

Geïntegreerde CTR- en Threat Grid-cloud

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[CTR-console - Threat Grid-module configureren](#)

[Threat Grid-console - Threat Grid-toegangsrechten voor Threat Grid-respons](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft de stappen om Cisco Threat Response (CTR) te integreren met Threat Grid (TG) Cloud om CTR-onderzoeken uit te voeren.

Bijgedragen door Jezus Javier Martinez en bewerkt door Yeraldin Sanchez, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Threat-respons
- Threat Grid

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- CTR-console (gebruikersaccount met Administrator-rechten)
- Threat Grid-console (gebruikersaccount met Administrator-rechten)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Cisco Threat Grid is een geavanceerde en geautomatiseerde malware-analyse en een platform voor alarmbedreigingen waarin verdachte bestanden of webbestemmingen kunnen worden

opgelost zonder dat dit de gebruikersomgeving beïnvloedt.

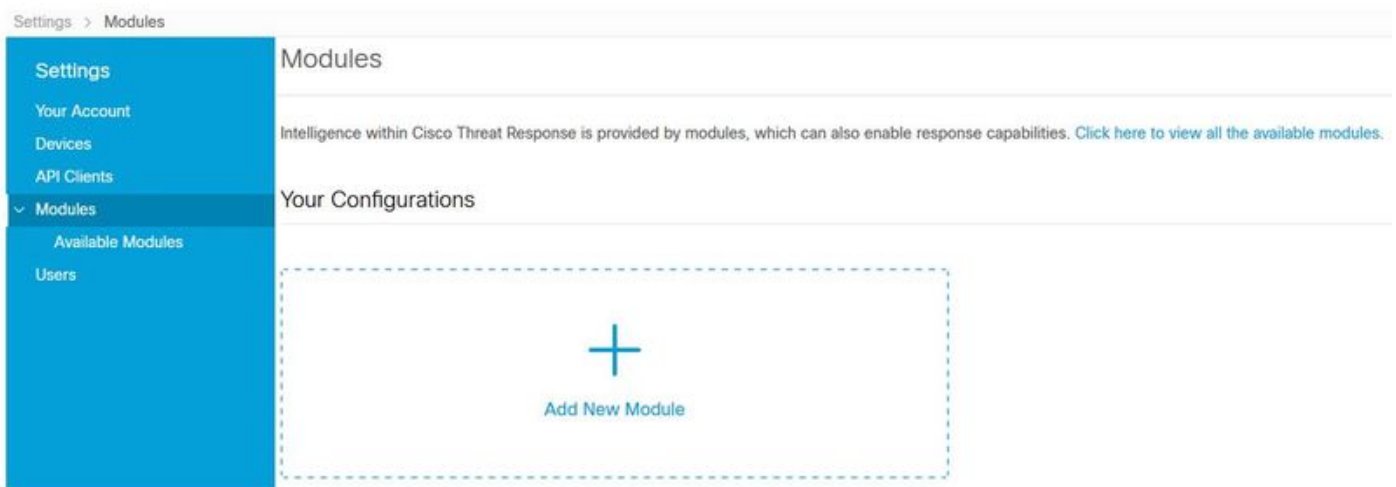
In de integratie met Cisco Threat Response is Threat Grid een referentiemodule en biedt Threat Grid de mogelijkheid om in Threat Grid Portal te draaien om extra informatie te verzamelen over bestandsshashes, IPs, domeinen en URLs in de Threat Grid-kenniswinkel.

Configureren

CTR-console - Threat Grid-module configureren

Stap 1. Meld u aan bij [Cisco Threat Response](#) met behulp van beheerdersreferenties.

Stap 2. Navigeer naar het tabblad Modules, selecteer **Modules > Nieuwe module toevoegen** zoals in de afbeelding.



Stap 3. Selecteer in de pagina Beschikbare modules de optie **Nieuwe module toevoegen** in het deelvenster met Threat Grid-modules, zoals in de afbeelding.



Stap 4. Het formulier **Nieuwe module toevoegen** wordt geopend. Vul het formulier in zoals in de afbeelding.

- **Module naam** - Laat de standaardnaam achter of voer een naam in die voor u betekenisvol is.
- **URL** - Kies in de vervolgkeuzelijst de juiste URL voor de locatie waar uw Threat Grid-account is gebaseerd (Noord-Amerika of Europa). Negeer voorlopig de **andere** optie.

Add New Threat Grid Module

Module Name*

URL*

[Save](#) [Cancel](#)

Stap 5. Selecteer **Save** om de configuratie van de Threat Grid-module te voltooien.

Stap 6. Threat Grid wordt nu onder uw configuraties weergegeven op de pagina **Modules** zoals in de afbeelding.

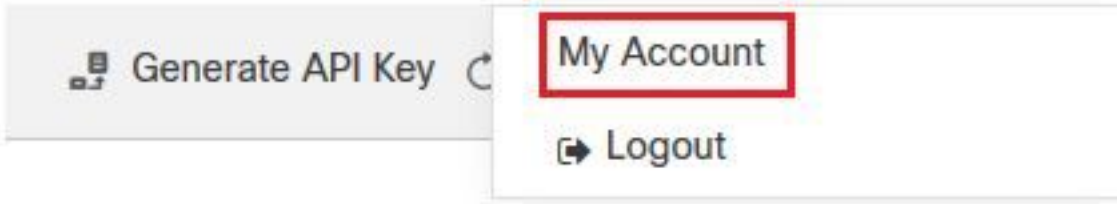
(TG is beschikbaar via pivotmenu's en in casebooks voor beter dreigingsonderzoek).

The screenshot shows the Cisco Threat Response interface. At the top, there is a navigation bar with the following items: Threat Response, Investigate, Snapshots, Incidents (marked as Beta), Intelligence, and Modules. Below the navigation bar, the breadcrumb path is 'Settings > Modules'. On the left side, there is a blue sidebar menu with the following items: Settings, Your Account, Devices, API Clients, Modules (expanded), Available Modules, and Users. The main content area displays the Threat Grid module configuration. It features a 'Tg' icon, the text 'Threat Grid' and 'Threat Grid', and a description: 'Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware.' Below the description, there are two buttons: 'Edit' and 'Learn More'.

Threat Grid-console - Threat Grid-toegangsrechten voor Threat Grid-respons

Stap 1. Meld u aan bij [Threat Grid](#) met behulp van Administrator-referenties.

Stap 2. Navigeer naar het gedeelte **Mijn account**, zoals in de afbeelding.



Stap 3. Navigeer naar het **gedeelte Connections** en selecteer **Connect Threat Response** optie zoals in de afbeelding getoond.

Connections

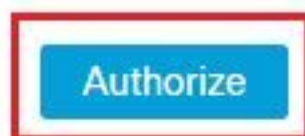


Stap 4. Selecteer de optie **autoriseren** om Threat Grid-toegang tot de Cisco Threat Response toe te staan, zoals in de afbeelding.

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.



Stap 5. Selecteer de optie **Threat Grid autoriseren** om toepassingstoegang te verlenen, zoals in de afbeelding.

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

Stap 6. Het bericht met toegangsvergunning lijkt te bevestigen dat Threat Grid toegang heeft tot de bedreigingsinformatie- en verrijkingmogelijkheden van Threat Response, zoals in de afbeelding wordt getoond.

Access Authorized

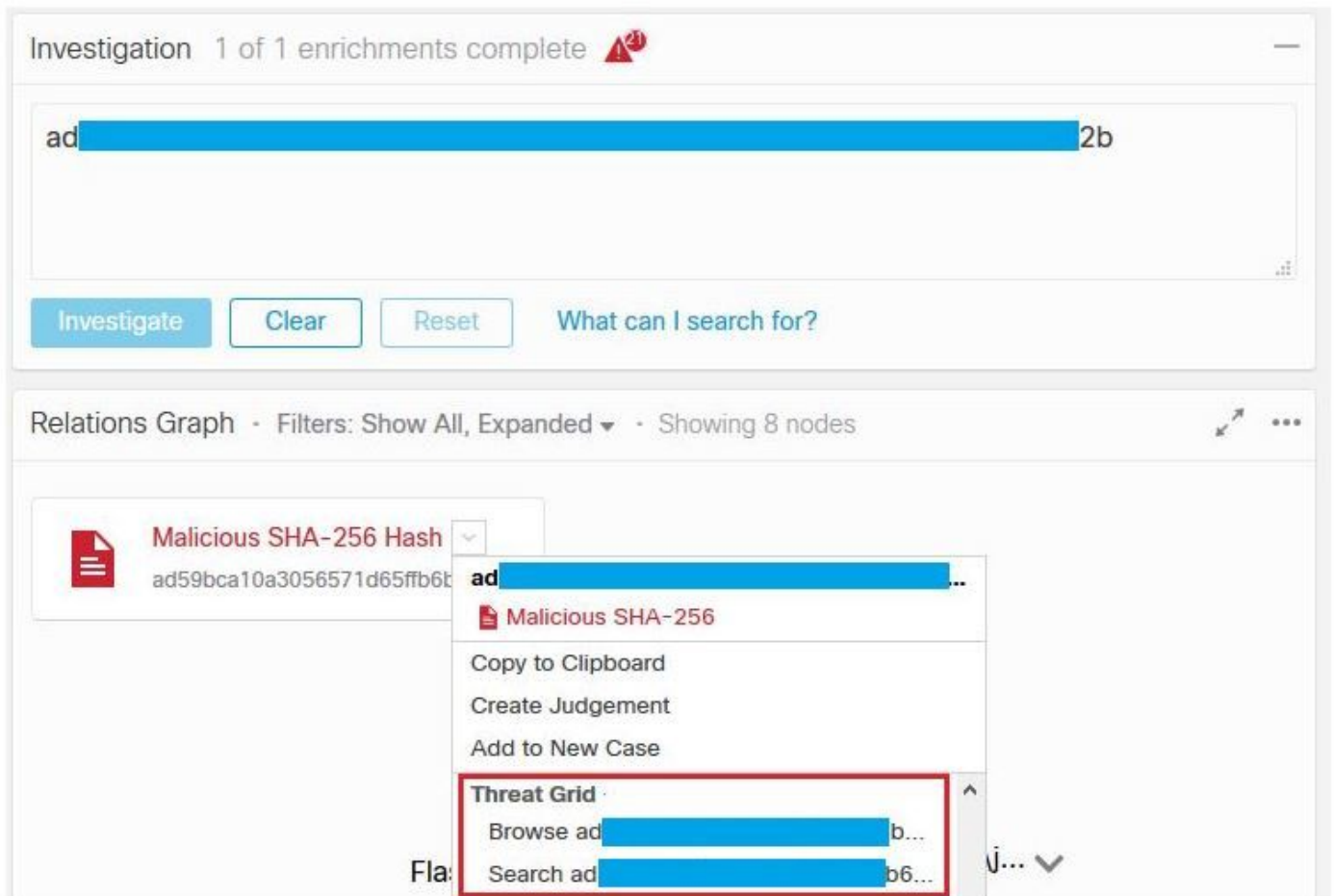
Threat Grid can now access Threat Response threat intelligence and enrichment capabilities.

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

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Om de integratie van CTR en TG te verifiëren kunt u een **Onderzoek** doen op de console van CTR, wanneer alle **van het Onderzoek** details verschijnen, kunt u de optie Threat Grid zien, zoals in de afbeelding wordt getoond.



U kunt de optie Bladeren of Zoeken op Threat Grid selecteren en deze wordt omgeleid naar het Threat Grid-portaal om extra informatie te verzamelen over bestanden / hashes / IPs / domeinen / URLs in de Threat Grid-kenniswinkel, zoals in de afbeelding wordt getoond.



Search / Samples

Hide Query Feedback

Artifacts

Domains

IPs

Paths

Registry Keys

Samples

URLs

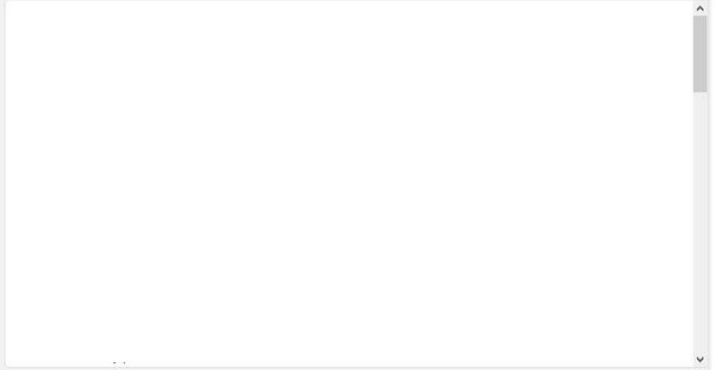
Query
 X

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...			🔒	⚠️