Exportar lista de identificadores de eventos de Windows para un extremo seguro

Contenido

Introducción

Este documento describe todos los ID de eventos para Cisco Secure Endpoint, lo que ayuda en la supervisión eficaz y la respuesta a incidentes.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Registro de eventos de Windows
- Cisco Secure Endpoint

Componentes Utilizados

La información de este documento se basa en las siguientes versiones de software:

- Cisco Secure Endpoint 8.4.0.30201
- Windows Server 2019

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

Los ID de eventos de Windows para Cisco Secure Endpoint son esenciales para una supervisión y resolución de problemas eficaces. Tener acceso a estas ID de evento es fundamental para diagnosticar problemas, garantizar la eficacia operativa y mejorar la seguridad general.

Solución

Abra File Explorer, navegue hasta el archivo C:\Program Files\Cisco\AMP\<version_number>\AMPEvents.man. Puede abrir este archivo en el Bloc de notas para ver toda la información relacionada con los eventos de Windows generados por Cisco Secure Endpoint.

Lista exportada de ID de eventos desde el archivo AMPEvents.man:

ID de evento	Evento	Motor/Tarea
100	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V1/V2/V3/V4	PrevenciónDeAtaques
101	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V1/V2/V3/V4	PrevenciónDeAtaques
102	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V3/V4_AUDIT	PrevenciónDeAtaques
103	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V3/V4_AUDIT	PrevenciónDeAtaques
104	EXPREV_SCRIPT_CONTROL_ATTACK_V4	PrevenciónDeAtaques
105	EXPREV_SCRIPT_CONTROL_ATTACK_V4_AUDIT	PrevenciónDeAtaques
200	MALICIOUS_ACTIVITY_PROTECTION_V1/V2	ProtecciónActividadMaliciosa
300	SD_BLOCK_PROCESS_ACTION_V1	SystemProcessProtection
400	CCMS_JOB_STARTED_V1	CCMS
401	JANUS_EVENT_V1	
500	ENDPOINT_ISOLATION_STARTED_V1	Aislamiento de terminales
501	ENDPOINT_ISOLATION_STOPPED_V1	Aislamiento de terminales
502	ENDPOINT_ISOLATION_STARTFAILED_V1	Aislamiento de terminales
503	ENDPOINT_ISOLATION_STOPFAILED_V1	Aislamiento de terminales
504	ENDPOINT_ISOLATION_UPDATED_V1	Aislamiento de terminales
505	ENDPOINT_ISOLATION_UPDATEFAILED_V1	Aislamiento de terminales
600	ORBITAL_INSTALL_SUCCESS_V1	Orbital
601	ORBITAL_INSTALL_FAILED_V1	Orbital
602	ORBITAL_UPDATE_SUCCESS_V1	Orbital
603	ORBITAL_UPDATE_FAILED_V1	Orbital
700	ENDPOINT_ISOLATION_BRUTE_FORCE_ATTEMPT	Aislamiento de terminales
800	SCRIPT_PROTECTION_DETECTION_V1	ProtecciónScript
801	SCRIPT_PROTECTION_QUARANTINE_V1	ProtecciónScript
900	ENGINE_DETECTION_HANDLED	ProtecciónComportamiento
901	ENGINE_DETECTION_NOT_HANDLED	ProtecciónComportamiento
902	ENGINE_DETECTION_AUDIT	ProtecciónComportamiento
903	ENGINE_DETECTION_NO_ACTION	ProtecciónComportamiento
904	ENGINE_CLEANUP_REQUIRED	ProtecciónComportamiento
1248	SCAN_COMPLETED_CLEAN_V1	Escanear
1249	SCAN_COMPLETED_DIRTY_V1	Escanear
1250	SCAN_FAILED_V1	Escanear

1300	DETECTION_V1	Detección
1310	QUARANTINE_SUCCESS_V1	Cuarentena
1311	QUARANTINE_FAILED_V1	Cuarentena
1320	EXECUTION_BLOCK_V1	BloqueDeEjecución
1321	EXECUTION_BLOCK_BAD_PARENT_V1	BloqueDeEjecución
1700	WMI_RECON_V1	WMIRecon

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).