Export List of Windows Event IDs for Secure Endpoint

Contents

Introduction

This document describes all event IDs for Cisco Secure Endpoint, aiding in effective monitoring and incident response.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Windows Event Logging
- Cisco Secure Endpoint

Components Used

The information in this document is based on these software verisons:

- Cisco Secure Endpoint 8.4.0.30201
- Windows Server 2019

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

Windows Event IDs for Cisco Secure Endpoint are essential for effective monitoring and troubleshooting. Having access to these Event IDs is critical for diagnosing issues, ensuring operational efficiency, and enhancing overall security.

Solution

Open **File Explorer**, navigate to **C:\Program**

Files\Cisco\AMP\<version_number>\AMPEvents.man file. You can open this file in Notepad to view all the infomation related to Windows events generated by Cisco Secure Endpoint.

Exported list of Event IDs from the AMPEvents.man file:

Event ID	Event	Engine/Task	Level
100	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V1/V2/V3/V4	ExploitPrevention	Inform
101	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V1/V2/V3/V4	ExploitPrevention	Inform
102	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V3/V4_AUDIT	ExploitPrevention	Inform
103	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V3/V4_AUDIT	ExploitPrevention	Inform
104	EXPREV_SCRIPT_CONTROL_ATTACK_V4	ExploitPrevention	Inform
105	EXPREV_SCRIPT_CONTROL_ATTACK_V4_AUDIT	ExploitPrevention	Inform
200	MALICIOUS_ACTIVITY_PROTECTION_V1/V2	MaliciousActivityProtection	Inform
300	SD_BLOCK_PROCESS_ACTION_V1	SystemProcessProtection	Inform
400	CCMS_JOB_STARTED_V1	CCMS	Inform
401	JANUS_EVENT_V1		Inform
500	ENDPOINT_ISOLATION_STARTED_V1	EndpointIsolation	Inform
501	ENDPOINT_ISOLATION_STOPPED_V1	EndpointIsolation	Inform
502	ENDPOINT_ISOLATION_STARTFAILED_V1	EndpointIsolation	Error
503	ENDPOINT_ISOLATION_STOPFAILED_V1	EndpointIsolation	Error
504	ENDPOINT_ISOLATION_UPDATED_V1	EndpointIsolation	Inform
505	ENDPOINT_ISOLATION_UPDATEFAILED_V1	EndpointIsolation	Error
600	ORBITAL_INSTALL_SUCCESS_V1	Orbital	Inform
601	ORBITAL_INSTALL_FAILED_V1	Orbital	Error
602	ORBITAL_UPDATE_SUCCESS_V1	Orbital	Inform
603	ORBITAL_UPDATE_FAILED_V1	Orbital	Error
700	ENDPOINT_ISOLATION_BRUTE_FORCE_ATTEMPT	EndpointIsolation	Warn
800	SCRIPT_PROTECTION_DETECTION_V1	ScriptProtection	Inform
801	SCRIPT_PROTECTION_QUARANTINE_V1	ScriptProtection	Inform
900	ENGINE_DETECTION_HANDLED	BehavioralProtection	Inform
901	ENGINE_DETECTION_NOT_HANDLED	BehavioralProtection	Error
902	ENGINE_DETECTION_AUDIT	BehavioralProtection	Inform
903	ENGINE_DETECTION_NO_ACTION	BehavioralProtection	Inform
904	ENGINE_CLEANUP_REQUIRED	BehavioralProtection	Inform
1248	SCAN_COMPLETED_CLEAN_V1	Scan	Inform
1249	SCAN_COMPLETED_DIRTY_V1	Scan	Inform
1250	SCAN_FAILED_V1	Scan	Error
1300	DETECTION_V1	Detection	Inform
1310	QUARANTINE_SUCCESS_V1	Quarantine	Inform
1311	QUARANTINE_FAILED_V1	Quarantine	Error
1320	EXECUTION_BLOCK_V1	ExecutionBlock	Inform
1321	EXECUTION_BLOCK_BAD_PARENT_V1	ExecutionBlock	Inform
1700	WMI_RECON_V1	WMIRecon	Inform