CTR 및 Threat Grid 클라우드 통합

목차

소개

이 문서에서는 CTR 조사를 수행하기 위해 Cisco CTR(Threat Response)과 TG(Threat Grid) 클라우드를 통합하는 단계에 대해 설명합니다.

기고자: Jesus Javier Martinez, Yeraldin Sanchez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 위협 대응
- 위협 그리드

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- CTR 콘솔(관리자 권한이 있는 사용자 계정)
- Threat Grid 콘솔(관리자 권한이 있는 사용자 계정)

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

배경 정보

Cisco Threat Grid는 사용자 환경에 영향을 주지 않고 의심스러운 파일 또는 웹 대상을 실행할 수 있는 지능적이고 자동화된 악성코드 분석 및 악성코드 위협 인텔리전스 플랫폼입니다.

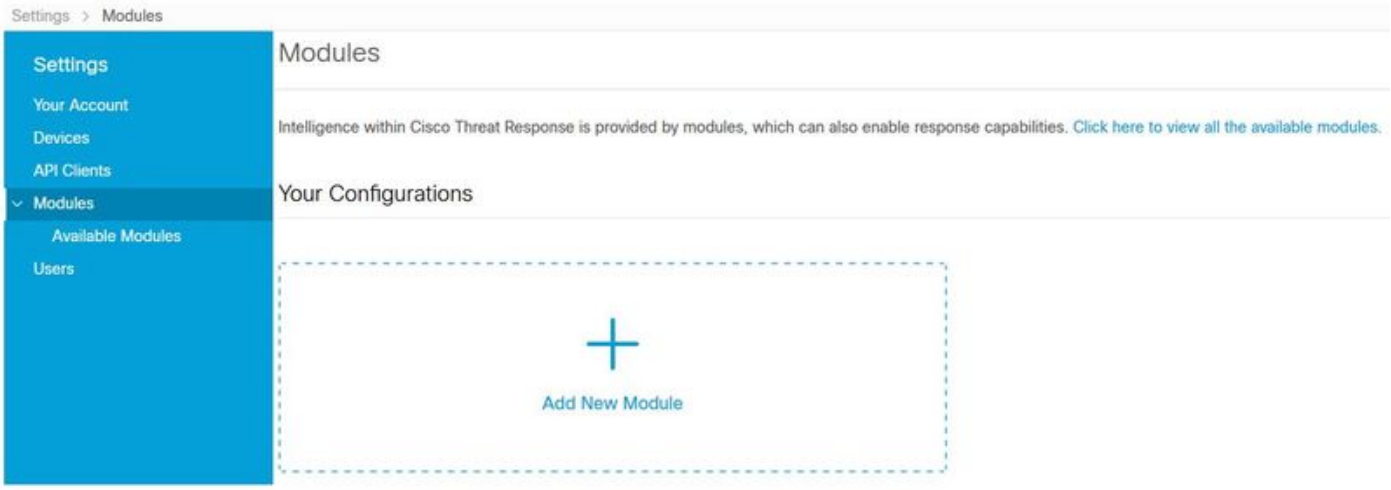
Cisco Threat Response와의 통합에서 Threat Grid는 참조 모듈이며 Threat Grid 포털로 피벗하여 Threat Grid 지식 저장소의 파일 해시, IP, 도메인 및 URL에 대한 추가 인텔리전스를 수집할 수 있는 기능을 제공합니다.

구성

CTR Console - Threat Grid Module 구성

1단계. 관리자 자격 증명을 사용하여 Cisco Threat Response에 로그인합니다.

2단계. Modules(모듈) 탭으로 이동하여 이미지에 표시된 대로 Modules(모듈) > Add New Module(새 모듈 추가)을 선택합니다.



3단계. Available Modules(사용 가능한 모듈) 페이지에서 이미지에 표시된 대로 Threat Grid 모듈 창에서 **Add New Module**(새 모듈 추가)을 선택합니다.

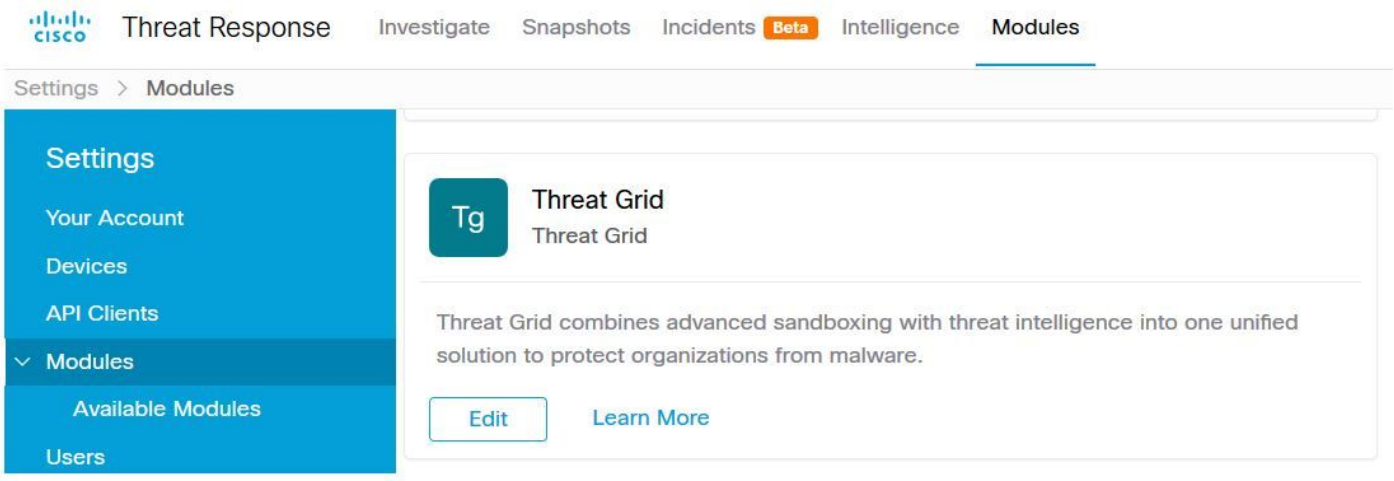
4단계. Add **New Module** 양식이 열립니다.이미지에 표시된 대로 양식을 작성합니다.

- **Module Name**(모듈 이름) - 기본 이름을 그대로 두거나 사용자에게 의미 있는 이름을 입력합니다.
- **URL** - 드롭다운 목록에서 Threat Grid 어카운트의 기반이 되는 위치(북미 또는 유럽)에 적합한 URL을 선택합니다. 지금은 **기타** 옵션을 무시합니다.

5단계. Save를 선택하여 Threat Grid 모듈 컨피그레이션을 완료합니다.

6단계. 이제 이미지에 표시된 대로 **Modules** 페이지의 컨피그레이션 아래 Threat Grid가 표시됩니다 .

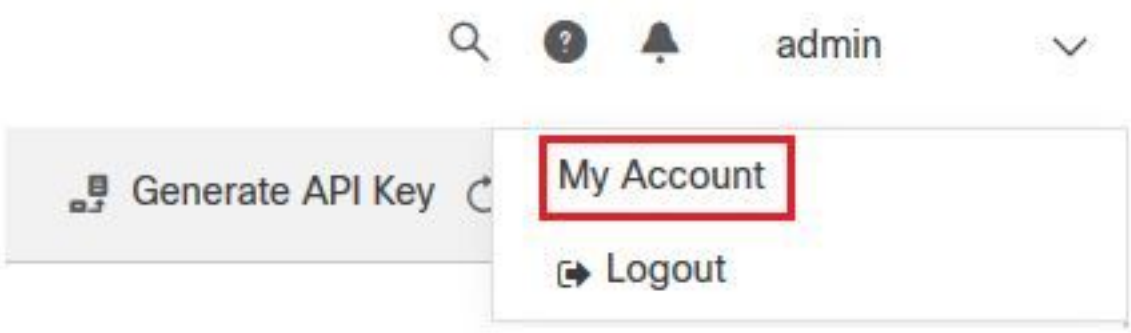
(TG는 위협 조사 개선을 위해 피벗 메뉴와 케이서에서도 사용할 수 있습니다.)



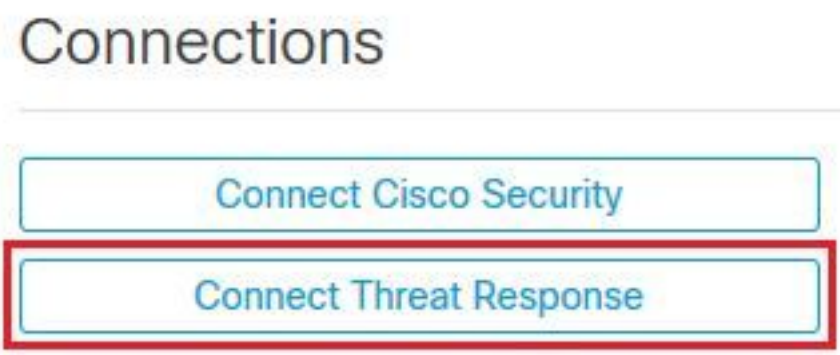
Threat Grid 콘솔 - Threat Grid에서 위협 응답에 액세스하도록 권한 부여

1단계. 관리자 자격 증명을 사용하여 Threat Grid에 로그인합니다.

2단계. 이미지에 표시된 **내 계정** 섹션으로 이동합니다.

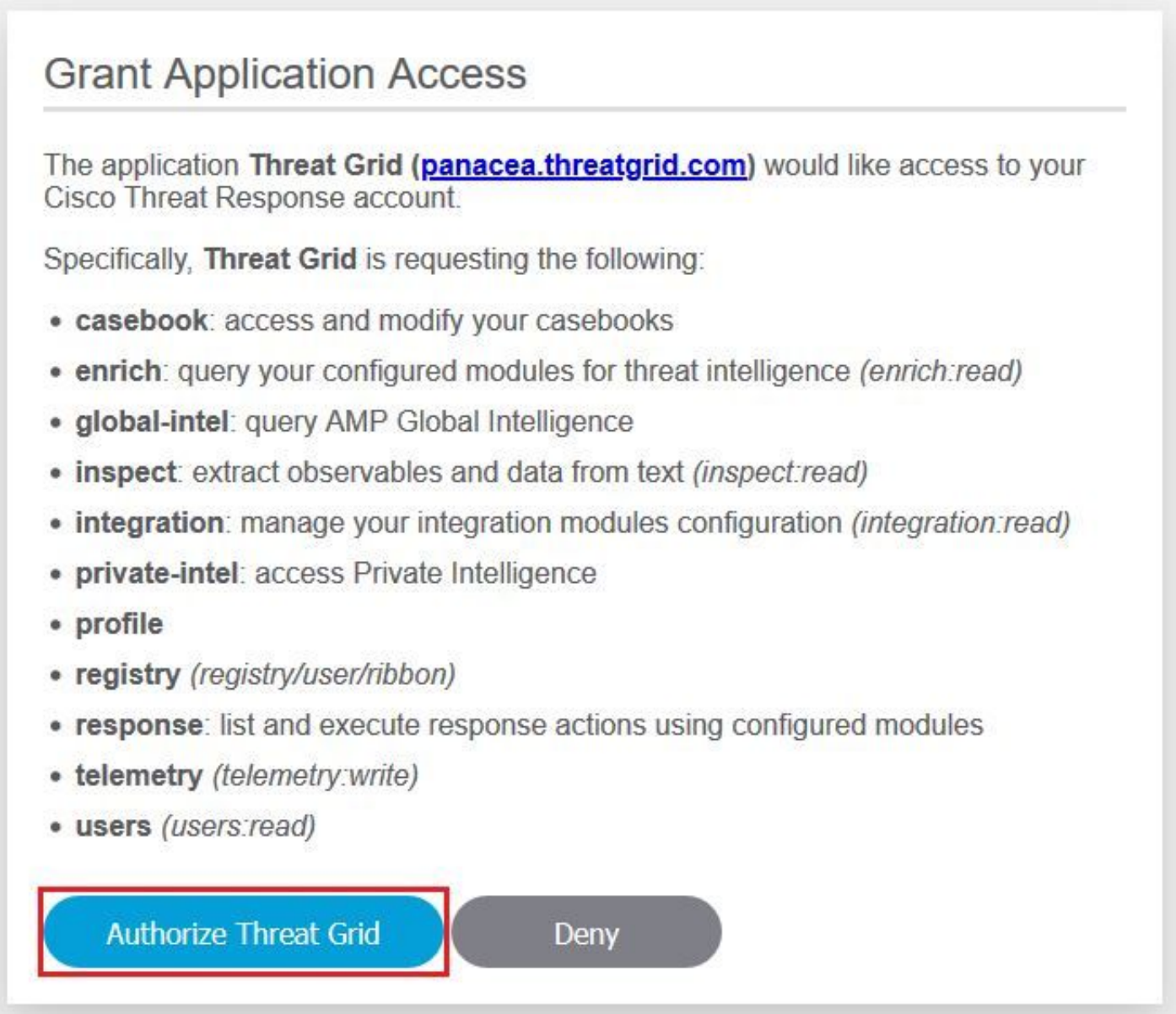


3단계. Connections 섹션으로 이동하고 이미지**에** 표시된 대로 Connect Threat Response 옵션을 선택합니다.

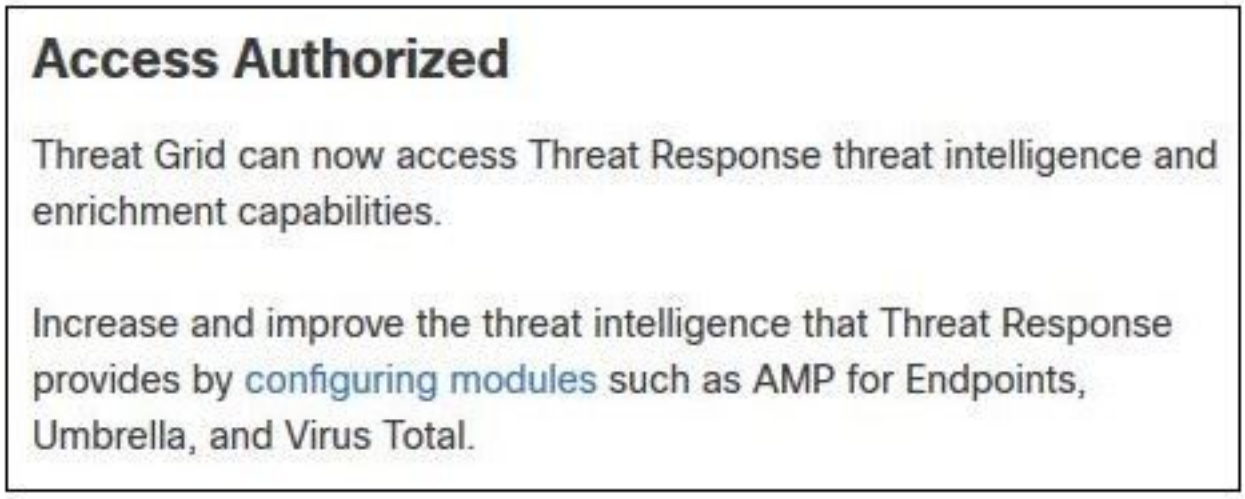


4단계. 이미지에 표시된 대로 Threat Grid가 Cisco Threat Response에 액세스하도록 허용하려면 Authorize(권한 부여) 옵션을 선택합니다.

5단계. 이미지에 표시된 대로 애플리케이션 액세스 권한을 부여하려면 Authorize **Threat** Grid 옵션을 선택합니다.



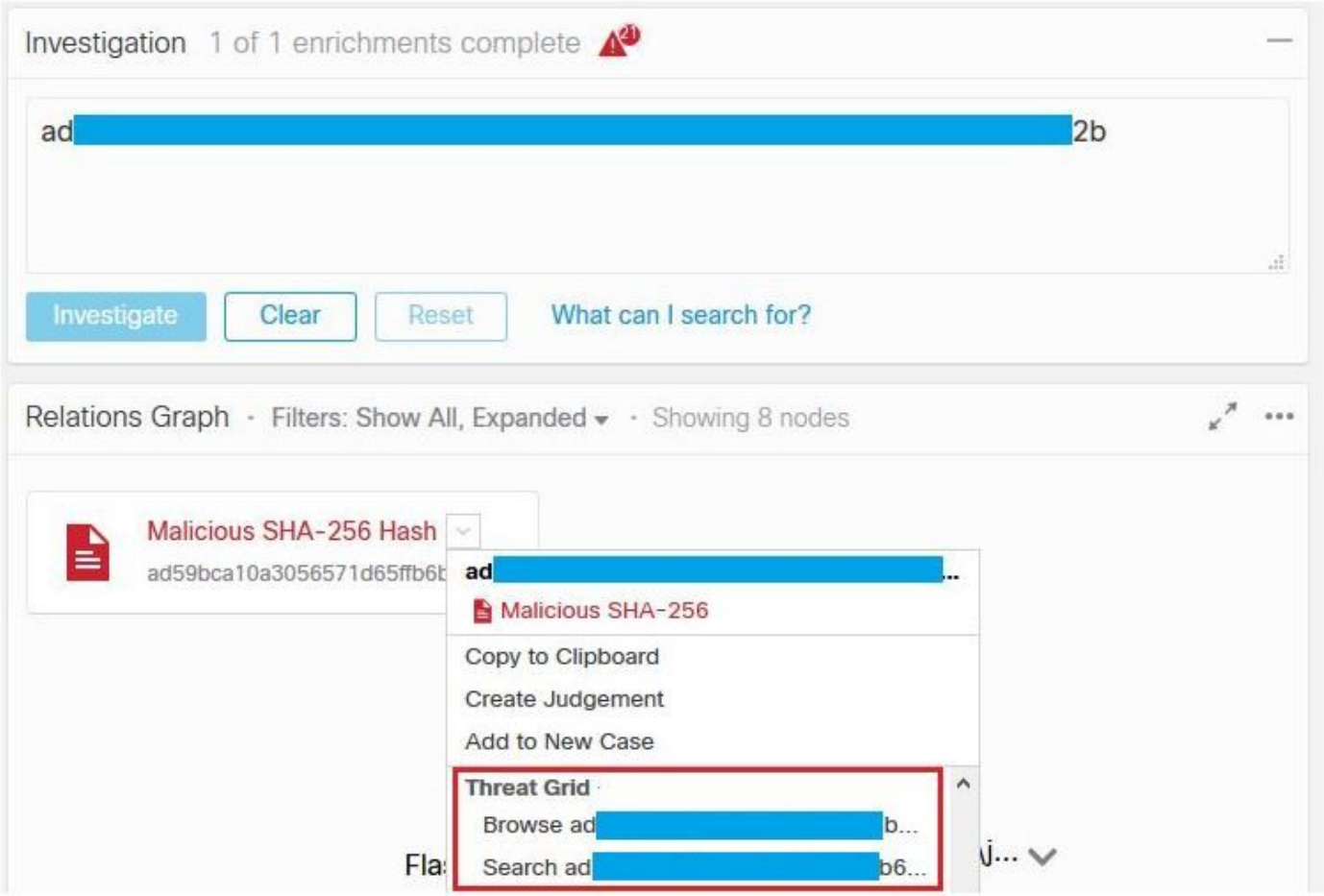
6단계. Access Authorized(액세스 권한 부여) 메시지가 나타나 Threat Grid가 이미지에 표시된 대로 Threat Response 위협 인텔리전스 및 보강 기능에 액세스할 수 있는지 확인합니다.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

CTR 및 TG 통합을 확인하기 위해 CTR 콘솔에서 **Investigate**를 수행할 수 있습니다. 모든 **Investigation** 세부 정보가 나타나면 이미지에 표시된 대로 Threat Grid 옵션을 볼 수 있습니다.



Browse(찾아보기) 또는 Search Threat Grid(위협 그리드 검색) 옵션을 선택하고 Threat Grid Portal로 리디렉션하여 이미지에 표시된 것처럼 Threat Grid 지식 저장소의 파일/해시/IPs/도메인/URL에 대한 추가 인텔리전스를 수집합니다.