了解适用于自定义集成的保护伞实施API

目录

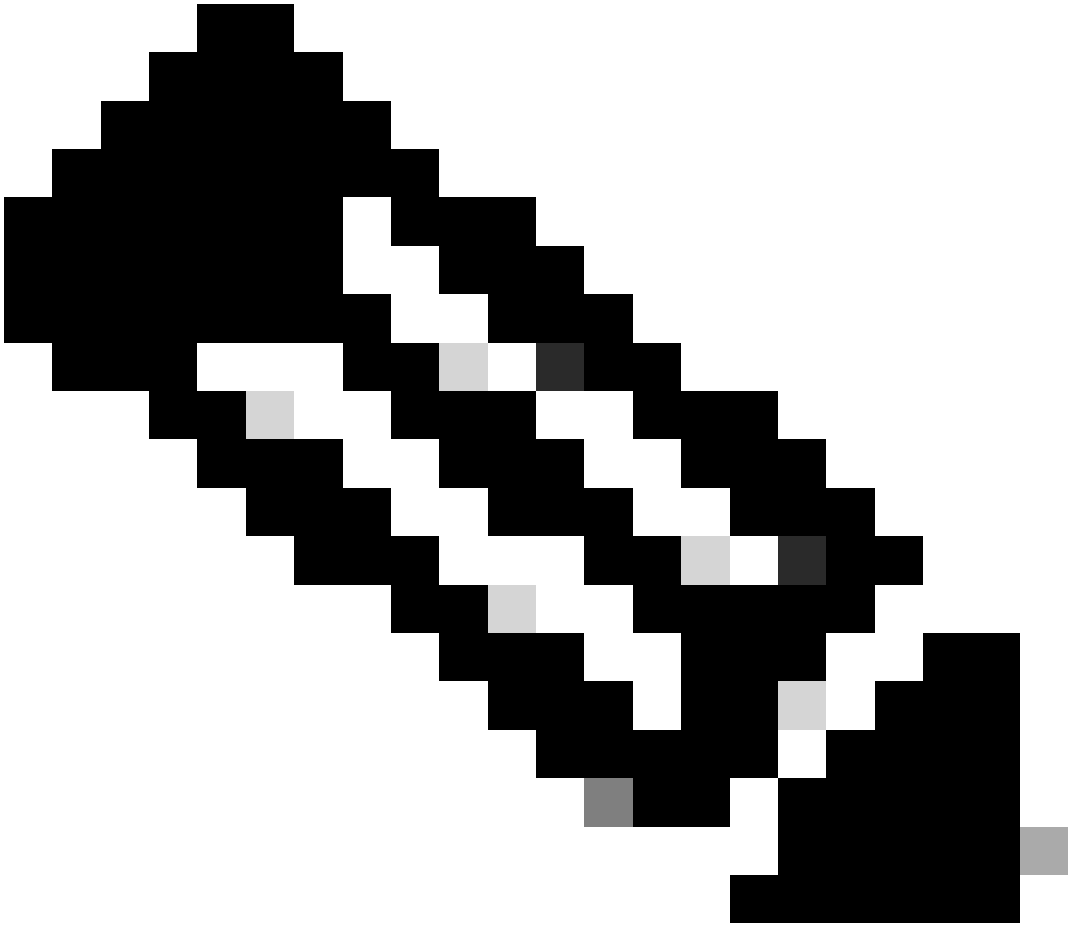
简介

本文档介绍用于自定义集成的Umbrella Enforcement API。

什么是Umbrella Enforcement API?

Umbrella Enforcement API允许合作伙伴和拥有自己自主开发的SIEM/威胁情报平台(TIP)环境的客户将事件和/或威胁情报注入其Umbrella环境中。然后，这些事件会立即转换为可视性和强制性，从而扩展到边界之外，进而扩展到可能生成这些事件或威胁情报的系统。

实施API可以采用此API文档中描述的通用事件格式接收事件，并可支持ADD、DELETE或LIST函数。



注意：如果您的Umbrella控制面板中没有用于自定义集成的Umbrella实施API，并且希望拥有访问权限，请与您的Cisco Umbrella代表联系。

我为什么要用它？

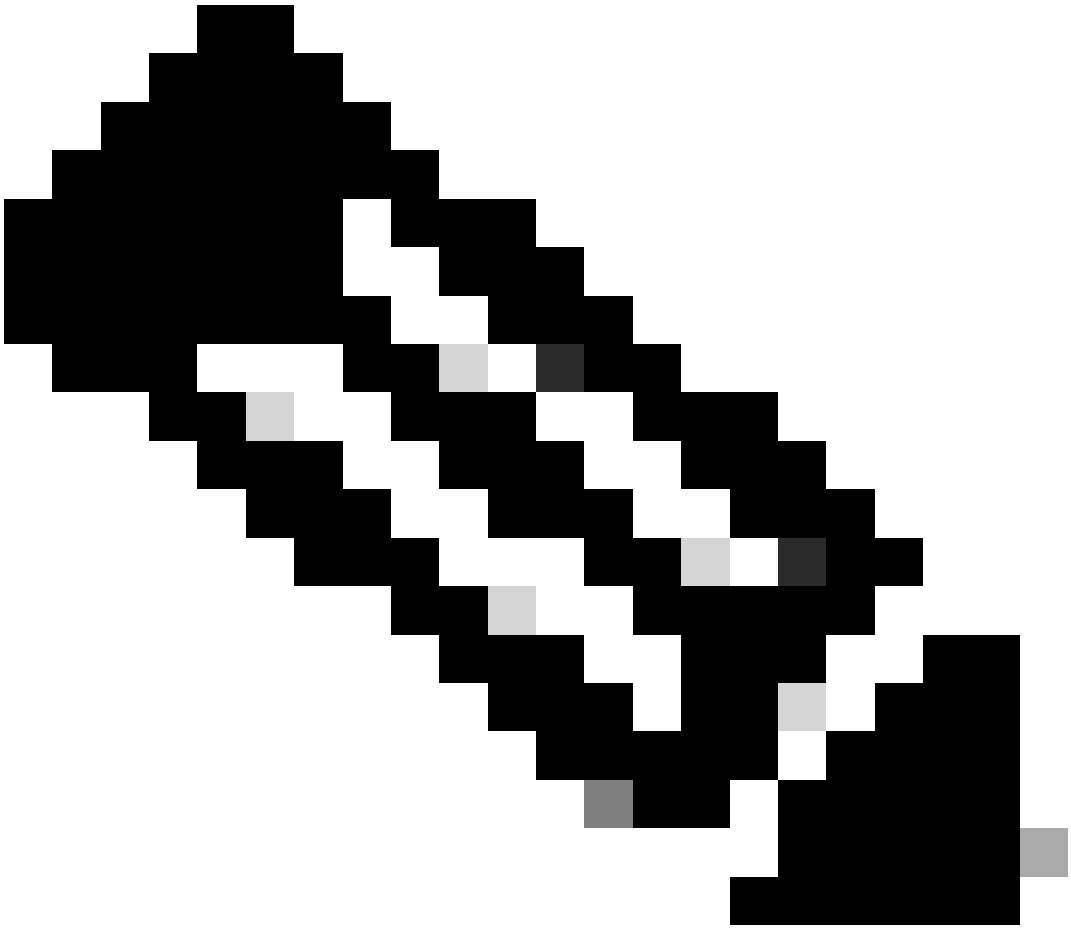
您可能已经处理、管理和创建自己的威胁情报系统和流程，从而产生对识别为恶意或可疑的域采取措施的愿望。在这种情况下，一旦决定需要对事件执行操作（例如，将其转换为保护），而不是出于实施目的手动向Umbrella添加保护，您就可以使用实施API自动化此过程并根据与事件关联的域立即实施保护。

这样，您的安全团队可以将时间和精力集中在调查上，而不是持续配置Umbrella。它使您的安全团队能够保持其工具和流程不变，而不必跳到Umbrella控制面板来更新目标列表。实质上，您可以从Umbrella中创建一个目标列表，该列表来自您通过API直接管理的外部源，然后选择阻止这些目标以查找Umbrella中的身份。

如何使用？

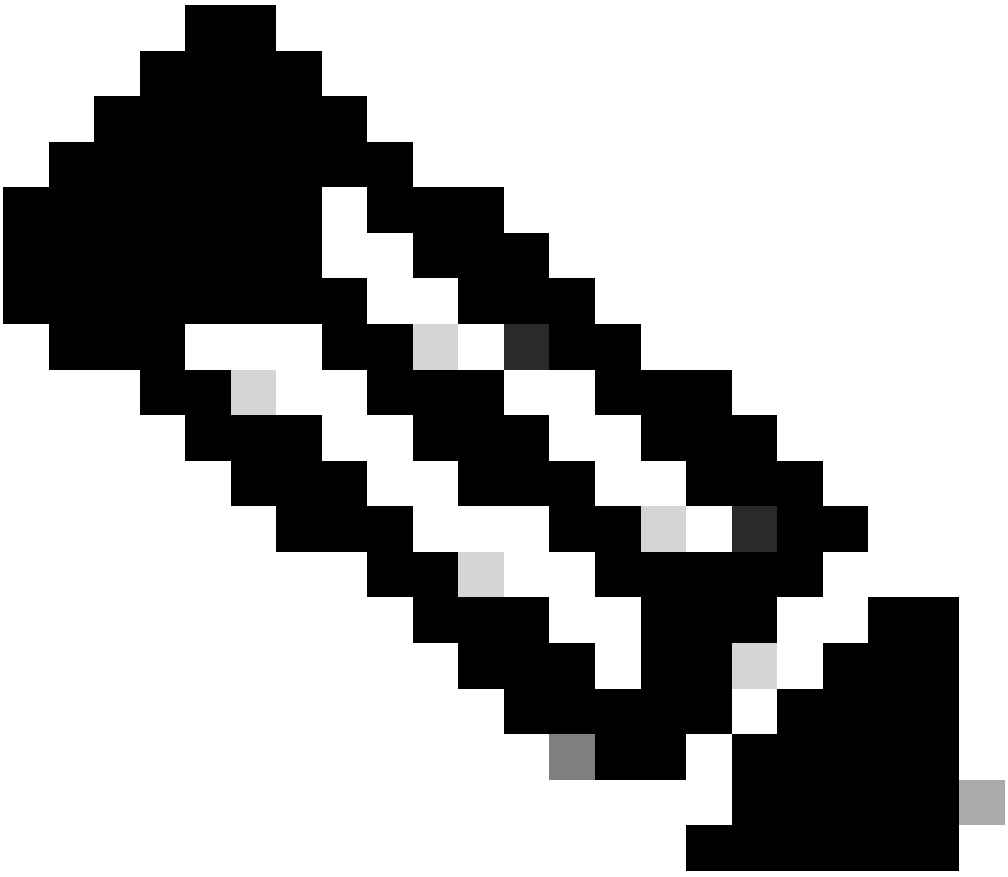
将事件添加到实施API

添加事件后，实施会尝试从事件中提取域。



注意：未来将增加对IP地址和URL的支持。

- 事件可以包含任何您想要的原始事件详细信息，但是必须遵守该API文档中描述的规范。



注意：将来可能会在Umbrella控制面板中添加对表面事件详细信息的支持。

- 如果提取了某个域，则通过Cisco Umbrella安全图对其进行验证，以确保该域不是已知正常的域，否则可能会导致误报，或者已被思科Umbrella安全图视为恶意域。
- 如果它通过验证（例如，它不可知且可以安全阻止），则会将其添加到与该自定义集成关联的目标列表，并在Umbrella控制面板中显示为自定义安全类别。
- 可以基于每个策略阻止或允许自定义安全类别，以允许对可疑请求进行主动实施或被动的“审核”。

实施API列表的列表域

- 如果工作流程包括取消阻止由于以前注入的事件而被阻止的域，LIST请求会提供当前包括在与该集成相关联的目标列表中的所有域。

从实施API列表中删除域

- 如果工作流程包括取消阻止由于以前注入的事件而被阻止的域，则DELETE请求允许您从与该

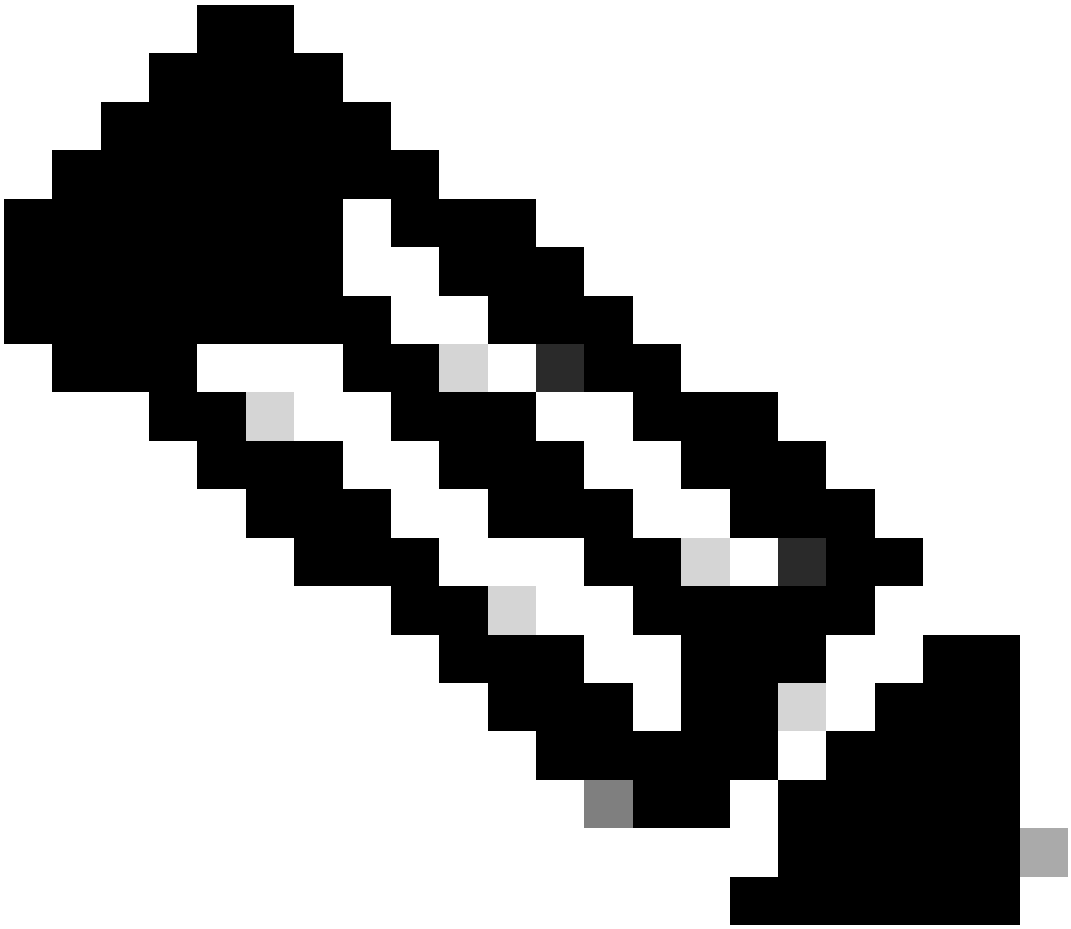
集成相关联的目标列表中删除域。

- 如果来自某个Umbrella标识的传入DNS请求发往自定义集成目标列表中的域，则根据与触发该请求的策略关联的自定义集成的安全设置阻止或允许该请求。
- 结果将连同所有其他Umbrella事件一起记录，可通过活动搜索或使用S3集成的Amazon S3访问。因此，与自定义集成关联的流量可以选择性地重新被吸回到您的SIEM/TIP并关闭反馈循环。

使用实施API的演练

步骤 1：创建自定义集成

一次最多可以有10个自定义集成。



注意：如果组织是Umbrella MSP、MSSP或MOC的子组织，则在子组织级别创建集成之前，将显示从控制台级别共享的自定义集成。

1. 在Umbrella中，导航到Policies > Policy Components > Integrations，然后单击Add。
2. 添加自定义集成的名称，然后单击Create。
3. 展开新的自定义集成，选中Enable，复制集成URL，然后单击Save。

步骤 2：创建自定义脚本。

1. 请参阅本文档附录中的generate_event和delete_domain示例脚本，或使用API文档创建自己的脚本，为生成事件、删除域或列出域生成格式正确的请求。接下来您需要在这些脚本中使用自定义集成URL。

步骤 3：注入示例事件

1. 使用您创建的脚本将事件插入到自定义集成中。在我们的示例中，我们注入了一个包含域“creditcards.com”的事件。

步骤 4：检查Umbrella控制面板中的目标列表

1. 返回Settings > Integrations，并在表中展开自定义集成。
2. 单击See Domains。系统将显示已添加域的可搜索列表，并且您在第4步中的示例事件现在已在该列表中。

步骤 5：检查管理员审核日志。

1. 另一种验证与自定义集成关联的活动的方法是查看管理员审核日志。
2. 导航到报告>管理员审核日志。
3. 在Filters下，在Filter by Identities & Settings中输入自定义集成的名称，然后单击Run Filter。

展开条目时，您现在会看到导致示例事件(creditcards.com)添加到自定义集成中的事件。

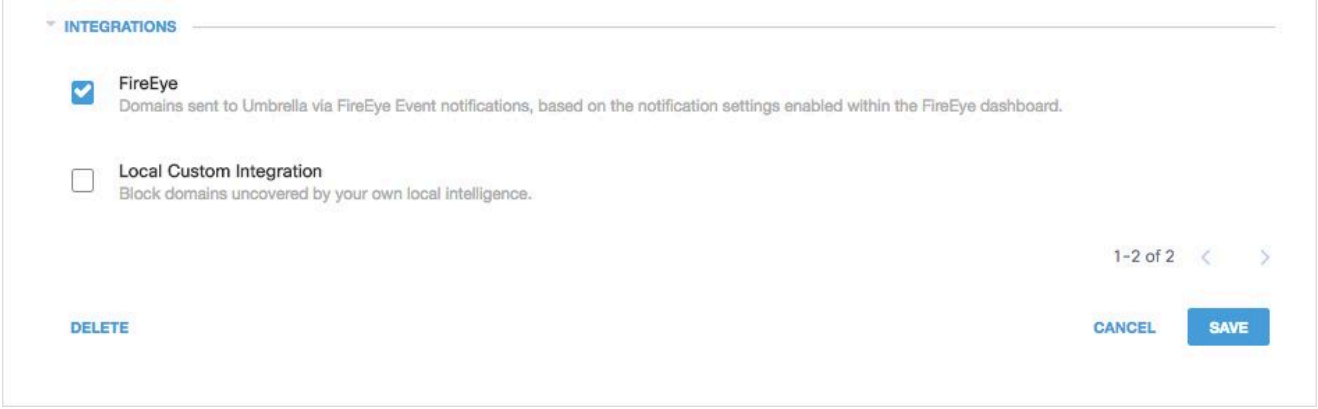
可选步骤：列出或删除域

您可能还希望进行测试，以确保在自定义集成中列出域并删除域，以免您不再想强制执行该域或在集成中将其删除。使用API文档中概述的步骤来列出和删除域。

配置安全设置

现在，您已验证可以插入事件（或者可以列出和删除域），您可以从您的身份配置要发送到自定义集成的安全类别中的域的DNS请求所发生的情况。

1. 导航到Policies > Security Settings，在Integrations下，检查已启用的集成（在本例中为FireEye），然后单击Save。

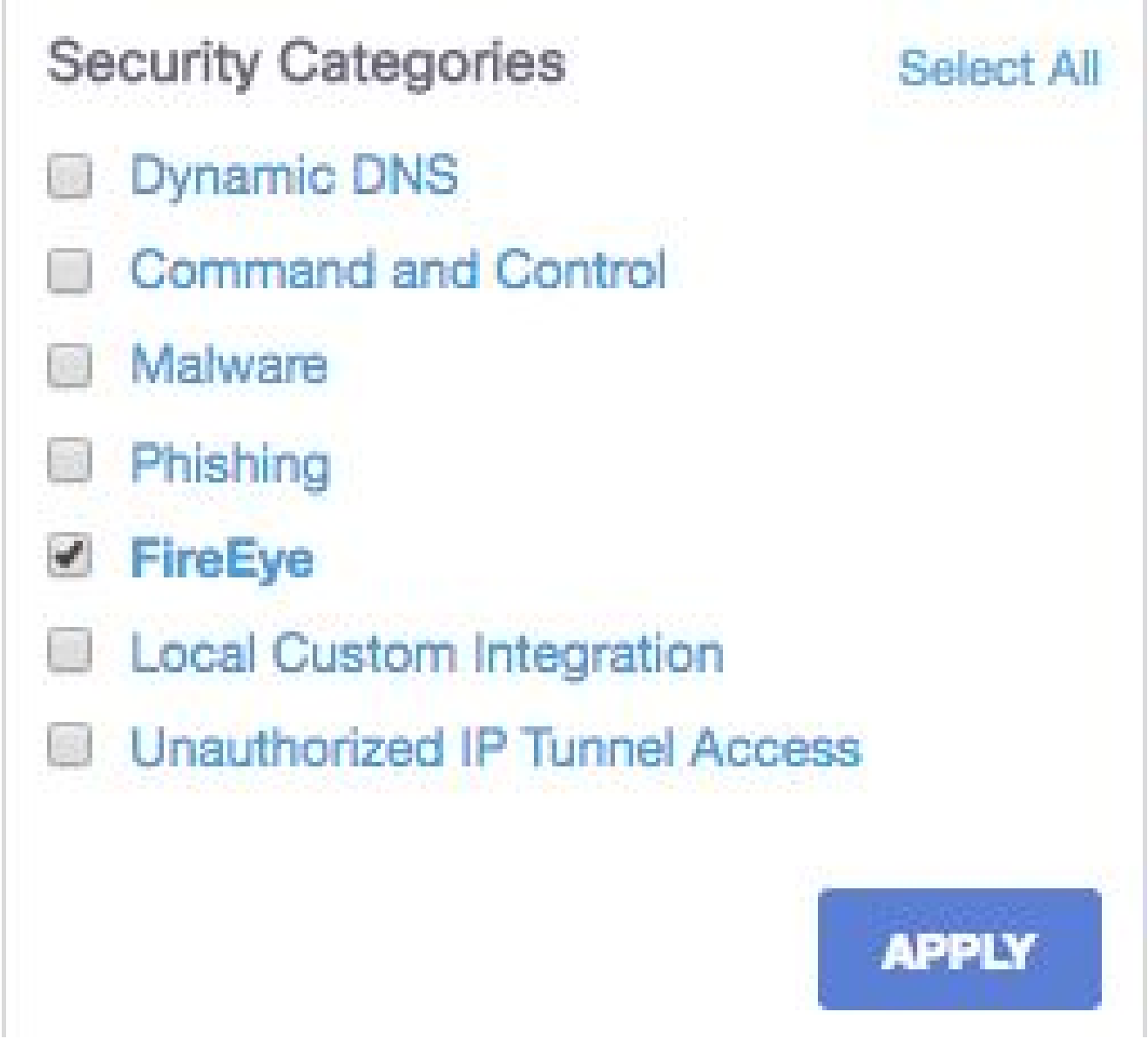


115014145103

查看自定义集成的报告

从您的身份之一（例如，网络或漫游计算机）生成发往自定义集成中的域（示例中为“creditcards.com”）的DNS请求。 从客户端的角度来看，您现在会看到相应的阻止或允许结果，具体取决于您如何配置安全设置。

1. 导航到报告>活动搜索，在安全类别下，选择自定义集成（在本示例中为FireEye）以过滤报告，以便只显示FireEye的安全类别。

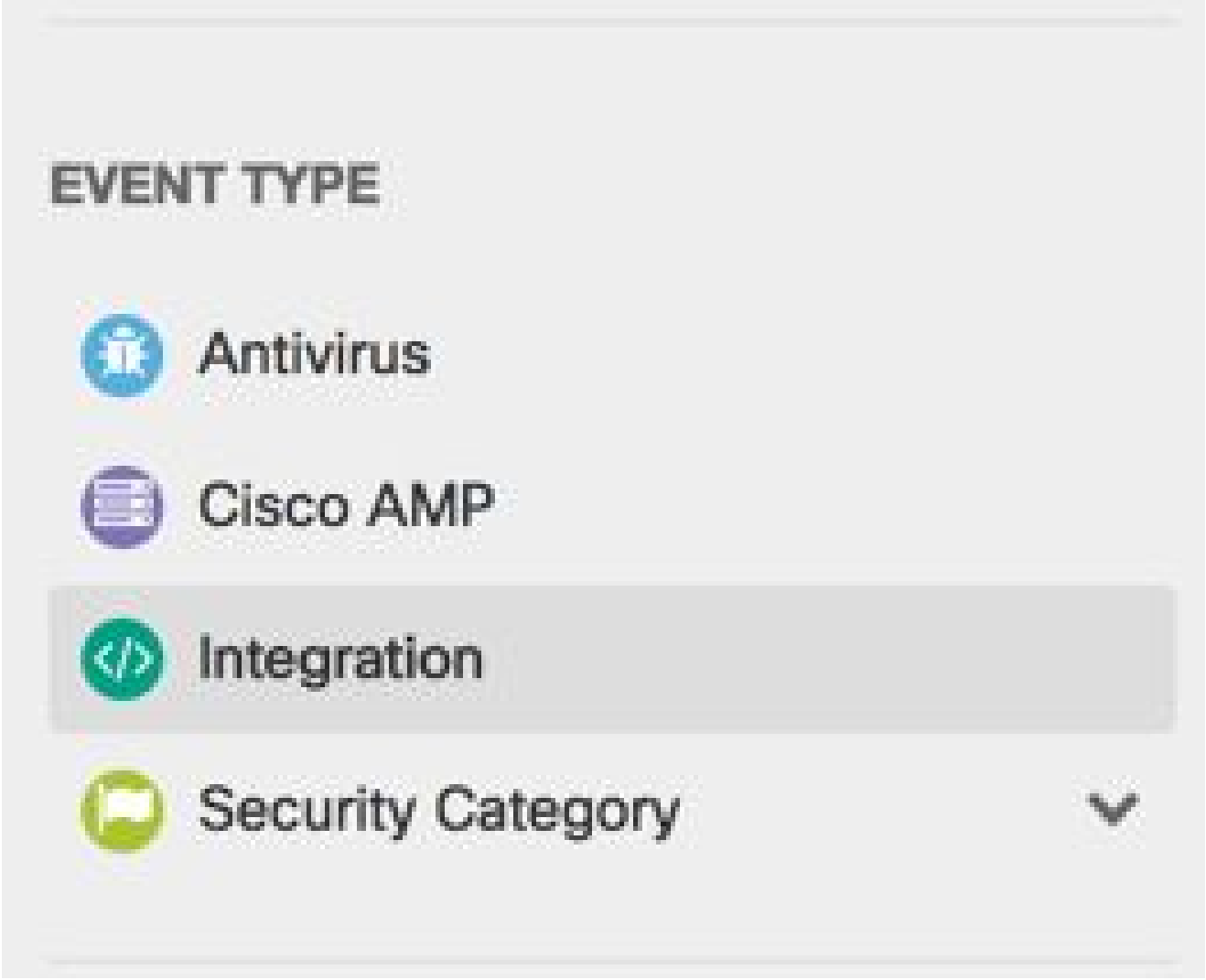


115013981706

2. 单击Apply查看报告中选定时间段的活动。

您还可以查看“活动卷”报告，查看快照或随时间推移的趋势计数报告，包括自定义集成。

1. 导航到报告>安全活动卷。
2. 在Event Type下，选择Integration。



115013982286

配置S3集成以实现日志存储和使用（可选）

如果您想将包含您环境的所有请求的Umbrella日志反馈到SIEM/TIP环境中，可以使用我们的S3集成来完成此操作，S3集成使您可以将DNS活动事件流式处理回来。

附录：示例脚本

这些perl脚本提供有关如何为自定义集成生成事件的指导。请在两个脚本中替换集成的customerKey值。请注意，这些脚本作为示例提供，可能需要自定义或更新。

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);
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。