

Cas pratiques de quelques Attaques et comment wazuh les détecte

➤ Surveillance de l'intégrité des fichiers

La surveillance de l'intégrité des fichiers (FIM) est un processus de sécurité utilisé pour surveiller l'intégrité des fichiers système et applicatifs. Elle constitue une couche de sécurité essentielle pour toute organisation surveillant des actifs sensibles. Elle protège les données sensibles, les fichiers d'applications et les fichiers des appareils en les surveillant, en les analysant régulièrement et en vérifiant leur intégrité. Elle aide les organisations à détecter les modifications apportées aux fichiers critiques de leurs systèmes, réduisant ainsi le risque de vol ou de compromission de données. Ce processus permet de gagner du temps et de l'argent en termes de perte de productivité, de perte de revenus, d'atteinte à la réputation et de sanctions pour non-conformité légale et réglementaire.

Wazuh intègre une fonctionnalité de surveillance de l'intégrité des fichiers. Le module FIM de Wazuh surveille les fichiers et les répertoires et déclenche une alerte lorsqu'un utilisateur ou un processus crée, modifie ou supprime des fichiers surveillés. Il exécute une analyse de référence, stockant la somme de contrôle cryptographique et d'autres attributs des fichiers surveillés. Lorsqu'un utilisateur ou un processus modifie un fichier, le module compare sa somme de contrôle et ses attributs à la référence. Il déclenche une alerte en cas de non-concordance. Le module FIM effectue des analyses en temps réel et planifiées, selon la configuration FIM des agents et du gestionnaire.

Ce cas d'utilisation utilise le module Wazuh FIM pour détecter les modifications dans les répertoires surveillés sur les terminaux Ubuntu et Windows. Le module Wazuh FIM enrichit les données d'alerte en récupérant des informations sur l'utilisateur et le processus ayant effectué les modifications à l'aide de who-data audit .

Cas pratique en place de la surveillance FIM avec Wazuh (Serveur Ubuntu + A

Configurer la surveillance de l'intégrité des fichiers (FIM) avec Wazuh pour :

Machine Ubuntu (collecte et analyse des alertes)

Machine virtuelle Ubuntu Focal (surveillance du dossier /root)

1. Configurer la connexion au serveur depuis l'agent : c'est-à-dire renseigner l'adresse IP du serveur wazuh

```
<ossec_config>
<client>
<server>
  <address>192.168.2.20</address>
  <port>1514</port>
  <protocol>tcp</protocol>
</server>
<config-profile>ubuntu, ubuntu20, ubuntu20.04</config-profile>
```

2. Activation du FIM pour /root

Modifiez le fichier de configuration sur le terminal surveillé. Ajoutez les répertoires à surveiller dans le bloc. Pour ce cas d'utilisation, configurez Wazuh pour surveiller le répertoire. Et pour cela ajouter cette ligne dans le 'syscheck' qui se trouve dans ce chemin `/var/ossec/etc/ossec.conf`

```
<directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>
```

```
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>
  <directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>
  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

  <!-- Directories to check (perform all possible verifications) -->
```

3. Redémarrage de l'agent

```
sudo systemctl enable wazuh-agent
```

```
sudo systemctl start wazuh-agent
```

4. Test et validation

Pour ce faire nous devons créer des fichiers et les supprimer pour vérifier que notre configuration fonctionne correctement

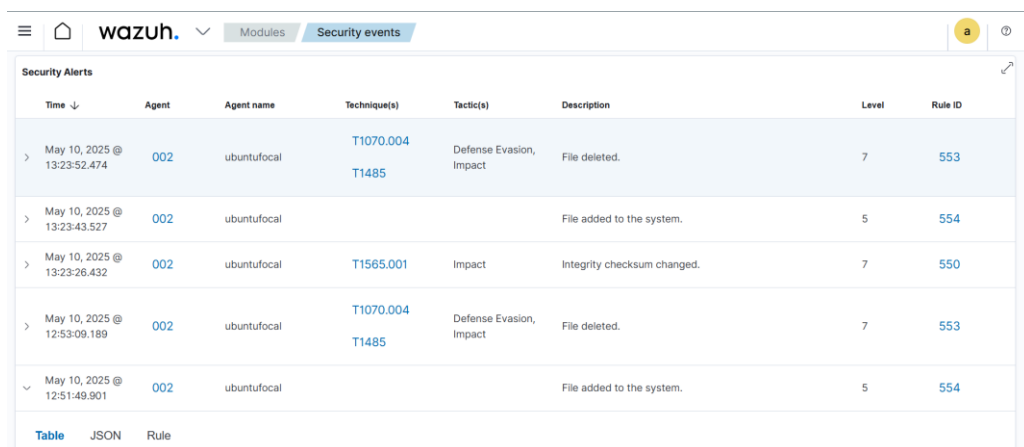
```
root@ubuntu-focal:~# vim /var/ossec/etc/ossec.conf
root@ubuntu-focal:~# sudo touch /root/mikemikemike.txt
root@ubuntu-focal:~# sudo rm /root/mikemikemike.txt
root@ubuntu-focal:~#
```

5. Vérification des alertes

- ✓ Connectez-vous au Dashboard Wazuh
- ✓ Allez dans **Security Events**
- ✓ Appliquez le filtre :

rule.id: (550 OR 553 OR 554) AND agent.name:"ubuntufocal"

Pour avoir les derniers logs qui ont été fait



The screenshot shows the Wazuh Security Events dashboard. The top navigation bar includes the Wazuh logo, a dropdown menu, and a 'Modules' tab with 'Security events' selected. Below the navigation bar, there's a 'Security Alerts' section with a table of alerts. The table has columns for Time, Agent, Agent name, Technique(s), Tactic(s), Description, Level, and Rule ID. There are five rows of alerts, all for agent '002' and agent name 'ubuntufocal'. The first row shows a file deletion event (Rule ID 553) at May 10, 2025 @ 13:23:52.474. The second row shows a file addition event (Rule ID 554) at May 10, 2025 @ 13:23:43.527. The third row shows an integrity checksum change event (Rule ID 550) at May 10, 2025 @ 13:23:26.432. The fourth row shows another file deletion event (Rule ID 553) at May 10, 2025 @ 12:53:09.189. The fifth row shows another file addition event (Rule ID 554) at May 10, 2025 @ 12:51:49.901. At the bottom of the table, there are tabs for 'Table', 'JSON', and 'Rule'.

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> May 10, 2025 @ 13:23:52.474	002	ubuntufocal	T1070.004 T1485	Defense Evasion, Impact	File deleted.	7	553
> May 10, 2025 @ 13:23:43.527	002	ubuntufocal			File added to the system.	5	554
> May 10, 2025 @ 13:23:26.432	002	ubuntufocal	T1565.001	Impact	Integrity checksum changed.	7	550
> May 10, 2025 @ 12:53:09.189	002	ubuntufocal	T1070.004 T1485	Defense Evasion, Impact	File deleted.	7	553
✓ May 10, 2025 @ 12:51:49.901	002	ubuntufocal			File added to the system.	5	554

Table JSON Rule

Nous avons donc ici présent tout ce qui a été fait. Wazuh nous notifie de la création et de la suppression du fichier et notifie également l'heure et la date et tout ce qui se fait dans le système concernant les fichiers.