檢測未授權的進程

Wazuh 的命令監控功能可以在端點上運行命令並監視命令的輸出。

在這個使用案例中，您使用 Wazuh 的命令監控功能來檢測 Ubuntu 端點上是否正在運行 Netcat。Netcat 是一個用於端口掃描和監聽的電腦網絡工具。

基礎架構

端點

描述

Ubuntu 22.04

您將在此端點上配置 Wazuh 的命令監控模組，以檢測正在運行的 Netcat 進程。

配置

Ubuntu 端點

採取以下步驟來配置命令監控並查詢 Ubuntu 端點上所有運行中進程的列表。

將以下配置區塊添加到 Wazuh 代理程式的/var/ossec/etc/ossec.conf 文件。這將允許定期獲取運行中進程的列表：

```
<ossec_config>
<localfile>
<log_format>full_command</log_format>
<alias>process list</alias>
<command>ps -e -o pid,uname,command</command>
<frequency>30</frequency>
</localfile>
</ossec_config>
```

重新啟動 Wazuh 代理程式以應用更改：

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

安裝 Netcat 和所需的相依性：

```
sudo apt install ncat nmap -y
```

Wazuh 伺服器

您需要在 Wazuh 伺服器上配置以下步驟，以創建一個規則，每次 Netcat 程序啟動時觸發。

將以下規則添加到 Wazuh 伺服器上的/var/ossec/etc/rules/local_rules.xml 文件：

```
<group name="ossec,">
  <rule id="100050" level="0">
    <if_sid>530</if_sid>
    <match>^ossec: output: 'process list'</match>
    <description>運行中進程的列表。</description>
    <group>process_monitor,</group>
  </rule>
  <rule id="100051" level="7" ignore="900">
```

```
    <if_sid>100050</if_sid>
    <match>nc -l</match>
    <description>netcat 監聽傳入連接。</description>
    <group>process_monitor,</group>
  </rule>
</group>
```

重新啟動 Wazuh 管理器以應用更改：
sudo systemctl restart wazuh-manager

攻擊模擬
在受監控的 Ubuntu 端點上運行 nc -l 8000，持續30秒。

可視化警報資料
您可以在 Wazuh 儀表板中視覺化警報資料。要做到這一點，請前往安全事件模組，並在搜尋欄中添加過濾器來查詢警報。

rule.id:(100051)