匯出安全端點的Windows事件ID清單

目錄

簡介

本文檔介紹思科安全終端的所有事件ID，有助於有效監控和事件響應。

必要條件

需求

思科建議您瞭解以下主題：

- Windows事件記錄
- 思科安全端點

採用元件

本檔案中的資訊是根據以下軟體版本：

- 思科安全終端8.4.0.30201
- Windows Server 2019

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

Cisco Secure Endpoint的Windows事件ID對於有效的監控和故障排除非常重要。訪問這些事件ID對於診斷問題、確保運營效率和增強總體安全性至關重要。

解決方案

打開檔案資源管理器，導航到C:\Program Files\Cisco\AMP\<version_number>\AMPEvents.man 檔案。您可以在記事本中打開此檔案，以檢視由Cisco Secure Endpoint生成的Windows事件的所有相

關資訊。

從AMPEvents.man檔案匯出的事件ID清單：

事件ID	事件	引擎/任務	層級
100	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V1/V2/V3/V4	ExploitPrevention	資訊
101	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V1/V2/V3/V4	ExploitPrevention	資訊
102	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V3/V4_AUDIT	ExploitPrevention	資訊
103	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V3/V4_AUDIT	ExploitPrevention	資訊
104	EXPREV_SCRIPT_CONTROL_ATTACK_V4	ExploitPrevention	資訊
105	EXPREV_SCRIPT_CONTROL_ATTACK_V4_AUDIT	ExploitPrevention	資訊
200	MALICIOUS_ACTIVITY_PROTECTION_V1/V2	惡意活動保護	資訊
300	SD_BLOCK_PROCESS_ACTION_V1	SystemProcessProtection	資訊
400	CCMS_JOB_STARTED_V1	CCMS	資訊
401	JANUS_EVENT_V1		資訊
500	ENDPOINT_ISOLATION_STARTED_V1	端點隔離	資訊
501	端點_隔離_停止_V1	端點隔離	資訊
502	ENDPOINT_ISOLATION_STARTFAILED_V1	端點隔離	錯誤
503	ENDPOINT_ISOLATION_STOPFAILED_V1	端點隔離	錯誤
504	ENDPOINT_ISOLATION_UPDATED_V1	端點隔離	資訊
505	ENDPOINT_ISOLATION_UPDATEFAILED_V1	端點隔離	錯誤
600	軌道_安裝_成功_V1	軌道	資訊
601	軌道_安裝_失敗_V1	軌道	錯誤
602	軌道_更新_成功_V1	軌道	資訊

603	軌道_更新_失敗_V1	軌道	錯誤
700	ENDPOINT_ISOLATION_BRUTE_FORCE_ATTEMPT	端點隔離	警告
800	SCRIPT_PROTECTION_DETECTION_V1	ScriptProtection	資訊
801	SCRIPT_PROTECTION_QUARANTINE_V1	ScriptProtection	資訊
900	ENGINE_DETECTION_HANDLED	行為保護	資訊
901	ENGINE_DETECTION_NOT_HANDLED	行為保護	錯誤
902	ENGINE_DETECTION_AUDIT	行為保護	資訊
903	ENGINE_DETECTION_NO_ACTION	行為保護	資訊
904	ENGINE_CLEAN_REQUIRED	行為保護	資訊
1248	SCAN_COMPLETED_CLEAN_V1	掃描	資訊
1249	掃描_已完成_更新_V1	掃描	資訊
1250	SCAN_FAILED_V1	掃描	錯誤
1300	檢測_V1	偵測	資訊
1310	QUARANTINE_SUCCESS_V1	隔離	資訊
1311	QUARANTINE_FAILED_V1	隔離	錯誤
1320	EXECUTION_BLOCK_V1	執行區塊	資訊
1321	EXECUTION_BLOCK_BAD_PARENT_V1	執行區塊	資訊
1700	WMI_RECON_V1	WMIRecon	資訊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。