Integrazione di CTR e Threat Grid Cloud

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Configurazione](#)
[Console CTR - Configura modulo Threat Grid](#)
[Console Threat Grid - Autorizza Threat Grid ad accedere alla risposta alla minaccia](#)
[Verifica](#)

Introduzione

In questo documento viene descritto come integrare Cisco Threat Response (CTR) con Threat Grid (TG) Cloud per eseguire le indagini CTR.

Contributo di Jesus Javier Martinez e a cura di Yeraldin Sanchez, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Threat Response
- Threat Grid

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Console CTR (account utente con diritti di amministratore)
- Console Threat Grid (account utente con diritti di amministratore)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco Threat Grid è una piattaforma avanzata e automatizzata di analisi dei malware e malware threat intelligence in cui file sospetti o destinazioni Web possono essere detonati senza influire

sull'ambiente utente.

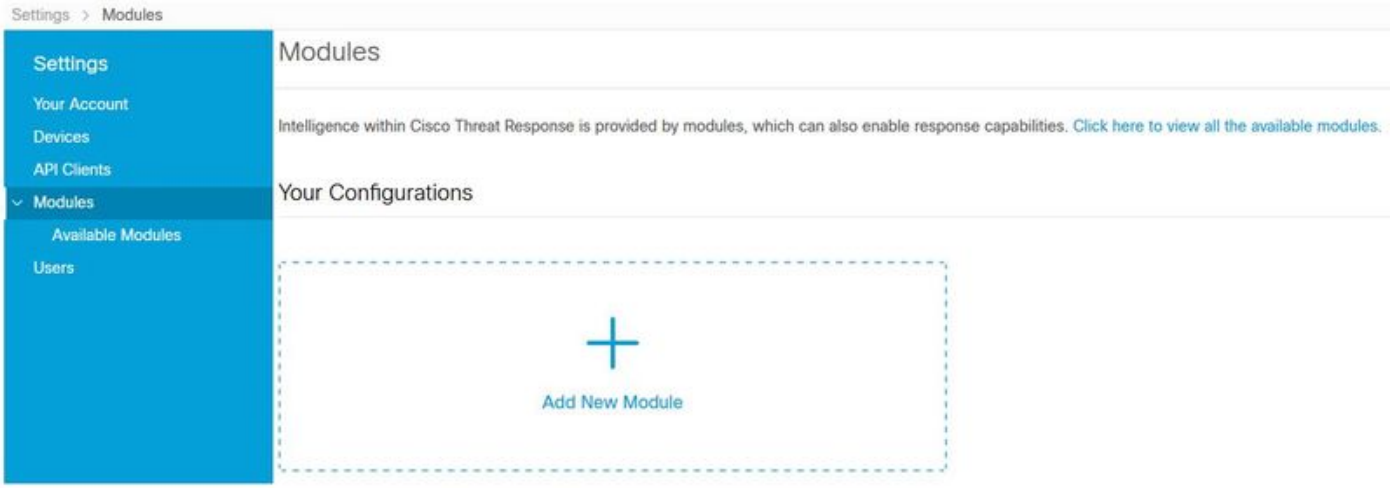
Nell'integrazione con Cisco Threat Response, Threat Grid è un modulo di riferimento e consente di eseguire il pivot nel portale Threat Grid per raccogliere informazioni aggiuntive su hash di file, IP, domini e URL nell'archivio delle informazioni di Threat Grid.

Configurazione

Console CTR - Configura modulo Threat Grid

Passaggio 1. Accedere a Cisco Threat Response utilizzando le credenziali di amministratore.

Passaggio 2. Passare alla scheda Moduli, selezionare **Moduli > Aggiungi nuovo modulo**, come mostrato nell'immagine.



Passaggio 3. Nella pagina Moduli disponibili, selezionare **Aggiungi nuovo modulo** nel riquadro del modulo Griglia minacce, come mostrato nell'immagine.

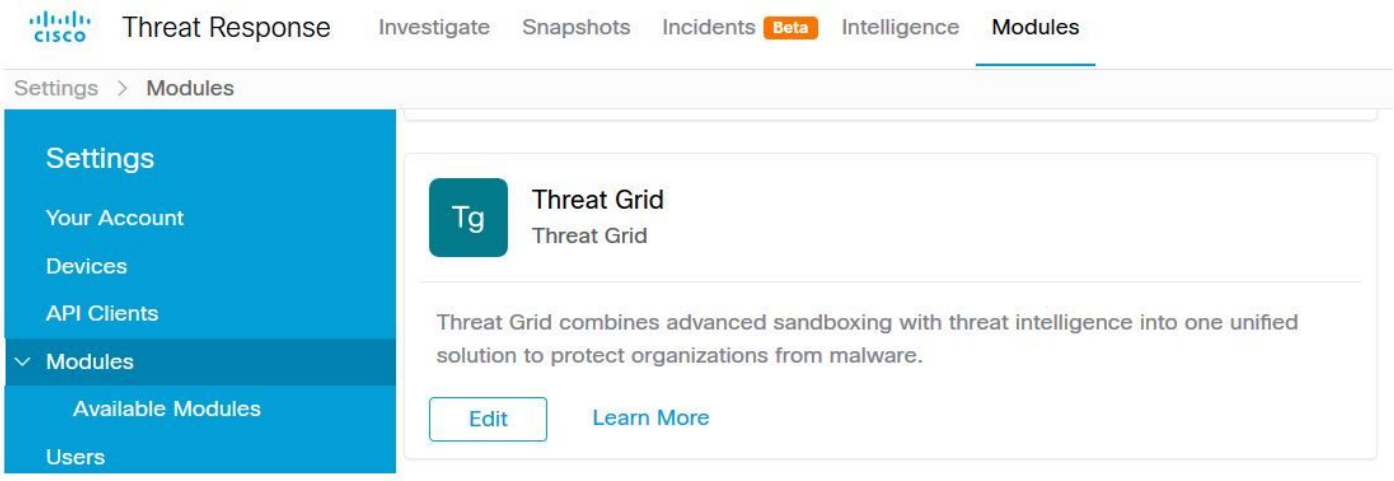
Passaggio 4. Verrà aperta la maschera **Aggiungi nuovo modulo**. Completare il modulo come illustrato nell'immagine.

- **Nome modulo**: lasciare il nome predefinito o immettere un nome significativo.
- **URL**: dall'elenco a discesa, scegliere l'URL appropriato per la posizione su cui si basa l'account Threat Grid (Nord America o Europa). Ignorare l'opzione **Altro** per il momento.

Passaggio 5. Selezionare **Salva** per completare la configurazione del modulo Threat Grid.

Passaggio 6. La griglia delle minacce è ora visualizzata nelle configurazioni nella pagina **Moduli**, come mostrato nell'immagine.

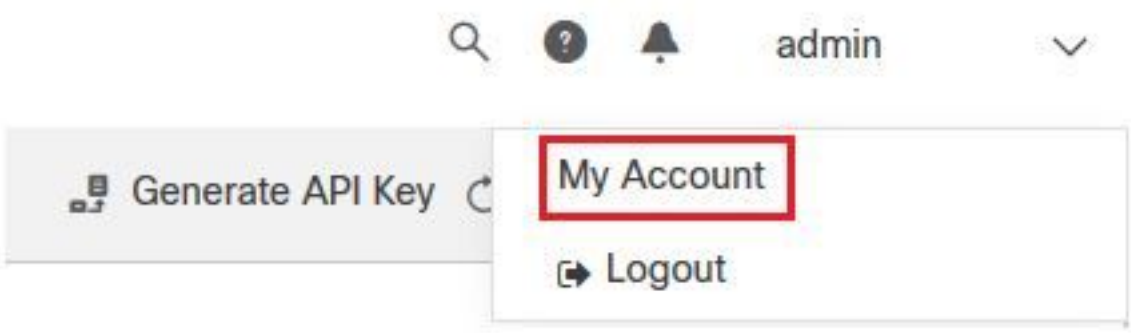
(TG è disponibile nei menu pivot e nei casebook per una migliore indagine delle minacce).



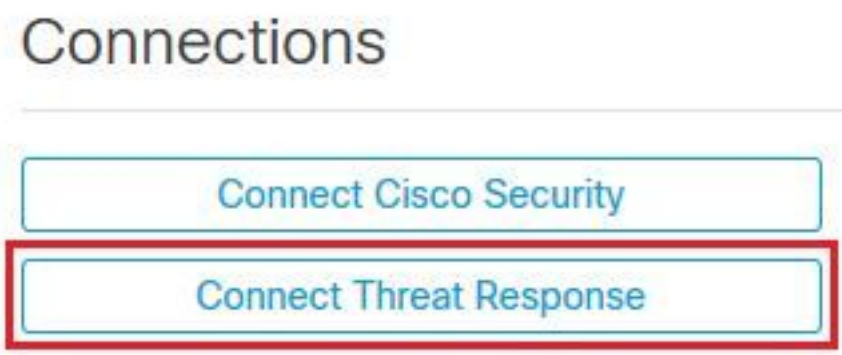
Console Threat Grid - Autorizza Threat Grid ad accedere alla risposta alla minaccia

Passaggio 1. Accedere alla griglia delle minacce utilizzando le credenziali di amministratore.

Passaggio 2. Passare alla sezione **Account personale**, come mostrato nell'immagine.

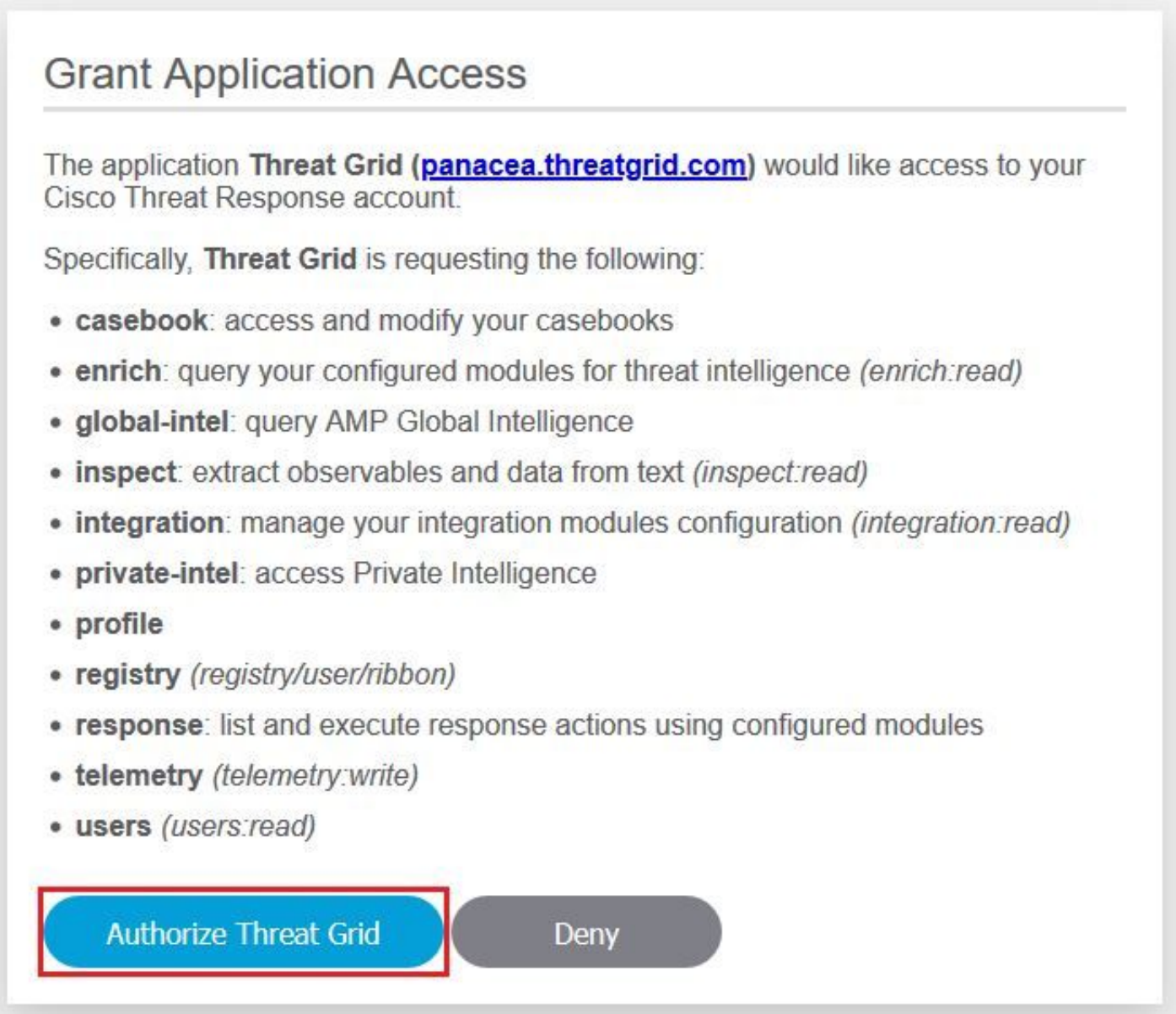


Passaggio 3. Passare alla sezione **Connessioni** e selezionare l'opzione **Connetti risposta alla minaccia** come mostrato nell'immagine.

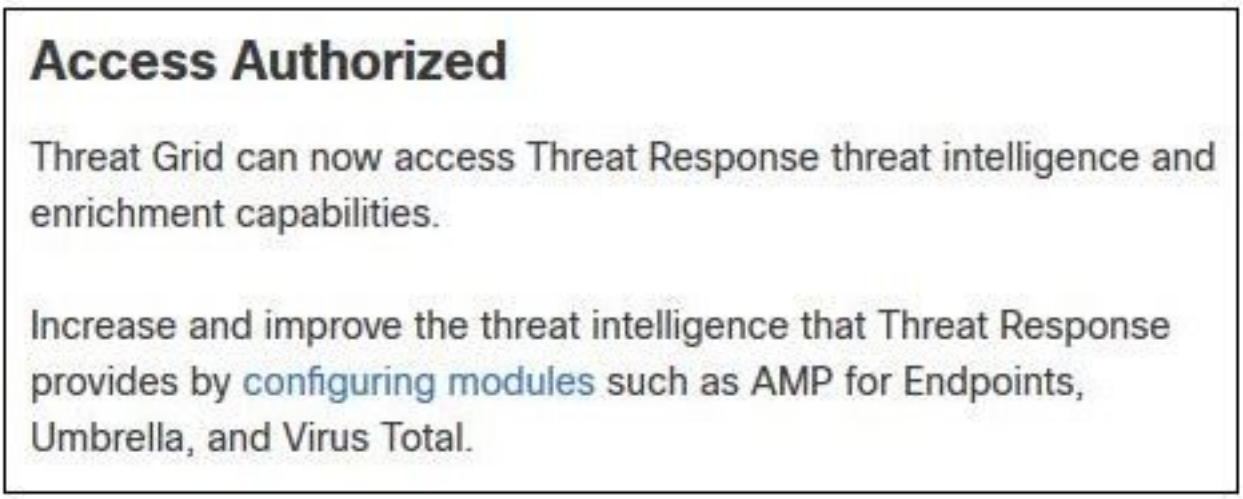


Passaggio 4. Selezionare l'opzione **Authorize** per consentire a Threat Grid di accedere a Cisco Threat Response, come mostrato nell'immagine.

Passaggio 5. Selezionare l'opzione **Autorizza griglia delle minacce** per concedere l'accesso all'applicazione, come mostrato nell'immagine.



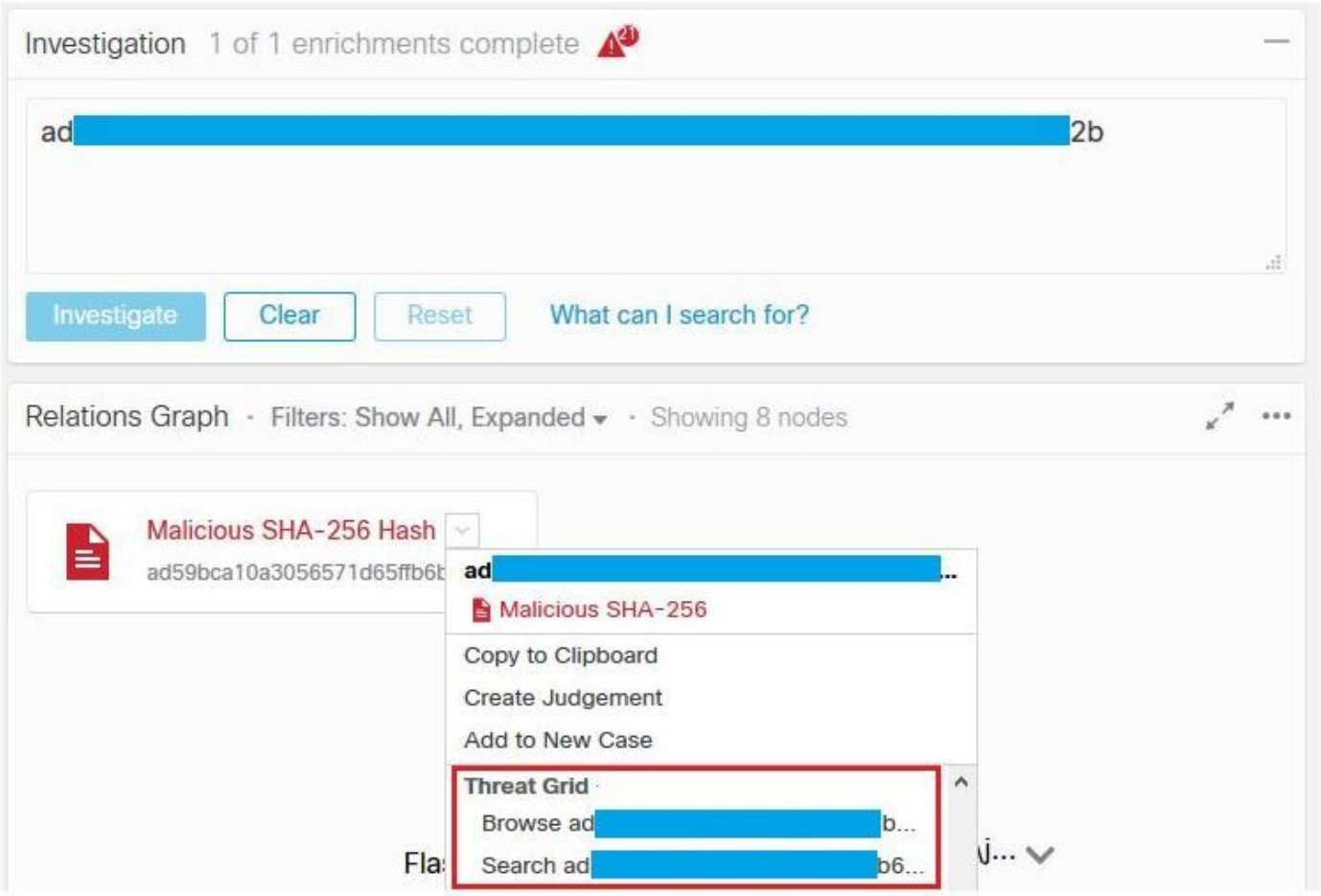
Passaggio 6. Viene visualizzato il messaggio Accesso autorizzato per verificare che Threat Grid abbia accesso alle funzionalità di rilevamento e arricchimento delle minacce di risposta alle minacce, come mostrato nell'immagine.



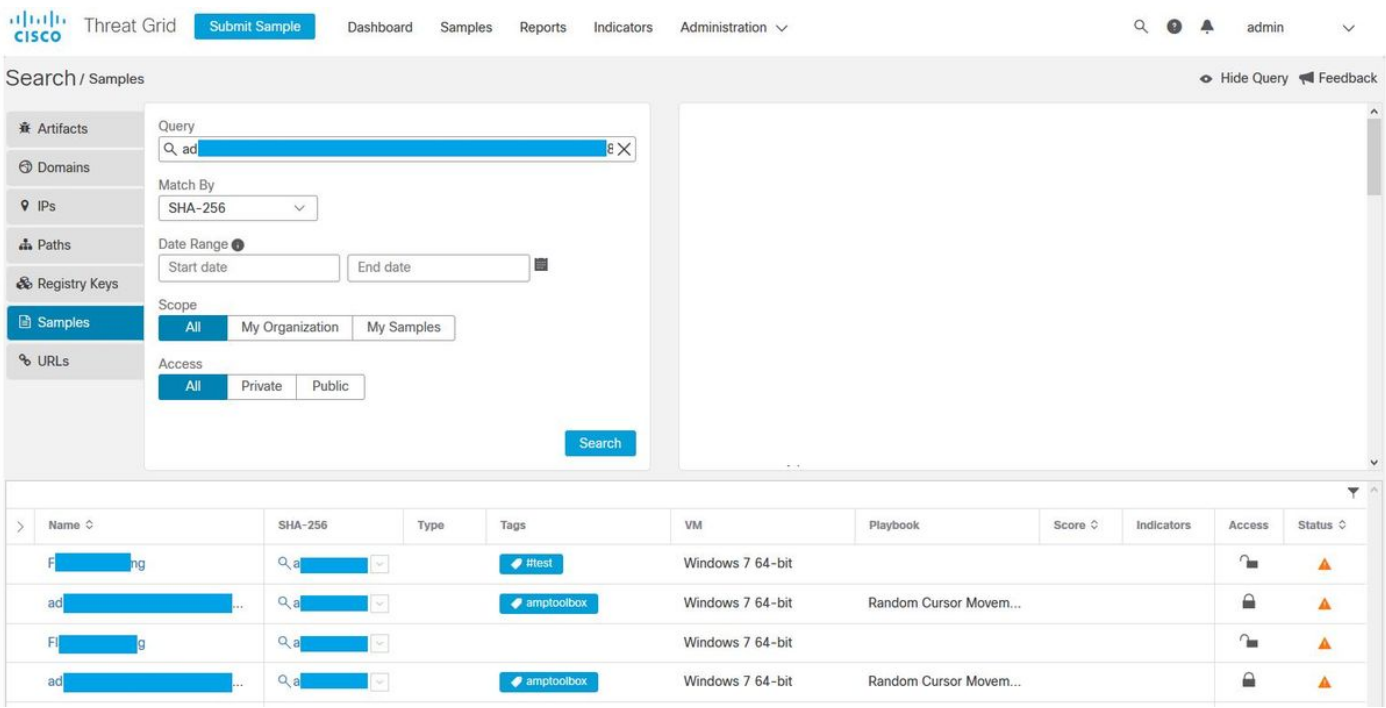
Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Per verificare l'integrazione di CTR e TG, potete eseguire un'**investigazione** sulla console CTR; quando vengono visualizzati tutti i dettagli dell'**investigazione**, potete visualizzare l'opzione Griglia minacce (Threat Grid), come mostrato nell'immagine.



Èpossibile selezionare l'opzione Sfoglia o Cerca nella griglia delle minacce e il reindirizzamento nel portale delle minacce per raccogliere informazioni aggiuntive su file / hash / IP / domini / URL nell'archivio delle informazioni sulla griglia delle minacce, come mostrato nell'immagine.


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...