檢測隱藏進程
在這個使用案例中，我們展示了 Wazuh 如何檢測在 Linux 端點上由 Rootkit 創建的隱藏進程。在這個使用案例中，您將在 Ubuntu 端點上部署一個內核模式的 Rootkit。

這個 Rootkit 會從內核模塊列表中隱藏。它還會從 ps 工具中隱藏選定的進程。但是，Wazuh 使用 setsid()、getpid()和 kill()系統調用來檢測它。

我們的文檔中的惡意軟件檢測部分包含了有關 Wazuh 如何檢測惡意軟件和 rootcheck 模組的更多詳細信息。

基礎架構
端點

描述

Ubuntu 22.04

在這個端點上下載、編譯並加載 Rootkit。然後，在這個端點上配置 Wazuh rootcheck 模組進行異常檢測。

配置
在 Ubuntu 端點上執行以下步驟來模擬一個 Rootkit，並運行 rootcheck 掃描來檢測它。

切換到根用戶並更新此端點的內核：

sudo su
apt update
安裝構建 Rootkit 所需的套件：

apt -y install gcc git
接下來，在/var/ossec/etc/ossec.conf 文件中配置 Wazuh agent 以每2分鐘運行 rootcheck 掃描。在<rootcheck>部分中設置 frequency 選項為120：

```
<rootcheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>

  <!-- rootcheck execution frequency - every 12 hours by default-->

  <frequency>120</frequency>

  <rootkit_files>etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>etc/shared/rootkit_trojans.txt</rootkit_trojans>
  <skip_nfs>yes</skip_nfs>
```

</rootcheck>

重新啟動 Wazuh agent 以應用更改：

systemctl restart wazuh-agent

攻擊模擬

Ubuntu 端點

從 GitHub 上獲取 Diamorphine Rootkit 源代碼：

git clone https://github.com/m0nad/Diamorphine
切換到 Diamorphine 目錄並編譯源代碼：

cd Diamorphine
make

加載 Rootkit 內核模塊：

insmod diamorphine.ko

現在，內核級 Rootkit“Diamorphine”已安裝在 Ubuntu 端點上。

注意

根據環境，該模塊有時無法加載或正常運行。如果您在最後一步收到錯誤信息“insmod: ERROR: could not insert module diamorphine.ko: Invalid parameters”，請重新啟動 Linux 端點，然後重試。有時它需要幾次嘗試才能正常運行。

執行 kill 信號63與在 Ubuntu 端點上運行的一個隨機進程的 PID。這將使 Diamorphine Rootkit 變得可見。預設情況下，Diamorphine 會隱藏自己，所以我們不能通過運行 lsmod 命令來檢測它。試試看：

lsmod | grep diamorphine
kill -63 509
lsmod | grep diamorphine

在執行這些最後的命令時，您會期望看到空的輸出。在 Diamorphine 的情況下，向任何進程發送任何 kill 信號63，無論進程是否存在，都會切換 Diamorphine 內核模塊的隱藏或顯示。

執行以下命令，看看 rsyslogd 進程首先是可見的，然後不再可見。這個 Rootkit 允許您從 ps 命令中隱藏選定的進程。發送 kill 信號31可以隱藏/顯示任何進程。

ps auxw | grep rsyslogd | grep -v grep
Output
root 732 0.0 0.7 214452 3572 ? Ssl 14:53 0:00 /usr/sbin/rsyslogd -n

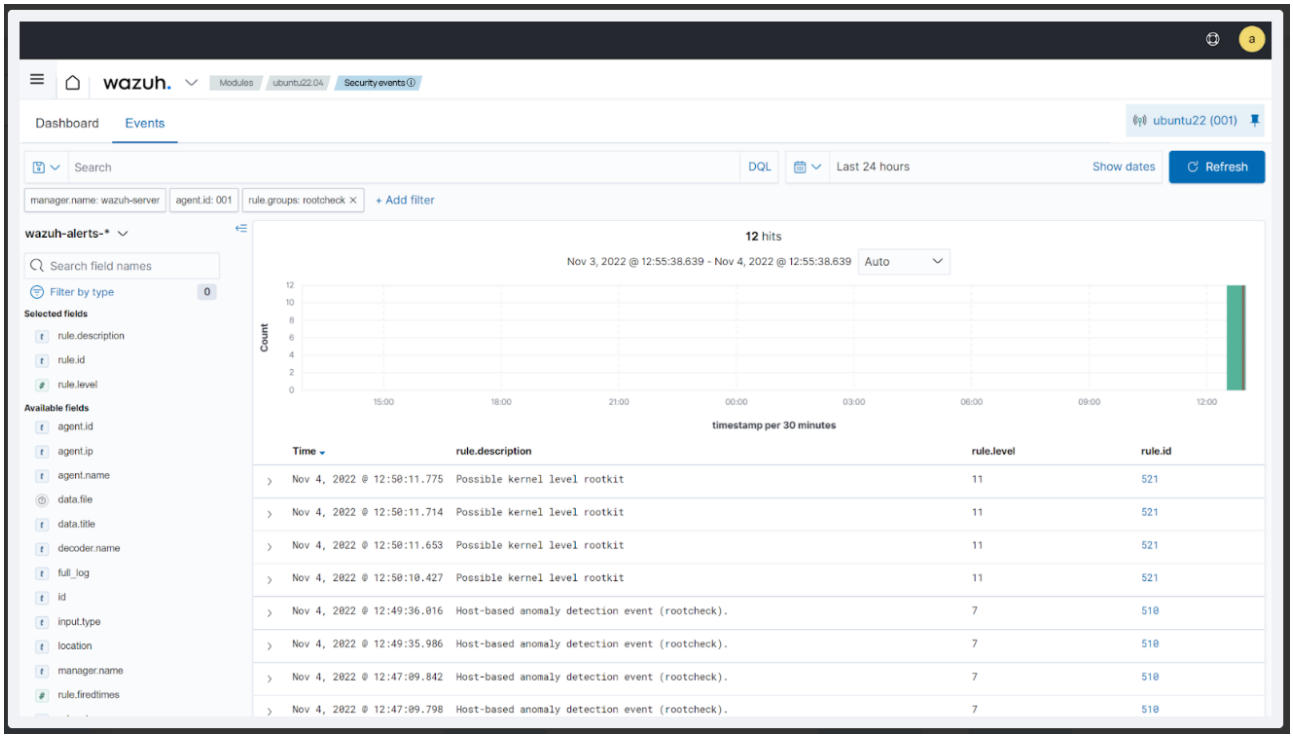
kill -31 <RSYSLOGD 的 PID>

ps auxw | grep rsyslog | grep -v grep
在執行這個最後的命令時，您會期望看到空的輸出。

下一個 rootcheck 掃描將運行並警告我們有關使用 Diamorphine Rootkit 隱藏的 rsyslogd 進程。

視覺化警報
您可以在 Wazuh 儀表板中視覺化警報數據。要這樣做，請轉到 Security events 模塊，並在搜索欄中添加過濾條件以查詢警報。

rule.groups:rootcheck



請記住，如果您再次對 rsyslogd 運行相同的 kill -31命令，rsyslogd 進程將再次變得可見。隨後的 rootcheck 掃描將不再生成有關它的警報。