Exportar Lista de IDs de Eventos do Windows para Ponto de Extremidade Seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

- [Requisitos](#)
- [Componentes Utilizados](#)

[Problema](#)

[Solução](#)

Introdução

Este documento descreve todas as IDs de evento do Cisco Secure Endpoint, ajudando no monitoramento e na resposta a incidentes eficazes.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Log de Eventos do Windows
- Endpoint seguro da Cisco

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Endpoint Cisco Secure 8.4.0.30201
- Windows Server 2019

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

As IDs de Evento do Windows para o Cisco Secure Endpoint são essenciais para monitoramento e solução de problemas eficientes. Ter acesso a essas IDs de evento é essencial para diagnosticar problemas, garantir a eficiência operacional e melhorar a segurança geral.

Solução

Abra o Explorador de Arquivos, navegue para o arquivo C:\Program Files\Cisco\AMP\<número_da_versão>\AMPEvents.man. Você pode abrir esse arquivo no Bloco de Notas para exibir todas as informações relacionadas aos eventos do Windows gerados pelo Cisco Secure Endpoint.

Lista exportada de IDs de eventos do arquivo AMPEvents.man:

ID do evento	Evento	Mecanismo/Tarefa
100	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V1/V2/V3/V4	Prevenção deexploração
101	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V1/V2/V3/V4	Prevenção deexploração
102	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V3/V4_AUDIT	Prevenção deexploração
103	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V3/V4_AUDIT	Prevenção deexploração
104	EXPREV_SCRIPT_CONTROL_ATTACK_V4	Prevenção deexploração
105	EXPREV_SCRIPT_CONTROL_ATTACK_V4_AUDIT	Prevenção deexploração
200	MALICIOUS_ACTIVITY_PROTECTION_V1/V2	ProteçãoContraAtividadeMal-Intencionada
300	SD_BLOCK_PROCESS_ACTION_V1	ProteçãoDoProcessoDoSiste
400	CCMS_JOB_STARTED_V1	CCMS
401	JANUS_EVENT_V1	
500	ENDPOINT_ISOLATION_STARTED_V1	IsolamentoDePontoDeExtrem
501	ENDPOINT_ISOLATION_STOPPED_V1	IsolamentoDePontoDeExtrem
502	ENDPOINT_ISOLATION_STARTFAILED_V1	IsolamentoDePontoDeExtrem
503	ENDPOINT_ISOLATION_STOPFAILED_V1	IsolamentoDePontoDeExtrem
504	ISOLAMENTO_PONTO_EXTREMIDADE_ATUALIZADO_V1	IsolamentoDePontoDeExtrem
505	ENDPOINT_ISOLATION_UPDATEFAILED_V1	IsolamentoDePontoDeExtrem
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	IsolamentoDePontoDeExtrem
800	SCRIPT_PROTECTION_DETECTION_V1	ProteçãoDeScript
801	SCRIPT_PROTECTION_QUARANTINE_V1	ProteçãoDeScript
900	ENGINE_DETECTION_HANDLED	Proteção comportamental
901	ENGINE_DETECTION_NOT_HANDLED	Proteção comportamental
902	ENGINE_DETECTION_AUDIT	Proteção comportamental
903	ENGINE_DETECTION_NO_ACTION	Proteção comportamental
904	ENGINE_CLEANUP_REQUIRED	Proteção comportamental
1248	SCAN_COMPLETED_CLEAN_V1	Verificar
1249	SCAN_COMPLETED_DIRTY_V1	Verificar

1250	SCAN_FAILED_V1	Verificar
1300	DETECÇÃO_V1	Detecção
1310	QUARANTINE_SUCCESS_V1	Quarentena
1311	QUARANTINE_FAILED_V1	Quarentena
1320	EXECUTION_BLOCK_V1	Bloco deExecução
1321	EXECUTION_BLOCK_BAD_PARENT_V1	Bloco deExecução
1700	WMI_RECON_V1	WMIRecon

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.