檢測 SQL 注入攻擊

您可以使用 Wazuh 來從包含 select、union 和其他常見 SQL 注入模式的網頁伺服器日誌中檢測 SQL 注入攻擊。

SQL 注入是一種攻擊，其中威脅者將惡意代碼插入傳送到資料庫伺服器以進行解析和執行的字串中。成功的 SQL 注入攻擊將給予未經授權的訪問權限，以存取資料庫中包含的機密資訊。

在這個使用案例中，您將模擬對 Ubuntu 端點的 SQL 注入攻擊，並使用 Wazuh 來偵測它。

基礎架構

端點

描述
Ubuntu 22.04 運行 Apache 2.4.54網頁伺服器的受害者端點。
RHEL 9.0 發動 SQL 注入攻擊的攻擊者端點。

配置

Ubuntu 端點

執行以下步驟來安裝 Apache 並配置 Wazuh 代理程式以監視 Apache 日誌。

更新本地套件並安裝 Apache 網頁伺服器：

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

如果防火牆已啟用，請修改它以允許對 Web 端口的外部訪問。如果防火牆已禁用，則跳過此步驟。

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

檢查 Apache 服務的狀態，以驗證網頁伺服器是否運行：

```
sudo systemctl status apache2
```

使用 curl 命令或在瀏覽器中打開 http://<UBUNTU_IP>來查看 Apache 首頁，以驗證安裝是否成功：

```
curl http://<UBUNTU_IP>
```

將以下行添加到 Wazuh 代理程式的/var/ossec/etc/ossec.conf 文件中。這允許 Wazuh 代理程式監視您的 Apache 伺服器的存取日誌：

```
<ossec_config>
<localfile>
```

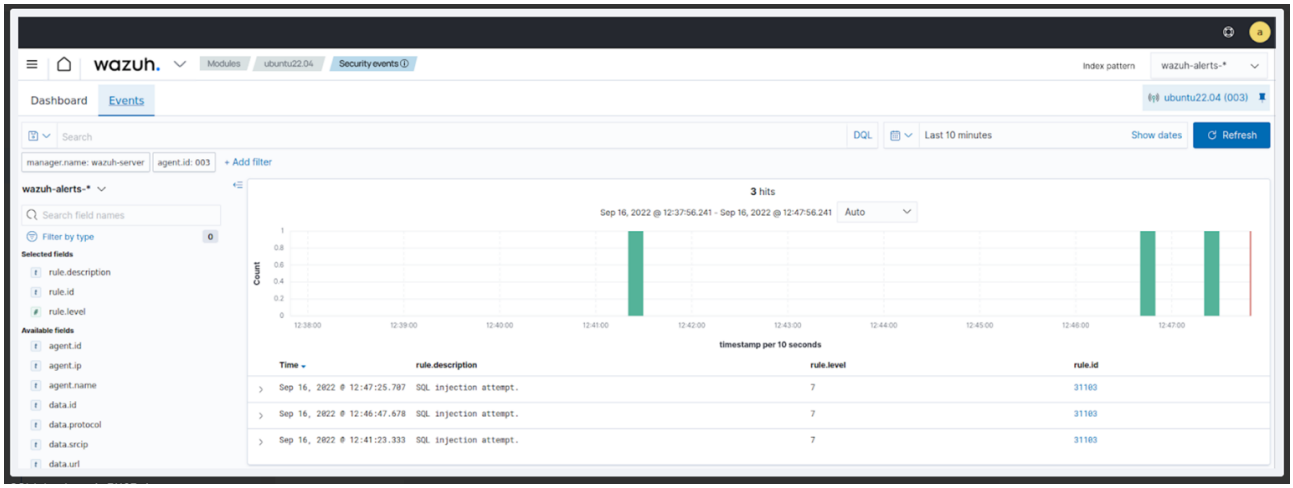
<log_format>apache</log_format>
<location>/var/log/apache2/access.log</location>
</localfile>
</ossec_config>
重新啟動 Wazuh 代理程式以應用配置更改：

sudo systemctl restart wazuh-agent
攻擊模擬
將<UBUNTU_IP>替換為適當的 IP 地址，並從攻擊者端點執行以下命令：

curl -XGET "http://<UBUNTU_IP>/users/?id=SELECT+*+FROM+users";
預期的結果是一個帶有規則 ID 31103的警報，但成功的 SQL 注入嘗試將生成一個帶有規則 ID 31106的警報。

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:31103



rule.id:31106