

# Projet de Fin Module

## Implémentation du Atelier Sécurité

**Projet de Atelier Sécurité des endpoints  
et supervision SIEM**

Réalisé par :  
Abdelali Saadali

Encadré par :  
Prof. Azeddine KHIAT

Année universitaire : 2025/2026

## **Introduction**

Dans un contexte marqué par l'augmentation des cyberattaques ciblant les infrastructures Cloud et les systèmes hétérogènes, la mise en place de solutions de supervision et de détection centralisées devient indispensable. Les entreprises modernes s'appuient de plus en plus sur des plateformes SIEM et EDR afin de garantir la visibilité, la traçabilité et la détection proactive des incidents de sécurité.

Ce projet s'inscrit dans cette logique et consiste à la mise en œuvre d'une architecture de supervision de la sécurité des endpoints basée sur Wazuh, combinant les fonctionnalités SIEM (Security Information and Event Management) et EDR (Endpoint Detection and Response). Le lab a été déployé dans un environnement AWS Learner Lab, intégrant des systèmes Linux et Windows, afin de simuler un environnement réel multi-OS.

L'objectif principal est d'observer, centraliser et analyser en temps réel les événements de sécurité générés sur différents hôtes, tout en illustrant les concepts de sécurité des endpoints, gestion des identités et des accès (IAM/PAM) et threat detection / threat hunting.

# 1. Architecture générale du lab :

L'architecture du lab repose sur une infrastructure Cloud simple mais réaliste, composée de trois instances EC2 déployées dans le même VPC AWS.

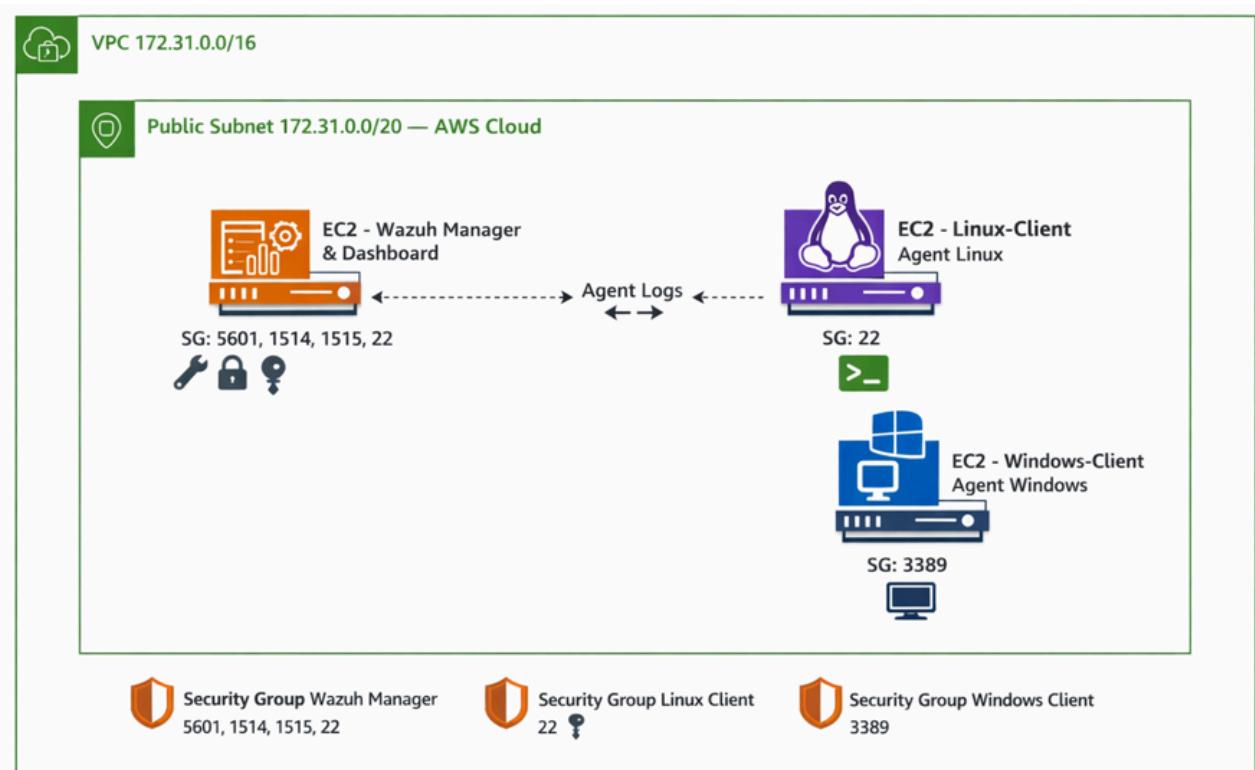
## 1.1 Composants de l'architecture :

- EC2-1 : Serveur Wazuh (Ubuntu 24.04 LTS)
  - Wazuh Manager
  - Wazuh Indexer
  - Wazuh Dashboard
  - Rôle : centralisation, corrélation, analyse et visualisation des événements
- EC2-2 : Client Linux (Ubuntu 24.04)
  - Wazuh Agent
  - Rôle : génération d'événements Linux (authentification, priviléges, intégrité)
- EC2-3 : Client Windows (Windows Server)
  - Wazuh Agent
  - Rôle : génération d'événements Windows Security et EDR

## 1.2 Flux réseau :

Les communications entre les composants sont basées sur les ports standards Wazuh :

- 1514/TCP : communication agent → serveur
- 1515/TCP : enrôlement automatique des agents
- 443/TCP (ou 5601) : accès au Dashboard Wazuh



## 2. Mise en place de l'environnement AWS :

Les trois instances EC2 ont été déployées dans le même VPC et le même subnet afin de garantir la communication directe entre les agents et le serveur Wazuh.

Un Security Group dédié a été configuré pour restreindre strictement les accès réseau, conformément aux bonnes pratiques de sécurité Cloud (principe du moindre privilège).

Accès SSH et RDP limités à l'adresse IP de l'administrateur

Ouverture des ports Wazuh uniquement entre les clients et le serveur

Cette configuration permet de simuler un environnement sécurisé proche d'un contexte professionnel.

### 2.1 Les instances :

The screenshot shows the AWS EC2 Instances page. The left sidebar includes sections for Tableau de bord, Vue globale EC2, Événements, Instances (with sub-options like Instances, Modèles de lancement, Demande Spot, Savings Plans, Instances réservées, Hôtes dédiés, Réservations de capacité, Capacity Manager), Images (AMI, Catalogue des AMI), Elastic Block Store (Volumes, Instantanés, Gestionnaire de cycle de vie), and Réseau et sécurité (Groupes de sécurité). The main content area displays a table of instances:

| Name           | ID d'instance       | État de l'instance | Type d'instance | Contrôle des statu...  | Statut d'alarm...     | Zone de dispon... | DNS IPv4 pub... |
|----------------|---------------------|--------------------|-----------------|------------------------|-----------------------|-------------------|-----------------|
| tp7_ubuntu     | i-0edd87afc45e14be  | Arrêté(e)          | t2.micro        | -                      | Afficher les alarm... | us-east-1d        | -               |
| Linux-Client   | i-05165e59f799434e  | En cours d'...     | t2.micro        | 2/2 vérifications r... | Afficher les alarm... | us-east-1d        | ec2-18-209-4... |
| Windows-Client | i-05c34d918b1ef3e5b | En cours d'...     | t3.medium       | Initialisation en cc   | Afficher les alarm... | us-east-1b        | ec2-44-222-7... |
| MonWindowsS... | i-0886a80494088e8cf | Arrêté(e)          | t3.medium       | -                      | Afficher les alarm... | us-east-1f        | -               |
| ubuntu_tp      | i-08c150de843e1b895 | Arrêté(e)          | t3.micro        | -                      | Afficher les alarm... | us-east-1f        | -               |
| LINUX_MACHINE  | i-0f7812512574acdd8 | Arrêté(e)          | t3.micro        | -                      | Afficher les alarm... | us-east-1f        | -               |
| Wazuh-Server   | i-0f281587151159099 | En cours d'...     | t3.large        | 3/3 vérifications r... | Afficher les alarm... | us-east-1a        | ec2-100-30-2... |

### 2.2 Groupe de sécurité :

The screenshot shows the AWS Security Groups page. The left sidebar includes sections for Modèles de lancement, Demande Spot, Savings Plans, Instances réservées, Hôtes dédiés, Réservations de capacité, Capacity Manager, Images (AMI, Catalogue des AMI), Elastic Block Store (Volumes, Instantanés, Gestionnaire de cycle de vie), Réseau et sécurité (Groupes de sécurité, Adresses IP élastiques, Groupes de placement, Paires de clés, Interfaces réseau), and Équilibrage de charge (Équilibreurs de charge, Groupes cibles, Trust Stores). The main content area displays a table of security groups:

| Name | ID du groupe de sécurité | Nom du groupe de sécurité | ID de VPC             | Description            |
|------|--------------------------|---------------------------|-----------------------|------------------------|
| -    | sg-029c16376f0bed81e     | launch-wizard-7           | vpc-01a45b7ea1008e2d8 | launch-wizard-7 cre... |
| -    | sg-0877943d223bf718f     | launch-wizard-2           | vpc-01a45b7ea1008e2d8 | launch-wizard-2 cre... |
| -    | sg-06de6bff59814901b     | launch-wizard-4           | vpc-01a45b7ea1008e2d8 | launch-wizard-4 cre... |
| -    | sg-07cf830c51d72605b     | SG-Clients                | vpc-01a45b7ea1008e2d8 | Linux & Windows cli... |
| -    | sg-0dc036b153ade201      | launch-wizard-5           | vpc-01a45b7ea1008e2d8 | launch-wizard-5 cre... |
| -    | sg-02c830e3a5730ac1a     | launch-wizard-1           | vpc-01a45b7ea1008e2d8 | launch-wizard-1 cre... |
| -    | sg-025eeef44b4dc5085     | launch-wizard-8           | vpc-01a45b7ea1008e2d8 | launch-wizard-8 cre... |
| -    | sg-05021d5c668013695     | default                   | vpc-01a45b7ea1008e2d8 | default VPC security   |
| -    | sg-03d1a78b186f71dce     | launch-wizard-3           | vpc-01a45b7ea1008e2d8 | launch-wizard-3 cre... |
| -    | sg-0d71b3062912f6571     | launch-wizard-6           | vpc-01a45b7ea1008e2d8 | launch-wizard-6 cre... |
| -    | sg-08ccf2e64641ff701     | SG-Wazuh-Server           | vpc-01a45b7ea1008e2d8 | sg du wazuh            |

## 2.2.1 Groupe de sécurité des clients (Linux + Windows) :

The screenshot shows the AWS EC2 Groups page for the security group "sg-07cf830c51d72605b - SG-Clients". The "Règles entrantes" tab is selected, displaying two rules:

| ID de règle de groupe | Version IP | Type | Protocole | Plage de ports | Source | Description |
|-----------------------|------------|------|-----------|----------------|--------|-------------|
| sgr-0d1faa41d2e7f3d2c | IPv4       | SSH  | TCP       | 22             | 41.1   | ssh         |
| sgr-0d21bab8594eb5cf3 | IPv4       | RDP  | TCP       | 3389           | 41.1   | RDP         |

### 2.2.1.1 Client Linux :

The screenshot shows the AWS EC2 Instances page for the instance "i-05165e59f7a99434e (Linux-Client)". The "Actions" dropdown menu is open, showing the "Lancer des instances" option.

**Instances (1/7) Informations**

| Name                | ID d'instance              | État de l'instance    | Type d'instance | Contrôle des statu...         | Statut d'alarme              | Zone de dispon... | DNS IPv4 pub...        |
|---------------------|----------------------------|-----------------------|-----------------|-------------------------------|------------------------------|-------------------|------------------------|
| tp7_ubuntu          | i-0e0dd87afc45e14be        | Arrêté(e)             | t2.micro        | -                             | Afficher les alarm...        | us-east-1d        | -                      |
| <b>Linux-Client</b> | <b>i-05165e59f7a99434e</b> | <b>En cours d'...</b> | <b>t2.micro</b> | <b>2/2 vérifications r...</b> | <b>Afficher les alarm...</b> | <b>us-east-1d</b> | <b>ec2-18-209-4...</b> |
| Windows-Client      | i-05c34d918b1ef3e5b        | En cours d'...        | t3.medium       | 3/3 vérifications r...        | Afficher les alarm...        | us-east-1b        | ec2-44-222-7...        |
| MonWindowsS...      | i-088ea80494088e8cf        | Arrêté(e)             | t3.medium       | -                             | Afficher les alarm...        | us-east-1f        | -                      |
| ubuntu_tp           | i-08c150de843e1b895        | Arrêté(e)             | t3.micro        | -                             | Afficher les alarm...        | us-east-1f        | -                      |
| LINUX_MACHINE       | i-0f7812512574acdd8        | Arrêté(e)             | t3.micro        | -                             | Afficher les alarm...        | us-east-1f        | -                      |
| Wazuh-Server        | i-0f281587151159099        | En cours d'...        | t3.large        | 3/3 vérifications r...        | Afficher les alarm...        | us-east-1a        | ec2-100-30-2...        |

**i-05165e59f7a99434e (Linux-Client)**

**Règles entrantes**

| Nom | ID de règle du groupe de... | Plage de ports | Protocole | Source | Groupes de sécurité |
|-----|-----------------------------|----------------|-----------|--------|---------------------|
| -   | sgr-0d1faa41d2e7f3d2c       | 22             | TCP       | 41.1   | SG-Clients ↗        |
| -   | sgr-0d21bab8594eb5cf3       | 3389           | TCP       | 41.1   | SG-Clients ↗        |

**Règles sortantes**

## 2.2.1.1 Client Windows :

The screenshot shows the AWS EC2 Instances page. A green banner at the top indicates that security groups for the instance have been modified. The main table lists seven instances, with 'Windows-Client' being the selected one. Below the table, a detailed view for 'Windows-Client' shows its security group rules, which include two inbound rules from '41.1' (TCP port 22) and one outbound rule to '41.1' (TCP port 3389). The left sidebar contains links for various EC2 services like Instances, Images, and Elastic Block Store.

## 2.2.2 Groupe de sécurité du serveur Wazuh :

The screenshot shows the AWS Groups page for the security group 'sg-08ccf2e64641ff701 - SG-Wazuh-Server'. The 'Règles entrantes' tab is selected, displaying four inbound rules: TCP port 1514 (tcp-07cf830c51d72605b...), TCP port 1515 (sg-07cf830c51d72605b...), SSH (TCP port 22, 41.1 ssh), and HTTPS (TCP port 443, 41.1 https). The left sidebar lists various AWS services like EC2, Images, and Elastic Block Store.

The screenshot shows the AWS Management Console with the EC2 service selected. The left sidebar has sections for Tableau de bord, Vue globale EC2, Événements, Instances (selected), Types d'instances, Modèles de lancement, Demandes Spot, Savings Plans, Instances réservées, Hôtes dédiés, Réservations de capacité, Capacity Manager, Images (AMI), Elastic Block Store (Volumes, Instantanés, Gestionnaire de cycle de vie), and Réseau et sécurité (Groupes de sécurité). The main content area displays a table of instances with columns for Name, ID d'instance, État de l'instance, Type d'instance, Contrôle des statut, Statut d'alarme, Zone de disponibilité, and DNS IPv4 pub. The Wazuh-Server instance (i-0f281587151159099) is selected and its details are shown in the right panel, including its security group rules.

### 3. Installation de la plateforme Wazuh :

La plateforme Wazuh a été installée en mode All-in-One sur une instance Ubuntu 24.04. Cette installation regroupe le manager, l'indexer et le dashboard sur une seule machine, ce qui est adapté à un lab pédagogique.

Une fois l'installation terminée, l'accès au Dashboard Wazuh a permis de vérifier le bon fonctionnement des services et de commencer l'enrôlement des agents.

#### 3.1 Connection ssh + mise a jour au système :

```
mac@MacBook-Pro-de-Abdelali Projet_de_fin_module % ssh -i key-Wazuh-Server.pem ubuntu@100.30.218.189
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)

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

System information as of Wed Dec 31 20:57:41 UTC 2025

  System load:  0.0              Temperature:      -273.1 C
  Usage of /:   6.2% of 28.02GB  Processes:          111
  Memory usage: 3%              Users logged in:   0
  Swap usage:   0%              IPv4 address for ens5: 172.31.46.35

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 comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-46-35:~$ sudo apt update && sudo apt -y upgrade
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
[Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
```

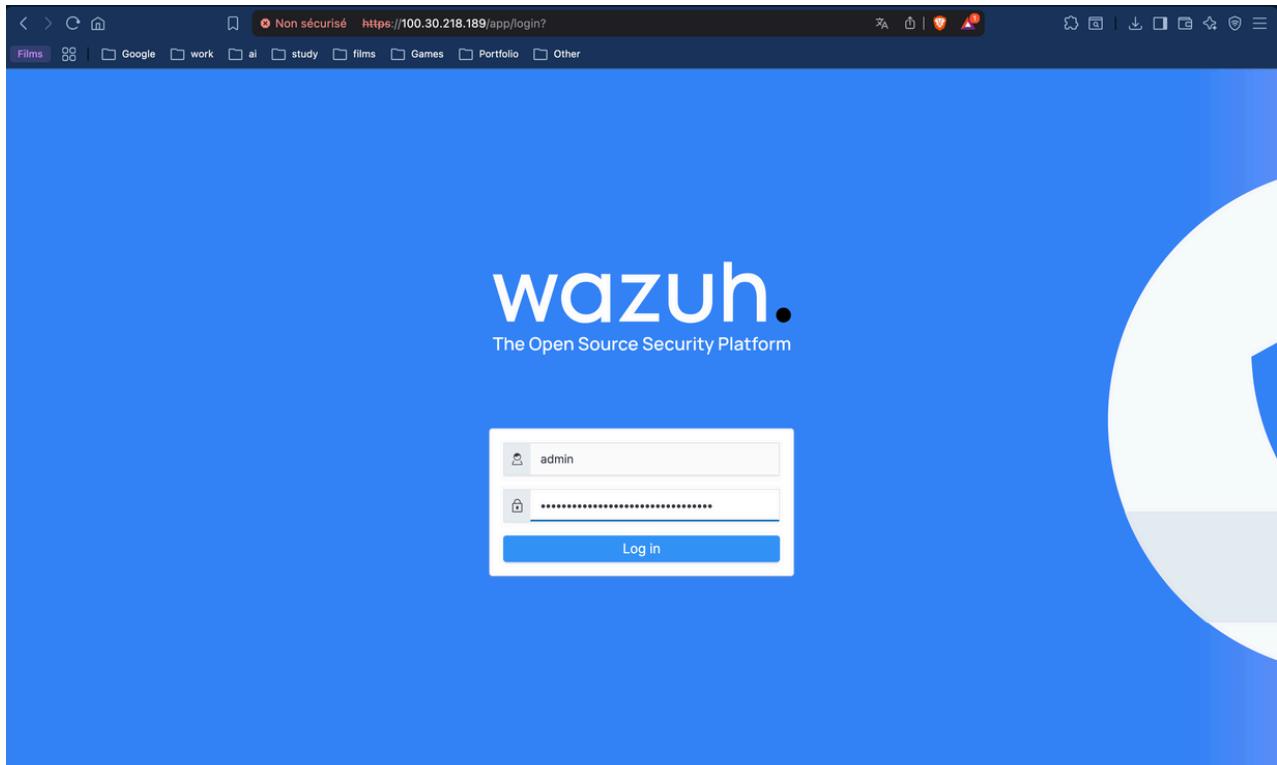
### 3.2 Installation du wazuh :

```
[ubuntu@ip-172-31-46-35:~$ sudo bash wazuh-install.sh -a -i
31/12/2025 21:01:14 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.5
31/12/2025 21:01:14 INFO: Verbose logging redirected to /var/log/wazuh-install.log
31/12/2025 21:01:24 WARNING: Hardware and system checks ignored.
31/12/2025 21:01:30 INFO: Wazuh web interface port will be 443.
31/12/2025 21:01:30 INFO: --- Dependencies ---
31/12/2025 21:01:30 INFO: Installing apt-transport-https.
31/12/2025 21:01:30 INFO: Wazuh repository added.
31/12/2025 21:01:36 INFO: --- Configuration files ---
31/12/2025 21:01:36 INFO: Generating configuration files.
31/12/2025 21:01:38 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
31/12/2025 21:01:39 INFO: --- Wazuh indexer ---
31/12/2025 21:01:39 INFO: Starting Wazuh indexer installation.
31/12/2025 21:02:44 INFO: Wazuh indexer installation finished.
31/12/2025 21:02:44 INFO: Wazuh indexer post-install configuration finished.
31/12/2025 21:02:44 INFO: Starting service wazuh-indexer.
31/12/2025 21:03:05 INFO: wazuh-indexer service started.
31/12/2025 21:03:05 INFO: Initializing Wazuh indexer cluster security settings.
31/12/2025 21:03:16 INFO: Wazuh indexer cluster initialized.
31/12/2025 21:03:16 INFO: --- Wazuh server ---
31/12/2025 21:03:16 INFO: Starting the Wazuh manager installation.
31/12/2025 21:04:12 INFO: Wazuh manager installation finished.
31/12/2025 21:04:12 INFO: Starting service wazuh-manager.
31/12/2025 21:04:28 INFO: wazuh-manager service started.
31/12/2025 21:04:28 INFO: Starting Filebeat installation.
31/12/2025 21:04:38 INFO: Filebeat installation finished.
31/12/2025 21:04:38 INFO: Filebeat post-install configuration finished.
31/12/2025 21:04:38 INFO: Starting service filebeat.
31/12/2025 21:04:40 INFO: filebeat service started.
31/12/2025 21:04:40 INFO: --- Wazuh dashboard ---
31/12/2025 21:04:40 INFO: Starting Wazuh dashboard installation.
31/12/2025 21:05:26 INFO: Wazuh dashboard installation finished.
31/12/2025 21:05:26 INFO: Wazuh dashboard post-install configuration finished.
31/12/2025 21:05:26 INFO: Starting service wazuh-dashboard.
31/12/2025 21:05:26 INFO: wazuh-dashboard service started.
31/12/2025 21:06:04 INFO: Initializing Wazuh dashboard web application.
31/12/2025 21:06:05 INFO: Wazuh dashboard web application initialized.
31/12/2025 21:06:05 INFO: --- Summary ---
31/12/2025 21:06:05 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
      User: admin
      Password: v3lN87G7aytg5ZnCUZY9vN+Zztj4NzwA
31/12/2025 21:06:05 INFO: Installation finished.
ubuntu@ip-172-31-46-35:~$ ]
```

### 3.3 Verification :

```
Projet_de_fin_module — ubuntu@ip-172-31-46-35: ~ — ssh -i key-Wazuh...
[ubuntu@ip-172-31-46-35:~$ sudo systemctl status wazuh-manager
sudo systemctl status wazuh-indexer
[sudo systemctl status wazuh-dashboard
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; pr>
     Active: active (running) since Wed 2025-12-31 21:04:28 UTC; 4min 28s ago
       Tasks: 121 (limit: 9296)
      Memory: 377.0M (peak: 525.2M)
        CPU: 45.244s
      CGroup: /system.slice/wazuh-manager.service
              └─58573 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr>
                ├─58612 /var/ossec/bin/wazuh-authd
                ├─58625 /var/ossec/bin/wazuh-db
                ├─58634 /var/ossec/bin/wazuh-execd
                ├─58645 /var/ossec/bin/wazuh-analysisd
                ├─58670 /var/ossec/bin/wazuh-syscheckd
                ├─58716 /var/ossec/bin/wazuh-remoted
                ├─58749 /var/ossec/bin/wazuh-logcollector
                ├─58769 /var/ossec/bin/wazuh-monitord
                ├─58771 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr>
                ├─58774 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr>
                ├─58777 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr>
                └─58800 /var/ossec/bin/wazuh-modulesd
```

### 3.4 Login :



### 3.4 Dashboard :

A screenshot of the Wazuh dashboard. At the top, there are statistics: Total agents (0), Active agents (0), Disconnected agents (0), Pending agents (0), and Never connected agents (0). A message says "No agents were added to this manager. Add agent". The dashboard is divided into four main sections: SECURITY INFORMATION MANAGEMENT, AUDITING AND POLICY MONITORING, THREAT DETECTION AND RESPONSE, and REGULATORY COMPLIANCE. Each section contains two cards with icons and descriptions.

## 4. Enrôlement des agents Linux et Windows :

### 4.1 Agent Linux :

L'agent Wazuh a été déployé sur le client Linux via la fonctionnalité “Deploy new agent” du Dashboard.

Après installation, l'agent apparaît comme actif et connecté, confirmant la bonne communication avec le serveur.

The screenshot shows the Wazuh Dashboard with the 'Agents' tab selected. A modal window titled 'Deploy new agent' is open, guiding the user through the deployment process:

- Select the package to download and install on your system:**
  - LINUX**:
    - RPM amd64
    - RPM aarch64
    - DEB amd64** (selected)
    - DEB aarch64
  - WINDOWS**:
    - MSI 32/64 bits
  - macOS**:
    - Intel
    - Apple silicon

For additional systems and architectures, please check our documentation.
- Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address: 172.31.46.35
- Optional settings:**

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: Linux-Client

The agent name must be unique. It can't be changed once the agent has been enrolled.
- Select one or more existing groups:**

default
- Run the following commands to download and install the agent:**

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb && sudo WAZUH_MANAGER='172.31.46.35' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Linux-Client' dpkg -i ./wazuh-agent_4.7.5-1_amd64.deb
```

**Requirements**

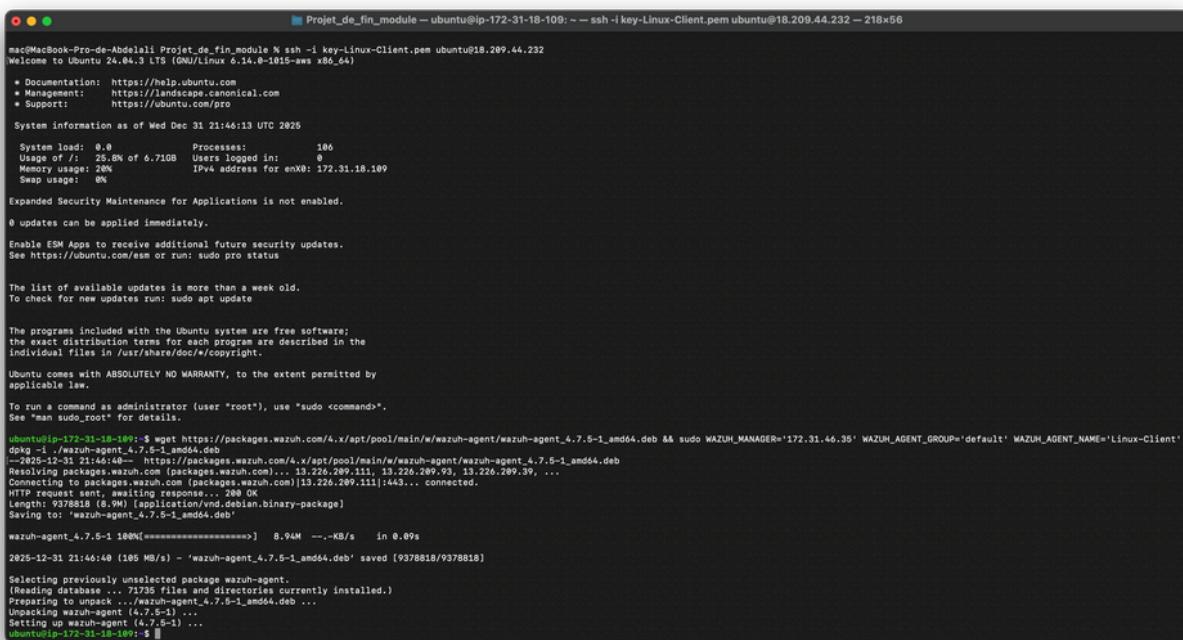
  - You will need administrator privileges to perform this installation.
  - Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.
- Start the agent:**

```
sudo systemctl daemon-reload  
sudo systemctl enable wazuh-agent  
sudo systemctl start wazuh-agent
```

**Close**

#### 4.1.1 Installation d'agent :



```
mac@MacBook-Pro-de-Abdelali Projet_de_fin_module ~ ssh -i key-Linux-Client.pem ubuntu@18.209.44.232 -- 218x56
mac@MacBook-Pro-de-Abdelali Projet_de_fin_module ~ ssh -i key-Linux-Client.pem ubuntu@18.209.44.232 -- ssh -i key-Linux-Client.pem ubuntu@18.209.44.232 -- 218x56
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)

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

System information as of Wed Dec 31 21:46:13 UTC 2025

System load: 0.0 Processes:           106
Usage of /: 25.8% of 6.71GB Users logged in: 0
Memory usage: 20% IPv4 address for enX8: 172.31.18.109
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 comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

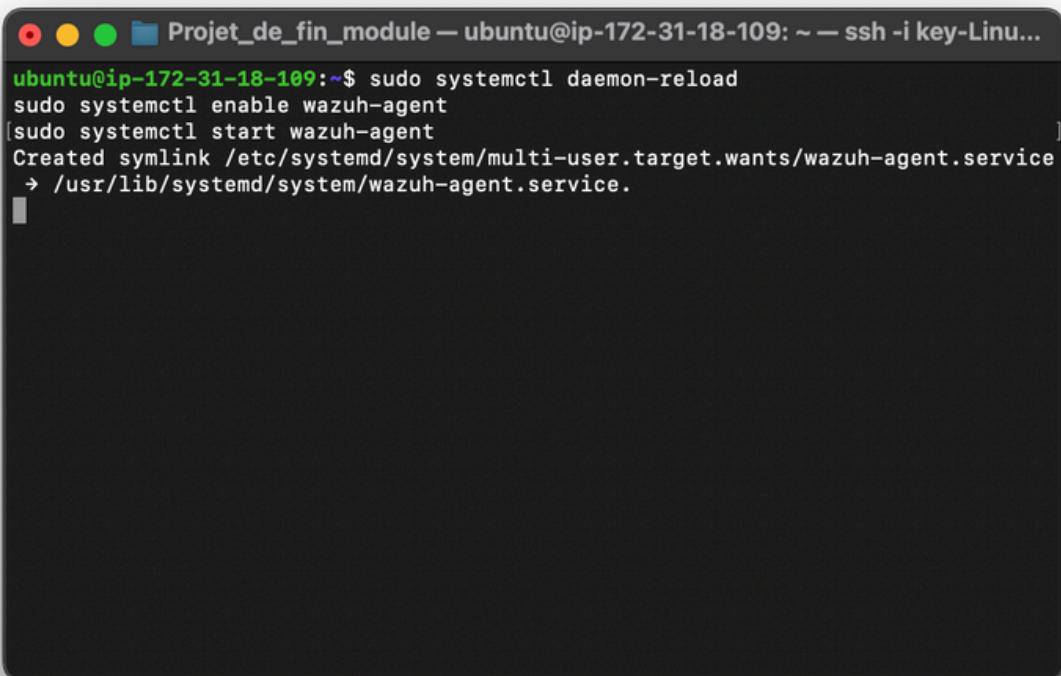
ubuntu@ip-172-31-18-109:~$ wget https://packages.wazuh.com/4.x/api/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb && sudo WAZUH_MANAGER='172.31.46.35' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Linux-Client'
dpkg: info: selecting previously unselected package wazuh-agent.
--2025-12-31 21:46:40-- https://packages.wazuh.com/4.x/api/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 13.226.209.111, 13.226.209.93, 13.226.209.39, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|13.226.209.111|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9378818 (8.9MiB) [application/xdeb.debian.binary-package]
Saving to: "wazuh-agent_4.7.5-1_amd64.deb"

wazuh-agent_4.7.5-1 100%[=====] 8.94M ---.KB/s in 0.09s

2025-12-31 21:46:48 (105 MB/s) - 'wazuh-agent_4.7.5-1_amd64.deb' saved [9378818/9378818]

Selecting previously unselected package wazuh-agent.
(Reading database ... 7779 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.7.5-1_amd64.deb ...
Unpacking wazuh-agent (4.7.5-1) ...
Setting up wazuh-agent (4.7.5-1) ...
ubuntu@ip-172-31-18-109:~$
```

#### 4.1.2 Demmarage d'agent :



```
ubuntu@ip-172-31-18-109:~$ sudo systemctl daemon-reload
[sudo] password for ubuntu:
ubuntu@ip-172-31-18-109:~$ sudo systemctl enable wazuh-agent
[sudo] password for ubuntu:
ubuntu@ip-172-31-18-109:~$ sudo systemctl start wazuh-agent
[sudo] password for ubuntu:
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service
→ /usr/lib/systemd/system/wazuh-agent.service.
```

#### 4.1.3 Affichage d'agent :

The screenshot shows the Wazuh Agents interface. At the top, there are three main sections: STATUS, DETAILS, and EVOLUTION. The STATUS section has a large green circle icon and a legend: Active (1), Disconnected (0), Pending (0), and Never connected (0). The DETAILS section shows 1 Active agent, 0 Disconnected, 0 Pending, 0 Never connected, and 100.00% Agents coverage. It also lists the Last registered agent as Linux-Client and the Most active agent as Linux-Client. The EVOLUTION section shows a chart for the last 24 hours with no results found. Below these, there is a table titled 'Agents (1)' listing one agent: ID 001, Name Linux-Client, IP address 172.31.18.109, Group(s) default, Operating system Ubuntu 24.04.3 LTS, Cluster node node01, Version v4.7.5, Status active. There are buttons for Deploy new agent, Refresh, Export formatted, and Refresh.

#### 4.2 Agent Windows :

L'agent Wazuh a été installé sur le client Windows via PowerShell.

Le service Wazuh Agent est en état Running et les événements Windows sont correctement transmis au serveur.

The screenshot shows the 'Deploy new agent' dialog box. It starts with a step to 'Select the package to download and install on your system' with options for LINUX (RPM and64, RPM aarch64, DEB and64, DEB aarch64), WINDOWS (MSI 32/64 bits), and macOS (Intel, Apple silicon). A note says to check documentation for other systems. The next step is 'Server address:' with an input field containing '172.31.46.35'. The 'Optional settings' step shows an 'Assign an agent name:' field with 'Windows-Client' entered, with a note that it must be unique. The 'Run the following commands to download and install the agent:' step contains a command: 

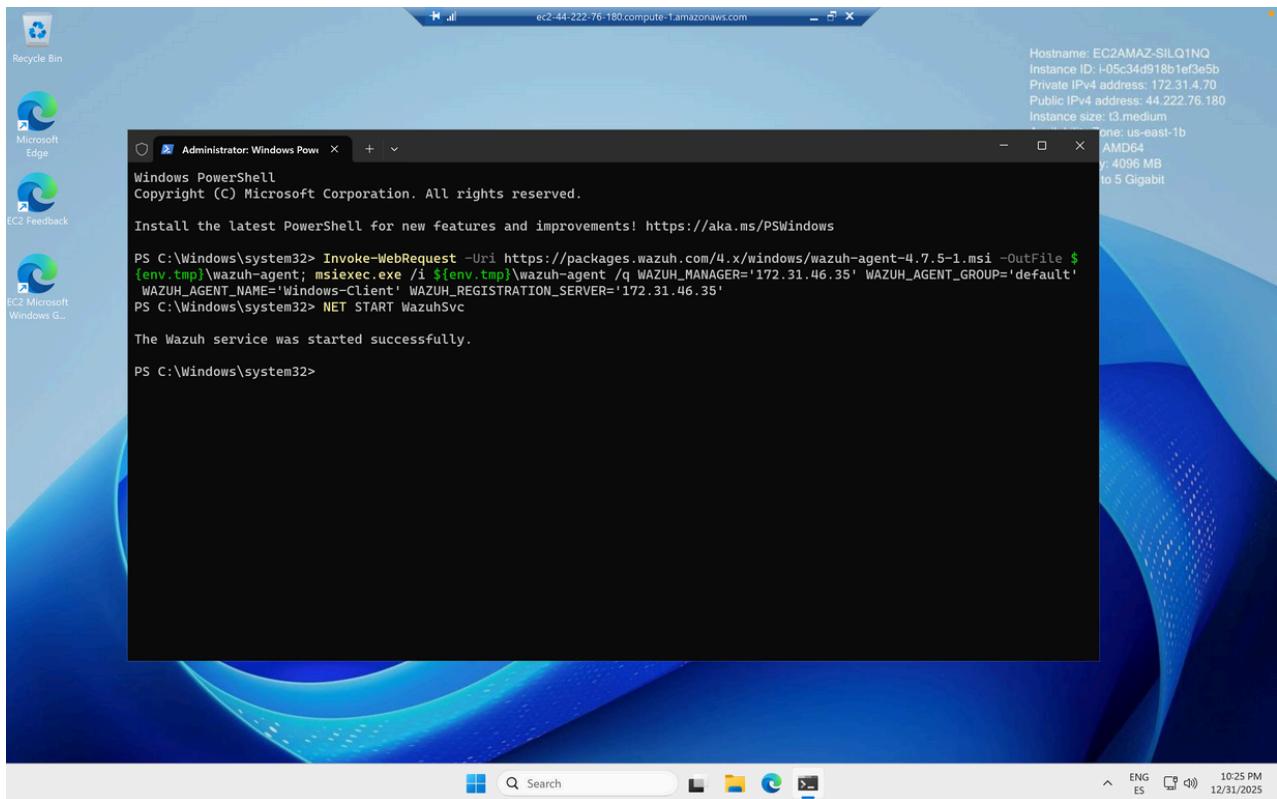
```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -Outfile C:\Windows\Temp\wazuh-agent.msi
```

 and environment variables: `WAZUH_AGENT_SKOOL=0`, `WAZUH_AGENT_NAME=Windows-Client`, `WAZUH_REGISTRATION_SERVER=172.31.46.35`. The 'Requirements' note says you need administrator privileges and PowerShell 3.0 or greater. The final step is 'Start the agent:' with a command: 

```
NET START WazuhSvc
```

.

#### 4.2.1 Telechargement et demmarage d'agent :



#### 4.2.2 Affichage d'agent :

The screenshot shows the Wazuh web interface under the "Agents" tab. The top section displays a status summary:

- STATUS: Active (1), Disconnected (1), Pending (0), Never connected (0)
- DETAILS: Active (1), Disconnected (1), Pending (0), Never connected (0), Agents coverage 50.00%
- EVOLUTION: A line chart showing agent activity over the last 24 hours, with one active point at 10:25 PM on 12/31/2025.

The bottom section lists the agents:

| ID  | Name           | IP address    | Group(s) | Operating system   | Cluster node | Version | Status       | Actions |  |
|-----|----------------|---------------|----------|--|--------------|---------|--------------|---------|--|
| 001 | Linux-Client   | 172.31.18.109 | default  | Ubuntu 24.04.3 LTS                                       | node01       | v4.7.5  | active       |         |  |
| 002 | Windows-Client | 172.31.4.70   | default  | Microsoft Windows Server 2025 Datacenter 10.0.26100.7462 | node01       | v4.7.5  | disconnected |         |  |

## 5. Démonstrations SIEM et EDR :

Afin de valider le fonctionnement de la plateforme, plusieurs scénarios de sécurité ont été simulés.

### 5.1 Scénarios SIEM – Linux :

Tentatives de connexion SSH échouées (bruteforce simulé)

Élévation de privilège via sudo

Modification d'un fichier sensible (/etc/passwd)

Ces actions ont généré des alertes visibles dans le Dashboard, notamment des événements liés à sshd, à l'authentification et au File Integrity Monitoring (FIM).

```
Projet_de_fin_module – root@ip-172-31-18-109: /home/ubuntu – ssh -i...
[root@ip-172-31-18-109:/home/ubuntu# exit
exit
[ubuntu@ip-172-31-18-109:~$ ssh fakeuser@18.209.44.232
ssh: connect to host 18.209.44.232 port 22: Connection timed out
ubuntu@ip-172-31-18-109:~$ [ubuntu@ip-172-31-18-109:~$ echo "test" | sudo tee -a /etc/passwd
test
[ubuntu@ip-172-31-18-109:~$ sudo su
root@ip-172-31-18-109:/home/ubuntu# ]
```

wazuh. ▾ Agents / Linux-Client

Security events Integrity monitoring SCA System Auditing Vulnerabilities MITRE ATT&CK More... ▾

Inventory data Stats Configuration

|        |                 |                          |                      |                |                                     |                     |   |  |
|--------|-----------------|--------------------------|----------------------|----------------|-------------------------------------|---------------------|---|--|
| ID 001 | Status ● active | IP address 172.31.18.109 | Version Wazuh v4.7.5 | Groups default | Operating system Ubuntu 24.04.3 LTS | Cluster node node01 | Registration date Dec 31, 2025 @ 22:48:09.000 | Last keep alive Jan 1, 2026 @ 00:08:04.000 |
|--------|-----------------|--------------------------|----------------------|----------------|-------------------------------------|---------------------|---|--|

Last 24 hours ▾

MITRE

Top Tactics

- Defense Evasion 21
- Privilege Escalation 20
- Initial Access 14
- Persistence 14
- Lateral Movement 7

Compliance

PCI DSS

- 10.2.5 (34)
- 10.6.1 (12)
- 10.2.2 (5)
- 10.2.4 (5)
- 10.2.6 (2)

FIM: Recent events

| Time             | Path | Action | Rule description | Rule Level | Rule Id |
|------------------|------|--------|------------------|------------|---------|
| No recent events |      |        |                  |            |         |

Events count evolution

Count

SCA: Lastest scans

</>

You don't have SCA scans in this agent.

Check your agent settings to generate scans.

## 5.1.1 Tentatives SSH échouées (bruteforce simulé) :

The screenshot shows the Wazuh interface for a Linux Client. The top navigation bar includes 'Agents' and 'Linux-Client'. The main dashboard displays 'Valid Accounts' with a 'Technique details' section for T1078 (Initial Access), tactics Persistence, Privilege Escalation, Defense Evasion, and Initial Access, and a version of 2.4. A 'Recent events' table lists three entries from Jan 1, 2026, at 00:05:08.18, all categorized under T1078 and labeled as 'PAM: Login session opened.' The table also includes columns for Time, Technique(s), Tactic(s), Level, Rule ID, and Description.

| Time                              | Technique(s) | Tactic(s)  | Level | Rule ID | Description                |
|-----------------------------------|--------------|--|-------|---------|----------------------------|
| Jan 1, 2026<br>@ 00:05:08.18<br>3 | T1078        | Defense Evasion,<br>Persistence, Privilege<br>Escalation, Initial Access | 3     | 5501    | PAM: Login session opened. |
| Jan 1, 2026<br>@ 00:05:08.18<br>3 | T1078        | Defense Evasion,<br>Persistence, Privilege<br>Escalation, Initial Access | 3     | 5501    | PAM: Login session opened. |
| Jan 1, 2026<br>-                  |              | Defense Evasion,   |       |         |                            |

## 5.1.2 Élévation de privilèges :

The screenshot shows the Wazuh interface for a Linux Client. The top navigation bar includes 'Agents' and 'Linux-Client'. The main dashboard displays 'Valid Accounts' with a 'Technique details' section for T1078 (Privilege Escalation), tactics Persistence, Privilege Escalation, Defense Evasion, and Initial Access, and a version of 2.4. A 'Recent events' table lists four entries from Jan 1, 2026, at 00:05:08.18, all categorized under T1078 and labeled as 'PAM: Login session opened.' The table also includes columns for Time, Technique(s), Tactic(s), Level, Rule ID, and Description.

| Time                              | Technique(s) | Tactic(s)  | Level | Rule ID | Description                |
|-----------------------------------|--------------|--|-------|---------|----------------------------|
| Jan 1, 2026<br>@ 00:05:08.18<br>3 | T1078        | Defense Evasion,<br>Persistence, Privilege<br>Escalation, Initial Access | 3     | 5501    | PAM: Login session opened. |
| Jan 1, 2026<br>@ 00:05:08.18<br>3 | T1078        | Defense Evasion,<br>Persistence, Privilege<br>Escalation, Initial Access | 3     | 5501    | PAM: Login session opened. |
| Jan 1, 2026<br>@ 00:04:04.09<br>3 | T1078        | Defense Evasion,<br>Persistence, Privilege<br>Escalation, Initial Access | 3     | 5501    | PAM: Login session opened. |
| Dec 31, 2025 @                    | T1078        | Defense Evasion,<br>Persistence, Privilege                               | 3     | 5501    | PAM: Login session opened. |

### 5.1.3 FIM (File Integrity Monitoring) :

The screenshot shows the Wazuh interface for a Linux Client. The top navigation bar has tabs for 'Agents' and 'Linux-Client'. The main dashboard includes a 'Compliance' donut chart and a table of 'Recent events' for SSH activity. The table lists five events from December 31, 2025, at various times, all categorized as 'ssh: Attempt to login using a non-existent user'.

| Time                        | Technique(s)           | Tactic(s)                           | Level | Rule ID | Description                                      |
|-----------------------------|------------------------|-------------------------------------|-------|---------|--|
| Dec 31, 2025 @ 23:55:43.606 | T1110.001<br>T1021.004 | Credential Access, Lateral Movement | 5     | 5710    | sshd: Attempt to login using a non-existent user |
| Dec 31, 2025 @ 23:45:10.946 | T1110.001<br>T1021.004 | Credential Access, Lateral Movement | 5     | 5710    | sshd: Attempt to login using a non-existent user |
| Dec 31, 2025 @ 23:45:08.944 | T1110.001<br>T1021.004 | Credential Access, Lateral Movement | 5     | 5710    | sshd: Attempt to login using a non-existent user |
| Dec 31, 2025 @ 23:45:04.940 | T1110.001<br>T1021.004 | Credential Access, Lateral Movement | 5     | 5710    | sshd: Attempt to login using a non-existent user |
| Dec 31, 2025 @ 23:44:50.924 | T1110.001<br>T1021.004 | Credential Access, Lateral Movement | 5     | 5710    | sshd: Attempt to login using a non-existent user |

### 5.2 Scénarios EDR – Windows :

Échecs de connexion (Event ID 4625)

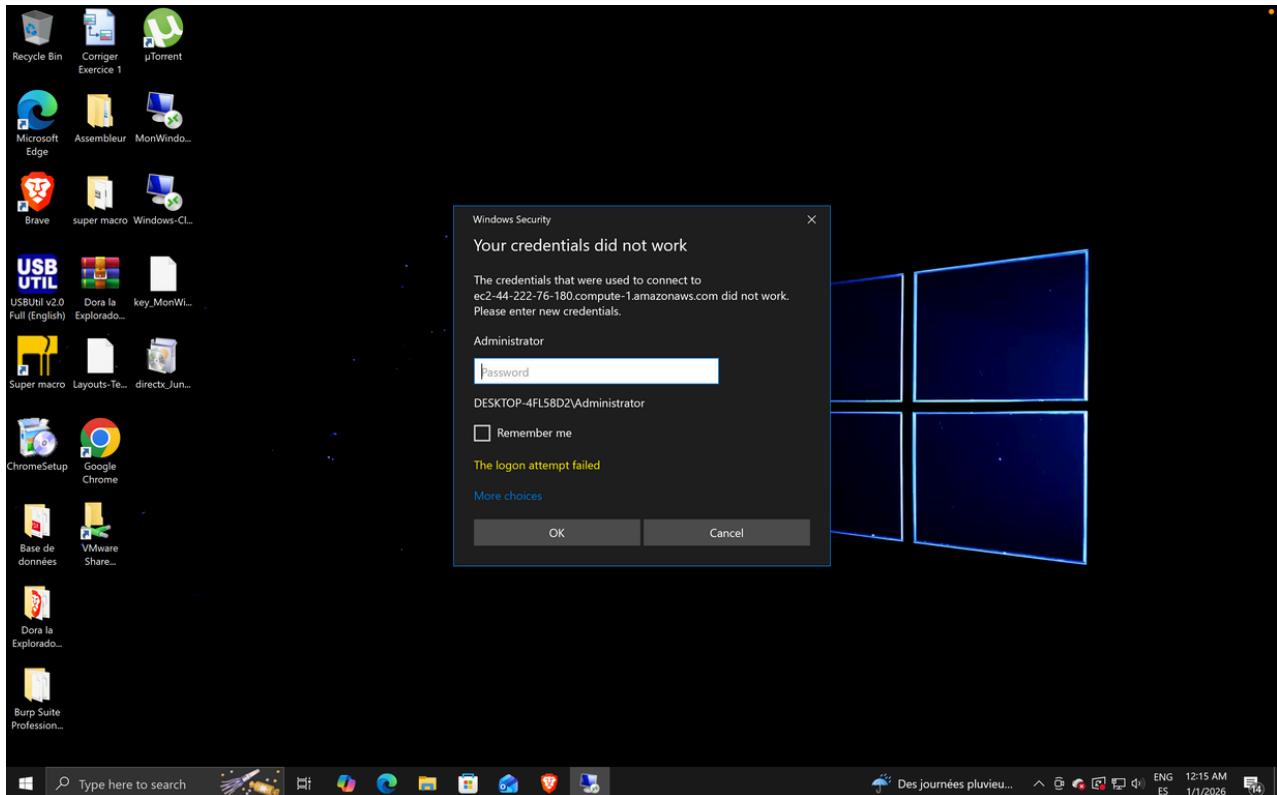
Création d'un utilisateur local et ajout au groupe Administrateurs

Ces événements ont été détectés par Wazuh et classifiés comme événements critiques liés à la gestion des identités et des priviléges.

The screenshot shows the Wazuh interface for a Windows Client. The top navigation bar has tabs for 'Agents' and 'Windows-Client'. The main dashboard includes a 'Compliance' donut chart and a table of 'FIM: Recent events'. The table shows no recent events.

| Time             | Path | Action | Rule description | Rule Level | Rule Id |
|------------------|------|--------|------------------|------------|---------|
| No recent events |      |        |                  |            |         |

## 5.2.1 Échecs de login (4625) :



wazuh. ▾ Agents Windows-Client

Valid Accounts

| ID  | Status | IP address  | Version      |
|-----|--------|-------------|--------------|
| 002 | active | 172.31.4.70 | Wazuh v4.7.5 |

MITRE

Compliance

Recent events 19 hits

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

Events count evolution

Count

## 5.2.2 Création utilisateur (IAM) :

```
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> |
```

| Time                            | Technique(s) | Tactic(s)  | Level | Rule ID | Description            |
|---------------------------------|--------------|--|-------|---------|------------------------|
| Jan 1, 2026<br>00:17:26.02<br>6 | T1078        | Defense Evasion,<br>Persistence, Privilege<br>Escalation, Initial Access | 3     | 60106   | Windows logon success. |
| Jan 1, 2026<br>00:17:24.42<br>1 | T1078        | Defense Evasion,<br>Persistence, Privilege<br>Escalation, Initial Access | 3     | 60106   | Windows logon success. |
| Jan 1, 2026<br>00:17:23.34<br>7 | T1078        | Defense Evasion,<br>Persistence, Privilege<br>Escalation, Initial Access | 3     | 60106   | Windows logon success. |
| Jan 1, 2026<br>00:17:22.75<br>5 | T1078        | Defense Evasion,<br>Persistence, Privilege<br>Escalation, Initial Access | 3     | 60106   | Windows logon success. |
| Jan 1, 2026<br>00:17:22.43<br>2 | T1078        | Defense Evasion,<br>Persistence, Privilege<br>Escalation, Initial Access | 3     | 60106   | Windows logon success. |

## 6. Analyse : SIEM, EDR et IAM :

SIEM : centralisation et corrélation des logs Linux et Windows

EDR : surveillance comportementale des endpoints (processus, utilisateurs, actions critiques)

IAM / PAM : détection des changements de priviléges et des tentatives d'accès non autorisées

Cette combinaison permet une visibilité complète sur les activités des systèmes et constitue la base d'un SOC moderne.

## 7. Security Monitoring et Threat Detection :

La plateforme Wazuh permet également de réaliser des requêtes de threat hunting, par exemple :

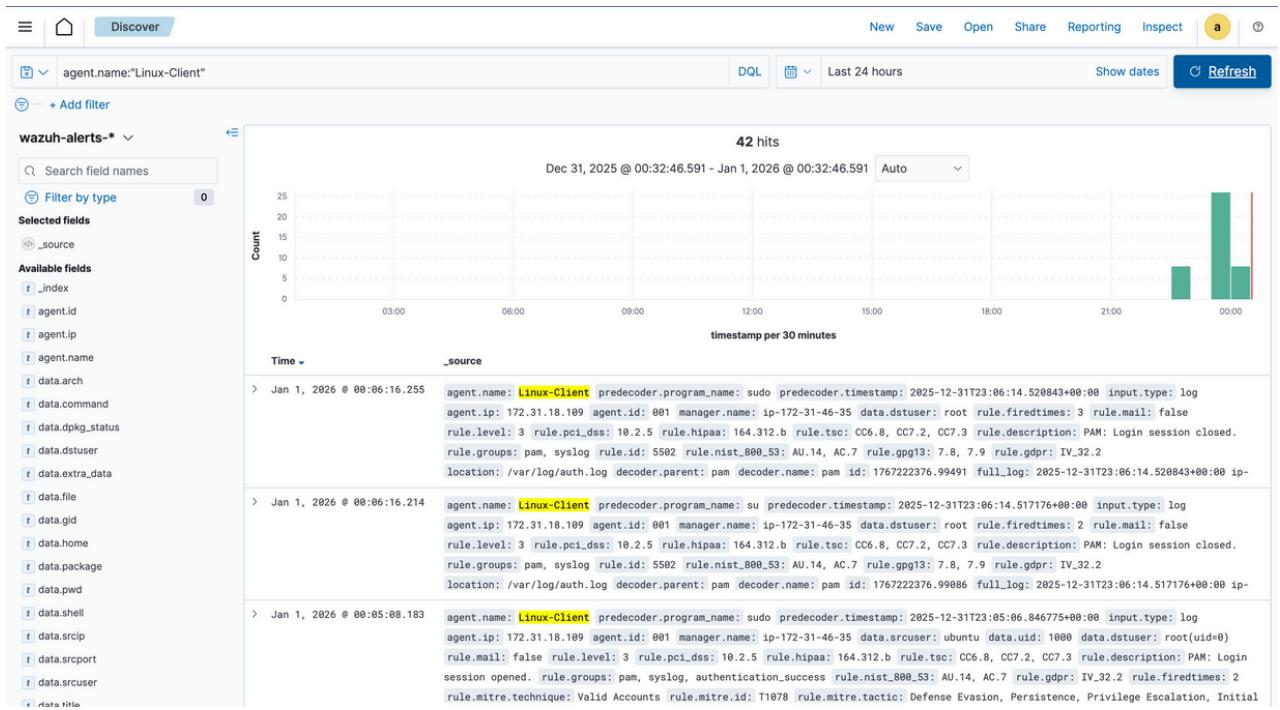
Recherche des tentatives d'authentification échouées répétées

Détection des créations de comptes administrateurs

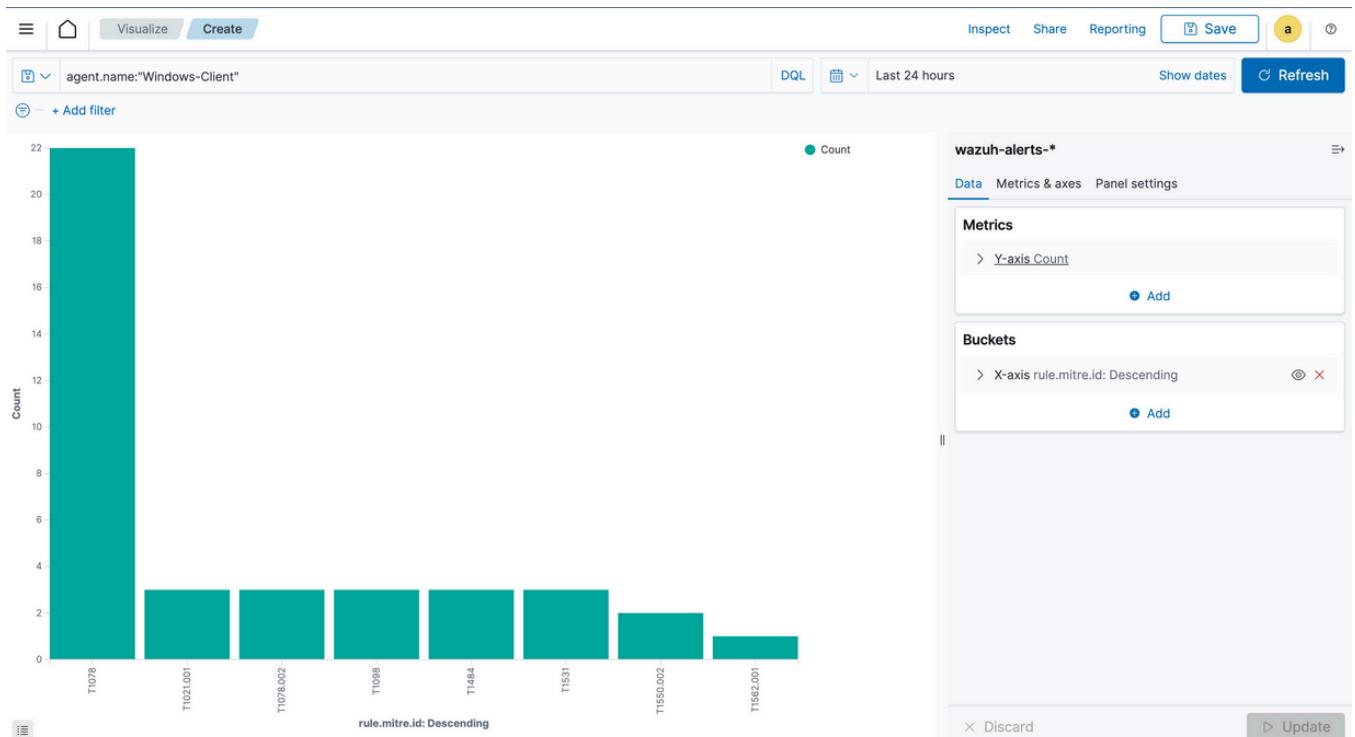
Analyse des actions sensibles sur les fichiers système

Ces requêtes renforcent la capacité de détection proactive des menaces.

## 7.1 Dashboard + exemple d'un filtre :



## 7.2 Affichage en diagramme :

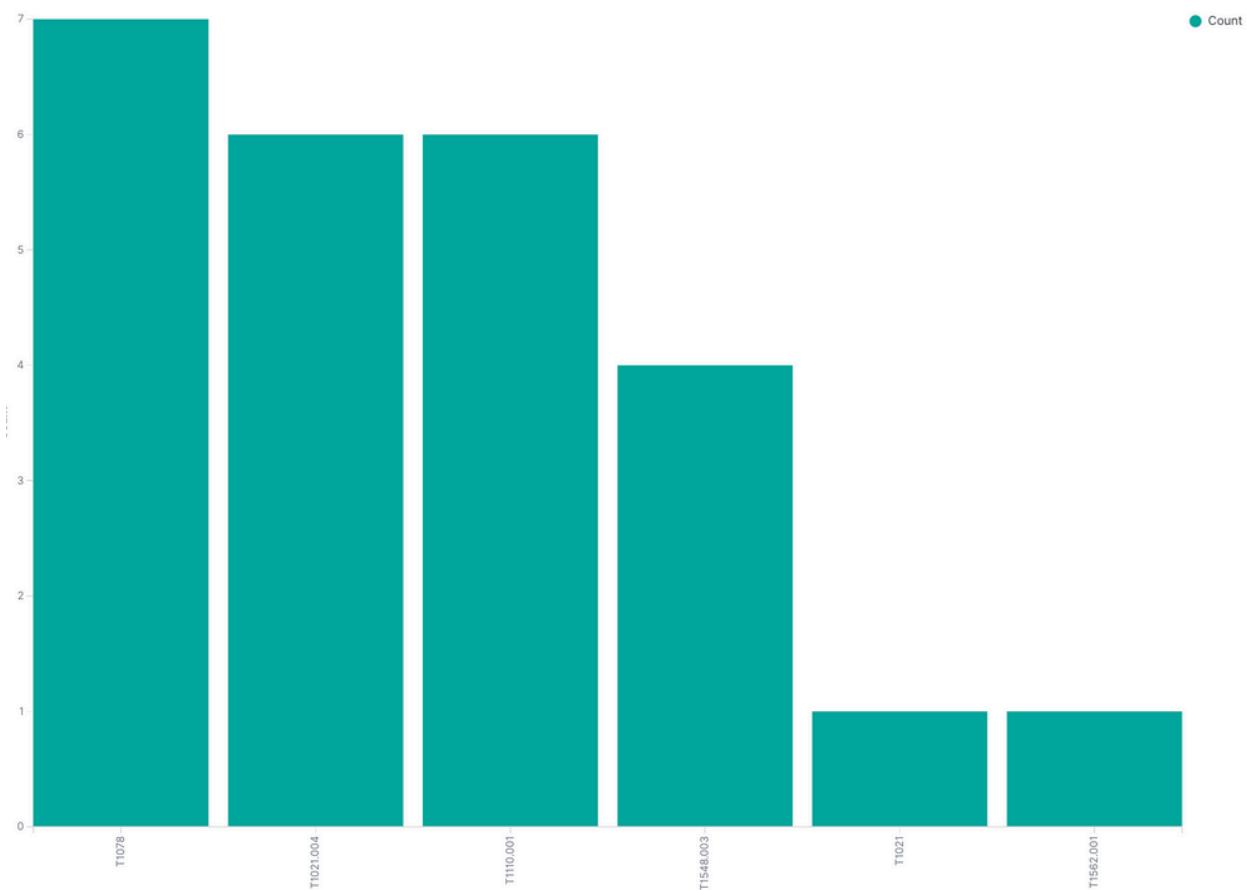


## 7.3 Threat Detection 1 :

### 7.3.1 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 : 172.31.4.70 (adresse privée, donc probablement interne à un réseau/VPC).

Machine cible : serveur Linux (agent Wazuh ID 001, IP publique 41.141.x.x).

Géolocalisation de la machine cible : Casablanca, Maroc.

Date de l'événement : début décembre 2025.

|  |   |  |  |
|--|---|--|--|
| Jan 1, 2026 @ 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.sruser: fakeuser data.srchip: 41... data.srport: 51310 manager.name: ip-172-31-44-110 rule.level: 5 rule.hipas: 164.312.b rule.pci_dss: 10.2.4, 10.2.5, 10.6.1 rule.tsc: C06.1, C06.8, OC7.2, C07.3 rule.description: sshd: Attempt to login using a non-existent user rule.group: syslog, sshd, authentication_failed, invalid_login rule.mist_800_53: AU.14, AC.7, AU.6 rule.gdpr: 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: S710 rule.gpg13: 7.1 location: /var/log/auth.log decoder.parent: sshd decoder.name: sshd id: 1767222111.24646 Geolocation.city.name: Casablanca Geolocation.country.name: Morocco Geolocation.region.name: Casablanca Geolocation.location: { "lon": -7.6184, "lat": 33.5922 } full_log: 2025-12-31T23:01:51.732610+00:00 ip-172-31-7-211 sshd[3436]: Invalid user fakeuser from 41... port 51310 | <a href="#">View surrounding documents</a> | <a href="#">View single document</a>   |
| Expanded document                          |   |  |  |
| <a href="#">Table</a> <a href="#">JSON</a> |   |  |  |
| r GeoLocation.city.name                    | Casablanca  | r _index                                   | wazuh-alerts-4.x-2025.12.31  |
| r GeoLocation.country.name                 | Morocco   | r agent.id                                 | 001  |
| o GeoLocation.location                     | { "lon": -7.6184, "lat": 33.5922 }  | r agent.ip                                 | 172.31.7.211   |
| r GeoLocation.region.name                  | Casablanca  | r agent.name                               | Linux  |
| r _index                                   | wazuh-alerts-4.x-2025.12.31   | r data.srchip                              | 41...  |
| r agent.id                                 | 001   | r data.srport                              | 51310  |
| r agent.ip                                 | 172.31.7.211  | r data.sruser                              | fakeuser   |
| r agent.name                               | Linux   | r decoder.name                             | sshd   |
| r data.srchip                              | 41...   | r decoder.parent                           | sshd   |
| r data.srport                              | 51310   | r full_log                                 | 2025-12-31T23:01:51.732610+00:00 ip-172-31-7-211 sshd[3436]: Invalid user fakeuser from 41... port 51310 |
| r data.sruser                              | fakeuser  | r id                                       | 1767222111.24646   |
| r decoder.name                             | sshd  | r input.type                               | log  |
| r decoder.parent                           | sshd  | r location                                 | /var/log/auth.log  |

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

## 7.4 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

|  |  |  |  |
|--|--|--|--|
| Jan 1, 2026 @ 00:20:35.887   | agent.name: Windows_S rule.mitre.id: T1484 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: EC2AMAZ-PI6E93K data.win.eventdata.targetDomainName: Builtin data.win.eventdata.targetSids: S-1-5-32-544 data.win.eventdata.subjectUserName: Administrator data.win.system.eventID: 4732 data.win.system.keywords: 0x8020000000000000 data.win.system.providerGuid: {54849625-5478-4994-a5b0-3e3b0328c30d} 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: EC2AMAZ-PI6E93K Logon ID: 0x41fd6b Member: Security ID: S-1-5-21-1267691158-3860027324-3782535310-1000 | <a href="#">View surrounding documents</a> | <a href="#">View single document</a>                   |
| Expanded document  |  |  |  |
| <a href="#">Table</a> <a href="#">JSON</a>   |  |  |  |
| r _index   | wazuh-alerts-4.x-2025.12.31  | r agent.id                                 | 002  |
| r agent.ip   | 172.31.7.145   | r agent.name                               | Windows_S  |
| r agent.name   | Windows_S  | r data.win.eventdata.memberSid             | S-1-5-21-1267691158-3860027324-3782535310-1000         |
| r data.win.eventdata.subjectDomainName   | EC2AMAZ-PI6E93K  | r data.win.eventdata.subjectLogonId        | 0x41fd6b   |
| r data.win.eventdata.subjectUserName   | Administrator  | r data.win.eventdata.subjectUserId         | S-1-5-21-1267691158-3860027324-3782535310-500          |
| r data.win.eventdata.subjectUserName   | Builtin  | r data.win.eventdata.targetDomainName      | S-1-5-32-544   |
| r data.win.eventdata.targetSids  | S-1-5-32-544   | r data.win.eventdata.targetUserName        | Administrators   |
| r data.win.eventdata.targetUserName  | Administrators   | r data.win.system.channel                  | Security   |
| r data.win.system.eventID  | 4732   | r data.win.system.computer                 | EC2AMAZ-PI6E93K  |
| r data.win.system.eventRecordID  | 84773  | r data.win.system.eventID                  | 4732   |
| r data.win.system.keywords   | 0x8020000000000000   | r data.win.system.level                    | 0  |
| r data.win.system.level  | 0  | r data.win.system.message                  | "A member was added to a security-enabled local group. |
| Subject:<br>Security ID: S-1-5-21-1267691158-3860027324-3782535310-500<br>Account Name: Administrator<br>Account Domain: EC2AMAZ-PI6E93K |  |  |  |

- Machine concernée : Agent Wazuh ID 002, nom "Windows\_S", IP 172.31.4.70 (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                    |
| t rule.id              | 60154   |
| # rule.level           | 12  |
| o rule.mail            | true  |
| t rule.mitre.id        | <b>T1484</b>  |
| 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).

## 7.5 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<br>data.win.eventdata.subjectLogonId: 0xb69387 data.win.eventdata.scriptPath: %1793 data.win.eventdata.passwordLastSet: %1794<br>data.win.eventdata.homeDirectory: %1793 data.win.eventdata.userParameters: %1793 data.win.eventdata.subjectDomainName: EC2AMAZ-SILQ1NQ<br>data.win.eventdata.displayName: %1793 data.win.eventdata.accountExpires: %1794 data.win.eventdata.homePath: %1793<br>data.win.eventdata.samAccountName: labuser data.win.eventdata.targetUserName: labuser data.win.eventdata.subjectUserSid: S-1-5-21-887713911-3399705033  |
| > 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<br>data.win.eventdata.subjectLogonId: 0xb69387 data.win.eventdata.scriptPath: %1793 data.win.eventdata.passwordLastSet: %1794<br>data.win.eventdata.homeDirectory: %1793 data.win.eventdata.userParameters: %1793 data.win.eventdata.subjectDomainName: EC2AMAZ-SILQ1NQ<br>data.win.eventdata.displayName: %1793 data.win.eventdata.accountExpires: %1794 data.win.eventdata.homePath: %1793<br>data.win.eventdata.samAccountName: labuser data.win.eventdata.targetUserName: labuser data.win.eventdata.subjectUserSid: S-1-5-21-887713911-3399705033  |
| > 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<br>data.win.eventdata.subjectLogonId: 0x3e7 data.win.eventdata.restrictedAdminMode: %1843 data.win.eventdata.subjectDomainName: WORKGROUP<br>data.win.eventdata.targetLinkedLogonId: 0x0 data.win.eventdata.impersonationLevel: %1833 data.win.eventdata.ipAddress: 41.141.26.111<br>data.win.eventdata.authenticationPackageName: Negotiate data.win.eventdata.workstationName: EC2AMAZ-SILQ1NQ data.win.eventdata.targetLogonId: 0xda92f8<br>data.win.eventdata.logonProcessName: User32 data.win.eventdata.logonGuid: {00000000-0000-0000-0000-000000000000}                        |
| > Jan 1, 2026 @ 00:17:21.020 | agent.name: Windows-Client rule.mitre.id: T1021.001, <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<br>data.win.eventdata.subjectLogonId: 0x0 data.win.eventdata.targetLinkedLogonId: 0x0 data.win.eventdata.impersonationLevel: %1833<br>data.win.eventdata.ipAddress: data.win.eventdata.authenticationPackageName: NTLM data.win.eventdata.workstationName: DESKTOP-4FL58D2<br>data.win.eventdata.lmPackageName: NTLM V2 data.win.eventdata.targetLogonId: 0xda0555 data.win.eventdata.logonProcessName: NtLmSsp<br>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-SILQ1NQ).
- 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

## Conclusion

Ce projet a permis de mettre en œuvre une solution complète de supervision de la sécurité des endpoints dans un environnement Cloud réel. L'intégration de Wazuh avec des systèmes Linux et Windows a démontré l'efficacité des solutions SIEM et EDR pour la détection, l'analyse et la réponse aux incidents de sécurité.

Les résultats obtenus confirment l'importance de la centralisation des logs, de la surveillance des endpoints et de la gestion des identités dans la protection des infrastructures modernes.

## Lien GitHub :

Le dépôt GitHub du projet, contenant la documentation, les fichiers de configuration et les captures d'écran, est disponible à l'adresse suivante :

<https://github.com/AbdelaliSaadali/wazuh-siem-edr-cloud-lab.git>



The screenshot shows the GitHub repository page for the project. At the top, the repository name "AbdelaliSaadali/wazuh-siem-edr-cloud-lab" is displayed in bold black text. To the right of the name is a blue circular icon with a white logo. Below the name, there are four metrics: 1 contributor, 0 issues, 0 stars, and 0 forks. A GitHub logo is also present. At the bottom of the page, there is a link to the repository's page: "AbdelaliSaadali/wazuh-siem-edr-cloud-lab". Below this link, there is a message encouraging users to contribute by creating an account on GitHub.