Secure Malware Analytics(이전의 Threat Grid)와 Umbrella의 통합 구성

목차

소개

이 문서에서는 Secure Malware Analytics(이전의 Threat Grid)를 Umbrella와 통합하는 방법에 대해 설명합니다.

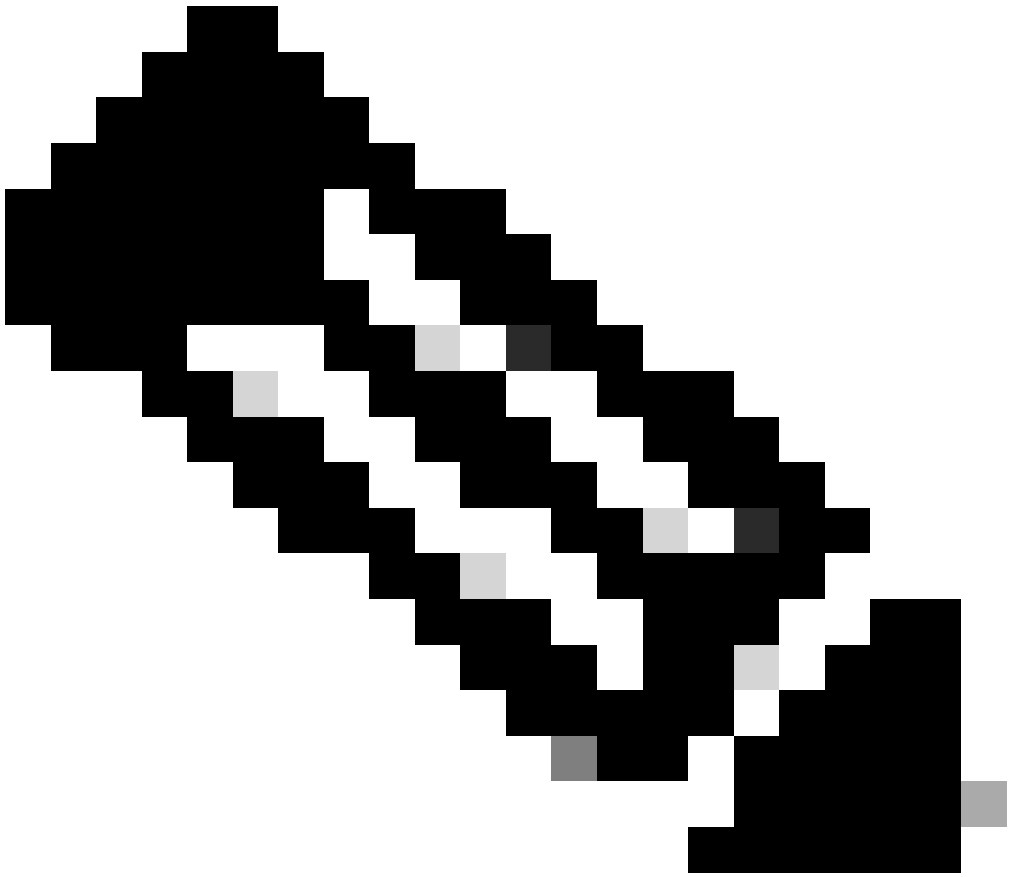
Cisco Secure Malware Analytics(Threat Grid) Integration for Cisco Umbrella 개요

Cisco Secure Malware Analytics(이전의 Threat Grid)와 Cisco Umbrella가 통합되어 이제 보안 팀은 가시성을 확장하고 로밍 중인 노트북, 태블릿 또는 전화에 대한 오늘날의 지능형 위협에 대한 보호를 시행하는 동시에 분산된 기업 네트워크에 또 다른 계층의 적용을 제공할 수 있습니다.

이 가이드에서는 Cisco Secure Malware Analytics(Threat Grid)에서 생성된 위협 인텔리전스를 Cisco Umbrella의 클라이언트를 보호할 수 있는 정책에 자동으로 통합할 수 있도록 Cisco Secure Malware Analytics(Threat Grid)가 Cisco Umbrella와 통신하도록 구성하는 방법을 설명합니다.

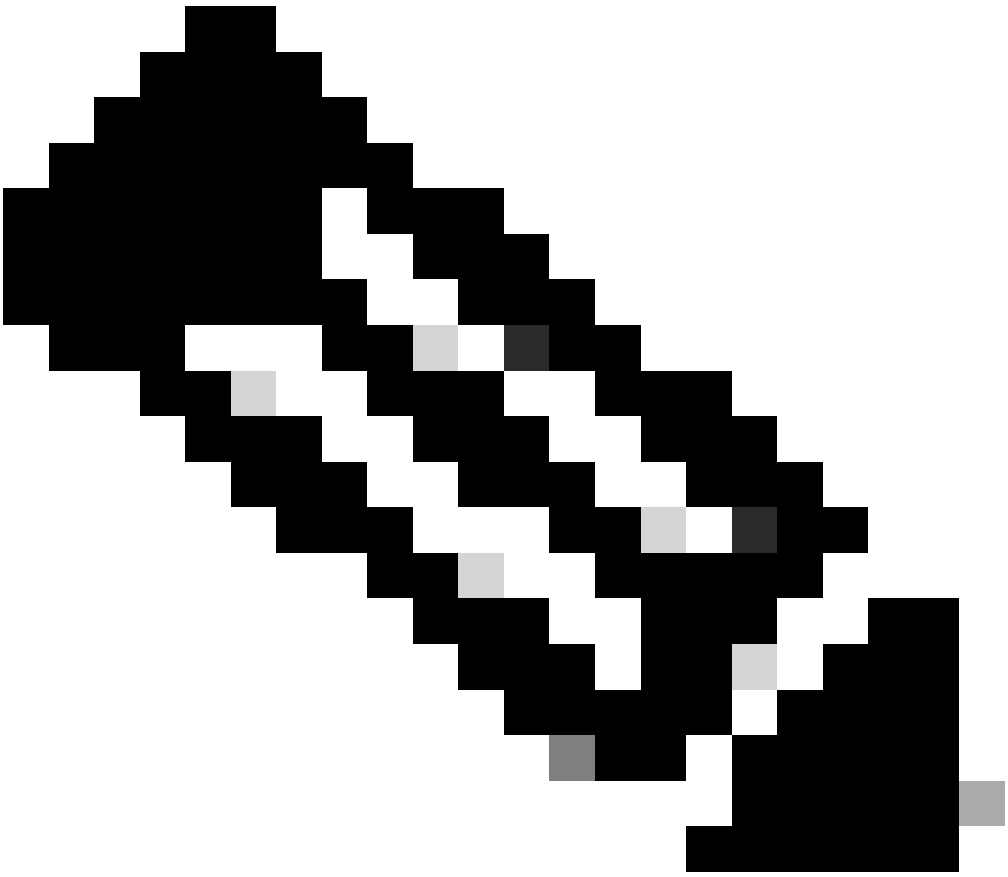
사전 요구 사항

- 계정의 API 키에 액세스할 수 있는 Cisco Secure Malware Analytics(Threat Grid) 기능 대시보드



참고: Cisco Secure Malware Analytics(Threat Grid) 어플라이언스 및 엔드포인트는 현재 지원되지 않습니다.

- Cisco Umbrella Dashboard 관리 권한
- Cisco Umbrella 대시보드에서는 Cisco Secure Malware Analytics(Threat Grid) 통합을 활성화해야 합니다.



참고: Cisco Secure Malware Analytics(Threat Grid) 통합은 DNS Essentials, DNS Advantage, SIG Essentials 또는 SIG Advantage와 같은 Cisco Umbrella 패키지에만 포함됩니다. Cisco Umbrella 패키지가 없고 이 통합을 원하는 경우 Cisco Umbrella Account Manager에게 문의하십시오. Cisco Umbrella 패키지가 있지만 Cisco Secure Malware Analytics(Threat Grid)를 대시보드의 통합으로 보지 않는 경우 Cisco Umbrella Support에 문의하십시오.

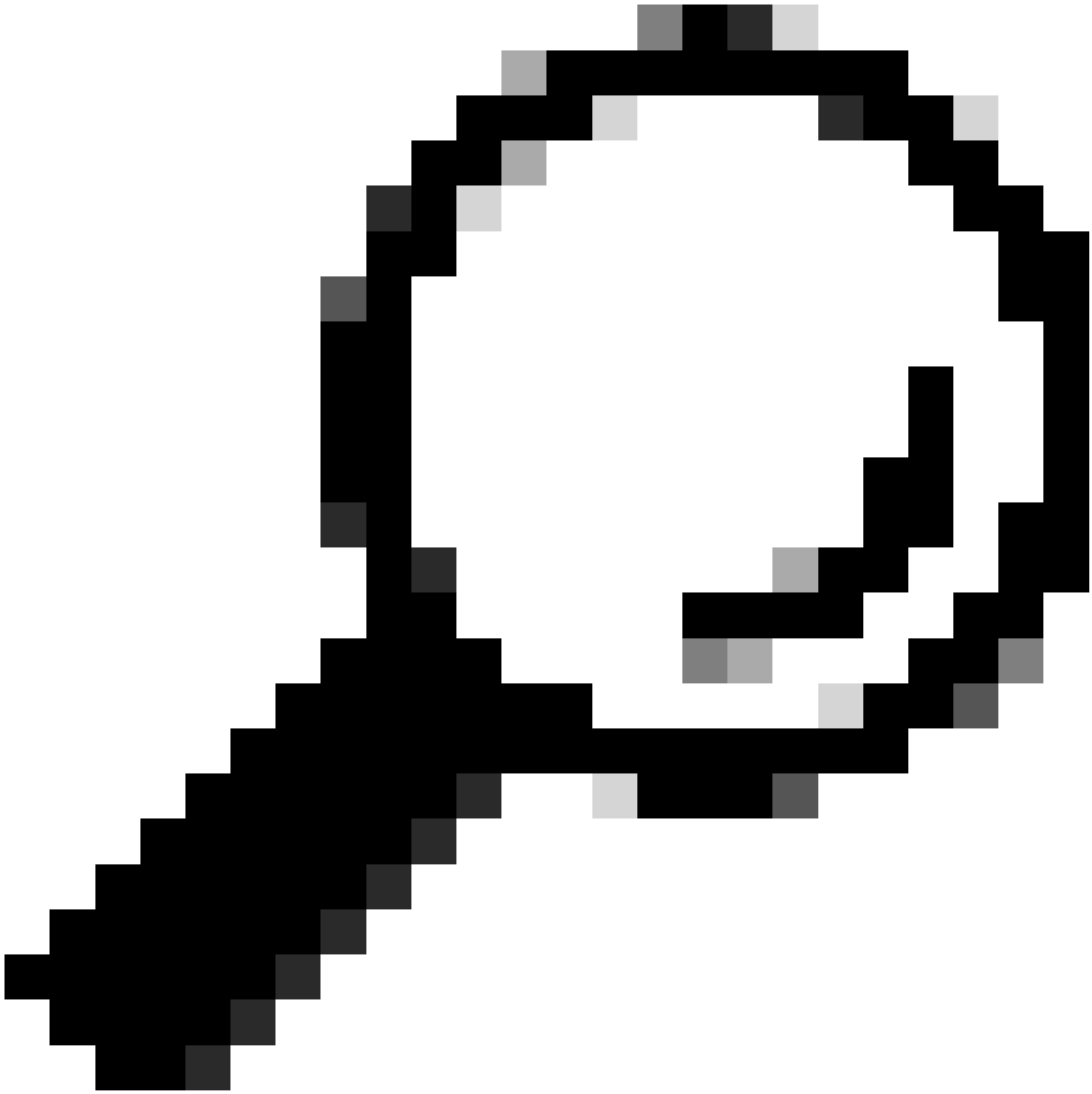
이러한 통합은 어떻게 이루어집니까?

Cisco Umbrella는 Cisco Secure Malware Analytics(Threat Grid) API에 접속하여 악성 샘플 분석에서 생성된 도메인 목록을 검색합니다. 그런 다음 Cisco Umbrella는 Cisco Umbrella 시행 API를 통해 이 목록을 가져옵니다. 이 접근 방식은 Cisco Umbrella가 Cisco Secure Malware Analytics(Threat Grid) API에 API 쿼리를 수행하여 위협 인텔리전스를 가져오는 다른 통합 방식과 다르며, 위협 인텔리전스를 Cisco Umbrella 서비스로 보내는 다른 시스템의 인시던트를 받아들이는 것이 아닙니다.

그런 다음 Cisco Umbrella가 위협을 검증하여 정책에 추가할 수 있는지 확인합니다. Cisco Secure Malware Analytics(Threat Grid)의 정보가 위협으로 확인되었거나 정상 작동이 확인된 도메인이 아닌 경우 Cisco Umbrella 정책에 적용될 수 있는 보안 설정의 일부로서 도메인 주소가 Cisco Secure

Malware Analytics(Threat Grid) 대상 목록에 추가됩니다. 이 정책은 Cisco Secure Malware Analytics(Threat Grid) 통합을 활용하는 정책을 사용하여 디바이스에서 생성되는 모든 요청에 즉시 적용됩니다.

Cisco Umbrella는 Cisco Secure Malware Analytics(Threat Grid)에서 두 개의 개별 피드를 가져옵니다. 퍼블릭(글로벌) 피드 및 고객 전용(단일 고객에만 해당하는 프라이빗) 피드



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 모든 도메인을 추가하는 것이 좋습니다.

예를 들면 다음과 같습니다.

- 조직의 홈 페이지입니다.

- 사용자가 제공하는 서비스를 나타내는 도메인으로서 내부 및 외부 레코드를 모두 포함할 수 있습니다. 예: "mail.myservicedomain.com" 및 "portal.myotherservicedomain.com"
- Cisco Umbrella에서 인식하지 못하거나 자동 도메인 검증에 포함하지 못할 정도로 많이 의존하는 덜 알려진 클라우드 애플리케이션입니다. 예: "localcloudservice.com".

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

Cisco Secure Malware Analytics(Threat Grid)에서 정보를 가져오도록 Cisco Umbrella 대시보드 구성

첫 번째 단계는 Cisco Secure Malware Analytics(Threat Grid) 대시보드에서 API 키를 찾거나 생성하는 것입니다.

1. Cisco Secure Malware Analytics(Threat Grid) 대시보드에 로그인하여 계정 세부 정보를 선택합니다.
2. Account Details(어카운트 세부사항)에서 이미 생성한 API 키가 표시될 수 있습니다. 그렇지 않은 경우 "Generate New API Key(새 API 키 생성)"를 선택합니다.

   그러면 API 키가 User Details(사용자 세부사항) > API Key(API 키)에 표시됩니다.

그런 다음 Cisco Umbrella Dashboard에 API 키를 추가하여 Cisco Secure Malware Analytics(Threat Grid)에서 데이터를 가져옵니다.

1. Cisco Umbrella 대시보드에 관리자로 로그인합니다.
2. 에서 Policies(정책) > Policy Components(정책 구성 요소) > Integrations(통합)로 이동하고 표에서 "Cisco AMP Threat Grid"(Cisco Secure Malware Analytics (Threat Grid))를 선택하여 확장합니다.
3. Enable(활성화)을 선택하고 API Key(API 키) 상자에 API Key(API 키)를 붙여넣은 다음 Save(저장)를 선택합니다.

이때 오류가 발생하면 API 키 또는 서비스 간 통신에 문제가 있을 수 있습니다. API 키를 확인하고 다시 시도하십시오. 그래도 실패하는 경우 Cisco Umbrella Support에 문의하십시오.

성공 메시지가 표시되면 Cisco Umbrella 서비스가 API 키를 사용하여 Cisco Secure Malware Analytics(Threat Grid) API에 처음 연결할 수 있음을 나타냅니다. Cisco Umbrella 서비스는 5분의 폴링 간격을 사용하여 Cisco Secure Malware Analytics(Threat Grid)에서 데이터를 검색합니다.

5분 간격이 지난 후에도 Cisco Umbrella Dashboard에서 가져올 수 있는 유효한 데이터 또는 유효한 위협 이벤트가 없는 경우 정보가 표시되지 않을 수 있습니다. 통합이 처음 활성화되면 글로벌 및 조직 전용 피드 모두에 대해 5분 전으로 되돌아가는 것만으로 시작되며, 데이터를 처음 가져오는 시점이 다음 5분 간격이므로 데이터가 즉시 나타나지 않을 수 있습니다.

Cisco Secure Malware Analytics(Threat Grid) 측의 API 키가 비활성화되거나 제거된 경우, 통합이 비활성화됩니다. 통합을 복원하려면 Cisco Umbrella Dashboard에 새 API 키를 제공해야 합니다. Cisco Umbrella와 Cisco Secure Malware Analytics(Threat Grid) 간에 시간 초과 또는 내부 서비스

오류가 발생할 경우 다른 종류의 예외가 발생하여 통합이 비활성화되지 않지만, 그 대신 일반 상황에서처럼 5분마다 연결이 계속 시도됩니다.

기술 세부사항

Cisco Secure Malware Analytics(Threat Grid)에서 정보를 가져오는 데 사용되는 정확한 API 쿼리가 아래에 나열되어 있습니다. 심각도가 90보다 크고, 신뢰도가 90보다 크며, Domains 유형의 이벤트만 수집됩니다. 이 예제의 시간은 다음 쿼리에 대해 증가하는 5분 범위입니다. Cisco `Umbrella`에 제공된 api_`key`는 `<key>` 변수 대신 사용됩니다.

- 공용(글로벌 피드):

```
hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

- 고객만(비공개 피드):

```
hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

또는:

- 공용(글로벌 피드):

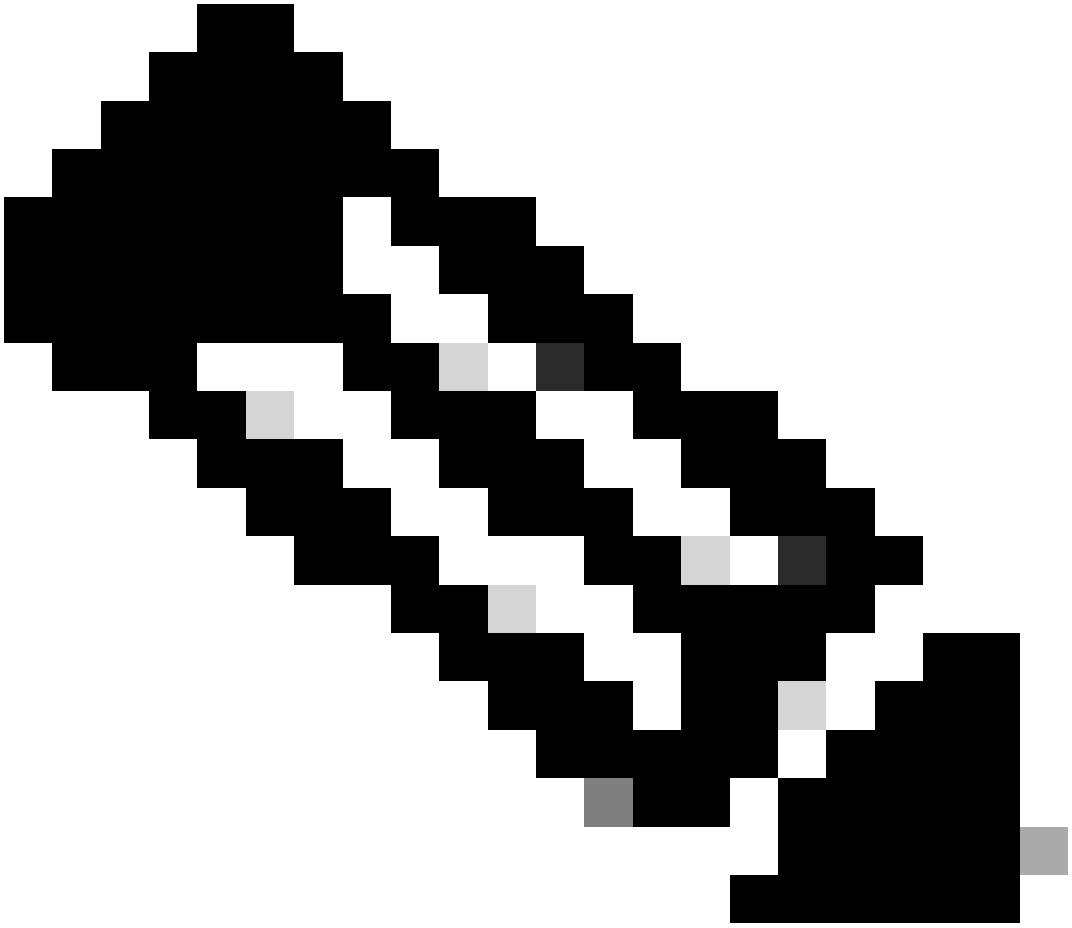
```
 hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

- 고객만(비공개 피드):

```
hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence=
```

"감사 모드"에서 Cisco Secure Malware Analytics(Threat Grid)에 추가된 이벤트 관찰

시간이 지남에 따라 Cisco Secure Malware Analytics(Threat Grid)의 이벤트가 Cisco Secure Malware Analytics(Threat Grid) Category(Cisco Secure Malware Analytics(Threat Grid) 카테고리) 정책에 적용될 수 있는 특정 대상 목록을 채우기 시작합니다. 기본적으로 대상 목록 및 보안 카테고리는 "감사 모드"에 있으며 어떤 정책에도 적용되지 않으므로 어떤 요청도 차단되지 않습니다. 그러나 Cisco AMP Threat Grid Security Category에서 어떤 요청이 연결되어 있고 차단되었을 수 있는지 확인할 수 있습니다.



참고: "감사 모드"는 구축 프로파일 및 네트워크 구성에 따라 필요한 경우 또는 무기한 활성화할 수 있습니다.

대상 목록 검토

언제든지 Cisco Secure Malware Analytics(Threat Grid)Destination List를 검토할 수 있습니다.

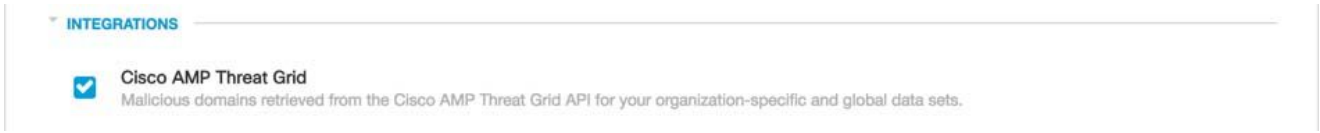
1. Policies(정책) > Policy Components(정책 구성 요소) > Integrations(통합)로 이동합니다.
2. 표에서 "Cisco AMP Threat Grid"(Cisco Secure Malware Analytics (Threat Grid))를 확장하고 "See Domains(도메인 보기)"를 선택합니다.

정책에 대한 보안 설정 검토

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

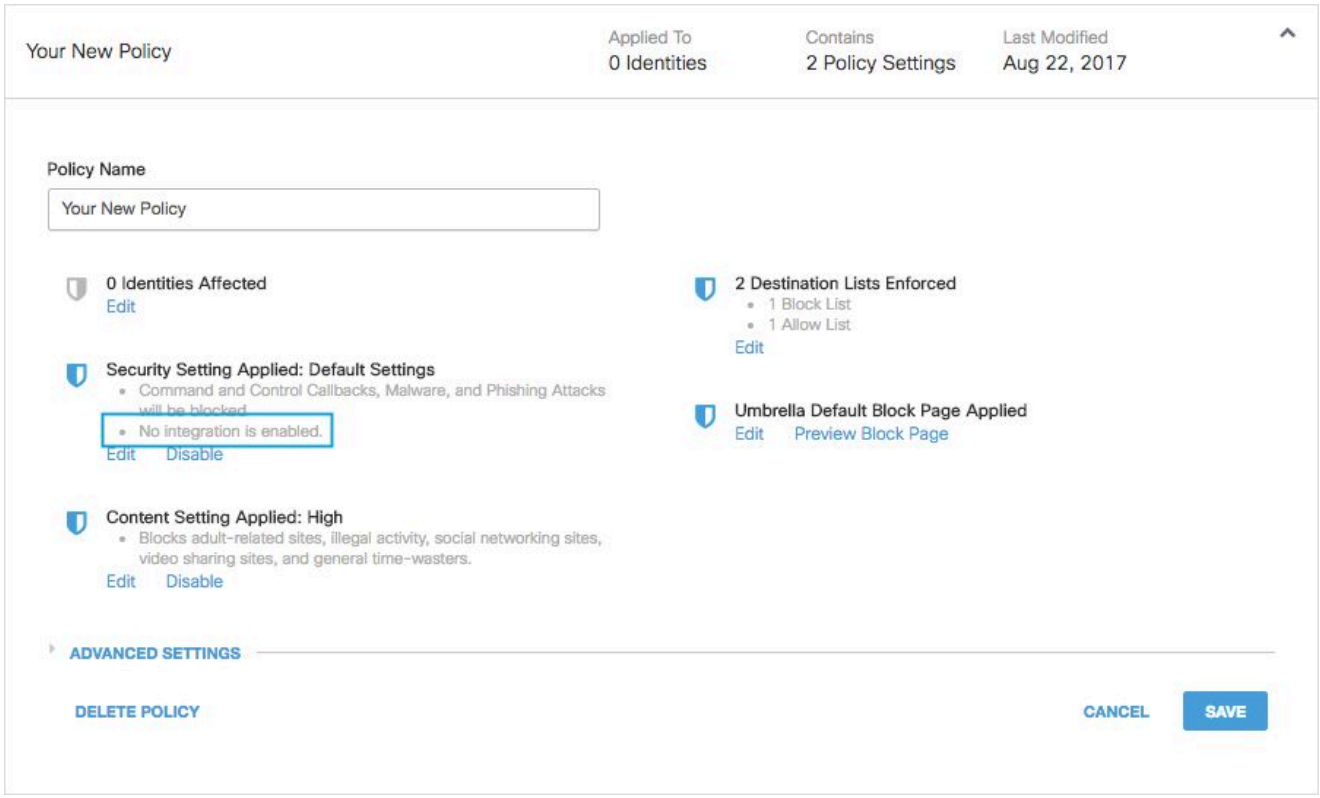
1. Policies(정책) > Policy Components(정책 구성 요소) > Security Settings(보안 설정)로 이동합니다.

2. 테이블에서 보안 설정을 클릭하여 확장합니다.
3. Integrations(통합) 섹션으로 스크롤한 다음 섹션을 확장하여 Cisco AMP Threat Grid(Cisco Secure Malware Analytics(Threat Grid)) 통합을 표시합니다.
4. Cisco AMP Threat Grid 통합(Cisco Secure Malware Analytics(Threat Grid)) 확인란을 선택하고 Save를 선택합니다.

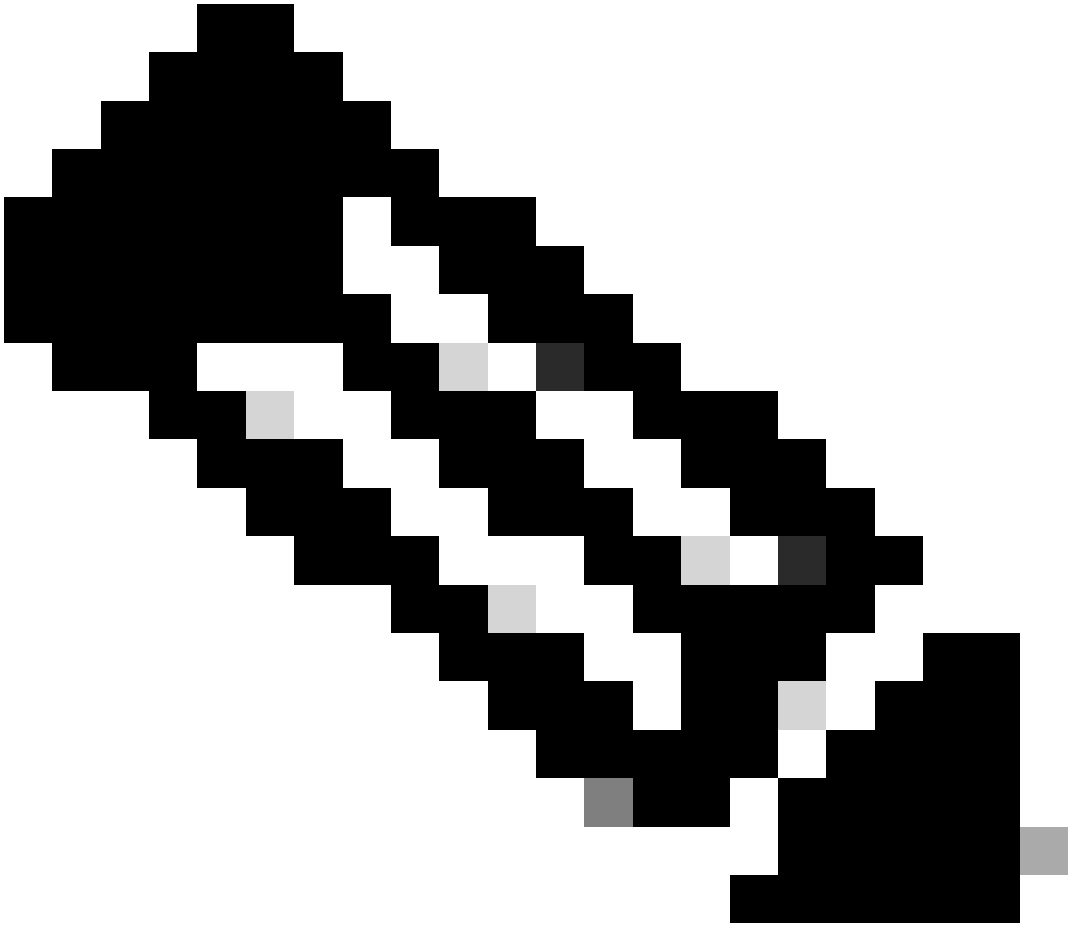


115014151543

보안 설정 요약 페이지를 통해 통합 정보를 검토할 수도 있습니다.



20993269073556



참고: 설정을 적용하는 데 최대 5분이 소요될 수 있으며, Cisco Secure Malware Analytics(Threat Grid) 시스템에 새 이벤트가 주입되지 않을 경우 통합에 새 도메인이 추가되지 않을 수 있습니다.

"차단 모드"의 Cisco Secure Malware Analytics(Threat Grid) 보안 설정을 관리되는 클라이언트에 대한 정책에 적용

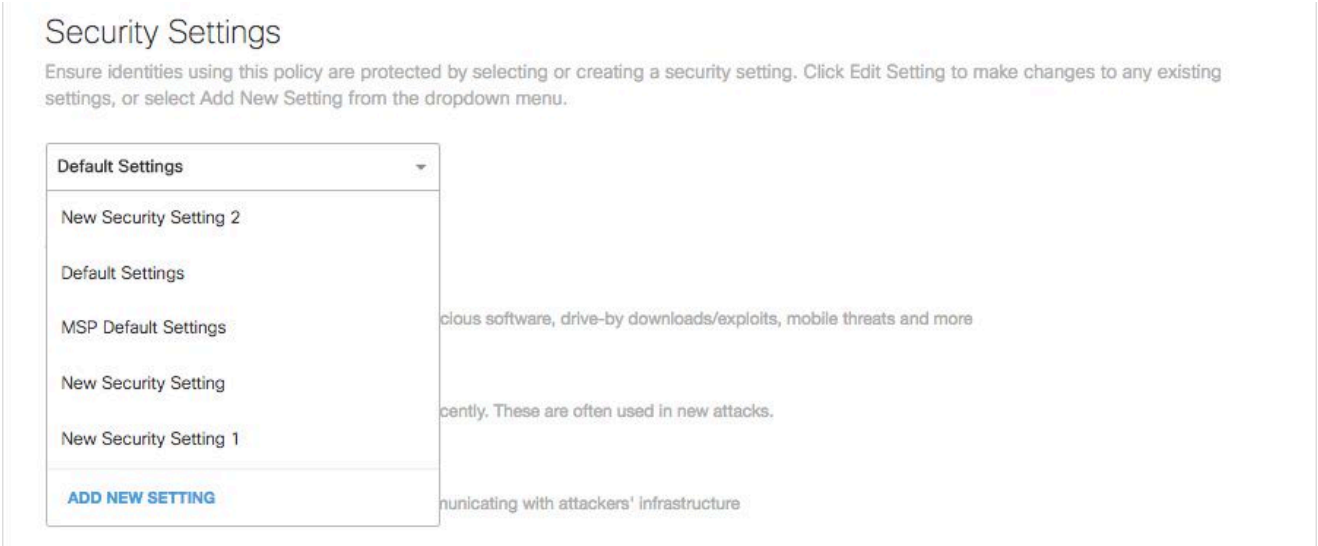
Cisco Umbrella에서 관리하는 클라이언트에 대해 이러한 도메인을 차단할 준비가 되면 기존 정책의 보안 설정을 변경하거나 기본 정책 위에 있는 새 정책을 생성하여 해당 정책이 먼저 시행되도록 합니다.

1. Policies(정책) > Policy Components(정책 구성 요소) > Security Settings(보안 설정)로 이동합니다.
2. Integrations(통합)에서 "Cisco AMP Threat Grid" 상자가 선택되었는지 확인합니다. 그렇지 않은 경우 상자를 선택하고 저장을 선택합니다.

115013987086

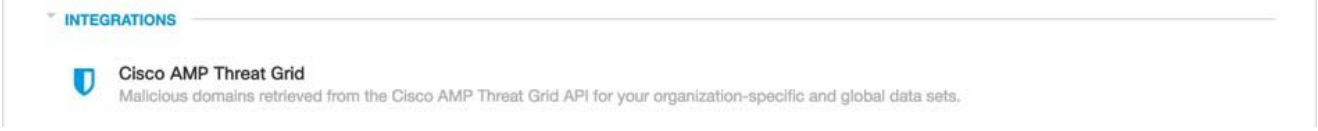
다음으로, Cisco Umbrella Policy(Cisco Umbrella 정책) 마법사에서 수정 중인 정책에 보안 설정을 추가합니다.

1. Policies(정책) > Management(관리) > All Policies(모든 정책)로 이동합니다.
2. 정책을 확장하고 Security Setting Applied(보안 설정 적용됨)에서 Edit(편집)를 선택합니다.
3. Security Settings(보안 설정) 폴다운에서 "Cisco AMP Threat Grid" 설정이 포함된 보안 설정을 선택합니다.



20993282642708

Integrations(통합) 아래의 실드 아이콘이 파란색으로 업데이트됩니다.



115013987446

4. Set & Return을 선택합니다.

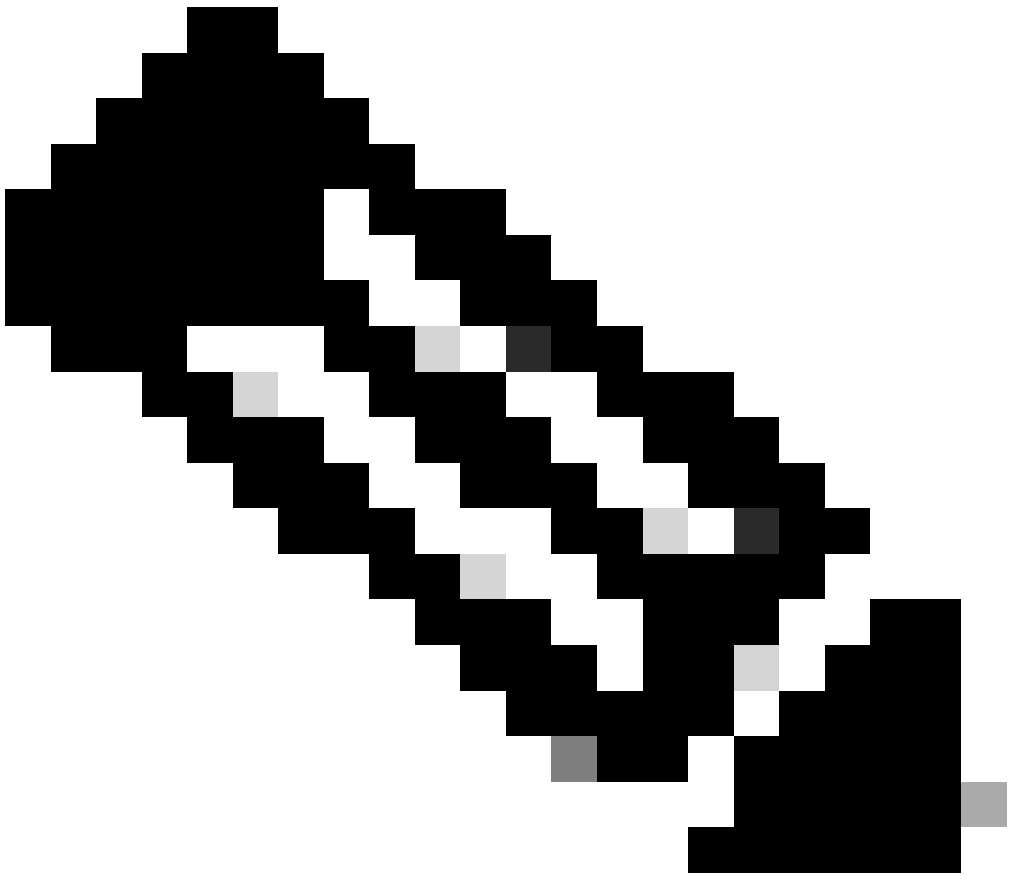
Cisco Secure Malware Analytics(Threat Grid)의 보안 설정에 포함된 Cisco Secure Malware Analytics(Threat Grid) 도메인은 정책을 사용하여 이러한 ID에 대해 차단됩니다.

Cisco Umbrella 내의 보고 - Cisco Secure Malware Analytics 이벤트

Cisco Secure Malware Analytics(Threat Grid) 보안 이벤트 보고

Cisco Secure Malware Analytics(Threat Grid) 대상 목록은 보고할 수 있는 보안 범주 목록 중 하나입니다. 보고서의 대부분 또는 모두가 보안 카테고리를 필터로 사용합니다. 예를 들어, Cisco Secure Malware Analytics(Threat Grid) 관련 활동만 표시하도록 보안 카테고리를 필터링할 수 있습니다.

1. Reporting(보고) > Core Reports(핵심 보고서) > Activity Search(활동 검색)로 이동하고 Security Categories(보안 범주)에서 "Cisco AMP Threat Grid"(Cisco Secure Malware Analytics(Threat Grid))를 선택하여 Cisco Secure Malware Analytics(Threat Grid)에 대한 보안 범주만 표시하도록 보고서를 필터링합니다.



참고: Cisco AMP Threat Grid 통합이 비활성화된 경우 Security Categories(보안 카테고리) 필터에 나타나지 않습니다.

115014210123

2. Apply를 선택합니다.

도메인이 Cisco Secure Malware Analytics(Threat Grid) 대상 목록에 추가된 시기 보고

Cisco Umbrella Admin Audit(Cisco Umbrella 관리 감사) 로그에는 Cisco Secure Malware Analytics(Threat Grid) 대시보드에서 목적지 목록에 도메인을 추가하는 이벤트가 포함됩니다. Cisco 로고가 브랜드화된 "Cisco AMP Threat Grid Domain List"라는 사용자는 이벤트를 생성합니다. 이러한 이벤트에는 추가된 도메인 및 추가된 시간이 포함됩니다.

Admin Audit Log(관리 감사 로그) 항목을 선택하면 추가된 특정 도메인을 비롯한 세부사항이 표시되도록 항목이 확장됩니다.

"Cisco AMP Threat Grid Domain List" 사용자에 대한 필터를 적용하여 Cisco Secure Malware Analytics(Threat Grid) 변경 사항만 포함하도록 필터링할 수 있습니다.

원치 않는 탐지 또는 오탐 처리

2가지 유형의 Cisco Secure Malware Analytics(Threat Grid) 탐지 및 2가지 해결

현재 Cisco Secure Malware Analytics(Threat Grid) 블록에는 두 가지 유형이 있습니다. 하나의 가능한 해상도를 갖는 하나 및 원하지 않는 검출에 대한 하나의 전류 해상도를 갖는 두 번째.

1. 전역 Threat Grid 항목(공용): 현재 도메인을 허용하는 유일한 방법은 허용 목록에 도메인을 추가하는 것입니다.
2. 고객 전용 피드(비공개): 허용 목록 항목을 사용하거나 AMP Threat Grid 통합 목록에서 삭제하여 해결할 수 있습니다.

허용 목록

Cisco Secure Malware Analytics(Threat Grid) 통합에 의해 자동으로 추가된 도메인은 가능성이 있지만, 사용자가 특정 웹 사이트에 액세스하지 못하도록 차단하는 원치 않는 탐지를 트리거할 수 있습니다. 이러한 상황에서는 도메인을 허용 목록(Policies > Destination Lists)에 추가하는 것이 좋습니다. 이 목록은 보안 설정을 비롯한 다른 모든 유형의 차단 목록보다 우선합니다.

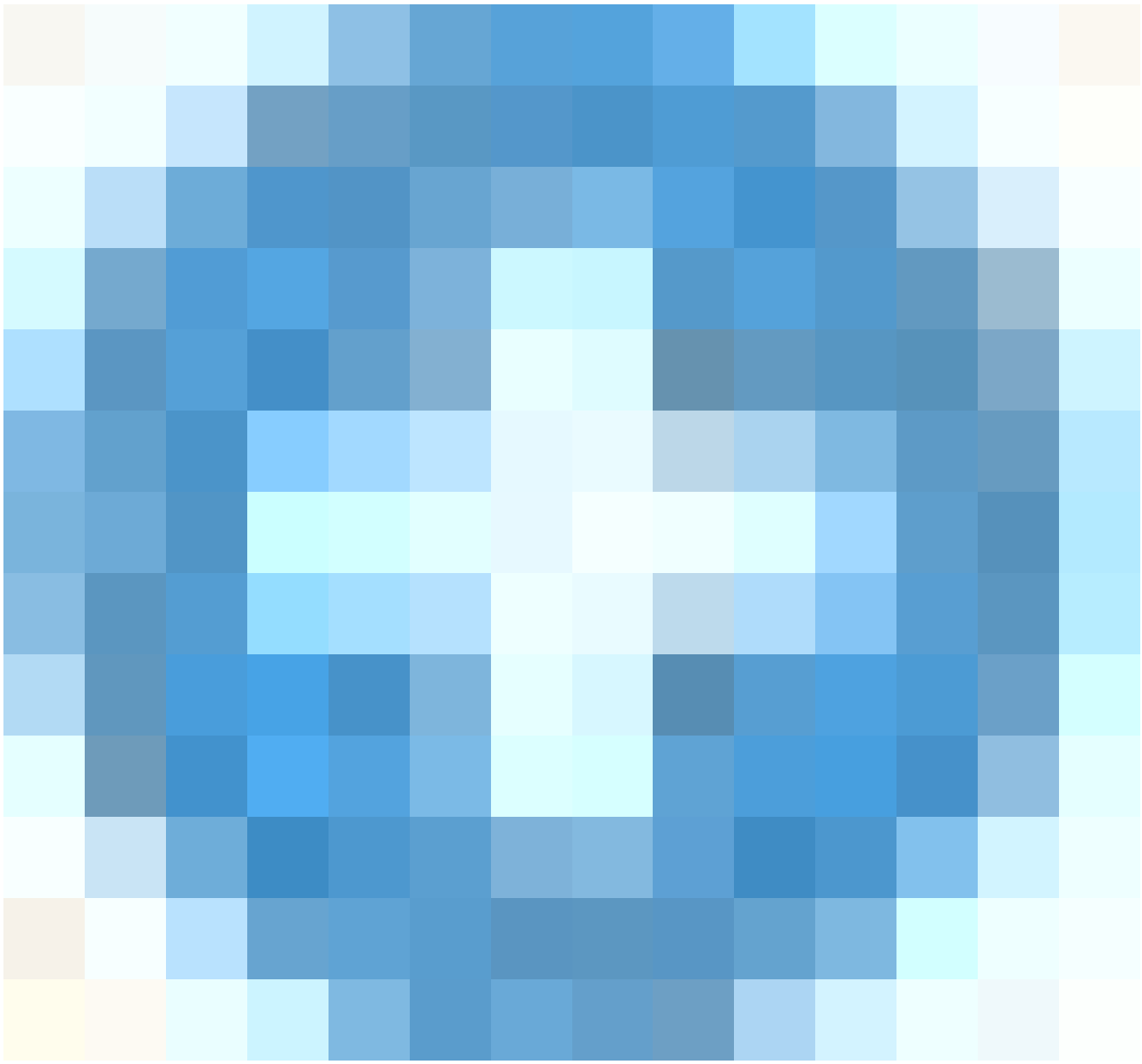
이 접근 방식이 선호되는 두 가지 이유가 있다. 먼저, Cisco Secure Malware Analytics(Threat Grid) 대시보드에서 도메인을 제거한 후 다시 추가하는 경우 허용 목록에 따라 추가 문제가 발생할 수 있습니다. 둘째, 허용 목록에는 포렌식 또는 감사 보고서에 사용할 수 있는 문제가 있는 도메인의 기록 레코드가 표시됩니다.

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

차단 모드의 Cisco Secure Malware Analytics(Threat Grid) 보안 설정이 관리되는 Cisco Umbrella ID의 하위 집합에만 적용되는 경우(예: 로밍 컴퓨터 및 모바일 디바이스에만 적용되는 경우) 이러한 ID 또는 정책에 대한 특정 허용 목록을 생성할 수 있습니다.

허용 목록을 생성하려면

1. Policies(정책) > Policy Components(정책 구성 요소) > Destination Lists(대상 목록)로 이동하고 선택합니다



25463394696852

("추가").
2. Allow(허용)를 선택하고 목록에 도메인을 추가합니다.
3. 저장을 선택합니다.

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

Cisco Secure Malware Analytics(Threat Grid) 대상 목록에서 도메인 삭제

Cisco Secure Malware Analytics(Threat Grid) 목록의 각 도메인 이름 옆에는 ("삭제") 아이콘이 있습니다. 도메인을 삭제하면 원치 않는 탐지가 발생할 경우 Cisco Secure Malware Analytics(Threat Grid) 대상 목록을 정리할 수 있습니다.

Cisco Secure Malware Analytics(Threat Grid) 대시보드에서 도메인을 Cisco Umbrella로 재전송하는 경우 삭제되지 않습니다.

1. Policies(정책) > Policy Components(정책 구성 요소) > Integrations(통합)로 이동하고 "Cisco AMP Threat Grid"(Cisco Secure Malware Analytics (Threat Grid))를 선택하여 확장합니다.
2. See Domains를 선택합니다.
3. 삭제할 도메인 이름을 검색합니다.
4. ("삭제") 아이콘을 선택합니다.
5. 닫기를 선택합니다.
6. 저장을 선택합니다.

원치 않는 탐지 또는 오탐의 경우 Cisco Umbrella에서 즉시 허용 목록을 생성한 다음 Cisco Secure Malware Analytics(Threat Grid) 대시보드 내에서 오탐을 해결하는 것이 좋습니다. 나중에 Cisco Secure Malware Analytics(Threat Grid) Destination List(대상 목록)에서 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.