FORMATION CONTINUE
CÉGEP DE LANAUDIÈRE

Cégep Régional de Lanaudière

Travail de Session

420-B01-HU – Surveillance préventive en cybersécurité

PRÉSENTÉ À :
Jocelyn Baril

PRODUIT PAR :
Lina Nzouechim
6382883

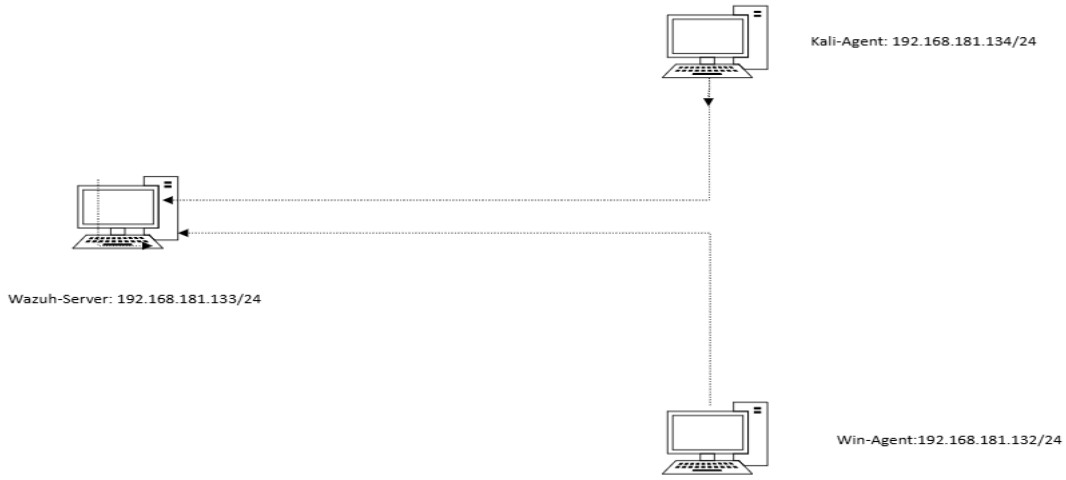
07 Décembre 2025

Version 1.0

Table des matières

1-ENVIRONNEMENT D'EXPÉRIMENTATION

Rôle	Nom	Système d'exploitation	Adresse IP
Serveur Wazuh	Wazuh-server	Ubuntu Server 22.04.5	192.168.181.133/24
Cible Linux	kali-Agent	Kali-Linux-2025.3	192.168.181.134/24
Cible Windows	win-Agent	Windows 11	192.168.181.132/24



2-INSTALLATION DU SERVEUR WAZUH

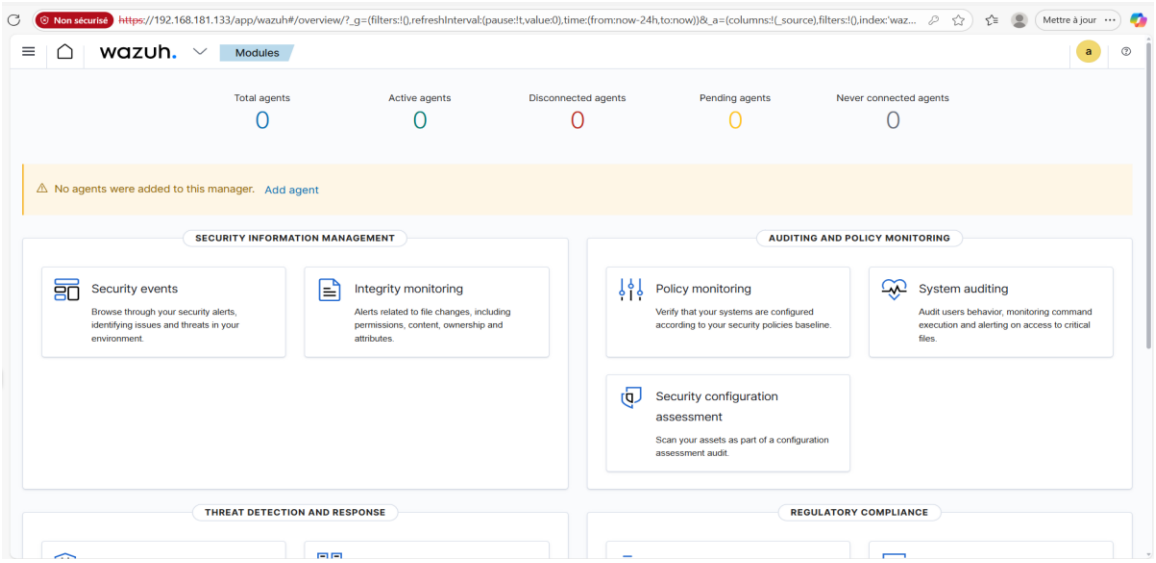
Procédure d'installation du serveur Wazuh sur une machine ayant les caractéristiques minimales nécessaires :

a- Téléchargez et exécutez l'assistant d'installation de Wazuh.
```
curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

b- A la fin de l'installation, récupérer le login et le mot de passe

```
01/12/2025 01:39:36 INFO: Updating the internal users.
01/12/2025 01:39:43 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
01/12/2025 01:39:55 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
01/12/2025 01:40:21 INFO: Initializing Wazuh dashboard web application.
01/12/2025 01:40:22 INFO: Wazuh dashboard web application initialized.
01/12/2025 01:40:22 INFO: --- Summary ---
01/12/2025 01:40:22 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: IkZbmPbIJJqciK7vEee+AGF*2UINyGL6
01/12/2025 01:40:22 INFO: Installation finished.
lina@wazuh-server:~$
```

c- Accéder à l'interface de Wazuh (https://<wazuh-dashboard-ip>:443)
Dans notre cas : https://192.168.181.133:443



3- INSTALLATION ET INTÉGRATION DES AGENTS WAZUH

3-1- INSTALLATION DE L'AGENT WAZUH SUR LA CIBLE LINUX

Procédure à suivre sur une machine ayant les caractéristiques minimales nécessaires et à jour:

a- Ajouter le dépôt wazuh :

```
# apt-get install gnupg apt-transport-https
# sudo curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo
gpg --no-default-keyring --keyring gnupg-
ring:/usr/share/keyrings/wazuh.gpg --import && sudo chmod 644
/usr/share/keyrings/wazuh.gpg
# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg]
https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee -a
/etc/apt/sources.list.d/wazuh.list
# sudo apt-get update
```

b- Déployer l'agent wazuh

```
# sudo WAZUH_MANAGER="192.168.181.133" apt-get install wazuh
```

```
┌──(lina1㉿kali-Agent)-[~]
└─$ sudo WAZUH_MANAGER="192.168.181.133"  apt-get install wazuh-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Solving dependencies... Done
The following NEW packages will be installed:
  wazuh-agent
0 upgraded, 1 newly installed, 0 to remove and 1207 not upgraded.
Need to get 13.1 MB of archives.
After this operation, 48.4 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-agent amd64 4.14.1-1 [13.1 MB]
Fetched 13.1 MB in 1s (18.9 MB/s)
Preconfiguring packages ...
Selecting previously unselected package wazuh-agent.
(Reading database ... 416809 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.14.1-1_amd64.deb ...
Unpacking wazuh-agent (4.14.1-1) ...
Setting up wazuh-agent (4.14.1-1) ...

┌──(lina1㉿kali-Agent)-[~]
└─$
```

c- Activez et démarrez le service d'agent Wazuh
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent

```
┌──(lina1㉿kali-Agent)-[~]
└─$ sudo systemctl daemon-reload

┌──(lina1㉿kali-Agent)-[~]
└─$ sudo systemctl enable wazuh-agent
Created symlink '/etc/systemd/system/multi-user.target.wants/wazuh-agent.service' → '/usr/lib/systemd/system/wazuh-agent.service'.

┌──(lina1㉿kali-Agent)-[~]
└─$ sudo systemctl start wazuh-agent
```

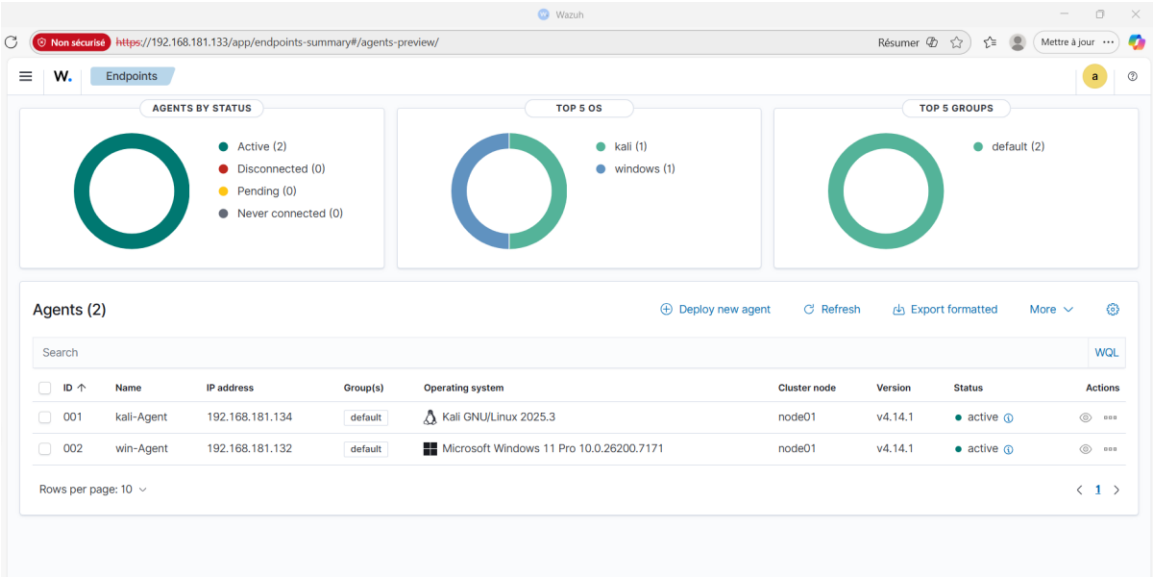
```
┌──(lina1㉿kali-Agent)-[~]
└─$ sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; preset: disabled)
     Active: active (running) since Sun 2025-11-30 18:01:49 EST; 8min ago
 Invocation: 2453e10ccaf249f8bd2147c9b763f600
    Process: 26278 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 28 (limit: 2162)
     Memory: 62.7M (peak: 66.5M)
        CPU: 7.783s
     CGroup: /system.slice/wazuh-agent.service
             ├─26301 /var/ossec/bin/wazuh-execd
             ├─26320 /var/ossec/bin/wazuh-agentd
             ├─26340 /var/ossec/bin/wazuh-syscheckd
             ├─26351 /var/ossec/bin/wazuh-logcollector
             └─26376 /var/ossec/bin/wazuh-modulesd

Nov 30 18:01:43 kali-Agent systemd[1]: Starting wazuh-agent.service - Wazuh agent...
Nov 30 18:01:43 kali-Agent env[26278]: Starting Wazuh v4.14.1...
Nov 30 18:01:44 kali-Agent env[26278]: Started wazuh-execd...
Nov 30 18:01:45 kali-Agent env[26278]: Started wazuh-agentd...
Nov 30 18:01:45 kali-Agent env[26278]: Started wazuh-syscheckd...
Nov 30 18:01:46 kali-Agent env[26278]: Started wazuh-logcollector...
Nov 30 18:01:47 kali-Agent env[26278]: Started wazuh-modulesd...
Nov 30 18:01:49 kali-Agent env[26278]: Completed.
Nov 30 18:01:49 kali-Agent systemd[1]: Started wazuh-agent.service - Wazuh agent.

┌──(lina1㉿kali-Agent)-[~]
└─$
```

3-2- INSTALLATION DE L'AGENT WAZUH SUR LA CIBLE WINDOWS

a- Téléchargez le programme d'installation Windows pour démarrer le processus d'installation à l'adresse suivante :
https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi

b- Puis ouvrir le PowerShell en tant qu'administrateur, se déplacer dans le dossier où se trouve l'assistant d'installation .msi précédemment téléchargé et exécuter la commande :
.\wazuh-agent-4.14.1-1.msi /q WAZUH_MANAGER="192.168.181.133"

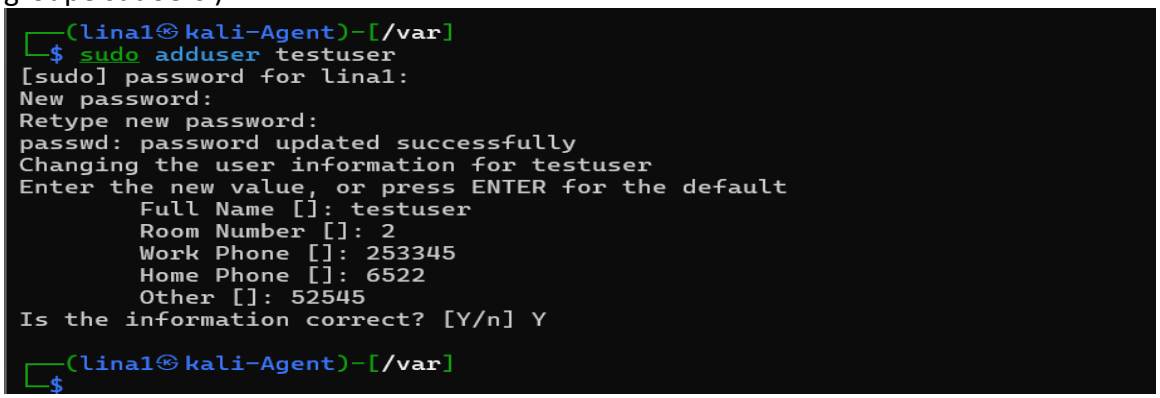
c- Démarrer l'agent à l'aide de la commande suivante toujours dans en PowerShell en tant qu'administrateur :
Start-Service wazuhsvc



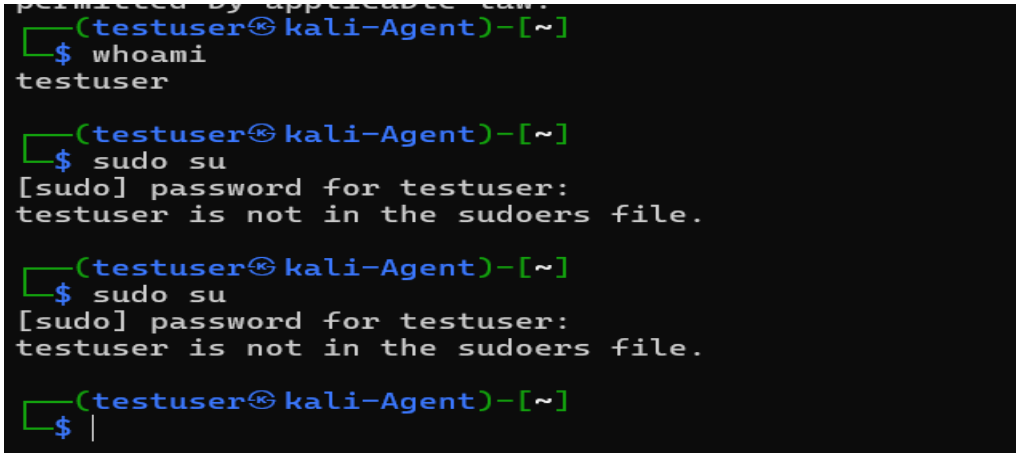
4-DÉTECTIONS DE NATURE DIFFÉRENTE

- **Sur l'hôte linux**

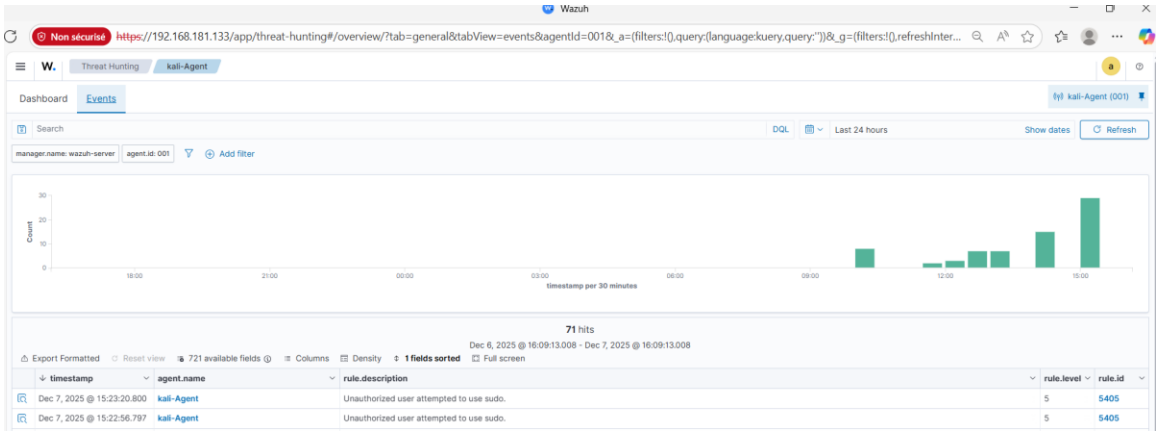
Sur l'agent Kali, j'ai crée simple utilisateur (c'est-à-dire qui n'est pas dans le groupe sudoers).



Je me suis ensuite connecté avec cet utilisateur puis j'ai fait une tentative d'élévation de privilège qui a bien évidemment échouée.



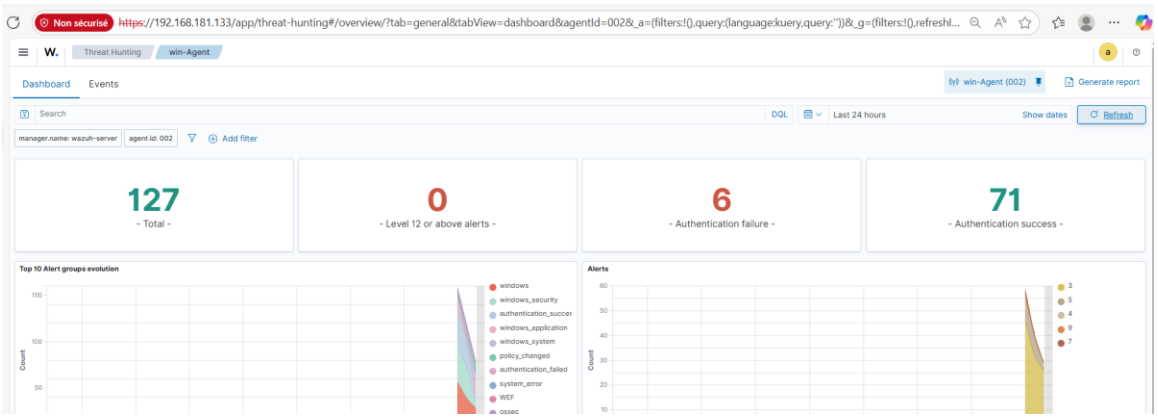
Cet incident a aussitôt été rapporté par l'agent wazuh au niveau du manager.

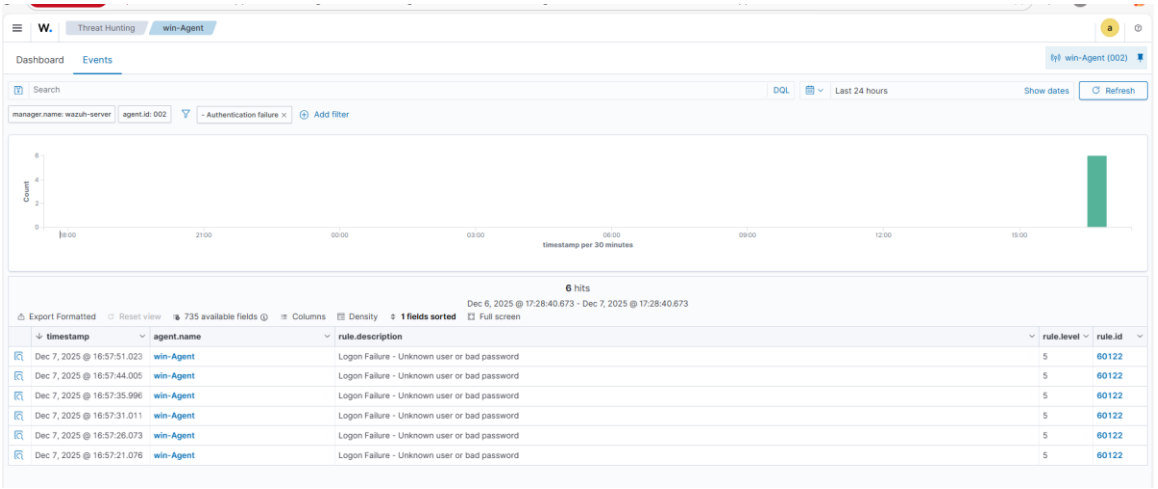


- **Sur l'hôte Windows**

Pour ce qui est de l'hôte Windows, je me suis connectée normalement avec le compte « lina2 » et son mot de passe, puis j'ai verrouillé la session. J'ai en suite réessayé à me connecter avec le compte « lina2 » sauf que cette fois ci j'ai entré un faux mot de passe. La tentative de connexion a bien sûr échoué mais j'ai répété cela plusieurs fois. Après la 5^{ième} tentative j'ai eu le message présent sur la capture d'écran ce dessous.

Cet incident a effectivement été rapporté par l'agent wazuh au manager.

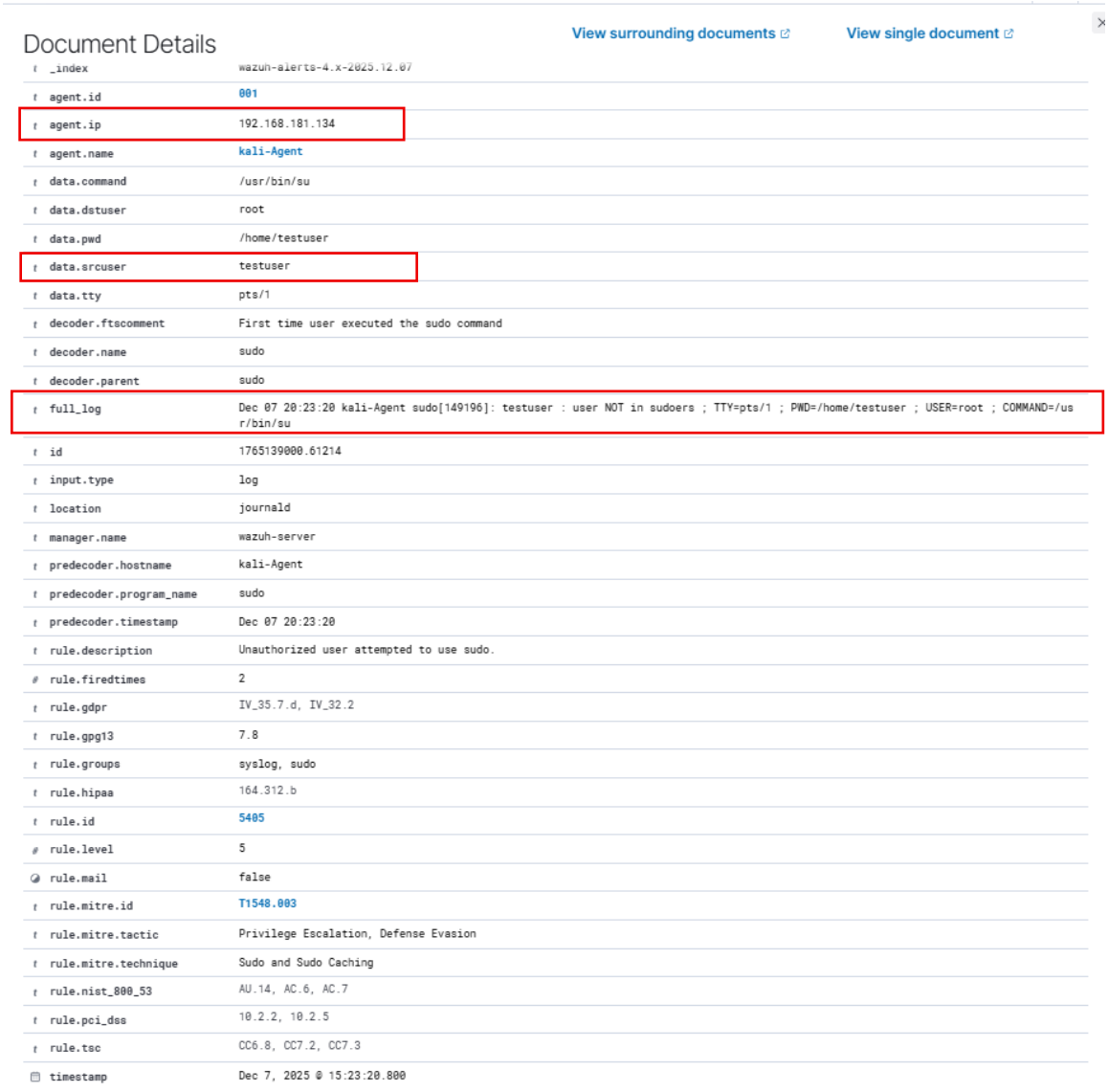




NB : Il est à noter que pour chacun des agents j'ai modifié la fréquence de report des évènements pour la mettre à 10s dans le fichier ossec.conf.

5-ÉLÉMENTS D'ANALYSE LIÉS À CES DEUX DÉTECTIONS

- Pour la tentative d'élévation de privilège, afin de déterminer s'il s'agit d'un vrai positif ou un faux positif, je chercherai à connaitre : l'utilisateur qui est à l'origine de cet incident, cet utilisateur est-il dans le fichier sudoers, l'adresse ip de la machine depuis laquelle il a effectué la tentative. Pour répondre à ces questions, je vais consulter les détails de l'incident.



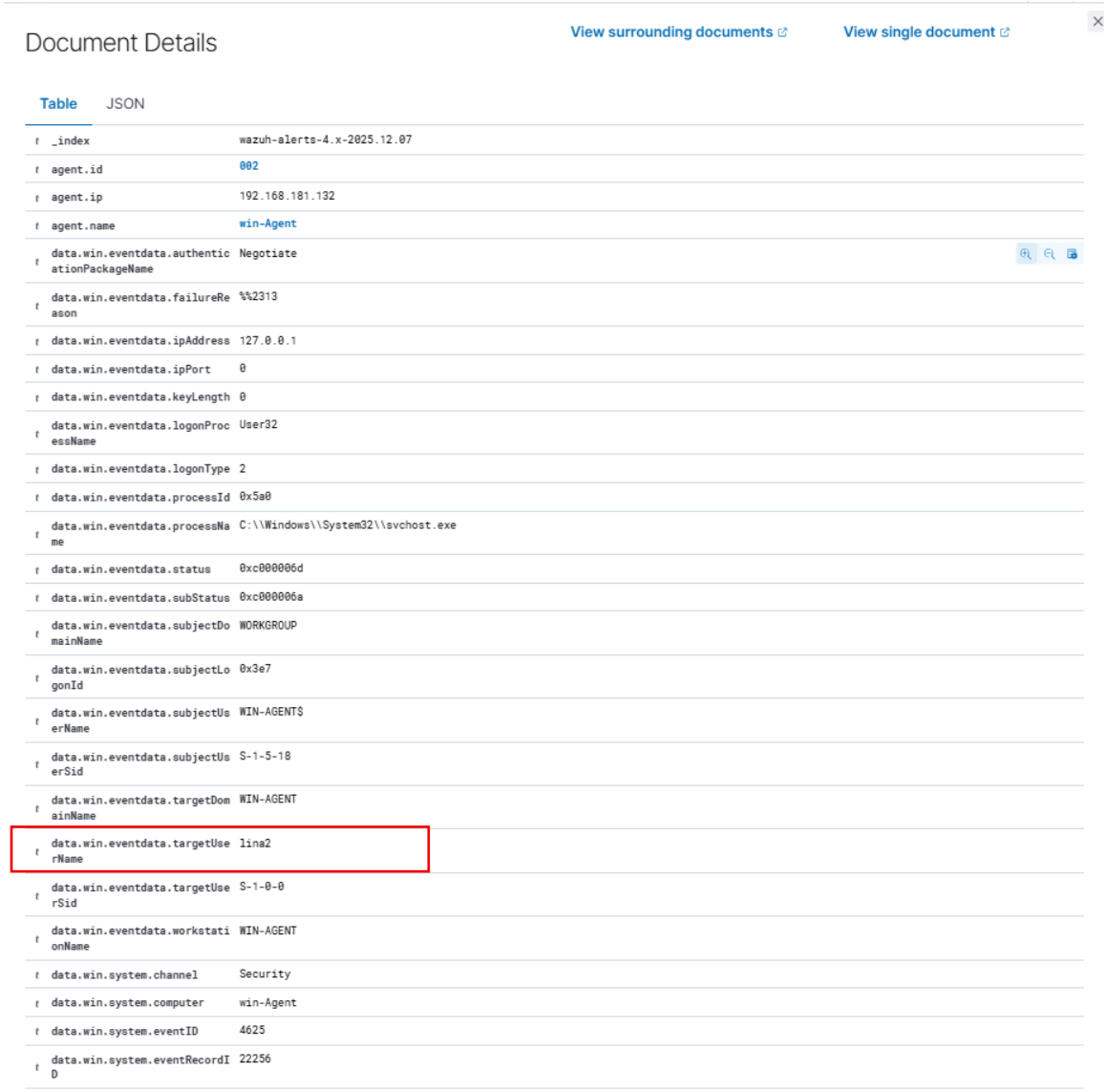
Document Details

View surrounding documents | View single document

_index	wazuh-alerts-4.x-2025.12.07
agent.id	001
agent.ip	192.168.181.134
agent.name	kali-Agent
data.command	/usr/bin/su
data.dstuser	root
data.pwd	/home/testuser
data.srcuser	testuser
data.tty	pts/1
decoder.ftscomment	First time user executed the sudo command
decoder.name	sudo
decoder.parent	sudo
full_log	Dec 07 20:23:20 kali-Agent sudo[149196]: testuser : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/testuser ; USER=root ; COMMAND=/usr/bin/su
id	1765139000.61214
input.type	log
location	journald
manager.name	wazuh-server
predecoder.hostname	kali-Agent
predecoder.program_name	sudo
predecoder.timestamp	Dec 07 20:23:20
rule.description	Unauthorized user attempted to use sudo.
rule.firedtimes	2
rule.gdpr	IV_35.7.d, IV_32.2
rule.gpg13	7.8
rule.groups	syslog, sudo
rule.hipaa	164.312.b
rule.id	5405
rule.level	5
rule.mail	false
rule.mitre.id	T1548.003
rule.mitre.tactic	Privilege Escalation, Defense Evasion
rule.mitre.technique	Sudo and Sudo Caching
rule.nist_800_53	AU.14, AC.6, AC.7
rule.pci_dss	10.2.2, 10.2.5
rule.tsc	CC6.8, CC7.2, CC7.3
timestamp	Dec 7, 2025 @ 15:23:20.800

D’après ces détails, l’utilisateur en question est « testuser » et il n’est pas dans le fichier sudoers(Voir les encadrés rouges sur l’image ci-dessus) donc il s’agit d’un **vrai positif**.

- Pour les tentatives de connexion échouée, afin de déterminer s’il s’agit d’un vrai positif ou d’un faux positif, je vais regarder les détails de l’incident pour savoir quel utilisateur en est l’auteur. Je vais également regarder le nombre de tentatives ainsi que l’intervalle de temps entre les différentes tentatives.



D’après les détails, je vois qu’il s’agit de l’utilisateur « lina2 ». Lorsque je me rapproche d’elle pour avoir plus d’information sur les causes de cet incident, elle me confirme qu’effectivement elle s’est bien connectée quelques minutes avant, puis elle a verrouillé son compte parce qu’elle avait une envie pressante, sauf qu’à son retour elle a constaté que la fenêtre d’authentification était bloquée. Fort de toutes ces informations, je conclue qu’il s’agit d’un vrai positif (tentative de brute forcing).

6-RAPPORT WAZUH

Pour produire le rapport à partir de wazuh, je me rends sur la page d'accueil de wazuh puis je clique sur « threat Hunting ». Une fois rendu sur cette interface, j'entre le filtre suivant « agent_id : 001 OR agent_id : 002 » puis je clique sur « Generate report » (Voir les encadrés rouges sur l'image ci-dessous).