查看威胁智能控制面板

威胁智能 (Threat Intelligence) 页面列出了 Cisco Secure Workload 管道的最新数据集，该管道通过根据外部已知的恶意软件命令和控制地址检查数据中心工作负载以及进程和地理位置中的安全漏洞来识别和隔离威胁。

要管理威胁智能，请从导航窗格中选择**管理 (Manage)** > **服务设置 (Service Settings)** > **威胁智能 (Threat Intelligence)**。

威胁智能 (Threat Intelligence) 页面显示威胁智能数据集的更新状态。这些数据集都会自动更新。

注释 威胁智能功能需要连接到思科 Cisco Secure Workload 服务器才能自动更新。您的企业出站 HTTP 请求可能需要：

- 允许来自企业防火墙出站规则的以下域：`UAS.tetrationcloud.com`
- 配置出站 HTTP 连接。

在没有出站连接的环境中，直接上传数据集。有关详细信息，请参阅**手动上传**部分。

表 *1:* 数据集

数据集	说明
NVD CVE	与安全相关的软件缺陷、CVSS 基本评分、易受攻击的产品配置和漏洞分类
MaxMind Geo	识别源 IP 的位置和其他特征
NIST RDS	NIST 参考数据集，包含已知的可追溯软件应用的数字签名
Team Cymru	洞察 3,000 多个僵尸网络命令和控制 IP
Hash Verdict	进程散列上的 Cisco Secure Workload 判定（仅适用于“自动更新”部分）。

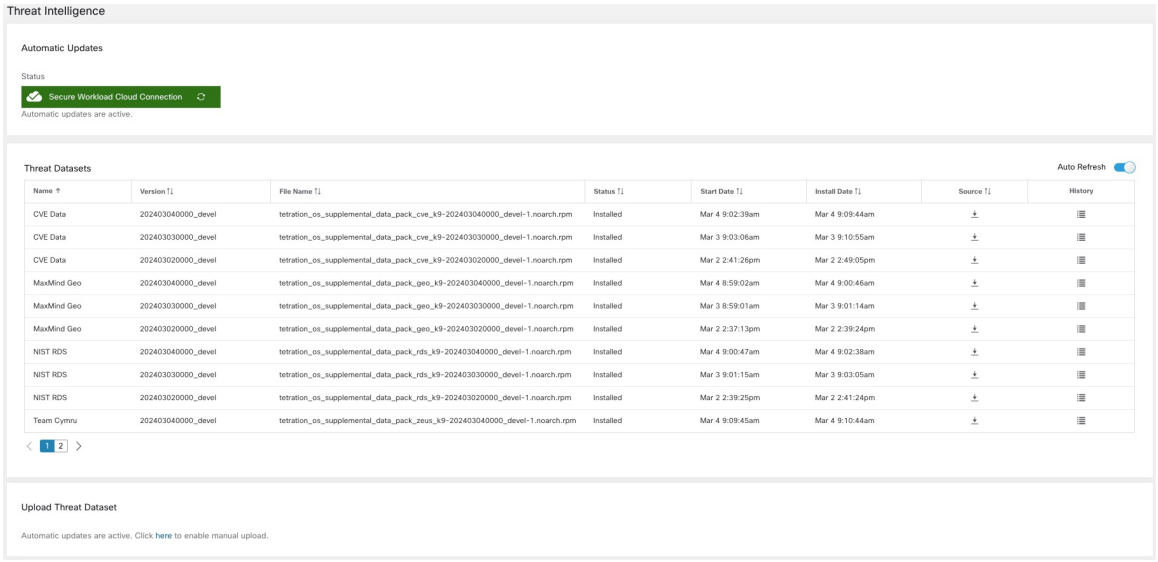
注释 如果 MaxMind Geo 数据集是在早期版本中手动上传的，则必须重新上传相应的 RPM，才能在“流可视性”页面上查看位置和相关信息。

- 自动更新, on page 2
- 手动上传数据集, on page 2

自动更新

Cisco Secure Workload 通过与此处提供的全局数据集同步，在 UTC 每天凌晨 3 点至 4 点更新威胁数据集。全局数据集每周、周五或周一刷新。威胁智能控制面板列出数据集以及数据集的最后更新日期。

Figure 1: 威胁智能



手动上传数据集

Note **安排手动上传：**数据集 RPM 文件每周都会被发布到 Cisco Secure Workload 更新门户。建议您通过为管理员配置计划来定期安装最新版本。

下载更新的数据集

从此处下载最新的威胁数据集。

上传最新的数据集

Before you begin

以**站点管理员**或**客户支持主管**身份登录。

Procedure

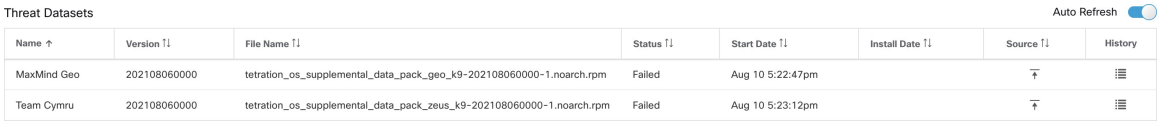
步骤 1 从导航窗格中，选择**管理 (Manage)** > **服务设置 (Service Settings)** > **威胁智能 (Threat Intelligence)**。

步骤 2 在**上传威胁数据集 (Upload Threat Dataset)** 部分下，启用手动上传。

步骤 3 点击**选择补充 RPM (Select Supplemental RPM)**，然后选择从 Cisco Secure Workload 更新门户下载的 RPM 文件。

步骤 4 点击**上传 (Upload)**。
系统将启动 RPM 上传过程，并在进度条上显示状态。上传后，系统会在后台处理和安装 RPM 文件。威胁数据集在安装完成后更新。

Figure 2: 威胁数据集



上传最新的数据集

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。