FireEye와 Umbrella 통합

목차

소개

이 문서에서는 Cisco Umbrella를 FireEye와 통합하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 공용 인터넷에 액세스할 수 있는 FireEye 어플라이언스입니다.
- Cisco Umbrella Dashboard 관리 권한
- Cisco Umbrella Dashboard에서 FireEye 통합을 활성화해야 합니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

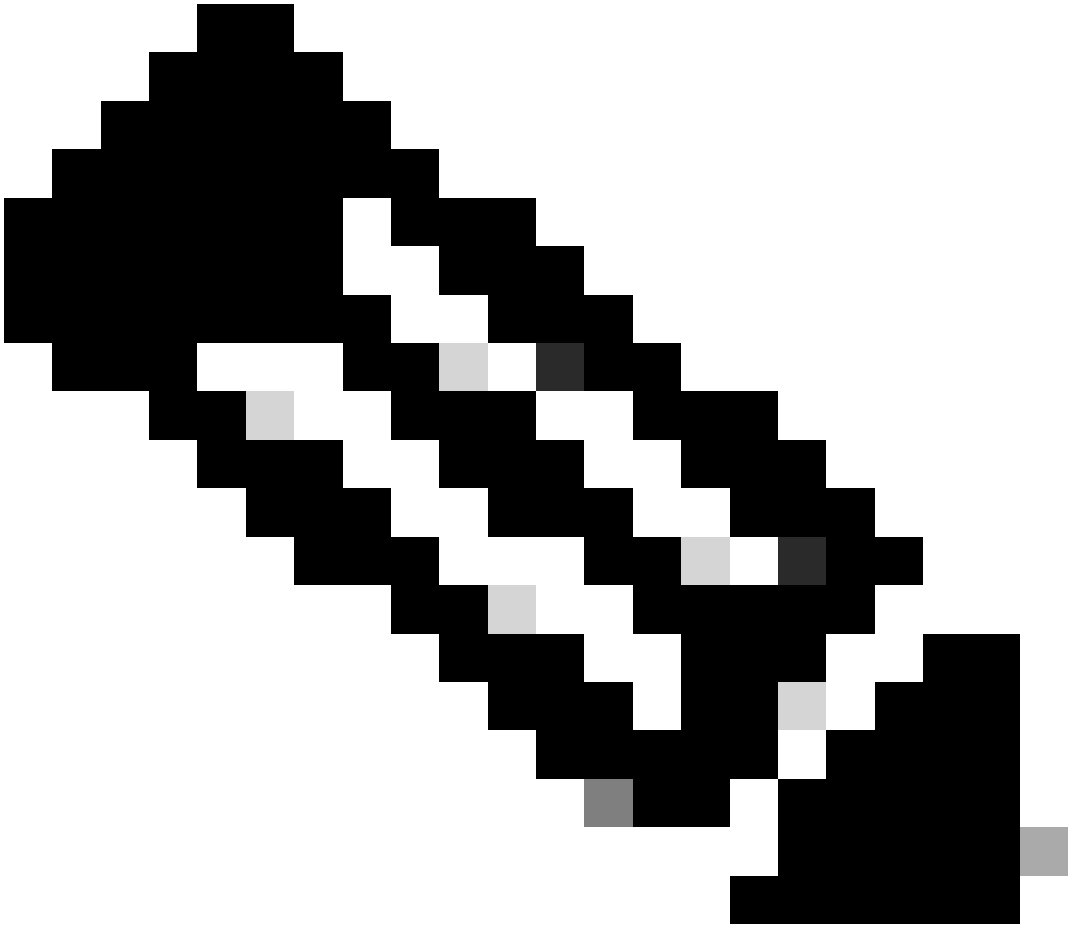
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

FireEye 보안 어플라이언스와 Cisco Umbrella가 통합됨에 따라, 이제 보안 담당자 및 관리자는 로밍 중인 노트북, 태블릿 또는 전화에 대한 지능형 위협에 대한 보호 기능을 확장하는 동시에 분산된 기업 네트워크에 또 다른 레이어의 적용을 제공할 수 있습니다.

이 설명서에서는 FireEye의 보안 이벤트가 Cisco Umbrella로 보호되는 클라이언트에 적용할 수 있는 정책에 통합될 수 있도록 FireEye가 Cisco Umbrella와 통신하도록 구성하는 방법을 설명합니다.



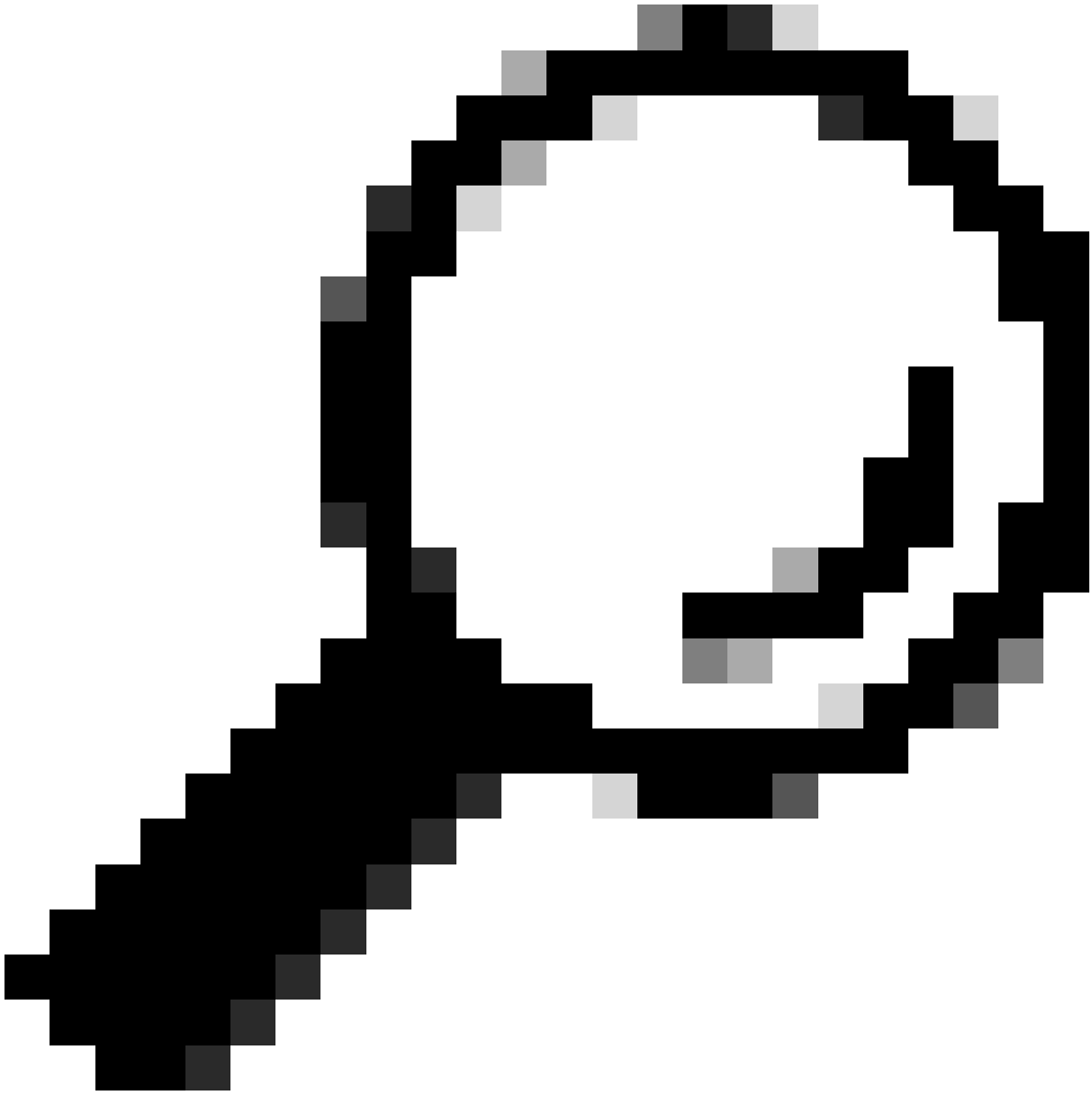
참고: FireEye 통합은 DNS Essentials, DNS Advantage, SIG Essentials 또는 SIG Advantage와 같은 Cisco Umbrella 패키지에만 포함됩니다. 이러한 패키지 중 하나가 없는 상태에서 FireEye 통합을 원하는 경우 Cisco Umbrella Account Manager에게 문의하십시오. 올바른 Cisco Umbrella 패키지가 있지만 대시보드의 통합으로 FireEye가 보이지 않는 경우 Cisco Umbrella Support에 문의하십시오.

통합 기능

FireEye 어플라이언스는 먼저 발견된 인터넷 기반 위협(예: 악성코드를 호스팅하는 도메인, 봇넷을 위한 명령 및 제어 또는 피싱 사이트)을 Cisco Umbrella로 전송합니다.

Cisco Umbrella는 Cisco Umbrella에 전달된 정보가 유효하고 정책에 추가될 수 있는지 검증합니다. FireEye의 정보가 올바른 형식이 아닌 것으로 확인되면(예: 파일, 복잡한 URL 또는 널리 사용되는 도메인이 아님) Cisco Umbrella 정책에 적용할 수 있는 보안 설정의 일부로서 도메인 주소가 FireEye 대상 목록에 추가됩니다. 이 정책은 FireEye 대상 목록의 정책을 사용하여 디바이스에서 생성되는 모든 요청에 즉시 적용됩니다.

앞으로 Cisco Umbrella는 FireEye 알림을 자동으로 구문 분석하고 악의적인 사이트를 FireEye 대상 목록에 추가합니다. 따라서 FireEye 보호 기능이 모든 원격 사용자 및 디바이스로 확대되고 회사 네트워크에 또 다른 시행 레이어가 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.

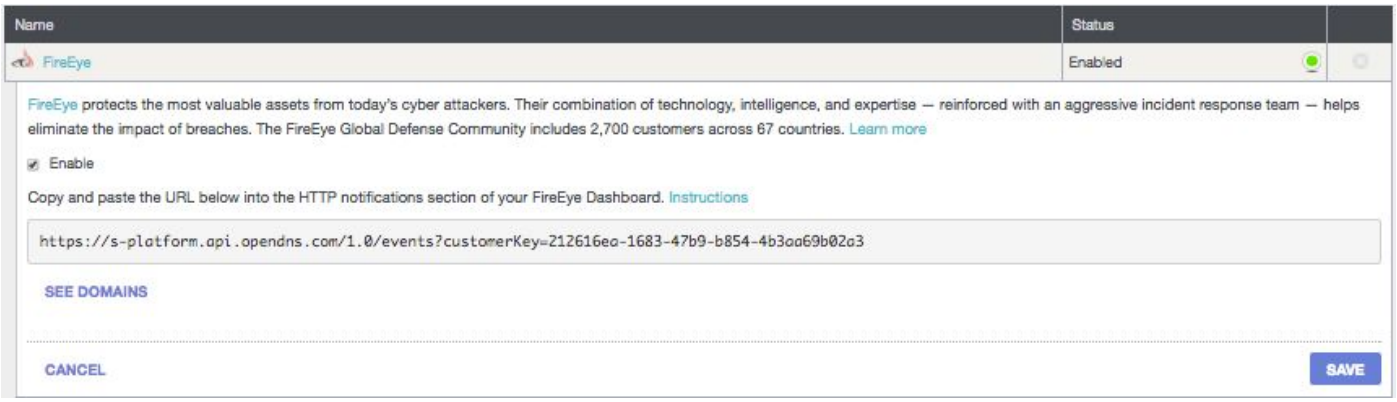
FireEye에서 정보를 수신하도록 Cisco Umbrella 대시보드 구성

첫 번째 단계는 FireEye 어플라이언스가 통신할 수 있는 Cisco Umbrella의 고유한 URL을 찾는 것입니다.

1. Cisco Umbrella 대시보드에 관리자로 로그인합니다.

2. Policies(정책) > Policy Components(정책 구성 요소) > Integrations(통합)로 이동하고 테이블에서 FireEye를 선택하여 확장합니다.

3. 사용가능 박스를 선택한 다음 저장을 선택합니다. 이렇게 하면 Cisco Umbrella에 속한 조직의 고유한 특정 URL이 생성됩니다.

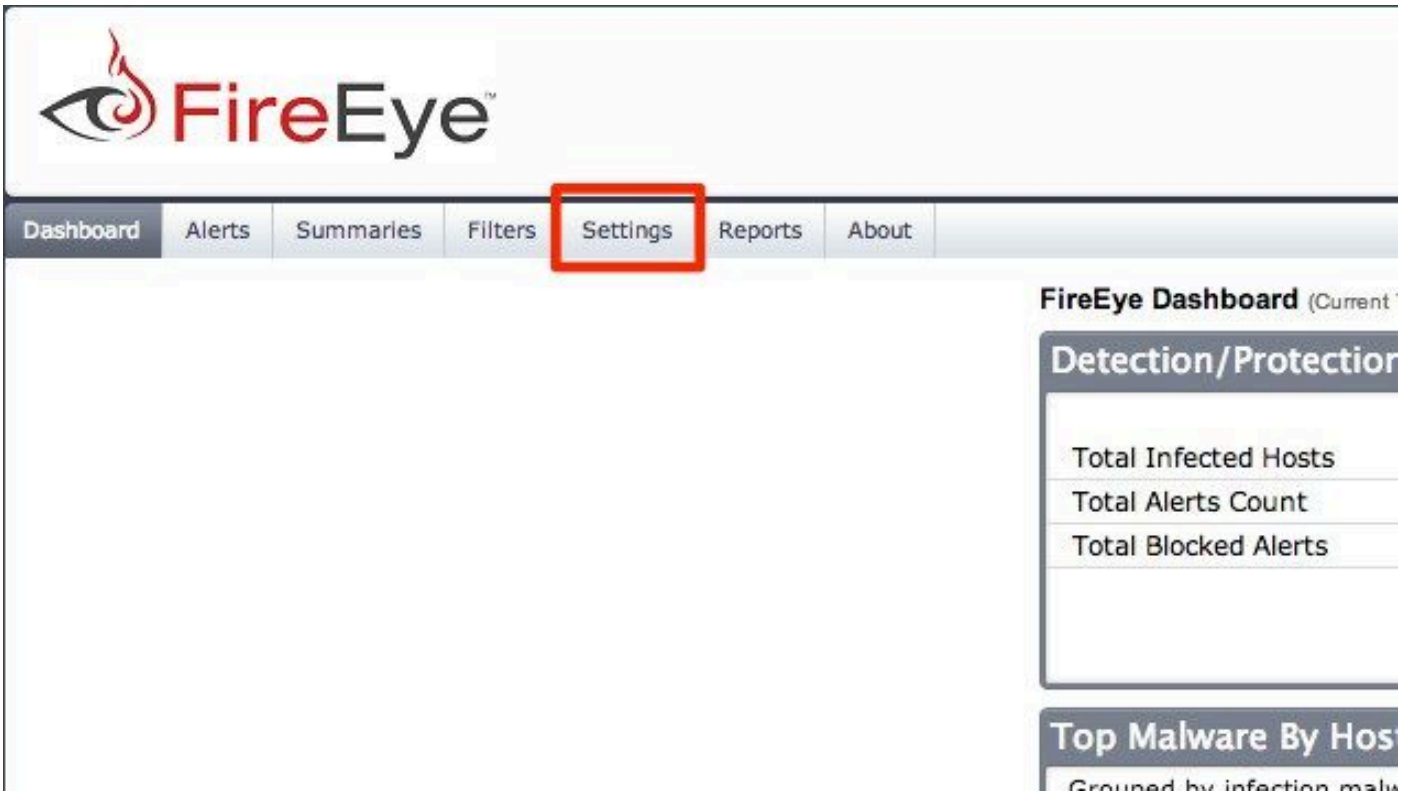


나중에 이 URL을 사용하여 FireEye 어플라이언스에서 Cisco Umbrella로 데이터를 전송하도록 구성할 수 있으므로 URL을 복사해야 합니다.

Cisco Umbrella와 통신하도록 FireEye 구성

FireEye 어플라이언스에서 Cisco Umbrella로 트래픽을 전송하려면 이전 섹션에서 생성된 URL 정보로 FireEye를 구성해야 합니다.

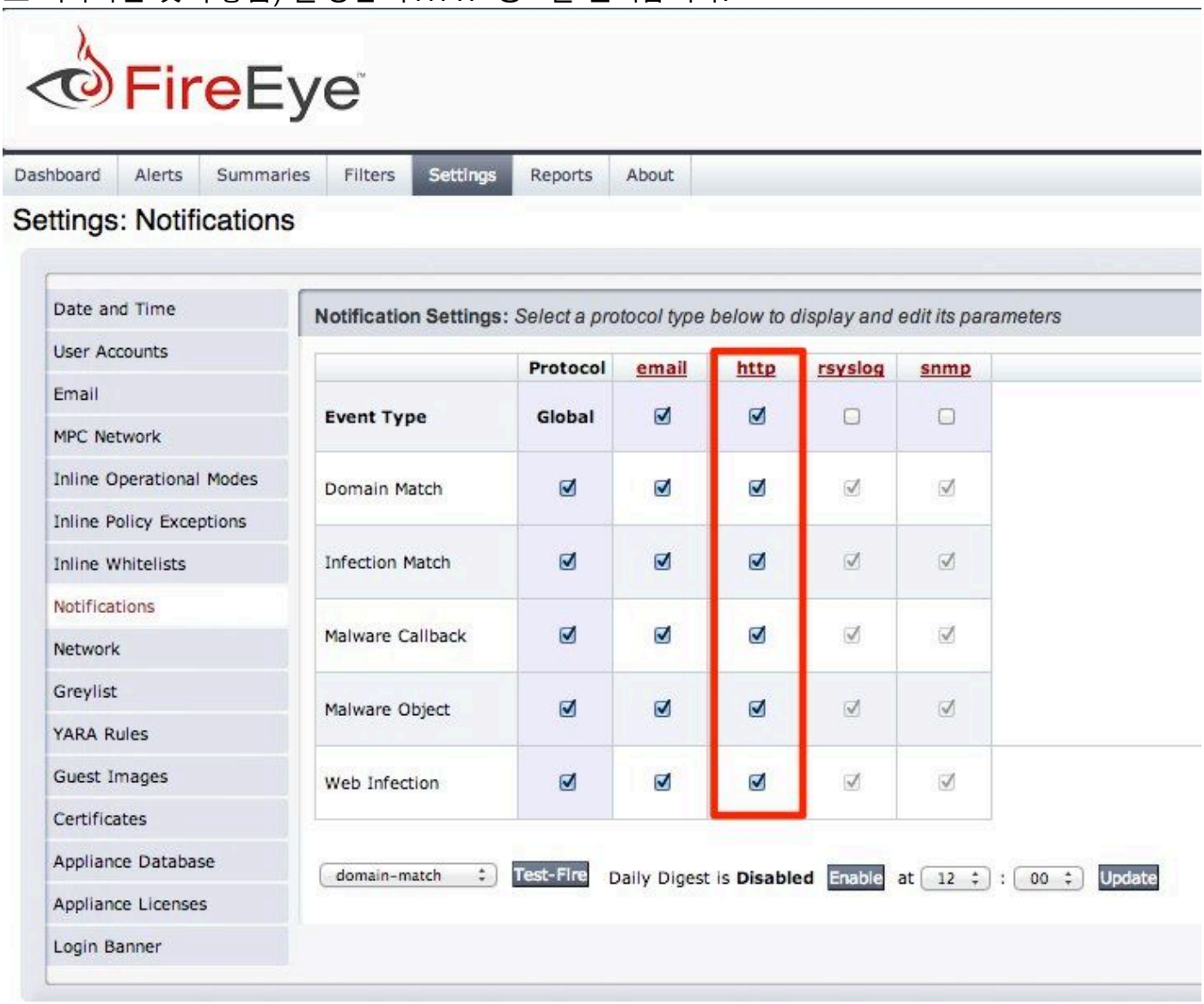
1. FireEye에 로그인하여 설정을 선택합니다.



2. 설정 목록에서 통지를 선택합니다.

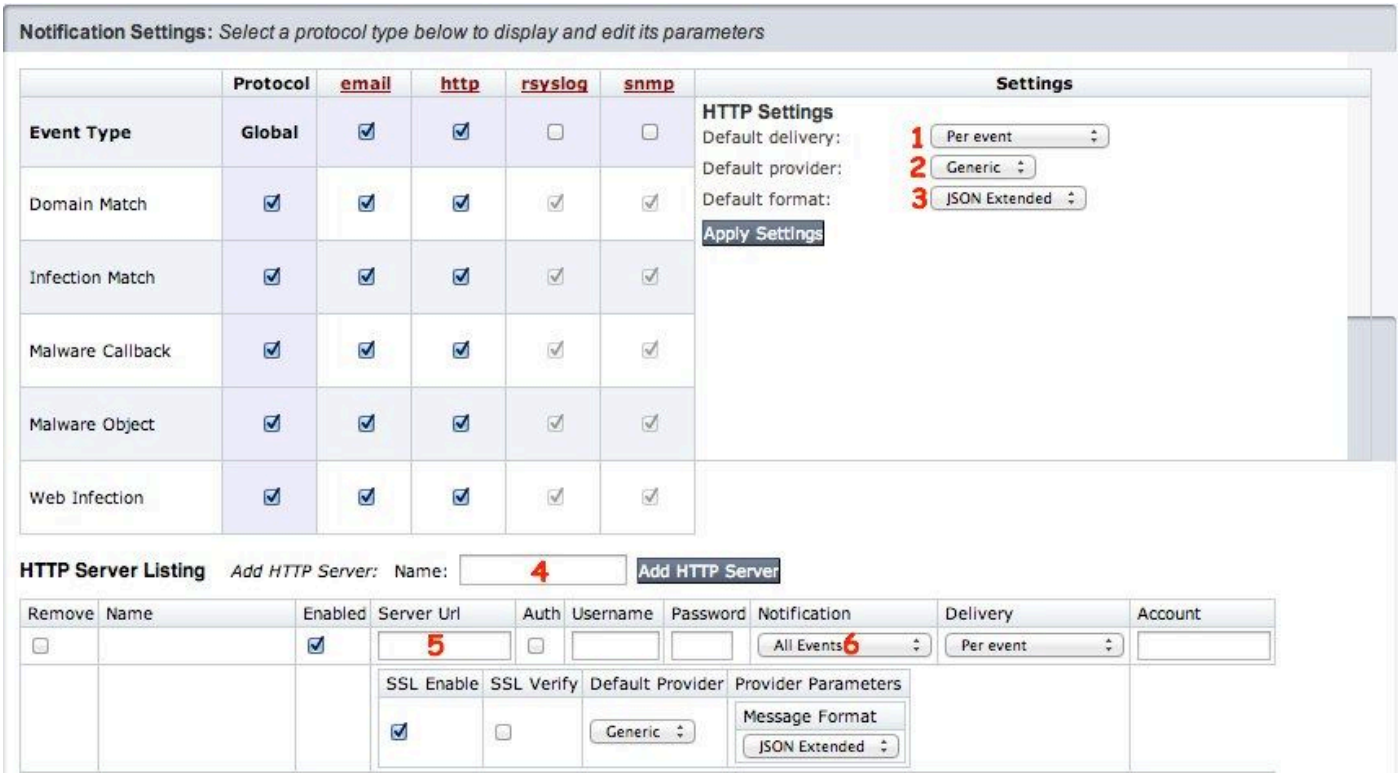

FireEye
Dashboard
Alerts
Summaries
Filters
Settings
Reports
About
Settings: Date and Time
Date and Time
User Accounts
Email
MPC Network
Inline Operational Modes
Inline Policy Exceptions
Inline Whitelists
Notifications
Network
Greylist
YARA Rules
Guest Images
Certificates
Appliance Database
Appliance Licenses
Login Banner
Date and Time Settings
Manually set the date, time, and time zone. Or, op
synchronization.
(Current Time: 11/11/13 17:29:24 UTC)
Set Manually:
November
11
2013
17
Enable NTP:
Add NTP Server:
NTP Server
Delete
Update T
pool.ntp.org
Update T
time.nist.gov
Update T
Remove Selected NTP Servers
Set Time Zone:
UTC
Set Time Zone

3. Cisco Umbrella로 전송할 모든 이벤트 유형이 선택되어 있는지 확인한 후(Umbrella에서는 모두로 시작하는 것이 좋음) 열 상단의 HTTP 링크를 선택합니다.



4. 메뉴가 확장되면 이벤트 통지를 사용으로 설정하려면 이 옵션을 선택합니다. 번호가 매겨진 단계는 스크린샷에 설명되어 있습니다.

1. 기본 배달: 이벤트당
2. 기본 공급자: 일반
3. 기본 형식: JSON 확장
4. HTTP 서버 이름을 "OpenDNS"로 지정합니다.
5. 서버 Url: 앞서 Cisco Umbrella 대시보드에서 생성한 Cisco Umbrella URL을 여기에 붙여넣습니다.
6. 알림 드롭다운: All Events(모든 이벤트)를 선택하여 최대 지원 범위를 확인합니다.



5. 전달, 기본 공급자 및 공급자 매개변수 드롭다운 모두 기본 설정과 일치하는지 또는 여러 통지 서버가 사용되고 있는지 확인합니다.

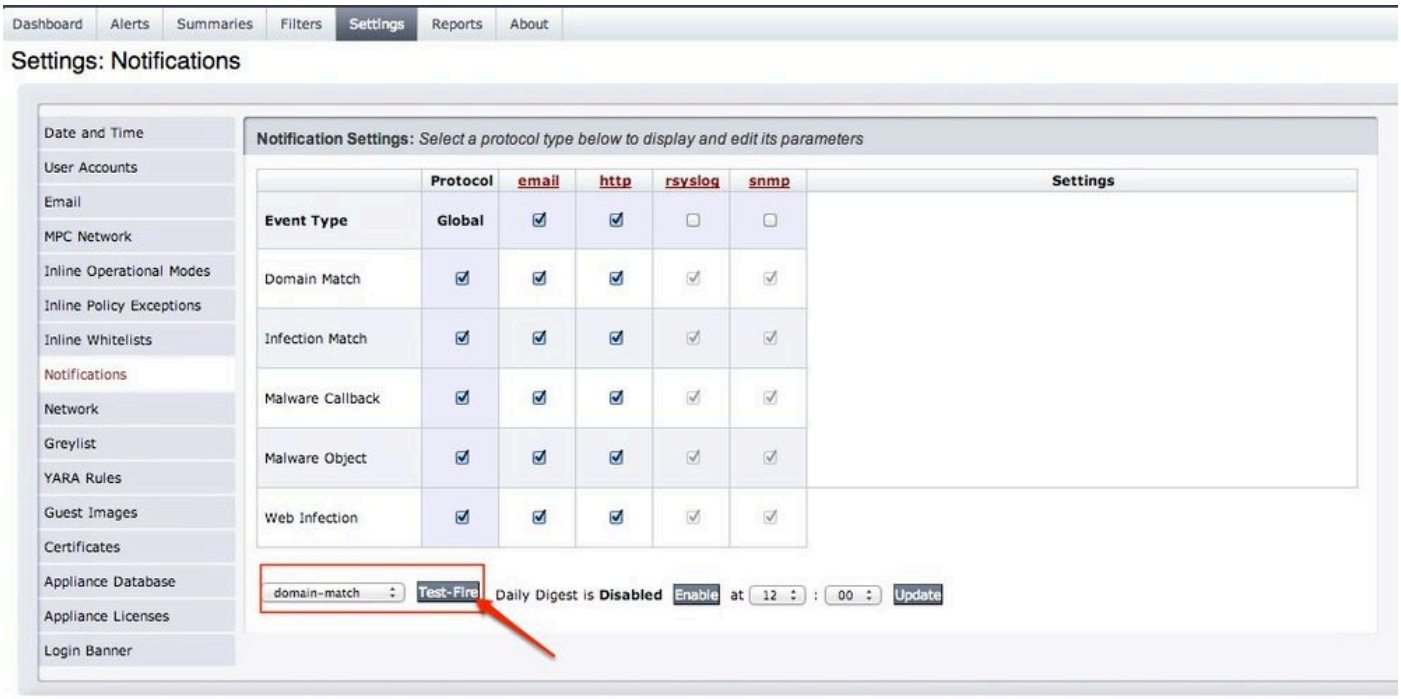
- 제공: 이벤트당
- 기본 공급자: 일반
- 공급자 매개변수: 메시지 형식 JSON 확장
- (선택 사항) SSL을 통해 트래픽을 전송하려면 SSL Enable을 선택합니다.

이 시점에서 FireEye 어플라이언스는 선택한 이벤트 유형을 Cisco Umbrella로 전송하도록 설정됩니다. 다음으로, Cisco Umbrella Dashboard에서 이 정보를 보고 이 트래픽에 대해 차단할 정책을 설정하는 방법을 알아보십시오.

연결 확인: FireEye와 Cisco Umbrella 간의 "테스트 실행"

이때 연결을 테스트하고 모든 것이 올바르게 설정되었는지 확인하는 것이 좋습니다.

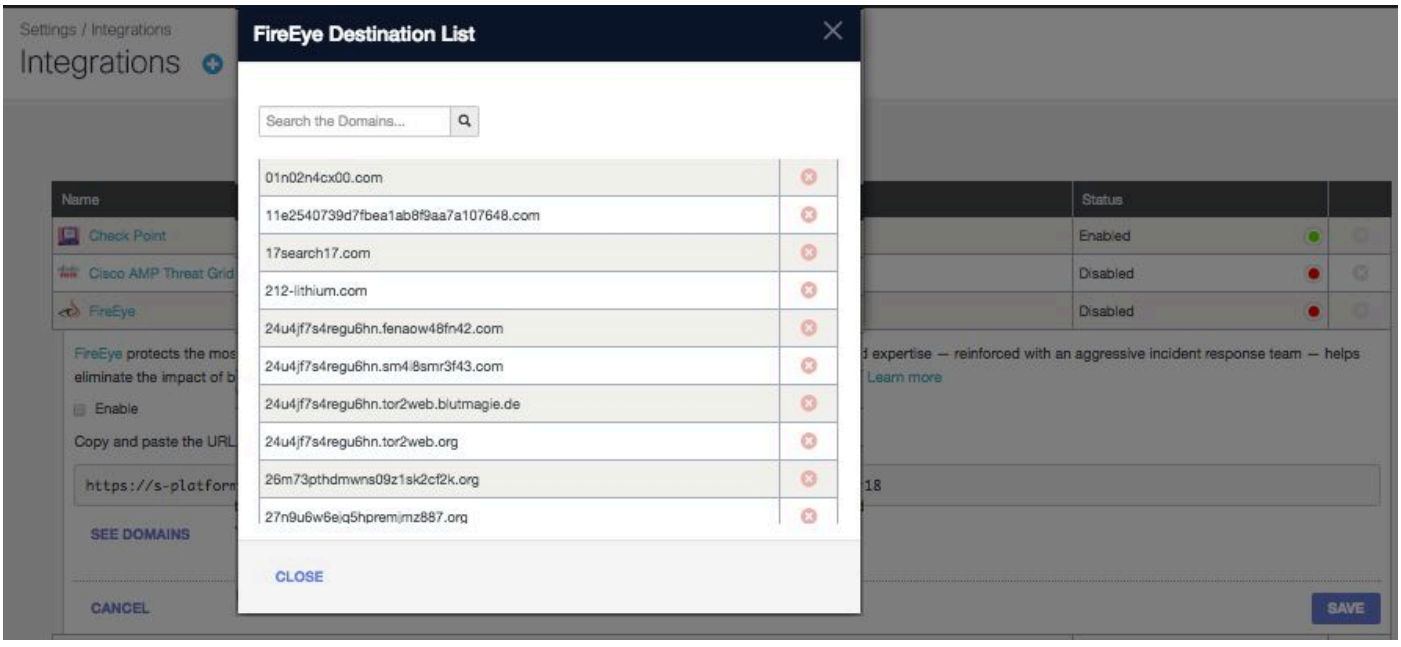
1. FireEye의 Test Fire(화재 테스트) 드롭다운에서 domain-match(도메인 일치)를 선택하고 Test Fire(화재 테스트)를 선택합니다.



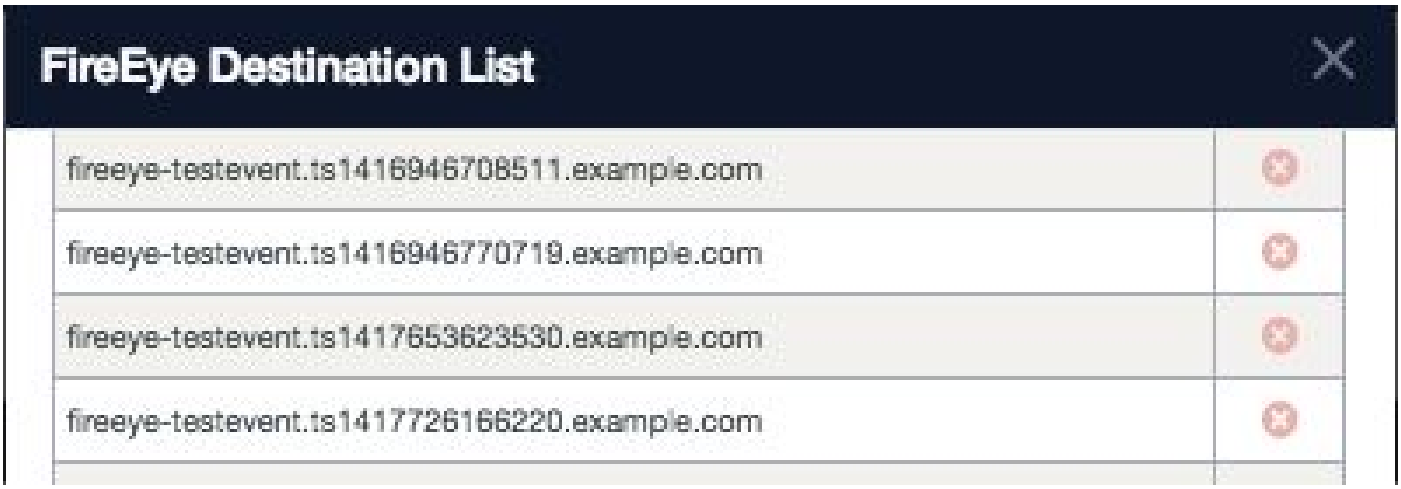
Cisco Umbrella에서 FireEye 통합에는 FireEye 어플라이언스에서 제공하는 도메인 목록이 포함되어 어떤 도메인이 현재 추가되고 있는지 확인할 수 있습니다.

2. Test Fire를 선택한 후 Cisco Umbrella에서 Settings(설정) > Integrations(통합)로 이동하고 테이블에서 FireEye를 선택하여 확장합니다.

3. 도메인 보기를 선택합니다.



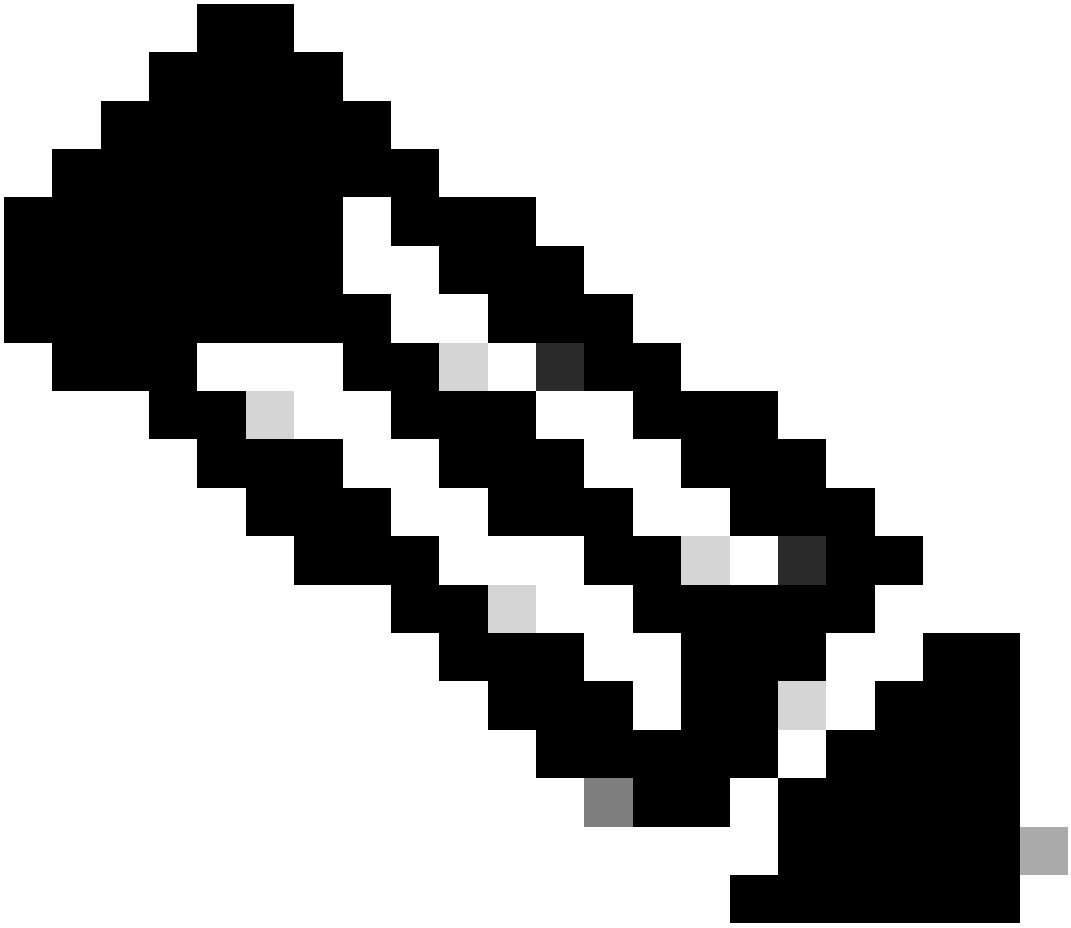
Fire 테스트를 선택하면 FireEye 대상 목록에서 "fireeye-testevent.example.com-[date]"라는 도메인이 생성됩니다. FireEye에서 Test Fire를 선택할 때마다 UNIX Epoch 시간 형식의 날짜가 테스트에 첨부된 고유 도메인이 생성되므로, 향후 테스트에서는 고유한 테스트 도메인 이름을 가질 수 있습니다.



Test Fire가 성공하면 FireEye의 더 많은 이벤트가 Cisco Umbrella로 전송되고 검색 가능한 목록이 채워져 증가하기 시작합니다.

"감사 모드"에서 FireEye 보안 설정에 추가된 이벤트 관찰

FireEye 어플라이언스의 이벤트는 FireEye 보안 카테고리로 정책에 적용할 수 있는 특정 대상 목록을 채우기 시작합니다. 기본적으로 대상 목록 및 보안 카테고리는 "감사 모드"에 있으며 어떤 정책에도 적용되지 않으며 기존 Cisco Umbrella 정책을 변경할 수 없습니다.



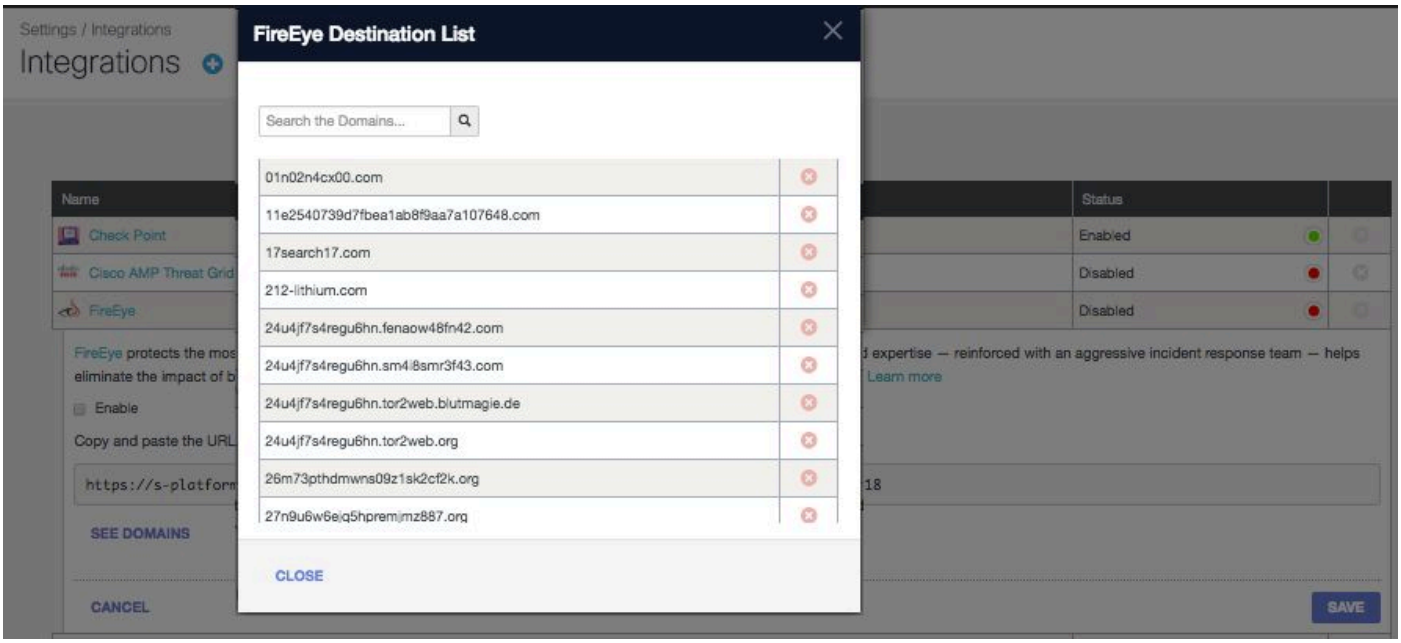
참고: "감사 모드"는 구축 프로파일 및 네트워크 컨피그레이션에 따라 얼마든지 활성화할 수 있습니다.

대상 목록 검토

언제든지 FireEye 대상 목록을 검토할 수 있습니다.

1. Policies(정책) > Policy Components(정책 구성 요소) > Integrations(통합)로 이동합니다.

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

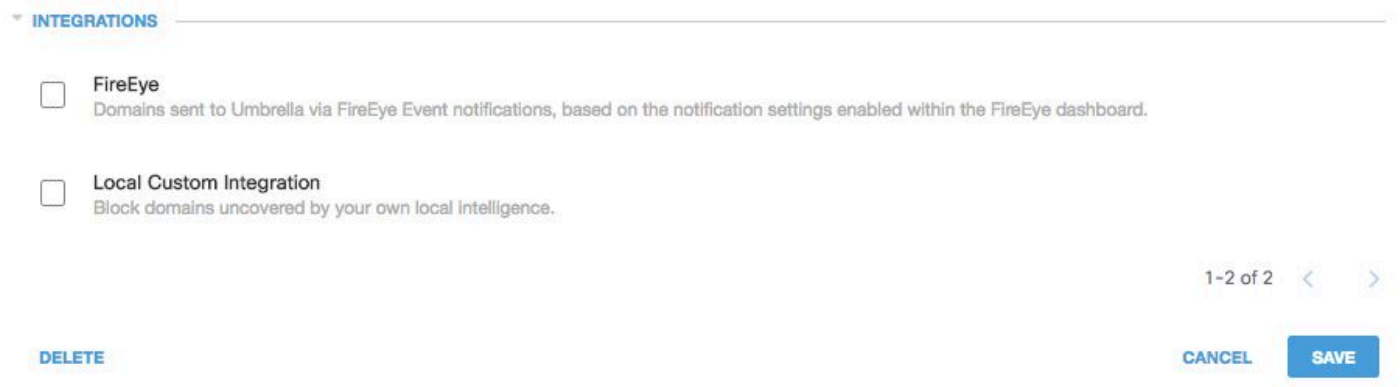


정책에 대한 보안 설정 검토

언제든지 정책에 추가할 수 있는 보안 설정을 검토할 수 있습니다.

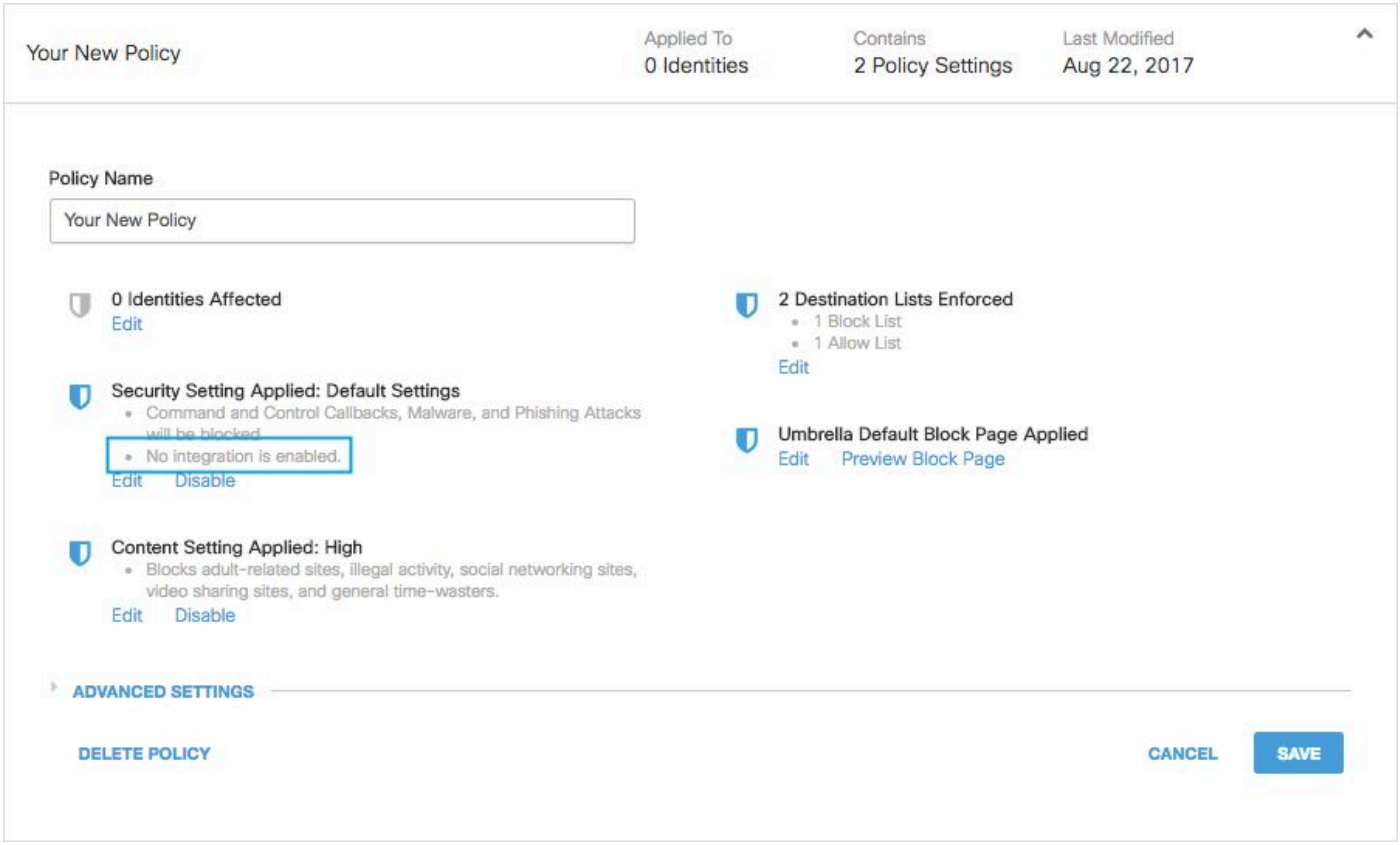
1. Policies(정책) > Policy Components(정책 구성 요소) > Security Settings(보안 설정)로 이동합니다.

2. 테이블에서 보안 설정을 선택하여 확장한 다음 통합으로 스크롤하여 FireEye 설정을 찾습니다.



115014080803

보안 설정 요약 페이지를 통해 통합 정보를 검토할 수도 있습니다.



115013920526

시작할 때 도메인이 "감사 모드"에서 올바르게 입력되도록 하려면 이 보안 설정을 지운 상태로 두는 것이 좋습니다.

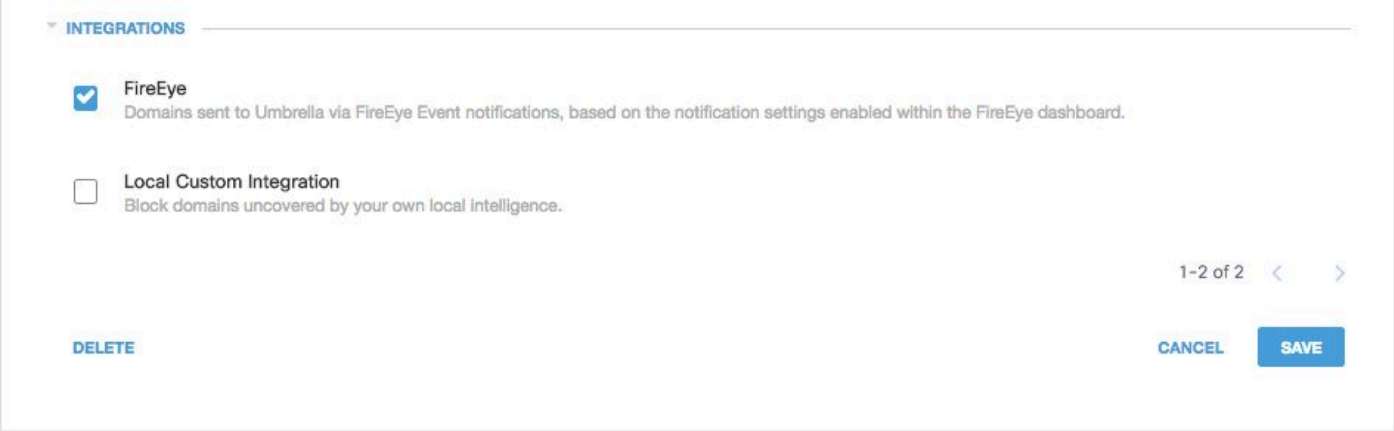
관리되는 클라이언트에 대한 정책에 "차단 모드"의 FireEye 보안 설정 적용

Cisco Umbrella에서 관리하는 클라이언트에 의해 이러한 추가 보안 위협이 시행될 준비가 되면 기존 정책의 보안 설정을 변경하거나 기본 정책 위에 있는 새 정책을 생성하여 해당 정책이 먼저 시행되도록 합니다.

먼저 보안 설정을 만들거나 업데이트합니다.

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

2. Integrations(통합) 아래에서 FireEye를 선택하고 Save(저장)를 선택합니다.



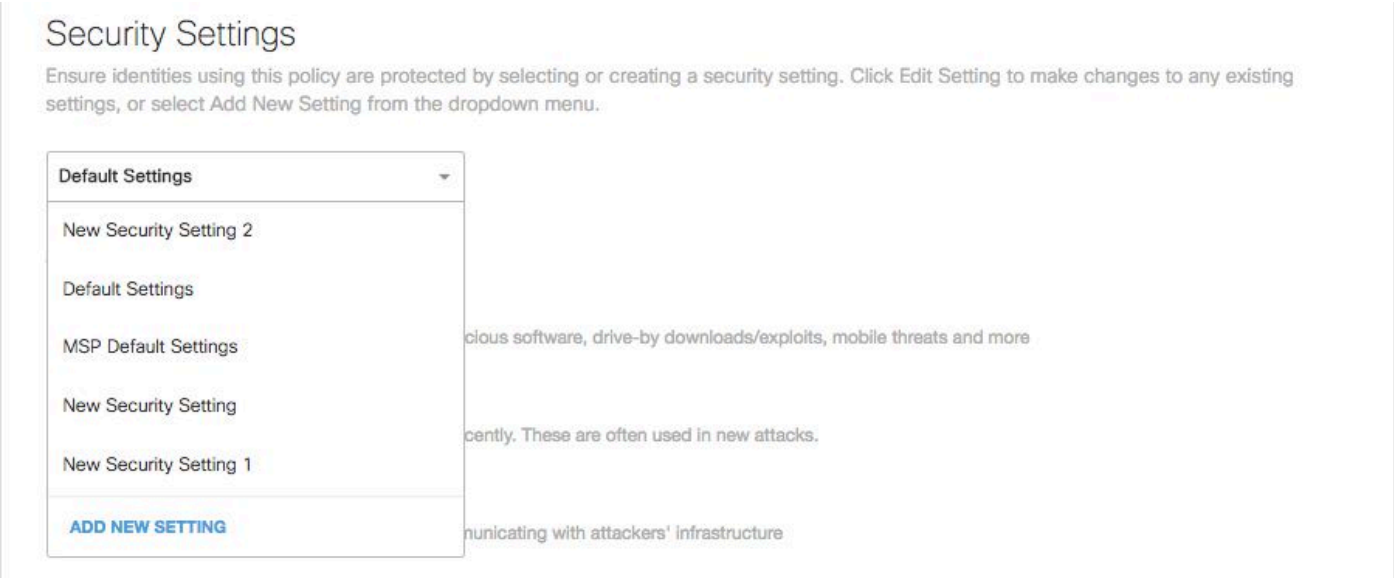
115013921406

그런 다음 정책 마법사에서 편집 중인 정책에 이 보안 설정을 추가합니다.

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

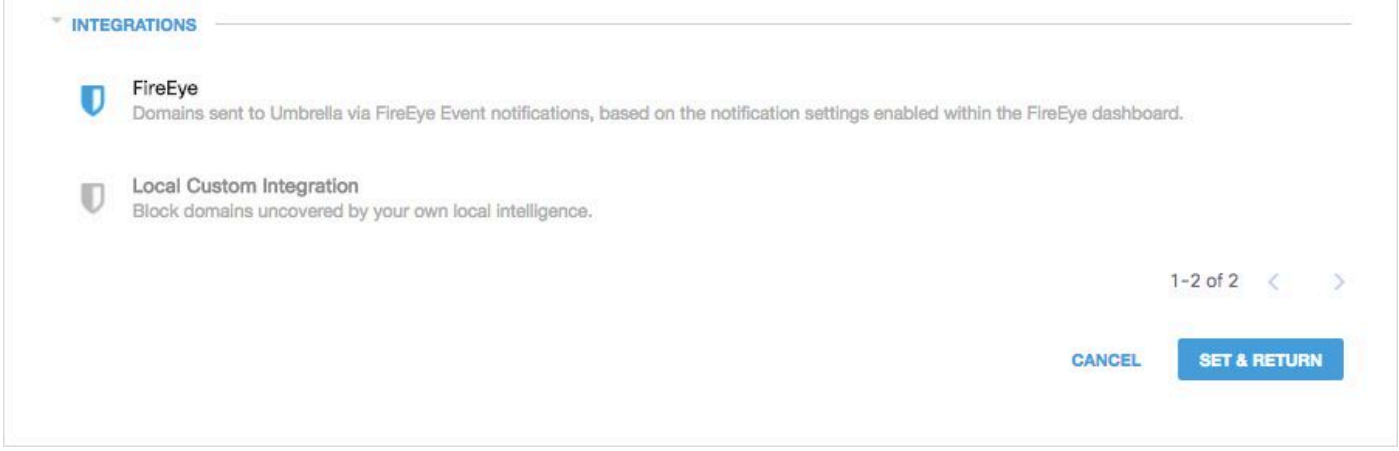
2. 정책을 확장하고 Security Setting Applied(보안 설정 적용됨)에서 Edit(편집)를 선택합니다.

3. Security Settings(보안 설정) 드롭다운에서 FireEye 설정이 포함된 보안 설정을 선택합니다.



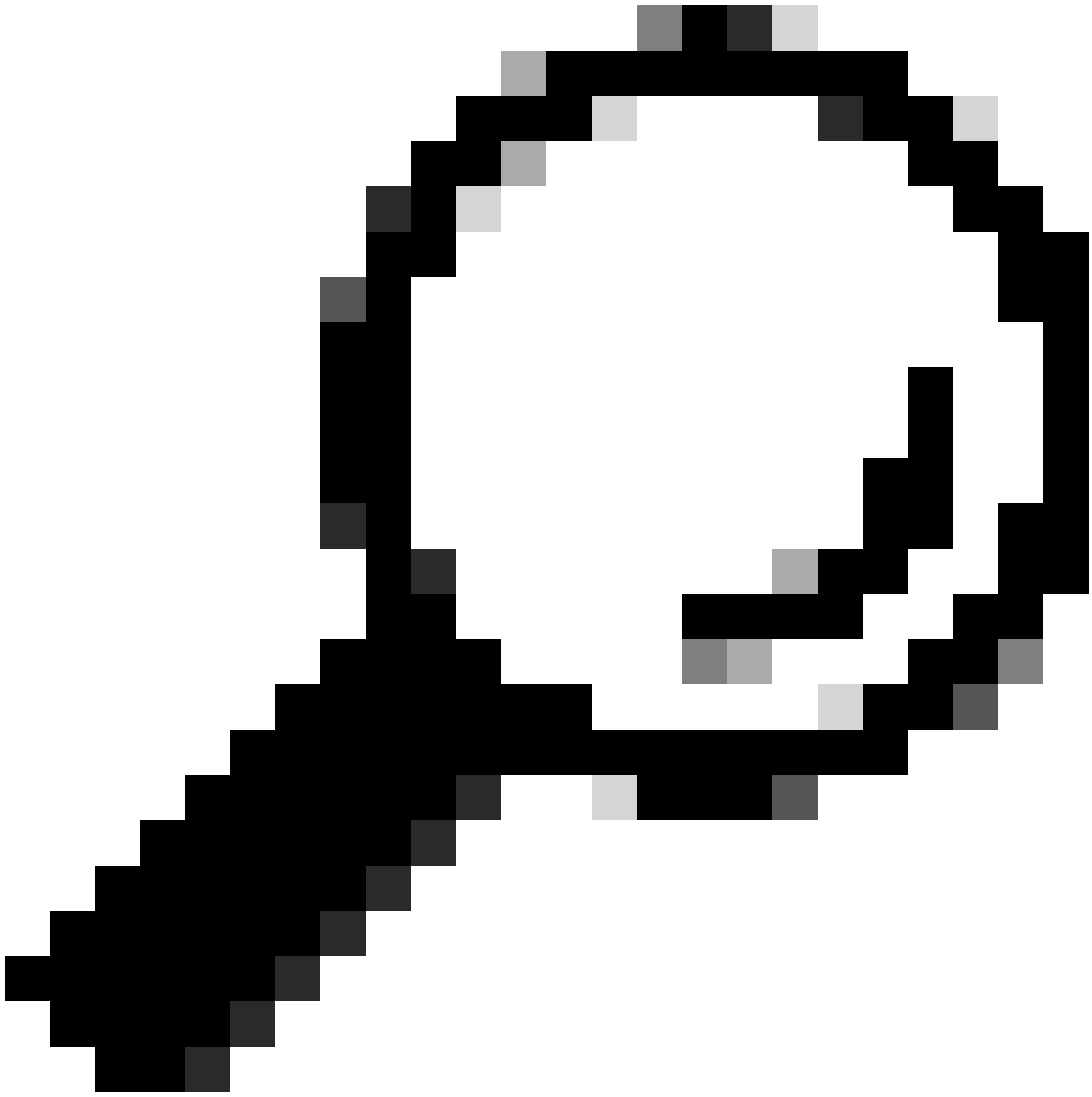
115014083083

Integrations(통합) 아래의 실드 아이콘이 파란색으로 업데이트됩니다.



115013922146

4. 설정 &Return을 선택합니다.



팁: 정책 마법사에서 보안 설정을 수정할 수도 있습니다.

FireEye의 보안 설정에 포함된 FireEye 도메인은 정책을 사용하는 ID에 대해 차단됩니다.

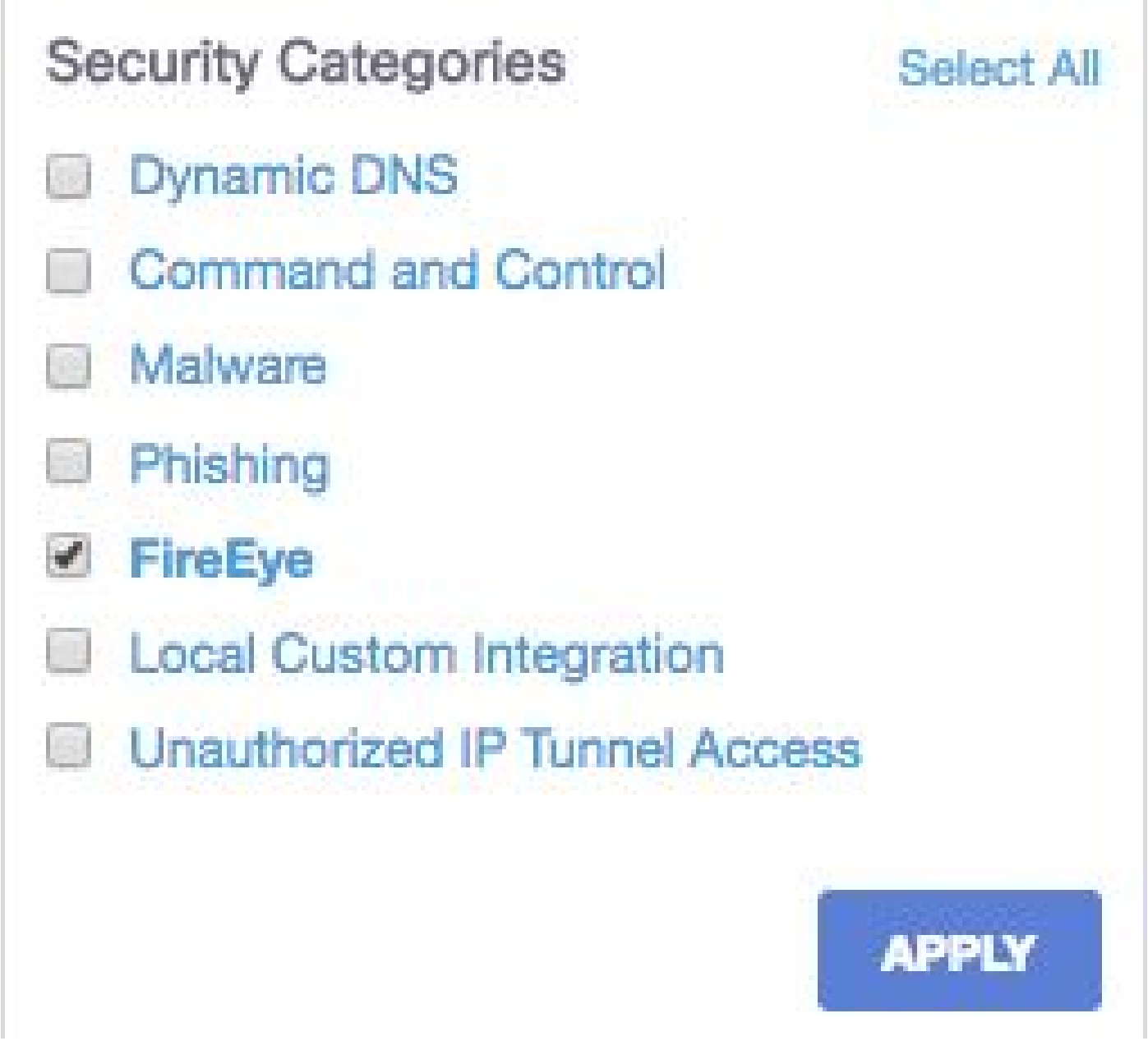
FireEye 이벤트를 위한 Cisco Umbrella 내의 보고

FireEye 보안 이벤트 보고

FireEye 대상 목록은 보고서에 사용할 수 있는 보안 범주 중 하나입니다. 보고서의 대부분 또는 모두가 보안 카테고리를 필터로 사용합니다. 예를 들어 보안 카테고리를 필터링하여 FireEye 관련 활동만 표시할 수 있습니다.

1. 보고 > 활동 검색으로 이동합니다.

2. Security Categories(보안 카테고리)에서 FireEye를 선택하여 FireEye에 대한 보안 카테고리만 표시하도록 보고서를 필터링합니다.



115013924986

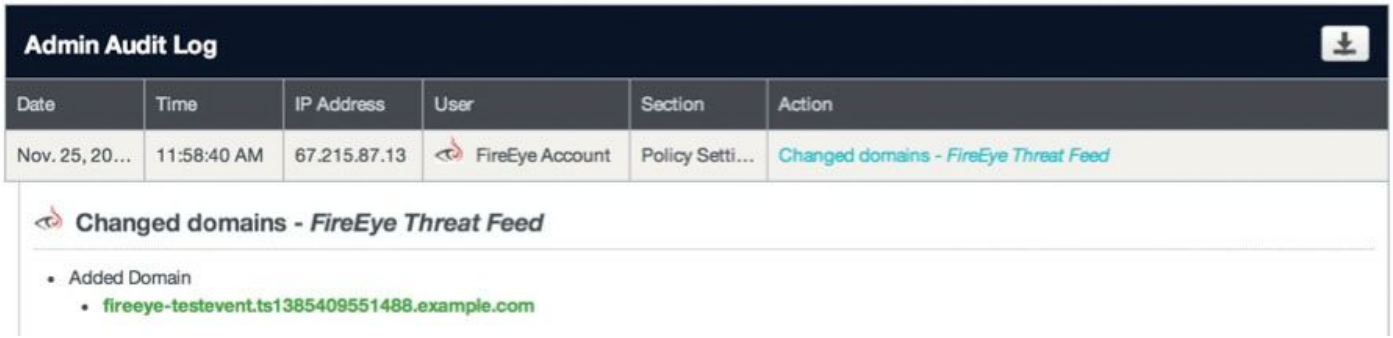
3. 적용을 선택하여 보고서에서 선택한 기간에 대한 FireEye 관련 활동을 확인합니다.

도메인이 FireEye 대상 목록에 추가된 시기 보고

관리 감사 로그에는 대상 목록에 도메인을 추가할 때 FireEye 어플라이언스의 이벤트가 포함됩니다. FireEye 로고가 브랜드화된 "FireEye Account"라는 사용자가 이벤트를 생성합니다. 이러한 이벤트에는 추가된 도메인 및 추가된 시간이 포함됩니다.

"FireEye Account(FireEye 어카운트)" 사용자에 대한 필터를 적용하여 FireEye 변경 사항만 포함하도록 필터링할 수 있습니다.

이전에 "Test Fire(테스트 실행)" 단계를 수행한 경우 FireEye 테스트 도메인을 추가하면 감사 로그에 나타날 수 있습니다.



원치 않는 탐지 또는 오탐 처리

허용 목록

FireEye 어플라이언스에 의해 자동으로 추가된 도메인은 경우에 따라 사용자가 특정 웹 사이트에 액세스하지 못하도록 차단하는 원치 않는 탐지를 트리거할 수 있습니다. 이와 같은 경우 Umbrella에서는 도메인을 허용 목록(Policies(정책) > Destination Lists(대상 목록))에 추가할 것을 권장합니다. 이는 보안 설정을 포함하여 다른 모든 유형의 차단 목록보다 우선합니다.

이러한 접근 방식이 바람직한 이유는 두 가지가 있다.

- 먼저, FireEye 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 FireEye 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) > 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.

FireEye 대상 목록에서 도메인 삭제

FireEye 대상 목록의 각 도메인 이름 옆에는 삭제 아이콘이 있습니다. 도메인을 삭제하면 원치 않는 탐지가 발생할 경우 FireEye 대상 목록을 정리할 수 있습니다.

그러나 FireEye 어플라이언스가 Cisco Umbrella에 도메인을 재전송하는 경우 삭제는 영구적이지 않습니다.

도메인을 삭제하려면

1. Settings(설정) > Integrations(통합)로 이동한 다음 "FireEye"를 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 Cisco Umbrella에서 즉시 허용 목록을 생성한 다음 FireEye 어플라이언스 내에서 오탐을 제거할 것을 권장합니다. 나중에 FireEye 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.