보안 끝점에 대한 Windows 이벤트 ID 목록 내보내기

목차

소개

이 문서에서는 효과적인 모니터링 및 사고 대응을 돕는 Cisco Secure Endpoint의 모든 이벤트 ID에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Windows 이벤트 로깅
- Cisco Secure Endpoint

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco Secure Endpoint 8.4.0.30201
- Windows Server 2019

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

Cisco Secure Endpoint의 Windows 이벤트 ID는 효과적인 모니터링 및 문제 해결에 필수적입니다. 이러한 이벤트 ID에 대한 액세스 권한은 문제를 진단하고 운영 효율성을 보장하며 전반적인 보안을 강화하는 데 매우 중요합니다.

솔루션

파일 탐색기를 열고 C:\Program Files\Cisco\AMP\<version_number>\AMPEvents.man 파일로 이동합니다. 메모장에서 이 파일을 열어 Cisco Secure Endpoint에서 생성한 Windows 이벤트와 관련된 모든 정보를 볼 수 있습니다.

AMPEvents.man 파일에서 이벤트 ID 목록을 내보냈습니다.

이벤트 ID	이벤트	엔진/작업	수준
100	EXPRESS_ATTACK_WITHOUT_SUSPICIOUS_FILES_V1/V2/V3/V4	익스플로잇 방지	정보
101	EXPRESS_ATTACK_WITH_SUSPICIOUS_FILES_V1/V2/V3/V4	익스플로잇 방지	정보
102	EXPRESS_ATTACK_WITHOUT_SUSPICIOUS_FILES_V3/V4_AUDIT	익스플로잇 방지	정보
103	EXPRESS_ATTACK_WITH_SUSPICIOUS_FILES_V3/V4_AUDIT	익스플로잇 방지	정보
104	EXPRESS_SCRIPT_CONTROL_ATTACK_V4	익스플로잇 방지	정보
105	EXPRESS_SCRIPT_CONTROL_ATTACK_V4_AUDIT	익스플로잇 방지	정보
200	MALICIOUS_ACTIVITY_PROTECTION_V1/V2	악의적활동보호	정보
300	SD_BLOCK_PROCESS_ACTION_V1	SystemProcessProtection	정보
400	CCMS_JOB_STARTED_V1	CCMS	정보
401	JANUS_EVENT_V1		정보
500	ENDPOINT_ISOLATION_STARTED_V1	엔드포인트격리	정보
501	ENDPOINT_ISOLATION_STOPPED_V1	엔드포인트격리	정보
502	ENDPOINT_ISOLATION_STARTFAILED_V1	엔드포인트격리	오류
503	ENDPOINT_ISOLATION_STOPFAILED_V1	엔드포인트격리	오류
504	ENDPOINT_ISOLATION_UPDATED_V1	엔드포인트격리	정보
505	ENDPOINT_ISOLATION_UPDATEFAILED_V1	엔드포인트격리	오류
600	ORBITAL_INSTALL_SUCCESS_V1	궤도	정

			보
601	ORBITAL_INSTALL_FAILED_V1	궤도	오류
602	ORBITAL_UPDATE_SUCCESS_V1	궤도	정보
603	ORBITAL_UPDATE_FAILED_V1	궤도	오류
700	ENDPOINT_ISOLATION_BRUTE_FORCE_ATTEMPT	엔드포인트격리	경고
800	SCRIPT_PROTECTION_DETECTION_V1	스크립트보호	정보
801	SCRIPT_PROTECTION_QUARANTINE_V1	스크립트보호	정보
900	ENGINE_DETECTION_처리됨	동작보호	정보
901	ENGINE_DETECTION_NOT_처리됨	동작보호	오류
902	ENGINE_DETECTION_AUDIT	동작보호	정보
903	ENGINE_DETECTION_NO_ACTION	동작보호	정보
904	ENGINE_클린업_필수	동작보호	정보
1248	SCAN_COMPLETED_CLEAN_V1	스캔	정보
1249	SCAN_COMPLETED_DIRTY_V1	스캔	정보
1250	SCAN_FAILED_V1	스캔	오류
1300	탐지_V1	탐지	정보
1310	QUARANTINE_SUCCESS_V1	쿼런틴	정보
1311	QUARANTINE_FAILED_V1	쿼런틴	오류
1320	EXECUTION_BLOCK_V1	실행 블록	정보
1321	EXECUTION_BLOCK_BAD_PARENT_V1	실행 블록	정보
1700	WMI_RECON_V1	WMIRecon	정보

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.