Esporta elenco di ID eventi Windows per l'endpoint protetto

Sommario

[Introduzione](#)

[Prerequisiti](#)

- [Requisiti](#)
- [Componenti usati](#)

[Problema](#)

[Soluzione](#)

Introduzione

Questo documento descrive tutti gli ID evento per Cisco Secure Endpoint, contribuendo a un monitoraggio efficace e alla risposta agli incidenti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Registrazione eventi di Windows
- Cisco Secure Endpoint

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Cisco Secure Endpoint 8.4.0.30201
- Windows Server 2019

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Gli ID evento Windows per Cisco Secure Endpoint sono essenziali per un monitoraggio e una risoluzione dei problemi efficaci. L'accesso a questi ID evento è fondamentale per diagnosticare i problemi, garantire l'efficienza operativa e migliorare la sicurezza complessiva.

Soluzione

Aprire Esplora file, passare al file C:\Program Files\Cisco\AMP\<numero_versione>\AMPEvents.man. È possibile aprire questo file in Blocco note per visualizzare tutte le informazioni correlate agli eventi di Windows generati da Cisco Secure Endpoint.

Elenco esportato di ID evento dal file AMPEvents.man:

ID evento	Evento	Motore/Attività
100	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V1/V2/V3/V4	ExploitPrevention
101	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V1/V2/V3/V4	ExploitPrevention
102	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_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	ATTIVITÀ_DANNOSA_PROTEZIONE_V1/V2	ProtezioneAttivitàDannosa
300	SD_BLOCK_PROCESS_ACTION_V1	ProtezioneProcessoSistema
400	CCMS_JOB_STARTED_V1	CCMS
401	JANUS_EVENT_V1	
500	ENDPOINT_ISOLATION_STARTED_V1	IsolamentoEndpoint
501	ENDPOINT_ISOLATION_STOPPED_V1	IsolamentoEndpoint
502	ENDPOINT_ISOLATION_STARTFAILED_V1	IsolamentoEndpoint
503	ENDPOINT_ISOLATION_STOPFAILED_V1	IsolamentoEndpoint
504	ENDPOINT_ISOLATION_UPDATED_V1	IsolamentoEndpoint
505	ENDPOINT_ISOLATION_UPDATEFAILED_V1	IsolamentoEndpoint
600	ORBITAL_INSTALL_SUCCESS_V1	Orbitale
601	ORBITAL_INSTALL_FAILED_V1	Orbitale
602	ORBITAL_UPDATE_SUCCESS_V1	Orbitale
603	ORBITAL_UPDATE_FAILED_V1	Orbitale
700	TENTATIVO_BRUTE_ISOLATION_ENDPOINT	IsolamentoEndpoint
800	SCRIPT_PROTECTION_DETECTION_V1	ProtezioneScript
801	SCRIPT_PROTECTION_QUARANTINE_V1	ProtezioneScript
900	RILEVAMENTO_MOTORE_GESTITO	Protezione comportamentale
901	RILEVAMENTO_MOTORE_NON_GESTITO	Protezione comportamentale
902	ENGINE_DETECTION_AUDIT	Protezione comportamentale
903	RILEVAMENTO_MOTORE_NESSUNA_AZIONE	Protezione comportamentale

904	ENGINE_CLEANUP_REQUIRED	Protezione comportamentale
1248	SCAN_COMPLETED_CLEAN_V1	Scansione
1249	SCAN_COMPLETED_DIRTY_V1	Scansione
1250	SCAN_FAILED_V1	Scansione
1300	V1_RILEVAMENTO	Rilevamento
1310	QUARANTENA_RIUSCITA_V1	Quarantena
1311	QUARANTENA_NON RIUSCITA_V1	Quarantena
1320	EXECUTION_BLOCK_V1	BloccoEsecuzione
1321	ESECUZIONE_BLOCK_BAD_PARENT_V1	BloccoEsecuzione
1700	WMI_RECON_V1	WMIR econ

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).