監控 Docker 事件

Docker 自動化部署不同應用程式於軟體容器內。Wazuh 的 Docker 模組可以在容器中識別安全事件並即時發出警報。在這個使用案例中，您將配置 Wazuh 來監控在 Ubuntu 端點上運行 Docker 容器的 Docker 事件。

請參閱文件的"監控容器活動"章節，以瞭解更多關於監控 Docker 和 docker-listener 模組的資訊。

基礎架構

端點

描述

Ubuntu 22.04

這是 Docker 主機，您在此建立和刪除容器。

配置

執行以下步驟來在 Ubuntu 端點上安裝 Docker 並配置 Wazuh 來監控 Docker 事件。

安裝 Python 和 pip：

```
sudo apt install python3 python3-pip
```

升級 pip：

```
pip3 install --upgrade pip
```

安裝 Docker 和 Python Docker Library：

```
curl -sSL https://get.docker.com/ | sh
sudo pip3 install docker==4.2.0
```

編輯 Wazuh 代理程式的配置文件/var/ossec/etc/ossec.conf，添加以下區塊來啟用 docker-listener 模組：

```
<ossec_config>
<wodle name="docker-listener">
<interval>10m</interval>
<attempts>5</attempts>
<run_on_start>yes</run_on_start>
<disabled>no</disabled>
</wodle>
</ossec_config>
```

重新啟動 Wazuh 代理程式以應用更改：

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

測試配置

執行幾個 Docker 活動，例如拉取 Docker 映像，啟動實例，執行其他 Docker 命令，然後刪除容器。

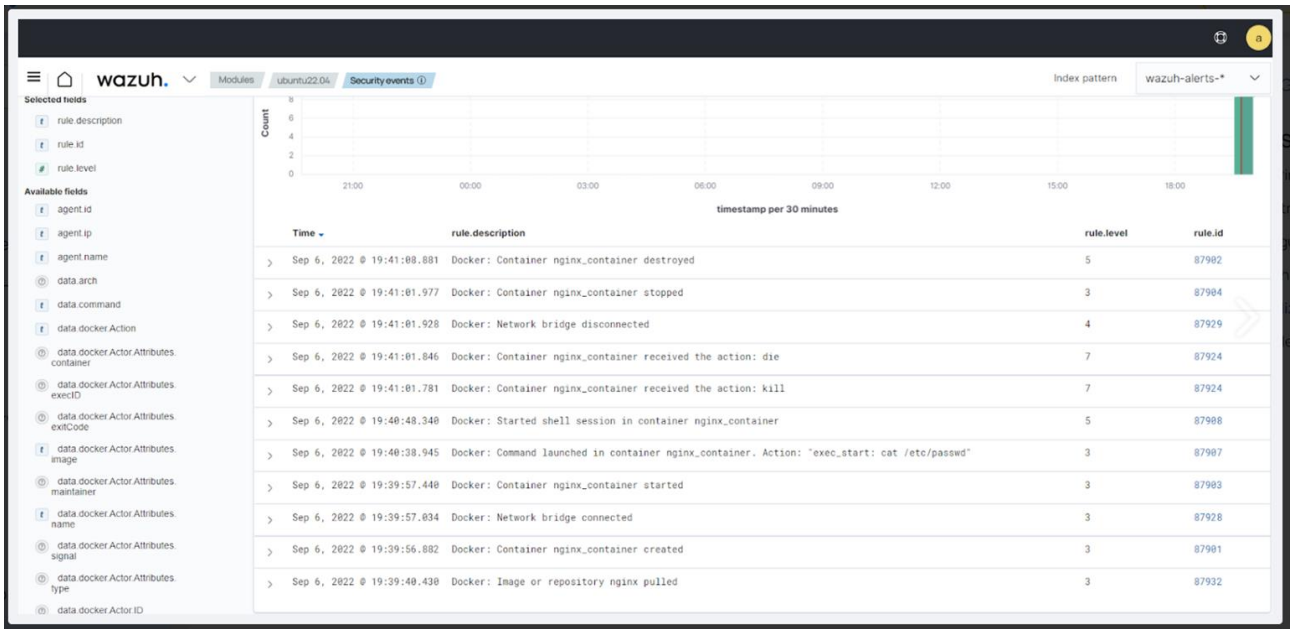
拉取映像，例如 NGINX 映像，並運行容器：

sudo docker pull nginx
sudo docker run -d -P --name nginx_container nginx
sudo docker exec -it nginx_container cat /etc/passwd
sudo docker exec -it nginx_container /bin/bash
exit
停止並刪除容器：

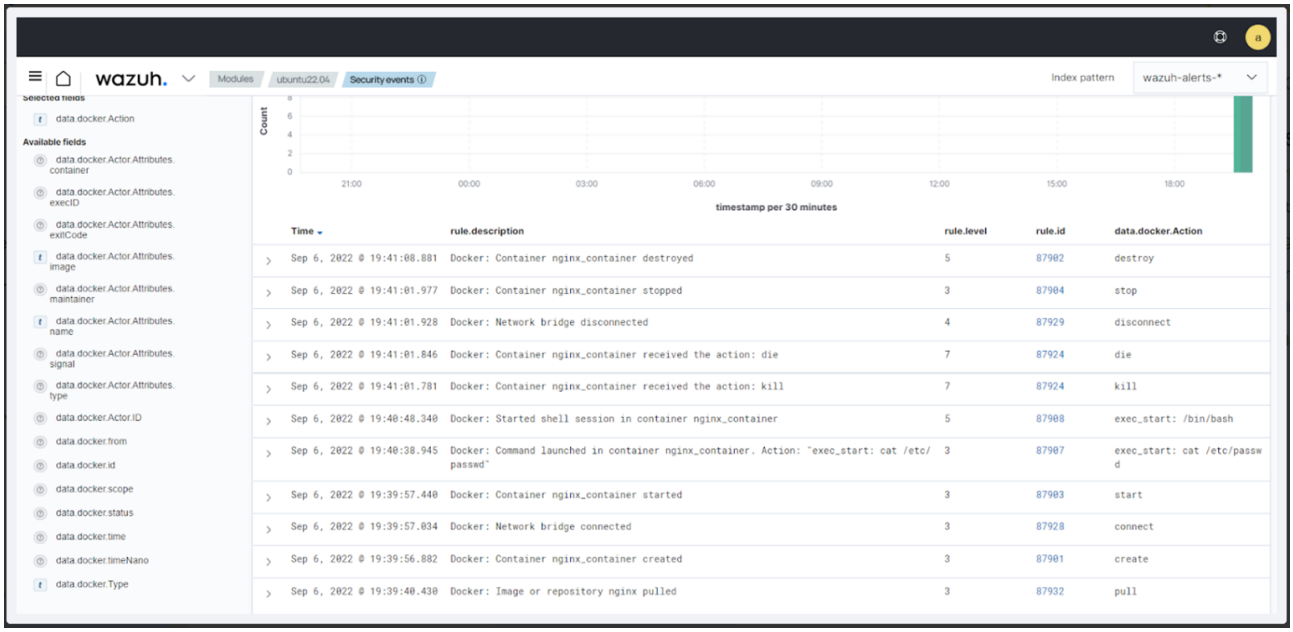
sudo docker stop nginx_container
sudo docker rm nginx_container

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: "docker"



此外，使用「按類型過濾」搜尋欄，應用 data.docker.Action 過濾器，以顯示執行的動作。



故障排除

錯誤日誌：

wazuh-modulesd:docker-listener: ERROR: /usr/bin/env: ‘python’: No such file or directory
位置：Wazuh 代理程式日誌 - /var/ossec/logs/ossec.log

解決方法：您可以創建一個符號連結來解決此問題：

sudo ln -s /usr/bin/python3 /usr/bin/python