安全情报

通过安全智能策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。以下主题介绍如何实施安全智能。

- 关于安全情报， 第 1 页
- 安全智能许可证要求， 第 3 页
- 配置安全智能， 第 3 页
- 监控安全智能， 第 4 页
- 安全智能示例， 第 5 页

关于安全情报

通过安全智能策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。在使用访问控制策略评估不良流量前，系统会将其丢弃，从而减少系统资源的使用量。

您可以根据以下条件阻止流量：

- 思科 Talos 情报小组 (Talos) 源 - Talos 提供对定期更新的安全智能源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。系统定期下载智能源更新，从而提供新的威胁智能，而无需重新部署配置。

注释 默认情况下，Talos 源每小时更新一次。您可以从**设备 (Device)** > **更新 (Updates)**页面更改更新频率，甚至根据需要更新智能源。

- 网络和 URL 对象 - 如果您知道要阻止的特定 IP 地址或 URL，则可为其创建对象并将其添加到阻止列表或例外列表。请注意，您无法使用 FQDN 或范围规格的网络对象。

创建用于 IP 地址（网络）和 URL 的单独列表。

注释 如果 HTTP/HTTPS 请求针对使用 IP 地址而不是主机名的 URL，则系统会在网络地址列表中查找 IP 地址信誉。无需在网络和 URL 列表中复制 IP 地址。

创建阻止列表例外

对于每个阻止列表，您可以创建关联的例外列表，也称为不阻止列表。例外列表的唯一目的是豁免阻止出现在阻止列表中的 IP 地址或 URL。也就是说，如果发现需使用且已知安全的地址或 URL 位于在阻止列表上配置的智能源中，则可豁免该网络/URL，而无需从阻止列表中完全删除该类别。

随后访问控制策略会评估被豁免的流量。有关允许或丢弃连接的最终决定基于连接匹配的访问控制规则。访问规则还会决定恶意软件检查是否应用于连接。

安全智能源类别

下表介绍思科 Talos 情报小组 (Talos) 源中的可用类别。这些类别可用于网络和 URL 阻止操作。

这些类别可能会随时间而变化，因此新下载的源可能会存在类别更改。配置安全智能时，您可以点击类别名称旁边的信息图标以查看说明。

表 *1:* 思科 *Talos* 情报小组 *(Talos)* 源类别

安全情报类别	说明
攻击者	出站恶意活动已知的活动扫描工具和主机
Banking_fraud	从事与电子银行相关的欺诈活动的网站
Bogon	Bogon 网络和未分配的 IP 地址
Bots	托管二进制恶意软件丢弃程序的站点
CnC	托管僵尸网络的命令和控制服务器的站点
加密货币挖矿活动	提供对用于挖掘加密货币的池和钱包的远程访问的主机
Dga	用于生成作为与命令和控制服务器的交汇点的大量域名的恶意软件算法
Exploitkit	指定用于识别客户端中的软件漏洞的软件包
High_risk	根据来自安全图的 OpenDNS 预测安全算法进行匹配的域和主机名
IOC	观察到涉及感染指标 (IOC) 的主机
Link_sharing	未经许可共享版权文件的网站
恶意	表现出不一定属于另一种更精细的威胁类别的恶意行为的站点
恶意软件	托管恶意软件二进制或漏洞包的站点

安全情报类别	说明
Newly_seen	最近注册或尚未通过遥测发现的域。 **注意** 目前，此类别没有任何有效的源，已预留以供将来使用。
Open_proxy	允许匿名 Web 浏览的开放代理
Open_relay	已知用于垃圾邮件的开放邮件中继
网络钓鱼	托管网络钓鱼页面的站点
解决方案	主动参与恶意或可疑活动的 IP 地址和 URL
垃圾邮件	已知用于发送垃圾邮件的邮件主机
间谍软件	已知包含、提供或支持间谍软件和广告软件活动的网站
可疑	看似可疑并具有类似于已知恶意软件的特征的文件
Tor_exit_node	已知为 Tor Anonymizer 网络提供出口节点服务的主机

安全智能许可证要求

必须启用 **威胁**许可证，才能使用安全智能。请参阅启用或禁用可选许可证。

配置安全智能

通过安全智能策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。所有允许的连接仍会通过访问控制策略进行评估，并且最终可能会被丢弃。必须启用 IPS 许可证 (IPS license)，才能使用安全智能。

过程

步骤 1 依次选择**策略 (Policies)** > **安全智能 (Security Intelligence)**。

步骤 2 如果未启用策略，请点击**启用安全智能 (Enable Security Intelligence)**按钮。

您可以通过点击**安全智能 (Security Intelligence)** 开关切换到**关闭 (Off)** 随时禁用策略。配置将被保留，因此，当您再次启用该策略时，无需重新配置。

步骤 3 配置安全智能。

网络（IP 地址）和 URL 有单独的阻止列表。

a) 点击**网络**或 **URL** 选项卡显示要配置的列表。

b) 在阻止/丢弃列表中，点击 **+**，选择要立即丢弃其连接的对象或智能源。

对象选择器按类型对单独选项卡上的对象和智能源进行分门别类。如果所需的对象尚不存在，请点击列表底部的**创建新对象**链接，立即创建对象。有关思科 Talos 情报小组 (Talos) 源的说明，请点击源旁边的 **i** 按钮。另请参阅安全智能源类别，第 2 页。

注释 安全智能会忽略使用 /0 掩码的 IP 地址块。这包括 any-ipv4 和 any-ipv6 网络对象。不得选择将这些对象用于网络阻止操作。

c) 在“不阻止”列表中，点击 **+** 并选择阻止列表的任何例外情况。

配置该列表的唯一原因是对阻止列表中的 IP 地址或 URL 进行例外处理。被免除的连接随后将通过访问控制策略进行评估，且仍然可能会被丢弃。

d) 重复此过程以配置其他阻止列表。

步骤 4 （可选。）点击**编辑日志记录设置**按钮 (⚙) 来配置日志记录。

如果启用了日志记录，系统会记录与阻止列表条目匹配的任意项。系统不记录例外条目的匹配项，但如果被免除的连接与启用日志记录的访问控制规则匹配，您会收到日志消息。

配置以下设置：

- **连接事件日志记录** - 点击开关以启用或禁用日志记录。
- **系统日志** - 如果要将事件副本发送到外部系统日志服务器，请选择该选项并选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**添加系统日志服务器**并创建对象。

  由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

监控安全智能

如果启用安全智能策略的日志记录，则系统会为与阻止列表中项目匹配的每个连接生成安全智能事件。这些连接已有匹配的连接事件。

已丢弃连接的统计信息显示在“监控”(Monitoring) 页面上的各控制面板中。

监控 > **访问和 SI 规则**控制面板显示排名靠前的访问规则及匹配流量的安全智能等效对象。

此外，可依次选择**监控** > **事件**，然后选择**安全智能**视图，查看安全智能事件以及**连接**选项卡上的相关连接事件。

- 事件中的“SI 类别 ID”字段指示阻止列表中匹配的对象，如网络或 URL 对象或源。
- 连接事件中的“原因”字段解释为什么应用了事件中显示的操作。例如，与“IP 阻止”或“URL 阻止”等原因配对的“阻止”操作表示某连接已被安全智能丢弃。

安全智能示例

使用案例章节涵盖实施安全智能策略的示例。请参阅如何阻止威胁。

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。