檔案完整性監控

檔案完整性監控（FIM）有助於審計敏感檔案並滿足法規合規要求。Wazuh 具有內建的 FIM 模組，可監控檔案系統變更，以檢測檔案的建立、修改和刪除。

此使用案例使用 Wazuh FIM 模組來檢測 Ubuntu 和 Windows 端點上受監控目錄的變更。Wazuh FIM 模組通過使用 who-data 審計來獲取有關進行變更的使用者和進程的信息來豐富警報資料。

基礎架構

端點

描述

Ubuntu 22.04

Wazuh FIM 模組監控此端點上的目錄，以檢測檔案的建立、變更和刪除。

Windows 11

Wazuh FIM 模組監控此端點上的目錄，以檢測檔案的建立、變更和刪除。

配置

Ubuntu 端點

執行以下步驟來配置 Wazuh 代理程式以監視/root 目錄中的檔案系統變更。

編輯 Wazuh 代理程式的/var/ossec/etc/ossec.conf 配置文件。在<syscheck>區塊中添加要監視的目錄。在這個使用案例中，您要配置 Wazuh 來監視/root 目錄。為了獲取有關進行變更的使用者和進程的附加信息，啟用 who-data 審計：

<directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>
注意：您也可以在<directories>區塊中配置任何您選擇的路徑。
重新啟動 Wazuh 代理程式以應用配置更改：

sudo systemctl restart wazuh-agent

Windows 端點

採取以下步驟來配置 Wazuh 代理程式以監視 C:\Users\Administrator\Desktop 目錄中的檔案系統變更。

編輯受監控的 Windows 端點上的 C:\Program Files (x86)\ossec-agent\ossec.conf 配置文件。在<syscheck>區塊中添加要監視的目錄。在這個使用案例中，您要配置 Wazuh 來監視 C:\Users\Administrator\Desktop 目錄。為了獲取有關進行變更的使用者和進程的附加信息，啟用 who-data 審計：

<directories check_all="yes" report_changes="yes"
realtime="yes">C:\Users<USER_NAME>\Desktop</directories>
注意：您也可以在<directories>區塊中配置任何您選擇的路徑。
以管理員特權使用 PowerShell 重新啟動 Wazuh 代理程式以應用更改：

Restart-Service -Name wazuh
作為 Wazuh 代理程式的本地配置的替代方案，您可以集中配置一組代理程式。

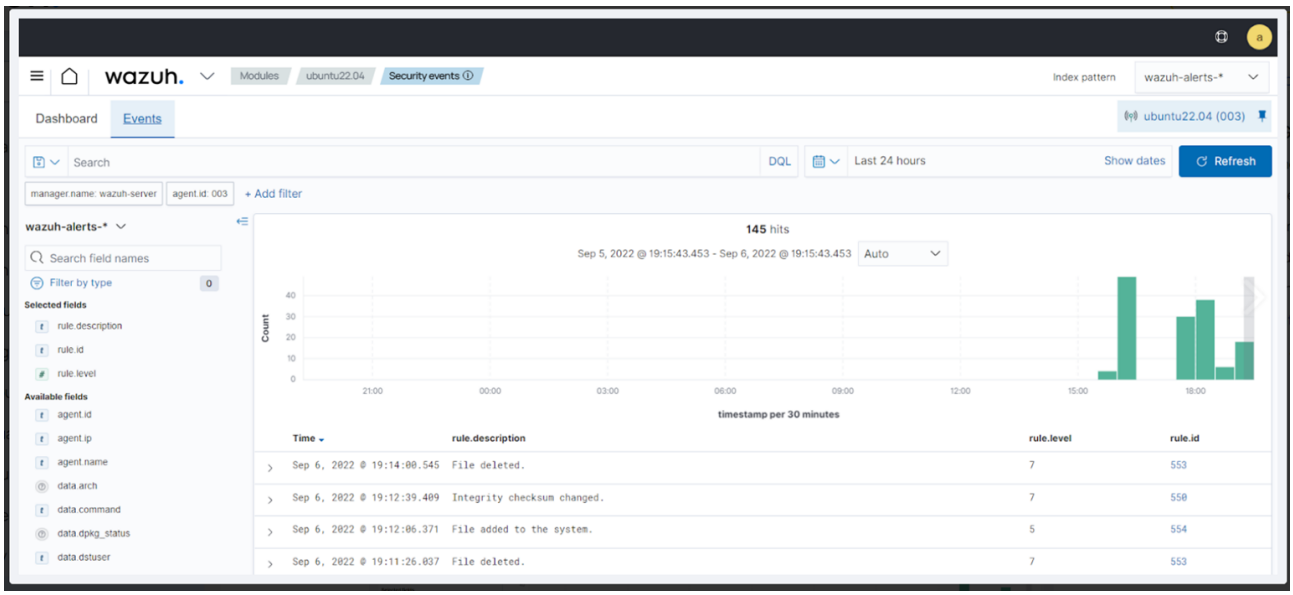
測試配置
在受監控的目錄中創建一個文本檔，然後等待5秒。

向文本檔添加內容並保存。等待5秒。

從受監視的目錄中刪除文本檔。

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：

Ubuntu - rule.id: is one of 550,553,554



Windows - rule.id: is one of 550,553,554