Lijst met gebeurtenissen-ID's van Windows exporteren voor beveiligde endpoints

Inhoud

Inleiding

Dit document beschrijft alle gebeurtenis-ID's voor Cisco Secure Endpoint en helpt u bij effectieve bewaking en respons op incidenten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Vastlegging gebeurtenissen in Windows
- Cisco Secure-endpoint

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco Secure Endpoint 8.4.0.30201
- Windows Server 2019

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem

Windows Event ID's voor Cisco Secure Endpoint zijn essentieel voor effectieve bewaking en probleemoplossing. Het hebben van toegang tot deze Event IDs is cruciaal voor het diagnosticeren van problemen, het verzekeren van operationele efficiency, en het verbeteren van

algemene veiligheid.

Oplossing

Open File Explorer, navigeer naar C:\Program Files\Cisco\AMP\<version_number>\AMPEevents.man bestand. U kunt dit bestand in Kladblok openen om alle informatie te bekijken die betrekking heeft op Windows-gebeurtenissen die door Cisco Secure Endpoint zijn gegenereerd.

Geëxporteerde lijst van Event ID's uit het bestand AMPEevents.man:

Event-ID	Gebeurtenis	Engine/taak	Waterpa
100	EXPREV_ATTACK_ZONDER_VERDACHTE_FILES_V1/V2/V3/V4	Preventie van uitbuiting	informati
101	EXPREV_ATTACK_WITH_suspICIOUS_FILES_V1/V2/V3/V4	Preventie van uitbuiting	informati
102	EXPREV_ATTACK_NOT_VERDACHTE_FILES_V3/V4_AUDIT	Preventie van uitbuiting	informati
103	EXPREV_ATTACK_WITH_suspICIOUS_FILES_V3/V4_AUDIT	Preventie van uitbuiting	informati
104	EXPREV_SCRIPT_CONTROL_ATTACK_V4	Preventie van uitbuiting	informati
105	EXPREV_SCRIPT_CONTROL_ATTACK_V4_AUDIT	Preventie van uitbuiting	informati
200	KWAADAARDIGE_ACTIVITEIT_BESCHERMING_V1/V2	Kwaadaardige activiteitsbescherming	informati
300	SD_BLOK_PROCES_ACTION_V1	Procesbescherming voor systemen	informati
400	CCMS_TAAK_GESTART_V1	CCMS	informati
401	JANUS_EVENT_V1		informati
500	ENDPOINT_ISOLATION_START_V1	Endpoint-isolatie	informati
501	ENDPOINT_ISOLATION_STOPSTED_V1	Endpoint-isolatie	informati
502	ENDPOINT_ISOLATION_STARTFAILL_V1	Endpoint-isolatie	Fout
503	ENDPOINT_ISOLATION_STOPFAILL_V1	Endpoint-isolatie	Fout
504	ENDPOINT_ISOLATION_UPDATE_V1	Endpoint-isolatie	informati
505	ENDPOINT_ISOLATION_UPDATEFILED_V1	Endpoint-isolatie	Fout
600	ORBITAL_INSTALL_SUCCESS_V1	orbitaal	informati
601	ORBITAL_INSTALL_FAILL_V1	orbitaal	Fout
602	ORBITAL_UPDATE_SUCCESS_V1	orbitaal	informati
603	ORBITAL_UPDATE_FAILL_V1	orbitaal	Fout
700	ENDPOINT_ISOLATION_BRUTE_FORCE_TRY	Endpoint-isolatie	WAARS
800	SCRIPT_PROTECTION_DETECTION_V1	Script-bescherming	informati

801	SCRIPT_PROTECTION_QUARANTAINE_V1	Script-bescherming	informati
900	MOTOR_DETECTIE_BEHANDELD	Gedragsbescherming	informati
901	ENGINE_DETECTIE_NIET_BEHANDELD	Gedragsbescherming	Fout
902	ENGINE_DETECTIE_AUDIT	Gedragsbescherming	informati
903	ENGINE_DETECTIE_NO_ACTION	Gedragsbescherming	informati
904	MOTOR_OPRUIMEN_VEREIST	Gedragsbescherming	informati
1248	SCAN_VOLTOOID_CLEAN_V1	Scannen	informati
1249	SCAN_VOLTOOID_DIRTY_V1	Scannen	informati
1250	SCAN_MISLUKT_V1	Scannen	Fout
1300	DETECTIE_V1	Detectie	informati
1310	QUARANTAINE_SUCCESS_V1	quarantaine	informati
1311	QUARANTAINE_MISLUKT_V1	quarantaine	Fout
1320	UITVOERING_BLOK_V1	ExecutionBlock	informati
1321	UITVOERING_BLOK_BAD_PARENT_V1	ExecutionBlock	informati
1700	WMI_RECON_V1	WMIRecon	informati

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.