Cisco Security Cloud 제품에서 HAR 로그 수집

목차

소개

이 문서에서는 브라우저에서 HAR(HTTP 아카이브) 로그를 수집하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

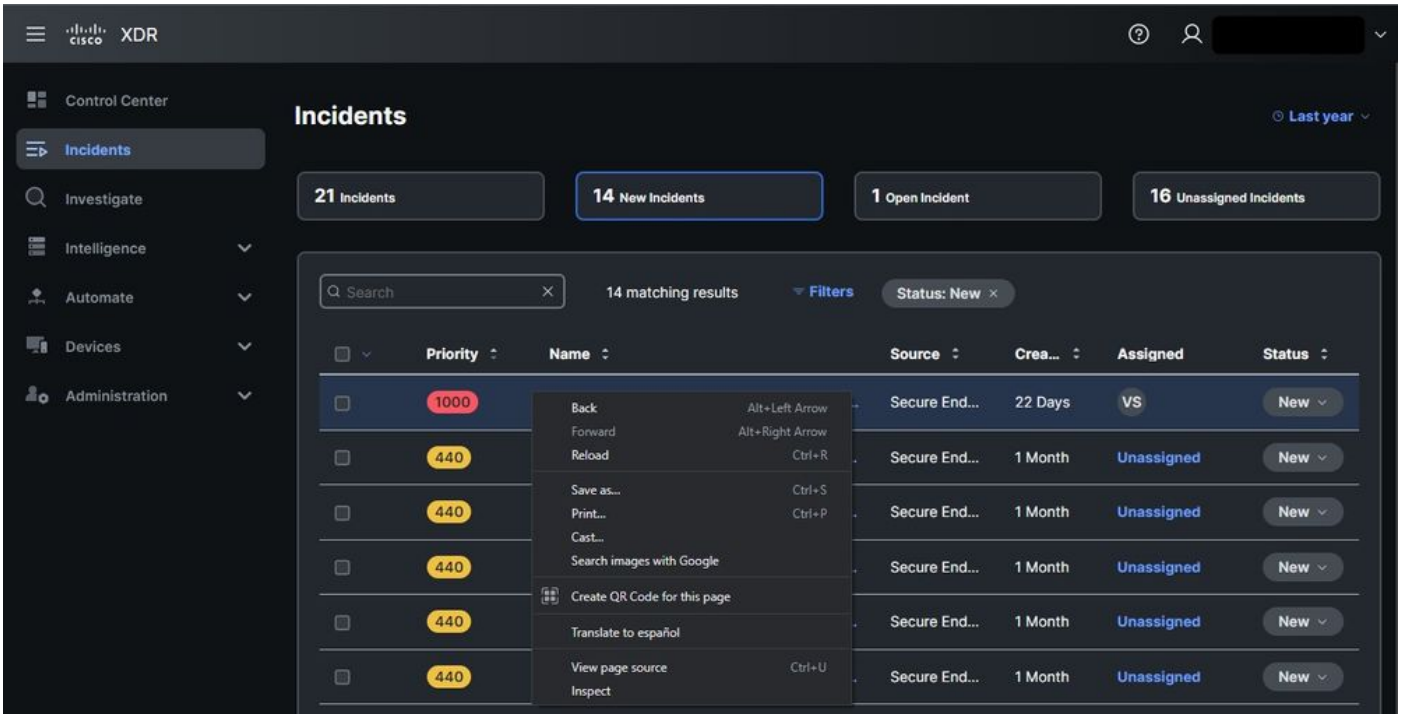
문제/장애:

TAC에서는 HAR 로그를 사용하여 XDR 콘솔과 같은 Cisco 보안 제품과 관련된 문제를 해결합니다.

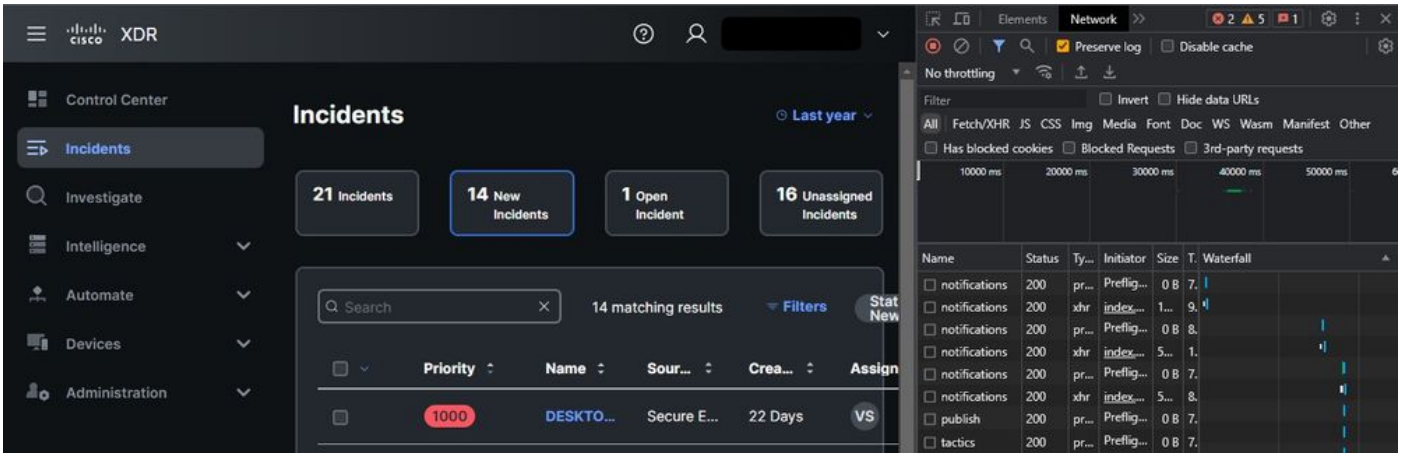
HAR 로그의 정보를 사용하여 TAC는 백엔드 서버에 대한 API 쿼리를 검토하고 문제를 효율적으로 격리할 수 있습니다.

해결책:

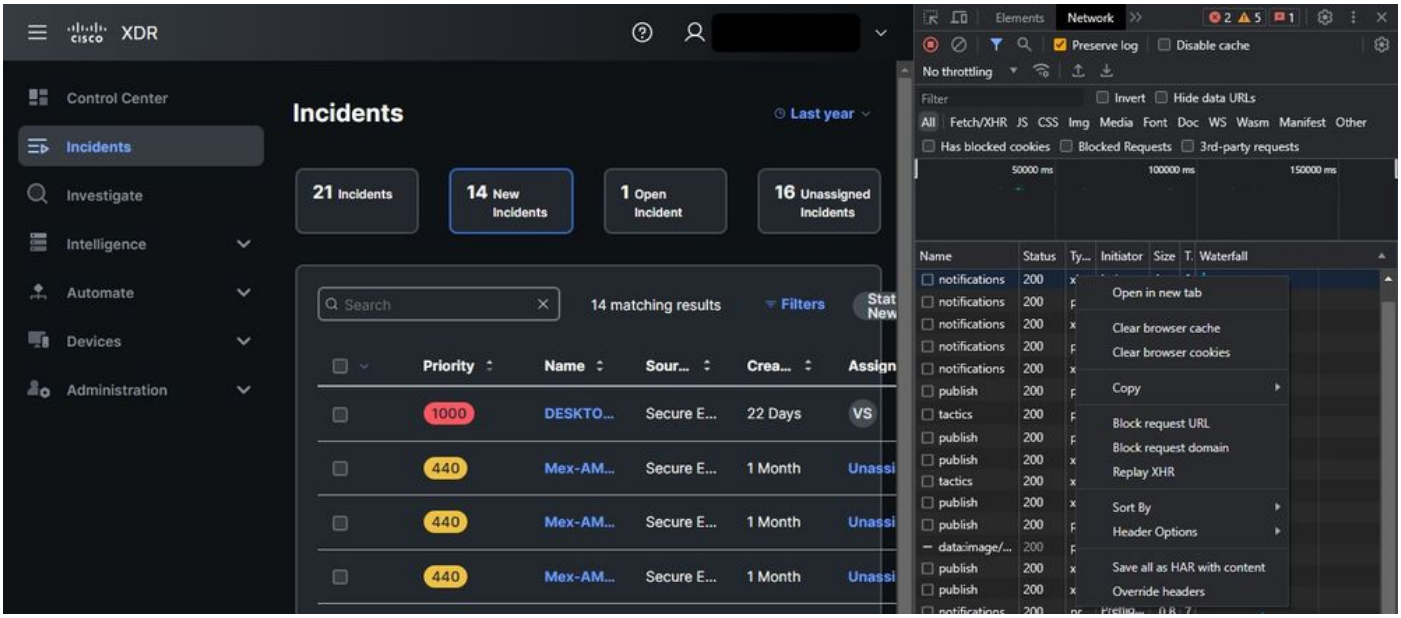
1단계. Cisco Security Cloud Product 콘솔로 이동합니다. 이 예에서는 XDR 콘솔을 사용했습니다.
2단계. 문제가 있는 섹션으로 이동하여 마우스 오른쪽 버튼을 클릭합니다.
3단계. 선택 **Inspect.**

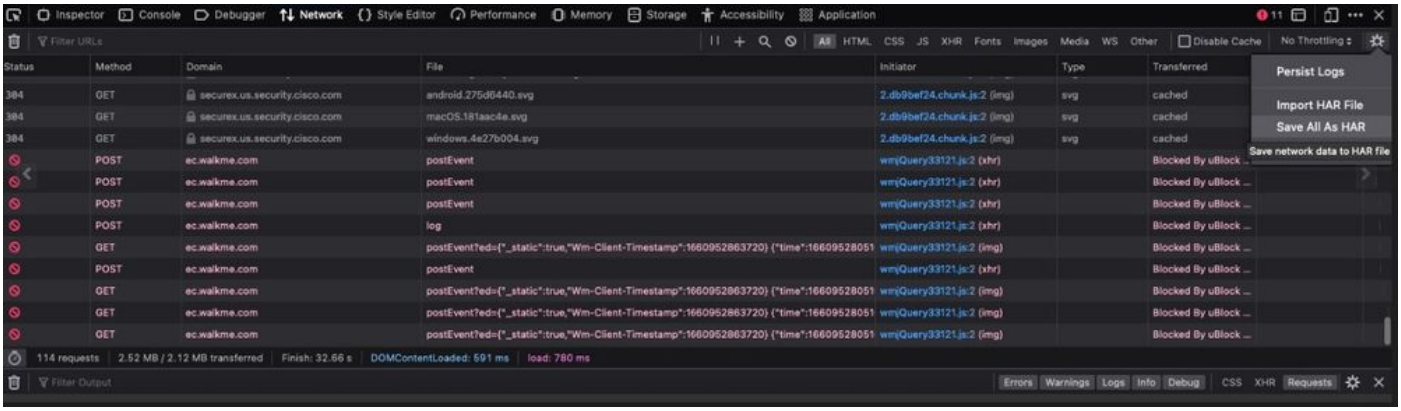


4단계. 탐색: **Network** 탭을 클릭합니다.



5단계. 모든 쿼리를 로그에서 캡처할 수 있도록 문제를 재현하거나 페이지를 다시 로드합니다.
6단계. 마우스 오른쪽 버튼을 클릭하고 **Save All as HAR with content** 를 클릭하여 컴퓨터에 로그를 아카이브하거나 브라우저에 따라 엔진 아이콘을 선택하여 Save All as HAR with content 옵션을 시각화합니다.





7단계. HAR 파일이 생성되면 파일을 지원 케이스 관리자 자세히 살펴보겠습니다.

관련 정보

- 공식 XDR 문서
- 기술 지원 및 문서 – Cisco Systems

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.