Collecte de journaux Windows Defender

Windows Defender est l'outil anti-malware intégré dans les systèmes d'exploitation Windows de **Microsoft**.

En collectant les journaux de **Windows Defender**, il est possible d'obtenir une visibilité sur les menaces détectées par ce logiciel sur les points de terminaison **Windows**.

1. **Configuration :**

   - Il suffit de modifier le fichier **ossec.conf** situé à l'emplacement : **C:\Program Files (x86)\ossec-agent\ossec.conf**.
   - On ajoute le bloc suivant au fichier de configuration pour activer la collecte des journaux **Windows Defender** :

```
<localfile>
  <location>Microsoft-Windows-Windows Defender/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

2. **Décodeurs et règles :**

   - **Wazuh** offre des décodeurs préconfigurés pour les journaux **Windows**, y compris ceux de **Windows Defender**. Il n'y a donc pas besoin de créer de décodeurs supplémentaires.

   - Des règles spécifiques pour **Windows Defender** sont également fournies par **Wazuh**. On peut les trouver dans le fichier **0600-win-wdefender_rules.xml** dans le répertoire des règles sur le serveur **Wazuh**, généralement situé à **/var/ossec/ruleset/rules/**.

En suivant ces étapes, on peut configurer l'agent **Wazuh** pour collecter les journaux **Windows Defender**, fournissant ainsi une visibilité précieuse sur les activités de sécurité de vos points de terminaison **Windows**.

On pense à bien redémarrer l'agent :

- soit avec le **Gestionnaire des Tâches** ou
- avec la commande à exécuter dans **PowerShell** :

```
Restart-Service -Name WazuhSvc
```