라이센스 변경 후 SIEM에서 보안 액세스 파일 이벤트 로그 누락

목차

문제

DNS 로그가 계속해서 성공적으로 전달되는 동안 AWS S3 스토리지에서 SIEM이 파일 이벤트 로그를 수신하는 것을 중지했습니다. File Event 데이터 커넥터는 SIEM 인터페이스에 "disconnected(연결 끊김)" 아이콘을 표시했습니다. 표시가 중지된 로그는 DLP/IPS 관련 파일 이벤트 레코드로 식별되었습니다. DNS 레이어 로그는 이슈 기간 동안 계속 작동합니다.

마이그레이션 과정에서 환경에서 Umbrella와 Secure Access를 모두 사용했으며, 로그는 동일한 AWS 버킷으로 전송되었습니다. 키가 회전했고 제대로 작동하고 있는 것으로 확인됐다. 버전 16을 사용할 수 있는 동안 스키마 버전이 버전 10으로 기록되었습니다.

환경

- Umbrella 및 Secure Access 구성을 모두 갖춘 Cisco Secure Access 조직
- 로그 내보내기를 위한 AWS S3 스토리지 통합
- Microsoft Sentinel SIEM 플랫폼
- 사용 중인 스키마 버전 10(버전 16 사용 가능)
- Secure Access 라이센스가 Advantage에서 Essentials로 2026년 6월 23일 변경되었습니다.
- 파일 이벤트 로그가 2026년 6월 24일에 마지막으로 관찰됨

해결

조사 결과, 파일 이벤트 로그가 특정 라이센싱 기능이 필요한 DLP/IPS 기능과 관련된 것으로 나타났습니다. 다음 분석을 통해 근본 원인을 파악하였다.

1단계: 트래픽 분석

트래픽 패턴을 확인하려면 Secure Access에서 Activity Search를 선택합니다.

1.- Activity Search(활동 검색)로 이동하여 웹 트래픽 또는 악성 속성 이벤트를 필터링합니다. 분석 결과 DNS 트래픽이 있었지만 지난 30일 동안 웹 트래픽 이벤트가 보이지 않았고 파일 검사가 활성화된 규칙이 확인되지 않았습니다.
2.- Traffic Flow(트래픽 흐름) > Logs on the CSA report(CSA 보고서 로그) > S3 bucket(S3 버킷) - SIEM.

2단계: 라이센스 기록 검토

1.- Secure Access에서 라이센스 내역을 검토하여 파일 이벤트 로그 중지 시점과 일치하는 변경 사항을 확인합니다.

2.- Secure Access(보안 액세스) > Admin(관리) > Subscription(서브스크립션)으로 이동하여 현재 라이센스 레벨 및 기능 요약을 확인합니다.

조사 결과, 2026년 6월 23일 Secure Access 라이센스가 Secure Access Advantage에서 Secure Access Essentials로 변경되었으며, 이는 파일 이벤트 로그가 표시되지 않는 시점과 일치합니다.

3단계: 기능 확인

현재 라이센스 레벨에 어떤 기능이 포함되어 있는지 확인합니다. 파일 이벤트 로그를 생성하는 DLP 및 IPS 기능은 Secure Access Essentials 라이센스 계층에 포함되지 않습니다.

4단계: 확인 및 근본 원인

File Event 로그가 표시되지 않을 때 라이센스 변경 시점이 완벽하게 일치합니다. DNS 레이어 로깅이 계속 작동하고 기본 요구 사항이었으므로, 파일 이벤트 로그를 현재 Essentials 라이센스에서 사용할 수 없다는 점을 감안하여 이 사례를 해결했습니다.

원인

2026년 6월 23일 Secure Access Advantage에서 Secure Access Essentials로의 라이센스 변경으로 인해 파일 이벤트 로그 생성이 중지되었습니다. 파일 이벤트 로그는 Essentials 라이센스 계층에 포함되지 않는 DLP 및 IPS 기능과 연결됩니다. 이 라이센스는 이러한 특정 로그 유형을 생성하는 파일 검사 기능에 대한 액세스를 다운그레이드했습니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

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.