DETECTION AND RESPONSE" (Vulnerabilities, MITRE ATT&CK), and "REGULATORY COMPLIANCE" (PCI DSS, NIST 800-53).

## EC2-3 : Windows Client

The screenshot shows the AWS CloudWatch Metrics interface. At the top, there are two rows of metrics:

Windows-Client	i-079919e8779447ec7	En cours d'... (t3.medium)	Initialisation en cc (us-east-1a)	Afficher les alarm	ec2-3-238-62-106.com...	3.238.62.1
Wazuh-Server	i-06bac9b0f2550501	En cours d'... (t3.large)	3/3 vérifications r	Afficher les alarm	ec2-3-84-81-131.comp...	3.84.81.1

Below this, a specific metric for the Windows-Client instance is displayed:

i-079919e8779447ec7 (Windows-Client)

Détails | Statuts et alarmes | Surveillance | Sécurité | Mise en réseau | Stockage | Balises

▼ Résumé de l'instance Informations

ID d'instance	Adresse IPv4 publique	Adresses IPv4 privées
i-079919e8779447ec7	3.238.62.106   adresse ouverte	172.31.11.89
Adresse IPv6	État de l'instance	DNS public
-	En cours d'exécution	ec2-3-238-62-106.compute-1.amazonaws.com   adresse ouverte
Type de nom d'hôte	Nom DNS de l'IP privé (IPv4 uniquement)	Adresses IP élastiques
Nom de l'adresse IP: ip-172-31-11-89.ec2.internal	ip-172-31-11-89.ec2.internal	-
Réponse à un nom DNS de ressource privée	Type d'instance	
ip-172-31-11-89.ec2.internal	t3.medium	

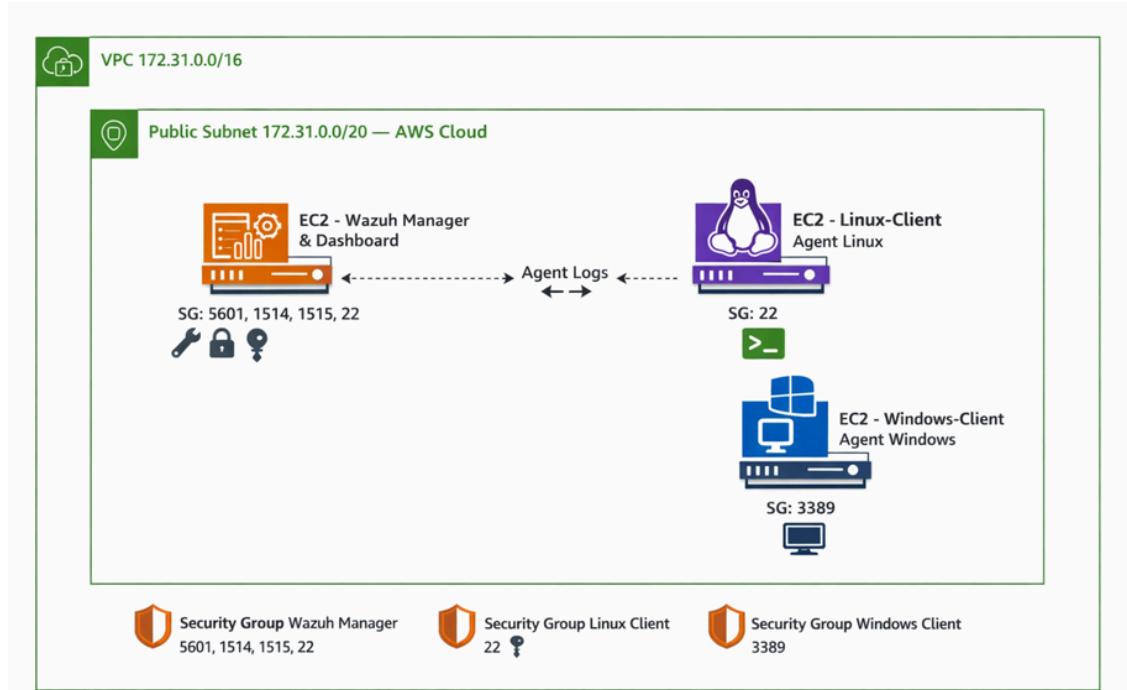
## 2.2 Configuration Réseau et Sécurité (Security Groups)

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 : même VPC	295801142161
-	sg-0582fbcc2d2bea8c4	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

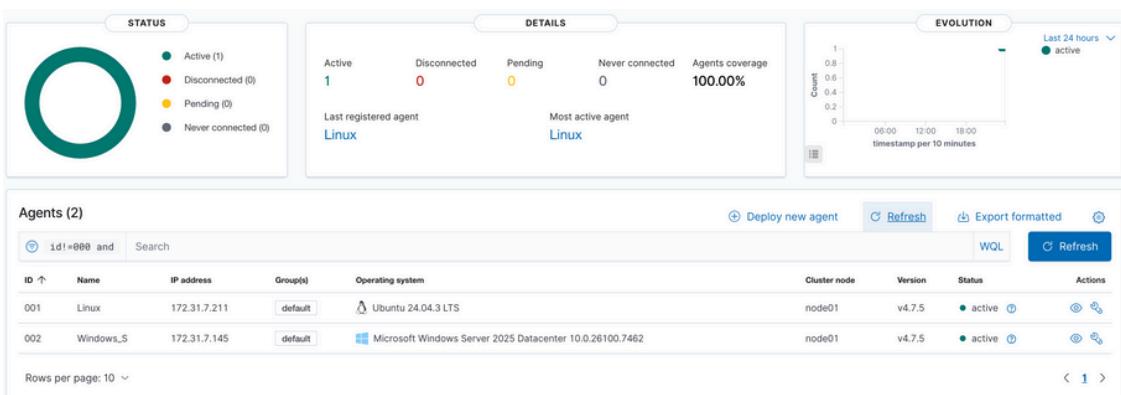
### 3.1 Installation du Serveur Wazuh

```
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.  
ubuntu@ip-172-31-44-110:~$ curl -s0 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 priviléges

#### 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:~$
```

**Valid Accounts**

ID: 001 Status: active IP address: 172.31.7.211 Version: Wazuh v4.7.5

**MITRE**

Initial Access: T1078, T1021

**Compliance**

Time	Technique(s)	Tactic(s)	Level	Rule ID	Description
Jan 1, 2026 00:06:48.01 6	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	5501	PAM: Login session opened.
Jan 1, 2026 00:06:43.97 8	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	5501	PAM: Login session opened.
Jan 1, 2026 00:06:42.97	T1078 T1021	Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	5715	sshd: authentication success.

**Events count evolution**

## 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: Wazuh a détecté l'ouverture de session privilégiée via PAM (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#
```

**Password Guessing**

Search DQL Last 24 hours Show dates Refresh

Time	Technique(s)	Tactic(s)	Level	Rule ID	Description
Jan 1, 2026 00:01:51.85 6	T1110.001 T1021.004	Credential Access, Lateral Movement	5	5710	sshd: Attempt to login using a non-existent user
Jan 1, 2026 00:01:51.66 3	T1110.001 T1021.004	Credential Access, Lateral Movement	5	5710	sshd: Attempt to login using a non-existent user
Dec 31, 2025 @ 23:59:27.51 3	T1110.001 T1021.004	Credential Access, Lateral Movement	5	5710	sshd: Attempt to login using a non-existent user
Dec 31, 2025 @ 23:59:25.51 1	T1110.001 T1021.004	Credential Access, Lateral Movement	5	5710	sshd: Attempt to login using a non-existent user
Dec 31, 2025 @ 23:59:23.50 9	T1110.001 T1021.004	Credential Access, Lateral Movement	5	5710	sshd: Attempt to login using a non-existent user
Dec 31, 2025 @ 23:59:19.70 0	T1110.001 T1021.004	Credential Access, Lateral Movement	5	5710	sshd: Attempt to login using a non-existent user

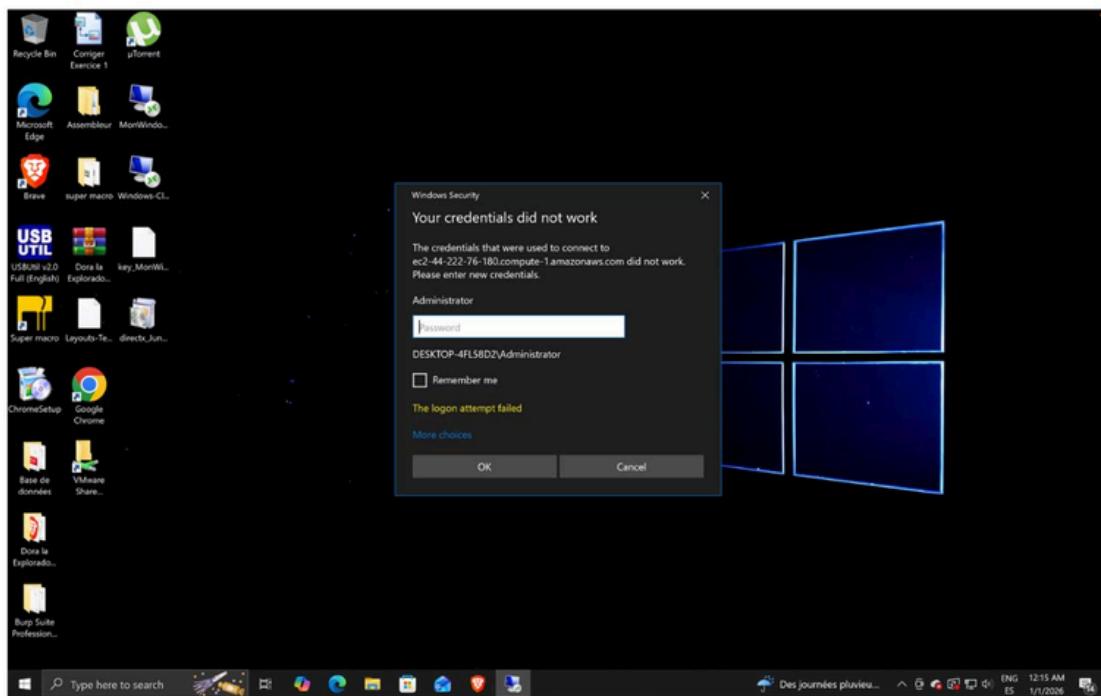
**Events count evolution**

## 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.

A screenshot of the Wazuh web interface. The top navigation bar includes 'wazuh.', 'Agents', and 'Windows-Client'. The main area is titled 'Valid Accounts' and shows 'Privilege Escalation', 'Defense Evasion', and 'Initial Access' under 'Version'. A 'Recent events' section displays 19 hits, with a search bar, DQL filter, and time range ('Last 24 hours'). Below this is a table of log entries:

Time	Technique(s)	Tactic(s)	Level	Rule ID	Description
Jan 1, 2026 00:17:26.02 6	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	60106	Windows logon success.
Jan 1, 2026 00:17:24.42 1	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	60106	Windows logon success.
Jan 1, 2026 00:17:23.34 7	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	60106	Windows logon success.
Jan 1, 2026 00:17:22.75 5	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	3	60106	Windows logon success.

A chart titled 'Events count evolution' is also present on the left side of the interface.

## 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) :

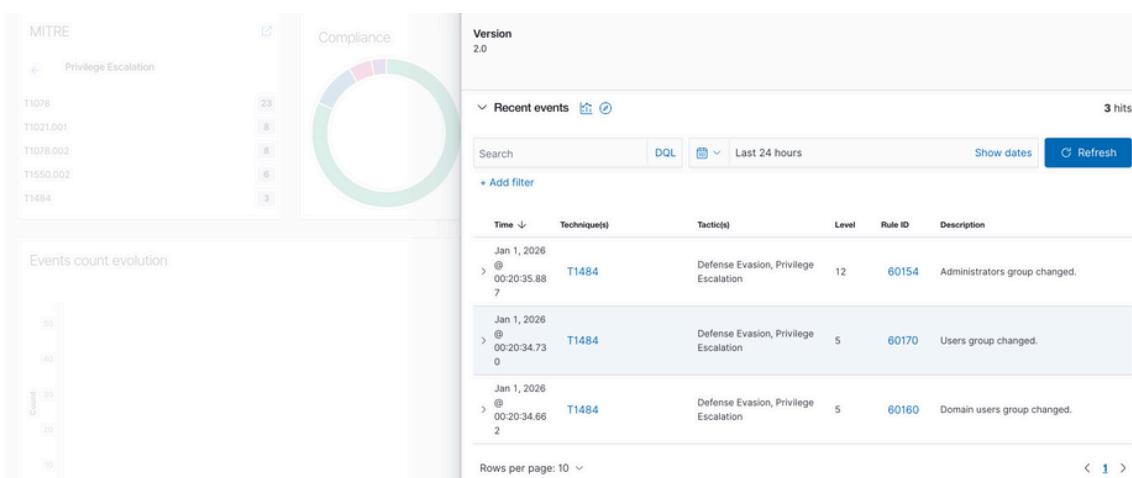
- Règle ID 60154 : "Administrators group changed".
- Règle ID 60170 : "Users group changed".

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>
```



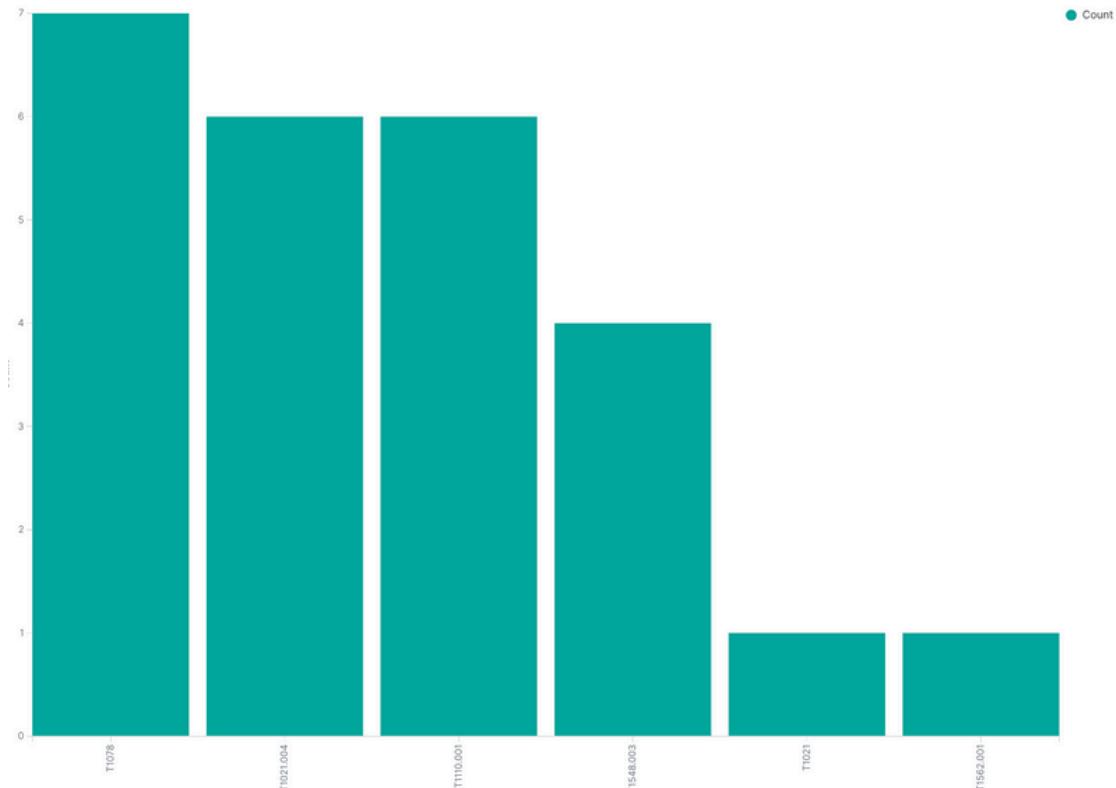
## 5 Security Monitoring et Threat Detection

### 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.

Jan 1, 2026 0:00:01:51.856	
agent.name:	linux rule.mitre.technique: Password Guessing, SSH predecoder.program_name: sshd predecoder.timestamp: 2025-12-31T23:01:51.732610+00:00 input.type: log agent.ip: 172.31.7.211 agent.id: 001 data.srouser: fakeuser data.srchip: 41 data.srport: 51318 manager.name: ip-172-31-44-110 rule.mail: false rule.level: 5 rule.hipas: 164.312.b rule.pci_dss: 10.2.4, 10.2.5, 10.6.1 rule.ttc: C06.1, C06.8, C07.2, C07.3 rule.description: sshd: Attempt to login using a non-existent user rule.groups: syslog, sshd, authentication_failed, invalid_login rule.mist.B88_53: AU.14, AC.7, AU.6 rule.gdr: IV.35.7.d, IV.32.2 rule.firetimes: 2 rule.mitre.id: T1110.001, T1021.004 rule.mitre.tactic: Credential Access, Lateral Movement rule.id: 5719 rule.gpg13: 7.1 location: /var/log/auth.log decoder.parent: sshd decoder.name: sshd id: 176722111.24646 Geolocation.city.name: Casablanca Geolocation.country.name: Morocco Geolocation.region.name: Casablanca Geolocation.location: { "lon": -7.6184, "lat": 33.5922 } full_log: 2025-12-
View surrounding documents View single document	

Table	JSON
r GeoLocation.city_name	Casablanca
r GeoLocation.country_name	Morocco
o GeoLocation.location	{ "lon": -7.6184, "lat": 33.5922 }
r GeoLocation.region_name	Casablanca
r _index	wazuh-alerts-4.x-2025.12.31
r agent.id	001
r agent.ip	172.31.7.211
r agent.name	linux
r data.srchip	41.
r data.srport	51318
r data.srouser	fakeuser
r decoder.name	sshd
r decoder.parent	sshd
r full_log	2025-12-31T23:01:51.732610+00:00 ip-172-31-7-211 sshd[3406]: Invalid user fakeuser from 41. port 51318
r id	176722111.24646
r input.type	log
r location	/var/log/auth.log

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

agent.name: Windows\_S X rule.mitre.id: T1484 X + Add filter

## Détail de l'alerte

Jan 1, 2026 @ 09:29:35.887																																														
agent.name: Windows_5 rule.mitre.id: T144 input.type: log agent.ip: 172.31.7.145 agent.id: 002 manager.name: ip-172-31-44-110 data.win.eventdata.subjectLogonId: 0x41fd6b data.win.eventdata.targetUserName: Administrators data.win.eventdata.memberSid: S-1-5-21-1267691158-3860027324-3782535310-1000 data.win.eventdata.subjectUserId: S-1-5-21-1267691158-3860027324-3782535310-500 data.win.eventdata.subjectDomainName: BuiltIn data.win.eventdata.targetSid: S-1-5-32-544 data.win.eventdata.subjectUserName: Administrator data.win.system.eventID: 4732 data.win.system.keywords: 0x8020000000000000 data.win.system.providerGuid: {5449625-5476-4994-a8b-3e3b0328c3d4} data.win.system.level: 0 data.win.system.channel: Security data.win.system.opcode: 0 data.win.system.message: "A member was added to a security-enabled local group. Subject: Security ID: S-1-5-21-1267691158-3860027324-3782535310-500 Account Name: Administrator Account Domain: EC2AMA2-PI16E9XK Logon ID: 0x41fd6b Member: Security ID: S-1-5-21-1267691158-3860027324-3782535310-1000																																														
Expanded document																																														
Table	JSON																																													
<table border="1"> <tr> <td>↑ _index</td><td>wazuh-alerts-4.x-2025.12.31</td></tr> <tr> <td>↑ agent.id</td><td>002</td></tr> <tr> <td>↑ agent.ip</td><td>172.31.7.145</td></tr> <tr> <td>↑ agent.name</td><td>Windows_5</td></tr> <tr> <td>○ data.win.eventdata.memberSid</td><td>△ S-1-5-21-1267691158-3860027324-3782535310-1000</td></tr> <tr> <td>○ data.win.eventdata.subjectDomainName</td><td>△ EC2AMA2-PI16E9XK</td></tr> <tr> <td>○ data.win.eventdata.subjectLogonId</td><td>△ 0x41fd6b</td></tr> <tr> <td>○ data.win.eventdata.subjectUserName</td><td>△ Administrator</td></tr> <tr> <td>○ data.win.eventdata.subjectUserSid</td><td>△ S-1-5-21-1267691158-3860027324-3782535310-500</td></tr> <tr> <td>○ data.win.eventdata.targetDomainName</td><td>△ BuiltIn</td></tr> <tr> <td>○ data.win.eventdata.targetSid</td><td>△ S-1-5-32-544</td></tr> <tr> <td>○ data.win.eventdata.targetUserName</td><td>△ Administrators</td></tr> <tr> <td>○ data.win.system.channel</td><td>△ Security</td></tr> <tr> <td>○ data.win.system.computer</td><td>△ EC2AMA2-PI16E9XK</td></tr> <tr> <td>○ data.win.system.eventID</td><td>△ 4732</td></tr> <tr> <td>○ data.win.system.eventRecordID</td><td>△ 84773</td></tr> <tr> <td>○ data.win.system.keywords</td><td>△ 0x8020000000000000</td></tr> <tr> <td>○ data.win.system.level</td><td>△ 0</td></tr> <tr> <td>○ data.win.system.message</td><td>△ A member was added to a security-enabled local group.</td></tr> <tr> <td>Subject:</td><td></td></tr> <tr> <td>    Security ID:</td><td>S-1-5-21-1267691158-3860027324-3782535310-500</td></tr> <tr> <td>    Account Name:</td><td>Administrator</td></tr> <tr> <td>    Account Domain:</td><td>EC2AMA2-PI16E9XK</td></tr> </table>	↑ _index	wazuh-alerts-4.x-2025.12.31	↑ agent.id	002	↑ agent.ip	172.31.7.145	↑ agent.name	Windows_5	○ data.win.eventdata.memberSid	△ S-1-5-21-1267691158-3860027324-3782535310-1000	○ data.win.eventdata.subjectDomainName	△ EC2AMA2-PI16E9XK	○ data.win.eventdata.subjectLogonId	△ 0x41fd6b	○ data.win.eventdata.subjectUserName	△ Administrator	○ data.win.eventdata.subjectUserSid	△ S-1-5-21-1267691158-3860027324-3782535310-500	○ data.win.eventdata.targetDomainName	△ BuiltIn	○ data.win.eventdata.targetSid	△ S-1-5-32-544	○ data.win.eventdata.targetUserName	△ Administrators	○ data.win.system.channel	△ Security	○ data.win.system.computer	△ EC2AMA2-PI16E9XK	○ data.win.system.eventID	△ 4732	○ data.win.system.eventRecordID	△ 84773	○ data.win.system.keywords	△ 0x8020000000000000	○ data.win.system.level	△ 0	○ data.win.system.message	△ A member was added to a security-enabled local group.	Subject:		Security ID:	S-1-5-21-1267691158-3860027324-3782535310-500	Account Name:	Administrator	Account Domain:	EC2AMA2-PI16E9XK
↑ _index	wazuh-alerts-4.x-2025.12.31																																													
↑ agent.id	002																																													
↑ agent.ip	172.31.7.145																																													
↑ agent.name	Windows_5																																													
○ data.win.eventdata.memberSid	△ S-1-5-21-1267691158-3860027324-3782535310-1000																																													
○ data.win.eventdata.subjectDomainName	△ EC2AMA2-PI16E9XK																																													
○ data.win.eventdata.subjectLogonId	△ 0x41fd6b																																													
○ data.win.eventdata.subjectUserName	△ Administrator																																													
○ data.win.eventdata.subjectUserSid	△ S-1-5-21-1267691158-3860027324-3782535310-500																																													
○ data.win.eventdata.targetDomainName	△ BuiltIn																																													
○ data.win.eventdata.targetSid	△ S-1-5-32-544																																													
○ data.win.eventdata.targetUserName	△ Administrators																																													
○ data.win.system.channel	△ Security																																													
○ data.win.system.computer	△ EC2AMA2-PI16E9XK																																													
○ data.win.system.eventID	△ 4732																																													
○ data.win.system.eventRecordID	△ 84773																																													
○ data.win.system.keywords	△ 0x8020000000000000																																													
○ data.win.system.level	△ 0																																													
○ data.win.system.message	△ A member was added to a security-enabled local group.																																													
Subject:																																														
Security ID:	S-1-5-21-1267691158-3860027324-3782535310-500																																													
Account Name:	Administrator																																													
Account Domain:	EC2AMA2-PI16E9XK																																													

- 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.firetimes         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
# rule.id                60154
# rule.level              12
Q 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

> Jan 1, 2026 @ 00:17:44.946	agent.name: Windows-Client rule.mitre.id: <b>T1098</b> input.type: log agent.ip: 172.31.4.70 agent.id: 002 manager.name: ip-172-31-46-35 data.win.eventdata.subjectLogonId: 0xb69387 data.win.eventdata.scriptPath: %1793 data.win.eventdata.passwordLastSet: %1794 data.win.eventdata.homeDirectory: %1793 data.win.eventdata.userParameters: %1793 data.win.eventdata.subjectDomainName: EC2AMAZ-SILQ1NQ data.win.eventdata.displayName: %1793 data.win.eventdata.accountExpires: %1794 data.win.eventdata.homePath: %1793 data.win.eventdata.samAccountName: labuser data.win.eventdata.targetUserName: labuser data.win.eventdata.subjectUserId: S-1-5-21-887713911-3399705033-550558572-1000
> Jan 1, 2026 @ 00:17:44.946	agent.name: Windows-Client rule.mitre.id: <b>T1098</b> input.type: log agent.ip: 172.31.4.70 agent.id: 002 manager.name: ip-172-31-46-35 data.win.eventdata.subjectLogonId: 0xb69387 data.win.eventdata.scriptPath: %1793 data.win.eventdata.passwordLastSet: %1794 data.win.eventdata.homeDirectory: %1793 data.win.eventdata.userParameters: %1793 data.win.eventdata.subjectDomainName: EC2AMAZ-SILQ1NQ data.win.eventdata.displayName: %1793 data.win.eventdata.accountExpires: %1794 data.win.eventdata.homePath: %1793 data.win.eventdata.samAccountName: labuser data.win.eventdata.targetUserName: labuser data.win.eventdata.subjectUserId: S-1-5-21-887713911-3399705033-550558572-1000
> Jan 1, 2026 @ 00:17:23.424	agent.name: Windows-Client rule.mitre.id: T1021.001, <b>T1078.002</b> input.type: log agent.ip: 172.31.4.70 agent.id: 002 manager.name: ip-172-31-46-35 data.win.eventdata.subjectLogonId: 0x2e7 data.win.eventdata.restrictedAdminMode: %1843 data.win.eventdata.subjectDomainName: WORKGROUP data.win.eventdata.targetGetLogonId: 0x0 data.win.eventdata.impersonationLevel: %1833 data.win.eventdata.ipAddress: 41.141.26.111 data.win.eventdata.authenticationPackageName: Negotiate data.win.eventdata.workstationName: EC2AMAZ-SILQ1NQ data.win.eventdata.targetLogonId: 0xaed92f8 data.win.eventdata.logonProcessName: User32 data.win.eventdata.logonGuid: {00000000-0000-0000-0000-000000000000}
> Jan 1, 2026 @ 00:17:26	agent.name: Windows-Client rule.mitre.id: T1550.002, <b>T1078.002</b> , T1021.001 input.type: log agent.ip: 172.31.4.70 agent.id: 002 manager.name: ip-172-31-46-35 data.win.eventdata.subjectLogonId: 0x0 data.win.eventdata.targetGetLogonId: 0x0 data.win.eventdata.impersonationLevel: %1833 data.win.eventdata.ipAddress: data.win.eventdata.authenticationPackageName: NTLM data.win.eventdata.workstationName: DESKTOP-4FL58D2 data.win.eventdata.logonProcessName: NTLMSP data.win.eventdata.logonGuid: {00000000-0000-0000-0000-000000000000} data.win.eventdata.targetUserName: Administrator data.win.eventdata.keyLength: 128

## 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.