

Integration von CTR- und Threat Grid-Cloud

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[CTR-Konsole - Konfigurieren des Threat Grid-Moduls](#)

[Threat Grid-Konsole - Autorisieren von Threat Grid für den Zugriff auf Bedrohungsreaktion](#)

[Überprüfen](#)

Einführung

Dieses Dokument beschreibt die Schritte zur Integration von Cisco Threat Response (CTR) in die Threat Grid (TG) Cloud, um CTR-Untersuchungen durchzuführen.

Verfasst von Jesus Javier Martinez und herausgegeben von Yeraldin Sanchez, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Reaktion auf Bedrohungen von Cisco
- Threat Grid

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- CTR-Konsole (Benutzerkonto mit Administratorrechten)
- Threat Grid-Konsole (Benutzerkonto mit Administratorrechten)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Cisco Threat Grid ist eine erweiterte und automatisierte Plattform zur Malware-Analyse und zum

Aufspüren von Malware-Bedrohungen, mit der verdächtige Dateien oder Web-Ziele detoniert werden können, ohne die Benutzerumgebung zu beeinträchtigen.

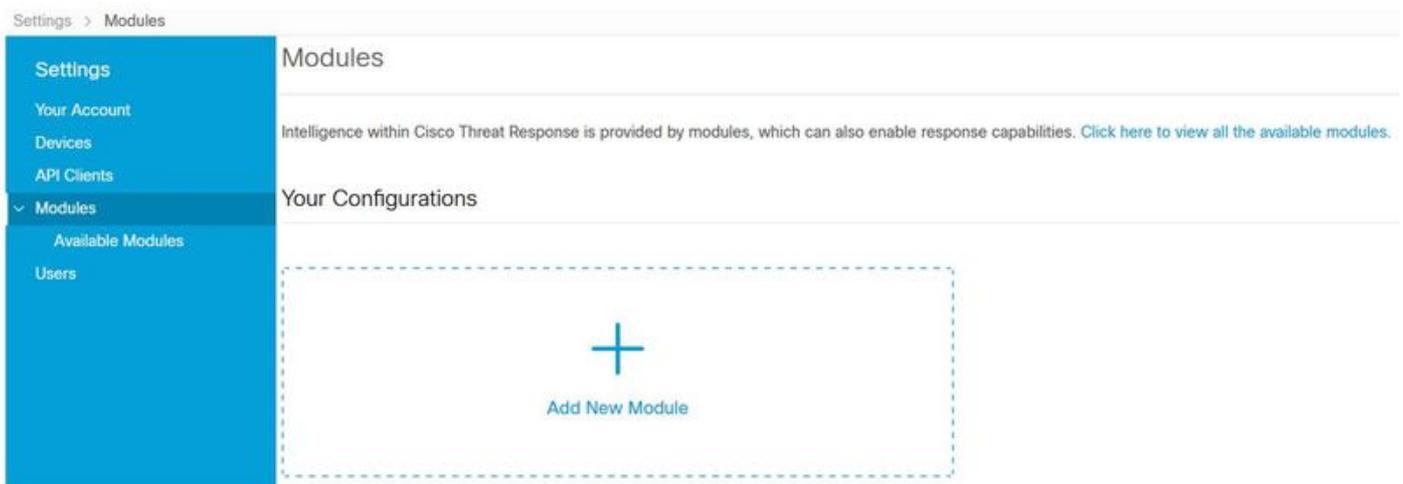
Threat Grid ist ein Referenzmodul in die Integration mit Cisco Threat Response und bietet die Möglichkeit, in das Threat Grid-Portal zu wechseln und im Threat Grid Knowledge Store zusätzliche Informationen zu Datei-Hashes, IPs, Domänen und URLs zu sammeln.

Konfigurieren

CTR-Konsole - Konfigurieren des Threat Grid-Moduls

Schritt 1: Melden Sie sich mit Administratoranmeldeinformationen bei [Cisco Threat Response an](#).

Schritt 2: Navigieren Sie zur Registerkarte Module, und wählen Sie **Module > Neues Modul hinzufügen aus**, wie im Bild gezeigt.



Schritt 3: Wählen Sie auf der Seite Available Modules (Verfügbare Module) **Add New Module (Neues Modul hinzufügen)** im Bereich Threat Grid aus, wie im Bild gezeigt.



Schritt 4: Das Formular **Neues Modul hinzufügen** wird geöffnet. Füllen Sie das Formular aus, wie im Bild gezeigt.

- **Modulname:** Behalten Sie den Standardnamen bei, oder geben Sie einen für Sie sinnvollen Namen ein.
- **URL:** Wählen Sie aus der Dropdown-Liste die entsprechende URL für den Standort aus, an

dem Ihr Threat Grid-Konto ansässig ist (Nordamerika oder Europa). Ignorieren Sie die Option **Andere**.



Add New Threat Grid Module

Module Name*
Threat Grid

URL*
https://panacea.threatgrid.com

Save Cancel

Schritt 5: Wählen Sie **Speichern**, um die Konfiguration des Threat Grid-Moduls abzuschließen.

Schritt 6: Threat Grid wird jetzt unter Ihren Konfigurationen auf der Seite **Module** angezeigt, wie im Bild gezeigt.

(TG ist in Pivot-Menüs und in Casebooks verfügbar, um Bedrohungsanalysen zu verbessern).



Settings > Modules

Settings
Your Account
Devices
API Clients
Modules
Available Modules
Users

Threat Grid
Threat Grid

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

Edit Learn More

Threat Grid-Konsole - Autorisieren von Threat Grid für den Zugriff auf Bedrohungsreaktion

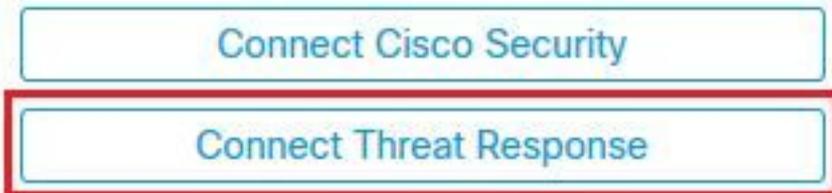
Schritt 1: Melden Sie sich mit Administratoranmeldeinformationen bei [Threat Grid](#) an.

Schritt 2: Navigieren Sie zum Abschnitt **Mein Konto**, wie im Bild gezeigt.



Schritt 3: Navigieren Sie zum Abschnitt **Verbindungen**, und wählen Sie die Option **Bedrohungsantwort verbinden** aus, wie im Bild gezeigt.

Connections

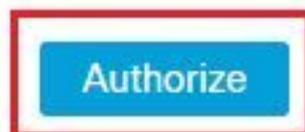


4. September Wählen Sie die Option **Authorize (Autorisieren)** aus, um Threat Grid den Zugriff auf Cisco Threat Response zu ermöglichen, wie im Bild gezeigt.

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.



Schritt 5: Wählen Sie die Option **Threat Grid autorisieren**, um wie im Bild gezeigt Anwendungszugriff zu gewähren.

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

Schritt 6: Die Meldung "Access Authorized" (Zugriff auf autorisierte Zugriffe) wird angezeigt, um zu überprüfen, ob Threat Grid Zugriff auf Bedrohungsinformationen und Anreicherungsfunktionen hat, wie im Bild gezeigt.

Access Authorized

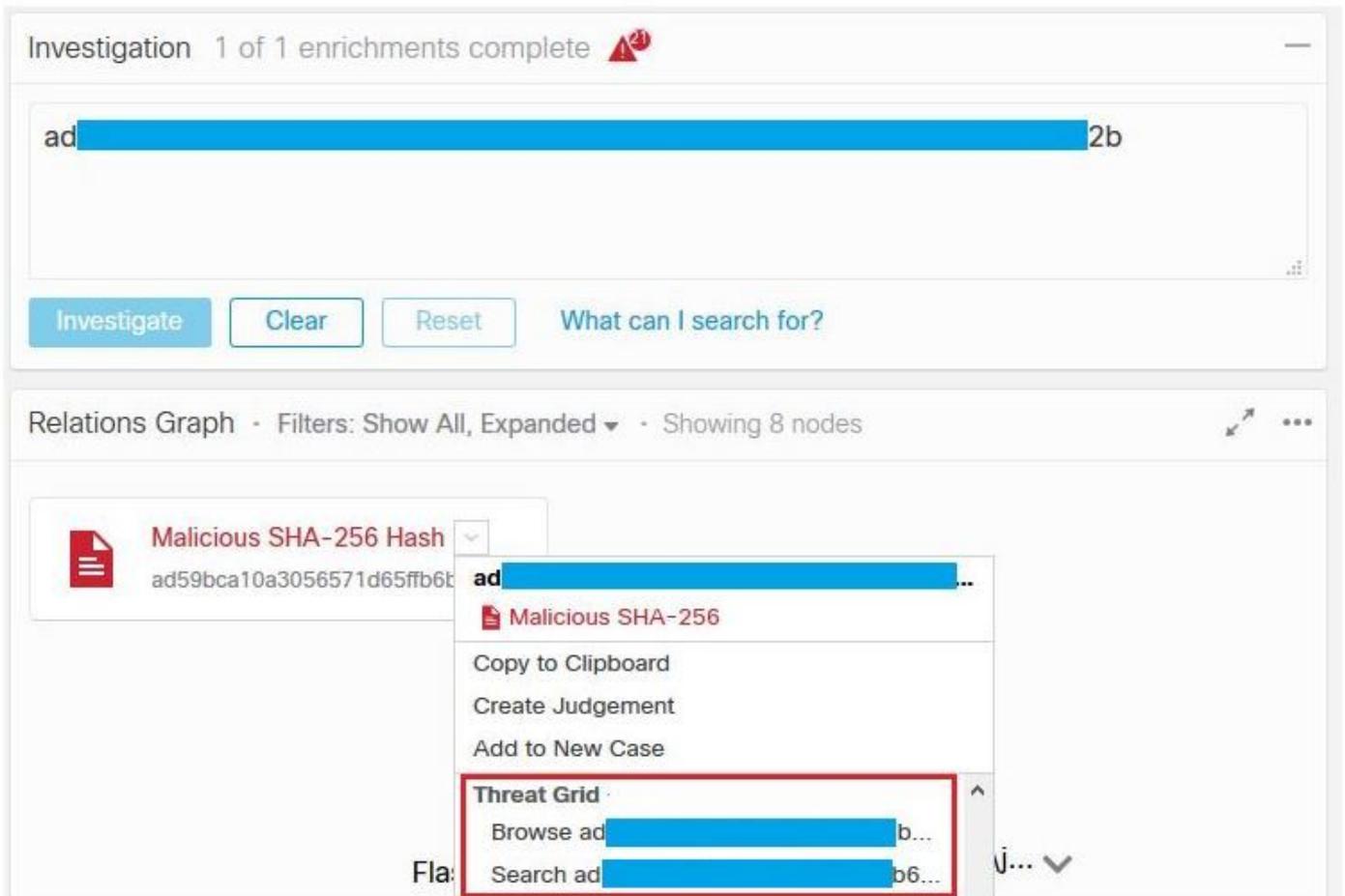
Threat Grid can now access Threat Response threat intelligence and enrichment capabilities.

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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Um die CTR- und TG-Integration zu überprüfen, können Sie eine **Investigation** auf der CTR-Konsole durchführen. Wenn alle **Investigation** Details angezeigt werden, können Sie die Threat Grid-Option sehen, wie im Bild gezeigt.



Sie können die Option "Durchsuchen" oder "Threat Grid durchsuchen" auswählen und sie wird in das Threat Grid-Portal umgeleitet, um zusätzliche Informationen zu Dateien/Hashes/IPs/Domänen/URLs im Threat Grid-Wissensspeicher zu sammeln, wie im Bild gezeigt.



Search / Samples

Hide Query Feedback

Artifacts

Domains

IPs

Paths

Registry Keys

Samples

URLs

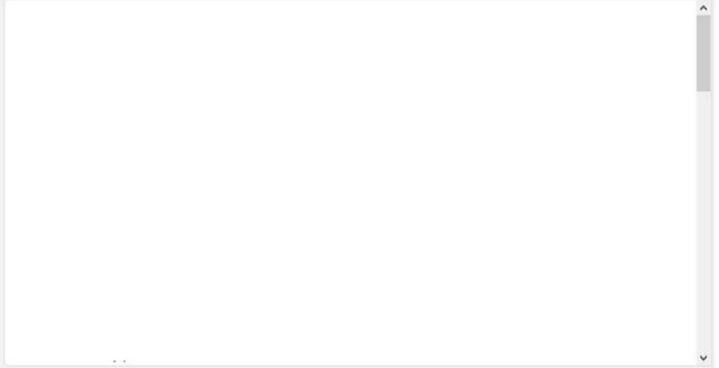
Query
 X

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...			🔒	⚠️