Exporter la liste des ID d'événements Windows pour Secure Endpoint

Table des matières

Introduction

Ce document décrit tous les ID d'événements pour Cisco Secure Endpoint, ce qui facilite la surveillance et la réponse aux incidents.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Journalisation des événements Windows
- Terminaux sécurisés Cisco

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles suivantes :

- Terminal sécurisé Cisco 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Les ID d'événements Windows pour Cisco Secure Endpoint sont essentiels pour une surveillance et un dépannage efficaces. L'accès à ces ID d'événements est essentiel pour diagnostiquer les problèmes, assurer l'efficacité opérationnelle et améliorer la sécurité globale.

Solution

Ouvrez l'Explorateur de fichiers, accédez au fichier C:\Program Files\Cisco\AMP\<numéro_version>\AMPEvents.man. Vous pouvez ouvrir ce fichier dans le Bloc-notes pour afficher toutes les informations relatives aux événements Windows générés par Cisco Secure Endpoint.

Liste d'ID d'événement exportée à partir du fichier AMPEvents.man :

ID d'événement	Événement	Moteur/Tâche
100	EXPREV_ATTACK_WITHOUT_SUSPCIOUS_FILES_V1/V2/V3/V4	Prévention des exploits
101	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V1/V2/V3/V4	Prévention des exploits
102	EXPREV_ATTACK_WITHOUT_SUSPCIOUS_FILES_V3/V4_AUDIT	Prévention des exploits
103	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V3/V4_AUDIT	Prévention des exploits
104	EXPREV_SCRIPT_CONTROL_ATTACK_V4	Prévention des exploits
105	EXPREV_SCRIPT_CONTROL_ATTACK_V4_AUDIT	Prévention des exploits
200	PROTECTION_ACTIVITÉ_MALVEILLANTE_V1/V2	Protection contre les ac malveillantes
300	SD_BLOCK_PROCESS_ACTION_V1	ProtectionProcessusSy
400	CCMS_JOB_STARTED_V1	CCMS
401	ÉVÉNEMENT_JANUS_V1	
500	ISOLATION_POINT_D'EXTRÉMITÉ_V1	Isolation des terminaux
501	POINT_TERMINAL_ISOLATION_STOPPED_V1	Isolation des terminaux
502	POINT_TERMINAL_ISOLATION_STARTFAILED_V1	Isolation des terminaux
503	POINT_TERMINAL_ISOLATION_STOPFAILED_V1	Isolation des terminaux
504	ISOLATION_POINT_TERMINAL_MIS_À_JOUR_V1	Isolation des terminaux
505	POINT_TERMINAL_ISOLATION_UPDATEFAILED_V1	Isolation des terminaux
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	TENTATIVE_FORCE_BRUTE_ISOLATION_POINT_TERMINAL	Isolation des terminaux
800	PROTECTION_SCRIPT_DÉTECTION_V1	ProtectionScript
801	SCRIPT_PROTECTION_QUARANTINE_V1	ProtectionScript
900	DÉTECTION_MOTEUR_TRAITÉ	Protection Comporteme
901	DÉTECTION_MOTEUR_NON_TRAITÉE	Protection Comporteme
902	AUDIT_DÉTECTION_MOTEUR	Protection Comporteme
903	DÉTECTION_MOTEUR_SANS_ACTION	Protection Comporteme
904	NETTOYAGE_MOTEUR_REQUIS	Protection Comporteme
1248	ANALYSE_TERMINÉE_NETTOYÉE_V1	Analyser
1249	BALAYAGE_TERMINÉ_SALE_V1	Analyser

1250	ECHEC_ANALYSE_V1	Analyser
1300	DÉTECTION_V1	Détection
1310	QUARANTAINE_SUCCESS_V1	Quarantaine
1311	ÉCHEC_QUARANTAINE_V1	Quarantaine
1320	BLOC_EXÉCUTION_V1	BlocExécution
1321	BLOC_EXÉCUTION_MAUVAIS_PARENT_V1	BlocExécution
1700	WMI_RECON_V1	WMIRecon

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.