将ThreatConnect与Umbrella集成

目录

简介

本文档介绍如何将ThreatConnect与Cisco Umbrella集成。

先决条件

要求

Cisco 建议您了解以下主题：

- 具有更新集成URL访问权限的ThreatConnect控制面板
- Umbrella控制面板管理权限
- Umbrella控制面板必须启用ThreatConnect集成。

使用的组件

本文档中的信息基于Cisco Umbrella。

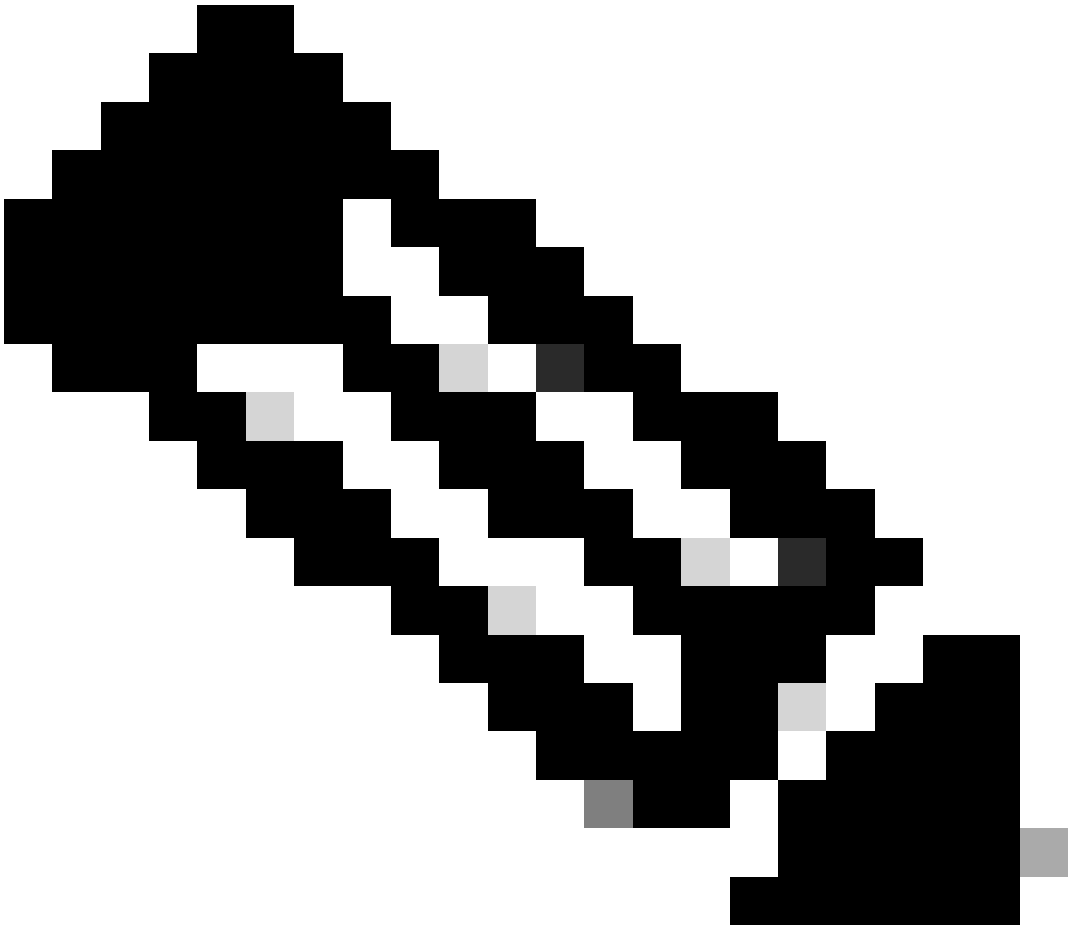
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

ThreatConnect和Cisco Umbrella集成概述

通过将ThreatConnect与Cisco Umbrella相集成，安全人员和管理员现在可以针对漫游笔记本电脑、平板电脑或电话的高级威胁提供保护，同时为分布式企业网络提供另一层实施。

本指南概述如何配置ThreatConnect以与Umbrella通信，以便将ThreatConnect TIP的安全事件集成到策略中，这些策略可应用到受思科Umbrella保护的客户端。

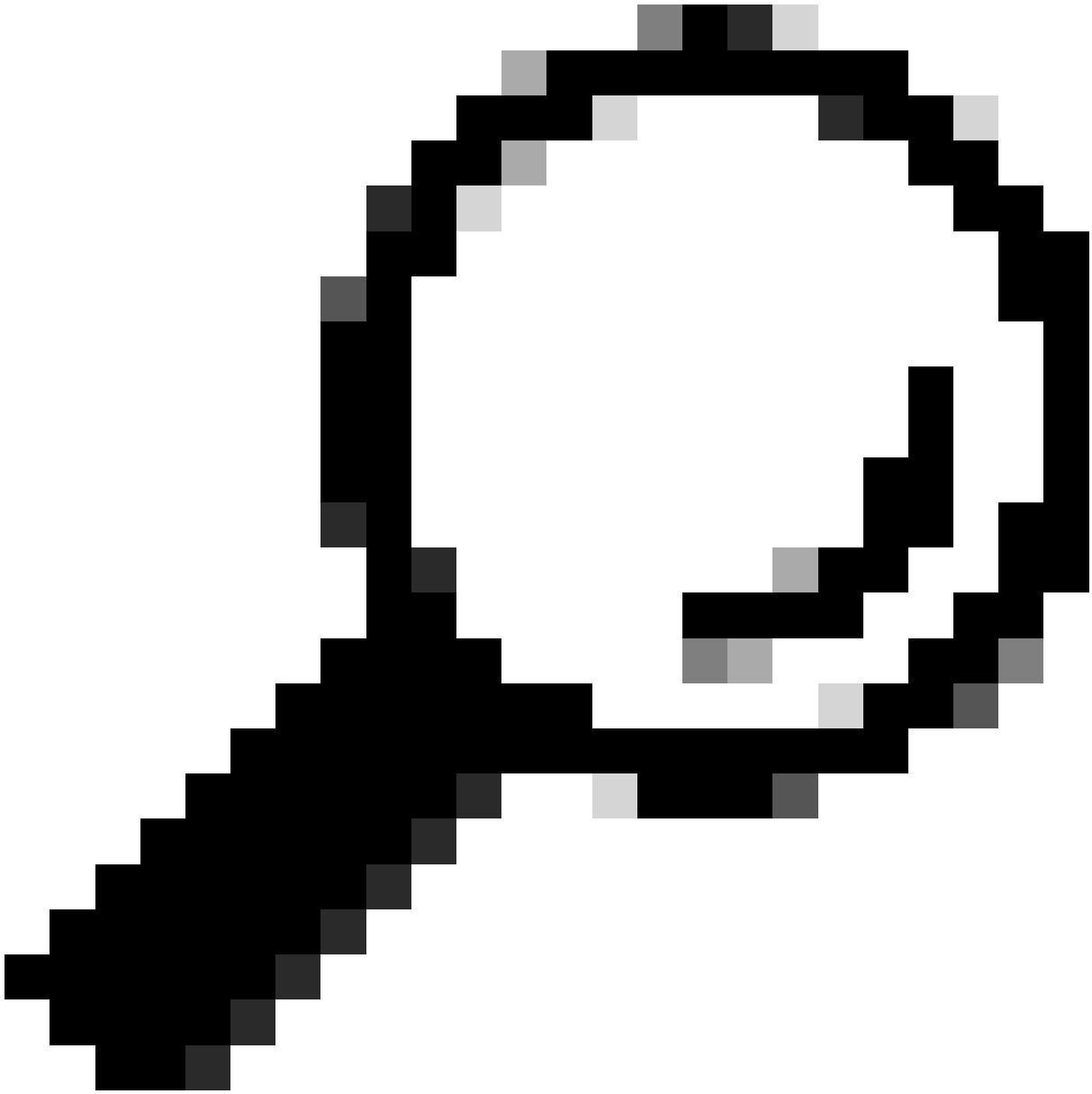


> 注意：ThreatConnect集成仅包含在特定的Cisco Umbrella软件包中。如果您没有包含此集成的软件包，请与您的Cisco Umbrella代表联系以获取该软件包。如果您有正确的软件包，但是没有将ThreatConnect视为控制面板的集成，请与Cisco Umbrella支持联系。

ThreatConnect平台首先将其发现的网络威胁情报（例如托管恶意软件的域、僵尸网络或网络钓鱼站点的命令和控制）发送到Umbrella。

然后，Umbrella验证威胁以确保将其添加到策略中。如果确认来自ThreatConnect的信息是威胁，则域地址会作为可应用到任何Umbrella策略的安全设置的一部分添加到ThreatConnect目标列表。该策略会立即应用于使用带有ThreatConnect目标列表的策略从设备发出的任何请求。

今后，Umbrella会自动解析ThreatConnect警报并将恶意站点添加到ThreatConnect目标列表，从而将ThreatConnect保护扩展到所有远程用户和设备，并为您的企业网络提供另一层实施功能。



提示：Umbrella会尽量验证和允许已知安全域（例如Google和Salesforce），以避免任何不需要的中断，同时建议根据您的策略，将您不希望被阻止的任何域添加到全局允许列表或其他目标列表。示例包括：

- 您组织的主页。例如，mydomain.com。
- 代表您提供的服务的域，可以同时具有内部和外部记录。例如，mail.myservicedomain.com和portal.myotherservicedomain.com。
- 您严重依赖但并不了解Umbrella在其自动域验证中或包括在其中的、不太为人知的云

应用。例如，localcloudservice.com。

全局允许列表位于Umbrella中的Policies > Destination Lists。有关详细信息，请参阅文档：管理目标列表

配置Umbrella控制面板以接收来自ThreatConnect的事件

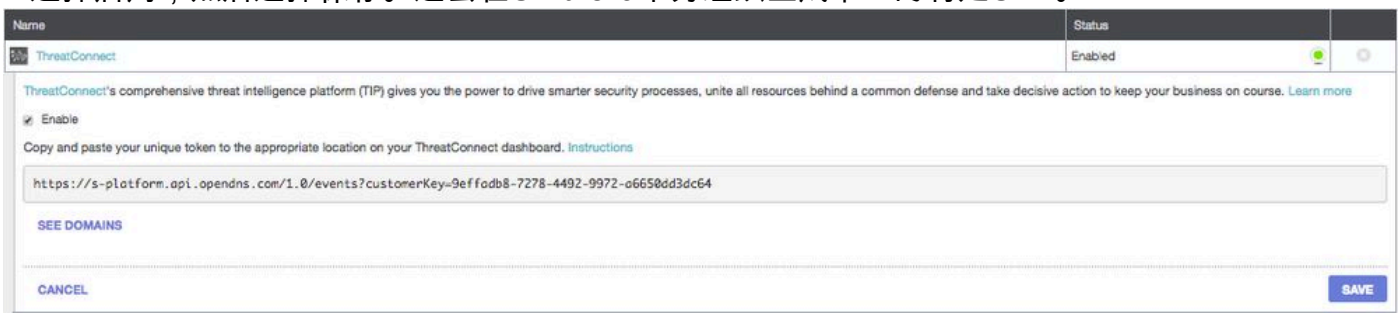
首先在Umbrella中查找您的唯一URL，以便ThreatQ设备与以下设备通信：

1.登录您的Umbrella控制面板。

2.定位至策略>集成。

3.在表中，选择ThreatConnect将其展开。

4.选择启用，然后选择保存。这会在Umbrella中为组织生成唯一的特定URL。



当您将ThreatConnect配置为向Umbrella发送数据时，您需要本文后面的URL。

配置ThreatConnect与Umbrella通信

为了开始将流量从ThreatConnect发送到Umbrella，您需要使用本文第一部分中生成的URL信息配置ThreatConnect:

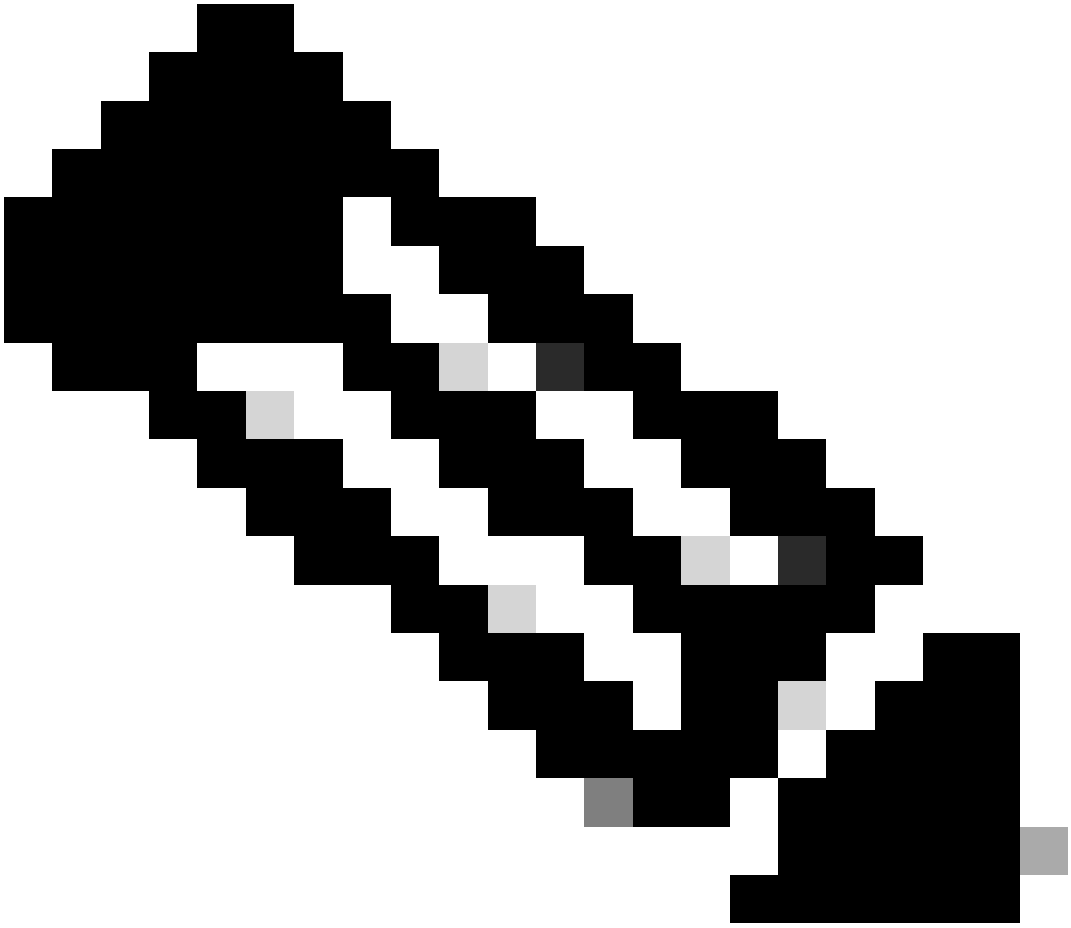
1.登录您的ThreatConnect控制面板。

2.在适当的区域添加URL以连接Umbrella。

具体说明各不相同，如果您不确定如何或何处在ThreatConnect中配置API集成，Umbrella建议联系ThreatConnect支持。

在审核模式下观察添加到ThreatConnect安全类别的事件

随着时间的推移，ThreatConnect控制面板中的事件可以开始填充一个特定目标列表，该列表可以作为ThreatConnect安全类别应用到策略。默认情况下，目标列表和安全类别处于审核模式，这意味着它们不会应用于策略，也不会导致对现有Umbrella策略进行任何更改。



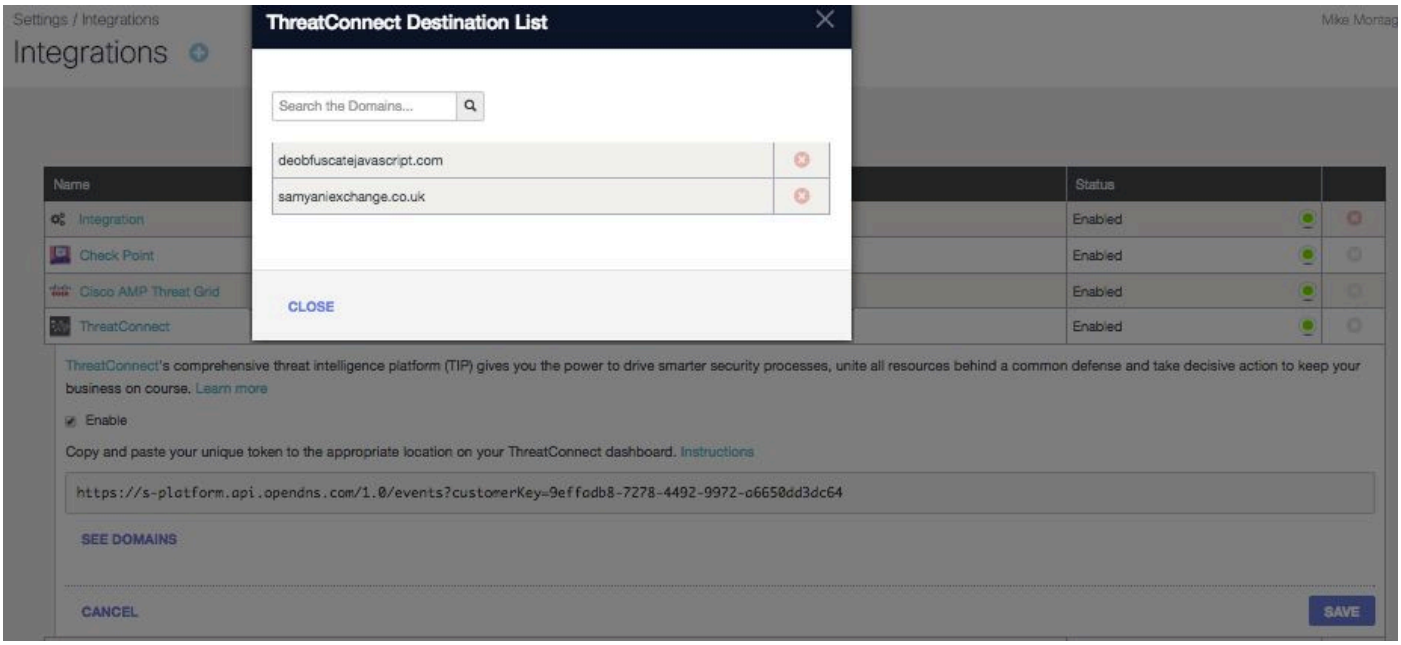
注意：可以启用审核模式，但根据您的部署配置文件和网络配置，审核模式需要多长时间。

查看目标列表

您可以随时查看Umbrella中的ThreatConnect目标列表：

1.在Umbrella控制面板中，导航至策略>集成。

2.在表中，展开ThreatConnect并选择See Domains。



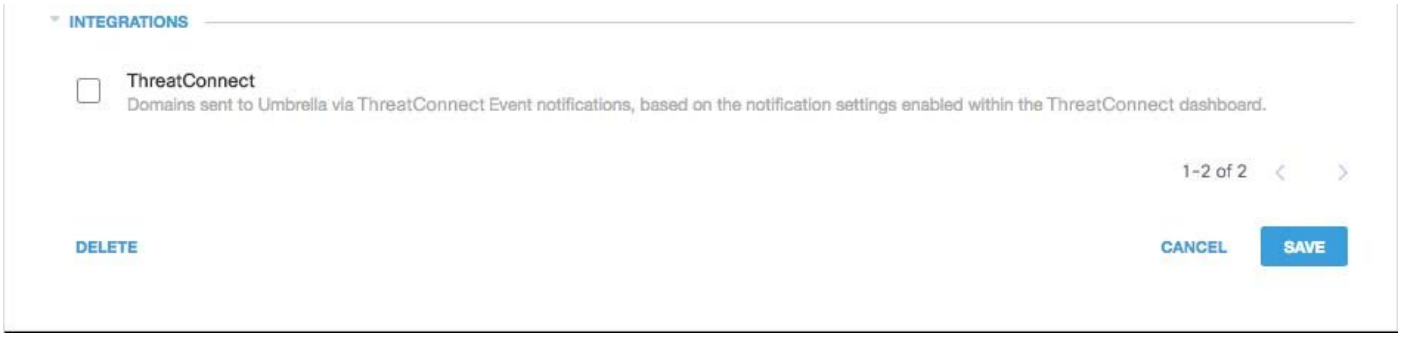
查看策略的安全设置

您可以随时查看可以为策略启用的安全设置：

1.在Umbrella控制面板中，导航至策略>安全设置。

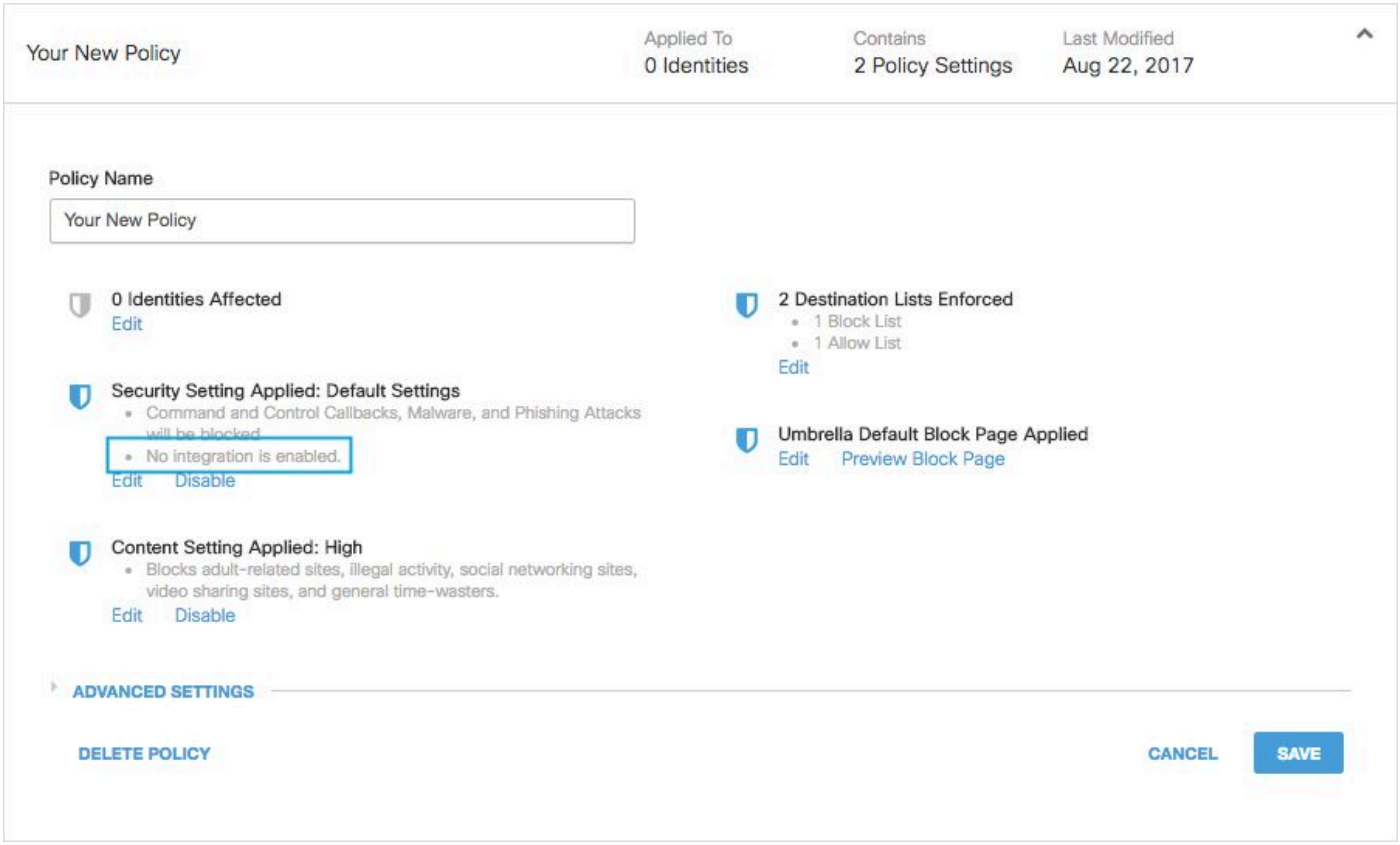
2.选择表中的安全设置将其展开。

3.滚动到集成以查找ThreatConnect设置。



115014036566

4.您还可以通过“安全性设置汇总”页查看集成信息。



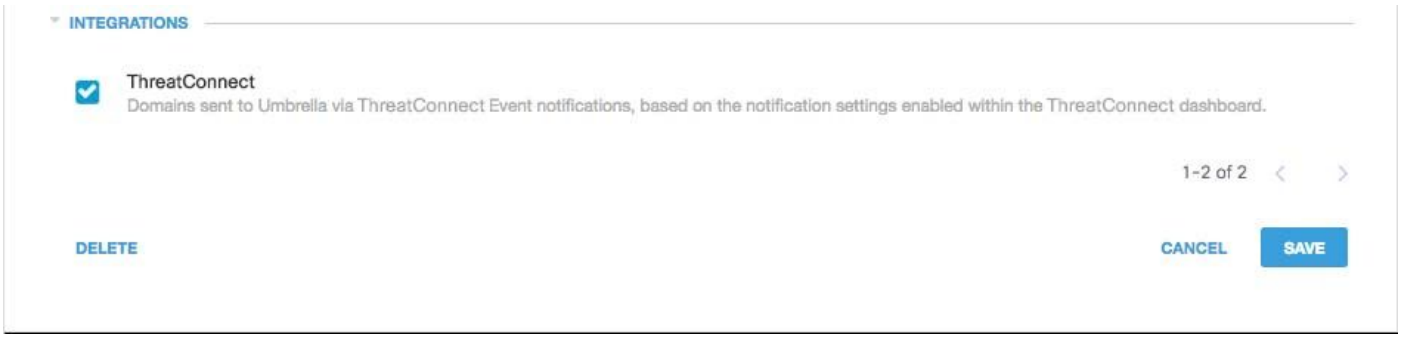
25464103885972

在阻止模式下将ThreatConnect安全设置应用于托管客户端的策略

当您准备好让这些附加安全威胁由Umbrella管理的客户端实施后，只需更改现有策略的安全设置，或创建位于默认策略之上的新策略，以确保首先实施该策略：

1.定位至策略>安全设置。

2.在集成下，选择ThreatConnect，然后选择保存。



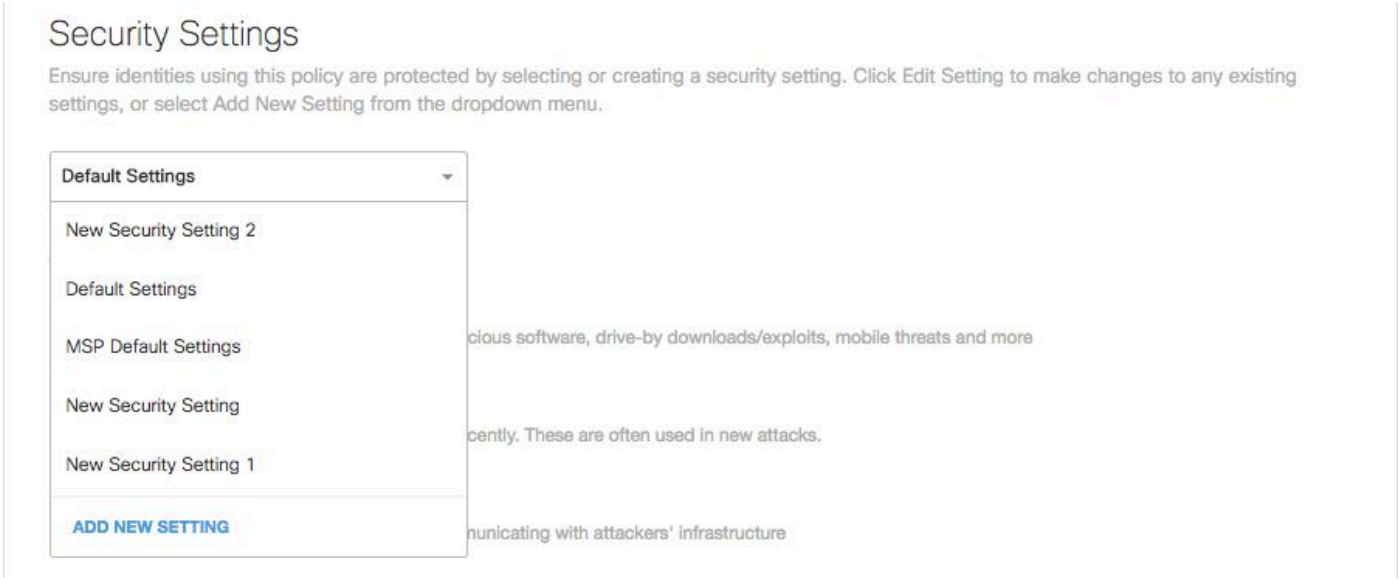
115014203703

接下来，在策略向导中，将安全设置添加到正在编辑的策略中：

1.定位至策略>策略列表。

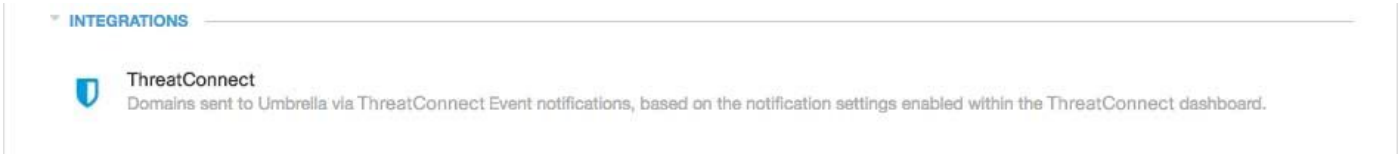
2.展开策略。在Security Setting Applied下，选择Edit。

3.在Security Settings下拉列表中，选择包含ThreatConnect设置的安全设置。



25464103908884

Integrations下的屏蔽图标将更新为蓝色。



115014037666

4.选择Set & Return。

然后，ThreatConnect的安全设置中包含的ThreatConnect域将被阻止，用于使用该策略的身份。

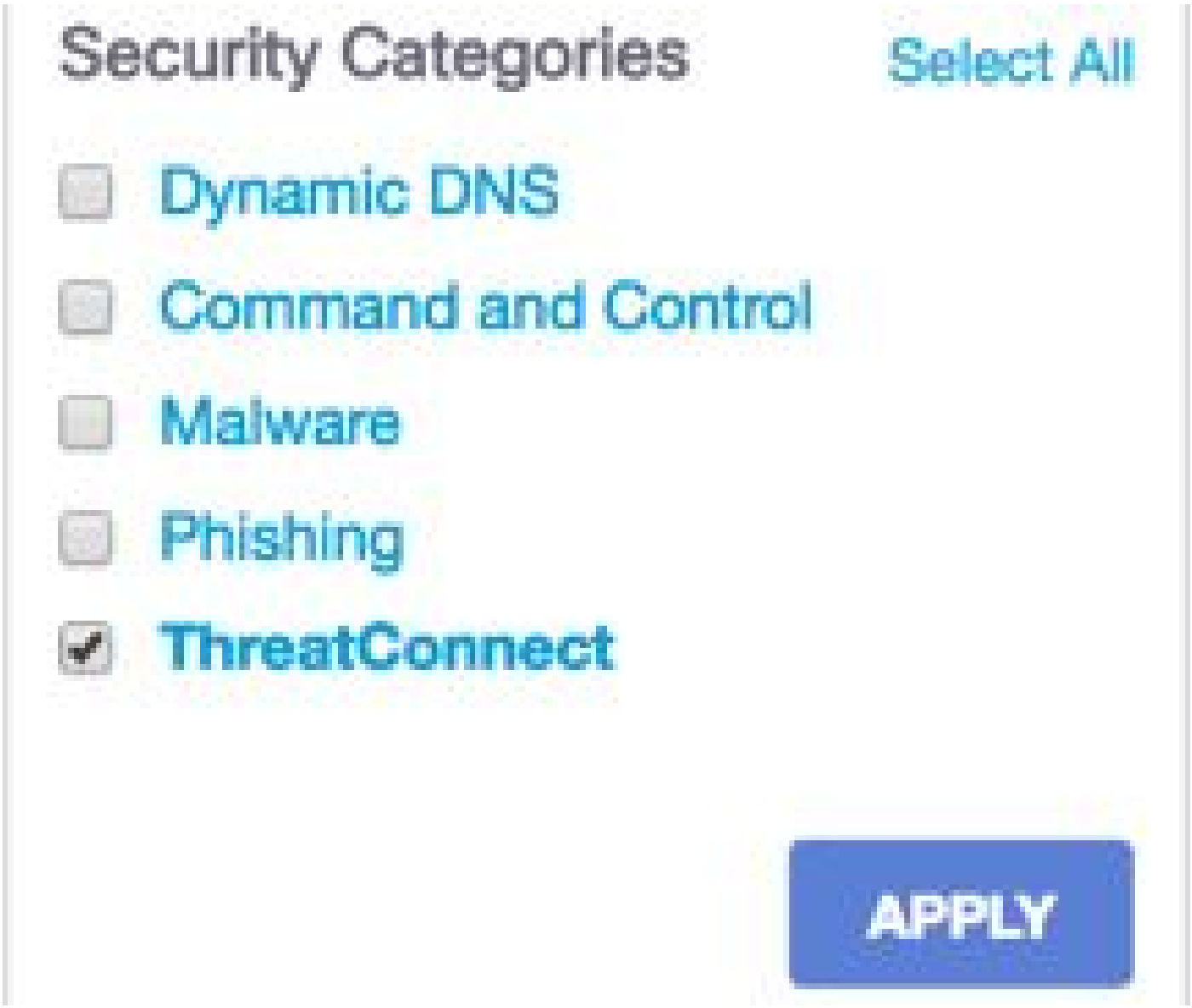
在Umbrella中报告ThreatConnect事件

报告ThreatConnect安全事件

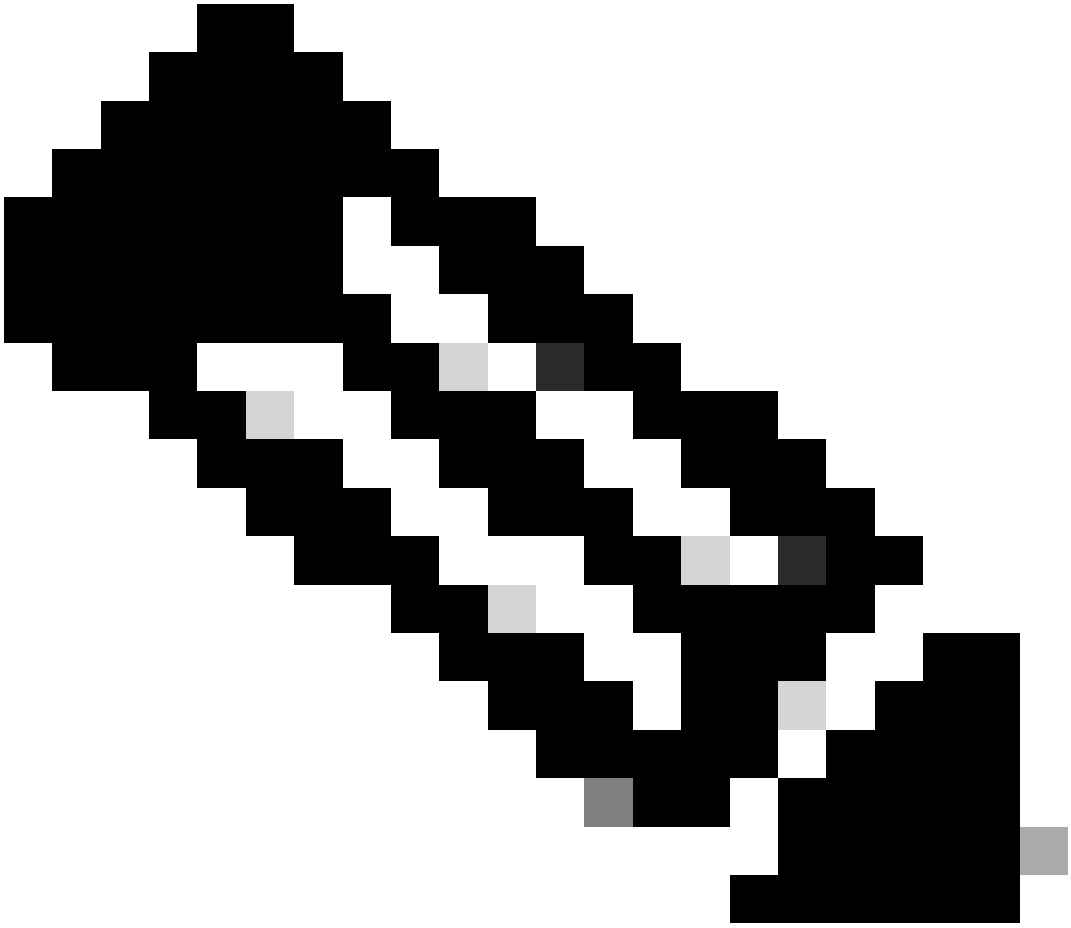
ThreatConnect Destination List是您可以报告的安全类别列表之一。大多数或所有报告都使用安全类别作为过滤器。例如，您可以过滤安全类别，以便仅显示与ThreatConnect相关的活动：

1.定位至“报告”>“活动搜索”。

2.在Security Categories下，选择ThreatConnect以过滤报告，以便仅显示ThreatConnect的安全类别。



115014206603



注意：如果ThreatConnect集成被禁用，则它不会出现在安全类别过滤器中。

3.选择Apply。

报告域添加到ThreatConnect目标列表的时间

管理员审核日志包含ThreatConnect控制面板中的事件，因为它将域添加到目标列表。名为“ThreatConnect帐户”（也带有ThreatConnect徽标）的用户生成事件。这些事件包括添加的域和添加的时间。

通过为“ThreatConnect帐户”用户应用过滤器，您可以过滤以仅包括ThreatConnect更改。

处理不需要的检测或误报

允许列表

虽然不太可能，但ThreatConnect自动添加的域可能会触发不需要的阻止，阻止用户访问特定网站。在这种情况下，Umbrella建议向允许列表添加域，该列表优先于所有其他类型的阻止列表，包括安全设置。

这一方法更可取的原因有两个：

- 首先，如果ThreatConnect控制面板在删除域后重新添加域，则允许列表可防止引起进一步问题的情况。
- 此外，允许列表还显示问题域的历史记录，可用于调查分析或审计报告。

默认情况下，全局允许列表应用于所有策略。将域添加到全局允许列表(Global Allow List)会导致在所有策略中允许该域。

如果阻止模式中的ThreatConnect安全设置仅应用于托管Umbrella身份的子集（例如，它仅适用于漫游计算机和移动设备），则可以为这些身份或策略创建特定允许列表。

要创建允许列表，请执行以下操作：

1.定位至策略>目标列表，然后选择添加(+)图标。

2.选择Allow并将您的域添加到列表中。

3.选择保存。

保存目标列表后，您可以将其添加到现有策略中，该策略涵盖了那些受到不需要的阻止影响的客户端。

从ThreatConnect目标列表中删除域

ThreatConnect目标列表中每个域名旁边都有一个Delete图标。通过删除域，您可以在出现不需要的检测时清除ThreatConnect目标列表。但是，如果ThreatConnect控制面板将域重新发送到Umbrella，则删除操作不是永久性的。

删除域的步骤：

1.定位至“策略”>“集成”。

2.选择ThreatConnect将其展开。

3.选择查看域。

4.搜索要删除的域名。

5.选择删除图标。

6.选择关闭，然后选择保存。

对于不需要的检测或误报，Umbrella建议立即在Umbrella中创建允许列表，然后在ThreatConnect控制面板中修复误报。稍后，您可以从ThreatConnect目标列表中删除该域。

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）。