封鎖已知惡意攻擊者

在這個使用案例中，我們展示如何阻止惡意 IP 地址從訪問 Web 伺服器上的網路資源。您將在 Ubuntu 和 Windows 端點上設置 Apache Web 伺服器，然後從 RHEL 端點嘗試存取它們。

這個案例使用一個包含某些惡意攻擊者 IP 地址的公共 IP 聲譽資料庫。IP 聲譽資料庫是一組被標記為惡意的 IP 地址。在這裡，RHEL 端點充當惡意攻擊者的角色，因此您將其 IP 地址添加到聲譽資料庫。然後，配置 Wazuh 來封鎖 RHEL 端點在 60 秒內從存取 Apache Web 伺服器上的網路資源。這是一種阻止攻擊者繼續進行惡意活動的方法。

在這個案例中，您將使用 Wazuh CDB 清單和主動回應功能。

基礎架構

端點

說明

RHEL 9.0

攻擊者端點，連接到受害者的 Web 伺服器，您將使用 Wazuh CDB 清單功能將其 IP 地址標記為惡意。

Ubuntu 22.04

受害者端點運行 Apache 2.4.54 Web 伺服器。在這裡，您將使用 Wazuh 主動回應模組自動封鎖來自攻擊者端點的連線。

Windows 11

受害者端點運行 Apache 2.4.54 Web 伺服器。在這裡，您將使用 Wazuh 主動回應模組自動封鎖來自攻擊者端點的連線。

配置

Ubuntu 端點

執行以下步驟來安裝 Apache Web 伺服器並使用 Wazuh 代理監控其日誌。

更新本地套件並安裝 Apache Web 伺服器：

```
sudo apt update
sudo apt install apache2
```

如果防火牆已啟用，請修改防火牆以允許對 Web 埠的外部訪問。如果防火牆已停用，請跳過此步驟：

```
sudo ufw status
sudo ufw app list
sudo ufw allow 'Apache'
```

檢查 Apache 服務的狀態，以確認 Web 伺服器正在運行：

```
sudo systemctl status apache2
```

使用 curl 命令或在瀏覽器中打開 http://<UBUNTU_IP> 來查看 Apache 的首頁並驗證安裝：
curl http://<UBUNTU_IP>

將以下內容添加到 /var/ossec/etc/ossec.conf 文件以配置 Wazuh 代理並監控 Apache 訪問日誌：

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/apache2/access.log</location>
</localfile>
```

重新啟動 Wazuh 代理以應用更改：

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

Windows 端點

安裝 Apache Web 伺服器
執行以下步驟來安裝和配置 Apache Web 伺服器。

安裝最新的 Visual C++ 可轉發套件。

下載 Apache Web 伺服器 ZIP 安裝檔。這是針對 Windows 作業系統的已編譯二進位檔。

解壓縮 Apache Web 伺服器 ZIP 檔案的內容，並將提取的 Apache24 資料夾複製到 C: 目錄。

在 PowerShell 終端中以系統管理員權限運行以下命令，瀏覽到 C:\Apache24\bin 資料夾：

```
C:\Apache24\bin>httpd.exe
```

第一次運行 Apache 二進位檔時，Windows Defender 防火牆彈出。

點擊 "允許存取"。這允許 Apache HTTP 伺服器根據您的網路設定在您的私人或公共網路上通信。它在防火牆中創建一個允許在埠 80 上進入流量的入站規則。

在瀏覽器中打開 http://<WINDOWS_IP> 以查看 Apache 的首頁並驗證安裝。同時，驗證從攻擊者端點是否可以存取此 URL。

配置 Wazuh 代理

執行以下步驟來配置 Wazuh 代理以監控 Apache Web 伺服器日誌。

將以下內容添加到 C:\Program Files (x86)\ossec-agent\ossec.conf 以配置 Wazuh 代理並監控 Apache 訪問日誌：

```
<localfile>
  <log_format>syslog</log_format>
  <location>C:\Apache24\logs\access.log</location>
</localfile>
```

在 PowerShell 終端中以系統管理員權限重新啟動 Wazuh 代理以應用更改：

```
Restart-Service -Name wazuh
```

Wazuh 伺服器

您需要在 Wazuh 伺服器上執行以下步驟來將 RHEL 端 Wazuh CDB 清單並設定規則和主動回應。

下載實用工具並配置 CDB 清單
使用命令列介面安裝 wget 實用工具以下載必要的藝術品：
sudo yum update && sudo yum install -y wget

下載 Alienvault IP 聲譽資料庫：
sudo wget https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/alienvault_reputation.ipset -O /var/ossec/etc/lists/alienvault_reputation.ipset

將攻擊者端點的 IP 地址附加到 IP 聲譽資料庫中。在以下命令中，用 RHEL IP 地址替換 <ATTACKER_IP>：

sudo echo "<ATTACKER_IP>" >> /var/ossec/etc/lists/alienvault_reputation.ipset
下載腳本以將 .ipset 格式轉換為 .cdb 清單格式：

sudo wget https://wazuh.com/resources/iplist-to-cdblist.py -O /tmp/iplist-to-cdblist.py
使用先前下載的腳本將 alienvault_reputation.ipset 檔案轉換為 .cdb 格式：

sudo /var/ossec/framework/python/bin/python3 /tmp/iplist-to-cdblist.py /var/ossec/etc/lists/alienvault_reputation.ipset /var/ossec/etc/lists/blacklist-alienvault
選擇性：移除不再需要的 alienvault_reputation.ipset 檔案和 iplist-to-cdblist.py 腳本：

sudo rm -rf /var/ossec/etc/lists/alienvault_reputation.ipset
sudo rm -rf /tmp/iplist-to-cdblist.py
將生成的檔案授予適當的權限和擁有者：

sudo chown wazuh:wazuh /var/ossec/etc/lists/blacklist-alienvault
配置主動回應模組以封鎖惡意 IP 地址
在 Wazuh 伺服器 /var/ossec/etc/rules/local_rules.xml 自訂規則集檔案中添加一個自訂規則，以觸發 Wazuh 主動回應腳本。這樣可以封鎖攻擊者的 IP 地址。

對於 Ubuntu 端點：

firewall-drop 命令與 Ubuntu 本地 iptables 防火牆整合，並在 60 秒內阻止來自攻擊者端點的入站網路連線：

```
<ossec_config>
<active-response>
<command>firewall-drop</command>
<location>local</location>
<rules_id>100100</rules_id>
<timeout>60</timeout>
</active-response>
</ossec_config>
```

對於 Windows 端點：

主動回應腳本使用 netsh 命令在 Windows 端點上封鎖攻擊者的 IP 地址。它運行 60 秒：

<ossec_config>
<active-response>
<command>netsh</command>
<location>local</location>
<rules_id>100100</rules_id>
<timeout>60</timeout>
</active-response>
</ossec_config>

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

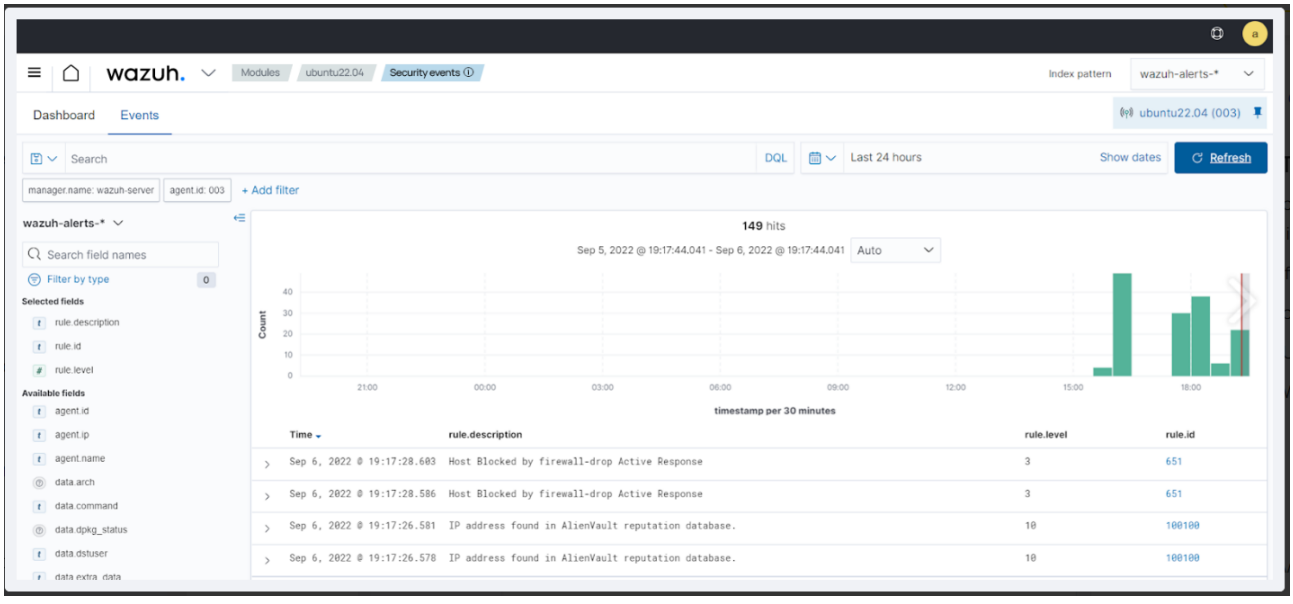
攻擊模擬

使用適當的值替換 <WEBSERVER_IP>，從 RHEL 端點存取任何 Web 伺服器。從攻擊者端點執行以下命令：

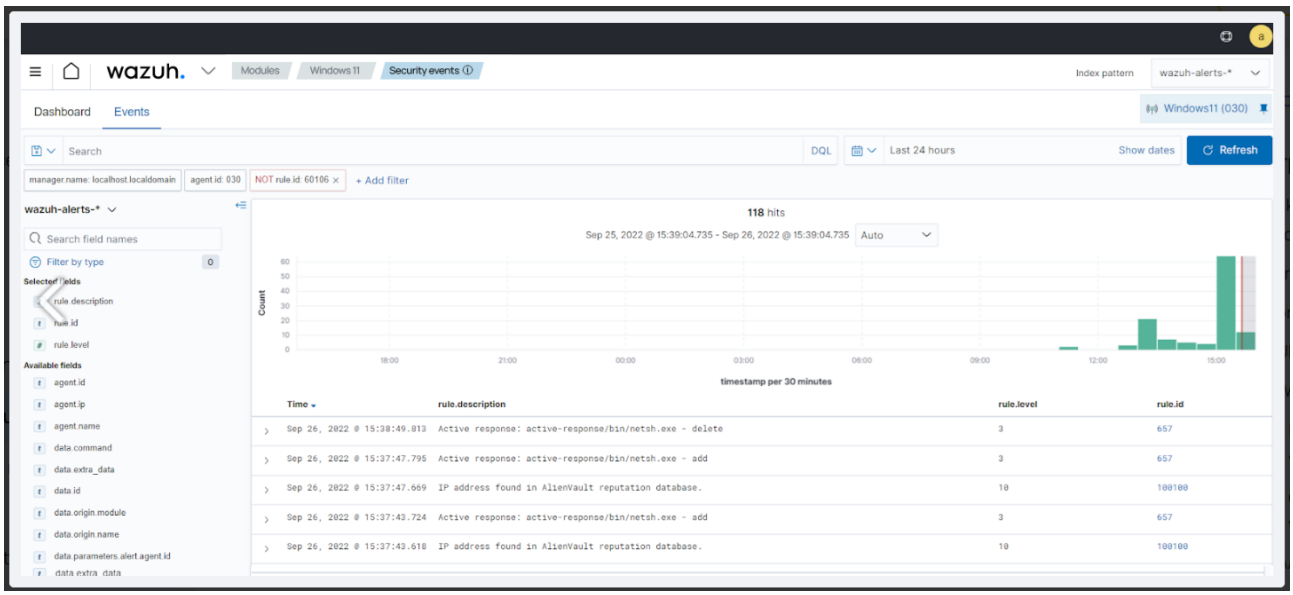
curl http://<WEBSERVER_IP>
攻擊者端點首次連接到受害者的 Web 伺服器。第一次連接後，Wazuh 主動回應模組會暫時封鎖連線 60 秒，阻止連續對 Web 伺服器的連接。

可視化警報
您可以在 Wazuh 儀表板中可視化警報資料。要這樣做，請進入 Security events 模組並在搜尋欄中添加篩選條件來查詢警報。

Ubuntu - rule.id:(651 OR 100100)



Windows - rule.id:(657 OR 100100)


wazuh.
Modules
Windows 11
Security events
Index pattern
wazuh-alerts-*
Dashboard
Events
Windows11 (030)
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: localhost.localdomain
agent.id: 030
NOT rule.id: 60106
+ Add filter
wazuh-alerts-*
Search field names
Filter by type
Selected fields
rule.description
rule.id
rule.level
Available fields
agent.id
agent.ip
agent.name
data.command
data.extra_data
data.id
data.origin.module
data.origin.name
data.parameters.alert.agent.id
data.extra_data
118 hits
Sep 25, 2022 @ 15:39:04.735 - Sep 26, 2022 @ 15:39:04.735
Auto
Count
timestamp per 30 minutes
Time
rule.description
rule.level
rule.id
Sep 26, 2022 @ 15:38:49.813
Active response: active-response/bin/netsh.exe - delete
3
657
Sep 26, 2022 @ 15:37:47.795
Active response: active-response/bin/netsh.exe - add
3
657
Sep 26, 2022 @ 15:37:47.669
IP address found in AlienVault reputation database.
10
100100
Sep 26, 2022 @ 15:37:43.724
Active response: active-response/bin/netsh.exe - add
3
657
Sep 26, 2022 @ 15:37:43.618
IP address found in AlienVault reputation database.
10
100100