Cisco Secure Firewall 威胁智能导向器

本章中的主题介绍如何配置和使用 威胁智能导向器。

Cisco Secure Firewall 威胁智能导向器 概述

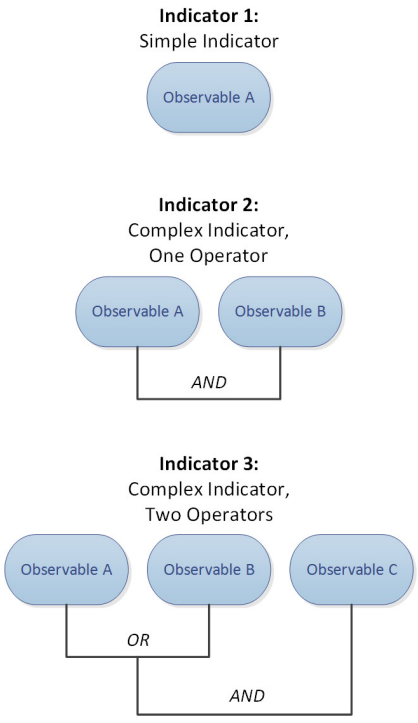
安全防火墙威胁智能导向器使用威胁情报数据进行操作，从而帮助您聚合情报数据，配置防御操作，并分析环境中的威胁。此功能旨在补充其他 Firepower 功能，可进一步加强对威胁的防御。

当在托管平台上配置 威胁智能导向器时，它会从威胁情报源摄取数据，并将数据发布到所有配置的托管设备（元素）。有关此版本中支持的托管平台和元素的更多信息，请参阅平台、元素和许可证要求， 第 4 页。

源包含指示器，其中包含可观察对象。指示器传递与威胁相关的所有特征，而单个可观察对象表示与威胁相关的单个特征（例如 SHA-256 值）。简单指示器包含单个可观察对象，而复杂指示器包含两个或更多可观察对象。

可观察对象以及它们之间的 AND/OR 运算符构成指示器的模式，如下面的示例所示。

图 *1:* 示例：指示器模式



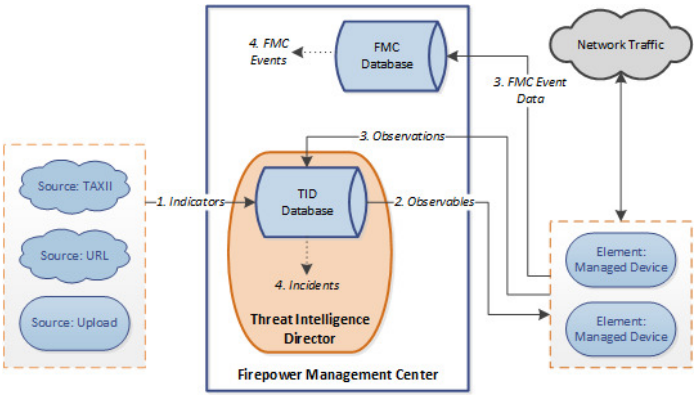
将可观察对象发布到元素后，在系统识别流量中的可观察对象时，元素会监控流量并将观察结果报告到 防火墙管理中心。

防火墙管理中心会从所有元素收集观察结果，根据 威胁智能导向器指示器评估观察结果，以及生成或更新与可观察对象的父指示器相关的事故。

当指示器的模式完成时，事件即完全实现。如果流量与指示器中的一个或多个可观察对象相匹配但未匹配整个模式，事故会部分实现。有关详细信息，请参阅观察和事故生成，第 15 页。

下图显示了系统配置示例中的数据流。

图 *2:* 防火墙管理中心 数据流



当 威胁智能导向器事故完全或部分实现时，系统会执行配置的操作（监控、阻止、部分阻止或无操作）。有关详细信息，请参阅影响所执行操作的因素， 第 23 页。

威胁智能导向器和安全智能

作为访问控制策略的一部分，安全智能使用信誉情报来快速阻止与IP地址、URL和域之间的往来连接。安全智能唯一地提供通过 Talos 智能小组 对业界领先的威胁情报的访问。有关安全智能的详细信息，请参阅关于安全智能。

威胁智能导向器增强了系统根据来自第三方来源的安全智能阻止连接的能力，如下所示：

- **威胁智能导向器 支持其他流量过滤条件** - 安全智能使您可以根据 IP 地址、URL 和（如果已启用 DNS 策略）域名来过滤流量。威胁智能导向器 还支持按这些条件进行过滤，并增加了对 SHA-256 散列值进行过滤的支持。
- **威胁智能导向器 支持其他情报注入方法** - 使用安全智能和 威胁智能导向器，可以通过手动上传平面文件或配置系统以从第三方主机检索平面文件，从而将威胁情报导入系统。威胁智能导向器 增强了管理这些平面文件的灵活性。此外，威胁智能导向器可以检索和摄取以结构化威胁信息表达式 (STIX™) 格式提供的情报。
- **威胁智能导向器提供对过滤操作的精细控制** - 使用安全智能，可以按网络、URL 或 DNS 对象指定过滤条件。安全智能对象（特别是列表和源）可以包含多个 IP 地址、URL 或 DNS 域名，但您只能根据整个对象来阻止或不阻止，而不是根据一个对象的单个组件来阻止。使用 威胁智能导向器，可以为单个条件（即简单指示器或单个可观察对象）配置过滤操作。
- **威胁智能导向器配置更改不需要重新部署** - 在访问控制策略中修改安全智能设置后，必须将更改的配置重新部署到托管设备。使用 威胁智能导向器，将访问控制策略初始部署到托管设备后，可以配置源、指示器和可观察对象而无需重新部署，系统会自动将新的 威胁智能导向器数据发布到这些元素。

有关安全智能或威胁智能导向器可以处理特定事件时系统操作的相关信息，请参阅威胁智能导向器-防火墙管理中心 操作优先级， 第 23 页。

威胁情报导向器的性能影响

Cisco Secure Firewall Management Center

在某些情况下，您可能会发现存在以下情况：

- 在摄取特别大的 STIX 源时，系统可能会遇到一些小的性能问题，而且摄取完成时间可能会比预期的要长。
- 系统可能需要 15 分钟才能将新的或修改后的威胁智能导向器数据向下发布到元素。

托管设备

对性能没有特殊影响。威胁智能导向器 对性能的影响与 Cisco Secure Firewall Management Center安全智能功能完全相同。

威胁情报导向器要求和前提条件

型号支持

任意

支持的域

任意

用户角色

管理员

威胁智能导向器 用户

其它要求

以下主题介绍了使用威胁情报导向器的其他要求。

平台、元素和许可证要求

托管平台

可以在物理和虚拟 Cisco Secure Firewall Management Center上托管 威胁智能导向器：

- 运行版本 6.2.2 或更高版本。
- 配置至少 15 GB 的内存。
- 配置为已启用 REST API 访问。请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 启用 *REST API* 访问。

元素

如果设备运行的是 6.2.2 或更高版本，则可以使用任何 Cisco Secure Firewall Management Center托管设备作为 威胁智能导向器 元素。

许可

要为 SHA-256 可观察对象发布配置文件策略，您需要以下许可设备：

- 对于智能许可设备：
  - IPS 许可证 - 适用于 IPv4、IPv6、URL 和 DNS 检测和可观察对象
  - 恶意软件防御 许可证 - 用于 SHA-256 检测和可观察对象

有关详细信息，请参阅 配置策略以支持威胁智能导向器，第 7 页和 《Cisco Secure Firewall Management Center 管理指南》中的 。

源要求

源类型要求

STIX

文件必须是 STIX 版本 1.0、1.1、1.1.1 或 1.2，并且遵守 STIX 文档中的准则：http://stixproject.github.io/documentation/suggested-practices/。

STIX 文件可以包括复杂的指示器。

通过 URL 下载或文件上传进行配置时，STIX 文件的最大大小为 40MB。如果您的 STIX 文件大于此值，我们建议使用 TAXII 服务器。

平面文件

文件必须是每行包含一个可观察值的 ASCII 文本文件。

平面文件仅包括简单的指示器（每个指示器一个可观察对象）。

平面文件上传的文件最大可达 500 MB。

威胁智能导向器 不支持：

- 分隔可观察值的分隔符字符（例如 `observable,` 无效）。
- 围绕可观察值的封闭字符（例如 `"observable"` 无效）。

每个文件应仅包含一种类型的内容：

- `SHA-256` - SHA-256 散列值。
- `域` - RFC 1035 中定义的域名。
- `URL` - RFC 1738 中定义的 URL。

注释 威胁智能导向器 会规范化包含端口、协议或身份验证信息的任何 URL，并在检测指示器时使用规范化的版本。例如，威胁智能导向器 会将以下任一 URL：

```
http://example.com/index.htm
http://example.com:8080/index.htm
example.com:8080/index.htm
example.com/index.htm
```

规范化为：

```
example.com/index.htm
```

再例如，威胁智能导向器 会将以下 URL：

```
http://abc@example.com:8080/index.htm
```

规范化为

```
abc@example.com/index.htm/
```

- `IPv4` - RFC 791 中定义的 IPv4 地址。

  威胁智能导向器 不接受 CIDR 块。

- `IPv6` - RFC 4291 中定义的 IPv6 地址。

  威胁智能导向器 不接受前缀长度。

源内容限制

系统仅会注入并匹配 URL 可观察对象的前 1000 个字符。

如何设置威胁智能导向器

注释 如果在 威胁智能导向器配置或操作期间遇到问题，请参阅对威胁智能导向器进行故障排除，第 41 页。

过程

步骤 1 确保您的安装符合 威胁智能导向器 运行要求。

请参阅 平台、元素和许可证要求，第 4 页

步骤 2 对于每个托管设备，配置支持 威胁智能导向器 所需的策略，并将这些策略部署到设备。

请参阅配置策略以支持威胁智能导向器，第 7 页。

可以在采集情报数据源之前或之后配置元素。

步骤 3 配置您希望 威胁智能导向器 采集的情报源。

请参阅源要求，第 5 页和采集数据源的选项，第 8 页下的主题。

步骤 4 如果尚未将数据发布到元素，请执行此操作。请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 39 页。

下一步做什么

- 将 威胁智能导向器 纳入定期计划备份。请参阅关于备份和恢复 威胁智能导向器 数据，第 14 页。

  如果您的 Cisco Secure Firewall Management Center 部署是高可用性配置，另请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 防火墙管理中心 高可用性灾难恢复 。

- （可选）根据需要为 威胁智能导向器 功能授予管理访问权限。请参阅 具有 威胁智能导向器 访问权限的用户角色，第 14 页 和 《Cisco Secure Firewall Management Center 管理指南》中的 用户 章节。

- 在运行期间，根据需要精细调节配置。例如，生成误报事件的白名单可观察对象。请参阅查看和更改威胁智能导向器 配置，第 27 页。

配置策略以支持威胁智能导向器

您必须配置访问控制策略，以将 威胁智能导向器 数据从防火墙管理中心发布到托管设备（元素）。此外，我们还建议配置访问控制策略，以最大化观察结果和 防火墙管理中心事件生成。

对于您要支持 威胁智能导向器 的每个托管设备，请执行以下步骤以配置相关联的访问控制策略。

配置为在已发布数据后使用 威胁智能导向器 的元素将自动接收所有当前已发布的可观察对象。

过程

步骤 1 验证并确保已选中访问控制策略的 **常规设置** 中的 **启用威胁情报导向器** 复选框。要导航到**常规设置**，请选择 **策略** > **访问控制标题** > **访问控制**，然后点击**编辑** > **更多** > **高级设置**。默认情况下，此选项已启用。

有关详细信息，请参阅访问控制策略高级设置。

步骤 2 如果尚不存在规则，请向访问控制策略添加规则。威胁智能导向器要求访问控制策略必须指定至少一个规则。

由于威胁智能导向器取决于检测，请确保允许流量而不是信任流量，因为信任流量的目的是绕过检测。有关详细信息，请参阅创建基本访问控制策略。

步骤 3 如果选择**入侵防御 (Intrusion Prevention)** 作为访问控制策略的默认操作，则请将 SSL 策略与该访问控制策略相关联；请参阅将其他策略与访问控制相关联。

步骤 4 如果您希望 `SHA-256` 可观察对象生成观察结果和 Cisco Secure Firewall Management Center事件：

a) 创建包含一个或多个**恶意软件云查找 (Malware Cloud Lookup)** 或**阻止恶意软件 (Block Malware)** 文件规则的文件策略。

有关详细信息，请参阅配置文件策略。

b) 将此文件策略与访问控制策略中的一个或多个规则相关联。

步骤 5 如果希望 `IPv4`、`IPv6`、`URL` 或域名观察结果生成连接和安全智能事件，则请在访问控制策略中启用连接和安全智能日志记录：

a) 在调用文件策略的访问控制规则中，启用**在连接结束时记录日志**和**文件事件：日志文件**（如果尚未启用）。

有关详细信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》中 的使用访问控制规则记录连接。

b) 验证并确保已在“安全智能”设置中启用了默认日志记录（**DNS 策略**、**网络**和 **URL**）。

有关详细信息，请 《Cisco Secure Firewall Management Center 管理指南》中的 参阅 中使用安全智能记录连接 。

步骤 6 部署配置更改；请参阅 部署配置更改。

下一步做什么

完成以下位置中的剩余项目： 如何设置威胁智能导向器，第 6 页

采集数据源的选项

请根据要使用的数据类型和传送机制选择配置选项。

有关这些数据类型的详细信息，请参阅源要求，第 5 页。

表 *1:* 采集数据源的选项

数据类型	采集选项
STIX	• 从 TAXII 服务器采集 STIX 源： 请参阅 获取要用作源的 TAXII 源，第 9 页 • 从 URL 下载 STIX 数据： 请参阅 从 URL 获取源，第 10 页 • 上传 STIX 文件： 请参阅 上传本地文件以用作源，第 11 页

数据类型	采集选项
平面文件	• 从 URL 下载数据： 请参阅 从 URL 获取源， 第 10 页 • 上传平面文件： 请参阅上传本地文件以用作源， 第 11 页

获取要用作源的 TAXII 源

如果在 TID 配置或操作期间遇到问题，请参阅 对威胁智能导向器进行故障排除， 第 41 页

过程

步骤 1 请确保源满足以下部分中的要求 源要求， 第 5 页

步骤 2 选择**集成** > **情报** > **源**。

步骤 3 请点击 **添加**（+）。

步骤 4 选择 TAXII 作为源的**传递**方法。

步骤 5 输入信息。

- 如果主机服务器需要加密连接，请按照为 威胁智能导向器 源配置 TLS/SSL 设置， 第 13 页中所述配置 **SSL 设置**。
- 不能更改 TAXII 源的**操作**选择。

  块不是 TAXII 源的**操作**选项，因为 STIX 数据可能包含复杂的指标，这是系统所无法阻止的。设备（元素）根据单个可观察对象存储和采取操作，无法根据多个可观察对象采取操作。

  但注入后，可以阻止从源获取的各个可观察对象和简单的指标。有关详细信息，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作， 第 37 页。
- 加载源列表可能需要一些时间。
- **更新间隔**指定 威胁智能导向器 从TAXII 检索更新的频率。

  更新频率应设置为对于数据源的更新频率有意义的值。例如，如果源每天更新 3 次，则将更新间隔设置为 1440/3 或 480 分钟，以定期捕获最新数据。
- 指定的 **TTL** 天数过后，威胁智能导向器 将删除：
  - 不包括在后续源更新中的所有源指示器。
  - 保留下来的指标未引用的所有可观察对象。

  注释
  如果源在为 TTL 指定的天数内没有更新，且源校验和保持不变，则下载将被视为没有更新的源。要让可观察对象接收新的 TTL 值，源必须包含一些更新。

步骤 6 如果要立即开始发布到元素，请确认已启用 **发布 滑块**（  ）。

启用此选项后，系统将自动发布初始源数据和任何后续更改。

有关详细信息，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 39 页。

步骤 7 点击**保存**。

下一步做什么

- TAXII 源可能包含大量数据，全部注入这些数据可能需要花费系统一些时间。要查看注入状态，请刷新“源”页面。
- 如果您看到此源的错误，请将鼠标悬停在状态上获取详细信息。
- 如果您执行的是初始 威胁智能导向器 配置，请返回到如何设置威胁智能导向器，第 6 页。

从 URL 获取源

如果希望 威胁智能导向器 从主机获取文件，请配置 URL 源。

如果在 TID 配置或操作期间遇到问题，请参阅 对威胁智能导向器进行故障排除，第 41 页

过程

步骤 1 请确保源满足以下部分中的要求 源要求，第 5 页

步骤 2 选择**集成** > **情报** > **源**。

步骤 3 请点击 **添加**（  ）。

步骤 4 选择 `URL` 作为源的**传递**方法。

步骤 5 完成表格。

- 如果要采集平面文件，请选择描述源中所包含数据的**类型 (Type)**。
- 如果主机服务器需要加密连接，请按照为 威胁智能导向器 源配置 TLS/SSL 设置，第 13 页中所述配置 **SSL 设置**。
- 对于名称：要基于威胁智能导向器简化分类和事故处理指标简化事故的排序和处理，请在所有源中使用一致的命名方案。例如， <source>-<type> 。

  包括源名称可简化返回到源，以获取进一步的信息或反馈。

  请确保按照一致的方式输入名称。例如，对于具有 IPv4 地址的源，您可能始终使用 IPV4（而不是 IPv4、ipv4、IP_v4、IP_V4、ip-v4、IP-v4 或 IP-V4 等。）
- 如果要采集 STIX 文件，`Block` 不是**操作**选项，因为 STIX 数据可能包含系统无法阻止的复杂指标。设备（元素）根据单个可观察对象存储和采取操作，无法根据多个可观察对象采取操作。

但注入后，可以阻止从源获取的各个可观察对象和简单的指标。有关详细信息，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 37 页。

- 更新频率应设置为对于数据源的更新频率有意义的值。例如，如果源每天更新 3 次，则将更新间隔设置为 1440/3 或 480 分钟，以定期捕获最新数据。
- 为 **TTL** 间隔指定的天数过后，威胁智能导向器 将删除：
  - 不包括在后续源更新中的所有源指示器。
  - 保留下来的指标未引用的所有可观察对象。

注释
如果源在为 TTL 指定的天数内没有更新，且源校验和保持不变，则下载将被视为没有更新的源。要让可观察对象接收新的 TTL 值，源必须包含一些更新。

步骤 6 如果要立即开始发布到元素，请确认已启用 **发布 滑块**（）。

启用此选项后，系统将自动发布初始源数据和任何后续更改。

有关详细信息，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 39 页。

步骤 7 点击**保存**。

下一步做什么

- 要查看注入状态，请刷新“源”页面。如果您看到错误，请将鼠标悬停在状态上获取详细信息。
- 如果您执行的是初始 威胁智能导向器 配置，请返回到如何设置威胁智能导向器，第 6 页。

上传本地文件以用作源

使用此程序一次性手动上传本地文件。

注入 STIX 文件时，威胁智能导向器将从 STIX 文件的内容创建一个简单或复杂的指示器。

注入平面文件时，威胁智能导向器将为平面文件中的每个可观察对象值创建一个简单指示器。

如果在 威胁智能导向器 配置或操作期间遇到问题，请参阅对威胁智能导向器进行故障排除，第 41 页

过程

步骤 1 请确保您的文件满足以下部分中的要求 源要求，第 5 页

步骤 2 选择**集成** > **情报** > **源**。

步骤 3 请点击 **添加**（  ）。

步骤 4 选择上传作为源的**交付**方法。

步骤 5 完成表格。

- 如果要上传平面文件，请选择描述源中所包含数据的 **内容** 类型。
- 对于名称：要基于 威胁智能导向器简化分类和事故处理指标简化事故的排序和处理，请在所有源中使用一致的命名方案。例如， <source>-<type> 。

  包括源名称可简化返回到源，以获取进一步的信息或反馈。

  请确保按照一致的方式输入名称。例如，对于具有 IPv4 地址的源，您可能始终使用 IPV4（而不是 IPv4、ipv4、IP_v4、IP_V4、ip-v4、IP-v4 或 IP-V4 等。）
- 如果您上传的是 STIX 文件，阻止不是一个**操作**选项，因为 STIX 数据可能包含比较复杂的指示器。设备（元素）基于单个可观察对象存储并执行操作；无法基于多个可观察对象执行操作。

  但是，您可以在指示器或可观察对象级别阻止简单指示器。有关详细信息，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作 ， 第 37 页。
- 为 **TTL** 间隔指定的天数过后，威胁智能导向器 将会删除：
  - 不包括在后续源上传中的所有源指示器。
  - 保留下来的指标未引用的所有可观察对象。

  注释
  如果源在为 TTL 指定的天数内没有更新，且源校验和保持不变，则下载将被视为没有更新的源。要让可观察对象接收新的 TTL 值，源必须包含一些更新。

步骤 6 如果要立即开始发布到元素，请确认已启用 **发布 滑块**（ ） 。

如果没有在注入时发布源，则以后无法再发布所有源指示器；只能单独发布每个可观察对象。请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据 ， 第 39 页。

步骤 7 点击**保存**。

下一步做什么

- 要查看注入状态，请刷新“源”页面。如果您看到错误，请将鼠标悬停在状态上获取详细信息。
- 如果您执行的是初始 威胁智能导向器 配置，请返回到如何设置威胁智能导向器 ， 第 6 页。

处理重复指示器

如果单个指示器包括在多个源中：

每个指示器实例都会生成一个事故，因此遇到一次特定威胁可能会生成多个事故。

为避免未来出现重复事故，请暂停发布除一个重复指示器之外的所有指示器。请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据 ， 第 39 页。

为 威胁智能导向器 源配置 TLS/SSL 设置

如果主机服务器需要加密连接，则配置 **SSL 设置**。

开始之前

- 开始配置 TAXII 或 URL 源，如获取要用作源的 TAXII 源， 第 9 页或从 URL 获取源， 第 10 页中所述。

过程

步骤 1 在 **编辑源** 对话框中，展开 **SSL 设置** 部分。

步骤 2 如果您的服务器证书是自签名证书：

a) 启用**自签名证书**。

b) 选择 **SSL 主机名验证**方法。

- 严格 - 威胁智能导向器 要求源 **URL** 与服务器证书中提供的主机名相匹配。

  如果主机名包含通配符，则 TID 不能匹配多个子域。

- 浏览器兼容 - 威胁智能导向器 要求源 **URL** 与服务器证书中提供的主机名相匹配。

  如果主机名包含通配符，则 TID 匹配所有子域。

- 允许所有 - 威胁智能导向器 不要求源 **URL** 与服务器证书中提供的主机名相匹配。

例如，如果 `subdomain1.subdomain2.cisco.com` 是您的源 **URL** 并且 `*.cisco.com` 是服务器证书中提供的主机名：

- 严格主机名验证失败。
- 浏览器兼容主机名验证成功。
- 允许所有主机名验证完全忽略主机名值。

c) 对于**服务器证书**：

- 如果您有权访问 PEM 编码的自签名服务器证书，请在文本编辑器中打开该证书，并复制整个文本块，包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行。在字段中输入此整个字符串。
- 如果您无权访问自签名服务器证书，请将该字段保留为空。保存源后，威胁智能导向器 将从服务器检索证书。

步骤 3 如果您的服务器需要用户证书：

a) 输入**用户证书**。

在文本编辑器中打开 PEM 编码的证书，复制整个文本块，包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行。在字段中输入此整个字符串。

b) 输入**用户私有密钥**：

在文本编辑器中打开私有密钥文件并复制整个文本块，包括`BEGIN RSA PRIVATE KEY`和`END RSA PRIVATE KEY`行。在字段中输入此整个字符串。

下一步做什么

- 记下证书的到期日期。您可能希望设置日历提醒，在当前证书到期后输入新的服务器证书。
- 继续配置源：
  - 获取要用作源的 TAXII 源， 第 9 页
  - 从 URL 获取源， 第 10 页

具有 威胁智能导向器 访问权限的用户角色

可以使用 防火墙管理中心用户帐户访问 威胁智能导向器 菜单和页面：

- 具有**管理员**或**威胁情报导向器用户**用户角色的帐户。
- 具有包含**情报**权限的自定义用户角色的帐户。

此外，还可使用具有**管理员**、**访问管理员**或**网络管理员**用户角色的 防火墙管理中心用户帐户可在访问控制策略中启用或禁用 威胁智能导向器。

有关用户账户的详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的 防火墙管理中心 的用户一章。

关于备份和恢复 威胁智能导向器 数据

您可以使用 防火墙管理中心备份和恢复 威胁智能导向器 所需的所有数据：元素数据、安全智能事件、连接事件、威胁智能导向器 配置和 威胁智能导向器 数据。有关详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的备份/恢复章节。

注释 如果使用高可用性配置在主用 防火墙管理中心上托管 威胁智能导向器，则系统不会将 威胁智能导向器配置与 威胁智能导向器数据同步到备用 防火墙管理中心。我们建议对主用 防火墙管理中心上的 威胁智能导向器数据定期执行备份，以便您可以在故障转移后恢复数据。

在尝试恢复主用 防火墙管理中心上的 威胁智能导向器 数据之前，请暂停主用对等设备上的同步。关于更多信息，请参阅在 《Cisco Secure Firewall Management Center 管理指南》中的 暂停已配对 *Firepower* 管理中心之间的通信 。

表 2: 威胁智能导向器相关的备份和恢复文件内容

威胁智能导向器相关的文件内容	备份选择	恢复选择
元素数据	备份配置	恢复配置数据
Cisco Secure Firewall Management Center事件数据	备份事件	恢复事件数据
威胁智能导向器配置和威胁智能导向器数据	备份威胁智能导向器	恢复威胁情报导向器数据

分析 威胁智能导向器 事件和观察数据

要分析 威胁智能导向器 元素生成的事件和观察数据，请使用“事件表和事件详细信息”页。

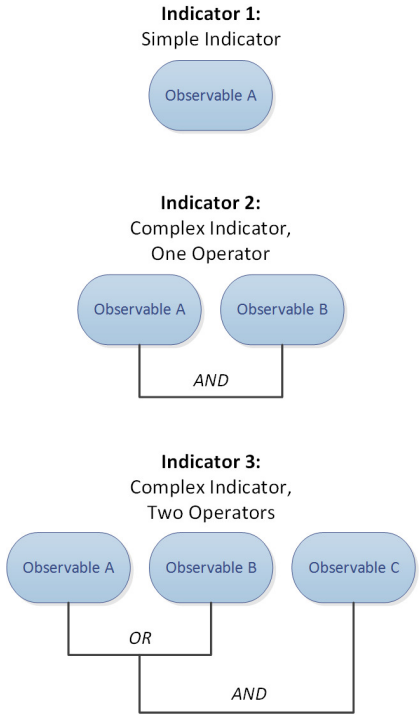
观察和事故生成

威胁智能导向器在流量中发现指示器的第一个可观察对象时生成事故。简单指示器在单个观察之后完全实现。复杂指示器直到一个或多个其他观察履行了其模式才会部分实现。在单个事务期间，不必满足复杂指示器的需要；随着时间推移，每个可观察对象均可通过不同事务单独完成。

注释 威胁智能导向器 在评估指示器模式时将忽略不支持的、无效的和已列入不阻止列表的可观察对象。

事故完全实现之后，后续观察将会触发新事故。

图 *3:* 示例：指示器模式



如果 威胁智能导向器从上面的示例中获取了可观察对象，并且可观察对象井然有序，则事故生成将按如下所示继续：

1. 当系统在流量中识别到可观察对象 A 时，威胁智能导向器：
   - 为指示器 1 生成完全实现的事故。
   - 为指示器 2 和指示器 3 生成部分实现的事故。
2. 当系统在流量中识别到可观察对象 B 时，威胁智能导向器：
   - 将事故更新为对指示器 2 完全实现，因为该模式已履行。
   - 将事件更新为对指示器 3 部分实现。
3. 当系统在流量中识别到可观察对象 C 时，威胁智能导向器：
   - 将事故更新为对指示器 3 完全实现，因为该模式已履行。
4. 当系统在流量中再次识别到可观察对象 A 时，威胁智能导向器：
   - 为指示器 1 生成完全实现的事故。
   - 为指示器 2 和指示器 3 生成部分实现的新事故。

如果特定指示器存在于多个源中，则您可能会看到重复事故。有关详细信息，请参阅对威胁智能导向器进行故障排除，第 41 页。

请注意，只会通过实际流量生成事故。如果对于URL B存在一个可观察对象，并且某个用户访问显示指向 URL B 的链接的 URL A，则除非该用户点击 URL B 链接，否则不会发生事故。

查看和管理事故

“事故”页面显示最多 110 万个最新 威胁智能导向器 事故的摘要信息；请参阅事故摘要信息，第 18 页。

开始之前

- 配置功能，如如何设置威胁智能导向器，第 6 页中所述。
- 了解观察和事件生成，如观察和事故生成，第 15 页中所述。

过程

步骤 1 选择**集成** > **情报** > **事件**。

步骤 2 查看您的事故：

- 点击 **过滤器**（）以添加一个或多个过滤器。默认过滤器是6个小时。有关详细信息，请参阅过滤表视图中的 威胁智能导向器 数据，第 34 页。
- 要查看上次由 威胁智能导向器 更新事故的日期和时间，请将光标悬停在**最后更新时间**列中的值上。
- 要查看与事件关联的指示器的详细信息，请点击**指示器名称**列中的文本；请参阅查看和管理指示器，第 30 页。

步骤 3 请通过点击**事故 ID (Incident ID)** 列中的值来查看其他详细信息。

有关您查看的详细信息的说明，请参阅事件详细信息，第 18 页。

- 要查看指示器详细信息，请点击窗口下半部分中**指示器 (Indicator)** 标题下的指示器值（例如，IP 地址或 SHA-256 值）。
- 要查看观察结果详细信息，请点击紧邻**观察结果 (Observations)** 标题下的观察结果左侧的箭头。
- 要在“安全智能事件”(Security Intelligence Events) 页面上查看此事故，请点击观察结果详细信息部分中的**事件 (Events)** 链接。

步骤 4 （可选）请在事故详细信息页面上输入描述性信息：

提示：要最大化一致性和下面的选项的作用，请提前规划和记录您的命名约定、类别选择和置信度级别条件。

- 在以下字段中输入您喜欢的任意值：**名称 (Name)**、**说明 (Description)** 和**类别 (Category)**。
- 点击**置信度 (Confidence)** 的评价级别。

- 请通过从**状态 (Status)** 字段中的下拉列表中选择一个值，指示调查事故的状态。

事故摘要信息

“事故”页显示所有 威胁智能导向器事故的摘要信息。

表 3: 事故摘要信息

字段	说明
上次更新日期	自系统或用户上次更新事故以来的天数。要查看更新的日期和时间，请将光标悬停在该列中的相应值上。
事故 ID	事故的唯一标识符。此 ID 具有以下格式： `<type>-<date>-<number>` • `<type>` - 事故中涉及的指示器或可观察对象的类型。对于简单指示器，此值指示可观察对象类型：`IP`（IPv4 或 IPv6）、`URL` (URL)、`DOM`（域）或 `SHA` (SHA-256)。对于复杂指示器，此值为 `COM`。 • `<date>` - 创建事故的日期 (*yyyymmdd*)。 • `<number>` - 每日事故编号，即指定事故在每日事故序列中的发生位置的编号。</number> 请注意，此序列从 0 开始。例如，`DOM-20170828-10` 是当天创建的第 11 个事故。 在标识符旁边，系统会显示一个图标来指示事故是**部分实现**还是**完全实现**。有关详细信息，请参阅观察和事故生成，第 15 页。
指示器名称	事故中涉及的指示器的名称。要查看有关指示器的其他信息，请点击此列中的值；请参阅查看和管理指示器，第 30 页。
类型	事故中涉及的指示器的类型。 • 包含一个可观察对象的指示器显示数据类型（`URL`、`SHA-256` 等） • 包含两个或多个可观察对象的指示器显示为 `Complex` 。
采取的操作	系统就该事故所执行的操作。有关详细信息，请参阅事件详细信息，第 18 页。
状态	您对事故的调查状态。有关详细信息，请参阅事件详细信息，第 18 页。
删除（  ）	点击此图标将永久删除该事故。

事件详细信息

“事件详细信息”窗口显示了有关单个 威胁智能导向器 事件的相关消息。此窗口分为两个部分：

- 事故详细信息：基本信息，第 19 页

• 事故详细信息：指示器和观察结果 ，第 20 页

事故详细信息：基本信息

“事故详细信息”窗口的上半部分提供下述信息。

表 4: 基本事故信息字段

字段	说明
部分实现的 *IncidentID* 或完全实现的 *IncidentID*	一个图标，用于指示事故状态（已部分实现或已完全实现），以及事故的唯一标识符。 **注释** 在确定事故状态时，威胁智能导向器 会忽略不支持和无效的可观察对象以及不阻止列表中的可观察对象。
已打开	上次更新事故的日期和时间。
名称	您手动输入的自定义、可选事故名称。 提示：如果“说明”(Description) 字段（位于窗口底部）中有来自源的信息，则使用该字段中的信息来命名该事故。
说明	您手动输入的自定义、可选事故说明。 提示：如果“说明”(Description) 字段（位于窗口底部）中有来自源的信息，则使用该字段中的信息来说明该事故。
观察结果	事故中观察结果的数量。
置信度	您可以手动选择的可选评级，用于指示事故的相对重要性。
采取的操作	系统采取的操作：已监控、已阻止或已部分阻止。 已部分阻止表示事故同时包含已监控和已阻止观察结果。 **注释** **采取的操作**表示系统采取的操作，并不一定是在 威胁智能导向器 中选择的操作。有关详细信息，请参阅威胁智能导向器-防火墙管理中心 操作优先级 ，第 23 页。
类别	您手动添加到事故中的自定义可选标记或关键字。
状态	表示事故分析当前所处阶段的值。在首次更改**状态**之前，所有事故的状态值都将为新。 此字段为选填字段。根据贵组织的需求，可以考虑使用如下所示的状态值： • 新 - 事故需要调查，但尚未开始调查。 • 打开 - 目标正对事故进行调查。 • 已关闭 - 已对事故进行了调查，并已采取操作。 • 已拒绝 - 已对事故进行了调查，并已确定没有采取任何操作。

字段	说明
删除（  ）	点击此图标将永久删除此事故。

事故详细信息：指示器和观察结果

“事故详细信息”窗口的下半部分提供指示器和观察结果信息的深入视图。此信息以**指示器**字段、指示器模式和**观察结果**字段的形式组织。

指示器部分

当第一次查看指示器详细信息时，该部分仅显示指示器名称。

点击指示器名称可在“指示器”页上查看指示器。

点击指示器名称旁边的向下箭头可查看更多指示器详细信息，无需离开事故。详细信息字段包括：

表 *5:* 指示器字段

字段	说明
说明	源提供的指示器说明。
来源	包含指示器的源。点击此链接可访问完整的源详细信息。
过期	根据源的 **TTL** 值，事故将过期的日期和时间。
操作	与指示器关联的操作。有关详细信息，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作 ，第 37 页。
发布	指示器的发布设置。有关详细信息，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据 ，第 39 页。
下载 **STIX**	如果源类型为 `STIX`，请点击此按钮以下载 STIX 文件。

指示器模式

指示器模式是包含指示器的可观察对象和运算符的图形表示。运算符与指示器内的可观察对象链接。AND 关系通过 **AND** 运算符指示。OR 关系通过 **OR** 运算符或由多个可观察对象的紧密分组指示。

如果模式中的某个可观察对象已显示，则该可观察对象框为白色。如果某个可观察对象尚未显示，则该可观察对象框为灰色。

在指示器模式中：

- 点击**添加到不阻止列表 (Add to Do-Not-Block List)** 按钮 ，将可观察对象添加到不阻止列表。此图标在白色和灰色可观察对象框中均会显示。有关详细信息，请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表 ，第 40 页。
- 如果将光标悬停在白色可观察对象框上，则系统将在**观察结果**部分中突出显示相关的观察结果。

- 如果点击白色可观察对象框，则系统将在**观察结果**部分中突出显示相关的观察结果，将该观察结果滚动到视图中（如果存在多个观察结果），然后扩展该观察结果的详细显示。
- 如果将光标悬停在指示器模式中的灰色可观察对象框上方或点击它，则**观察结果**部分中没有任何更改。因为可观测对象未显示，因此没有可显示的观察结果详细信息。

观察结果部分

默认情况下，**观察结果**部分显示摘要信息，其中包括：

- 触发观察结果的可观察对象的类型（例如 `Domain`）
- 包含可观察对象的数据
- 观察结果是第一个观察结果还是随后的观察结果，例如 `1st` 或 `3rd`）

注释 如果单个可观察对象已显示三次或多次，则威胁智能导向器显示第一个和最后一个观察结果详细信息。有关中间观察结果的详细信息不可用。

- 观察结果的日期和时间
- 为可观测对象配置的操作

如果将光标悬停在**观察结果**部分中的某个观察结果上，系统将在指示器模式中突出显示相关的可观察对象。

如果点击**观察结果**部分中的某个观察结果，系统将在指示器模式中突出显示相关的可观察对象，并将第一个相关的可观察对象滚动到视图中（如果存在多个可观察对象）。点击某个观察结果还会在**观察结果**部分中展开观察结果的详细信息。

观察结果详细信息包括以下字段：

表 *6:* 观察结果详细信息字段

字段	说明
源代码	触发观察结果的流量的源 IP 地址和端口。
目的	触发观察结果的流量的目标 IP 地址和端口。
其他信息	与触发观察结果的流量相关的 DNS 和身份验证信息。
活动	如果观察结果生成连接、安全智能、文件或恶意软件事件，将显示此可点击的链接。点击该链接可查看 Cisco Secure Firewall Management Center事件表中的事件；请参阅《Cisco Secure Firewall Management Center 管理指南》。

查看 威胁智能导向器 观察的事件

有关 威胁智能导向器 观察结果生成的 Cisco Secure Firewall Management Center事件的更多信息，请参阅 Cisco Secure Firewall Management Center事件中的 威胁智能导向器 观察对象， 第 22 页。

为 威胁智能导向器 相关事件记录的系统操作可能会有所不同，具体取决于 威胁智能导向器 与其他 Cisco Secure Firewall Management Center 功能的交互。有关操作优先排序的详细信息，请参阅 威胁智能导向器-防火墙管理中心 操作优先级， 第 23 页。

开始之前

- 配置功能，如如何设置威胁智能导向器， 第 6 页中所述。
- 如配置策略以支持威胁智能导向器， 第 7 页中所述，确认在访问控制策略中启用了 威胁智能导向器 所需的事件日志记录。

过程

步骤 1 选择**集成** > **情报** > **事件**。

步骤 2 点击事故的**事故 ID** 值。

步骤 3 点击**指示器**部分中的观察结果以显示观察结果框。

步骤 4 通过点击该框左上角的箭头展开观察结果框。

步骤 5 点击观察结果信息中的**事件**链接。有关安全智能显示的详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的连接和安全智能事件一章。

Cisco Secure Firewall Management Center事件中的 威胁智能导向器 观察对象

如果完全配置了访问控制策略，威胁智能导向器 观察对象将生成以下 Cisco Secure Firewall Management Center事件：

表 *7:* 观察对象生成的 ***Cisco Secure Firewall Management Center***事件

观察对象内容	连接事件表	安全智能事件表	文件事件表	恶意软件事件表
SHA-256	是	否	是	是，如果处置是恶意软件或自定义检测。
域名、URL 或 IPv4/IPv6	是 威胁智能导向器相关的连接事件由与 威胁智能导向器相关的**安全智能类别**值标识。	是 威胁智能导向器相关的安全智能事件由与 威胁智能导向器相关的**安全智能类别**值标识。	否	否

影响所执行操作的因素

系统在检测到匹配威胁智能导向器可观察对象的流量后，何时采取操作以及采取何种操作由许多因素决定。

- 在威胁智能导向器采取操作前，安全智能之类的功能会采取操作。有关详细信息，请参阅威胁智能导向器-防火墙管理中心 操作优先级，第 23 页。
- 通常情况下，为可观察对象配置的操作（可能与为其父指示器或源配置的操作不同）是将要采取的操作。
- 由于 STIX 源可能包含复杂指示器，所以源的“操作”设置只能设为“监控”。不过，STIX 源中包含的各个简单指示器或可观察对象可以设置为“阻止”。
- 指示器和可观察对象的“操作”设置可以继承，也可以单独进行配置以覆盖继承设置。请参阅威胁智能导向器 配置中的继承，第 35 页 和 在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 37 页。
- 本来可以采取行动的流量可能在“不阻止”(Do Not Block) 列表中。有关详细信息，请参阅将威胁智能导向器 可观察对象添加到不阻止列表，第 40 页。
- 为部分和完全实现的事件执行配置的操作。
- 可部分阻止基于复杂指示器的事件。如果指示器包括受监控和已阻止的观察结果，可能会出现这种情况。
- 暂停发布会影响系统采取的操作。请参阅关于暂停发布，第 37 页 和 在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 39 页。
- 暂停 威胁智能导向器 功能将阻止所有操作。恢复功能后，可采取操作的数据可能与之前不同。有关详细信息，请参阅暂停 威胁智能导向器 并从元素中清除 威胁智能导向器 数据，第 38 页。

威胁智能导向器-防火墙管理中心 操作优先级

如果 威胁智能导向器 可观察对象操作与 防火墙管理中心 策略操作冲突，系统将优先执行以下操作：

- 安全智能不阻止
- TID 阻止
- 安全智能阻止
- TID 监控器
- 安全智能监控器

具体包括：

表 *8:* 威胁智能导向器 ***URL*** 可观察对象操作与安全智能操作

设置：安全智能操作	设置：威胁智能导向器可观察对象操作	威胁智能导向器事故字段：已执行的操作	安全智能事件字段：		
			操作	安全智能类别	原因
不阻止	监控或阻止	无 TID 事件	安全智能事件		
阻止	监控器	已阻止	阻止	由系统分析确定；请参阅 安全智能类别	URL 阻止 (URL Block)
	阻止	已阻止	阻止	TID URL 阻止	URL 阻止 (URL Block)
监控器	监控器	受监控	由在安全智能和 TID 之后处理的访问控制规则确定。	TID URL 监控器	URL 监控
	阻止	已阻止	阻止	TID URL 阻止	URL 阻止 (URL Block)

表 *9:* 威胁智能导向器 ***IPv4/IPv6*** 可观察对象操作与安全智能操作

设置：安全智能操作	设置：威胁智能导向器可观察对象操作	威胁智能导向器事故字段：已执行的操作	安全智能事件字段：		
			操作	安全智能类别	原因
不阻止	监控或阻止	无 TID 事件	安全智能事件		
阻止	监控器	无 TID 事件	阻止	由系统分析确定；请参阅 安全智能类别	IP 阻止
	阻止	已阻止	阻止	TID IPv4 阻止 TID IPv6 阻止	IP 阻止

设置：安全智能操作	设置：威胁智能导向器可观察对象操作	威胁智能导向器事故字段：已执行的操作	安全智能事件字段：		
			操作	安全智能类别	原因
监控器	监控器	受监控	由在安全智能和 TID 之后处理的访问控制规则确定。	TID IPv4 监控 TID IPv6 监控	IP 监控
	阻止	已阻止	阻止	TID IPv4 阻止 TID IPv6 阻止	IP 阻止

表 *10:* 威胁智能导向器域名可观察对象操作与 *DNS* 策略操作

设置：DNS 策略操作	设置：威胁智能导向器域名可观察对象操作	威胁智能导向器事故字段：已执行的操作	安全智能事件字段：		
			操作	安全智能类别	原因
不阻止	监控或阻止	无 TID 事件	安全智能事件		
丢弃、无法找到域 Sinkhole - 日志 Sinkhole - 阻止和记录	监控器	已阻止	阻止	由系统分析确定；请参阅 安全智能类别	DNS 阻止
	阻止	已阻止	阻止	TID 域名阻止	DNS 阻止
监控器	监控器	受监控	由在安全智能和 TID 之后处理的访问控制规则确定。	TID 域名监控器	DNS 监控
	阻止	已阻止	阻止	TID 域名阻止	DNS 阻止

表 *11: TID SHA-256* 可观察对象操作与恶意软件云查找文件策略

文件处置	威胁智能导向器 SHA-256 可观察对象操作	在 威胁智能导向器 事故中执行的操作	文件事件中的操作	恶意软件事件中的操作
清洁	监控或阻止	受监控	恶意软件云查找	不可用
恶意软件	监控或阻止	受监控	恶意软件云查找	不可用

文件处置	威胁智能导向器 **SHA-256** 可观察对象操作	在 威胁智能导向器 事故中执行的操作	文件事件中的操作	恶意软件事件中的操作
Custom	监控或阻止	受监控	• 恶意软件云查找，如果 SHA-256 不在自定义检测列表中。 • 自定义检测，如果 SHA-256 在自定义检测列表中。	• 恶意软件云查找，如果 SHA-256 不在自定义检测列表中。 • 自定义检测，如果 SHA-256 在自定义检测列表中。
未知	监控或阻止	受监控	恶意软件云查找	不可用

注释 先执行 威胁智能导向器 匹配，再由系统发送文件进行动态分析。

表 ***12: TID SHA-256*** 可观察对象操作与阻止恶意软件文件策略

文件处置	威胁智能导向器 **SHA-256** 可观察对象操作	在 威胁智能导向器 事故中执行的操作	文件事件中的操作	恶意软件事件中的操作
安全或未知	监控器	受监控	恶意软件云查找	不可用
	阻止	已阻止	• TID 阻止，如果 SHA-256 不在自定义检测列表中。 修改后的文件处置为自定义。 • 自定义检测阻止，如果 SHA-256 在自定义检测列表中。	TID 阻止 修改后的文件处置为自定义。

文件处置	威胁智能导向器 SHA-256 可观察对象操作	在 威胁智能导向器 事故中执行的操作	文件事件中的操作	恶意软件事件中的操作
恶意软件或自定义	监控器	已阻止	阻止恶意软件	阻止恶意软件
	阻止	已阻止	• TID 阻止，如果 SHA-256 不在自定义检测列表中。 修改后的文件处置为自定义。 • 自定义检测阻止，如果 SHA-256 在自定义检测列表中。	TID 阻止 修改后的文件处置为自定义。

查看和更改威胁智能导向器 配置

可以使用以下信息以查看并根据需要微调您的配置。

查看元素（托管设备）的 威胁智能导向器 状态

作为托管设备注册到 防火墙管理中心的所有设备都会在“元素”页面上自动显示。所有正确配置的元素（如配置策略以支持威胁智能导向器，第 7 页中的规定）都将收到所有当前已发布的可观察对象，包括在添加元素之前的注入的可观察对象。

过程

步骤 1 选择**集成** > **情报** > **元素**。

步骤 2 要查看元素是否已连接并已启用 威胁智能导向器，请将鼠标悬停在元素名称旁边的图标上。

注释
部署后，此页面上的信息最多可能需要 5 分钟才能更新，包括应用的访问控制策略以及是否启用 TID。

查看和管理源

"源”页面显示有关所有已配置源的摘要信息；请参阅源摘要信息，第 28 页。

过程

步骤 1 选择**集成** > **情报** > **源**。

步骤 2 查看您的源：

- 要过滤页面上显示的源，请点击 **过滤器**（）。有关详细信息，请参阅过滤表视图中的 威胁智能导向器 数据，第 34 页。
- 要查看详细的注入状态，请将光标悬停在**状态**列中的文本上。有关详细信息，请参阅源状态详细信息，第 29 页。

步骤 3 管理您的源：

- 要编辑**操作**设置，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 37 页。如果某个操作是固定的，则它是该源**类型**唯一支持的操作。
- 要编辑**发布 (Publish)** 设置，请点击 **滑块**（）。有关详细信息，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 39 页。
- 要暂停或继续 威胁智能导向器 更新源代码，请点击**暂停更新**或**继续更新**。如果暂停更新，则更新将暂停，但现有指示器和可观察对象仍保留在 TID 中。
- 要删除源，请点击 **删除**（）。如果源仍在处理，”删除“(Delete) 将灰显。删除一个源将删除与该源关联的所有指示器。关联的可观察对象也可能被删除；如果它们与系统中剩余的指示器关联，这些可观察对象将会保留。

源摘要信息

“源”页面显示所有已配置源的摘要信息。下表提供了对摘要显示中的字段的简要说明。有关这些字段的详细信息，请参阅源的相关配置主题中的说明：请参阅采集数据源的选项，第 8 页。

表 *13:* 源摘要信息

字段	说明
名称	源名称
类型	源的数据格式（STIX 或 平面文件）。
交付	威胁智能导向器 用于检索源的方法。
操作	系统配置为对匹配此源中所包含数据的流量执行的操作（阻止或监控）。 有关 威胁智能导向器 操作的详细信息，包括可用性、继承和重写继承，请参阅影响所执行操作的因素，第 23 页。

字段	说明
发布	开或关指定 威胁智能导向器 是否将源中的数据发布到已注册的元素（为支持 威胁智能导向器 而配置的托管设备）。 指示器可以从父源继承**发布**设置，而可观察对象可以从父指示器继承**发布**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 35 页。
上次更新时间	威胁智能导向器 上次更新源的日期和时间。
状态	源的当前状态。 • **新的** - 新建源。 • **已计划** - 已计划初始下载或后续更新，但尚未进行。 • **正在下载** - 威胁智能导向器 正在执行初始下载或更新刷新。 • **正在分析** 或 **正在处理**-威胁智能导向器 正在获取源代码。 • **已完成**-威胁智能导向器 已完成源代码的获取。 • **已完成，但有错误**-威胁智能导向器 已完成对源的获取，但某些可观察对象不受支持或无效。 • **错误**-威胁智能导向器 遇到问题。如果源是指定了**更新频率**的 TAXII 或 URL 源，并且未暂停更新，则 威胁智能导向器 将在下次计划更新时重试。 请刷新此页面更新状态。
编辑 ()	点击此图标可编辑源的设置。
删除（  ）	点击此图标将永久删除源。

源状态详细信息

当您将光标悬停在“源摘要”页面中的**状态**值上时，威胁智能导向器 提供下面所述的其他详细信息。

数据	说明
状态消息	简要说明源的当前状态。
上次更新日期	指定 威胁智能导向器 上次更新源的日期和时间。
下一次更新	对于 TAXII 和 URL 源，此值指定威胁智能导向器下次将在何时更新源。

数据	说明
指示灯	指定指示器计数： • **已消耗 (Consumed)** - 在最新的源更新过程中处理的指示器 威胁智能导向器 数量。此数字表示更新中包含的所有指示器，无论它们是被获取还是丢弃。 • **已丢弃** - 在最新更新期间，系统未添加到 威胁智能导向器 的格式错误的指示器数量。 **注释** 对于 TAXII 源，威胁智能导向器 提供单独的**上次更新时间**和**总数**指示器计数，因为 TAXII 更新会增加增量数据，而不是替换现有的数据。对于来自其他源类型的指示器，威胁智能导向器 仅提供**上次更新时间**计数，因为来自这些源的更新将完全替换现有的数据集。 如果所有指示器的可观察对象都**无效**，则 威胁智能导向器 将丢弃该指示器。
可观察对象	指定可观察对象计数： • **已消耗 (Consumed)** - 在最新的源更新过程中处理的可观察对象 威胁智能导向器 数量。此数字表示更新中包含的所有可观察对象，无论它们是被获取还是丢弃。 • **不受支持** - 在最新更新期间，系统未添加到威胁智能导向器 的不受支持的可观察对象数量。 有关受支持的可观察对象类型的详细信息，请参阅源要求，第 5 页中关于内容类型的信息。 • **无效** - 在最新更新期间，系统未添加到 威胁智能导向器 的无效可观察对象数量。 如果可观察对象未正确构造，则无效。例如，`10.10.10.10.123` 不是有效的 IPv4 地址。 **注释** 对于 TAXII 源，威胁智能导向器 提供单独的**上次更新时间**和**总数**可观察对象计数，因为 TAXII 更新会增加增量数据，而不是替换现有的数据。对于来自其他源类型的可观察性，威胁智能导向器 仅提供**上次更新时间**计数，因为来自这些源的更新将完全替换现有的数据集。

查看和管理指示器

指示器将从获取的源自动生成。有关此页面上的信息的详细信息，请参阅指示器摘要信息，第 31 页。

过程

步骤 1 选择**集成** > **情报** > **源**。

步骤 2 点击**指示器**。

步骤 3 查看您当前的指示器：

- 要过滤页面上显示的指示器，请点击**过滤器**（）。有关详细信息，请参阅过滤表视图中的威胁智能导向器 数据，第 34 页。
- 要查看有关指示器（包括关联的可观察对象）的其他详细信息，请点击指示器名称。有关详细信息，请参阅指标详细信息，第 32 页。
- 在**事件 (Incidents)** 列中，点击编号可查看与指示器关联的事故的信息，或将光标悬停在”事故“上以查看事故是完全实现还是部分实现。
- 要确定 威胁智能导向器 是否已完成从源获取指示器，请查看**状态**列。

步骤 4 管理您当前的指示器：

- 要编辑**操作**，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 37 页。如果某个操作是固定的，则它是该源**类型**唯一支持的操作。
- 要编辑**发布**设置，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 39 页。
- 要将一个指示器的一个或多个可观察对象列入不阻止名单，请点击指示器名称以访问“指示器详细信息”页面。有关详细信息，请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表，第 40 页。

指示器摘要信息

“指示器”页面显示与配置的源关联的所有指示器的摘要信息。

表 *14:* 指示器摘要信息

字段	说明
类型	• 使某一可观察对象列出该可观察对象的数据类型（URL、SHA-256 等）的指示器 • 使两个或多个可观察对象都被列复杂的指示器。 将鼠标指针悬停在类型上，以查看特定的可观察对象。
名称	指示器名称。
来源	包含指示器的源（父源）。
突发事件	有关与指示器关联的任何事故的信息： • 指定事故是 **部分** 或 **完全** 实现的图标 • 与指示器关联的事故的数量

字段	说明
操作	与指示器关联的操作。有关详细信息，请参阅在源、指示器或可观察对象级别编辑威胁智能导向器操作，第 37 页。 指示器可以从父源继承**操作**设置，而可观察对象可以从父指示器继承**操作**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 35 页。
发布	指示器的发布设置。有关详细信息，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 39 页。 指示器可以从父源继承**发布**设置，而可观察对象可以从父指示器继承**发布**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 35 页。
上次更新时间	威胁智能导向器上次更新指示器的日期和时间。
状态	指示器的当前状态。 • **待处理**-威胁智能导向器 正在获取指示器的可观察对象。 • **完成**-威胁智能导向器 已成功获取指示器的所有可观察对象。 • **已完成，但有错误**-威胁智能导向器 已完成获取指示器，但某些可观察对象不受支持或无效。

指标详细信息

“指示器详细信息”页面显示事件的指示器和可观察数据。

表 *15:* 指示器详细信息

字段	说明
名称	指示器名称。
说明	源提供的指示器说明。
来源	包含指示器的源。
过期	根据源的 **TTL** 值，指示器将过期的日期和时间。
操作	与指示器关联的操作。有关详细信息，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 37 页。 指示器可以从父源继承**操作**设置，而可观察对象可以从父指示器继承**操作**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 35 页。

字段	说明
发布	指示器的发布设置。有关详细信息，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 39 页。 指示器可以从父源继承**发布**设置，而可观察对象可以从父指示器继承**发布**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 35 页。
指示器模式	构成指示器模式的可观察对象和运算符。运算符与指示器内的可观察对象链接。AND 关系通过 **AND** 运算符指示。OR 关系通过 **OR** 运算符或由多个可观察对象的紧密分组指示。 或者，点击 **添加到不阻止列表** 按钮，将可观察对象添加到不阻止列表。有关详细信息，请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表，第 40 页。

查看和管理可观察对象

“可观察对象”页面显示所有成功注入的可观察对象；请参阅可观察对象摘要信息，第 34 页。

开始之前

- 按照获取要用作源的 TAXII 源，第 9 页、从 URL 获取源，第 10 页或上传本地文件以用作源，第 11 页中的说明配置一个或多个源。

过程

步骤 1 选择**集成** > **情报** > **源**。

步骤 2 点击**可观察对象**。

步骤 3 查看您当前的可观察对象：

- 要过滤页面上显示的可观看对象，请点击**过滤器**（  ）。有关详细信息，请参阅过滤表视图中的 威胁智能导向器 数据，第 34 页。
- 如果**值**列中的信息被剪切掉，请将鼠标指针悬停在值上。
- 要查看包含可观察对象的指示器，请点击**指示器**列中的数字。“事故”页面将会打开，并采用可观察对象值作为过滤器。有关详细信息，请参阅查看和管理指示器，第 30 页。

步骤 4 管理您当前的可观察对象：

- 要编辑**操作**，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 37 页。
- 要编辑可观察对象的**发布**设置，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 39 页。
- 要更改可观察对象的到期日期，请修改父源的**TTL**。有关详细信息，请参阅查看和管理源，第 27 页。

- 要将可观察对象添加到“不阻止”列表，请点击**添加到不阻止列表**按钮。有关详细信息，请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表，第 40 页。

可观察对象摘要信息

“可观察对象”页面显示所有获取的可观察对象的摘要信息。

表 *16:* 可观察对象摘要信息

字段	说明
类型	可观察对象数据的类型：SHA-256、Domain、URL、IPv4 或 IPv6。
值	包含可观察对象的数据。
指示灯	包含可观察对象的父指示器的数量。
操作	为可观察对象配置的操作。有关详细信息，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 37 页。 指示器可以从父源继承**操作**设置，而可观察对象可以从父指示器继承**操作**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 35 页。
发布	可观察对象的发布设置；请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 39 页。 指示器可以从父源继承**发布**设置，而可观察对象可以从父指示器继承**发布**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 35 页。
更新时间	威胁智能导向器上次更新可观察对象的日期和时间。
过期	基于父指示器的 **TTL** 自动从威胁智能导向器清除可观察对象的日期。
添加到不阻止列表 (Add to Do-Not-Block List) 按钮	点击此按钮会将可观察对象添加到“不阻止”列表；请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表，第 40 页。

过滤表视图中的 威胁智能导向器 数据

过程

步骤 1 选择以下其中一个 威胁智能导向器 表视图：

- **集成** > **情报** > **事件**

- **集成** > **情报** > **源**
- **集成** > **情报** > **源**，然后点击**指示器**
- **集成** > **情报** > **源**，然后点击**可观察对象**

步骤 2 点击 **过滤器**（） 并选择过滤器属性。

步骤 3 为该过滤器属性选择或输入一个值。

过滤器区分大小写。

步骤 4 （可选）若要按多个属性进行过滤，请点击 **过滤器**（），然后重复执行步骤 2 和步骤 3。

步骤 5 要取消上次应用过滤器后所做的更改，请点击**取消**。

步骤 6 点击**应用**以使用应用的过滤器刷新表。

步骤 7 要单独删除某个过滤器属性，请点击该过滤器属性旁边的 **删除**（），然后点击**应用 (Apply)** 以刷新表。

威胁智能导向器 配置中的继承

当威胁智能导向器摄取源中的智能数据时，将创建指示器和可作为该源子对象的可观察对象。创建后，这些子对象将从父配置继承**操作**和**发布**设置。

指示器从父源继承这些设置。指示器只能有一个父源。

可观察对象从父指示器继承这些设置。可观察对象可以有多个父指示器。

有关详细信息，请参阅：

- 继承多个父级的 TID 设置，第 35 页
- 关于覆盖继承的 TID 设置，第 36 页

继承多个父级的 TID 设置

如果某个可观察对象有多个父指示器，则系统会比较从所有父级继承的设置，并将最安全的选项分配给该可观察对象。因此：

- **操作**：`Block` 比 `Monitor` 安全
- **发布**：`On` 比 `Off` 安全

例如，SourceA 可能会贡献 IndicatorA 和相关的 ObservableA：

设置	SourceA	IndicatorA	ObservableA
操作	阻止 (Block)	阻止 (Block)	阻止 (Block)
发布	关闭	关闭	关闭

如果 SourceB 以后贡献 IndicatorB，其还包括 ObservableA，则系统会修改 ObservableA，如下所示：

设置	SourceB	IndicatorB	ObservableA
操作	监控器	监控器	`Block`（从 IndicatorA 继承）
发布	打开	打开	`On`（从 IndicatorB 继承）

在此示例中，ObservableA 有两个父级：一个父级用于其**操作**设置，另一个父级用于其**发布**设置。如果手动编辑可观察对象的设置，然后恢复设置，则系统会将**操作**设置设为 IndicatorA 值，并将**发布**设置设为 IndicatorB 值。

关于覆盖继承的 TID 设置

要覆盖继承的设置，请在子级更改此设置；请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 37 页和在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 39 页。覆盖继承的设置后，尽管父对象发生了更改，但子对象仍保留该设置。

例如，您可以先设置以下初始设置，而不设置任何覆盖：

设置	SourceA	IndicatorA	ObservableA1	ObservableA2
发布	关闭	关闭	关闭	关闭

如果覆盖 IndicatorA 的设置，则设置如下：

设置	SourceA	IndicatorA	ObservableA1	ObservableA2
发布	关闭	打开	打开	打开

在这种情况下，对 SourceA 的**发布**设置所做的任何更改都不再自动层叠到 IndicatorA。但是，从 IndicatorA 到 ObservableA1 和 ObservableA2 的继承仍在继续，因为可观察对象设置当前未设置为覆盖值。

如果以后覆盖 ObservableA1 的设置：

设置	SourceA	IndicatorA	ObservableA1	ObservableA2
发布	关闭	打开	关闭	打开

对 IndicatorA 的**发布**设置所做的任何更改都不再自动层叠到 ObservableA1。但是，这些更改将继续层叠到 ObservableA2，因为它未设置为覆盖值。

在可观察对象级别，您可以从覆盖设置恢复为继承的设置，系统会将层叠设置更改从父指示器自动恢复到该可观察对象。

在源、指示器或可观察对象级别编辑 威胁智能导向器操作

注意：

- 编辑父项的操作会为所有子项设置该操作。如果在源级别编辑该操作，则会为其所有指示器设置该操作。如果在指示器级别编辑该操作，则会为其所有可观察对象设置该操作。
- 编辑子项的操作会中断继承。如果在指示器级别编辑该操作，随后又在源级别编辑该操作，则在编辑单个指示器的操作之前，系统会保留该指示器的操作。如果在可观察对象级别编辑该操作，随后又在指示器级别编辑该，则在编辑单个可观察对象的操作之前，系统会保留该可观察对象的操作。在可观察对象级别，您可以自动恢复到父指示器的操作。有关继承的更多信息，请参阅威胁智能导向器 配置中的继承，第 35 页。

您可能还想要查看其他影响所执行操作的因素，第 23 页。

过程

步骤 1 选择如下选项之一：

- **集成** > **情报** > **源**

  注释
  威胁智能导向器不支持在源级别阻止 TAXII 源。如果 TAXII 源包含一个简单指示器，则可以在指示器或可观察对象级别进行阻止。

- **集成** > **情报** > **源**，然后点击**指示器**

  注释
  威胁智能导向器不支持阻止复杂的指示器，而是在复杂指示器中阻止单个可观察对象。

- **集成** > **情报** > **源**，然后点击**可观察对象**

步骤 2 使用 **操作 (Action)** 下拉列表选择 **监控**（  ） 或 **阻止图标**（  ）。

步骤 3 （仅可观察对象）如果要从父指示器继续继承操作设置，请点击可观察对象的**操作 (Action)** 设置旁边的 **恢复 (Revert)**。

关于暂停发布

- 如果在功能级别暂停发布，系统将清除存储在您的元素上的所有 威胁智能导向器可观察对象。这意味着 威胁智能导向器 无法检测、监控或阻止威胁。您的系统上的其他安全功能不受影响。
- 如果在源、指示器或可观察对象级别暂停发布，系统将从您的元素中删除暂停的 威胁智能导向器 可观察对象，以防它们匹配流量。

- 对父级暂停发布会暂停所有子项。如果在源级别暂停发布，则会为其所有指示器暂停发布。如果在指示器级别暂停发布，则会为其所有可观察对象暂停发布。
- 为子项暂停发布会中断继承。如果在指示器级别暂停发布，随后在源级别发布，则该指示器的发布将保持暂停状态，直到更改指示器的单个设置。如果在可观察对象级别暂停发布，随后在指示器级别发布，则该可观察对象的发布将保持暂停状态，直到更改可观察对象的单个设置。在可观察对象级别，您可以自动恢复到父指示器的发布状态。有关继承的更多信息，请参阅威胁智能导向器 配置中的继承，第 35 页。
- 对于上传源的发布只能在指示器级别暂停。
- 有关暂停发布可观察对象与将可观察对象添加到“不阻止”列表的比较，请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表，第 40 页。
- 如果已对个别可观察对象或指示器指定发布/暂停设置，则即便更新包含相同的可观察对象或指示器，源更新也不会更改。
- 在对象管理页面上可以禁用“发布”。请参阅修改可观察对象的发布频率，第 39 页。
- “源”页上用于暂停更新的选项与向元素发布数据无关；它适用于更新来自源的 防火墙管理中心上的源信息。

暂停 威胁智能导向器 并从元素中清除 威胁智能导向器 数据

⚠

注意 此设置将暂停向所有元素发布内容，清除元素中存储的所有 威胁智能导向器 可观察对象，并停止使用 威胁智能导向器 功能检查流量。

要在更精细的级别禁用可观察对象，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 39 页。

管理中心上的数据（现有事件和配置的源、指示器和可观察对象，以及来源采集）不受此设置影响。

过程

步骤 1 选择**集成** > **智能** > **设置**。

步骤 2 点击**暂停**。

下一步做什么

当您准备好恢复同步元素上的 威胁智能导向器 数据并生成观察结果时，请在此页面手动**恢复**发布。管理中心上的现有可观察对象将同时发布到所有元素。

在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据

如果在源级别启用发布，系统将自动发布初始源数据和任何后续更改，包括：

- 定期源刷新引起的更改
- 由系统操作引起的更改（例如，**TTL** 到期）
- 任何用户启动的更改（例如，指示器或可观察对象的**操作**设置的更改）

注释 要同时从设备（元素）中清除所有 威胁智能导向器 可观察对象，请参阅暂停 威胁智能导向器 并从元素中清除 威胁智能导向器 数据，第 38 页。

开始之前

在暂停发布之前，请了解关于暂停发布，第 37 页中所述的后果。

过程

步骤 1 选择如下选项之一：

- **集成** > **情报** > **源**
- **集成** > **情报** > **源**，然后点击**指示器**
- **集成** > **情报** > **源**，然后点击**可观察对象**

步骤 2 找到 **发布** 滑块（  ）并使用它切换发布到元素。

步骤 3 （仅可观察对象）如果要从父指示器继续继承发布设置，请点击可观察对象的**发布 (Publish)** 设置旁边的**恢复 (Revert)**。

下一步做什么

- 至少等待 10 分钟，以便元素接收更改。涉及大源的更改将需要更长时间。
- （可选）在可观察对象级别更改 TID 数据的发布频率；请参阅修改可观察对象的发布频率，第 39 页。

修改可观察对象的发布频率

默认情况下，系统每隔 5 分钟便会将可观察对象发布到 TID 元素。使用此过程可将该间隔设置为其他值。

开始之前

- 允许在可观察对象级别启用 TID 数据发布；请参阅在源、指示器或可观察对象级别暂停或发布威胁智能导向器 数据，第 39 页。

过程

步骤 1 选择**对象** > **对象管理** > **安全智能** > **网络列表和源**。

步骤 2 点击 **Cisco-TID-Feed** 接口旁边的 **编辑** (✎) 。

步骤 3 从**更新频率**下拉列表中选择值：

- 选择**禁用**可停止将可观察对象数据发布到元素。
- 选择任何其他值可设置可观察对象发布的间隔。

步骤 4 点击**保存**。

关于将 威胁智能导向器 可观察对象添加到“不阻止”列表

如果希望免除对简单指示器中的某个可观察对象执行指定的 **操作**（让流量通过，而不进行监控或阻止），可以将此可观察对象加入“不阻止”列表。

在复杂指示器中，威胁智能导向器 在评估流量时会忽略“不阻止”列表中的可观察对象，但仍会对该指示器中的其他可观察对象进行评估。例如，如果指示器包括可观察对象 1 和可观察对象 2，二者通过 AND 运算符链接，并且您将可观察对象 1 加入“不阻止”列表，则 威胁智能导向器 在看到可观察对象 2 时将生成完全实现的事故。

相比之下，在同一个复杂的指示器中，如果禁用可观察对象 1 的发布，而不是将其加入“不阻止”列表，则 威胁智能导向器 在看到可观察对象 2 时将生成部分实现的事故。

注释 如果将可观察对象添加到“不阻止”列表，则其优先级始终优于 **操作** 设置，与该可观察对象中的此设置是继承值还是覆盖值无关。

源更新不会影响它所包含的可观察对象的“不阻止”列表设置。

将 威胁智能导向器 可观察对象添加到不阻止列表

有关使用不阻止列表的详细信息，请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表，第 40 页。

提示 “添加至不阻止列表”(Add to Do Not Block List) 按钮 (☑) 可以显示在 Web 接口中的多个位置。您可以通过点击此按钮将可观察对象添加到任何这些位置的“不阻止”列表。

过程

步骤 1 选择 **集成** > **情报** > **源**，然后点击**可观察对象**。

步骤 2 导航到您希望允许的可观察对象。

步骤 3 点击该可观察对象的 （**添加到不阻止列表 (Add to Do-Not-Block List)**）。

下一步做什么

（可选）如果您需要从“不阻止”列表删除某可观察对象，再次点击该按钮即可。

查看 STIX 源文件

过程

步骤 1 选择 **集成** > **情报** > **源**，然后点击**指示器**。

步骤 2 点击指示器名称。

步骤 3 点击**下载 STIX**。

步骤 4 在文本编辑器中打开文件。

对威胁智能导向器进行故障排除

以下章节介绍常见 威胁智能导向器 问题可能的解决方案和缓解方案。

获取或上传平面文件源会生成错误

如果系统无法获取或上传平面文件源，请检查平面文件中的数据与**集成** > **情报** > **源**页面上的**类型**列是否匹配。

TAXII 或 URL 源更新会生成错误

如果 TAXII 或 URL 源更新生成源状态错误，请检查您的服务器证书是否已过期。如果证书已过期，请输入新的**服务器证书**或删除现有的**服务器证书**，以便威胁智能导向器可以检索新证书。有关详细信息，请参阅为 威胁智能导向器 源配置 TLS/SSL 设置，第 13 页。

“阻止”操作不是可用于指示器或源，只有“监控”可以

您可以更改指示器或源中单个可观察对象的操作。

威胁智能导向器 表视图返回“无结果”

表视图包括**源**、**指示器**、**可观察对象**和**事故**页面。

如果在某个 威胁智能导向器 表视图中没有看到数据：

- 检查您表过滤器并考虑展开**上次更新**过滤器属性的时间窗口；请参阅过滤表视图中的 威胁智能导向器 数据，第 34 页。
- 验证您是否正确配置了您的源；请参阅采集数据源的选项，第 8 页。
- 验证是否已将访问控制策略和相关策略配置为支持 威胁智能导向器；请参阅配置策略以支持威胁智能导向器，第 7 页。例如，如果您的 SHA-256 可观察对象没有生成观察结果，请验证您部署的访问控制策略是否包含一个或多个调用**恶意软件云查找**或**阻止恶意软件**文件策略的访问控制规则。
- 验证是否已将 威胁智能导向器 支持的访问控制策略和相关策略部署到您的元素；请参阅部署配置更改。
- 验证您没有在功能级别暂停 威胁智能导向器 数据发布；请参阅暂停 威胁智能导向器 并从元素中清除 威胁智能导向器 数据，第 38 页。

系统正在经历速度变慢或性能下降

有关性能影响的详细信息，请参阅威胁情报导向器的性能影响，第 3 页。

Cisco Secure Firewall Management Center表视图不显示 威胁智能导向器 数据

如果要将可观察对象发布到您的元素，但没有 威胁智能导向器数据显示在连接、安全智能、文件或恶意软件事件表中，请检查部署到您的元素的访问控制和文件策略。有关详细信息，请参阅配置策略以支持威胁智能导向器，第 7 页。

威胁智能导向器 数据导致一个或多个元素不堪重负

如果 威胁智能导向器 数据导致您的一个或多个设备不堪重负，请考虑暂停 威胁智能导向器 发布和清除存储在您的元素上的数据。有关详细信息，请参阅暂停 威胁智能导向器 并从元素中清除 威胁智能导向器 数据，第 38 页。

系统正在执行恶意软件云查找而不是 TID 块

这是由设计决定的。有关详细信息，请参阅威胁智能导向器-防火墙管理中心 操作优先级，第 23 页。

系统正在执行安全智能或 DNS 策略操作，而不是 TID 操作

这是由设计决定的。有关详细信息，请参阅威胁智能导向器-防火墙管理中心 操作优先级，第 23 页。

TID 被禁用

- 向设备添加内存。威胁情报导向器只能在内存至少为 15 GB 的设备上使用。

- 为 Cisco Secure Firewall Management Center启用 REST API 访问。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的启用 *REST API* 访问 。

系统不会生成 威胁智能导向器 事故或执行您预期的 威胁智能导向器 操作

- 验证是否所有托管设备均已为 威胁智能导向器 正确启用和配置。请参阅查看元素（托管设备）的 威胁智能导向器 状态， 第 27 页 和 配置策略以支持威胁智能导向器， 第 7 页。
- 将更改发布到元素至少需要 5-10 分钟时间，如果发布的数据源较大，可能需要更长的时间。
- 检查可观察对象的操作设置。请参阅查看和管理可观察对象， 第 33 页。
- 有关影响系统所执行的 威胁智能导向器 操作的其他因素列表，请参阅影响所执行操作的因素， 第 23 页。
- 元素（托管设备）可能不具备您认为它们应有的威胁数据。请参阅关于暂停发布， 第 37 页。

遇到一次特定威胁还会生成多个事故

如果单个指示器包括在多个源中，可能会出现这种情况：

有关详细信息，请参阅处理重复指示器， 第 12 页。

威胁智能导向器的历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
处理多个 STIX 源中包含的指示器	7.1	任意	如果 STIX 源包含相同的指示器，则会为每个源创建一个指示器，而这可能会导致为同一指示器生成多个事件。以前，只有最后下载的源才会生效。

功能	防火墙管理中心最低版本	最低版本	详细信息

操作优先级的变化	6.5	任意	如果有多项 Firepower 功能可能适用于特定可观察对象，这些变化将适用。
			TID 阻止/监控可观察对象操作的优先级现在高于安全智能的阻止/监控。
			重要事项
			系统仍会像以前一样有效地处理流量。之前被阻止的流量仍被阻止，并且受监控的流量仍受到监控。这只会将事件中报告的组件更改为负责操作。您可能还会看到生成了更多的 TID 事件。
			• 如果配置了阻止TID 可观察对象操作，即使流量也与设置为阻止的安全智能阻止操作匹配：
			  • 连接事件中的安全智能类别是 TID 阻止的变体。
			  • 系统会生成一个 TID 事件，其中包含被阻止的操作。
			• 如果您配置监控 TID 可观察对象操作，即使流量与安全智能监控规则匹配也是如此：
			  • 连接事件中的安全智能类别是TID 监控器的一种变体
			  • 系统会生成一个 TID 事件，其中包含被监控的操作。
			以前，在上述每种情况下，系统通过分析报告类别，但未生成 TID 事件。

安全防火墙威胁智能导向器	6.2.2	任意	引入的功能：利用该功能，您可以使用来自外部源的威胁智能来识别和处理威胁。 新屏幕： 包含多个选项卡的新顶级**智能**菜单。 支持的平台： Cisco Secure Firewall Management Center

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。