監控惡意指令的執行

Auditd 是 Linux 系統的原生審計工具，用於記錄 Linux 端點上的操作和變更。

在這個使用案例中，您需要在 Ubuntu 端點上配置 Auditd，以記錄特定用戶執行的所有指令。這包括用戶在 sudo 模式下或切換到 root 用戶後運行的指令。您還需要配置自定義的 Wazuh 規則來警報可疑指令。

請考慮閱讀 Monitoring system calls 章節，以了解更多有關利用此功能的方法。

基礎設施

端點

描述

Ubuntu 22.04

在這個端點上，您需要配置 Auditd 以監控惡意指令的執行。然後，利用 Wazuh 的 CDB 列表查找功能來創建一個潛在的惡意指令列表。

配置

Ubuntu 端點

按照以下步驟安裝 Auditd 並創建必要的審計規則，以查詢特權用戶運行的所有指令。

如果端點上尚未安裝 Auditd，請安裝、啟動和啟用它：

```
sudo apt -y install auditd
sudo systemctl start auditd
sudo systemctl enable auditd
```

以 root 用戶身份，執行以下命令將審計規則附加到/etc/audit/audit.rules 文件中：

```
echo "-a exit,always -F auid=1000 -F egid!=994 -F auid!=-1 -F arch=b32 -S execve -k audit-wazuh-c" >> /etc/audit/audit.rules
echo "-a exit,always -F auid=1000 -F egid!=994 -F auid!=-1 -F arch=b64 -S execve -k audit-wazuh-c" >> /etc/audit/audit.rules
```

重新加載規則並確認它們是否生效：

```
sudo auditctl -R /etc/audit/audit.rules

sudo auditctl -l
```

輸出

```
-a always,exit -F arch=b32 -S execve -F auid=1000 -F egid!=994 -F auid!=-1 -F key=audit-wazuh-c
-a always,exit -F arch=b64 -S execve -F auid=1000 -F egid!=994 -F auid!=-1 -F key=audit-wazuh-c
```

在 Wazuh 代理器的/var/ossec/etc/ossec.conf 文件中添加以下配置。這允許 Wazuh 代理器讀取 auditd 日誌文件：

```
<localfile>
  <log_format>audit</log_format>
  <location>/var/log/audit/audit.log</location>
```

</localfile>
重啟 Wazuh 代理器：
sudo systemctl restart wazuh-agent

Wazuh 服務器

按照以下步驟來創建惡意程序的 CDB 列表，並創建規則來檢測列表中程序的執行。

查看 lookup 文件/var/ossec/etc/lists/audit-keys 中的鍵值對。

audit-wazuh-w:write
audit-wazuh-r:read
audit-wazuh-a:attribute
audit-wazuh-x:execute
audit-wazuh-c:command
該 CDB 列表包含以冒號分隔的鍵和值。

注意

Wazuh 允許您維護平面文件 CDB 列表，必須是僅鍵或鍵值對。它們會被編譯成特殊的二進制格式，以方便在 Wazuh 規則中進行高性能查找。此類列表必須創建為文件，添加到 Wazuh 配置中，然後進行編譯。之後，可以建立規則來查找這些 CDB 列表中解碼字段作為其匹配條件的一部分。例如，除了文本文件/var/ossec/etc/lists/audit-keys 外，還有一個二進制文件/var/ossec/etc/lists/audit-keys.cdb，Wazuh 在實際查找時使用該文件。

創建一個 CDB 列表/var/ossec/etc/lists/suspicious-programs 並填充其內容如下：

ncat:yellow
nc:red
tcpdump:orange

在 Wazuh 服務器的/var/ossec/etc/ossec.conf 文件的<ruleset>部分中添加列表：
<list>etc/lists/suspicious-programs</list>

創建一個高級別規則，在執行“red”程序時觸發警報。將此新規則添加到 Wazuh 服務器的 /var/ossec/etc/rules/local_rules.xml 文件中。

```
<group name="audit">
  <rule id="100210" level="12">
     <if_sid>80792</if_sid>
  <list field="audit.command" lookup="match_key_value" check_value="red">etc/lists/suspicious-programs</list>
    <description>Audit: Highly Suspicious Command executed: $(audit.exe)</description>
     <group>audit_command,</group>
  </rule>
</group>
```

重啟 Wazuh 管理器：
sudo systemctl restart wazuh-manager

攻擊模擬

在 Ubuntu 端點上，安裝並運行一個“red”程序 netcat：

sudo apt -y install netcat
nc -v

視覺化警報

您可以在 Wazuh 儀表板中視覺化警報數據。要做到這一點，請轉到 Security events 模組，並在搜索欄中添加過濾器來查詢警報。

data.audit.command:nc