맞춤형 통합을 위한 Umbrella Enforcement API 이해

목차

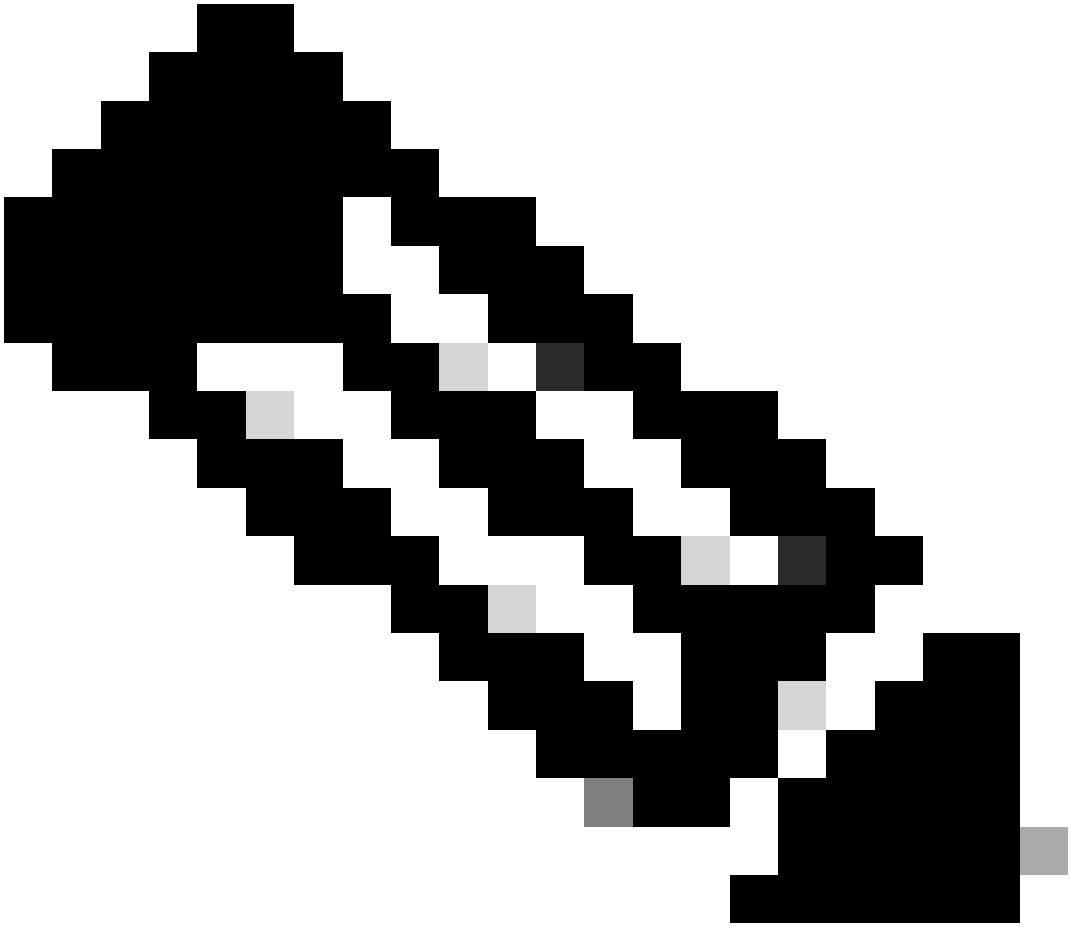
소개

이 문서에서는 맞춤형 통합을 위한 Umbrella Enforcement API에 대해 설명합니다.

Umbrella 시행 API란 무엇입니까?

Umbrella Enforcement API를 사용하면 자체 개발한 SIEM/TIP(Threat Intelligence Platform) 환경을 보유한 파트너와 고객이 이벤트 및/또는 위협 정보를 Umbrella 환경에 삽입할 수 있습니다. 그런 다음 이러한 이벤트는 경계 너머로 확장할 수 있는 가시성 및 시행으로 즉시 변환되고, 따라서 이러한 이벤트나 위협 인텔리전스를 생성했을 수 있는 시스템에 도달합니다.

Enforcement API는 이 API 설명서에 설명된 일반 이벤트 형식으로 이벤트를 수집할 수 있으며 ADD, DELETE 또는 LIST 함수를 지원할 수 있습니다.



참고: Umbrella 대시보드에 사용자 정의 통합을 위한 Umbrella Enforcement API가 없고 액세스 권한을 얻으려면 Cisco Umbrella 담당자에게 문의하십시오.

내가 왜 그걸 쓰겠어?

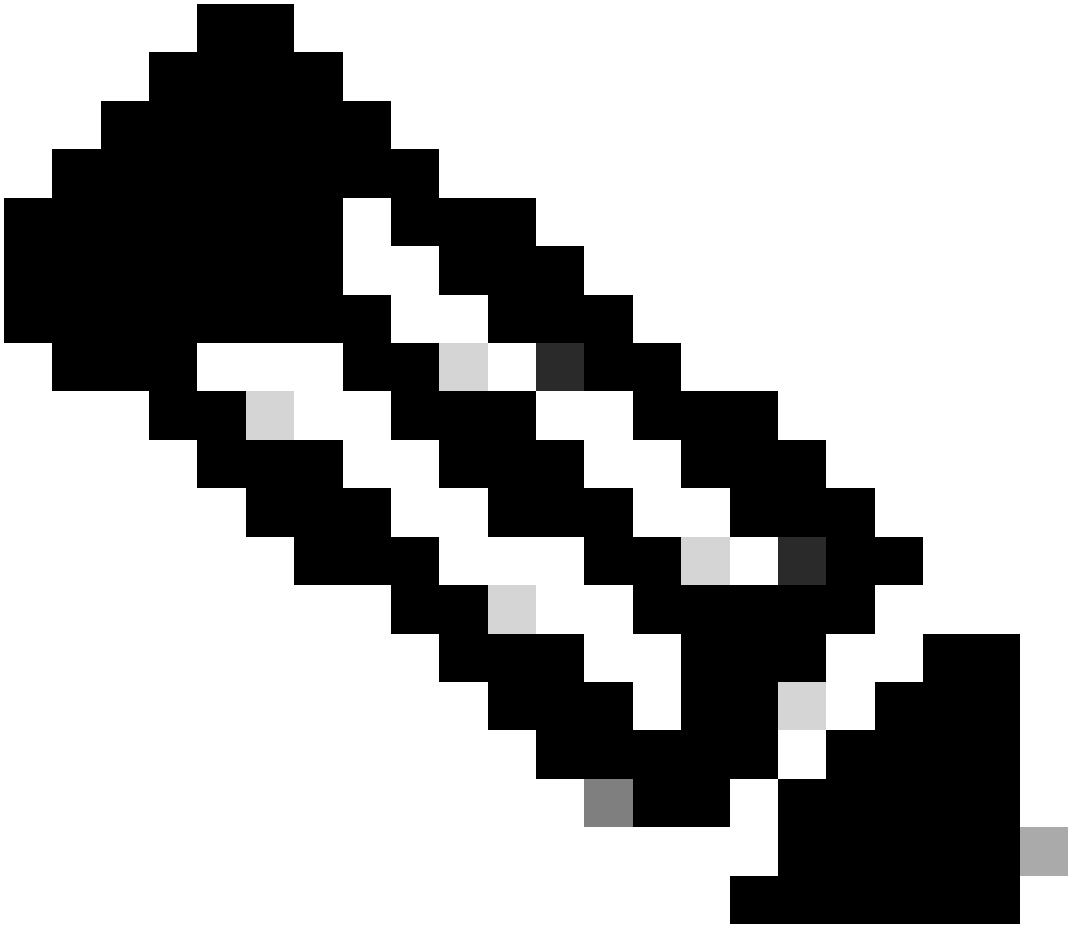
이미 자체 위협 인텔리전스 시스템과 프로세스를 처리, 관리 및 큐레이션하여 악의적이거나 의심스러운 도메인으로 식별된 도메인에 대한 조치를 취하고자 할 수 있습니다. 이 경우 시행 목적으로 Umbrella에 보호를 수동으로 추가하는 대신 이벤트를 작업(예: 보호로 변환)해야 한다고 결정하면 Enforcement API를 사용하여 이 프로세스를 자동화하고 이벤트와 관련된 도메인을 기반으로 즉시 보호를 적용할 수 있습니다.

따라서 보안 팀은 Umbrella의 지속적인 컨피그레이션보다는 조사에 시간과 노력을 집중할 수 있습니다. 보안 팀이 대상 목록을 업데이트하기 위해 Umbrella 대시보드로 이동할 필요 없이 툴과 프로세스에 머무를 수 있습니다. 기본적으로 API를 통해 직접 관리하는 외부 소스에서 Umbrella의 대상 목록을 생성한 다음 Umbrella 내의 ID에 대해 해당 대상을 차단하도록 선택할 수 있습니다.

어떻게 사용해야 합니까?

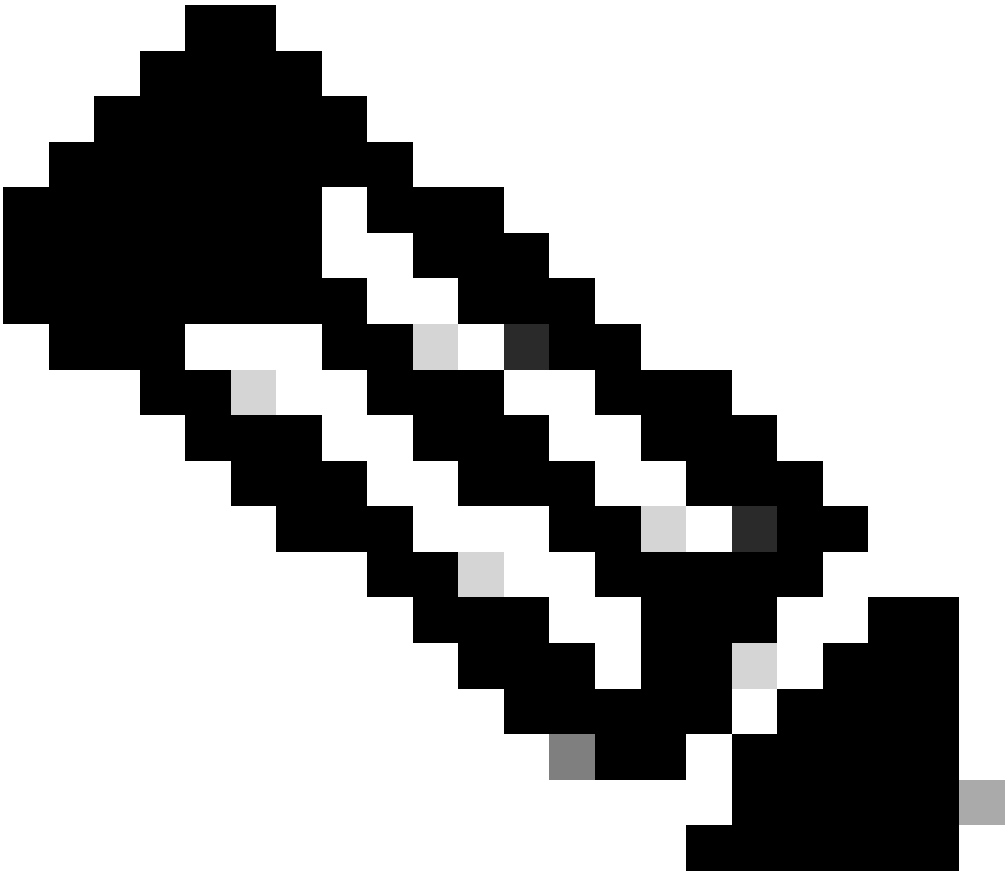
시행 API에 이벤트 추가

이벤트가 추가되면 시행에서는 이벤트에서 도메인을 추출하려고 시도합니다.



참고: 향후 IP 주소 및 URL에 대한 지원이 추가됩니다.

- 이벤트에는 원하는 양의 원본 이벤트 세부 정보가 포함될 수 있지만 API 설명서에 설명된 사양을 따라야 합니다.



참고: Umbrella 대시보드 내의 이벤트 세부사항 표출 지원은 향후 추가될 수 있습니다
.

- 도메인이 추출되면 Cisco Umbrella 보안 그래프에서 검증하여 오탐이 발생하거나 Cisco Umbrella 보안 그래프에서 악성으로 간주할 수 있는 알려진 양호한 도메인이 아닌지 확인합니다.
- 검증에 성공한 경우(예: 알 수 없고 차단해도 안전함), 해당 사용자 정의 통합과 연결된 대상 목록에 추가되고 Umbrella 대시보드 내에 사용자 정의 보안 카테고리로 표시됩니다.
- 사용자 지정 보안 카테고리는 정책별로 차단하거나 허용하여 의심스러운 요청의 적극적인 시행 또는 패시브 "감사"를 모두 허용할 수 있습니다.

시행 API 목록에 대한 도메인 나열

- 이전에 삽입된 이벤트로 인해 차단된 도메인의 차단 해제를 워크플로에 포함할 경우, LIST 요청은 해당 통합과 관련된 대상 목록에 현재 포함된 모든 도메인을 제공합니다.

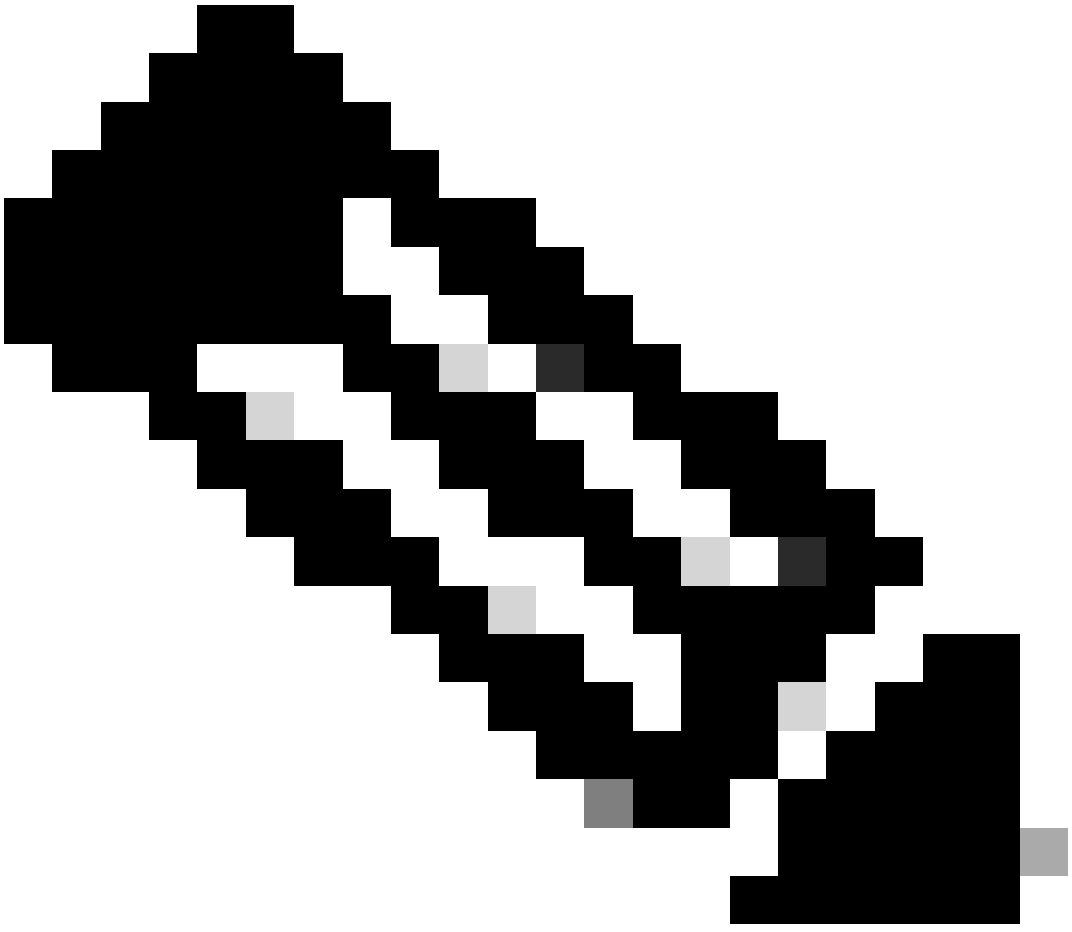
시행 API 목록에서 도메인 삭제

- 이전에 삽입된 이벤트로 인해 차단된 도메인의 차단 해제를 워크플로에 포함할 경우, DELETE 요청을 통해 해당 통합과 관련된 대상 목록에서 도메인을 제거할 수 있습니다.
- Umbrella ID 중 하나에서 오는 수신 DNS 요청이 사용자 지정 통합 대상 목록의 도메인으로 향하는 경우, 이를 트리거한 정책과 연결된 사용자 지정 통합의 보안 설정에 따라 차단되거나 허용됩니다.
- 결과는 활동 검색을 통해 또는 S3 통합을 사용하는 Amazon S3를 통해 액세스할 수 있는 다른 모든 Umbrella 이벤트와 함께 기록됩니다. 따라서 맞춤형 통합과 관련된 트래픽은 선택적으로 SIEM/TIP로 다시 수집될 수 있으며 피드백 루프는 닫힙니다.

시행 API 사용에 대한 설명

1단계: 사용자 정의 통합 생성

한 번에 최대 10개의 사용자 지정 통합을 가질 수 있습니다.



참고: 조직이 Umbrella MSP, MSSP 또는 MOC의 하위 조직인 경우 콘솔 레벨에서 공유되

는 사용자 정의 통합은 하위 조직 레벨에서 생성된 통합보다 먼저 표시됩니다.

1. Umbrella에서 Policies(정책) > Policy Components(정책 구성 요소) > Integrations(통합)로 이동하고 Add(추가)를 클릭합니다.
2. 사용자 정의 통합의 이름을 추가하고 Create(생성)를 클릭합니다.
3. 새 사용자 지정 통합을 확장하고 Enable(활성화)을 선택한 다음 통합 URL을 복사하고 Save(저장)를 클릭합니다.

2단계: 사용자 지정 스크립트를 만듭니다.

1. 이 문서의 부록에서 generate_event 및 delete_domain 샘플 스크립트를 참조하거나 API 설명서를 사용하여 자체 스크립트를 만들어 이벤트 생성, 도메인 삭제 또는 나열에 대한 올바른 형식의 요청을 생성합니다. 앞으로 이러한 스크립트에서 사용자 지정 통합 URL을 사용할 수 있습니다.

3단계: 샘플 이벤트 삽입

1. 생성한 스크립트를 사용하여 사용자 지정 통합에 이벤트를 삽입합니다. 이 예에서는 "creditcards.com" 도메인을 포함하는 이벤트를 삽입했습니다.

4단계: Umbrella 대시보드에서 대상 목록을 확인합니다.

1. Settings(설정) > Integrations(통합)로 돌아가서 테이블에서 사용자 정의 통합을 확장합니다.
2. See Domains(도메인 보기)를 클릭합니다. 추가된 도메인의 검색 가능한 목록이 나타나고 4단계의 샘플 이벤트가 목록에 표시됩니다.

5단계: Admin Audit Log를 선택합니다.

1. 사용자 정의 통합과 관련된 활동을 확인하는 또 다른 방법은 관리자 감사 로그를 검토하는 것입니다.
2. Reporting(보고) > Admin Audit Log(관리자 감사 로그)로 이동합니다.
3. Filters(필터)에서 Filter by Identities & Settings(ID 및 설정 기준 필터)에 사용자 지정 통합의 이름을 입력한 다음 Run Filter(필터 실행)를 클릭합니다.

항목을 확장하면 샘플 이벤트(creditcards.com)가 사용자 지정 통합에 추가된 이벤트가 표시됩니다.

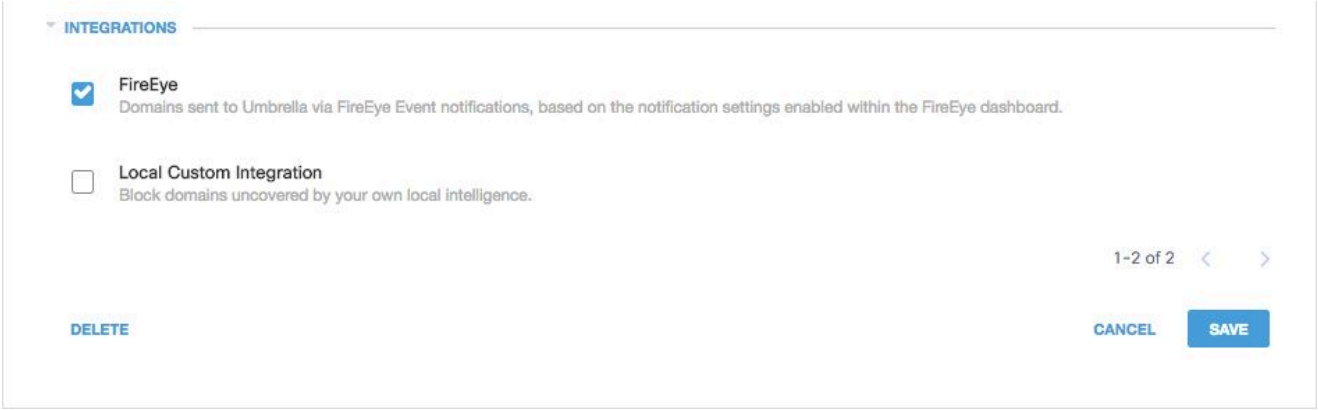
선택적 단계: 도메인 나열 또는 삭제

또한 사용자 지정 통합에서 도메인을 나열할 수 있는지 확인하고 도메인에 대해 더 이상 적용하거나 통합에서 보유하지 않으려는 경우 도메인을 삭제할 수 있는지 테스트할 수도 있습니다. API 설명서에 설명된 단계에 따라 도메인을 나열하고 삭제할 수 있습니다.

보안 설정 구성

이벤트를 삽입하고 선택적으로 도메인을 나열 및 삭제할 수 있음을 확인했으므로 사용자 지정 통합의 보안 카테고리에 있는 도메인으로 향하는 ID에서 DNS 요청에 대해 수행할 작업을 구성할 수 있습니다.

1. Policies(정책) > Security Settings(보안 설정)로 이동하고 Integrations(통합)에서 활성화된 통합(이 예에서는 FireEye)을 확인하고 Save(저장)를 클릭합니다.

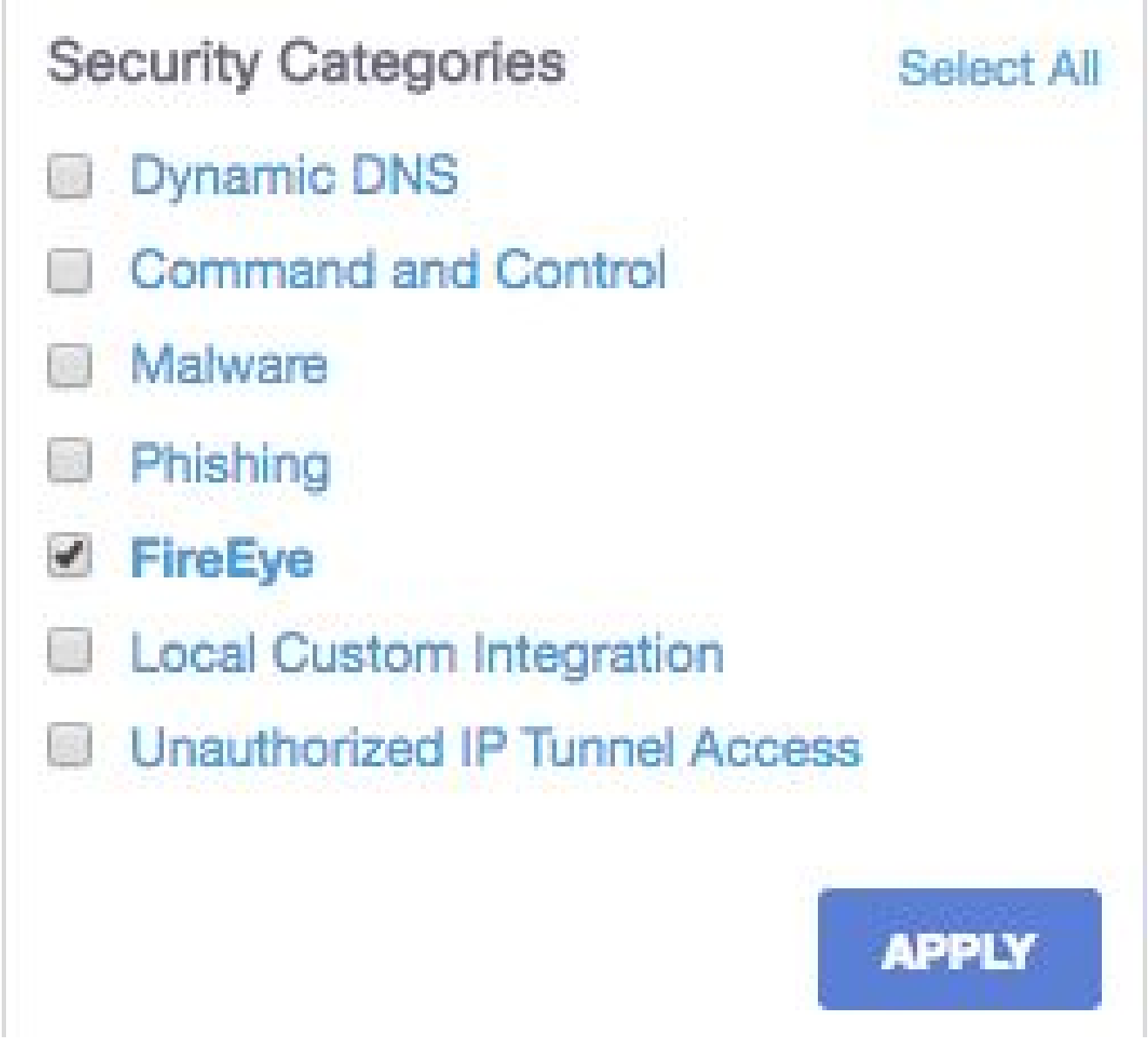


115014145103

사용자 정의 통합에 대한 보고 보기

사용자 지정 통합의 도메인으로 향하는 ID(예: 네트워크 또는 로밍 컴퓨터) 중 하나에서 DNS 요청을 생성합니다(이 예에서는 "creditcards.com"). 클라이언트의 관점에서 볼 때, 이제 보안 설정을 구성한 방법에 따라 적절한 차단 또는 허용 결과가 표시됩니다.

1. Reporting(보고) > Activity Search(활동 검색)로 이동하고 Security Categories(보안 카테고리)에서 사용자 정의 통합(이 예에서는 FireEye)을 선택하여 FireEye에 대한 보안 카테고리만 표시하도록 보고서를 필터링합니다.

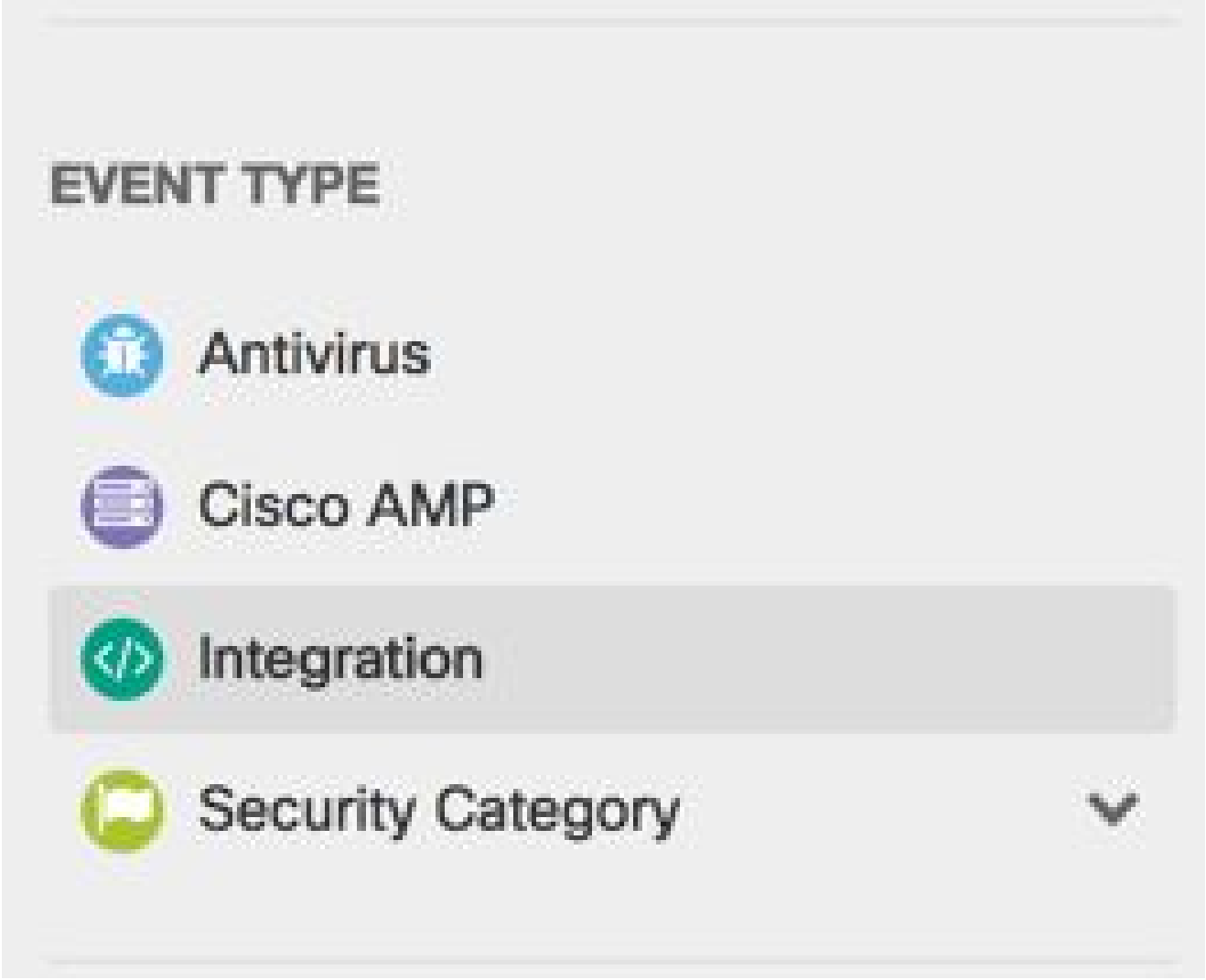


115013981706

2. Apply(적용)를 클릭하여 보고서에서 선택한 기간의 활동을 확인합니다.

또한 Activity Volume(활동 볼륨) 보고서를 보고 맞춤형 통합을 비롯한 스냅샷 또는 시간별 추세 집계 보고서를 볼 수 있습니다.

1. Reporting(보고) > Security Activity Volume(보안 활동 볼륨)으로 이동합니다.
2. Event Type(이벤트 유형) 아래에서 Integration(통합)을 선택합니다.



115013982286

로그 저장 및 사용을 위한 S3 통합 구성(선택 사항)

그런 다음 환경에 대한 모든 요청이 포함된 Umbrella 로그를 SIEM/TIP 환경으로 다시 제공하려는 경우 S3 통합을 사용하면 DNS 활동 이벤트를 다시 스트리밍할 수 있습니다.

부록: 스크립트 예

이러한 perl 스크립트는 사용자 정의 통합을 위해 이벤트를 생성하는 방법에 대한 지침을 제공합니다. 두 스크립트의 통합에서 customerKey 값을 대체하십시오. 이러한 스크립트는 예로 제공되며 사용자 지정 또는 업데이트가 필요할 수 있습니다.

generate_event.pl:

```
#!/usr/bin/perl -w
```

```
# Custom integration - ADD EVENT URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/events?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $json_blob = "{
    \"alertTime\" : \"2013-02-08T11:14:26.0Z\",
    \"deviceId\" : \"ba6a59f4-e692-4724-ba36-c28132c761de\",
    \"deviceVersion\" : \"13.7a\",
    \"dstDomain\" : \"$domain\",
    \"dstUrl\" : \"http://$domain/a-bad-url\",
    \"eventTime\" : \"2013-02-08T09:30:26.0Z\",
    \"protocolVersion\" : \"1.0a\",
    \"providerName\" : \"Security Platform\"
}";

my $curl_request = "curl '" . $cust_key . "' -v -X POST -H 'Content-Type: application/json' -d '" . $js

my $results = exec($curl_request);
```

delete_domain.pl:

```
#!/usr/bin/perl -w

# Custom integration - DELETE URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/domains?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $curl_request = "curl '" . $cust_key . "&where[name]=" . $domain . "' -v -i -g -X DELETE -H 'Content
my $results = exec($curl_request);
```

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.