

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

NOM: KOUASSI

PRENOM: GLOHNDY

ETABLISSEMENT: ORT-TOULOUSE

wazuh

Table des matières



Pré-requis



File Integrity Monitoring / Surveillance de l' intégrité des fichiers



Pour Debian 12



Pour Windows 10



Whodata



Détection d' une attaque par force brute



Conclusion

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\h
osts</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.

WAZUH DEBIAN 12

9 oct. 22:53

Wazuh

192.168.111.66/app/file-integrity-monitoring#/overview/?tab=fim&tabView=events&agentId=001&a=(filters:!(,query:(language:kuery,query:'))&_g=(filter

File Integrity M... debianglpi

Count

150

100

50

0

00:00

03:00

06:00

09:00

12:00

15:00

18:00

21:00

timestamp per 30 minutes

267 hits

Oct 8, 2025 @ 22:52:55.210 - Oct 9, 2025 @ 22:52:55.210

Export Formatted Reset view 540 available fields Columns Density 1 fields sorted Full screen

timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Oct 9, 2025 @ 22:52:06.359	debianglpi	/etc/hosts	modified	Integrity checksum changed.	7	550
Oct 9, 2025 @ 22:21:22.161	debianglpi	/home/jeanmarie/Bureau/fim-test-debian.txt	modified	Integrity checksum changed.	7	550
Oct 9, 2025 @ 22:20:55.961	debianglpi	/home/jeanmarie/Bureau/fim-test-debian.txt	added	File added to the system.	5	554
Oct 9, 2025 @ 20:22:50.371	debianglpi	/home/jeanmarie/Bureau/fim-test-debian.txt	modified	Integrity checksum changed.	7	550
Oct 9, 2025 @ 20:22:45.653	debianglpi	/home/jeanmarie/Bureau/fim-test-debian.txt	modified	Integrity checksum changed.	7	550
Oct 9, 2025 @ 20:22:45.613	debianglpi	/home/jeanmarie/Bureau/fim-test-debian.txt	modified	Integrity checksum changed.	7	550
Oct 9, 2025 @ 20:21:58.230	debianglpi	/home/jeanmarie/Bureau/fim-test-debian.txt	modified	Integrity checksum changed.	7	550
Oct 9, 2025 @ 20:21:58.217	debianglpi	/home/jeanmarie/Bureau/fim-test-debian.txt	modified	Integrity checksum changed.	7	550
Oct 9, 2025 @ 20:21:58.217	debianglpi	/home/jeanmarie/.mozilla/firefox/jmw8am9h.default-esr/...	modified	Integrity checksum changed.	7	550
Oct 9, 2025 @ 20:21:58.174	debianglpi	/home/jeanmarie/.mozilla/firefox/jmw8am9h.default-esr/...	modified	Integrity checksum changed.	7	550

WAZUH DEBIAN 12

9 oct. 23:47

Wazuh

192.168.111.66/app/file-integrity-monitoring#/overview/?tab=fim&tabView=events&agentId=002&a=(filters:!(,query:(language:kuery,query:'))&_g=(filter

File Integrity M... DESKTOP-SKVFJFP

Count

5

0

03:00

06:00

09:00

12:00

15:00

18:00

21:00

timestamp per 30 minutes

48 hits

Oct 8, 2025 @ 23:46:38.492 - Oct 9, 2025 @ 23:46:38.492

Export Formatted Reset view 541 available fields Columns Density 1 fields sorted Full screen

timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Oct 9, 2025 @ 23:43:53.738	DESKTOP-SKVFJFP	c:\windows\system32\drivers\etc\hosts	modified	Integrity checksum changed.	7	550
Oct 9, 2025 @ 23:38:16.973	DESKTOP-SKVFJFP	c:\windows\system32\drivers\etc\hosts	modified	Integrity checksum changed.	7	550
Oct 9, 2025 @ 14:36:56.867	DESKTOP-SKVFJFP	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Oct 9, 2025 @ 14:36:56.851	DESKTOP-SKVFJFP	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksum Changed	5	594
Oct 9, 2025 @ 14:36:56.835	DESKTOP-SKVFJFP	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Oct 9, 2025 @ 14:36:56.820	DESKTOP-SKVFJFP	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Oct 9, 2025 @ 14:36:56.804	DESKTOP-SKVFJFP	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Oct 9, 2025 @ 14:36:56.789	DESKTOP-SKVFJFP	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksum Changed	5	594
Oct 9, 2025 @ 14:36:56.773	DESKTOP-SKVFJFP	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Oct 9, 2025 @ 14:36:56.757	DESKTOP-SKVFJFP	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksum Changed	5	594
Oct 9, 2025 @ 14:36:56.742	DESKTOP-SKVFJFP	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750

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
```

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

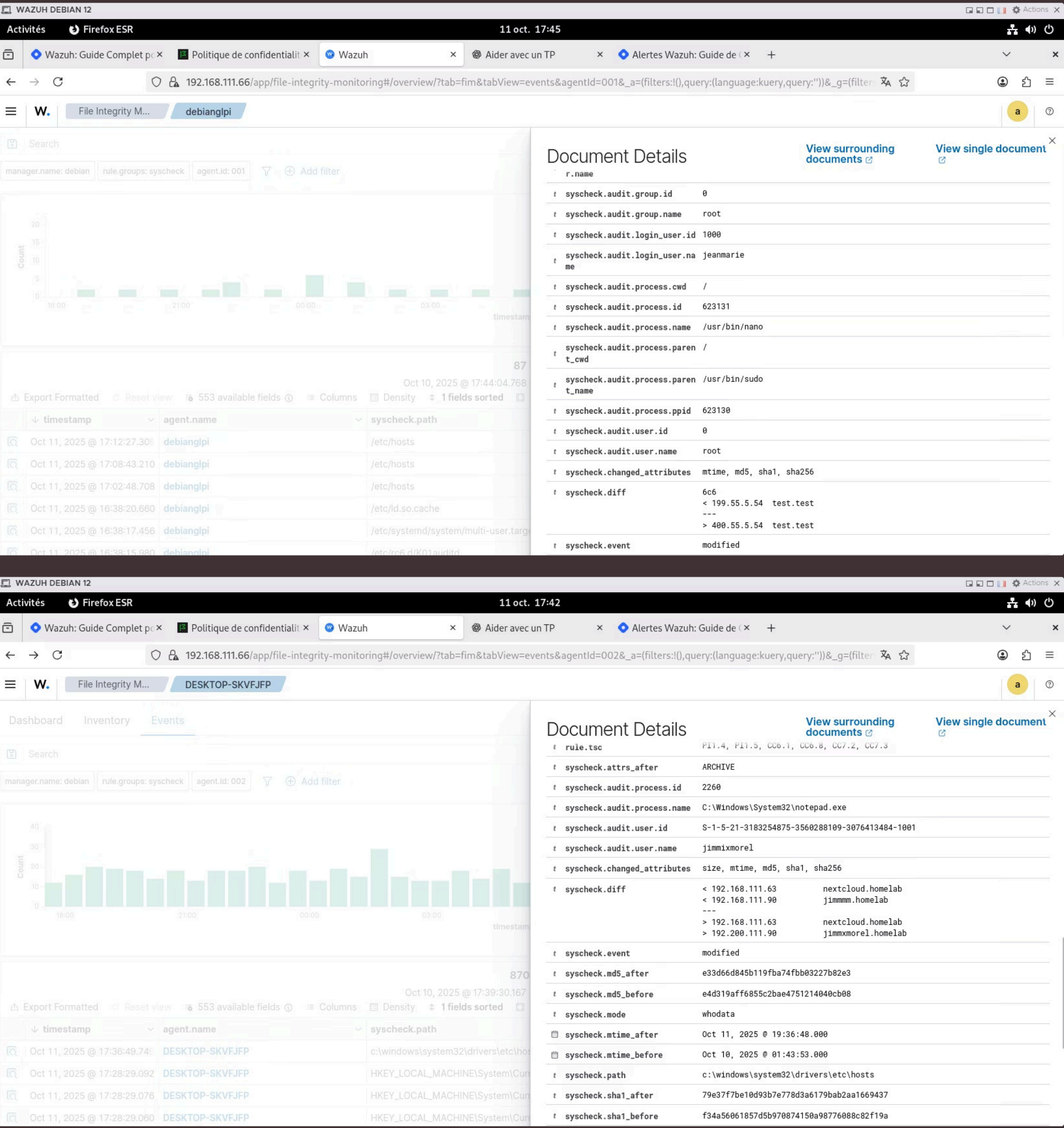
Pour Windows 10

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
```



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).

WAZUH DEBIAN 12

Un autre utilisateur a ouvert une session de console pour la machine virtuelle

Wazuh: Guide Complet p...Politique de confidentialit...Aider avec un TPAlertes Wazuh: Guide de...Wazuh

192.168.111.66/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=001&_a=(filters:!((),query:(language:kuery,query:"))&_g=(filters:!((),

Threat Huntingdebianglpi

timestamp per 30 minutes

125 hits

Oct 13, 2025 @ 05:11:36.258 - Oct 14, 2025 @ 05:11:36.258

Export FormattedReset view553 available fieldsColumnsDensity1 fields sortedFull screen

	timestamp	agent.name	rule.description	rule.level	rule.id
	Oct 14, 2025 @ 05:11:09.162	debianglpi	Host Blocked by firewall-drop Active Response	3	651
	Oct 14, 2025 @ 05:11:09.146	debianglpi	sshd: authentication failed.	5	5760
	Oct 14, 2025 @ 05:11:09.146	debianglpi	sshd: authentication failed.	5	5760
	Oct 14, 2025 @ 05:11:09.127	debianglpi	sshd: brute force trying to get access to the system. Authentication failed.	10	5763
	Oct 14, 2025 @ 05:11:09.124	debianglpi	sshd: authentication failed.	5	5760
	Oct 14, 2025 @ 05:11:09.118	debianglpi	sshd: authentication failed.	5	5760
	Oct 14, 2025 @ 05:11:09.116	debianglpi	sshd: authentication failed.	5	5760
	Oct 14, 2025 @ 05:11:09.114	debianglpi	sshd: authentication failed.	5	5760
	Oct 14, 2025 @ 05:11:09.110	debianglpi	sshd: authentication failed.	5	5760
	Oct 14, 2025 @ 05:11:09.101	debianglpi	sshd: authentication failed.	5	5760
	Oct 14, 2025 @ 05:11:09.098	debianglpi	sshd: authentication failed.	5	5760
	Oct 14, 2025 @ 05:11:07.142	debianglpi	PAM: User login failed.	5	5503
	Oct 14, 2025 @ 05:11:07.142	debianglpi	PAM: User login failed.	5	5503

WAZUH DEBIAN 12

Un autre utilisateur a ouvert une session de console pour la machine virtuelle

Wazuh: Guide Complet p...Politique de confidentialit...Aider avec un TPAlertes Wazuh: Guide de...Wazuh

192.168.111.66/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=002&_a=(filters:!((),query:(language:kuery,query:"))&_g=(filters:!((),

Threat HuntingDESKTOP-SKVFJFP

manager.name: debianagent.id: 002Add filter

Count

timestamp per 30 minutes

981 hits

Oct 13, 2025 @ 04:25:31.262 - Oct 14, 2025 @ 04:25:31.263

Export FormattedInspect document detailsReset view553 available fieldsColumnsDensity1 fields sortedFull screen

	agent.name	rule.description	rule.level	rule.id
	DESKTOP-SKVFJFP	Windows Logon Success	3	60106
	DESKTOP-SKVFJFP	Windows Logon Success	3	60106
	DESKTOP-SKVFJFP	Windows Logon Success	3	60106
	DESKTOP-SKVFJFP	Software protection service scheduled successfully.	3	60642
	DESKTOP-SKVFJFP	Windows Logon Success	3	60106
	DESKTOP-SKVFJFP	Software protection service scheduled successfully.	3	60642

5. Conclusion

Surveillance Essentielle

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

Configuration Détaillée

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

Traçabilité Complète

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

Alertes Fonctionnelles

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