Intégrer VirusTotal dans Wazuh & configurer la surveillance de l'intégrité des fichiers

I – Intégrer VirusTotal à Wazuh

VirusTotal est un service en ligne gratuit qui permet d'analyser des fichiers suspects et des URL en utilisant plusieurs antivirus et outils de détection de logiciels malveillants. Il a été acquis par **Google** en **2012**.

Les utilisateurs peuvent soumettre des fichiers ou des URL à **VirusTotal**, qui les analysera en utilisant une grande variété de logiciels antivirus et d'autres outils de sécurité.

VirusTotal fournit ensuite un rapport détaillé sur les résultats de l'analyse, permettant aux utilisateurs de déterminer si un fichier ou une URL est potentiellement dangereux.

C'est un outil largement utilisé par les chercheurs en sécurité, les administrateurs système et les utilisateurs individuels pour vérifier la sécurité des fichiers et des liens avant de les ouvrir ou de les télécharger.

Dans notre contexte de **Wazuh**, **VirusTotal** est souvent intégré comme un moyen supplémentaire d'analyser les fichiers suspects ou les événements potentiellement malveillants.

En intégrant **VirusTotal** à **Wazuh**, nous pouvons automatiser l'analyse des fichiers suspects ou des indicateurs de compromission en les envoyant à **VirusTotal** pour une évaluation supplémentaire. Cela nous permet d'obtenir une analyse plus complète et d'agir plus rapidement en cas de menace potentielle.

Pour intégrer VirusTotal :

1. On se rend sur le site web officiel de **VirusTotal**.
2. On crée un compte, ou on s'identifie, en haut à gauche.
3. On clique l'icône de son profil puis sur « **API Key** ».
4. On copie l'**API**.
5. On va sur l'interface web de notre **Wazuh**, puis on clique sur ≡ | ⌂ | wazuh. ⌄, après sur « **Settings** » et « **Modules** ».
6. On descend jusqu'à la partie « **Threat Detection and Response** » et on active « **VirusTotal** ».
7. Enfin, on va sur notre serveur en ligne de commande et on édite le fichier **/var/ossec/etc/ossec.conf.**
8. On ajoute la configuration suivant dans la partie **<ossec_config>** en y ajoutant l'API d**e VirusTotal** :

```
<!-- ajout virustotal -->
  <integration>
    <name>virustotal</name>
    <api_key>API_VirusTotal</api_key>
    <group>syscheck</group>
    <alert_format>json</alert_format>
  </integration>
```

9. On redémarre ensuite **Wazuh** : **systemctl restart wazuh-manager**

II - Configurer la surveillance de l'intégrité des fichiers

La **FIM**, ou **Files Integrity Monitoring** (surveillance de l'intégrité des fichiers), est une fonctionnalité essentielle de **Wazuh**. Elle permet de surveiller en temps réel les changements apportés aux fichiers critiques du système, tels que les fichiers système, de configuration ou de programme, afin de détecter toute altération ou accès non autorisé.

Voici comment cela fonctionne dans Wazuh :

1. **Surveillance des fichiers** : **Wazuh** surveille en permanence les fichiers spécifiés dans les règles de surveillance définies par l'utilisateur. Ces fichiers peuvent inclure des fichiers système, des fichiers de configuration, des fichiers de données sensibles, etc.
2. **Calcul des hachages** : Pour chaque fichier surveillé, **Wazuh** calcule un hachage (hash) à partir de son contenu au moment de la configuration initiale. Ce hachage constitue une empreinte numérique unique qui représente l'état « sain » du fichier.
3. **Détection des changements** : Ensuite, à intervalles réguliers, **Wazuh** compare les hachages actuels des fichiers surveillés avec les hachages initiaux. Tout changement dans le contenu d'un fichier entraîne une différence de hachage, ce qui déclenche une alerte.
4. **Alertes et réponse aux incidents** : Lorsque **Wazuh** détecte une altération ou une modification non autorisée d'un fichier, il génère une alerte en temps réel pour informer les administrateurs de la violation de l'intégrité des fichiers. Ces alertes sont envoyées dans **Slack** dans notre cas.

Pour configurer la surveillance de l'intégrité des fichiers :

1. On édite le fichier **/var/ossec/etc/ossec.conf**
2. On vérifie si on trouve ces paramètres ci-dessous dans la partie **<syscheck> :**

/!\ Nous devons contrôler ces paramètres dans ce même fichier sur tous les hôtes où se trouvent l'agent **Wazuh**.

```
<!-- File integrity monitoring -->
  <syscheck>
    <disabled>no</disabled>

    <!-- Frequency that syscheck is executed default every 12 hours (en secondes)-->
    <frequency>30</frequency>

    <scan_on_start>yes</scan_on_start>

    <!-- Generate alert when new file detected -->
    <alert_new_files>yes</alert_new_files>

    <!-- Don't ignore files that change more than 'frequency' times -->
    <auto_ignore frequency="10" timeframe="3600">no</auto_ignore>

    <!-- Directories to check  (perform all possible verifications) -->
    <directories check_all="yes" realtime="yes" report_changes="yes">/etc</directories>
    <directories check_all="yes" realtime="yes" report_changes="yes">/usr/bin</directories>
    <directories check_all="yes" realtime="yes" report_changes="yes">/usr/sbin</directories>
    <directories check_all="yes" realtime="yes" report_changes="yes">/bin</directories>
    <directories check_all="yes" realtime="yes" report_changes="yes">/sbin</directories>
    <directories check_all="yes" realtime="yes" report_changes="yes">/boot</directories>

    …
  <syscheck>
```

Les répertoires ci-contre sont analysés en temps réel et un chaque changement est notifié. Les sous-répertoires et fichiers sont analysés (check_all)

Par défaut, on trouve la configuration comme ci-dessous :

```
    <directories>/etc,/usr/bin,/usr/sbin</directories>
    <directories>/bin,/sbin,/boot</directories>
```

On peut personnaliser les répertoires / sous-répertoires à analyser ou non, puis redémarrer **Wazuh**.

III – Tests

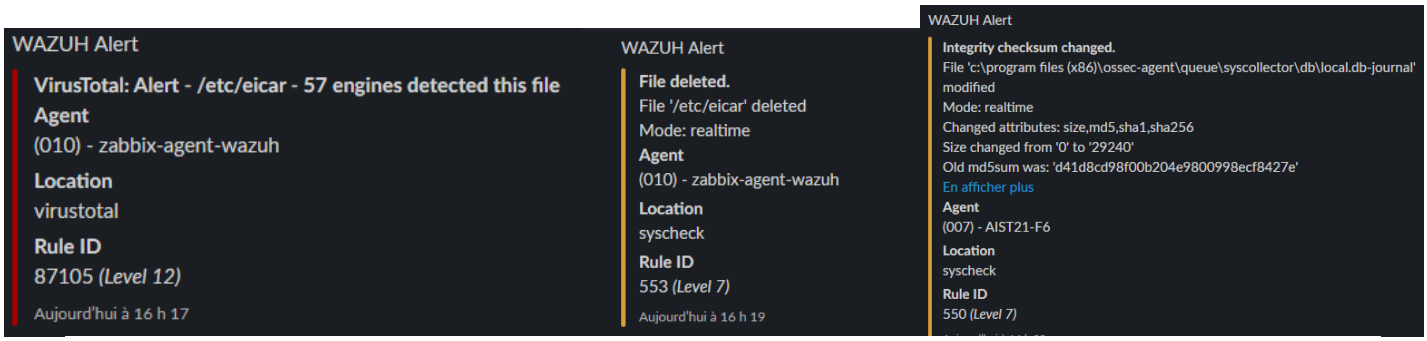
Nous pouvons réaliser un test simple sur un des hôtes où se trouve l'agent **Wazuh** avec le fichier de test **Eicar** qui est une chaîne de caractères, écrite dans un fichier informatique, destiné à tester le bon fonctionnement des logiciels antivirus.

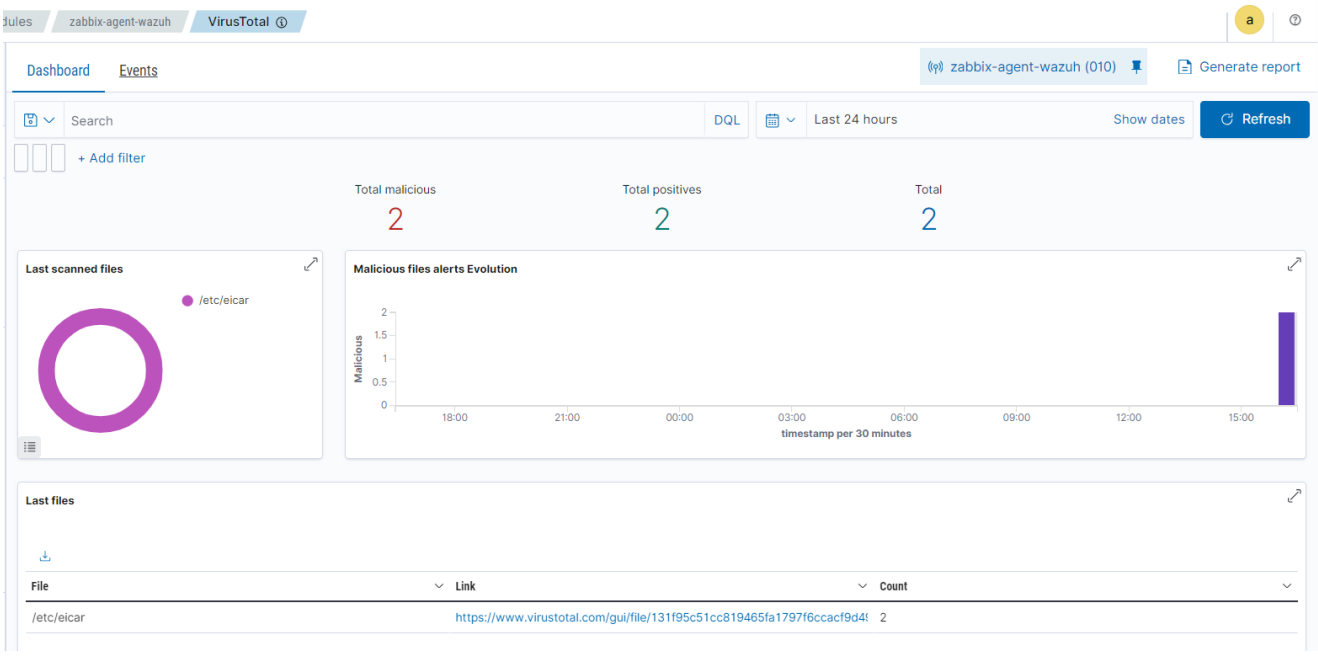
Pour cela :

1. On se connecte sur un de nos hôtes (en SSH de préférence)
2. On crée un fichier dans un des répertoires qui sont analysés par exemple : **nano /etc/eicar**
3. On y ajoute le contenu suivant :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

4. On enregistre et on contrôle nos alertes dans **Slack** par exemple ou autres applications de notifications ou est intégré **Wazuh**.





Ces trois captures d'écran montrent que notre test a fonctionné : nous pouvons voir respectivement la notification de **VirusTotal** sur **Slack** qui indique qu'il a détecté un fichier malveillant sur l'hôte qui héberge **Zabbix**, puis, que celui-ci a été supprimé (à la main), et que sur un autre PC (**AIST21-F6**) la différence du hachage sur un fichier.

Enfin sur l'interface web de **Wazuh**, nous pouvons voir sur l'hôte sur lequel se trouve **Zabbix** que ce test a été réalisé deux fois et que ce fichier se trouve dans /etc et se nomme eicar.