注意：
這是在 EndPoint 端安裝 Suricata，並由 Wazuh Agent 讀取並拋給 Wazuh Server

網路入侵檢測系統 (Network IDS) 整合

Wazuh 與基於網路的入侵檢測系統 (NIDS) 整合，通過監控網路流量來增強威脅檢測。

在這個使用案例中，我們演示如何將 Suricata 整合到 Wazuh 中。Suricata 能夠通過其網路流量檢查功能提供對您的網路安全的額外洞察。

基礎架構

端點

描述

Ubuntu 22.04

這是您安裝 Suricata 的端點。在這個使用案例中，Wazuh 監控和分析在此端點上產生的網路流量。

配置

請按照以下步驟在 Ubuntu 端點上配置 Suricata 並將產生的日誌發送到 Wazuh 伺服器。

在 Ubuntu 端點上安裝 Suricata。我們在6.0.8版本上測試了此過程，可能需要一些時間：

```
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
sudo apt-get install suricata -y
```

下載並提取 Emerging Threats Suricata 規則集：

```
cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/.rules
```

在/etc/suricata/suricata.yaml 文件中修改 Suricata 設定，並設置以下變數：

```
HOME_NET: "<UBUNTU_IP>"
EXTERNAL_NET: "any"

default-rule-path: /etc/suricata/rules
rule-files:
- "*.rules"

# Global stats configuration
stats:
enabled: no

# Linux high speed capture support
af-packet:
  - interface: enp0s3
```

其中 interface 代表您要監控的網路介面。請用 Ubuntu 端點的介面名稱替換該值。例如，enp0s3。

Ifconfig

輸出

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::9ba2:9de3:57ad:64e5 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:14:65:bd txqueuelen 1000 (Ethernet)
RX packets 6704315 bytes 1268472541 (1.1 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4590192 bytes 569730548 (543.3 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

重新啟動 Suricata 服務：

```
sudo systemctl restart suricata
```

將以下配置添加到 Wazuh 代理程式的/var/ossec/etc/ossec.conf 文件中。這將允許 Wazuh 代理程式讀取 Suricata 日誌文件：

```
<ossec_config>
<localfile>
<log_format>json</log_format>
<location>/var/log/suricata/eve.json</location>
</localfile>
</ossec_config>
```

重新啟動 Wazuh 代理程式以應用更改：

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

攻擊模擬

Wazuh 會自動解析來自/var/log/suricata/eve.json 的資料並在 Wazuh 儀表板上生成相關的警報。

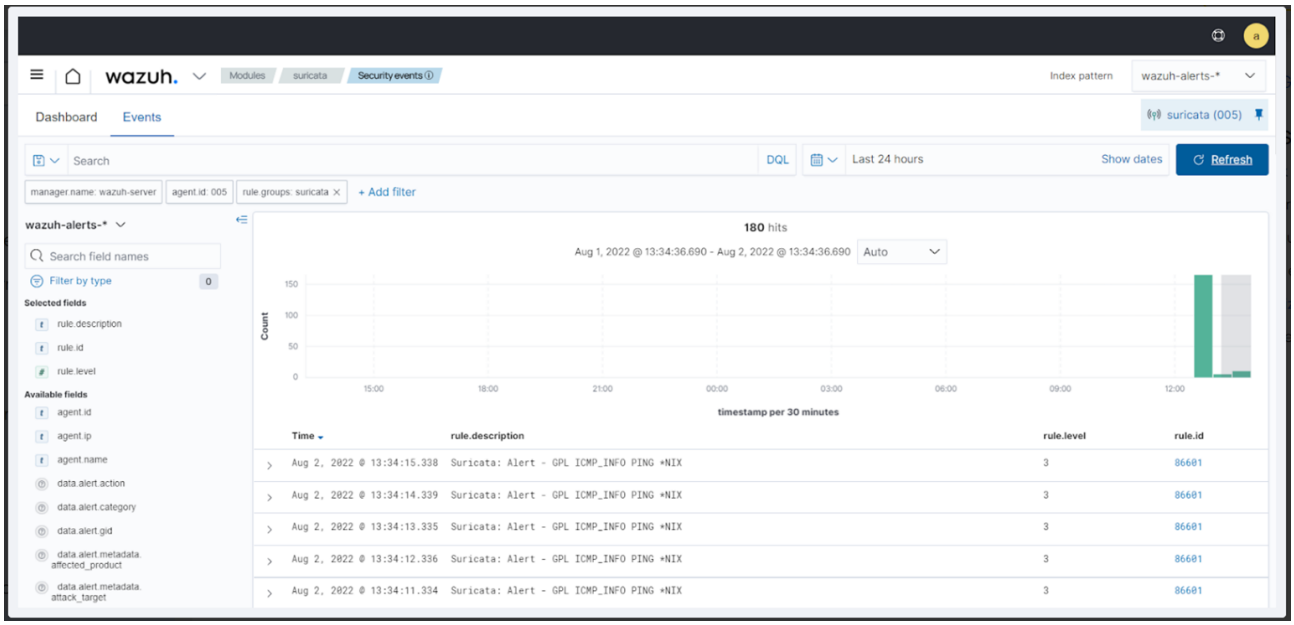
從 Wazuh 伺服器對 Ubuntu 端點 IP 地址進行 ping 測試：

```
ping -c 20 "<UBUNTU_IP>"
```

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.groups:suricata



故障排除
錯誤日誌：

16/9/2022 -- 12:32:16 - <Notice> - all 2 packet processing threads, 4 management threads initialized, engine started.
16/9/2022 -- 12:32:16 - <Error> - [ERRCODE: SC_ERR_AFP_CREATE(190)] - Unable to find iface eth0: No such device
16/9/2022 -- 12:32:16 - <Error> - [ERRCODE: SC_ERR_AFP_CREATE(190)] - Couldn't init AF_PACKET socket, fatal error
16/9/2022 -- 12:32:16 - <Error> - [ERRCODE: SC_ERR_FATAL(171)] - thread W#01-eth0 failed

位置：Suricata 日誌 - /var/log/suricata/suricata.log

解決方法：要解決此問題，請檢查您的網路介面名稱並在/etc/sysconfig/suricata 和 /etc/suricata/suricata.yaml 文件中相應地進行配置。