

Intégrez le CTR et le nuage de grille de menace

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Console CTR - Configurez le module de grille de menace](#)

[Console de grille de menace - Autorisez la grille de menace pour accéder à la réponse de menace](#)

[Vérifier](#)

Introduction

Ce document décrit les étapes pour intégrer les Solutions de sécurité pour neutraliser les menaces réseau Cisco (CTR) avec le nuage de la grille de menace (TG) afin d'exécuter des investigations CTR.

Contribué par Jésus Javier Martinez, et édité par Yeraldin Sanchez, ingénieurs TAC Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Solutions de sécurité pour neutraliser les menaces réseau Cisco
- [Grille contre les menaces \(Threat Grid\)](#)

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Console CTR (compte utilisateur avec des droits d'administrateur)
- Console de grille de menace (compte utilisateur avec des droits d'administrateur)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

[Informations générales](#)

La grille de menace de Cisco est une plate-forme avancée et automatisée de renseignement sur

analyse de malware et menace de malware en laquelle des fichiers ou les destinations méfiants de Web peuvent être détonés sans affecter l'environnement de l'utilisateur.

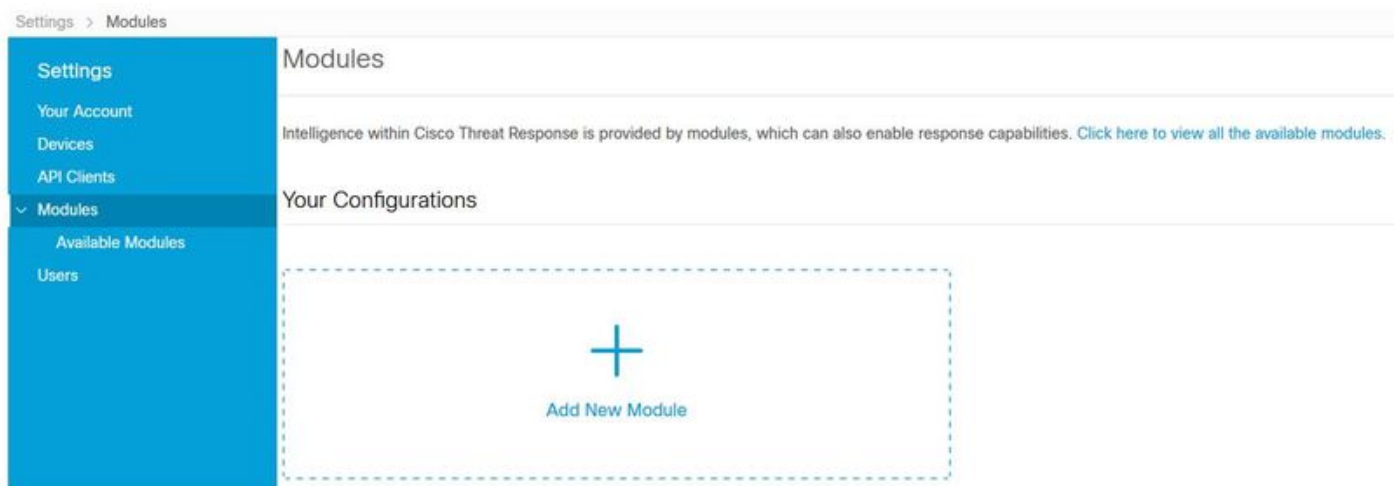
Dans l'intégration avec le Solutions de sécurité pour neutraliser les menaces réseau Cisco, la grille de menace est un module de référence et fournit la capacité de pivoter dans le portail de grille de menace pour recueillir l'intelligence supplémentaire au sujet du fichier hache, IPS, domaines, et URLs dans la mémoire de la connaissance de grille de menace.

Configurer

Console CTR - Configurez le module de grille de menace

Étape 1. Procédure de connexion au [Solutions de sécurité pour neutraliser les menaces réseau Cisco](#) utilisant des qualifications d'administrateur.

Étape 2. Naviguez vers l'onglet de modules, les **modules** choisis > **ajoutent le nouveau module**, suivant les indications de l'image.



Étape 3. Sur les modules disponibles pagez, choisi **ajoutent le nouveau module** dans le volet de module de grille de menace, suivant les indications de l'image.



Étape 4. La nouvelle forme de **module d'ajouter** s'ouvre. Remplissez le formulaire suivant les indications de l'image.

- **Nom du module** - Laissez le nom par défaut ou écrivez un nom qui est significatif à vous.

- **URL** - De la liste déroulante, choisissez l'URL approprié pour l'emplacement où votre compte de grille de menace est basé (l'Amérique du Nord ou l'Europe). Ignorez l'**autre** option pour l'instant.



Add New Threat Grid Module

Module Name*

Threat Grid

URL*

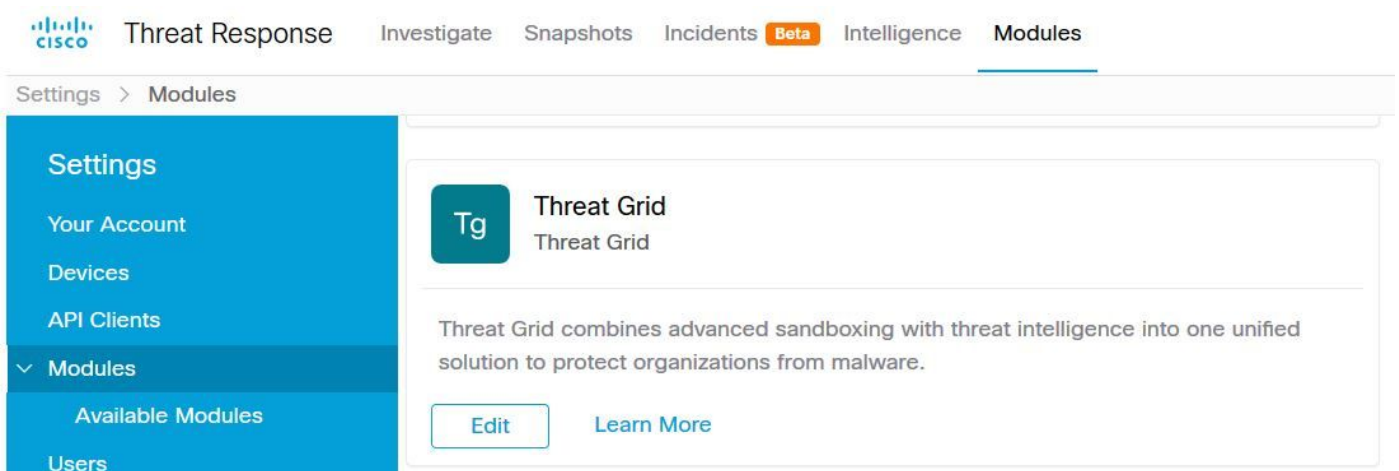
https://panacea.threatgrid.com

Save Cancel

Étape 5. Sélectionnez la **sauvegarde** pour se terminer la configuration de module de grille de menace.

Étape 6. La grille de menace est maintenant affichée sous vos configurations à la page de **modules** suivant les indications de l'image.

(le TG est disponible des menus de pivot et dans les casebooks pour l'enquête améliorée de menace).



Threat Response Investigate Snapshots Incidents **Beta** Intelligence **Modules**

Settings > Modules

Settings
Your Account
Devices
API Clients
Modules
Available Modules
Users

Tg Threat Grid
Threat Grid

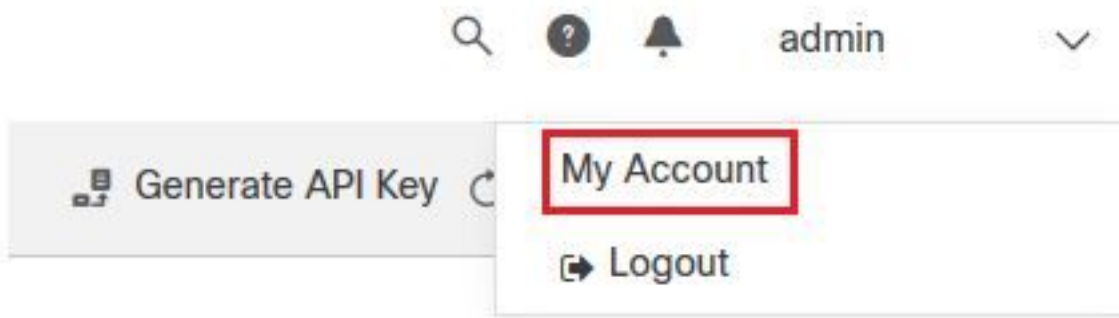
Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware.

Edit Learn More

Console de grille de menace - Autorisez la grille de menace pour accéder à la réponse de menace

Étape 1. Procédure de connexion à la [grille de menace](#) utilisant des qualifications d'administrateur.

Étape 2. Naviguez vers **ma** section de **compte**, suivant les indications de l'image.



Étape 3. Naviguez vers la section de **connexions** et choisi **connectez** l'option de **réponse de menace** suivant les indications de l'image.

Connections

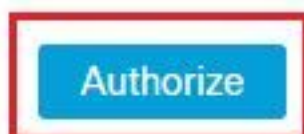


4 septembre. Choisi **autorisez** l'option afin de permettre à la grille de menace pour accéder à au Solutions de sécurité pour neutraliser les menaces réseau Cisco, suivant les indications de l'image.

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.



Étape 5. Choisi **autorisez** l'accès de demande de subvention d'option de **grille de menace**, suivant les indications de l'image.

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

Étape 6. Le message autorisé par Access semble vérifier la grille de menace a accès aux capacités de renseignement sur et d'enrichissement la menace de réponse de menace, suivant les indications de l'image.

Access Authorized

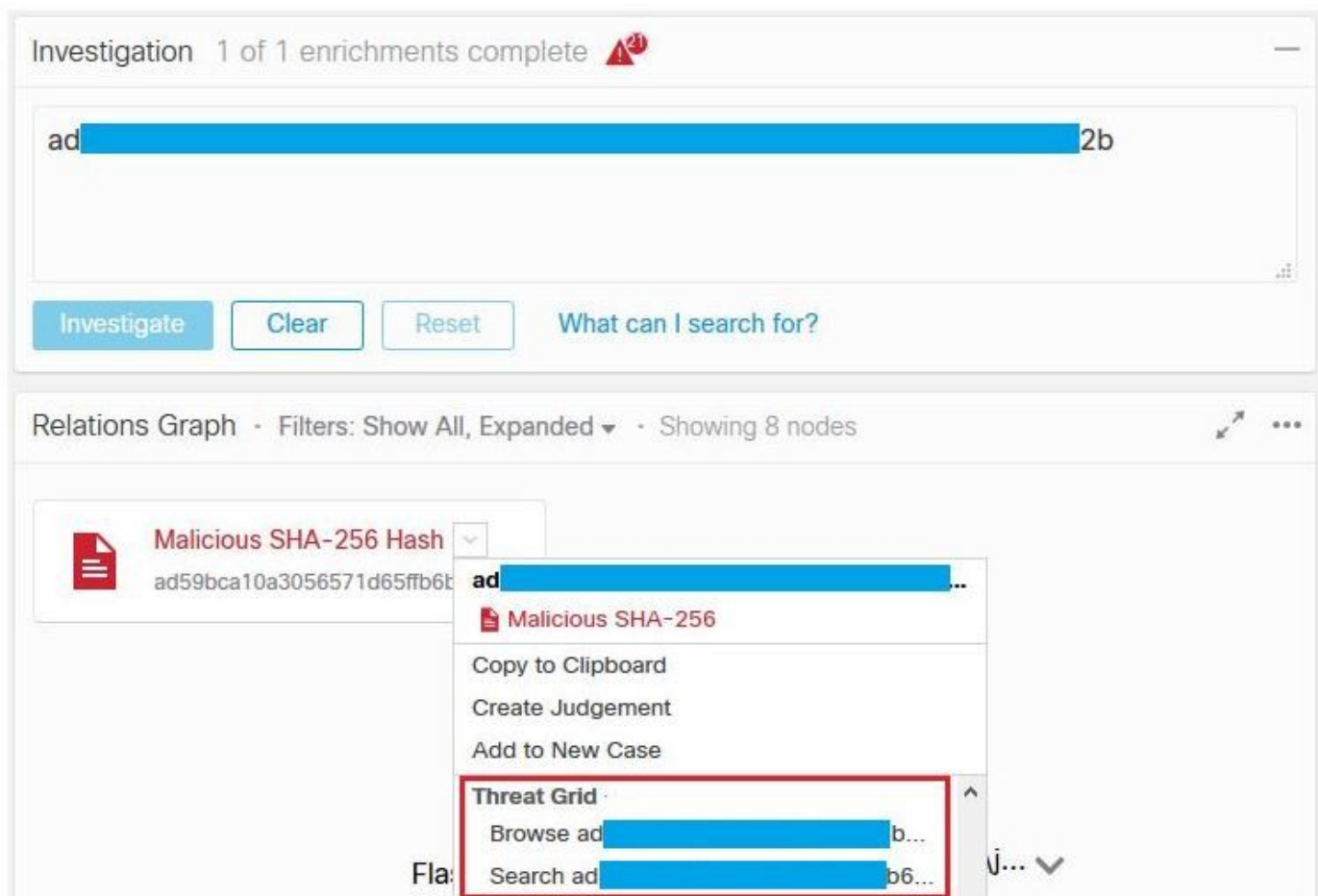
Threat Grid can now access Threat Response threat intelligence and enrichment capabilities.

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

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Afin de vérifier l'intégration CTR et TG, vous pouvez faire une **enquête** sur la console CTR, quand tous les détails d'**enquête** apparaissent, vous pouvez voir l'option de grille de menace, suivant les indications de l'image.



Vous pouvez sélectionner parcourir ou rechercher l'option de grille de menace et elle réoriente dans le portail de grille de menace pour recueillir l'intelligence supplémentaire au sujet des fichiers/hache/IPS/domaines/URLs dans la mémoire de la connaissance de grille de menace, suivant les indications de l'image.



Search / Samples

Hide Query Feedback

Artifacts

Domains

IPs

Paths

Registry Keys

Samples

URLs

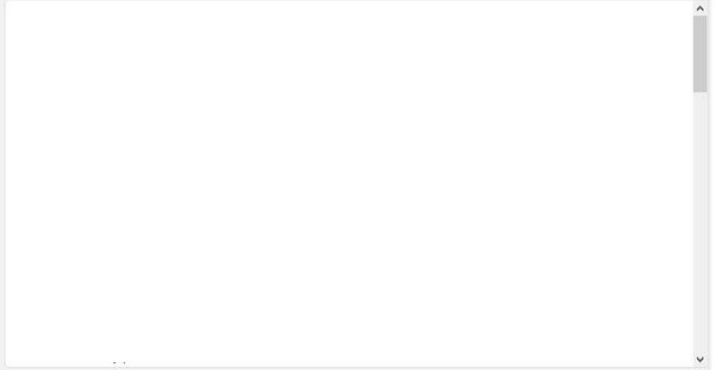
Query
 X

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...			🔒	⚠️