Configuration des alertes FIM sur Wazuh (surveillance du fichier hosts) Objectif

NOM: KOUASSI

PRENOM: GLOHNDY

ETABLISSEMENT: ORT-TOULOUSE

Table des matières

1. Pré-requis

- Installation complète de Wazuh (TP1).
- Déploiement des agents Wazuh sur Debian 12 et Windows 10 (TP2).
- Accès root/sudo sur Debian ; Administrateur sur Windows.
- Optionnel : Intégration Virus Total.

2. File Integrity Monitoring / Surveillance de l’ intégrité des fichiers

Les alertes FIM détectent toute modification sur les fichiers ou répertoires surveillés.

Dans ce TP, nous avons choisi de monitorer le fichier **hosts** :

Pour Debian 12

`/etc/hosts` sur Debian 12

Pour Windows 10

`C:\Windows\System32\drivers\etc\hosts` sur Windows 10

> Le FIM est crucial pour la détection précoce des compromissions de système, car le fichier `hosts` est souvent ciblé par les attaquants pour la redirection de trafic.

Configuration FIM

Pour Debian 12

Accéder au fichier de configuration de l’agent Wazuh :

```
sudo nano /var/ossec/etc/ossec.conf
```

Ajouter la ligne suivante dans le bloc :

```
<directories check_all="yes" report_changes="yes" realtime="yes">/etc/hosts</directories>
```

- `check_all="yes"` : surveille toutes les métadonnées du fichier.
- `report_changes="yes"` : signale toutes les modifications.
- `realtime="yes"` : active la surveillance en temps réel.

Redémarrer l’agent Wazuh :

```
sudo systemctl restart wazuh-agent
```

Vérifier que toutes les actions sont répertoriées après modification du fichier `/etc/hosts`.

Pour Windows 10

Accéder au fichier `ossec.conf` :

```
C:\Program Files (x86)\ossec-agent\ossec.conf
```

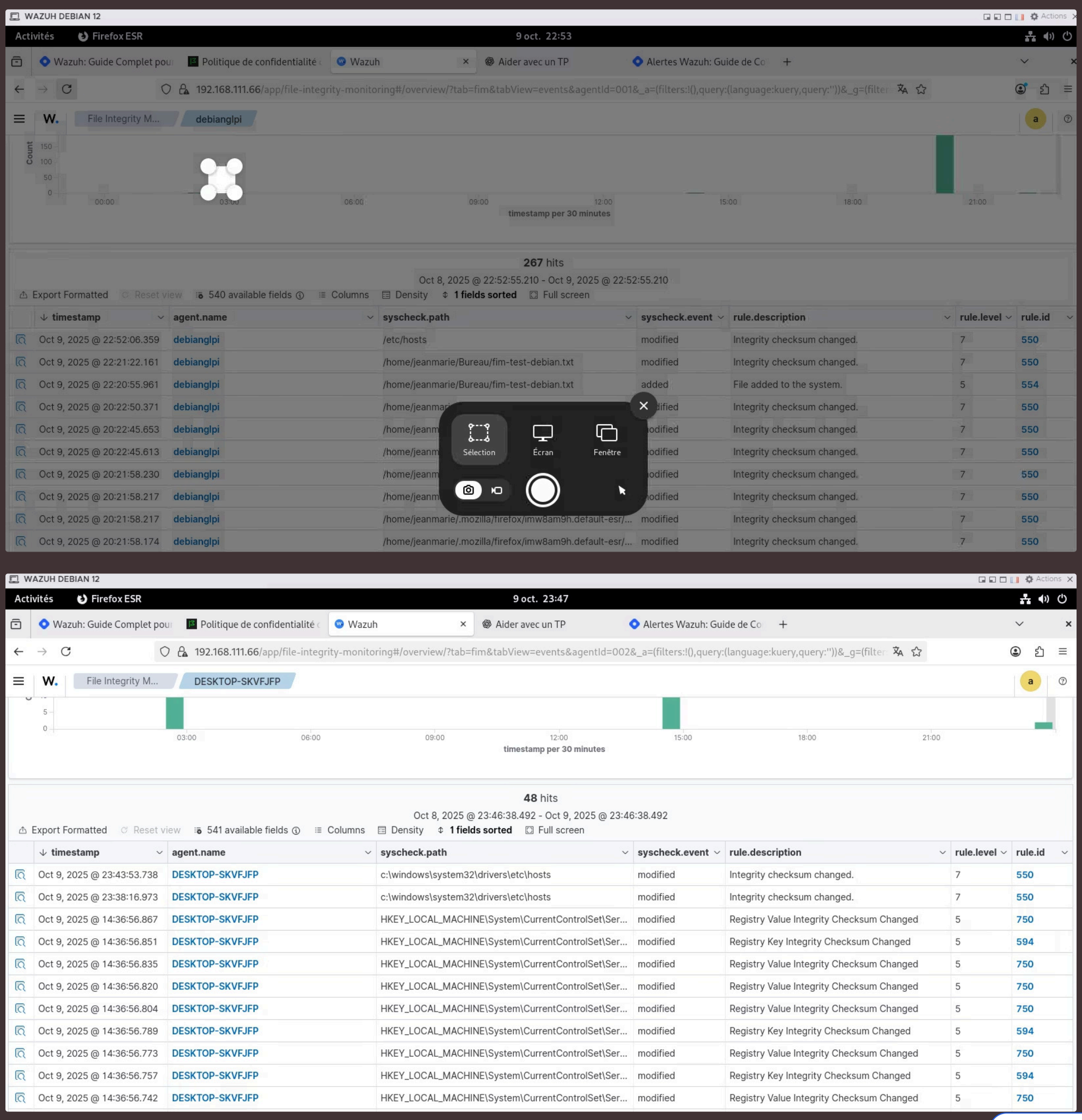
Ajouter dans le bloc :

```
<directories check_all="yes" report_changes="yes" realtime="yes">C:\Windows\System32\drivers\etc\hosts</directories>
```

Redémarrer le service Wazuh :

```
net stop WazuhSvc
net start WazuhSvc
```

Après modification du fichier hosts, Wazuh répertorie toutes les actions avec la date, l’événement, et l’agent concerné.



3. Whodata

La règle whodata fournit des informations sur l’ utilisateur et le processus ayant effectué la modification.

Pour Debian 12

Installer audit et les plugins nécessaires :

```
sudo apt-get install auditd audispd-plugins
sudo systemctl restart auditd
```

Modifier le fichier `/var/ossec/etc/ossec.conf` et ajouter dans :

```
<directories check_all="yes" report_changes="yes"
realtime="yes"
whodata="yes">/etc/hosts</directories>
```

Redémarrer l’ agent Wazuh :

```
sudo systemctl restart wazuh-agent
```

Pour Windows 10

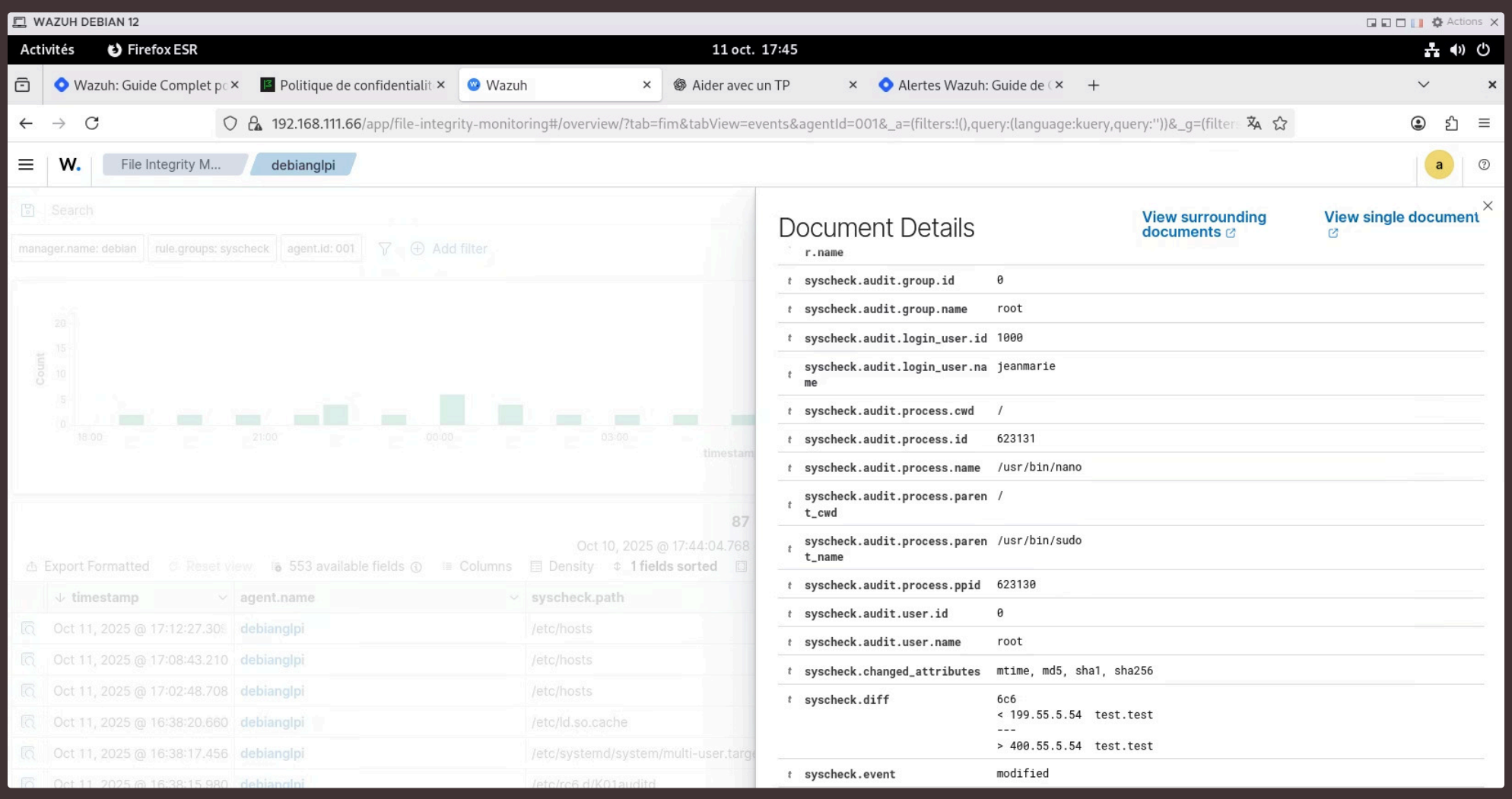
Dans le fichier `ossec.conf`, ajouter dans :

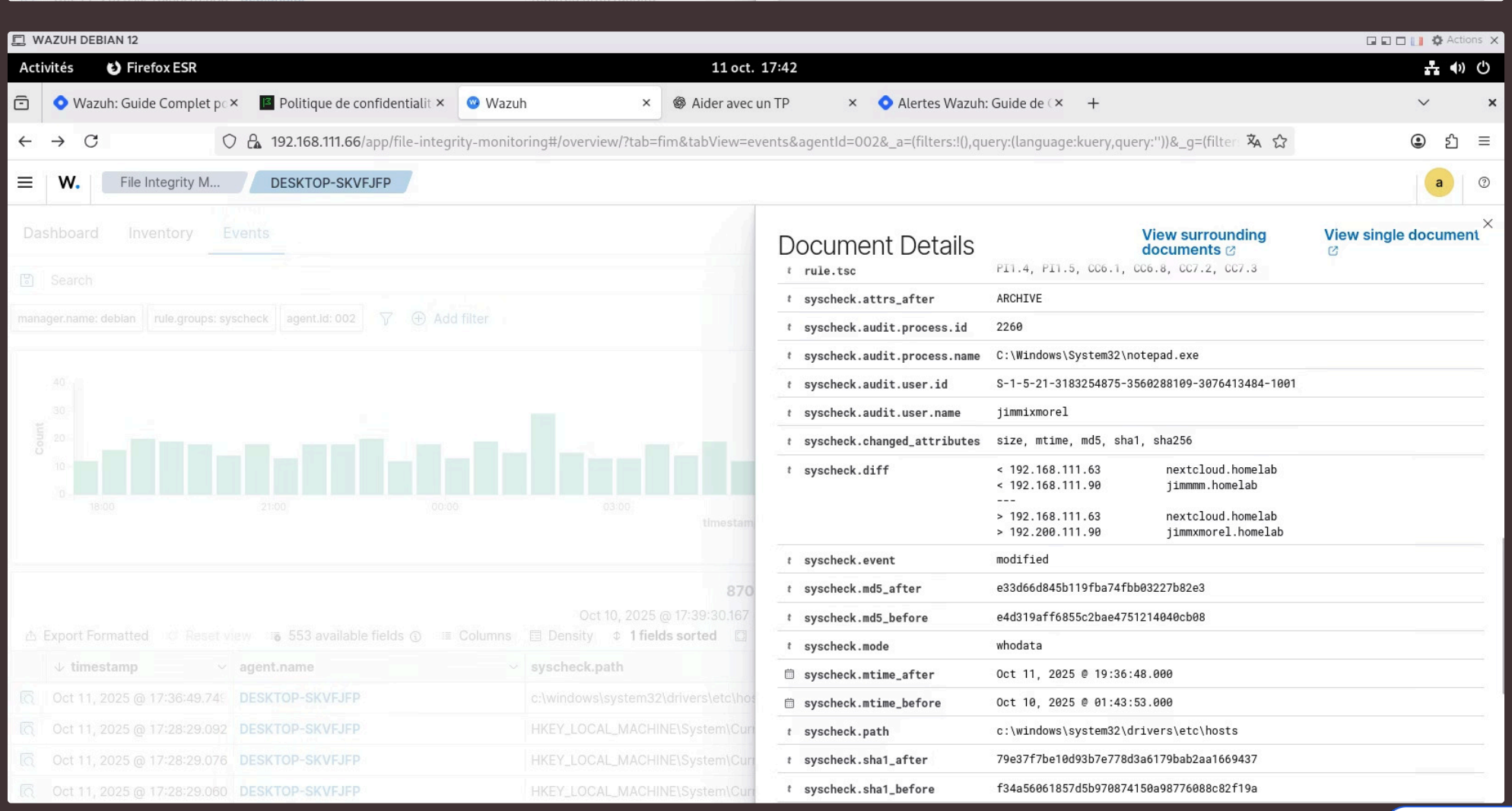
```
<directories check_all="yes" report_changes="yes"
realtime="yes"
whodata="yes">C:\Windows\System32\drivers\etc\
hosts</directories>
```

Redémarrer le service Wazuh :

```
net stop WazuhSvc
net start WazuhSvc
```

Le Dashboard Wazuh affichera le nom de l’ utilisateur et le processus ayant modifié le fichier hosts.





4. Détection d’ une attaque par force brute

Vérifier que le bloc pour `firewall-drop` est présent dans `/var/ossec/etc/ossec.conf` :

```
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>5760,5761,5762</rules_id>
  <timeout>180</timeout>
</active-response>
```

Ajouter la réponse active :

```
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>5763</rules_id>
  <timeout>180</timeout>
</active-response>
```

Redémarrer le manager :

```
sudo systemctl restart wazuh-manager
```

Préparation de l'attaque (Hydra)

Installer Hydra sur la machine attaquante :

```
sudo apt update
sudo apt install -y hydra
```

Créer un fichier de mots de passe pour l’ attaque :

```
pwdgen 8 10 > password.txt
```

Lancement de l'attaque

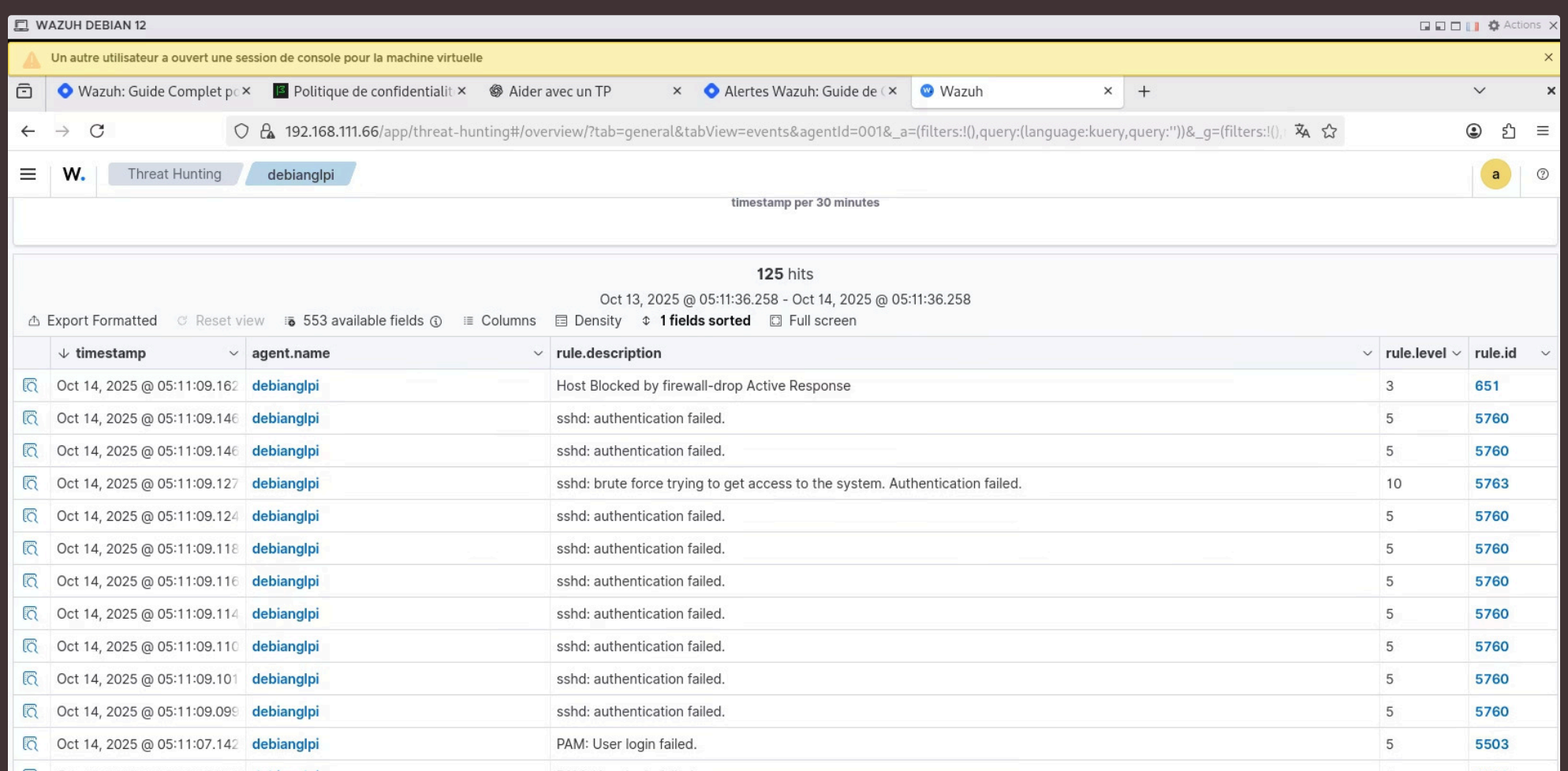
Lancer l’ attaque SSH :

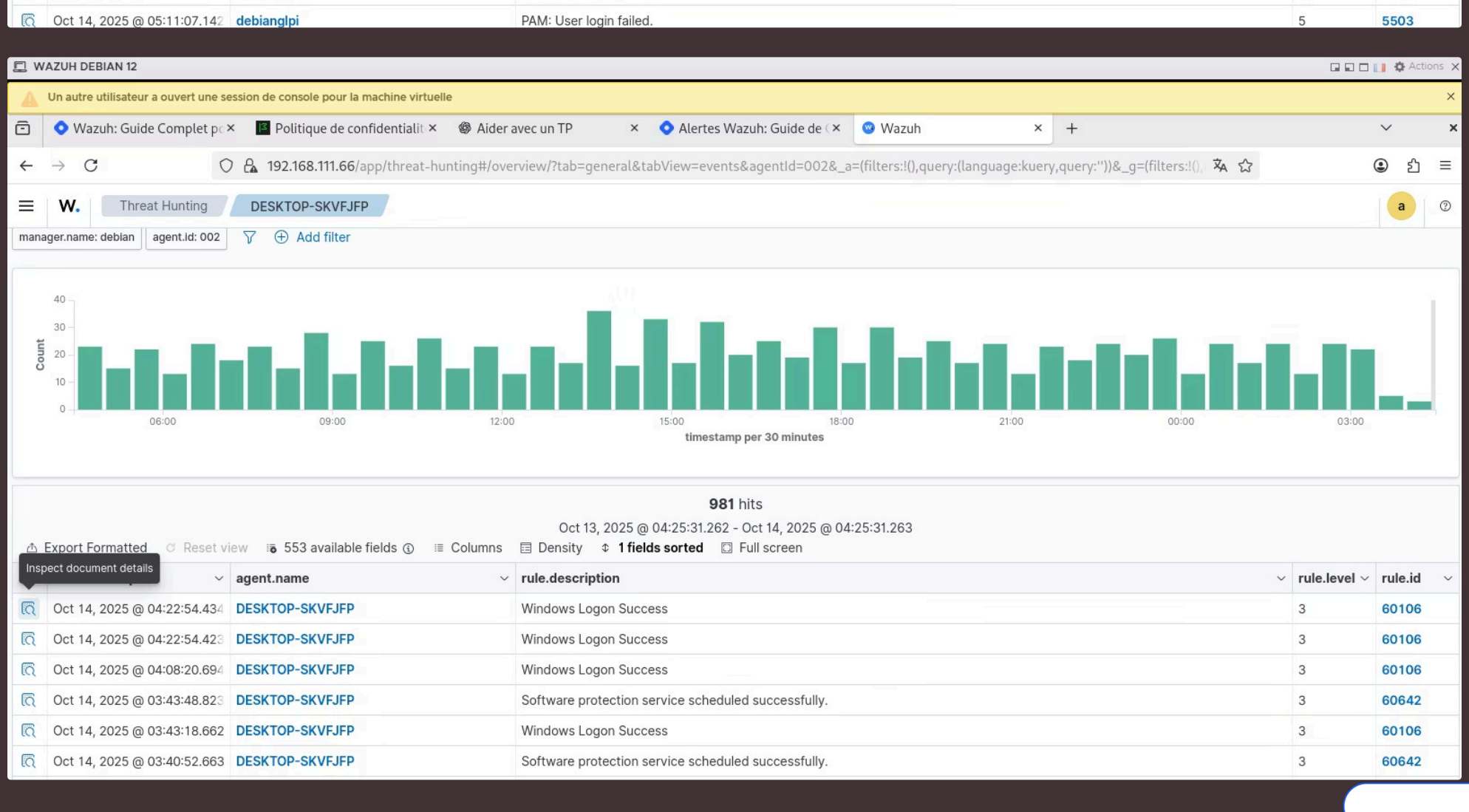
```
sudo hydra -l <user> -P password.txt
ssh://<target_ip>
```

Pour Windows (RDP) :

```
sudo hydra -l <user> -P password.txt
rdp://<target_ip>
```

Visualiser l’ incident dans le Dashboard Wazuh (Threat Hunting → Events).





5. Conclusion

Surveillance Essentielle

La surveillance du fichier hosts permet de détecter toute modification non autorisée.

Traçabilité Complète

Wazuh FIM avec **whodata** permet de savoir qui a modifié le fichier et quand.

Configuration Détaillée

Le TP montre la configuration sur Debian 12 et Windows 10 avec toutes les étapes détaillées du TP original.

Alertes Fonctionnelles

La configuration est complète et les alertes remontent correctement dans le Dashboard.