

Détection et suppression des logiciels malveillants avec VirusTotal

L'intégration de **VirusTotal** avec **Wazuh** permet de détecter et de supprimer les logiciels malveillants en utilisant le module intégrateur pour se connecter à des API externes. Ce guide détaille les étapes pour configurer cette intégration et effectuer la détection sur des points de terminaison **Linux** et **Windows**.

I – Configuration du point de terminaison Linux

1. On ouvre le fichier de configuration de l'agent **Wazuh** à l'emplacement **/var/ossec/etc/ossec.conf** et on s'assure que la valeur **<disabled>** du bloc **<syscheck>** est définie sur **no** pour permettre la surveillance des modifications du répertoire.

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

2. On ajoute une entrée pour surveiller le répertoire **/root** en temps quasi réel :

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

3. On met à jour les packages système et on installe l'utilitaire **jq** :

```
sudo apt update
sudo apt -y install jq
```

4. On crée le script **/var/ossec/active-response/bin/remove-threat.sh** en y ajoutant le contenu suivant :

```
#!/bin/bash

LOCAL=`dirname $0`;
cd $LOCAL
cd ../

PWD=`pwd`

read INPUT_JSON
FILENAME=$(echo $INPUT_JSON | jq -r .parameters.alert.data.virustotal.source.file)
COMMAND=$(echo $INPUT_JSON | jq -r .command)
LOG_FILE="${PWD}/../logs/active-responses.log"

#----- Analyze command -----#
if [ ${COMMAND} = "add" ]
then
  # Send control message to execd
  printf '{"version":1,"origin":{"name":"remove-threat","module":"active-response"},"command":"check_keys", "parameters":{"keys":[]}}\n'

  read RESPONSE
  COMMAND2=$(echo $RESPONSE | jq -r .command)
  if [ ${COMMAND2} != "continue" ]
  then
    echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Remove threat active response aborted" >> ${LOG_FILE}
    exit 0;
  fi
fi

# Removing file
rm -f $FILENAME
if [ $? -eq 0 ]; then
  echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Successfully removed threat" >> ${LOG_FILE}
else
  echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Error removing threat" >> ${LOG_FILE}
fi

exit 0;
```

Détection et suppression des logiciels malveillants avec VirusTotal

5. On modifie les autorisations du Script :

```
sudo chmod 750 /var/ossec/active-response/bin/remove-threat.sh  
sudo chown root:wazuh /var/ossec/active-response/bin/remove-threat.sh
```

6. On redémarre l'agent **Wazuh** :

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

II – Configuration du serveur Wazuh

1. On ajoute les règles dans le fichier **/var/ossec/etc/rules/local_rules.xml** sur le serveur **Wazuh** pour détecter les modifications dans le répertoire **/root**.

```
<group name="syscheck,pci_dss_11.5,nist_800_53_S1.7,">  
  <!-- Rules for Linux systems -->  
  <rule id="100200" level="7">  
    <if_sid>550</if_sid>  
    <field name="file">/root</field>  
    <description>File modified in /root directory.</description>  
  </rule>  
  <rule id="100201" level="7">  
    <if_sid>554</if_sid>  
    <field name="file">/root</field>  
    <description>File added to /root directory.</description>  
  </rule>  
</group>
```

2. On ajoute/modifie la configuration nécessaire dans le fichier **/var/ossec/etc/ossec.conf**, en remplaçant **<YOUR_VIRUS_TOTAL_API_KEY>** par la clé API **VirusTotal**.

```
<ossec_config>  
  <integration>  
    <name>virustotal</name>  
    <api_key><YOUR_VIRUS_TOTAL_API_KEY></api_key>  
    <rule_id>100200,100201</rule_id>  
    <alert_format>json</alert_format>  
  </integration>  
</ossec_config>
```

3. On ajoute les blocs nécessaires dans le fichier **/var/ossec/etc/ossec.conf** pour activer la réponse active et déclencher le script de suppression des menaces.

```
<ossec_config>  
  <command>  
    <name>remove-threat</name>  
    <executable>remove-threat.sh</executable>  
    <timeout_allowed>no</timeout_allowed>  
  </command>  
  
  <active-response>  
    <disabled>no</disabled>  
    <command>remove-threat</command>  
    <location>local</location>  
    <rules_id>87105</rules_id>  
  </active-response>  
</ossec_config>
```

4. On intègre les règles dans le fichier **/var/ossec/etc/rules/local_rules.xml** pour alerter des résultats de réponse active.

Détection et suppression des logiciels malveillants avec VirusTotal

```
<group name="virustotal,">
  <rule id="100092" level="12">
    <if_sid>657</if_sid>
    <match>Successfully removed threat</match>
    <description>$(parameters.program) removed threat located at $(parameters.alert.data.virustotal.source.file)</description>
  </rule>

  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Error removing threat located at $(parameters.alert.data.virustotal.source.file)</description>
  </rule>
</group>
```

5. On redémarre le gestionnaire **Wazuh** :

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

III – Émulation de l'attaque

1. On télécharge un fichier de test **EICAR** dans le répertoire **/root** du point de terminaison Linux en utilisant la commande :

```
sudo curl -Lo /root/eicar.com https://secure.eicar.org/eicar.com && sudo ls -lah /root/eicar.com
```

2. On visualise les alertes dans le tableau de bord de **Wazuh** en accédant module « **Security Events** » puis dans **Events** :

>	29 mars 2024 à 14:03:30.073	Fichier supprimé.	7	553
>	29 mars 2024 à 14:03:29.637	VirusTotal : Alerte - /root/eicar.com - 64 moteurs ont détecté ce fichier	12	87105

Fichier détecté comme malveillant puis supprimé