集成CTR和Threat Grid云

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[背景信息](#)
[配置](#)
[CTR控制台 — 配置Threat Grid模块](#)
[Threat Grid控制台 — 授权Threat Grid访问威胁响应](#)
[验证](#)

简介

本文档介绍将思科威胁响应(CTR)与Threat Grid(TG)云集成以执行CTR调查的步骤。

作者：Jesus Javier Martinez，编辑者：Cisco TAC工程师Yeraldin Sanchez。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科威胁响应
- Threat Grid

使用的组件

本文档中的信息基于以下软件版本：

- CTR控制台（具有管理员权限的用户帐户）
- Threat Grid控制台（具有管理员权限的用户帐户）

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。

背景信息

Cisco Threat Grid是一种高级且自动化的恶意软件分析和恶意软件威胁情报平台，可在不影响用户环境的情况下引爆可疑文件或网络目标。

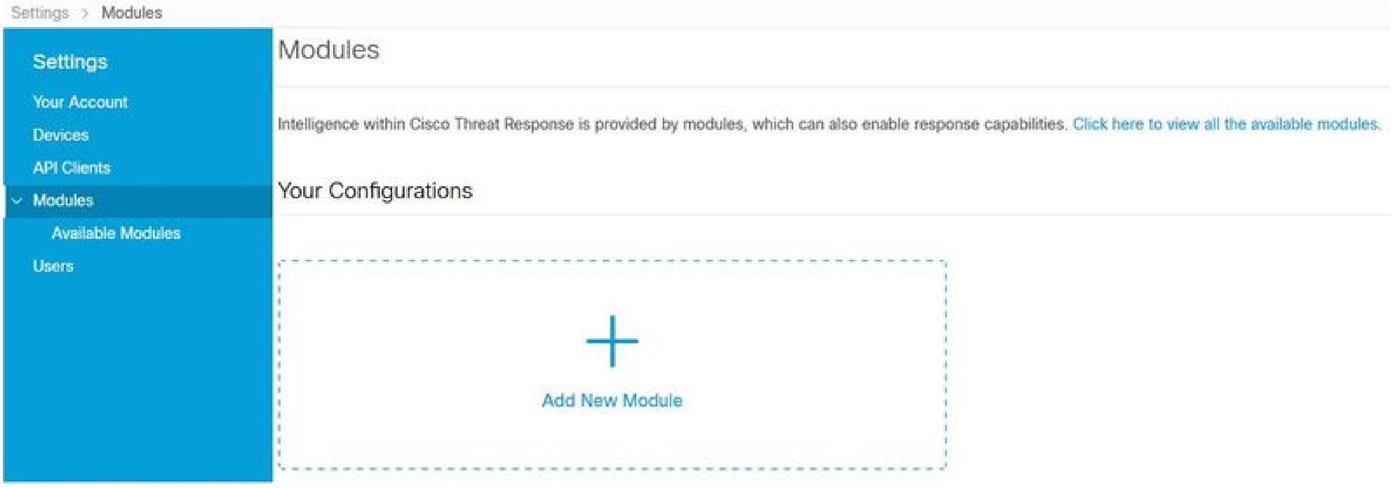
在与Cisco Threat Response的集成中，Threat Grid是一个参考模块，能够透视到Threat Grid门户，以收集有关Threat Grid知识库中文件哈希、IP、域和URL的其他情报。

配置

CTR控制台 — 配置Threat Grid模块

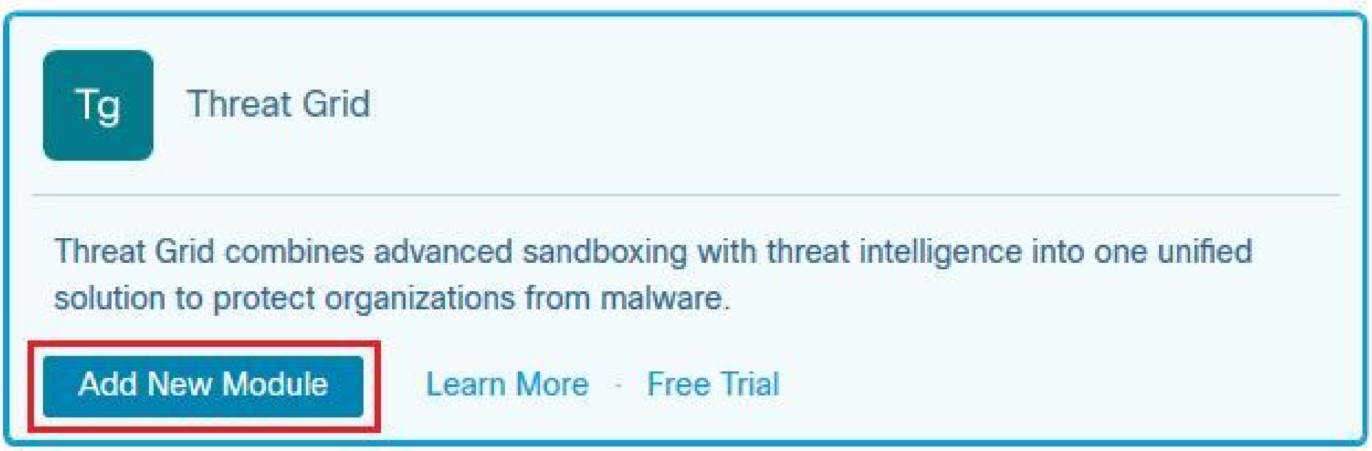
步骤1.使用管理员凭证登录到Cisco Threat Response。

步骤2.导航至Modules选项卡，选择**Modules > Add New Module**，如图所示。



Intelligence within Cisco Threat Response is provided by modules, which can also enable response capabilities. Click here to view all the available modules.

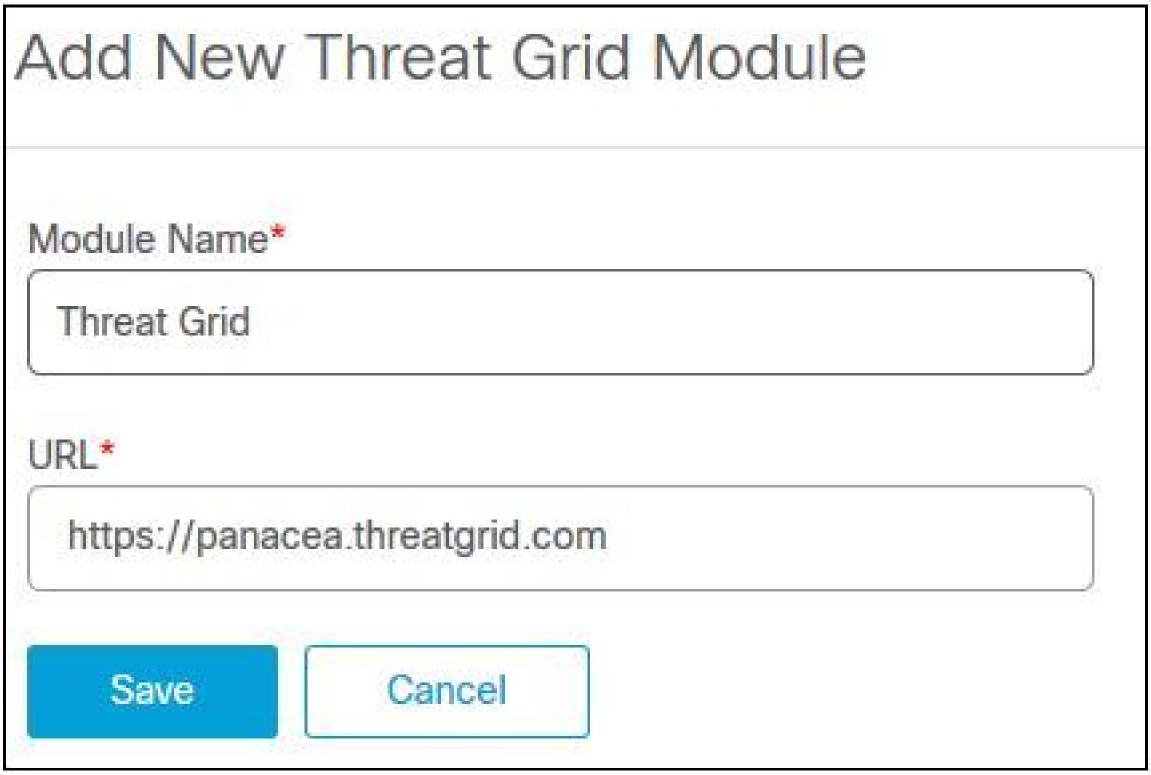
步骤3.在 Available Modules页面上，选择**Threat Grid模**块窗格中的Add New Module，如图所示。



Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware.

步骤4.“添**加新模块**”窗体。填写如图所示的表单。

- **模块名**称 — 保留默认名称或输入对您有意义的名称。
- **URL** — 从下拉列表中，为您的Threat Grid帐户所在位置（北美或欧洲）选择适当的URL。 暂时忽**略其**他选项。


Add New Threat Grid Module

Module Name*

Threat Grid

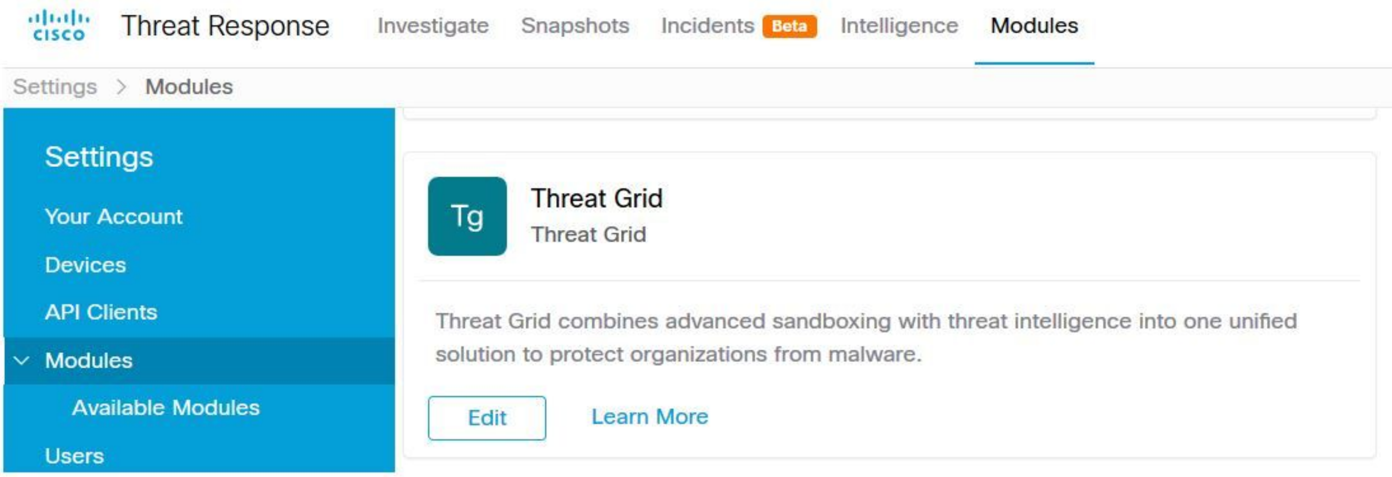
URL*

https://panacea.threatgrid.com

步骤5.选择“**保**存”以完成Threat Grid模块配置。

步骤6. Threat Grid现在显示在Modules页**面**的配置下，如图所示。

（TG可从透视菜单和案例簿中获得，以改进威胁调查）。

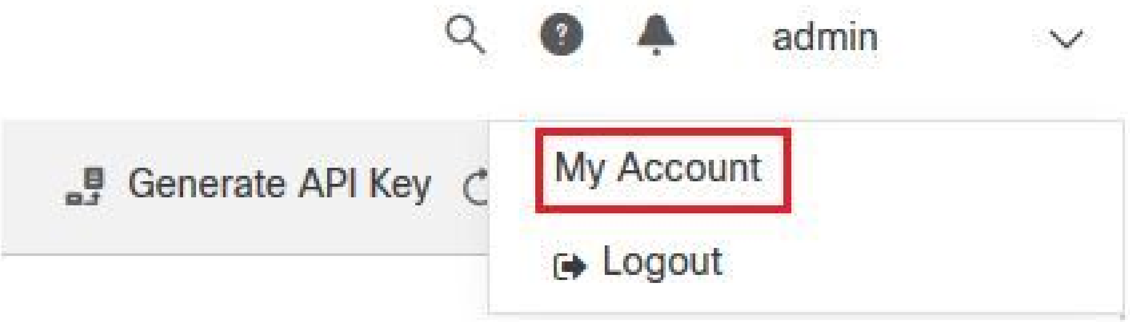


Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware.

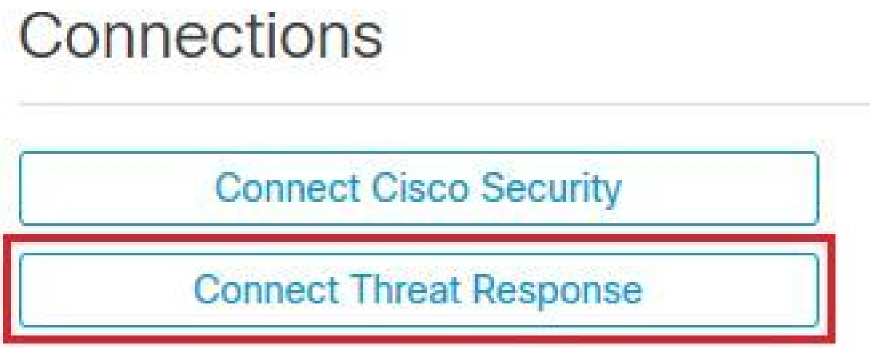
Threat Grid控制台 — 授权Threat Grid访问威胁响应

步骤1.使用管理员[凭据]登录Threat Grid。

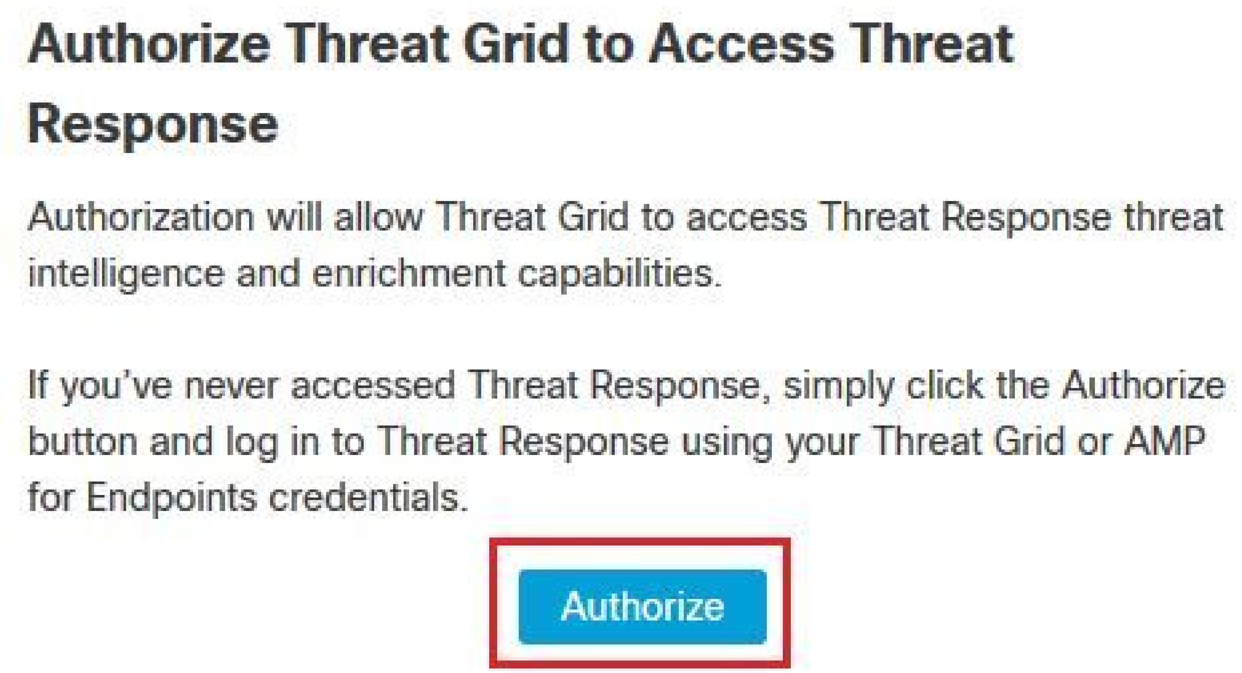
步骤2.导航至“**我的**帐户”部分，如图所示。



步骤3.导航至“连接”部分，然后选择连接威胁响应选项，如图所示。



第4步。选择Authorize选项以允许Threat Grid访问思科威胁响应，如图所示。

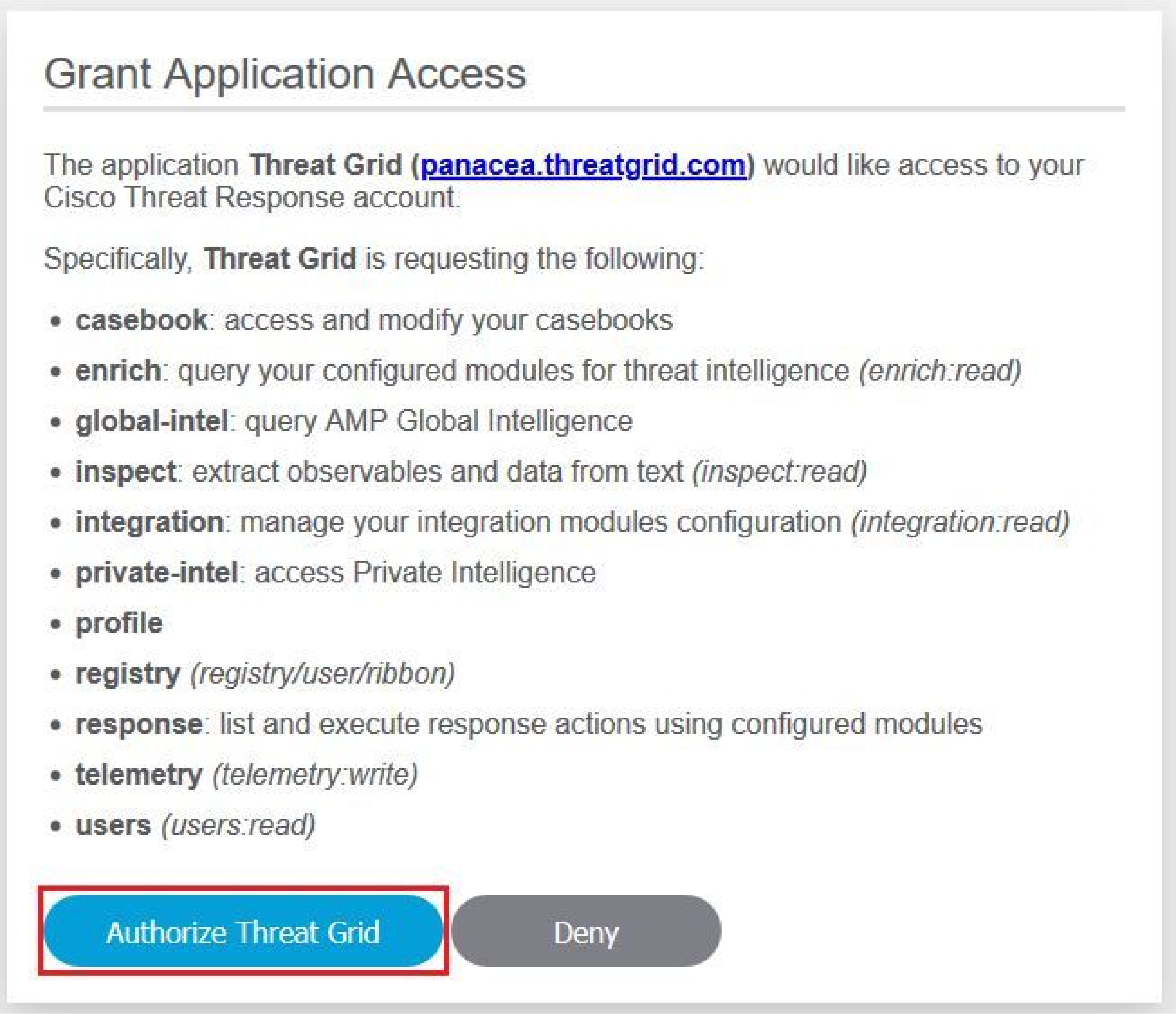


Authorize Threat Grid to Access Threat Response

Authorization will allow Threat Grid to access Threat Response threat intelligence and enrichment capabilities.

If you’ve never accessed Threat Response, simply click the Authorize button and log in to Threat Response using your Threat Grid or AMP for Endpoints credentials.

步骤5.选择Authorize Threat Grid选项以授予应用程序访问权限，如图所示。



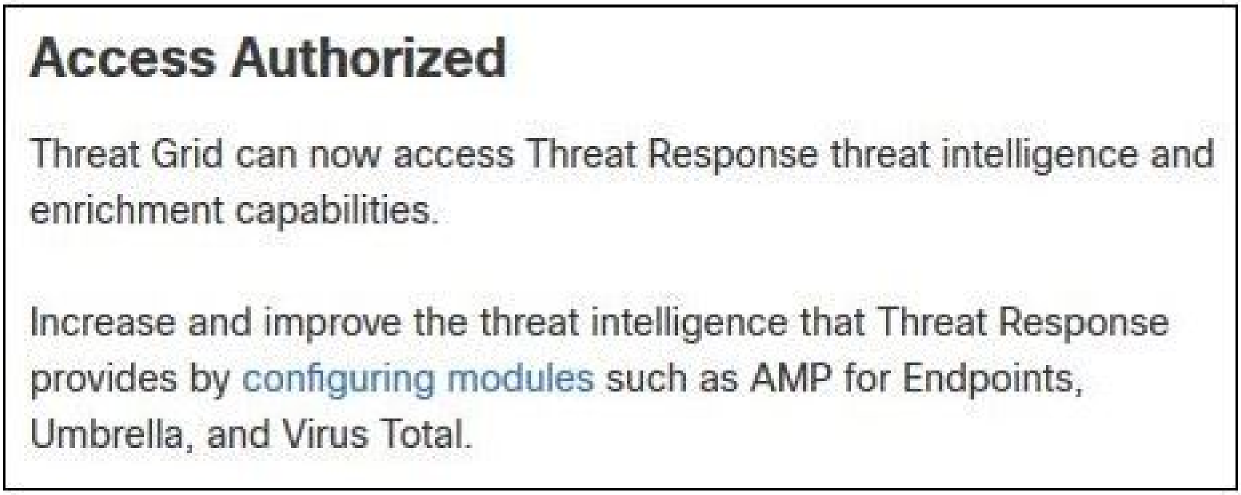
Grant Application Access

The application **Threat Grid** (panacea.threatgrid.com) would like access to your Cisco Threat Response account.

Specifically, **Threat Grid** is requesting the following:

- **casebook**: access and modify your casebooks
- **enrich**: query your configured modules for threat intelligence *(enrich:read)*
- **global-intel**: query AMP Global Intelligence
- **inspect**: extract observables and data from text *(inspect:read)*
- **integration**: manage your integration modules configuration *(integration:read)*
- **private-intel**: access Private Intelligence
- **profile**
- **registry** *(registry/user/ribbon)*
- **response**: list and execute response actions using configured modules
- **telemetry** *(telemetry:write)*
- **users** *(users:read)*

步骤6. Access Authorized（访问授权）消息显示为验证Threat Grid是否有权访问Threat Response威胁情报和浓缩功能，如图所示。



Access Authorized

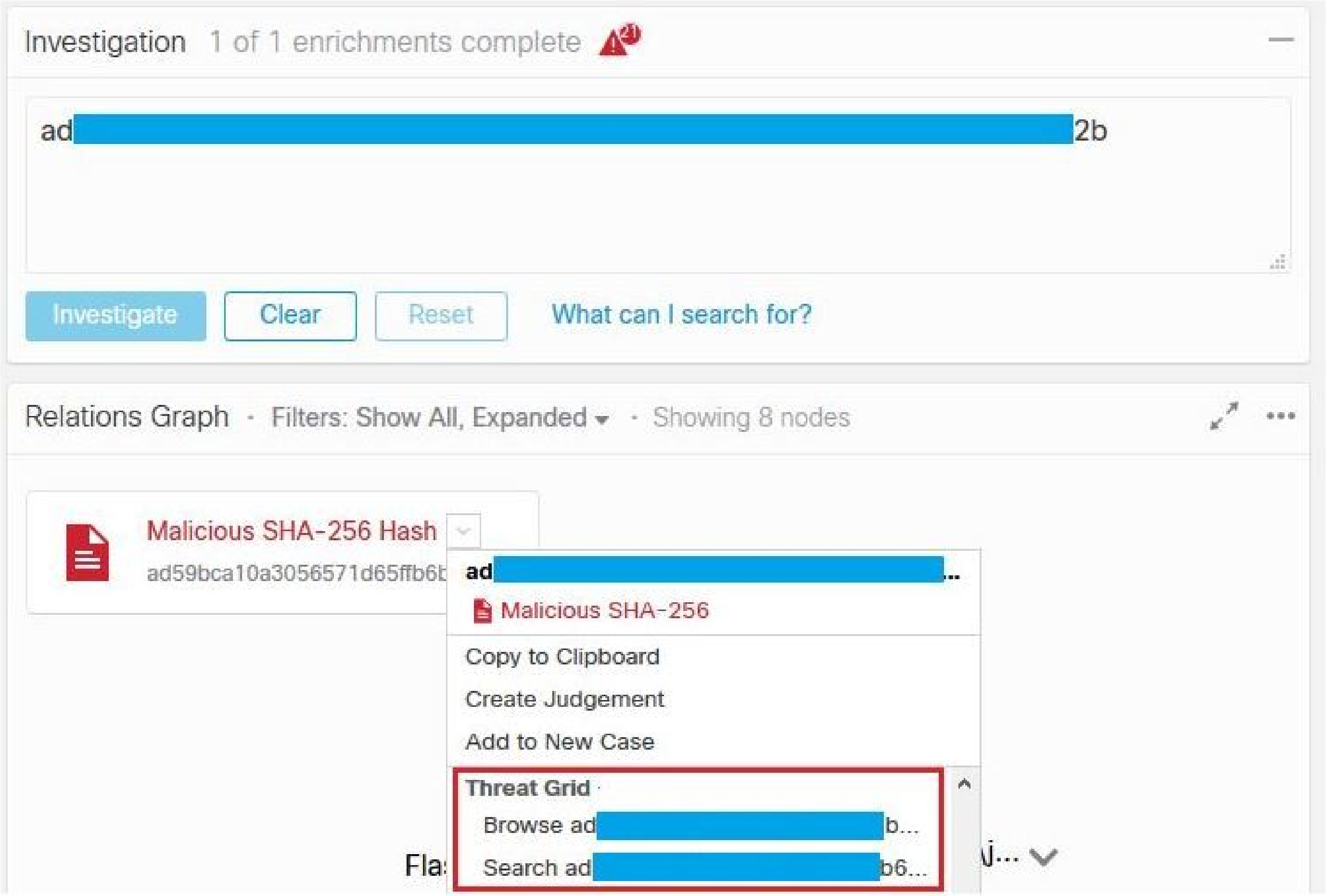
Threat Grid can now access Threat Response threat intelligence and enrichment capabilities.

Increase and improve the threat intelligence that Threat Response provides by configuring modules such as AMP for Endpoints, Umbrella, and Virus Total.

验证

使用本部分可确认配置能否正常运行。

为了验证CTR和TG集成，可以在CTR控制台上执行**调查**，当显示所有**调查**详细信息时，您可以看到Threat Grid选项，如图所示。



ad[redacted]2b

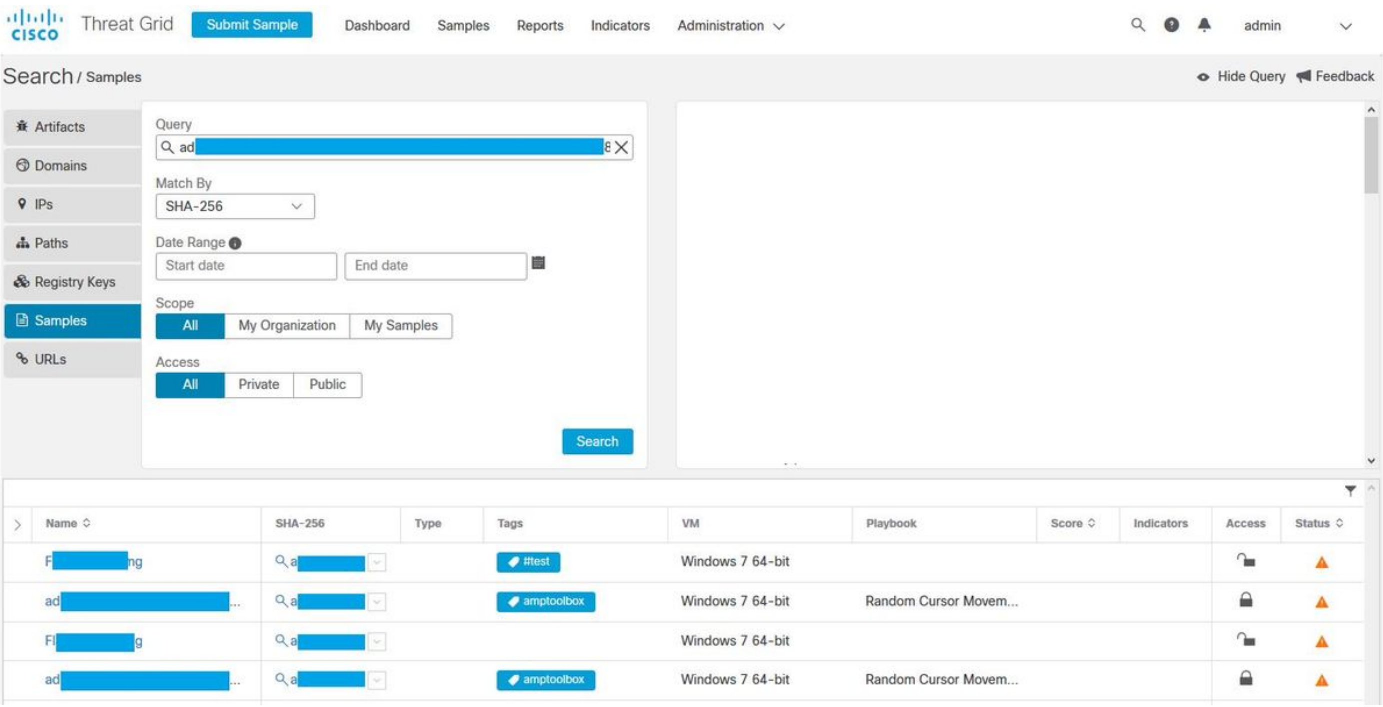
ad59bca10a3056571d65ffb6b

ad[redacted]...

Browse ad[redacted]b...

Search ad[redacted]b6...

您可以选择浏览或搜索Threat Grid选项，并重定向到Threat Grid门户以收集有关Threat Grid知识库中的文件/散列/IP/域/URL的其他情报，如图所示。



Query: ad[redacted]8

Match By: SHA-256

Date Range: Start date End date

Scope: All | My Organization | My Samples

Access: All | Private | Public

Name	SHA-256	Type	Tags	VM	Playbook	Score	Indicators	Access	Status
F[redacted]ng	a[redacted]		#test	Windows 7 64-bit				🔓	▲
ad[redacted]...	a[redacted]		amptoolbox	Windows 7 64-bit	Random Cursor Movem...			🔒	▲
Fl[redacted]g	a[redacted]			Windows 7 64-bit				🔓	▲
ad[redacted]...	a[redacted]		amptoolbox	Windows 7 64-bit	Random Cursor Movem...			🔒	▲