Liste der Windows-Ereignis-IDs für sichere Endpunkte exportieren

Inhalt

Einleitung

In diesem Dokument werden alle Ereignis-IDs für Cisco Secure Endpoint beschrieben, um eine effektive Überwachung und Reaktion auf Vorfälle zu ermöglichen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Windows-Ereignisprotokollierung
- Sichere Endgeräte von Cisco

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco Secure Endpoint 8.4.0.30201
- Windows Server 2019

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

Windows Event IDs für Cisco Secure Endpoint sind für eine effektive Überwachung und Fehlerbehebung unerlässlich. Der Zugriff auf diese Ereignis-IDs ist für die Diagnose von Problemen, die Sicherstellung der Betriebseffizienz und die Verbesserung der allgemeinen

Sicherheit von entscheidender Bedeutung.

Lösung

Öffnen Sie den Datei-Explorer, und navigieren Sie zur Datei C:\Program Files\Cisco\AMP\<Versionsnummer>\AMPEvents.man. Sie können diese Datei im Editor öffnen, um alle Informationen zu Windows-Ereignissen anzuzeigen, die von Cisco Secure Endpoint generiert wurden.

Liste der Ereignis-IDs aus der Datei AMPEvents.man exportiert:

Ereignis-ID	Veranstaltung	Engine/Task
100	EXPREV_ATTACK_OHNE_VERDÄCHTIGE_DATEIEN_V1/V2/V3/V4	ExploitPrevention
101	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V1/V2/V3/V4	ExploitPrevention
102	EXPREV_ATTACK_OHNE_VERDÄCHTIGE_DATEIEN_V3/V4_AUDIT	ExploitPrevention
103	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V3/V4_AUDIT	ExploitPrevention
104	EXPREV_SCRIPT_CONTROL_ATTACK_V4	ExploitPrevention
105	EXPREV_SCRIPT_CONTROL_ATTACK_V4_AUDIT	ExploitPrevention
200	SCHÄDLICHE_AKTIVITÄT_SCHUTZ_V1/V2	Schutz vor böswilligen Aktivitäten
300	SD_BLOCK_PROCESS_ACTION_V1	SystemProzessSchutz
400	CCMS_JOB_STARTS_V1	CCMS
401	JANUS_EVENT_V1	
500	ENDPUNKT_ISOLATION_STARTED_V1	Endpunktisolierung
501	ENDPUNKT_ISOLATION_STOPPED_V1	Endpunktisolierung
502	ENDPUNKT_ISOLATION_STARTFAILED_V1	Endpunktisolierung
503	ENDPUNKT_ISOLATION_STOPFAILED_V1	Endpunktisolierung
504	ENDPUNKT_ISOLATION_UPDATED_V1	Endpunktisolierung
505	ENDPUNKT_ISOLATION_UPDATEFAILED_V1	Endpunktisolierung
600	ORBITAL_INSTALL_SUCCESS_V1	Orbital
601	ORBITAL_INSTALL_FAILED_V1	Orbital
602	ORBITAL_UPDATE_SUCCESS_V1	Orbital
603	ORBITALE_UPDATE_FAILED_V1	Orbital
700	ENDPUNKT_ISOLIERUNG_BRUTE_FORCE_VERSUCH	Endpunktisolierung
800	SCRIPT_PROTECTION_DETECTION_V1	Skriptschutz
801	SCRIPT_PROTECTION_QUARANTINE_V1	Skriptschutz
900	MOTOR_ERKENNUNG_BEARBEITET	VerhaltensbasierterSchu
901	MOTOR_ERKENNUNG_NICHT_BEHANDELT	VerhaltensbasierterSchu
902	MODUL_ERKENNUNG_PRÜFUNG	VerhaltensbasierterSchu
903	MOTOR_ERKENNUNG_KEINE_AKTION	VerhaltensbasierterSchu
904	MOTOR_CLEANUP_REQUITED	VerhaltensbasierterSchu
1248	SCAN_COMPLET_CLEAN_V1	Scannen

1249	SCANNEN_ABGESCHLOSSEN_SCHMUTZ_V1	Scannen
1250	SCAN_FAILED_V1	Scannen
1300	ERKENNUNG_V1	Erkennung
1310	QUARANTÄNE_ERFOLG_V1	Quarantäne
1311	QUARANTÄNE_FEHLGESCHLAGEN_1	Quarantäne
1320	EXECUTION_BLOCK_V1	Ausführungsblock
1321	EXECUTION_BLOCK_BAD_PARENT_V1	Ausführungsblock
1700	WMI_RECON_V1	WMIRecon

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.