Intégrer le cloud CTR et Threat Grid

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Informations générales](#)
[Configuration](#)
[Console CTR - Configuration du module Threat Grid](#)
[Console Threat Grid - Autoriser Threat Grid à accéder à la réponse aux menaces](#)
[Vérification](#)

Introduction

Ce document décrit les étapes à suivre pour intégrer Cisco Threat Response (CTR) au cloud Threat Grid (TG) afin d'effectuer des enquêtes CTR.

Contribué par Jesus Javier Martinez, et édité par Yeraldin Sanchez, Ingénieurs du TAC de Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réponse Cisco aux menaces
- Grille contre les menaces (Threat Grid)

Components Used

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

- Console CTR (compte utilisateur avec droits d'administrateur)
- Console Threat Grid (compte utilisateur avec droits d'administrateur)

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Cisco Threat Grid est une plate-forme avancée et automatisée d'analyse des programmes malveillants et d'informations sur les menaces de programmes malveillants dans laquelle les fichiers suspects ou les destinations Web peuvent être déclenchés sans impact sur

l'environnement utilisateur.

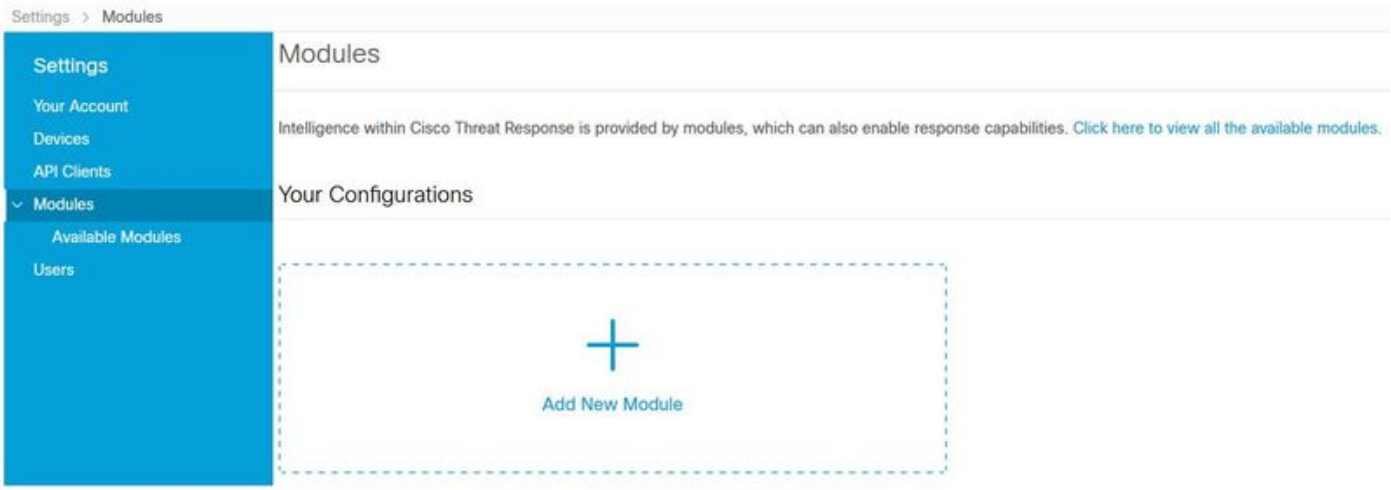
Dans le cadre de l'intégration avec Cisco Threat Response, Threat Grid est un module de référence qui permet de basculer vers le portail Threat Grid pour recueillir des informations supplémentaires sur les hachages de fichiers, les adresses IP, les domaines et les URL dans le magasin de connaissances Threat Grid.

Configuration

Console CTR - Configuration du module Threat Grid

Étape 1. Connectez-vous à Cisco Threat Response à l'aide des informations d'identification de l'administrateur.

Étape 2. Accédez à l'onglet Modules, sélectionnez **Modules > Ajouter un nouveau module**, comme illustré dans l'image.



Étape 3. Sur la page Modules disponibles, sélectionnez **Ajouter un nouveau module** dans le volet de module Threat Grid, comme illustré dans l'image.

Étape 4. Le formulaire **Ajouter un nouveau module** s'ouvre. Remplissez le formulaire comme indiqué dans l'image.

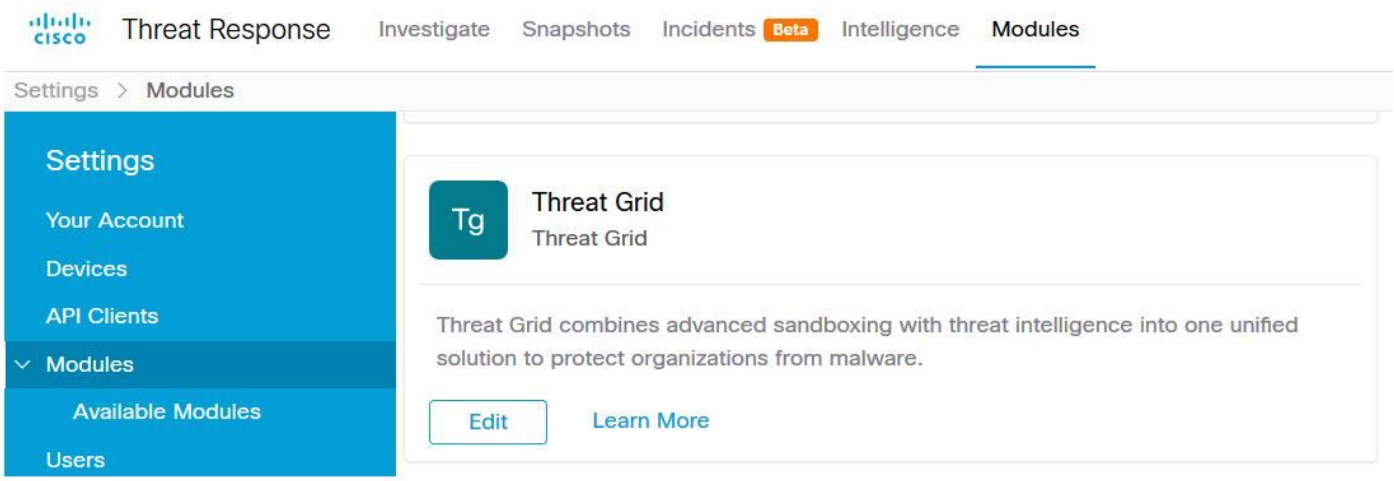
- **Nom du module** - Laissez le nom par défaut ou entrez un nom qui vous intéresse.
- **URL** - Dans la liste déroulante, sélectionnez l'URL appropriée pour l'emplacement où se

trouve votre compte Threat Grid (Amérique du Nord ou Europe). Ignorez l'option **Autre** pour l'instant.

Étape 5. Sélectionnez **Enregistrer** pour terminer la configuration du module Threat Grid.

Étape 6. Threat Grid s'affiche maintenant sous vos configurations sur la page **Modules** comme illustré dans l'image.

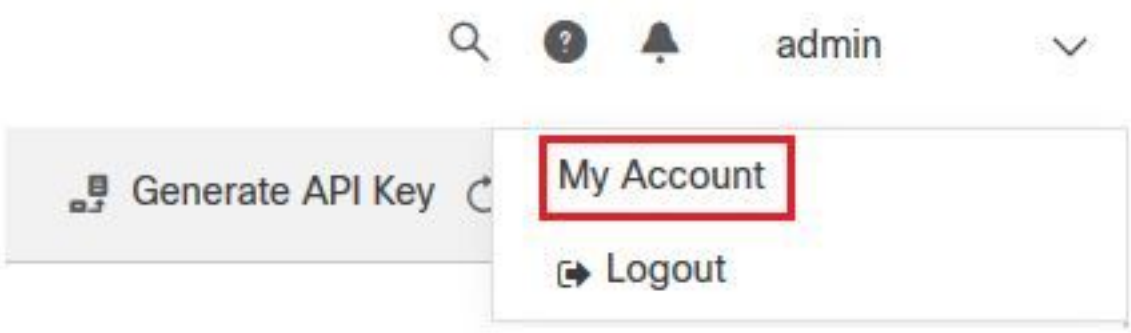
(TG est disponible dans les menus de pivot et dans les dossiers pour une meilleure analyse des menaces).



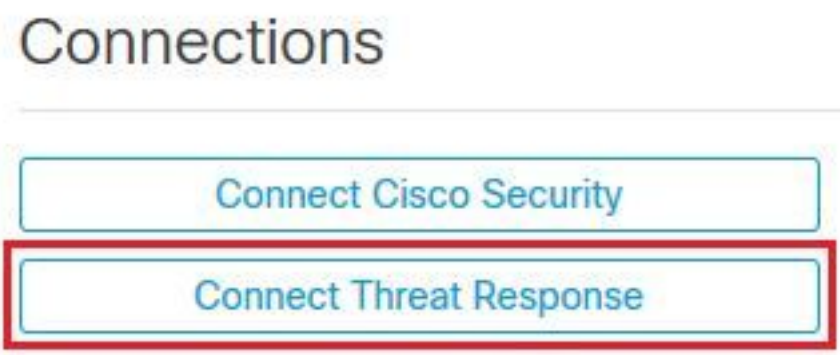
Console Threat Grid - Autoriser Threat Grid à accéder à la réponse aux menaces

Étape 1. Connectez-vous à Threat Grid à l'aide des informations d'identification de l'administrateur.

Étape 2. Accédez à la section **Mon compte**, comme illustré dans l'image.

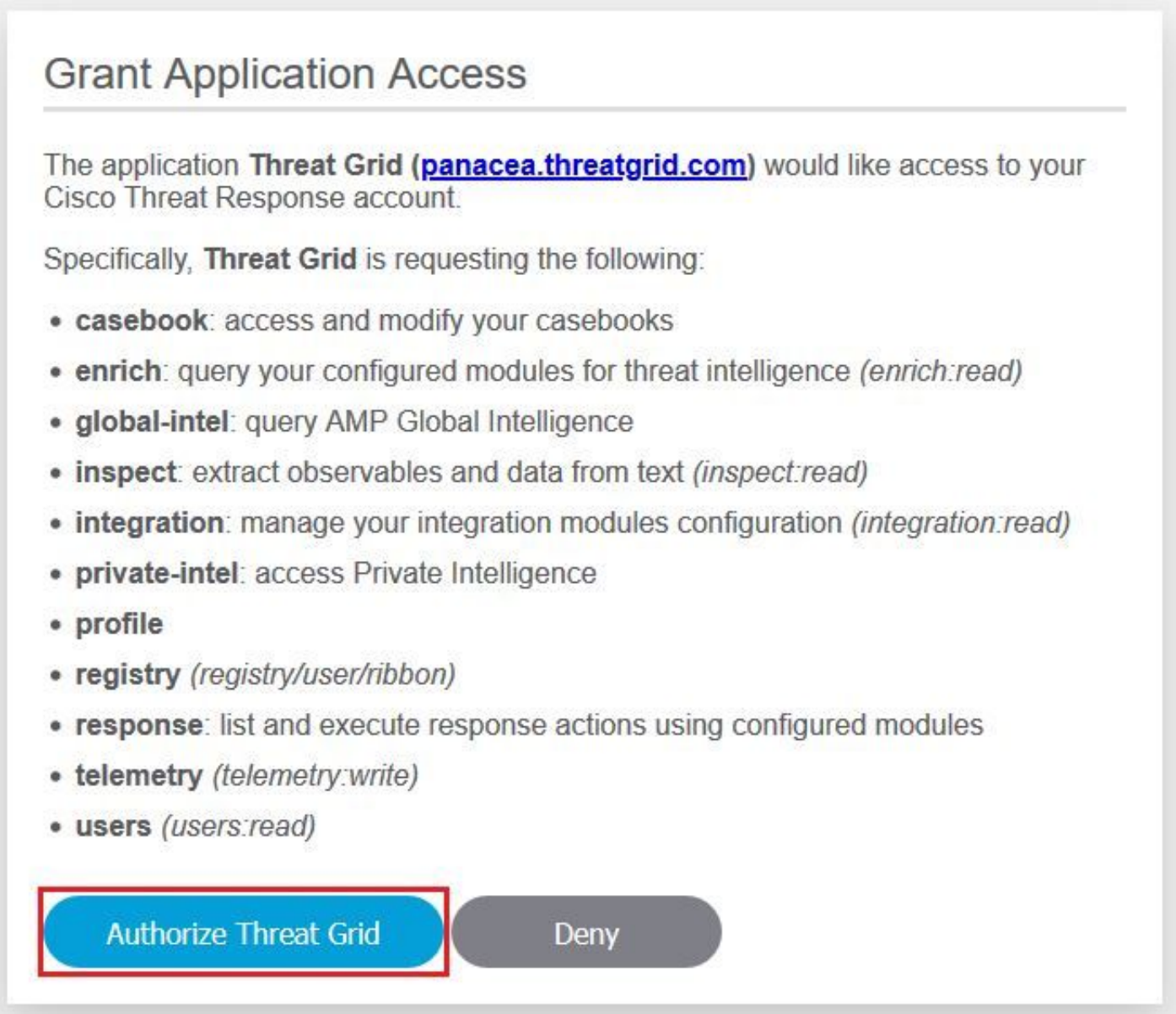


Étape 3. Accédez à la section **Connexions** et sélectionnez l'option **Connect Threat Response** comme indiqué dans l'image.

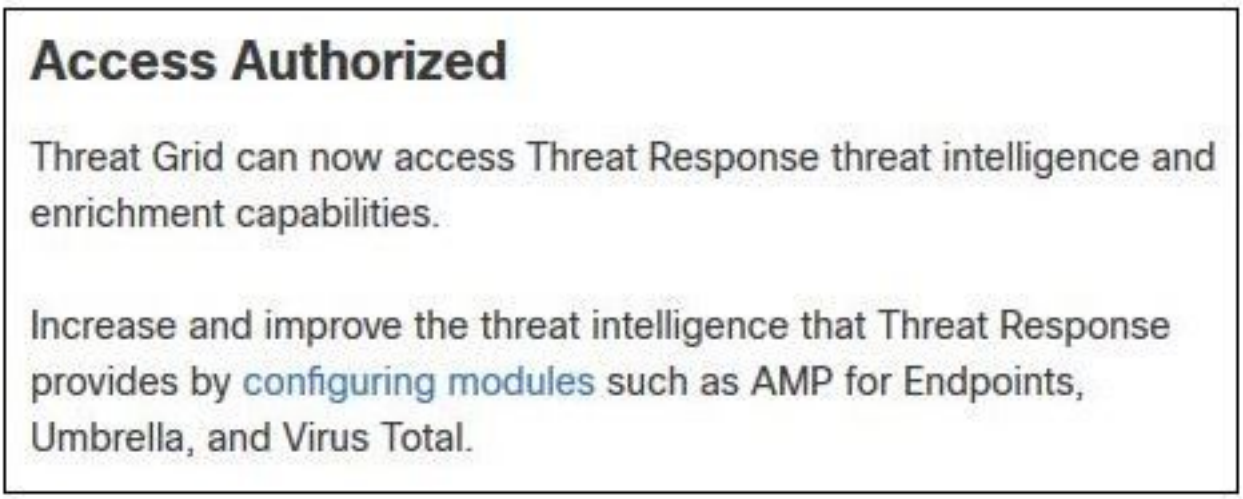


4 sept. Sélectionnez l'option **Autoriser** afin de permettre à Threat Grid d'accéder à Cisco Threat Response, comme illustré dans l'image.

Étape 5. Sélectionnez l'option **Autoriser la grille de menaces** afin d'accorder l'accès à l'application, comme illustré dans l'image.



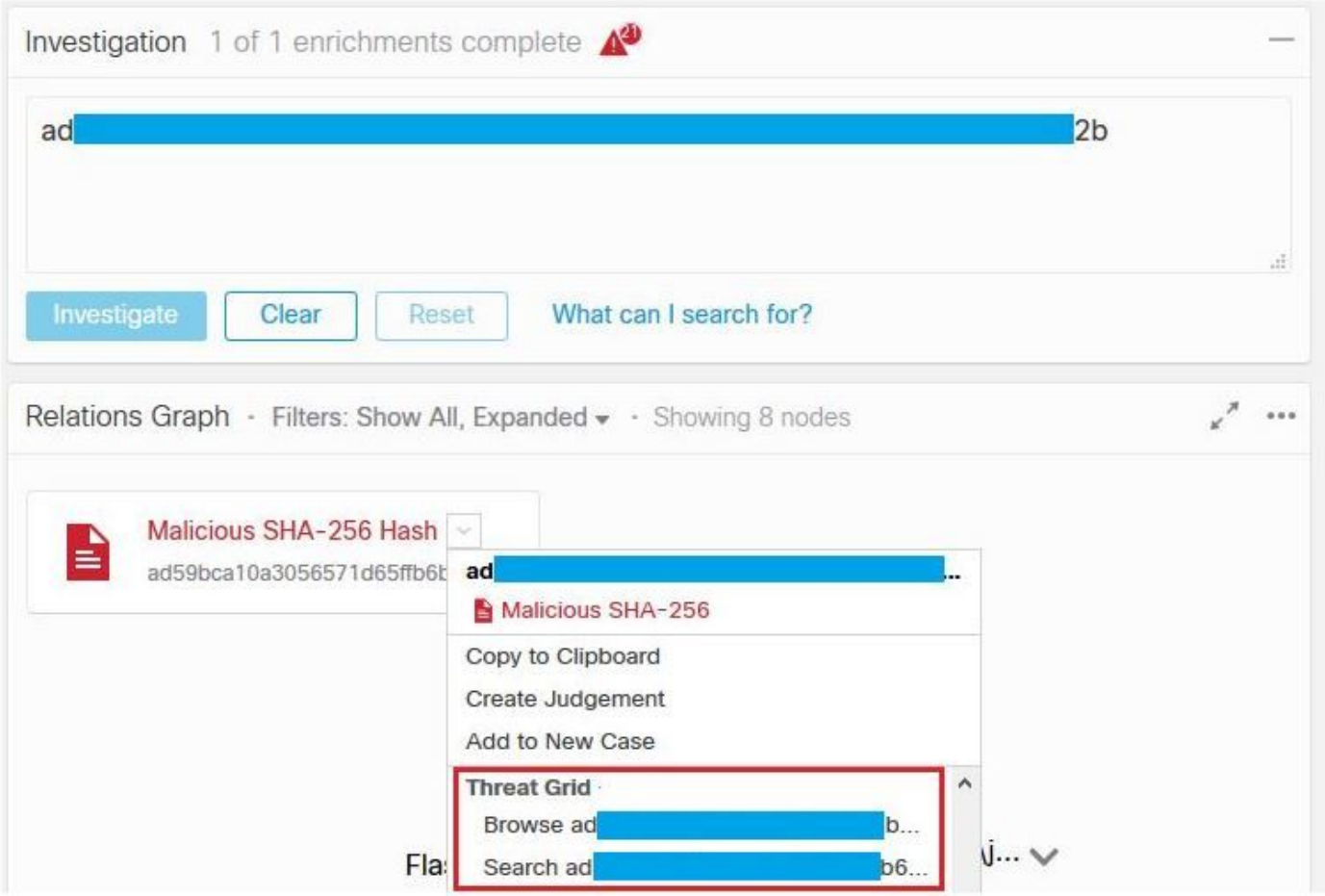
Étape 6. Le message Access Authorized (Autorisé d'accès) s'affiche pour vérifier que Threat Grid a accès aux fonctionnalités d'enrichissement et d'intelligence des menaces de la solution Threat Response, comme illustré sur l'image.



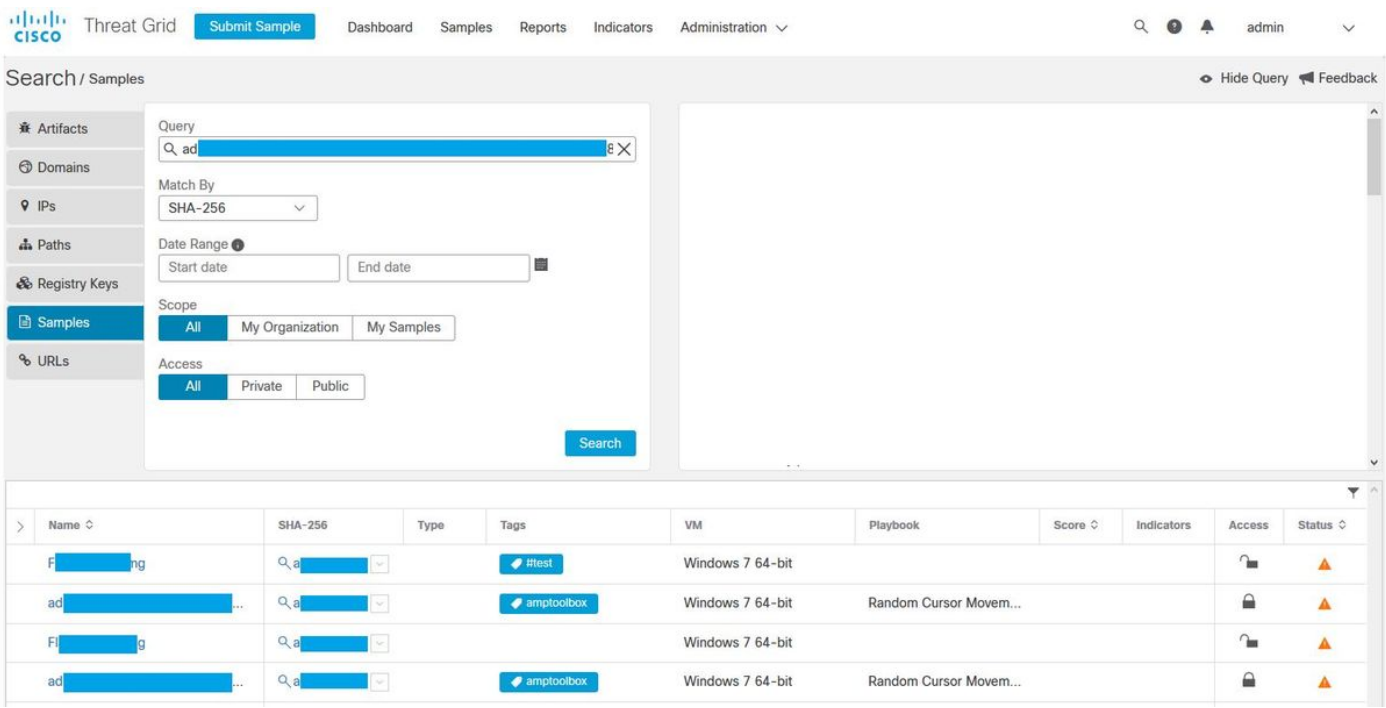
Vérification

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

Afin de vérifier l'intégration CTR et TG, vous pouvez effectuer une **enquête** sur la console CTR, lorsque tous les détails **d'enquête** apparaissent, vous pouvez voir l'option Threat Grid, comme illustré dans l'image.



Vous pouvez sélectionner l'option Parcourir ou Rechercher dans Threat Grid et l'option Redirige vers le portail Threat Grid pour collecter des informations supplémentaires sur les fichiers / hashs / IP / domaines / URL dans le magasin de connaissances Threat Grid, comme illustré dans l'image.


Threat Grid
Submit Sample
Dashboard
Samples
Reports
Indicators
Administration
admin
Search / Samples
Hide Query
Feedback
Artifacts
Domains
IPs
Paths
Registry Keys
Samples
URLs
Query
Match By
SHA-256
Date Range
Start date
End date
Scope
All
My Organization
My Samples
Access
All
Private
Public
Search
Name
SHA-256
Type
Tags
VM
Playbook
Score
Indicators
Access
Status
#test
Windows 7 64-bit
amptoolbox
Windows 7 64-bit
Random Cursor Movem...
Windows 7 64-bit
amptoolbox
Windows 7 64-bit
Random Cursor Movem...