ThreatQ를 Umbrella와 통합

목차

소개

이 문서에서는 ThreatQ를 Cisco Umbrella와 통합하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 통합을 위해 URL을 업데이트할 수 있는 액세스 권한이 있는 ThreatQ 대시보드
- Umbrella 대시보드 관리 권한
- Umbrella 대시보드에는 ThreatQ 통합이 활성화되어 있어야 합니다.

사용되는 구성 요소

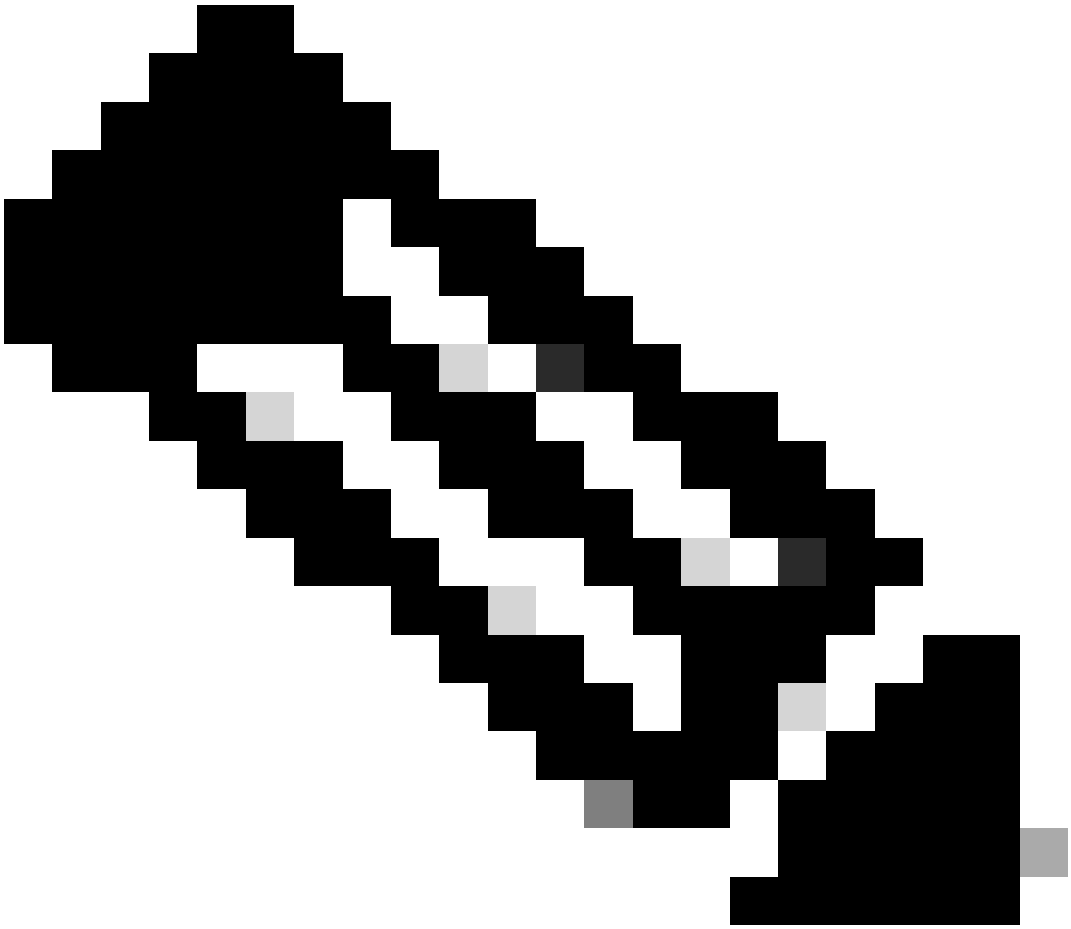
이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

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.

ThreatQ 및 Cisco Umbrella 통합 개요

ThreatQ를 Cisco Umbrella와 통합함으로써 보안 담당자 및 관리자는 로밍 중인 노트북, 태블릿 또는 전화에 대한 지능형 위협에 대한 보호 기능을 확장하는 동시에 분산된 기업 네트워크에 또 다른 계층의 적용을 제공할 수 있습니다.

이 설명서에서는 ThreatQ TIP의 보안 이벤트가 Cisco Umbrella에서 보호하는 클라이언트에 적용할 수 있는 정책에 통합될 수 있도록 ThreatQ가 Umbrella와 통신하도록 구성하는 방법을 설명합니다.



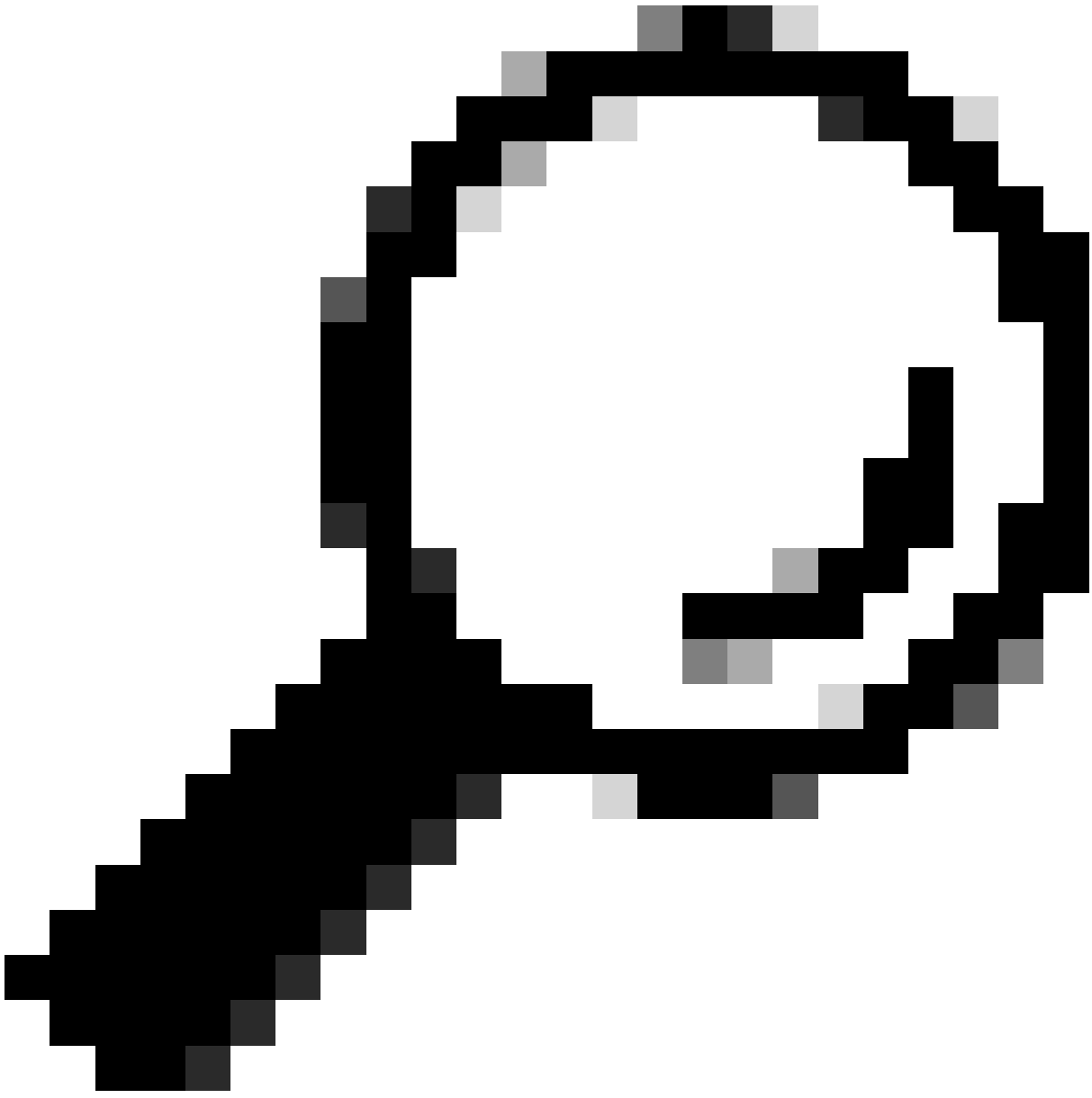
참고: ThreatQ 통합은 특정 Cisco Umbrella 패키지에만 포함됩니다. 필수 패키지가 없고 ThreatQ 통합을 원하는 경우 Cisco Umbrella 담당자에게 문의하십시오. 올바른 Cisco Umbrella 패키지를 가지고 있지만 대시보드의 통합으로 ThreatQ가 표시되지 않는 경우 Cisco Umbrella Support에 문의하십시오.

통합 기능

ThreatQ 플랫폼은 먼저 발견된 사이버 위협 인텔리전스(예: 봇넷 또는 피싱 사이트에 대한 악성코드, 명령 및 제어 호스팅 도메인)를 Umbrella로 전송합니다.

그런 다음 Umbrella가 위협을 검증하여 정책에 추가할 수 있는지 확인합니다. ThreatQ의 정보가 위협으로 확인되면 도메인 주소가 모든 Umbrella 정책에 적용할 수 있는 보안 설정의 일부로 ThreatQ 대상 목록에 추가됩니다. 이 정책은 ThreatQ Destination List의 정책을 사용하여 디바이스에서 생성되는 모든 요청에 즉시 적용됩니다.

앞으로 Umbrella는 ThreatQ 알림을 자동으로 구문 분석하고 악의적인 사이트를 ThreatQ Destination List에 추가합니다. 따라서 ThreatQ 보호 기능이 모든 원격 사용자 및 디바이스로 확대되고 회사 네트워크에 또 다른 시행 계층이 제공됩니다.



팁: Cisco Umbrella는 일반적으로 안전한 것으로 알려진 도메인(예: Google 및 Salesforce)을 검증하고 허용하여 원치 않는 중단을 방지하려고 최선을 다하고 있지만, 정책에 따라 Global Allow List(전역 허용 목록) 또는 다른 대상 목록에 차단하지 않으려는 도메인을 추가하는 것이 좋습니다. 예를 들면 다음과 같습니다.

- 조직의 홈 페이지
- 사용자가 제공하는 서비스를 나타내는 도메인으로서 내부 및 외부 레코드를 모두 포함할 수 있습니다. 예: "mail.myservicedomain.com" 및 "portal.myotherservicedomain.com"
- Cisco Umbrella에 의존하고 있는 잘 알려지지 않은 클라우드 기반 애플리케이션은 자동 도메인 검증에 포함되지 않습니다. 예: "localcloudservice.com".

이러한 도메인은 Cisco Umbrella의 Policies(정책) > Destination Lists(대상 목록)에 있는 Global Allow List(전역 허용 목록)에 추가할 수 있습니다.

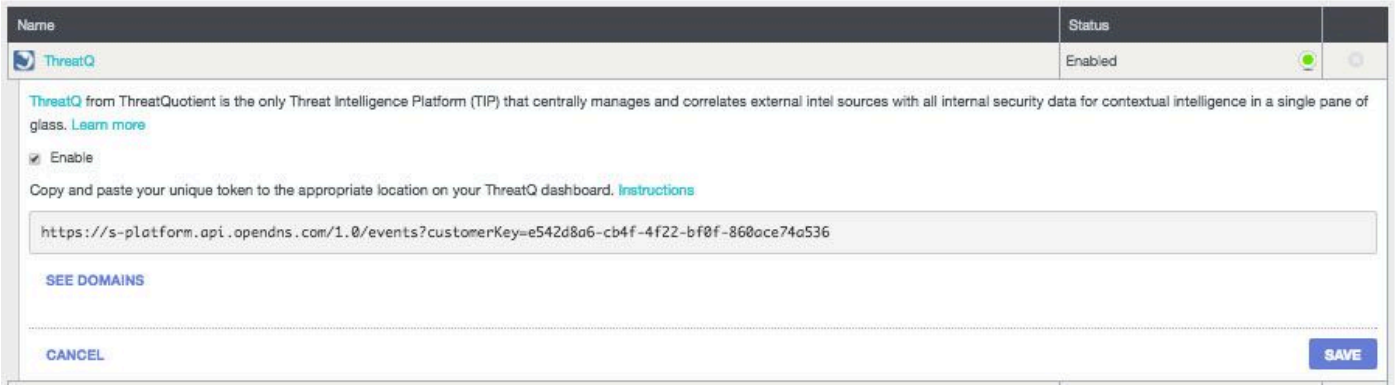
Umbrella 스크립트 및 API 토큰 생성

먼저 ThreatQ 어플라이언스가 통신할 수 있는 고유한 URL을 Umbrella에서 찾습니다.

1. Umbrella 대시보드에 로그인합니다.

2. Settings(설정) > Integrations(통합)로 이동하고 테이블에서 ThreatQ를 선택하여 확장합니다.

3. 사용을 선택한 다음 저장을 선택합니다. 이렇게 하면 Umbrella 내에서 조직에 대해 고유한 특정 URL이 생성됩니다.



나중에 ThreatQ를 구성하여 Umbrella로 데이터를 보낼 때 URL이 필요하므로 URL을 복사하고 ThreatQ 대시보드로 이동하십시오.

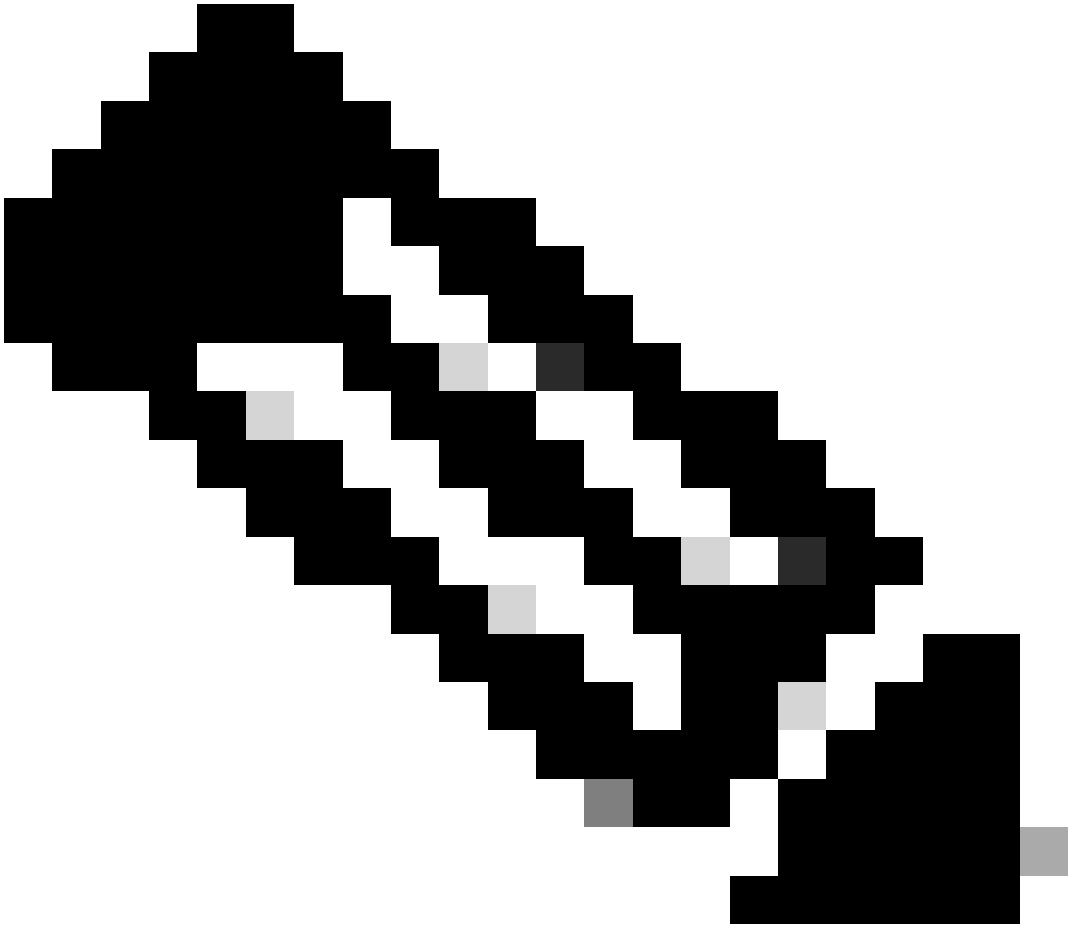
ThreatQ를 구성하여 Umbrella와 통신하는 방법

ThreatQ 대시보드에 로그인하고 적절한 영역에 URL을 추가하여 Umbrella에 연결합니다.

정확한 지침은 다양합니다. Umbrella는 ThreatQ 내에서 API 통합을 구성하는 방법이나 위치에 대해 잘 모르는 경우 ThreatQ 지원에 문의할 것을 권장합니다.

감사 모드에서 ThreatQ 보안 카테고리에 추가된 이벤트 관찰

시간이 지남에 따라 ThreatQ 대시보드의 이벤트는 ThreatQ 보안 카테고리로 정책에 적용할 수 있는 특정 대상 목록을 채우기 시작합니다. 기본적으로 대상 목록 및 보안 카테고리는 감사 모드에 있습니다. 즉, 이는 대상 목록이 어떤 정책에도 적용되지 않으며 기존 Umbrella 정책을 변경할 수 없음을 의미합니다.



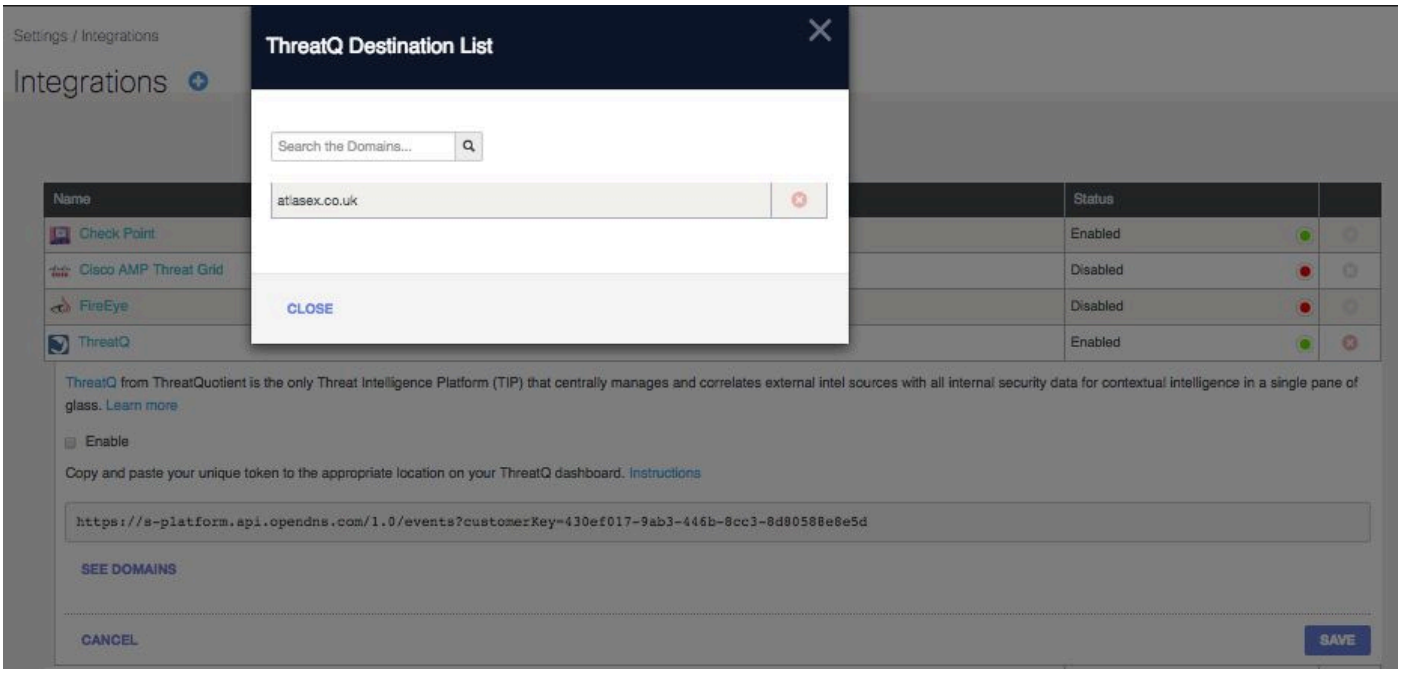
참고: 감사 모드는 활성화할 수 있지만 구축 프로파일 및 네트워크 컨피그레이션에 따라 시간이 오래 걸립니다.

대상 목록 검토

언제든지 Umbrella에서 ThreatQ 대상 목록을 검토할 수 있습니다.

1. 설정 > 통합으로 이동합니다.

2. 표에서 ThreatQ를 확장하고 See Domains(도메인 보기)를 선택합니다.



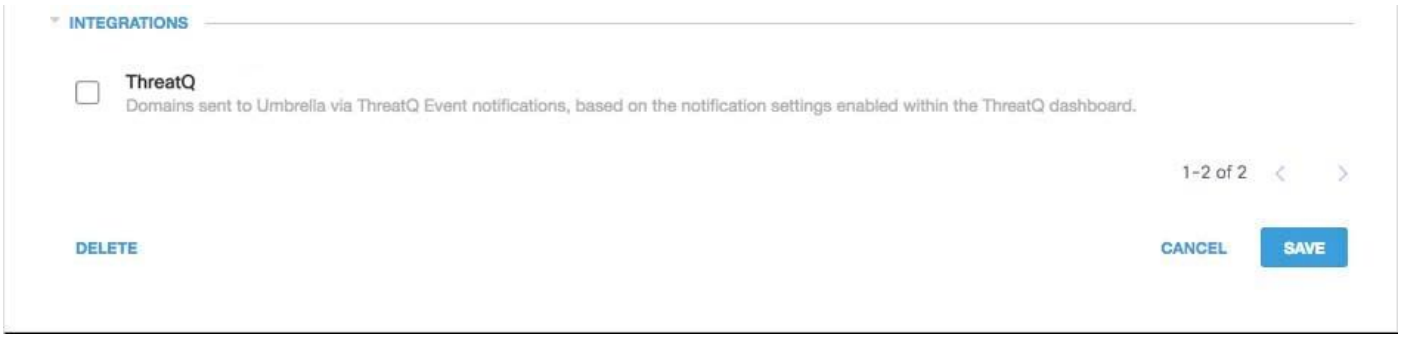
정책에 대한 보안 설정 검토

언제든지 Umbrella에서 정책에 대해 활성화할 수 있는 보안 설정을 검토할 수 있습니다.

1. Policies(정책) > Security Settings(보안 설정)로 이동합니다.

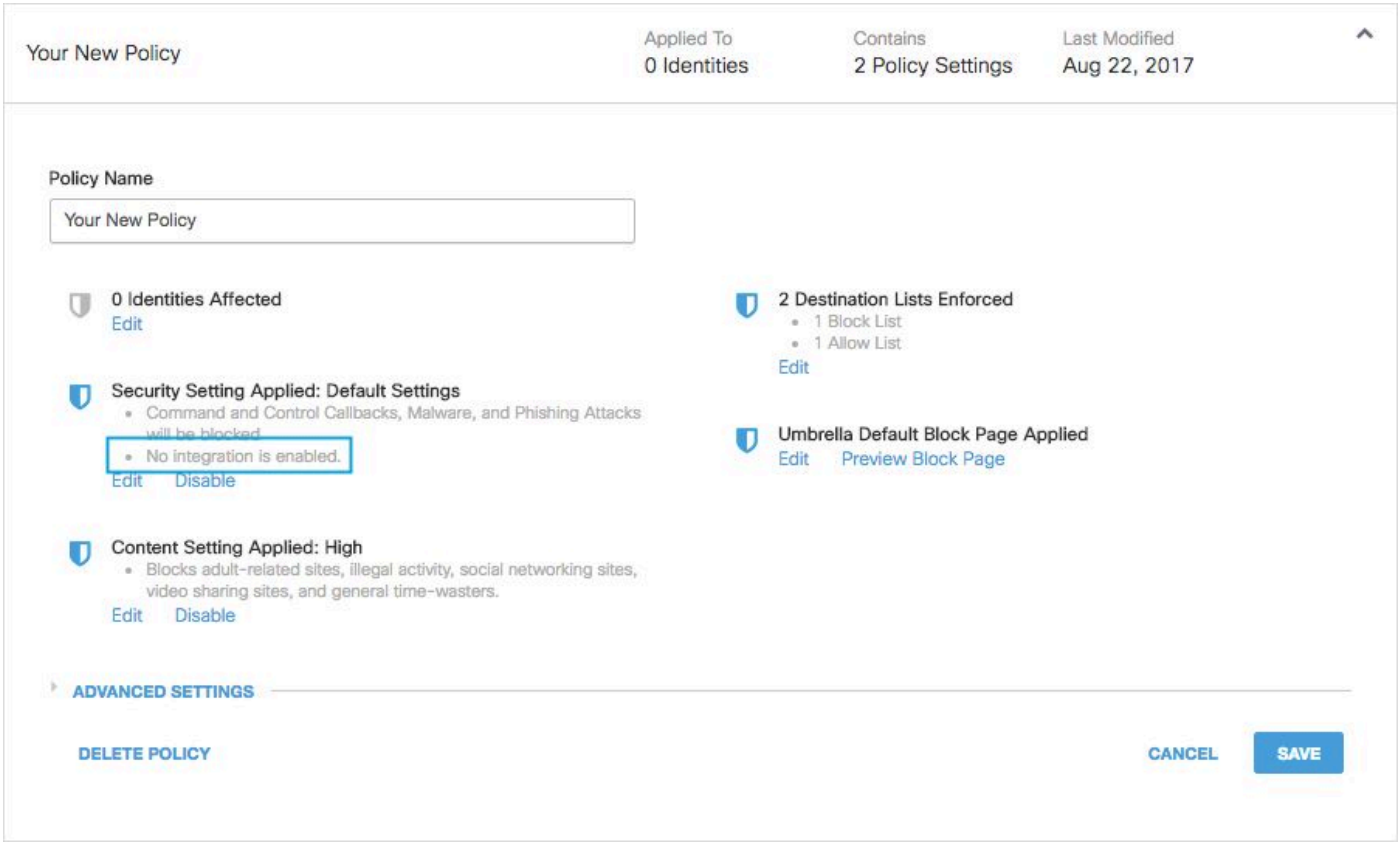
2. 테이블에서 보안 설정을 선택하여 확장합니다.

3. Integrations(통합)로 스크롤하여 ThreatQ 설정을 찾습니다.



115014040286

Security Settings Summary(보안 설정 요약) 페이지를 통해 통합 정보를 검토할 수도 있습니다.



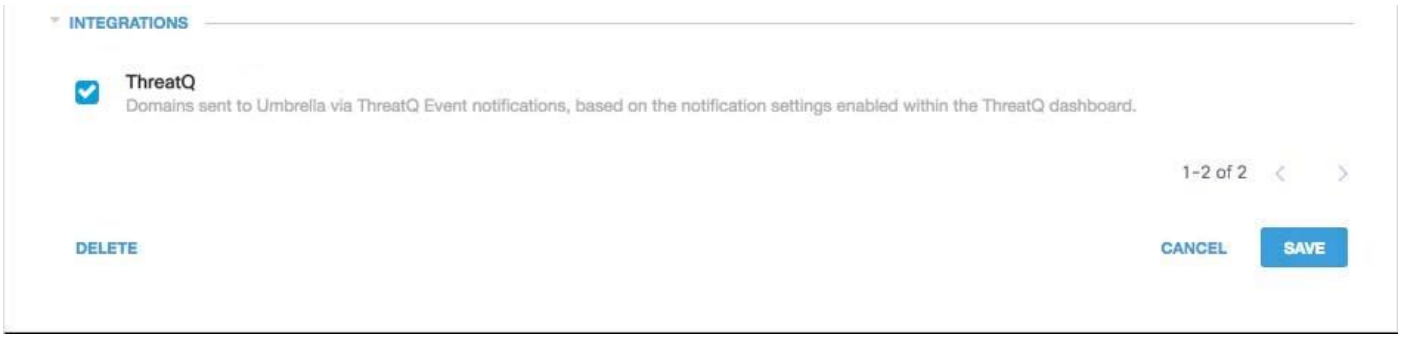
25464141748116

관리되는 클라이언트에 대한 정책에 블록 모드의 ThreatQ 보안 설정 적용

Umbrella에서 관리하는 클라이언트에 대해 이러한 추가 보안 위협을 적용할 준비가 되면 기존 정책의 보안 설정을 변경하거나 기본 정책보다 높은 위치에 있는 새 정책을 생성하여 먼저 적용되도록 할 수 있습니다.

1. Policies(정책) > Security Settings(보안 설정)로 이동합니다.

2. 통합에서 ThreatQ를 선택하고 저장을 선택합니다.



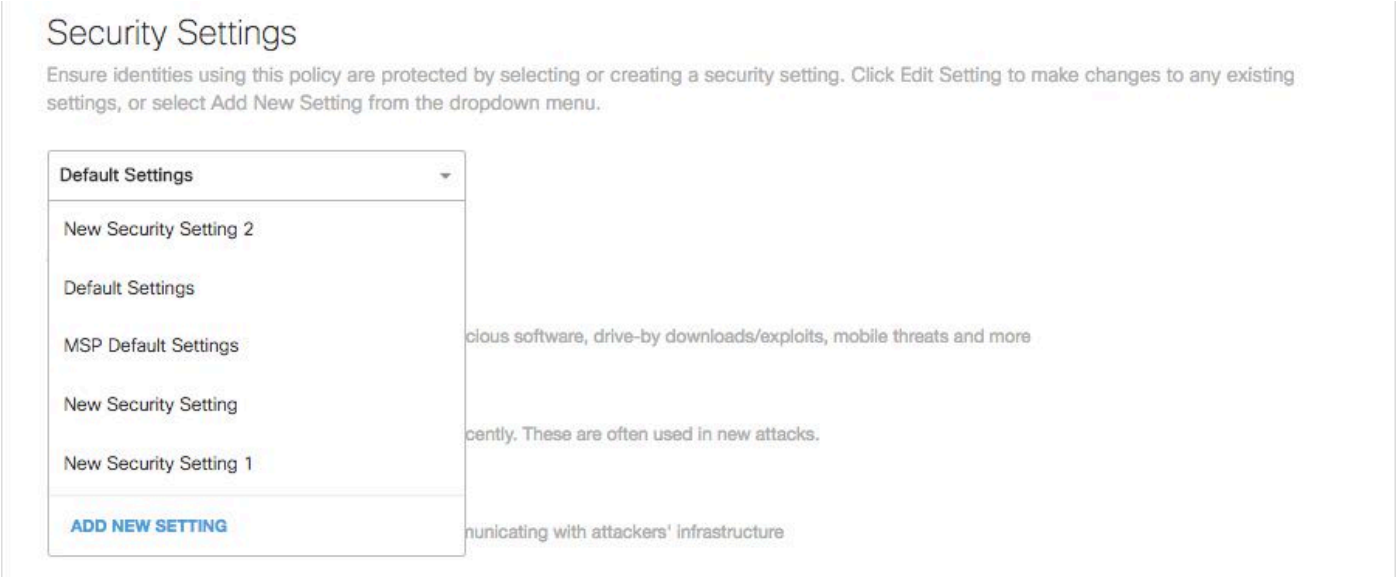
115014207403

다음으로, 정책 마법사에서 수정 중인 정책에 보안 설정을 추가합니다.

1. Policies(정책) > Policy List(정책 목록)로 이동합니다.

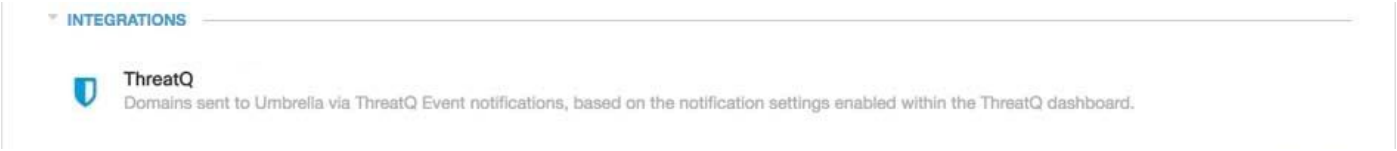
2. 정책을 확장하고 Security Setting Applied(보안 설정 적용됨)에서 Edit(편집)를 선택합니다.

3. Security Settings(보안 설정) 폴다운에서 ThreatQ 설정이 포함된 보안 설정을 선택합니다.



25464141787668

Integrations(통합) 아래의 실드 아이콘이 파란색으로 업데이트됩니다.



115014040506

4. 설정 및 반품을 선택합니다.

이제 ThreatQ의 보안 설정에 포함된 ThreatQ 도메인이 정책을 사용하는 ID에 대해 차단됩니다.

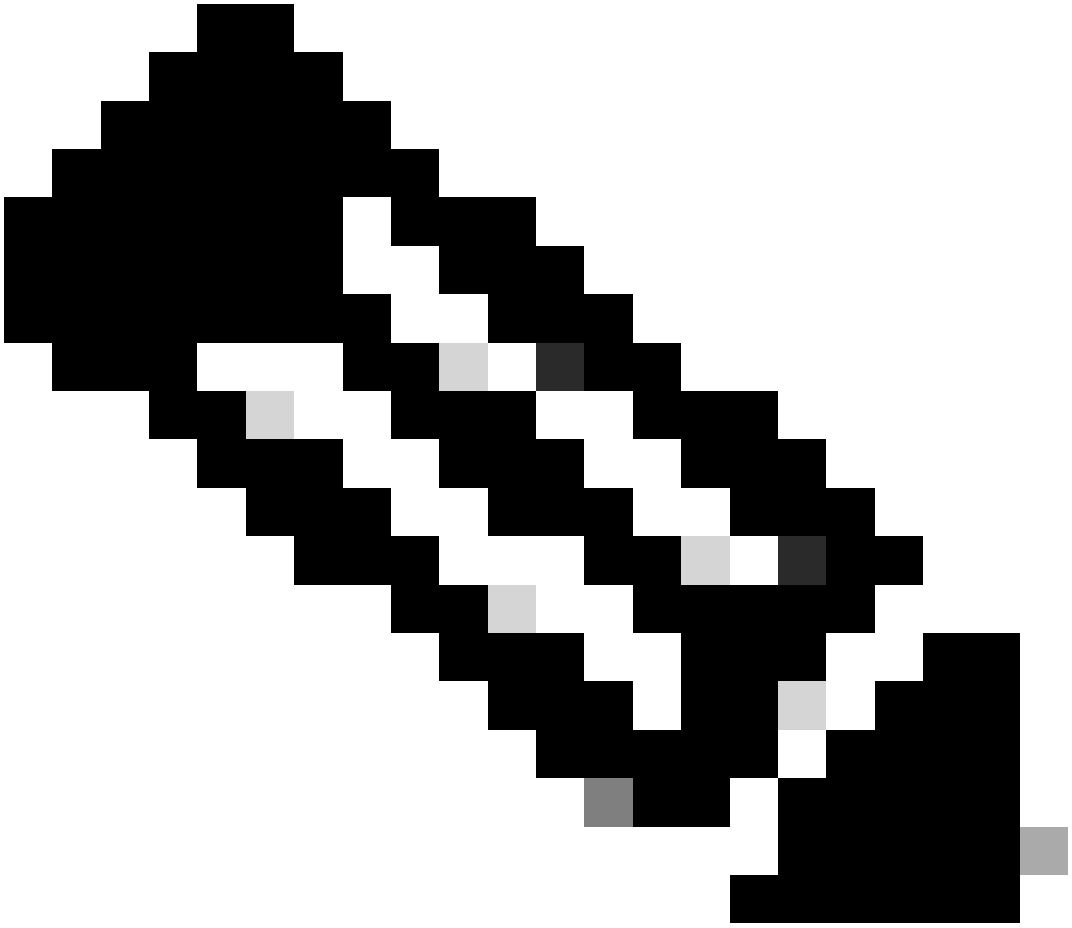
ThreatQ 이벤트에 대한 Umbrella의 보고

ThreatQ 보안 이벤트 보고

ThreatQ 대상 목록은 보고할 수 있는 보안 범주 목록 중 하나입니다. 보고서의 대부분 또는 모두가 보안 범주를 필터로 사용합니다. 예를 들어, 보안 범주를 필터링하여 ThreatQ 관련 활동만 표시할 수 있습니다.

1. 보고 > 활동 검색으로 이동합니다.

2. Security Categories(보안 카테고리)에서 ThreatQ를 선택하여 ThreatQ에 대한 보안 카테고리만 표시하도록 보고서를 필터링합니다.



참고: ThreatQ 통합이 비활성화된 경우 Security Categories(보안 카테고리) 필터에 표시되지 않습니다.

115014207603

3. 적용을 선택합니다.

도메인이 ThreatQ 대상 목록에 추가된 경우 보고

Umbrella Admin Audit(Umbrella 관리자 감사) 로그에는 대상 목록에 도메인을 추가할 때 ThreatQ 대시보드의 이벤트가 포함됩니다. ThreatQ 로고가 브랜드인 "ThreatQ Account"라는 사용자는 이벤트를 생성합니다. 이러한 이벤트에는 추가된 도메인 및 추가된 시간이 포함됩니다. Umbrella Admin Audit Log(Umbrella 관리자 감사 로그)는 Reporting(보고) > Admin Audit Log(관리자 감사 로그)에서 확인할 수 있습니다.

ThreatQ 계정 사용자에 대한 필터를 적용하여 ThreatQ 변경 내용만 포함하도록 필터링할 수 있습니다.

원치 않는 탐지 또는 오탐 처리

허용 목록

ThreatQ에 의해 자동으로 추가된 도메인은 사용자가 특정 웹 사이트에 액세스하지 못하도록 하는 원치 않는 차단을 트리거할 수 있습니다. 이와 같은 경우 Umbrella에서는 허용 목록에 도메인을 추가할 것을 권장합니다. 이는 보안 설정을 포함하여 다른 모든 유형의 차단 목록보다 우선합니다.

이 접근 방식이 바람직한 이유는 두 가지입니다.

- 먼저, ThreatQ 대시보드에서 도메인을 제거한 후 다시 추가해야 하는 경우 허용 목록은 추가 문제를 일으키지 않도록 보호합니다.
- 둘째, 허용 목록에는 포렌식 또는 감사 보고서에 사용할 수 있는 문제가 있는 도메인의 기록 레코드가 표시됩니다.

기본적으로 모든 정책에 적용되는 전역 허용 목록이 있습니다. 전역 허용 목록에 도메인을 추가하면 모든 정책에서 도메인이 허용됩니다.

블록 모드의 ThreatQ 보안 설정이 관리되는 Umbrella ID의 하위 집합에만 적용되는 경우(예: 로밍 컴퓨터 및 모바일 장치에만 적용되는 경우) 이러한 ID 또는 정책에 대한 특정 허용 목록을 만들 수 있습니다.

허용 목록을 생성하려면

1. Policies(정책) > Destination Lists(대상 목록)로 이동하고 Add(추가) 아이콘을 선택합니다.

2. 허용을 선택하고 목록에 도메인을 추가합니다.

3. 저장을 선택합니다.

대상 목록이 저장되면 원치 않는 블록의 영향을 받은 클라이언트를 다루는 기존 정책에 추가할 수 있습니다.

ThreatQ 대상 목록에서 도메인 삭제

ThreatQ Destination List의 각 도메인 이름 옆에 삭제 아이콘이 있습니다. 도메인을 삭제하면 원치 않는 탐지가 발생할 경우 ThreatQ 대상 목록을 정리할 수 있습니다. 그러나 ThreatQ 대시보드에서 Cisco Umbrella로 도메인을 재전송하는 경우 삭제는 영구적이지 않습니다.

도메인을 삭제하려면

1. Settings(설정) > Integrations(통합)로 이동한 다음 ThreatQ를 선택하여 확장합니다.

2. 도메인 보기를 선택합니다.

3. 삭제할 도메인 이름을 검색합니다.

4. 삭제 아이콘을 선택합니다.

5. 마감을 선택합니다.

6. 저장을 선택합니다.

원치 않는 탐지 또는 오탐의 경우 Umbrella는 즉시 Umbrella에 허용 목록을 만든 다음 ThreatQ 대시보드 내에서 오탐을 제거할 것을 권장합니다. 나중에 ThreatQ 대상 목록에서 도메인을 제거할 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.