

Cisco XDR 및 Secure Malware Analytics 클라우드 통합 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[문제 해결](#)

[라이선스](#)

[모듈 타일](#)

[관리자 역할](#)

[기간](#)

[모듈 다시 만들기](#)

소개

이 문서에서는 Cisco XDR을 통해 Secure Malware Analytics Cloud 모듈의 문제를 해결하는 방법에 대해 설명합니다.

기고자: Javi Martinez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 보안 악성코드 분석 클라우드
- Cisco XDR

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Secure Malware Analytics 클라우드 콘솔(관리자 권한이 있는 사용자 계정)
- Cisco XDR 콘솔(관리자 권한이 있는 사용자 계정)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco Secure Malware Analytics Cloud는 사용자 환경에 영향을 미치지 않고 의심스러운 파일 또는 웹 대상을 폭파할 수 있는 지능형 자동 악성코드 분석 및 악성코드 위협 인텔리전스 플랫폼입니다.

Cisco XDR과의 통합에서 Secure Malware Analytics는 참조 모듈이며 SMA 클라우드(Secure Malware Analytics Cloud) 지식 스토어에서 파일 해시, IP, 도메인 및 URL에 대한 추가 인텔리전스를 수집하기 위해 Secure Malware Analytics Portal로 피벗하는 기능을 제공합니다.

최신 Secure Malware Analytics 클라우드 통합 가이드를 참조하십시오.

- [NAM 클라우드](#).
- [EU 클라우드](#).

문제 해결

라이선스

- Secure Malware Analytics Cloud Console에 액세스하기 위해 적절한 SMA 라이선스가 있는지 확인합니다.

모듈 타일

- Secure Malware Analytics Cloud Module에 적합한 타일을 선택했는지 확인합니다.
Cisco XDR Portal(Cisco XDR 포털) > Dashboard(대시보드) > Customize(사용자 지정) 버튼 > Select the SMA Cloud(SMA 클라우드 모듈 선택) > Add the appropriate Tiles(적절한 타일 추가)로 이동합니다.

관리자 역할

- Secure Malware Analytics 포털에서 관리자 역할의 Secure Malware Analytics 계정이 있는지 확인합니다.
Cisco XDR Portal(Cisco XDR 포털) > Administration(관리) > Your Account(사용자 계정)로 이동합니다.
- SecureX 포털에서 관리자 권한이 있는 SecureX 계정이 있는지 확인합니다.
Malware Analytics portal(악성코드 분석 포털) > My Malware Analytics account(내 악성코드 분석 계정)로 이동합니다.

참고: Secure Malware Analytics 콘솔 및 Cisco XDR 콘솔에서 관리자 역할이 없는 경우, 관리자는 해당 포털에서 직접 계정 역할을 변경할 수 있습니다

기간

- Cisco XDR 포털에서 타임스탬프가 제대로 설정되었는지 확인합니다.
Cisco XDR Portal(Cisco XDR 포털) > Dashboard(대시보드) > Timeframe(기간) 옵션 > SMA 활동을 기반으로 적절한 기간을 선택합니다.

모듈 다시 만들기

- 기존 SMA 모듈을 삭제하고 새 SMA 모듈을 생성합니다.
Secure Malware Analytics Cloud console(Secure Malware Analytics 클라우드 콘솔) > My Malware Analytics 계정 > API Key(API 키) > Copy the API key(API 키 복사)로 이동합니다.
Cisco XDR Portal(Cisco XDR 포털) > Integration modules(통합 모듈) > Select the SMA Cloud module(SMA 클라우드 선택) > Add the API key and URL (Select the SMA Cloud)(SMA 클라우드 추가) > Create the Dashboard(대시보드 생성)로 이동합니다.

참고: 조직 관리자 또는 사용자 역할이 있는 사용자만 Cisco XDR에서 Secure Malware Analytics 통합 모듈을 활성화하는 API 키를 가져올 수 있습니다.

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.