Cisco SecureX를 Cisco Umbrella와 통합

목차

소개

이 문서에서는 3개의 사용 가능한 API를 사용하여 SecureX와의 Umbrella 통합을 구성하고 확인하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Umbrella
- Cisco Secure X
- Cisco 위협 대응

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- DNS Advantage 라이선스가 있는 Umbrella 계정
- 보안 X

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

배경 정보

이 통합을 모든 기능과 완벽하게 구성하려면 이 3가지 API에 액세스해야 합니다

- 보고 API(모든 라이센스에 포함)
- 시행 API
- Investigate API

Umbrella 통합을 구성하려면 먼저 Umbrella 인스턴스에서 일부 정보를 수집한 다음 Add New Umbrella Module(새 Umbrella 모듈 추가) 양식을 작성해야 합니다.

구성

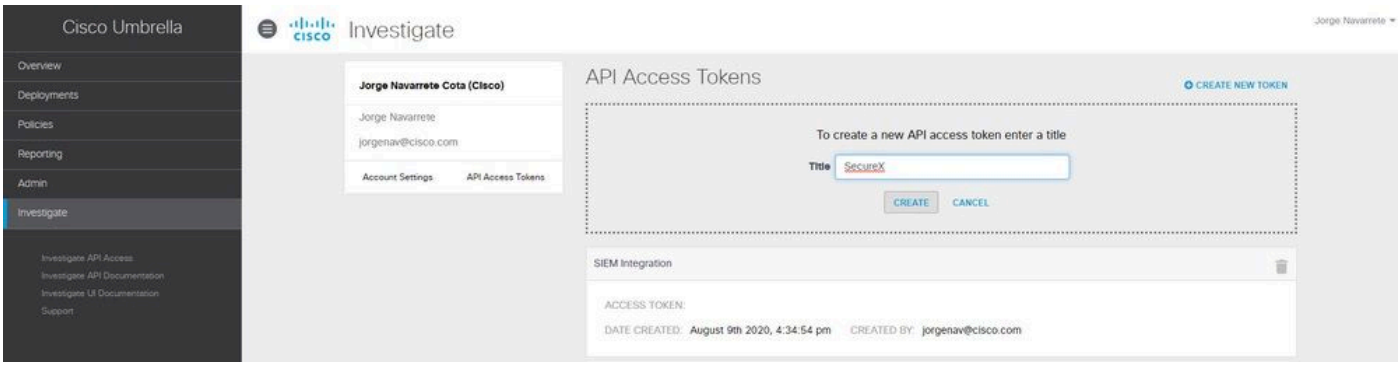
모듈 생성

1. Secure X 계정에 로그인합니다. 아직 계정이 없는 경우 Cisco Secure Sign-On을 사용하여 계정을 생성할 수 있습니다.
2. Integrations(통합) > Add New Module(새 모듈 추가)로 이동합니다. Available Integrations(사용 가능한 통합) 페이지에서 Umbrella(Umbrella) 옵션으로 스크롤하고 Add New Module(새 모듈 추가)을 클릭합니다.

다음 단계에 따라 Add New Umbrella Module(새 Umbrella 모듈 추가) 양식에서 제출하기 위해 Umbrella 계정에서 필요한 정보를 수집합니다.

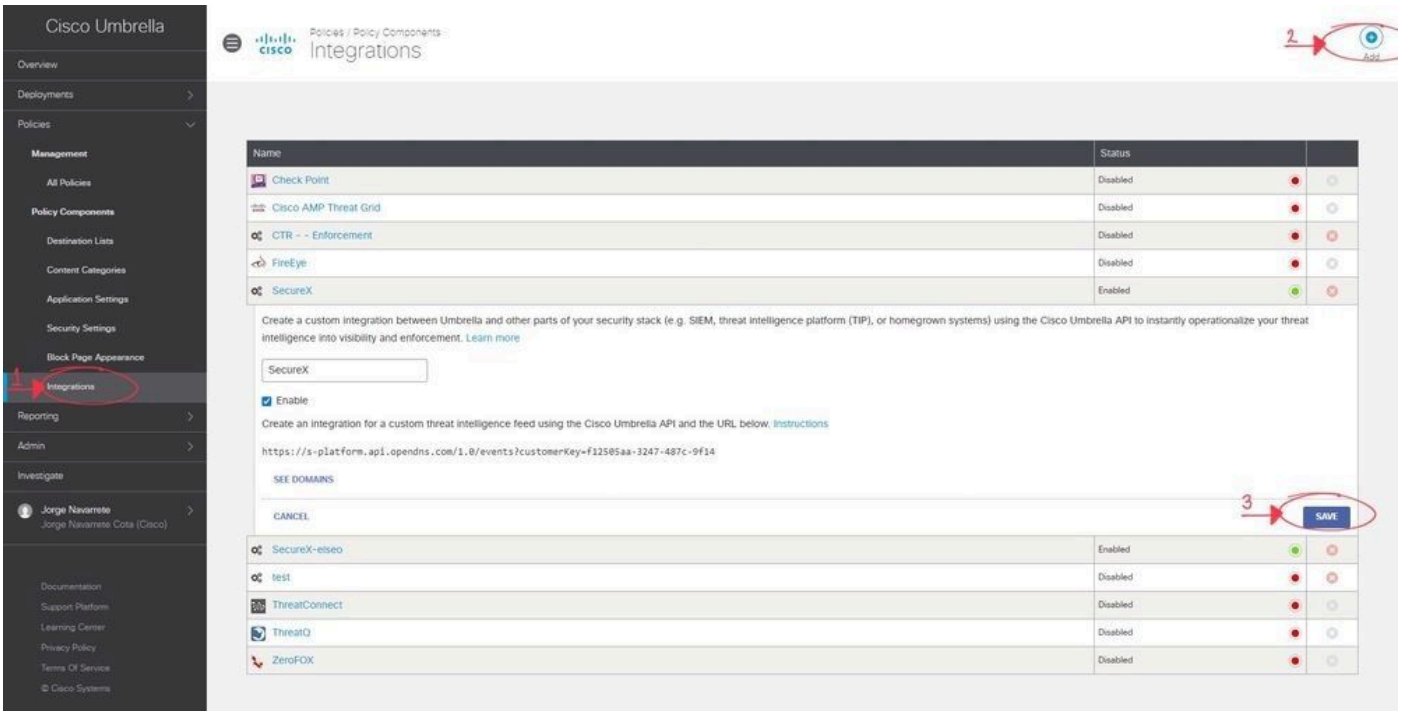
Investigate API

1. Umbrella에서 Investigate > Investigate API Access로 이동하고 Create New Token(새 토큰 생성)을 클릭한 다음 토큰 제목을 입력한 다음 Create New Token(새 토큰 생성)을 다시 클릭합니다.
2. Add New Umbrella Module(새 Umbrella 모듈 추가) 양식의 API Token(API 토큰) 필드에 액세스 토큰 값을 복사합니다.



시행 API

1. Umbrella에서 Policies(정책) > Policy Components(정책 구성 요소) > Integrations(통합)로 이동하고 Add(추가)를 클릭한 후 Name(이름)을 입력하고 Create(생성)를 클릭합니다.
2. 새로 생성된 통합 이름 링크를 클릭하고 Enablecheckbox를 선택한 다음 Save를 선택합니다.
3. 통합 URL을 표시하려면 통합 이름을 클릭합니다. 통합 URL을 Add New Umbrella Module(새 Umbrella 모듈 추가) 양식의 Custom Umbrella Integration URL(맞춤형 Umbrella 통합 URL) 필드에 복사합니다.



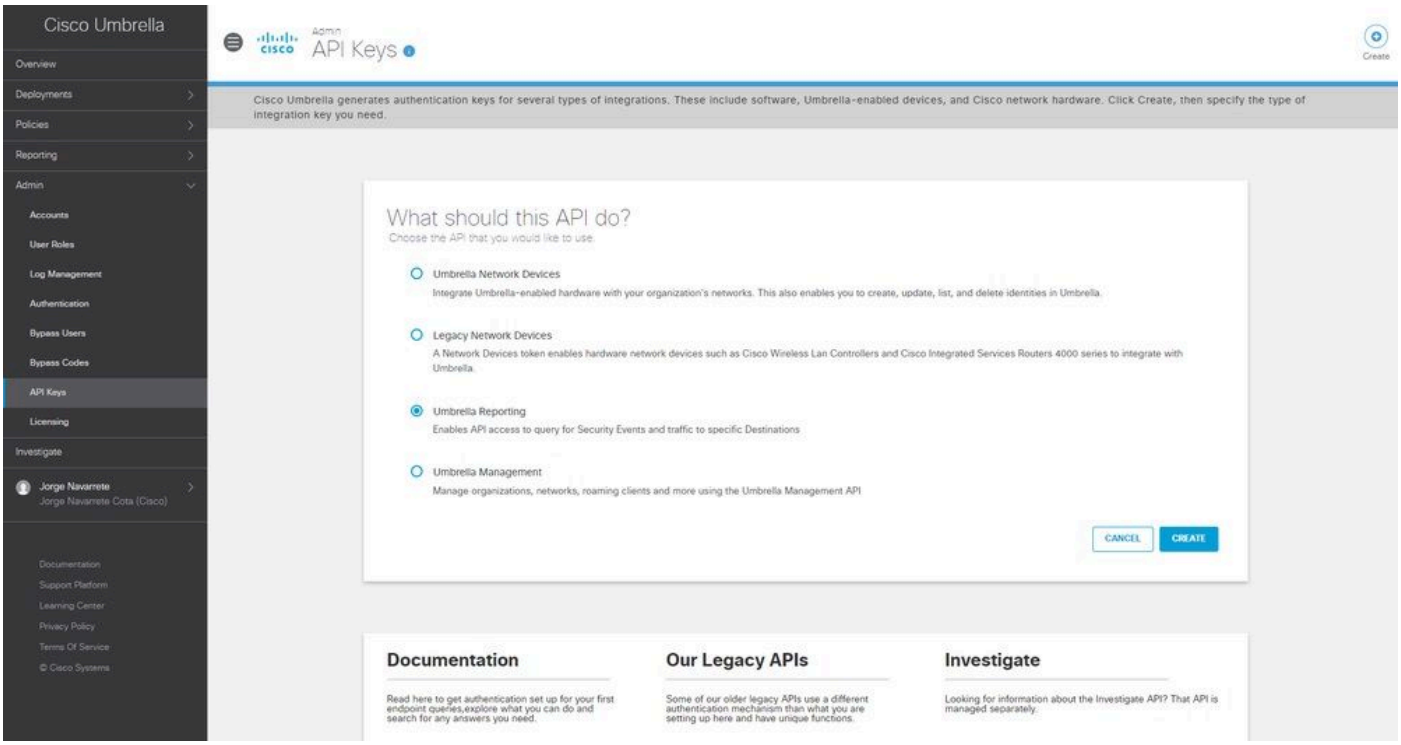
참고: Umbrella Enforcement API를 통합하려면 Umbrella 콘솔의 관리자 대신 Umbrella 독립형 조직 또는 하위 조직의 관리자여야 합니다.

보고 API

1. Umbrella에서 Admin(관리) > API Keys(API 키)로 이동하고 Create(생성)를 클릭합니다.
2. 이 API에서 수행해야 할 작업에서 Umbrella Reporting 라디오 버튼을 클릭한 다음 생성을 클릭합니다.

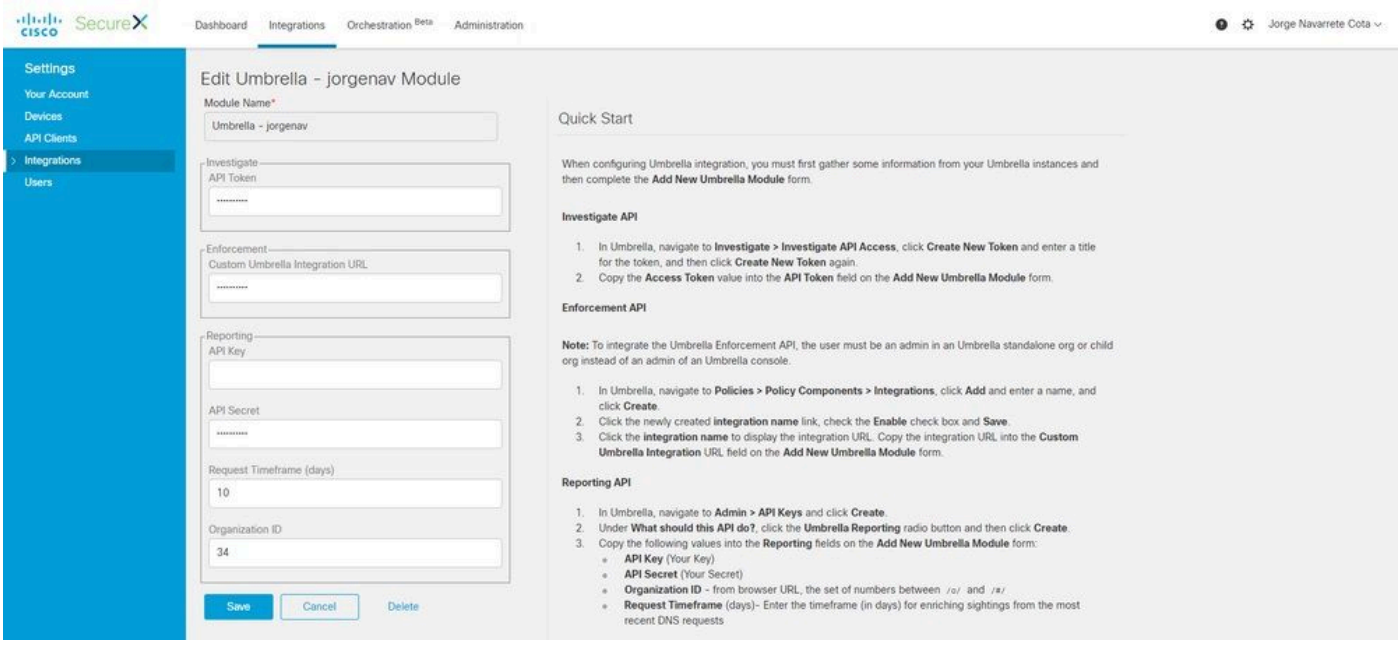
3. 다음 값을 Add New Umbrella Module(새 Umbrella 모듈 추가) 양식의 Reporting(보고) 필드에 복사합니다.

   - API 키(사용자 키)
   - API Secret(Your Secret)
   - 조직 ID - 브라우저 URL에서/o/및/#/
   - Request Timeframe(days)(요청 기간(일)) - 가장 최근의 DNS 요청을 보다 세부적으로 확인할 기간(일)을 입력합니다



모듈 저장

1. Umbrella 모듈에서 API 정보를 입력하고 Save(저장)를 클릭합니다.

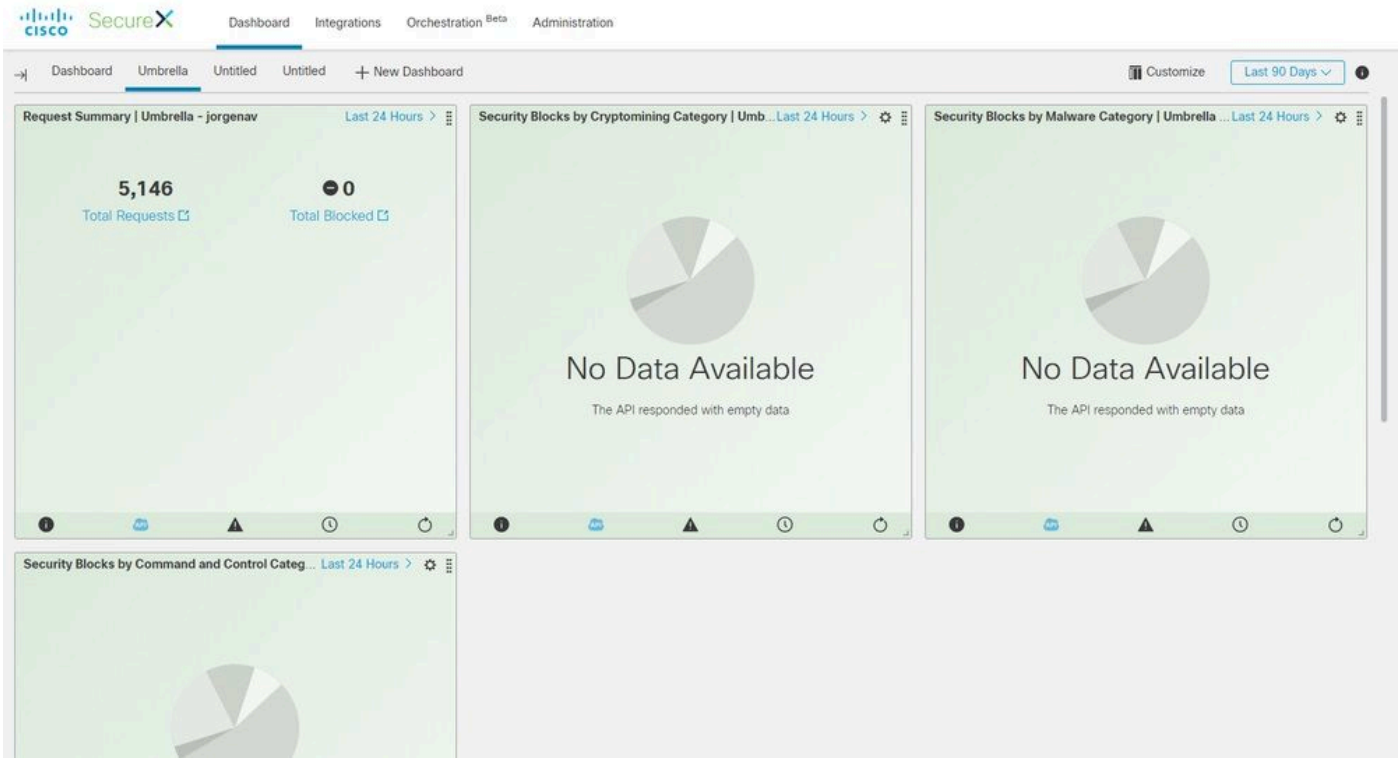


SecureX 대시보드 만들기

1. 모듈을 추가한 후에는 Secure X로 이동하여 새 대시보드를 생성할 수 있습니다.

2. 사용 가능한 대시보드에서 Umbrella 모듈을 선택하고 원하는 범주를 추가합니다.

3. 저장을 클릭하고 API를 통해 입력된 정보를 확인합니다.



다음을 확인합니다.

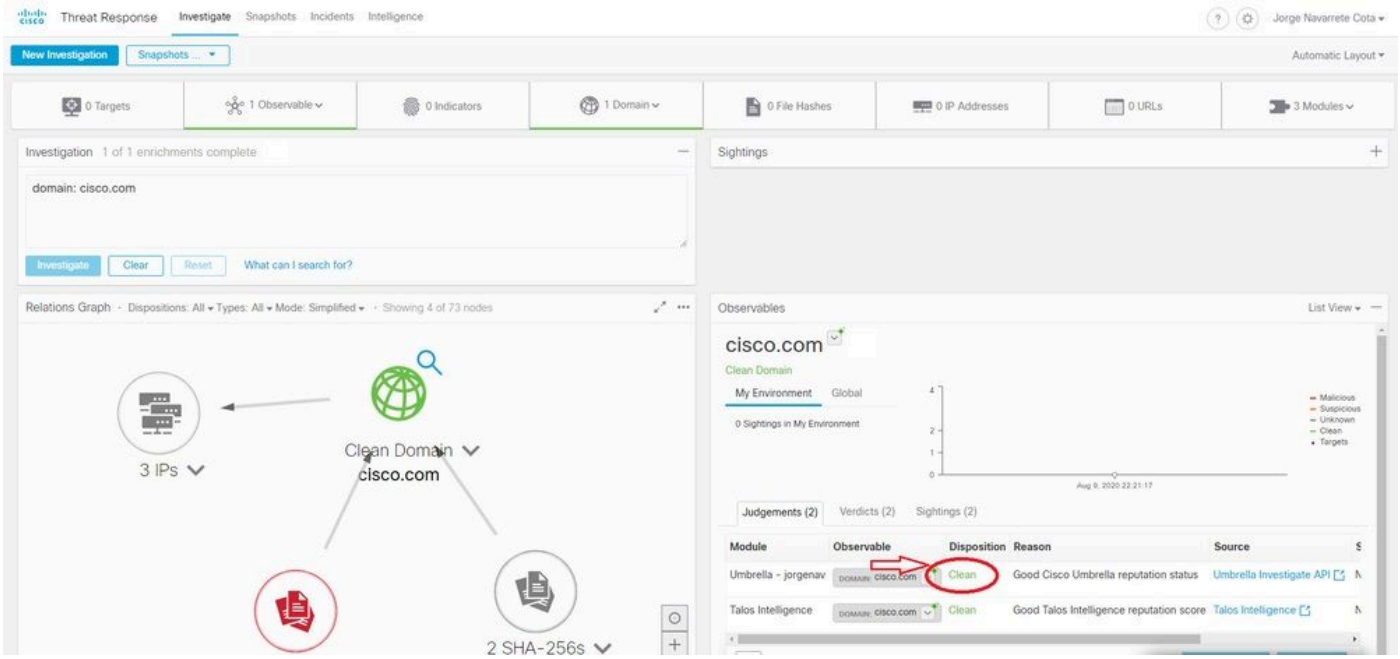
구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

조사

Investigate API에서는 CTR 조사에 피드를 추가하여 도메인의 처리를 보고 다른 모듈로 조사를 강화할 수 있습니다.

1. 이 통합을 확인하려면 Cisco Threat Response에서 새로운 조사를 수행하십시오. Umbrella에서 제공하는 Disposition은 cisco.com과 같은 알려진 도메인을 검색하면 찾을 수 있습니다.

2. 관계식 그래프에서 도메인 아래를 클릭하면 Umbrella의 Investigate 대시보드로 이동할 수도 있습니다.

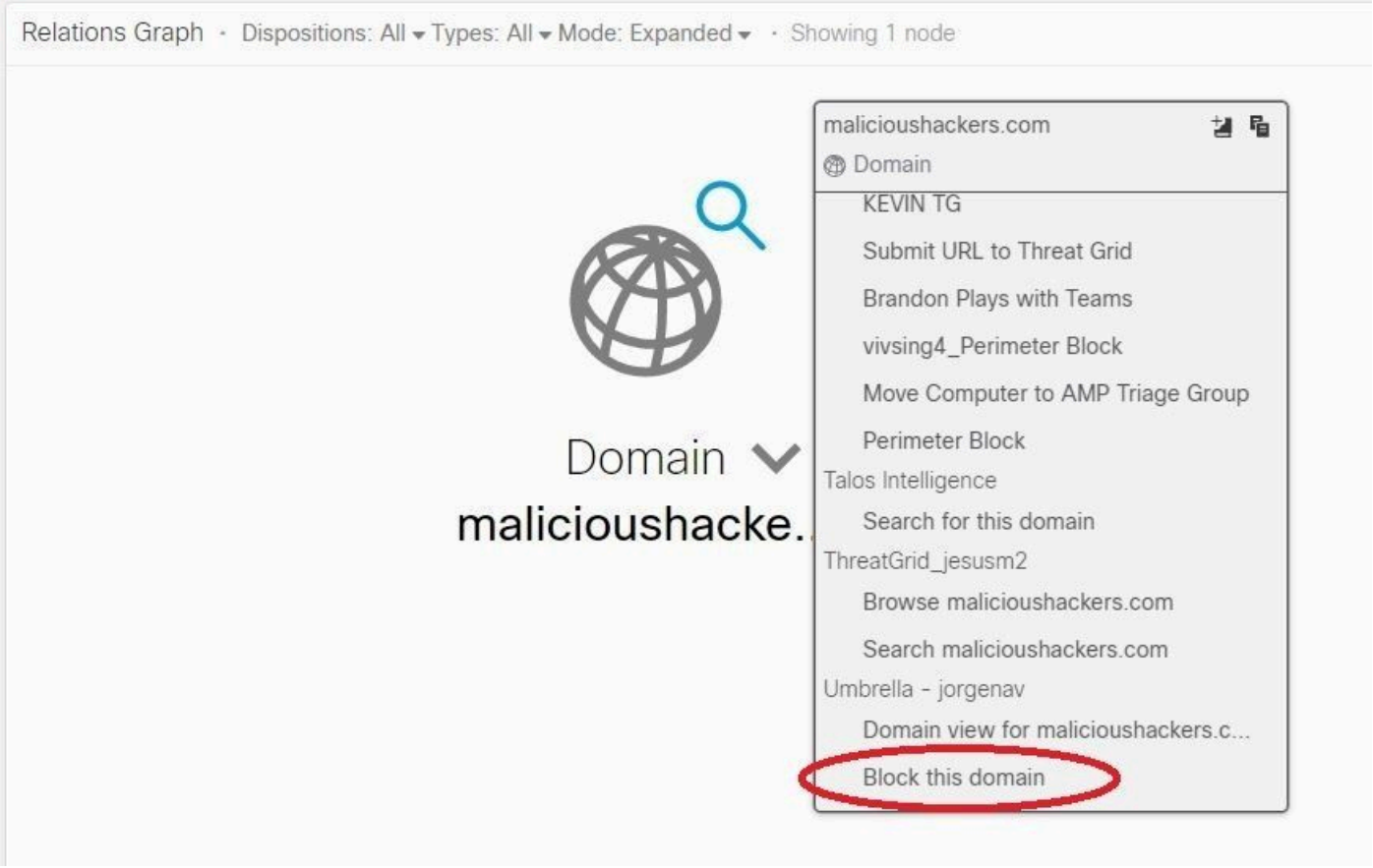


시행

Enforcement API를 사용하면 조사에서 도메인을 직접 차단하거나 차단을 해제할 수 있습니다.

1. API가 작동하는지 확인하기 위해 조사에서 표시된 도메인을 차단하고 Umbrella의 정책 차단 목록에 도메인을 추가할 수 있습니다.

2. URL이 차단 목록에 추가되었는지 확인하려면 Policies(정책) > Policy Components(정책 구성 요소) > Integrations(통합)로 이동합니다. SecureX 통합을 선택하고 See Domains(도메인 보기)를 클릭합니다. CTR에서 추가된 도메인이 창에 표시됩니다.



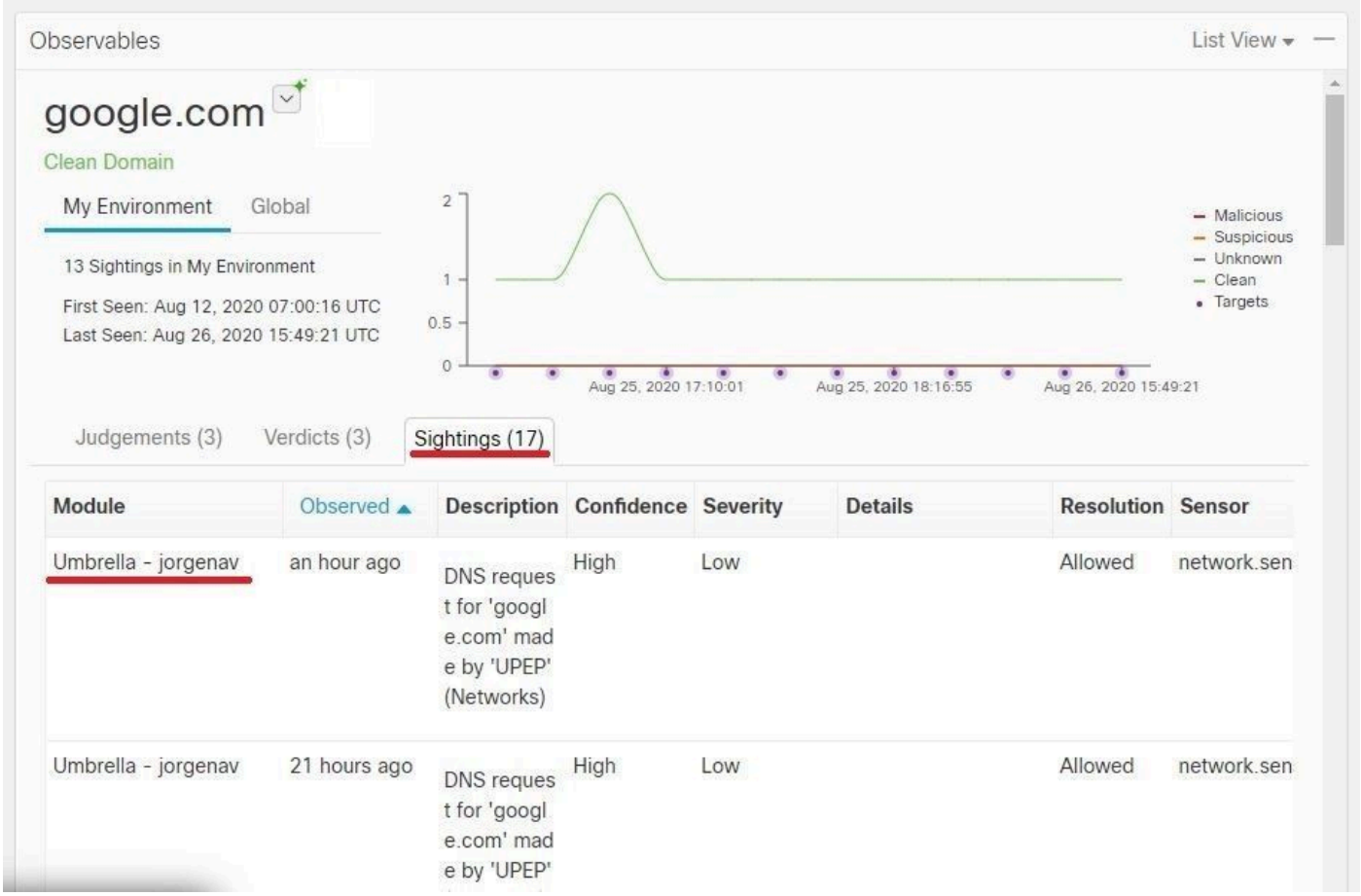
3. 도메인이 차단되지 않은 경우 Umbrella 대시보드에서 Policies(정책) > Policy Components(정책 구성 요소) > Security Settings(보안 설정)로 이동합니다. 통합에서 원하는 목록을 적용했는지 확인합니다.

보고

보고 API를 사용하면 SecureX 내에서 Umbrella 구축의 정보를 볼 수 있습니다.

CTR에서 사용자 환경에서 확인된 도메인의 조사와 통합을 확인할 수 있습니다.

CTR 조사에서 특정 도메인에 액세스한 컴퓨터의 목록이 Sightings 아래에 표시됩니다.



비디오

이 비디오에서 이 문서에 포함된 구성 정보를 찾을 수 있습니다.

관련 정보

- 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.