

Integre CTR y Threat Grid Cloud

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Consola CTR - Módulo Configurar Threat Grid](#)

[Consola de Threat Grid: autorice Threat Grid para acceder a Threat Response](#)

[Verificación](#)

Introducción

Este documento describe los pasos para integrar Cisco Threat Response (CTR) con Threat Grid (TG) Cloud para realizar investigaciones de CTR.

Colaborado por Jesús Javier Martínez, y editado por Yeraldin Sanchez, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Threat Response
- Threat Grid

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Consola CTR (cuenta de usuario con derechos de administrador)
- Consola Threat Grid (cuenta de usuario con derechos de administrador)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco Threat Grid es una plataforma avanzada y automatizada de análisis de malware e inteligencia de amenazas de malware en la que se pueden detonar archivos sospechosos o

destinos web sin que ello afecte al entorno del usuario.

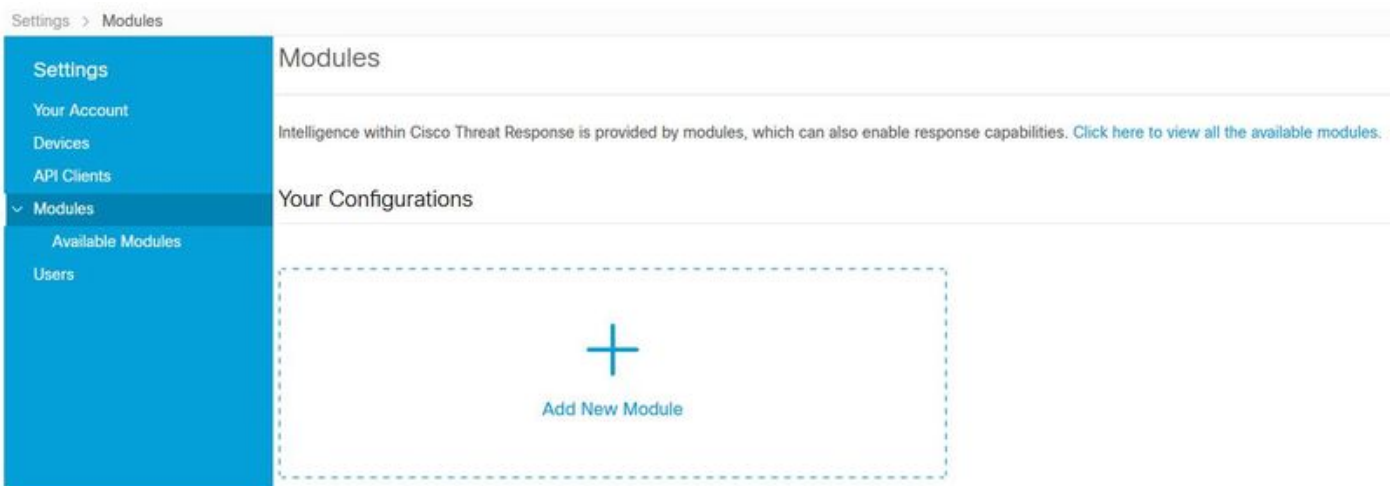
En la integración con Cisco Threat Response, Threat Grid es un módulo de referencia y proporciona la capacidad de adentrarse en el portal Threat Grid para recopilar información adicional sobre hash de archivos, IP, dominios y URL en el almacén de conocimientos de Threat Grid.

Configurar

Consola CTR - Módulo Configurar Threat Grid

Paso 1. Inicie sesión en [Cisco Threat Response](#) con las credenciales del administrador.

Paso 2. Vaya a la pestaña Módulos, seleccione **Módulos > Agregar nuevo módulo**, como se muestra en la imagen.



Paso 3. En la página Módulos disponibles, seleccione **Agregar nuevo módulo** en el panel del módulo Cuadrícula de amenazas, como se muestra en la imagen.



Paso 4. Se abre el formulario **Agregar nuevo módulo**. Complete el formulario como se muestra en la imagen.

- **Nombre de módulo:** deje el nombre predeterminado o introduzca un nombre que tenga sentido para usted.
- **URL:** en la lista desplegable, elija la dirección URL adecuada para la ubicación en la que se

encuentra su cuenta de Threat Grid (Norteamérica o Europa). Ignore la opción **Otro** por ahora.



Add New Threat Grid Module

Module Name*
Threat Grid

URL*
https://panacea.threatgrid.com

Save Cancel

Paso 5. Seleccione **Guardar** para completar la configuración del módulo Threat Grid.

Paso 6. Threat Grid ahora se muestra bajo sus configuraciones en la página **Modules** como se muestra en la imagen.

(TG está disponible en los menús principales y en los casos prácticos para mejorar la investigación de amenazas).



Consola de Threat Grid: autorice Threat Grid para acceder a Threat Response

Paso 1. Inicie sesión en [Threat Grid](#) con las credenciales del administrador.

Paso 2. Vaya a la sección **Mi cuenta**, como se muestra en la imagen.



Paso 3. Navegue hasta la sección **Conexiones** y seleccione la opción **Connect Threat Response** como se muestra en la imagen.

Connections

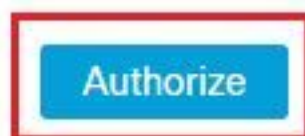


4 sep. Seleccione la opción **Authorize** para permitir que Threat Grid acceda a Cisco Threat Response, como se muestra en la imagen.

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.



Paso 5. Seleccione la opción **Authorize Threat Grid** para conceder acceso a la aplicación, como se muestra en la imagen.

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*)

Authorize Threat Grid

Deny

Paso 6. El mensaje Access Authorized (Acceso autorizado) parece comprobar que Threat Grid tiene acceso a la inteligencia de amenazas de Threat Response y a las capacidades de enriquecimiento, como se muestra en la imagen.

Access Authorized

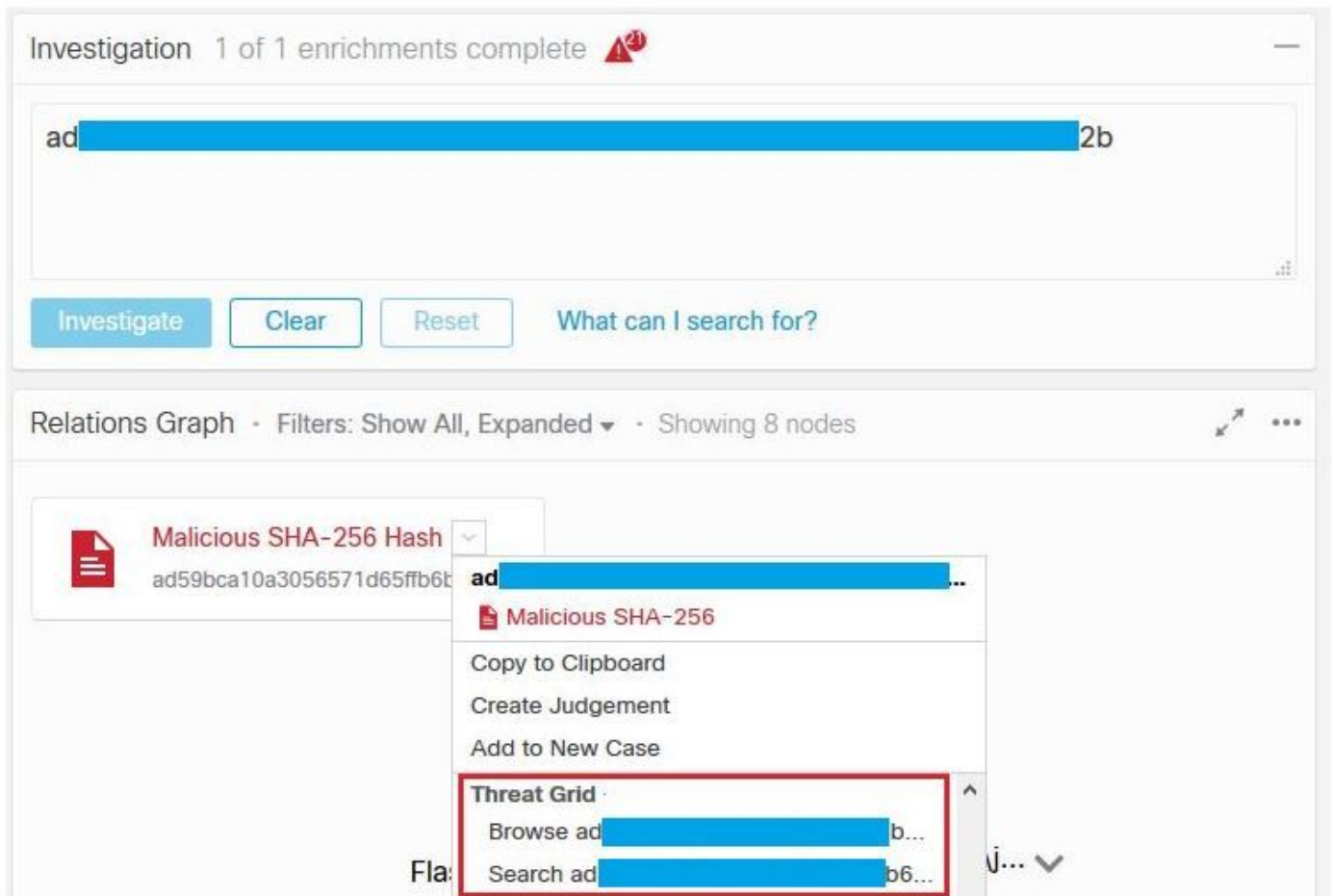
Threat Grid can now access Threat Response threat intelligence and enrichment capabilities.

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

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Para verificar la integración de CTR y TG, puede realizar una **investigación** en la consola de CTR, cuando aparezcan todos los detalles de **investigación**, podrá ver la opción Threat Grid, como se muestra en la imagen.



Puede seleccionar la opción Examinar o Buscar en Threat Grid y se redirige al portal Threat Grid para recopilar información adicional sobre archivos, hashes, IP, dominios y URL en el almacén de conocimientos de Threat Grid, como se muestra en la imagen.



Search / Samples

Hide Query Feedback

Artifacts

Domains

IPs

Paths

Registry Keys

Samples

URLs

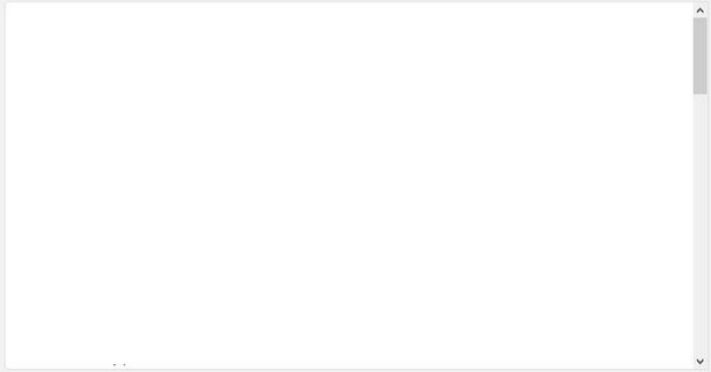
Query
 X

Match By
 SHA-256

Date Range
 Start date End date

Scope

Access



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