

Améliorer la détection avec le framework MITRE ATT&CK

Pour améliorer la détection des menaces, on peut intégrer le framework **MITRE ATT&CK** avec l'aide du module **MITRE | ATT&CK**® fourni par **Wazuh**.

Ce framework, créé par la **MITRE** Corporation, fournit un ensemble mondial d'actions et de comportements observés d'acteurs menaçants dans le monde réel.

Avec **14 tactiques et plusieurs techniques**, les analystes de sécurité peuvent mieux identifier les **attaques en cours**. On utilise des identifiants pour référencer la tactique ou la technique employée par un adversaire.

L'intégration de **Wazuh** avec le framework **MITRE ATT&CK** est rendue possible via un module prêt à l'emploi sur le tableau de bord **Wazuh**. Cela permet de mapper les alertes générées par **Wazuh** à des tactiques et techniques spécifiques, aidant ainsi les équipes de sécurité à mieux comprendre les menaces et à développer des stratégies d'atténuation efficaces.

Le module **Wazuh MITRE ATT&CK** se trouve dans la section **THREAT DETECTION AND RESPONSE** de la page principale du tableau de bord **Wazuh**. Il offre plusieurs fonctionnalités pour améliorer la détection des menaces.

I – Configuration du serveur Wazuh

- On ajoute les règles suivantes au fichier `/var/ossec/etc/rules/local_rules.xml` :

```
<group name="windows,sysmon,privilege-escalation">
  <rule id="110011" level="10">
    <if_sid>61615</if_sid>
    <field name="win.eventdata.targetObject" type="pcre2">HKLM\\\\System\\\\CurrentControlSet\\\\Services\\\\
PSEXESVC</field>
    <field name="win.eventdata.eventType" type="pcre2">^SetValue$</field>
    <field name="win.eventdata.user" type="pcre2">NT AUTHORITY\\\\SYSTEM</field>
    <options>no_full_log</options>
    <description>PsExec service running as $(win.eventdata.user) has been created on $
(win.system.computer)</description>
    <mitre>
      <id>T1543.003</id>
    </mitre>
  </rule>
</group>
```

La règle **110011** crée une alerte chaque fois qu'un service nommé **PSEXESVC** est créé, c'est ce qui se produit chaque fois que **PsExec** est exécuté sur le point de terminaison **Windows**.

Il est mappé à l'ID **MITRE ATT&CK T1543.003**, indiquant les tactiques de persistance et d'élévation de privilèges. Lorsque la règle se déclenche, l'alerte contient des informations sur l'ID **T1543.003 MITRE ATT&CK**.

- On redémarre l'agent **Wazuh** pour appliquer les modifications :

```
systemctl restart wazuh-agent
```

II – Configuration du point de terminaison Windows

- On télécharge [Sysmon](#) (on extrait du zip) et le fichier de configuration [sysmonconfig.xml](#) (le fichier .xml se trouve dans la 1^{ère} étape sur le site web de la documentation **Wazuh**, il faut le télécharger et le mettre au même niveau que le fichier .exe de Sysmon).
- On lance **PowerShell** avec des privilèges administratifs et on installe **Sysmon** comme suit :

```
.\Sysmon64.exe -accepteula -i .\sysmonconfig.xml
```

Note :

Par défaut la fenêtre **PowerShell** s'ouvre en affichant **PS C:\WINDOWS\system32>**, il faut alors naviguer jusqu'au répertoire de **Sysmon** (avec **cd**) puis exécuter la commande ci-dessus.

Améliorer la détection avec le framework MITRE ATT&CK

- On modifie le fichier **C:\Program Files (x86)\ossec-agent\ossec.conf** de l'agent **Wazuh** et on inclut les paramètres suivants dans le bloc : **<ossec_config>**

```
<!-- Configure Wazuh agent to receive events from Sysmon -->
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

- On redémarre l'agent **Wazuh** pour que les modifications prennent effet :

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

Test :

- On télécharge l'archive **PsTools** depuis la page **Microsoft Sysinternals** et on extrait le binaire **Psexec** de l'archive. La commande suivante fait passer un processus **Windows PowerShell** d'un utilisateur administrateur à un utilisateur **SYSTÈME** :

```
./psexec -i -s powershell /accepteula
```

- On exécute la commande ci-dessous pour confirmer que la nouvelle instance de **PowerShell** s'exécute en tant que **SYSTEM** :

```
whoami
```

Résultat attendu :

```
PS C:\Windows\system32> whoami
nt authority\system
```

Visualisation des alertes :

On se rend sur l'interface web de notre **Wazuh**, on sélectionne le « **Module de sécurité > MITRE ATT&CK > Events** » du tableau de bord **Wazuh** pour rechercher des ID, tactiques ou techniques MITRE spécifiques, comme le montre la figure ci-dessous :

>	27 mars 2024 à 11:10:51.374	AIST21-F6	T1021.002 , T156 9.002	Mouvement latéral, exécution	Nouveau service Windows Créé pour démarrer à partir du chemin racine de Windows. Événement suspect, car le binaire peut avoir été supprimé à l'aide des partages d'administrateur Windows.	12	92650
---	-----------------------------	-----------	---------------------------	------------------------------	--	----	-------

Améliorer la détection avec le framework MITRE ATT&CK

```

t  nom d'agent                AIST21-F6

t  data.win.eventdata.accountName  Système local

t  data.win.eventdata.imagePath    %SystemRoot%\PSEXESVC.exe

t  data.win.eventdata.serviceName  PSEXESVC

t  data.win.eventdata.serviceType  service en mode utilisateur

t  data.win.eventdata.startType    Démarrage à la demande

t  data.win.system.channel         Système

t  data.win.system.ordinateur      AIST21-F6.dijon.org

t  data.win.system.eventID         7045

t  data.win.system.eventRecordID   8266

t  data.win.system.eventSourceName Gestionnaire de contrôle des services

t  data.win.system.keywords        0x8080000000000000

t  data.win.system.level           4

t  data.win.system.message         "Un service a été installé sur le système. Nom du service : PSEXESVC Nom du fichier de service : %SystemRoot%\PSEXESVC.exe Type de service : service en mode utilisateur Type de démarrage du service : Démarrage à la demande Compte de service : Système local"

```