导出安全终端的Windows事件ID列表

目录

简介

本文档介绍思科安全终端的所有事件ID，有助于有效监控和事件响应。

先决条件

要求

Cisco 建议您了解以下主题：

- Windows事件日志记录
- Cisco Secure Endpoint

使用的组件

本文档中的信息基于以下软件版本：

- 思科安全终端8.4.0.30201
- Windows Server 2019

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

Cisco安全终端的Windows事件ID对于有效监控和故障排除至关重要。访问这些事件ID对于诊断问题、确保运营效率和增强整体安全性至关重要。

解决方案

打开文件资源管理器，导航到C:\Program Files\Cisco\AMP\<version_number>\AMPEvents.man文件。您可以在记事本中打开此文件，以查看与Cisco安全终端生成的Windows事件相关的所有信息。

从AMPEvents.man文件导出的事件ID列表：

事件ID	Event	引擎/任务	级别
100	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V1/V2/V3/V4	漏洞防御	信息
101	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V1/V2/V3/V4	漏洞防御	信息
102	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V3/V4_AUDIT	漏洞防御	信息
103	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V3/V4_AUDIT	漏洞防御	信息
104	EXPREV_SCRIPT_CONTROL_ATTACK_V4	漏洞防御	信息
105	EXPREV_SCRIPT_CONTROL_ATTACK_V4_AUDIT	漏洞防御	信息
200	MALICIOUS_ACTIVITY_PROTECTION_V1/V2	MaliciousActivityProtection	信息
300	SD_BLOCK_PROCESS_ACTION_V1	SystemProcessProtection	信息
400	CCMS_JOB_STARTED_V1	CCMS	信息
401	JANUS_EVENT_V1		信息
500	ENDPOINT_ISOLATION_STARTED_V1	终端隔离	信息
501	ENDPOINT_ISOLATION_STOPPED_V1	终端隔离	信息
502	ENDPOINT_ISOLATION_STARTFAILED_V1	终端隔离	Erro
503	ENDPOINT_ISOLATION_STOPFAILED_V1	终端隔离	Erro
504	ENDPOINT_ISOLATION_UPDATED_V1	终端隔离	信息
505	ENDPOINT_ISOLATION_UPDATEFAILED_V1	终端隔离	Erro
600	ORBAL_INSTALL_SUCCESS_V1	轨道	信息
601	ORBAL_INSTALL_FAILED_V1	轨道	Erro
602	ORBAL_UPDATE_SUCCESS_V1	轨道	信息
603	ORBAL_UPDATE_FAILED_V1	轨道	Erro
700	ENDPOINT_ISOLATION_BRUTE_FORCE_ATTEMPT	终端隔离	警告
800	SCRIPT_PROTECTION_DETECTION_V1	脚本保护	信息
801	SCRIPT_PROTECTION_QUARANTINE_V1	脚本保护	信息
900	ENGINE_DETECTION_HANDLED	行为保护	信息
901	ENGINE_DETECTION_NOT_HANDLED	行为保护	Erro
902	ENGINE_DETECTION_AUDIT	行为保护	信息
903	ENGINE_DETECTION_NO_ACTION	行为保护	信息
904	ENGINE_CLEANUP_REQUIRED	行为保护	信息
1248	SCAN_COMPLETED_CLEAN_V1	扫描	信息
1249	SCAN_COMPLETED_DIRTY_V1	扫描	信息
1250	SCAN_FAILED_V1	扫描	Erro
1300	DETECTION_V1	检测	信息
1310	QUARANTINE_SUCCESS_V1	隔离	信息
1311	QUARANTINE_FAILED_V1	隔离	Erro
1320	EXECUTION_BLOCK_V1	ExecutionBlock	信息
1321	EXECUTION_BLOCK_BAD_PARENT_V1	ExecutionBlock	信息
1700	WMI_RECON_V1	WMIRecon	信息

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。