Mise en place de la détection de modification dans les fichiers sensible avec Wazuh

Last updated by | Leslie Lemaire | 18 juin 2025 at 19:06 UTC+2

📋 Détection de fichiers avec Wazuh – FIM `/etc` + Fail2Ban

Ce fichier documente deux types de détections réalisées avec Wazuh sur un agent Debian 12 (`Zimbra`) :

- La **surveillance d'intégrité des fichiers** avec le module FIM

✅ 1. Détection FIM `/etc` (File Integrity Monitoring)

🔧 Configuration `ossec.conf` sur l'agent

```
<syscheck>
  <directories check_all="yes" realtime="yes" report_changes="yes">/etc</directories>
  <frequency>43200</frequency>
  <scan_on_start>yes</scan_on_start>
</syscheck>
```

🧪 Test manuel simple

```
# Créer un fichier de test
sudo touch /etc/wazuh_test

# Lancer un scan FIM manuel (si realtime ne fonctionne pas)
sudo /opt/wazuh-agent/bin/syscheck_control -u
```

🔍 Vérification locale

```
sudo tail -n 30 /var/ossec/logs/ossec.log
```

Tu devrais voir :

```
File '/etc/wazuh_test' added
```

🖥️ Vérification dans Wazuh Web

- **Endpoints > Zimbra > File Integrity Monitoring**
- Voir le fichier `/etc/wazuh_test` comme "added"
- Ou passer par `Explore > Discover` avec la requête :

```
rule.group: "syscheck"
```

🧠 Remarques

- Les événements Fail2Ban ne s'affichent **pas** dans `File Integrity Monitoring`, mais uniquement dans `Discover` ou des dashboards personnalisés.
- Le module FIM ne détecte **que les changements sur disque**, pas les logs ou événements système.