ZeroFOX를 Umbrella와 통합

목차

소개

ZeroFOX Enterprise 및 Cisco Umbrella 통합 개요

Cisco Umbrella 및 ZeroFox 통합: 어떻게 진행됩니까?

- 사전 요구 사항
- 1단계: Umbrella 스크립트 및 API 토큰 생성
- 2단계: ZeroFOX Enterprise Dashboard를 설정하여 Umbrella에 정보 보내기
- 3단계: Umbrella 내에서 차단될 ZeroFOX 이벤트 설정

감사 모드에서 ZeroFOX 보안 범주에 추가된 이벤트 관찰

- 대상 목록 검토
- 정책에 대한 보안 설정 검토

관리되는 클라이언트에 대한 정책에 블록 모드의 ZeroFOX 보안 설정 적용

ZeroFOX 이벤트에 대한 Umbrella에서 보고

- ZeroFOX 보안 이벤트 보고
- 도메인이 ZeroFOX 대상 목록에 추가된 경우 보고

원치 않는 탐지 또는 오탐 처리

- 원치 않는 탐지에 대한 허용 목록 관리
- ZeroFOX 대상 목록에서 도메인 삭제

소개

이 문서에서는 ZeroFOX Enterprise를 Umbrella와 통합하여 Umbrella로 보호되는 클라이언트에 보안 이벤트를 적용하는 방법에 대해 설명합니다.

ZeroFOX Enterprise 및 Cisco Umbrella 통합 개요

ZeroFOX Enterprise를 Cisco Umbrella와 통합하면 보안 담당자 및 관리자는 로밍 중인 노트북 컴퓨터, 태블릿 또는 전화에 대한 오늘날의 소셜 미디어 기반 위협에 대한 보호 기능을 확장하는 동시에 분산된 기업 네트워크에 또 다른 시행 계층을 제공할 수 있습니다.

Cisco Umbrella 및 ZeroFox 통합: 어떻게 진행됩니까?

ZeroFOX Enterprise는 표적 악성코드, 피싱, 소셜 엔지니어링, 사칭, 기타 사기 또는 악의적인 활동 등 소셜 미디어 기반 사이버 위협과 같이 발견된 모든 위협을 글로벌 시행을 위해 Cisco Umbrella에 푸시합니다.

그런 다음 Umbrella가 위협을 검증하여 정책에 추가할 수 있는지 확인합니다. ZeroFOX의 정보가 위협으로 확인되면 Umbrella 정책에 적용할 수 있는 보안 설정의 일부로 도메인 주소가 ZeroFOX 대상 목록에 추가됩니다. 해당 정책은 해당 정책에 할당된 디바이스에서 생성되는 모든 요청에 즉

시 적용됩니다.

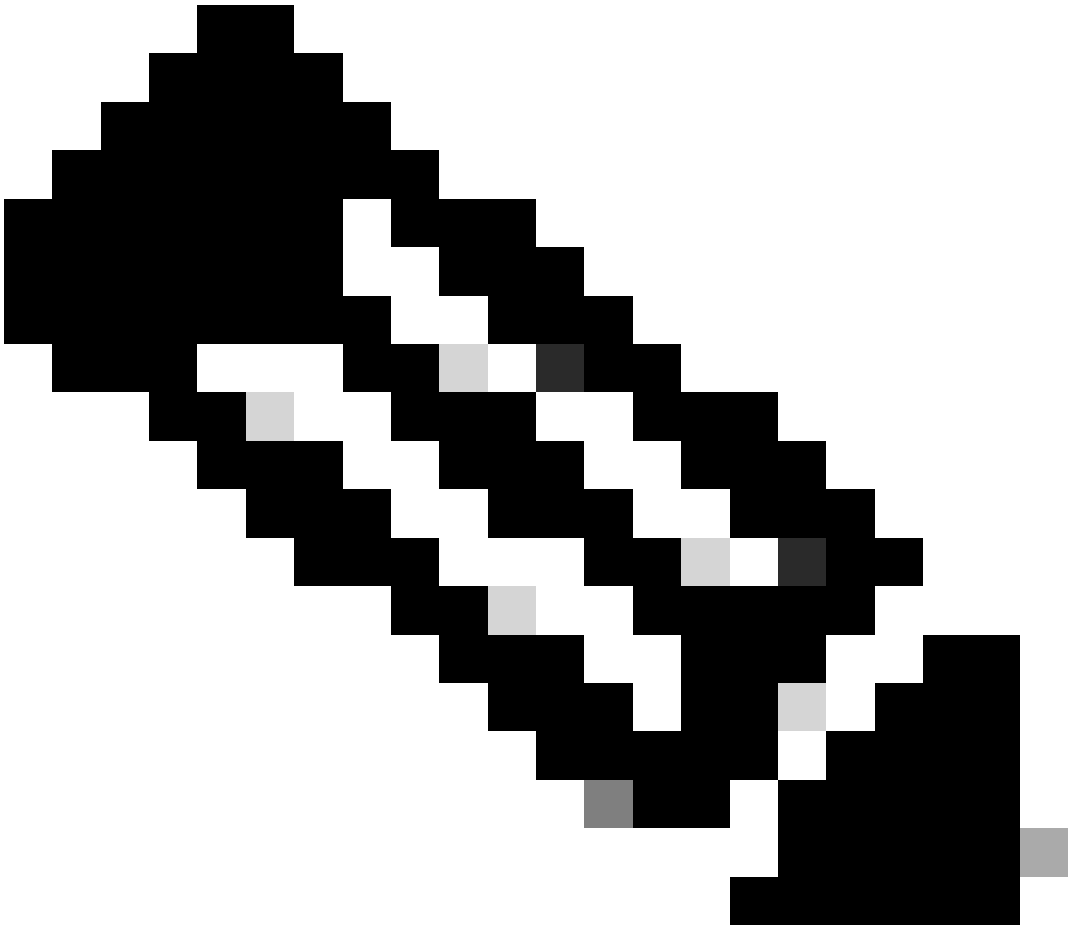
앞으로 Cisco Umbrella는 ZeroFOX 알림을 자동으로 구문 분석하고 악의적인 사이트를 ZeroFOX 대상 목록에 추가하여 모든 원격 사용자 및 장치에 ZeroFOX 인텔리전스를 확대하고 기업 네트워크에 또 다른 시행 계층을 제공합니다.

이는 다음과 같은 간단한 설정 단계를 통해 달성할 수 있습니다.

1. Umbrella에서 통합을 활성화하여 API 토큰을 생성합니다.
2. 해당 API 토큰을 ZeroFOX 계정에 붙여넣습니다.
3. 원하는 정책에 대한 보안 설정에서 ZeroFOX를 차단하도록 설정

사전 요구 사항

- ZeroFOX Enterprise 관리 권한
- Umbrella 대시보드 관리 권한
- Umbrella 대시보드에는 ZeroFOX 통합이 활성화되어 있어야 합니다



참고: ZeroFOX 통합은 Umbrella Platform 패키지에만 포함됩니다. 플랫폼 패키지가 없고 ZeroFOX 통합을 원하는 경우 Cisco Umbrella 담당자에게 문의하십시오. 플랫폼 패키지가 있지만 대시보드의 통합으로 ZeroFOX가 표시되지 않는 경우 Umbrella Support(우산 지원)에 문의하십시오.

중요: Umbrella는 일반적으로 안전한 것으로 알려진 도메인(예: Google 및 Salesforce)을 검증하고 허용하여 원치 않는 중단을 방지하려고 최선을 다하고 있지만, 정책에 따라 차단하지 않을 도메인을 전역 허용 목록 또는 다른 대상 목록에 추가하는 것이 좋습니다.

예를 들면 다음과 같습니다.

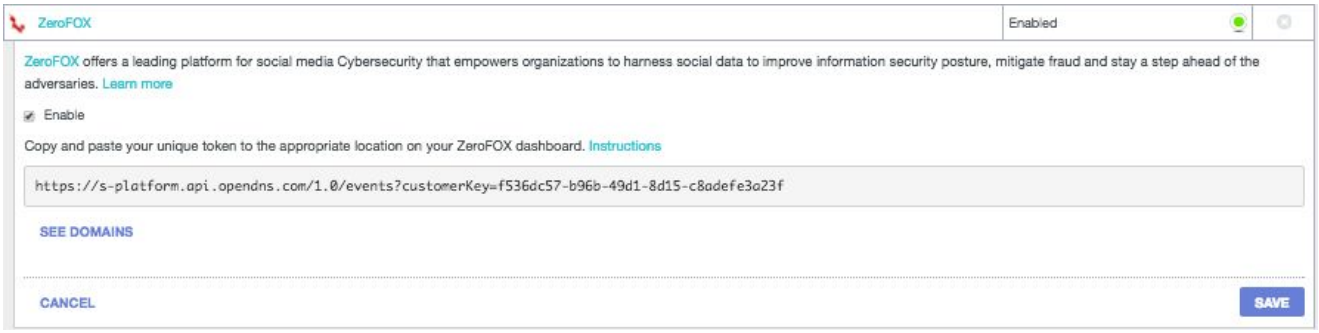
- 조직의 홈 페이지입니다. 예: mydomain.com.
- 사용자가 제공하는 서비스를 나타내는 도메인으로서 내부 및 외부 레코드를 모두 포함할 수 있습니다. 예: mail.myservicedomain.com 및 portal.myotherservicedomain.com.
- Umbrella가 자동 도메인 검증을 인식하지 못하거나 포함할 수 없는, 잘 알려지지 않은 클라우드 애플리케이션에 크게 의존하고 있습니다. 예: localcloudservice.com.

Global Allow List(전역 허용 목록)는 Policies(정책) > Destination Lists in Umbrella(Umbrella의 대상 목록)에 있습니다. 자세한 내용은 설명서를 참조하십시오. 대상 목록 관리

1단계: Umbrella 스크립트 및 API 토큰 생성

먼저 ThreatQ 어플라이언스가 통신할 수 있는 고유한 URL을 Umbrella에서 찾습니다.

1. Umbrella 대시보드에 관리자로 로그인하고 Settings(설정) > Integrations(통합)로 이동한 다음 테이블에서 "ZeroFOX"를 클릭하여 확장합니다.
2. Enable(활성화)을 선택한 다음 Save(저장)를 클릭합니다. 이렇게 하면 고객 키가 있는 고유한 URL이 생성됩니다.



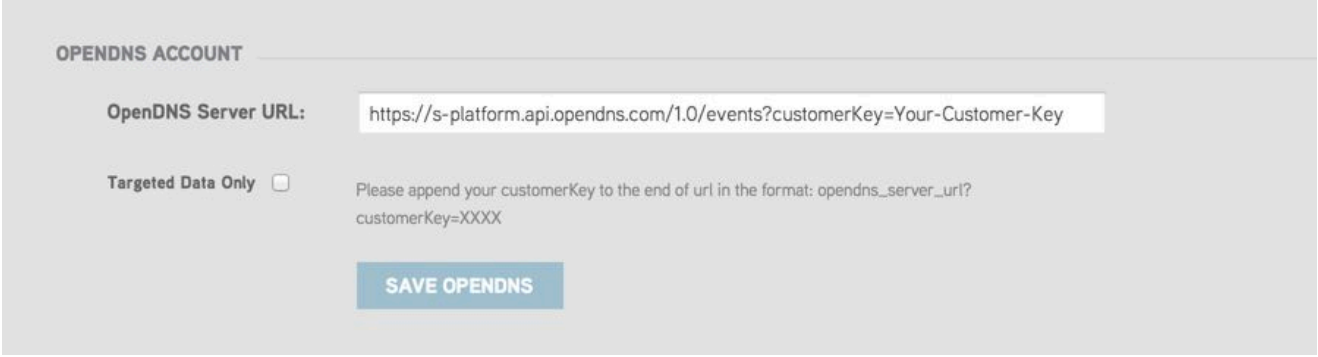
나중에 ZeroFOX를 구성할 때 URL이 필요하므로 URL을 복사하고 ThreatQ 대시보드로 이동하십시오.

2단계: ZeroFOX Enterprise Dashboard를 설정하여 Umbrella에 정보 보내기

다음 단계는 1단계에서 복사한 URL을 ZeroFOX 대시보드에 추가하는 것입니다.

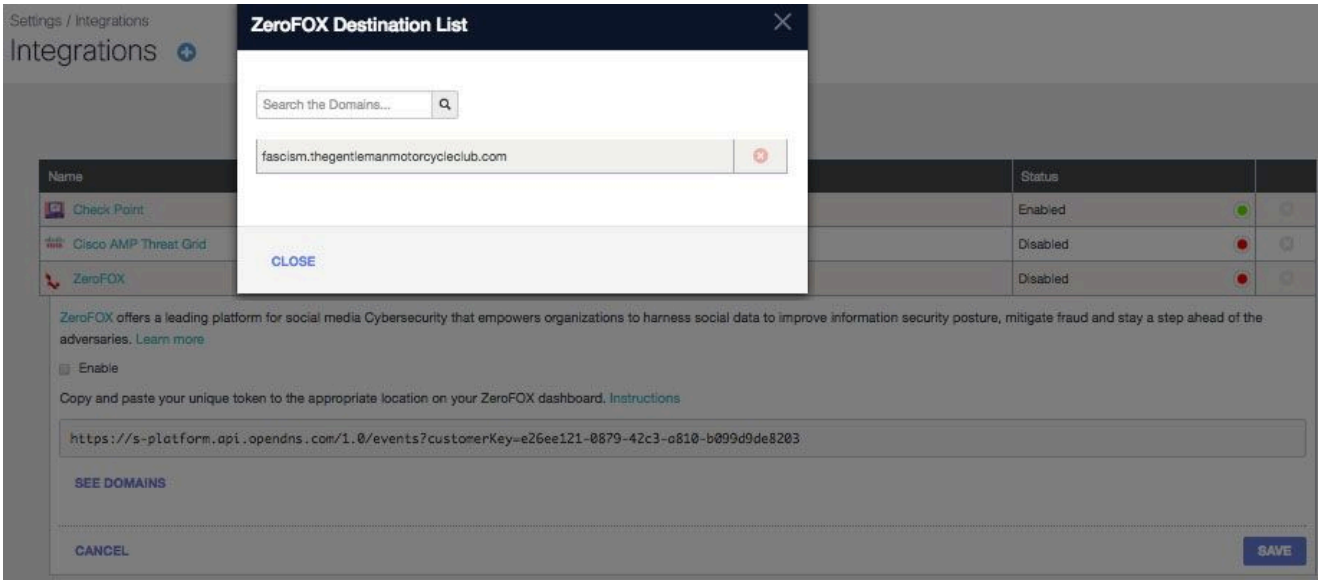
1. Zerofox 대시보드에서 톱니바퀴 아이콘을 클릭한 다음 Account Settings를 선택합니다.
2. OpenDNS Account(OpenDNS 어카운트) 정보가 표시될 때까지 통합 목록을 아래로 스크롤하

고 Umbrella의 URL을 OpenDNS Server URL(OpenDNS 서버 URL) 필드에 붙여넣습니다.
3. 통합을 처음 활성화한 후에는 Targeted Data Only(대상 데이터만)를 선택하는 것이 좋습니다.



3단계: Umbrella 내에서 차단될 ZeroFOX 이벤트 설정

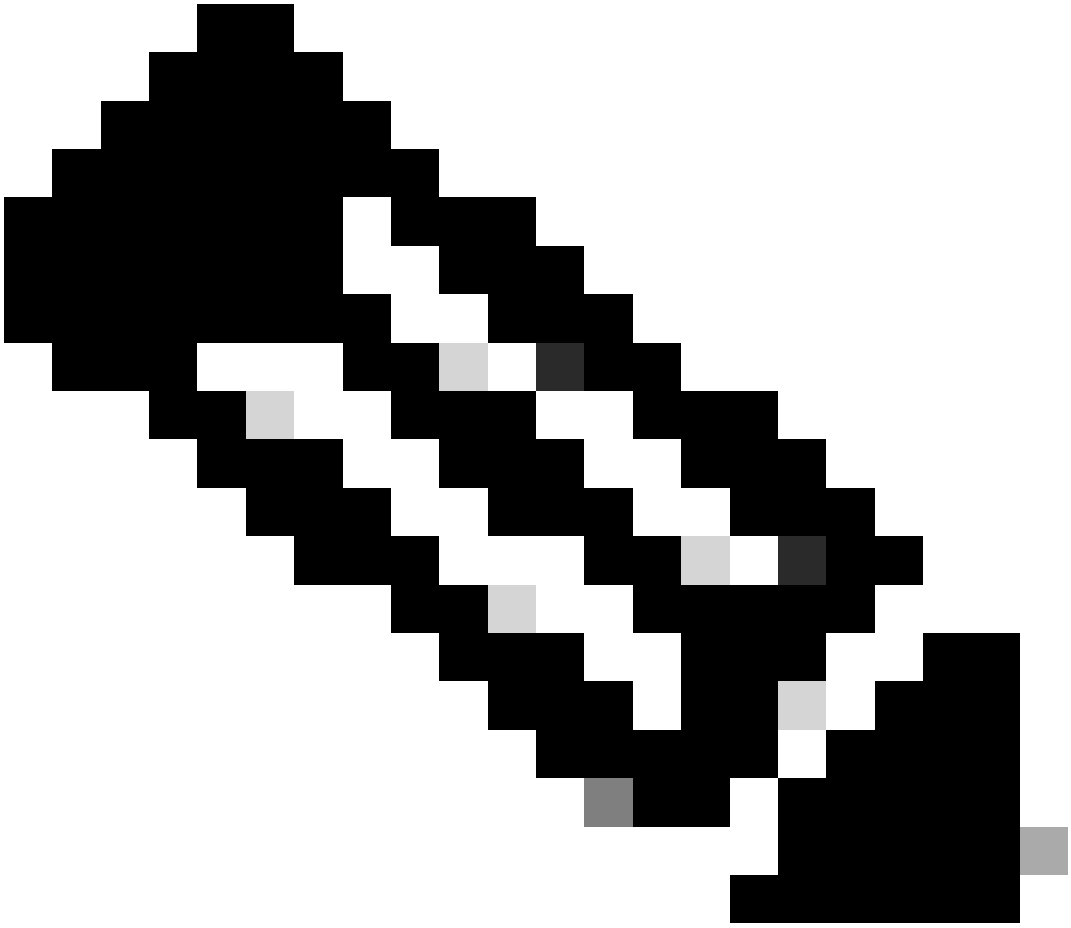
1. Umbrella 대시보드에 관리자로 다시 로그인합니다.
2. Settings(설정) > Integrations(통합)로 이동하고 테이블에서 "ZeroFOX"를 클릭하여 확장합니다.
3. See Domains(도메인 보기)를 클릭합니다.
   이렇게 하면 ZeroFOX 계정의 마지막 몇 시간 동안의 이벤트를 포함하는 도메인 목록이 확장됩니다. 그 시점부터 검색 가능한 목록이 채워지고 확장되기 시작합니다.



다음 단계는 새로운 ZeroFOX 보안 범주에 추가된 이벤트를 관찰하고 감사하는 것입니다.

감사 모드에서 ZeroFOX 보안 범주에 추가된 이벤트 관찰

ZeroFOX Enterprise의 이벤트는 정책에 ZeroFOX 보안 카테고리로 적용할 수 있는 특정 대상 목록을 채우기 시작합니다. 기본적으로 대상 목록 및 보안 카테고리는 감사 모드에 있으며 어떤 정책에도 적용되지 않으며 기존 Umbrella 정책이 변경되지 않습니다.



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

대상 목록 검토

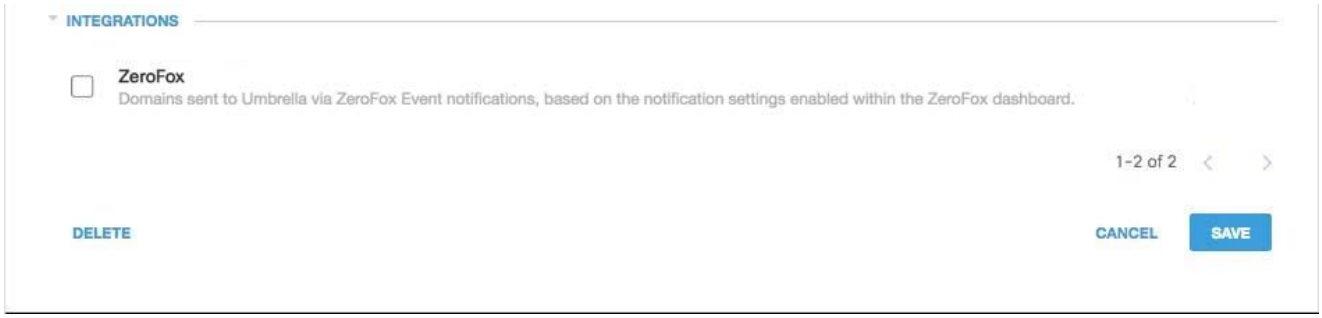
언제든지 ZeroFox 대상 목록을 검토할 수 있습니다.

1. Settings(설정) > Integrations(통합)로 이동합니다.
2. 테이블에서 "ZeroFOX"를 확장하고 See Domains(도메인 보기)를 클릭합니다.

정책에 대한 보안 설정 검토

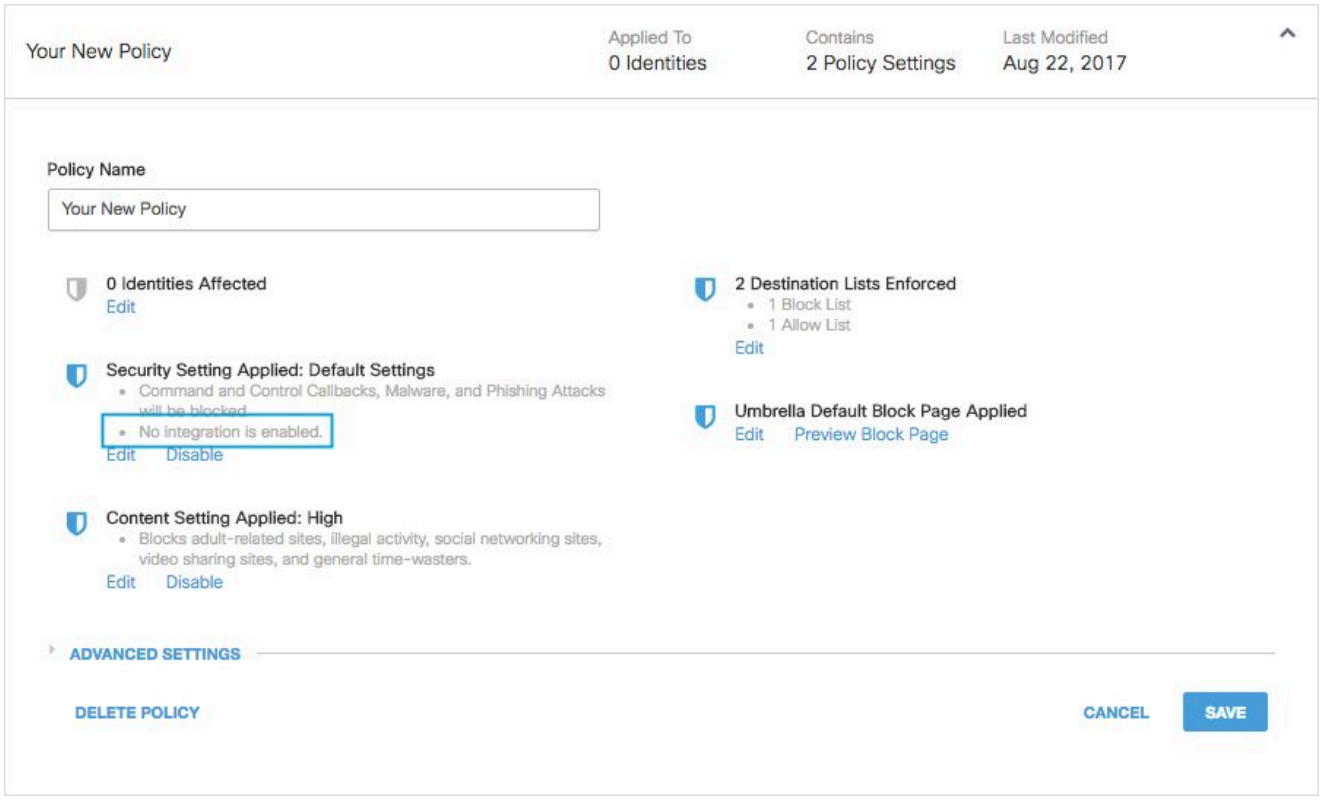
언제든지 정책에 대해 활성화할 수 있는 보안 설정을 검토할 수 있습니다.

1. Policies(정책) > Security Settings(보안 설정)로 이동합니다.
2. 테이블에서 보안 설정을 클릭하여 확장하고 Integrations(통합)로 스크롤하여 ZeroFOX 설정을 찾습니다.



115014041606

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

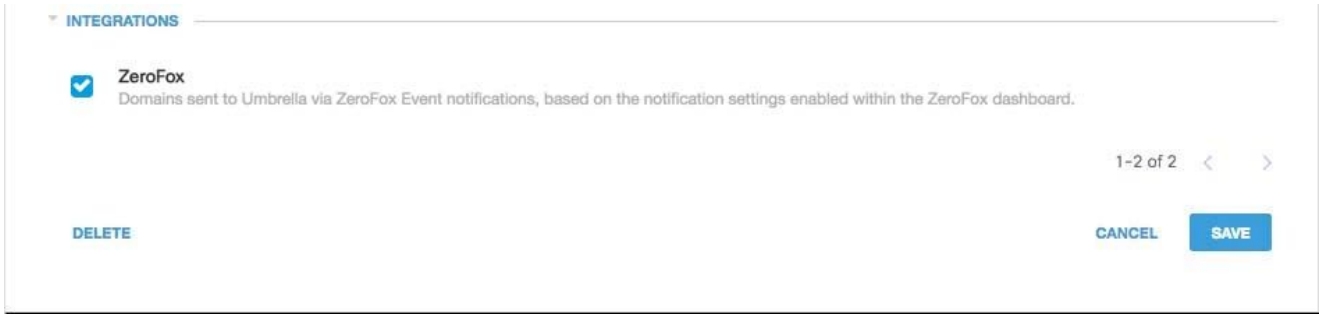


25464154913556

관리되는 클라이언트에 대한 정책에 블록 모드의 ZeroFOX 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 만들어 먼저 적용되도록 하면 됩니다.

1. Policies(정책) > Security Settings(보안 설정)로 이동하고 Integrations(통합)에서 ZeroFOX를 선택하고 Save(저장)를 클릭합니다.



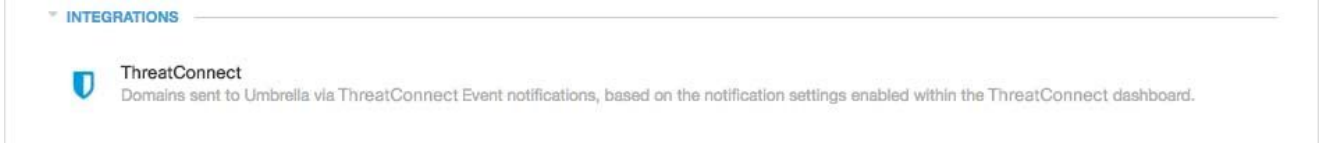
115014042806

그런 다음 정책 마법사에서 편집 중인 정책에 보안 설정을 추가합니다.

1. Policies(정책) > Policy List(정책 목록)로 이동합니다.
2. 정책을 확장하고 Security Setting Applied(보안 설정 적용됨) 아래에서 Edit(수정)를 클릭합니다.
3. Security Settings(보안 설정) 풀다운에서 ThreatConnect 설정이 포함된 보안 설정을 선택합니다.

25464147943700

Integrations(통합) 아래의 실드 아이콘이 파란색으로 업데이트됩니다.



25464147957652

4. Set & Return을 클릭합니다.

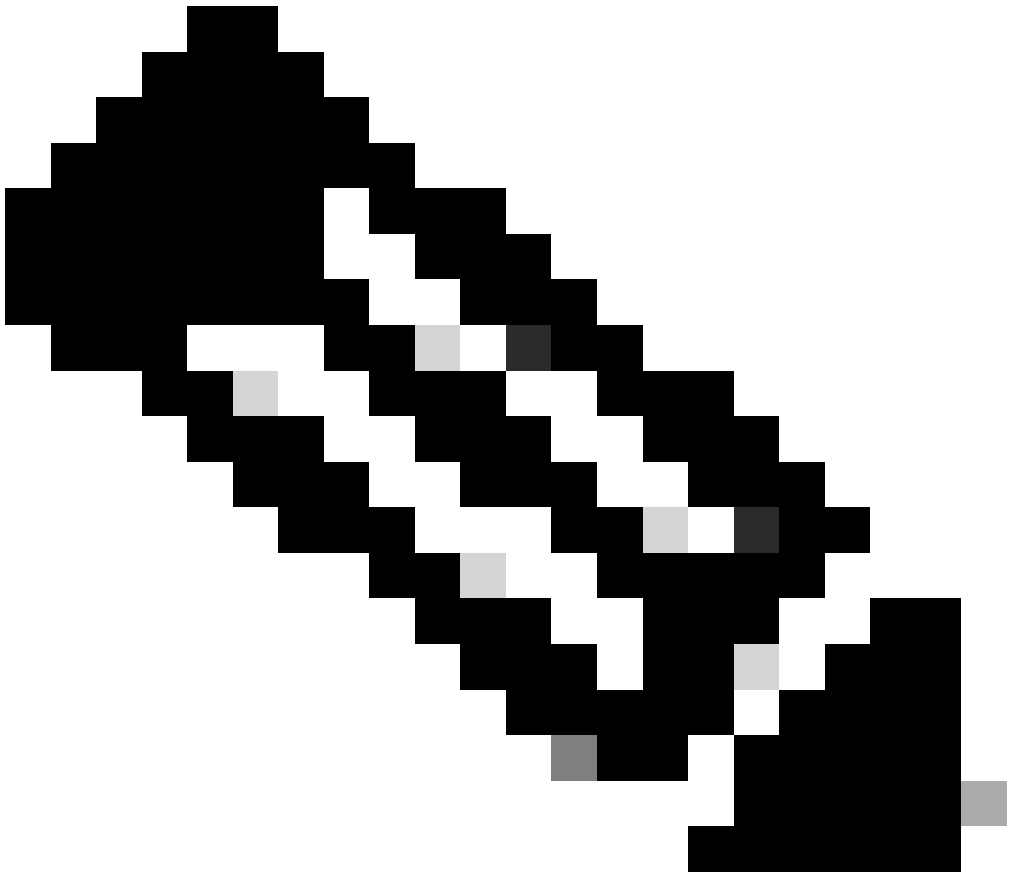
ZeroFOX에 대한 보안 설정에 포함된 ZeroFOX 도메인은 해당 정책을 사용하여 해당 ID에 대해 차단됩니다.

ZeroFOX 이벤트에 대한 Umbrella에서 보고

ZeroFOX 보안 이벤트 보고

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

1. Reporting(보고) > Activity Search(활동 검색)로 이동하고 Security Categories(보안 카테고리)에서 ZeroFOX를 선택하여 보고서를 필터링하면 ZeroFOX에 대한 보안 카테고리만 표시됩니다.



참고: ZeroFOX 통합이 비활성화되면 Security Categories(보안 카테고리) 필터에 나타나지 않습니다.

115014043046

2. 적용을 클릭합니다.

도메인이 ZeroFOX 대상 목록에 추가된 경우 보고

Umbrella Admin Audit(Umbrella 관리자 감사) 로그에는 ZeroFOX 계정에서 목적지 목록에 도메인을 추가할 때 발생하는 이벤트가 포함됩니다.

Umbrella Admin Audit Log(Umbrella 관리자 감사 로그)는 Reporting(보고) > Admin Audit Log(관리자 감사 로그)에서 확인할 수 있습니다. 도메인이 추가된 시기를 보고하려면 ZeroFox 대상 목록에 대한 ID 및 설정에 필터를 적용하여 ZeroFOX 변경 사항만 포함하도록 필터링합니다.

보고서를 실행하면 통합에서 ZeroFOX Destination List(ZeroFOX 대상 목록)가 추가되었을 때 변경된 내용이 표시됩니다.

원치 않는 탐지 또는 오탐 처리

원치 않는 탐지에 대한 허용 목록 관리

ZeroFOX에 의해 자동으로 추가된 도메인은 사용자가 특정 웹 사이트에 액세스하지 못하도록 하는 원치 않는 차단을 트리거할 수 있습니다. 이러한 상황에서는 허용 목록에 도메인을 추가하는 것이 좋습니다. 허용 목록은 보안 설정을 포함하여 다른 모든 유형의 차단 목록보다 우선합니다. 허용 목록은 둘 모두에 도메인이 있을 때 차단 목록보다 우선합니다.

이러한 접근 방식이 바람직한 이유는 두 가지가 있다. 먼저, ZeroFOX 어플라이언스가 제거된 후 도메인을 다시 추가해야 하는 경우 허용 목록에 따라 추가 문제가 발생합니다. 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 ZeroFOX 보안 설정이 관리되는 Umbrella ID의 하위 집합에만 적용되는 경우(예: 로밍 컴퓨터 및 모바일 장치에만 적용됨) 이러한 ID 또는 정책에 대한 특정 허용 목록을 만들 수 있습니다 .

허용 목록을 생성하려면

1. Policies(정책) > Destination Lists(대상 목록)로 이동하고

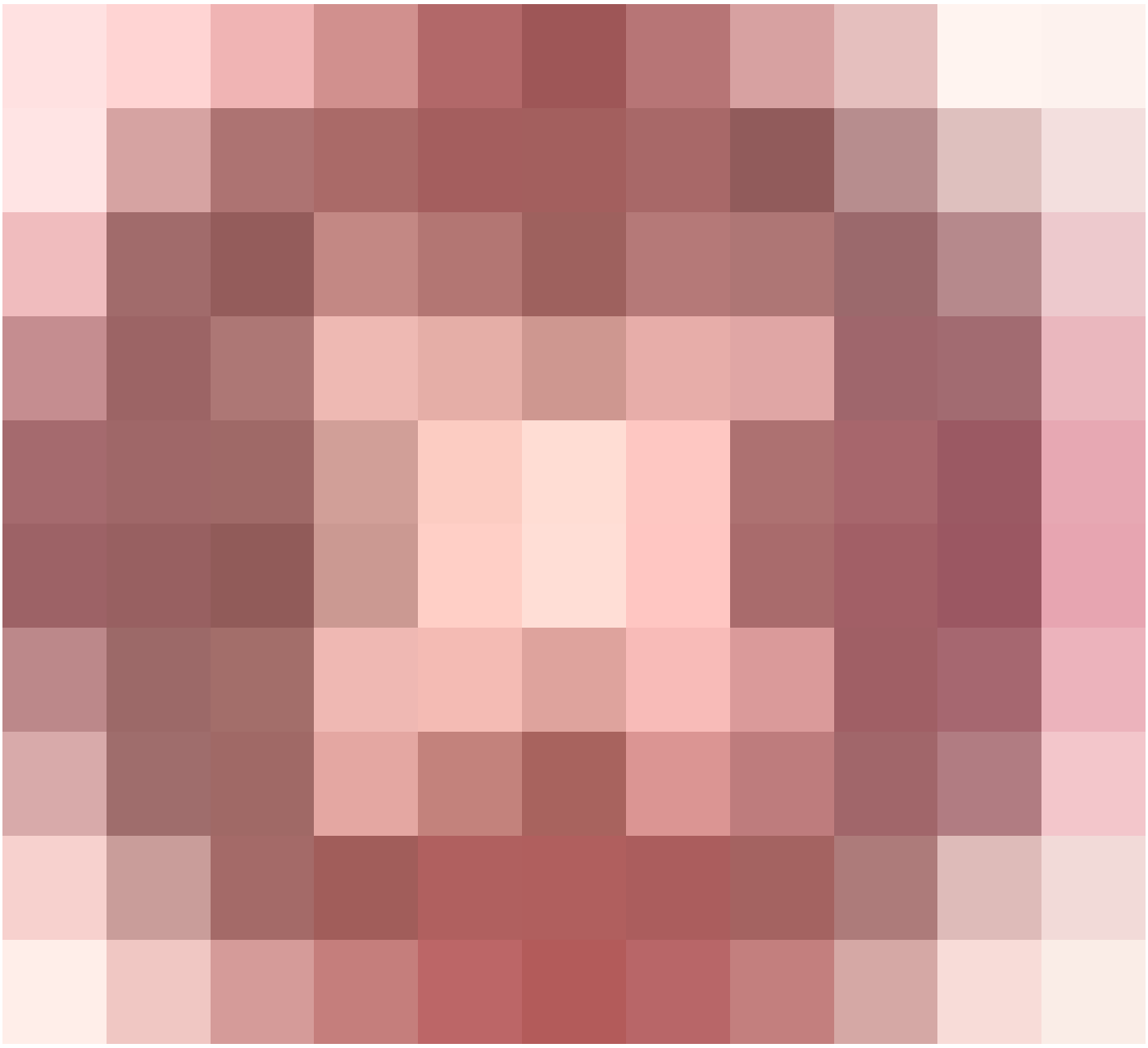
   25464155856404

   추가 아이콘
2. Allow(허용)를 선택하고 목록에 도메인을 추가합니다.
3. 저장을 클릭합니다.

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

ZeroFOX 대상 목록에서 도메인 삭제

Cisco의



(삭제) 아이콘은 ZeroFOX 대상 목록의 각 도메인 이름 옆에 있습니다. 도메인을 삭제하면 원치 않는 탐지가 발생할 경우 ZeroFOX 대상 목록을 정리할 수 있습니다.

그러나 ZeroFOX가 Umbrella에 도메인을 재전송하는 경우 삭제는 영구적이지 않습니다.

도메인을 삭제하려면

1. Settings(설정) > Integrations(통합)로 이동한 다음 "ZeroFOX"를 클릭하여 확장합니다.
2. See Domains(도메인 보기)를 클릭합니다.
3. 삭제할 도메인 이름을 검색합니다.
4. 삭제 아이콘을 클릭합니다.

5. 닫기를 클릭합니다.
6. 저장을 클릭합니다.

원치 않는 탐지 또는 오탐의 경우 즉시 Umbrella에서 허용 목록을 만든 다음 ZeroFOX 내에서 오탐을 치료하는 것이 좋습니다. 나중에 ZeroFOX 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.