Integre o CTR e a nuvem do Threat Grid

Contents

Introduction

Este documento descreve as etapas para integrar o Cisco Threat Response (CTR) à nuvem do Threat Grid (TG) para realizar investigações do CTR.

Contribuído por Jesus Javier Martinez, e editado por Yeraldin Sanchez, Engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Threat Response
- Threat Grid

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Console CTR (conta de usuário com direitos de administrador)
- Console do Threat Grid (conta de usuário com direitos de administrador)

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco Threat Grid é uma plataforma avançada e automatizada de análise de malware e inteligência de ameaças de malware na qual arquivos suspeitos ou destinos da Web podem ser

detonados sem afetar o ambiente do usuário.

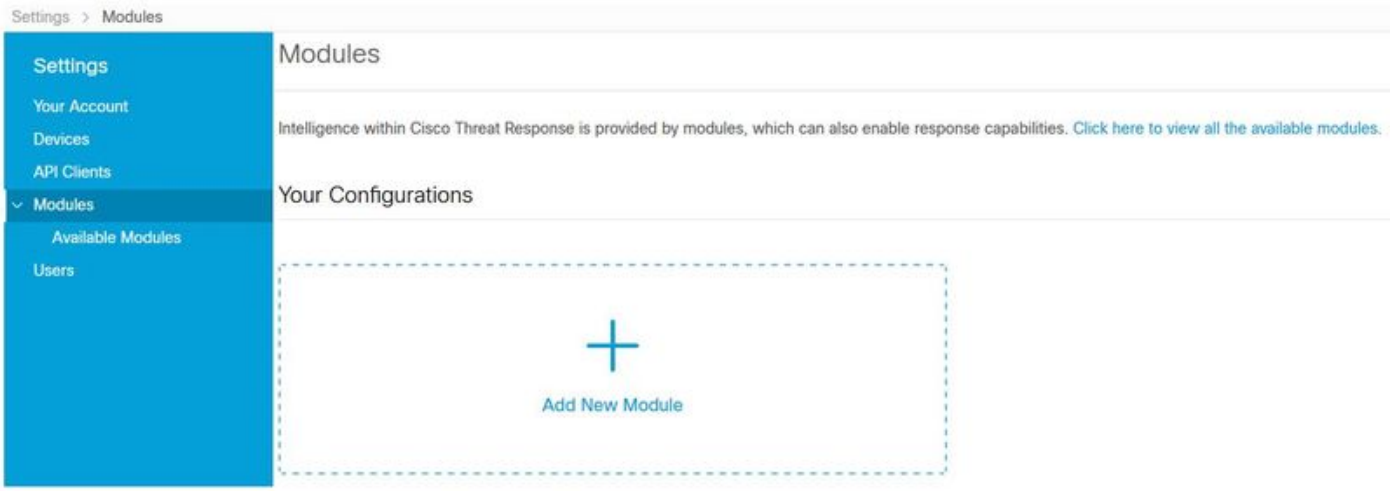
Na integração com o Cisco Threat Response, o Threat Grid é um módulo de referência e oferece a capacidade de fazer a migração para o Threat Grid Portal para coletar informações adicionais sobre hashes de arquivos, IPs, domínios e URLs no armazenamento de conhecimento do Threat Grid.

Configurar

Console CTR - Configurar o módulo Threat Grid

Etapa 1. Efetue login na Cisco Threat Response usando as credenciais do Administrador.

Etapa 2. Navegue até a guia Módulos, selecione **Módulos > Adicionar novo módulo**, conforme mostrado na imagem.



Etapa 3. Na página Módulos disponíveis, selecione **Adicionar novo módulo** no painel do módulo Threat Grid, como mostrado na imagem.

Etapa 4. O formulário **Adicionar novo módulo** é aberto. Preencha o formulário como mostrado na imagem.

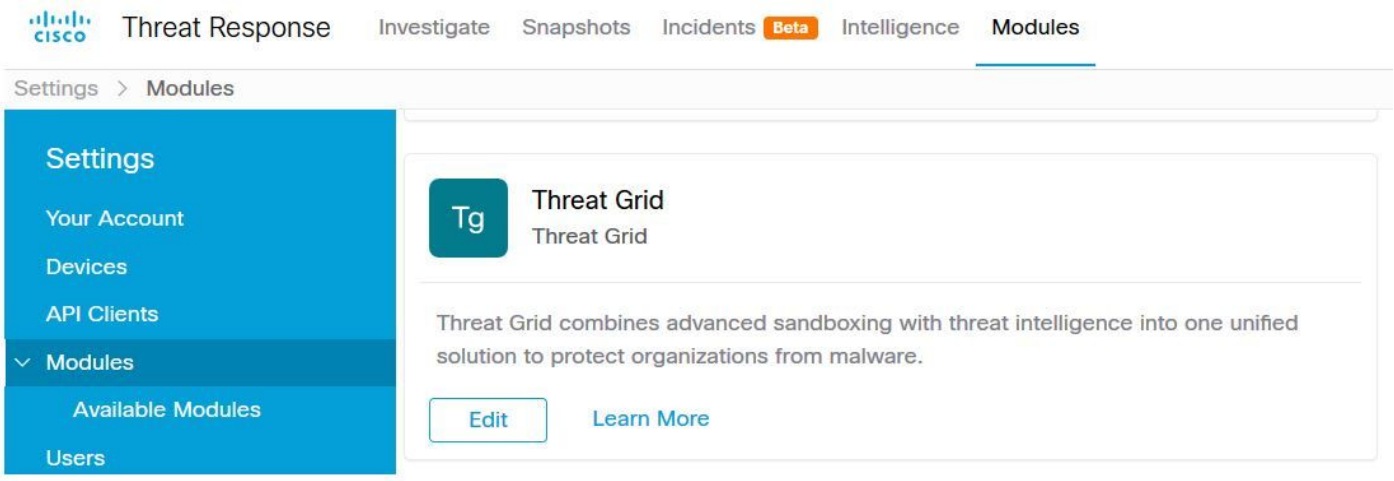
- **Module Name** - (Nome do módulo) Deixe o nome padrão ou insira um nome significativo para você.
- **URL** - Na lista suspensa, escolha o URL apropriado para o local onde sua conta do Threat

Grid está baseada (América do Norte ou Europa). Ignore a opção **Outro** por enquanto.

Etapa 5. Selecione **Salvar** para concluir a configuração do módulo Threat Grid.

Etapa 6. O Threat Grid agora é exibido em suas configurações na página **Módulos**, como mostrado na imagem.

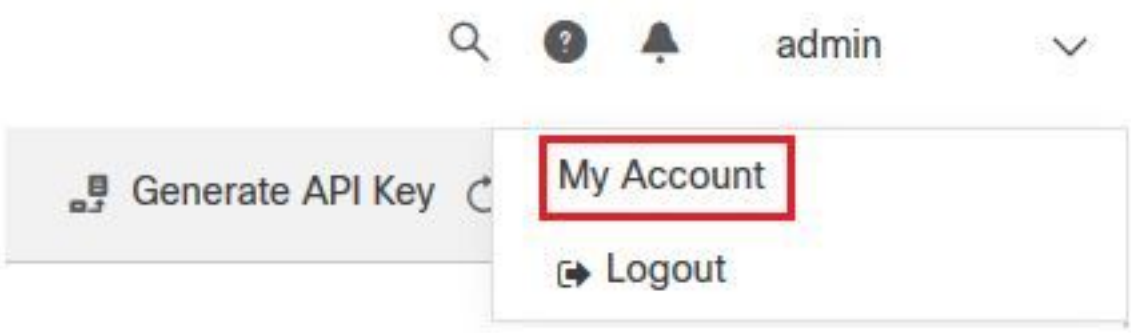
(O TG está disponível nos menus principais e nos gabinetes para uma melhor investigação de ameaças).



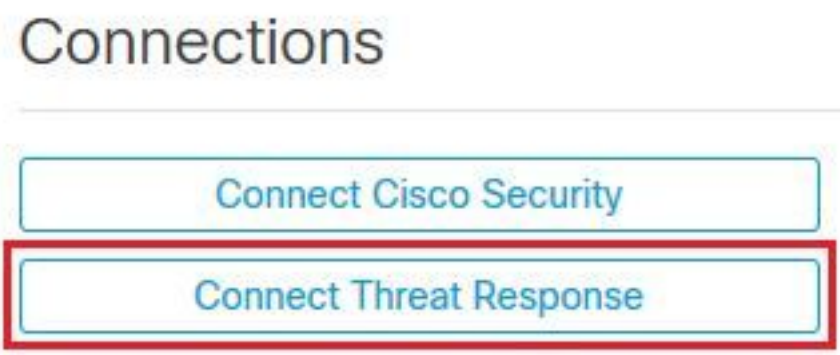
Console do Threat Grid - Autorizar o Threat Grid para acessar a resposta de ameaças

Etapa 1. Efetue login no Threat Grid usando as credenciais de Administrador.

Etapa 2. Navegue até a seção **Minha conta**, conforme mostrado na imagem.

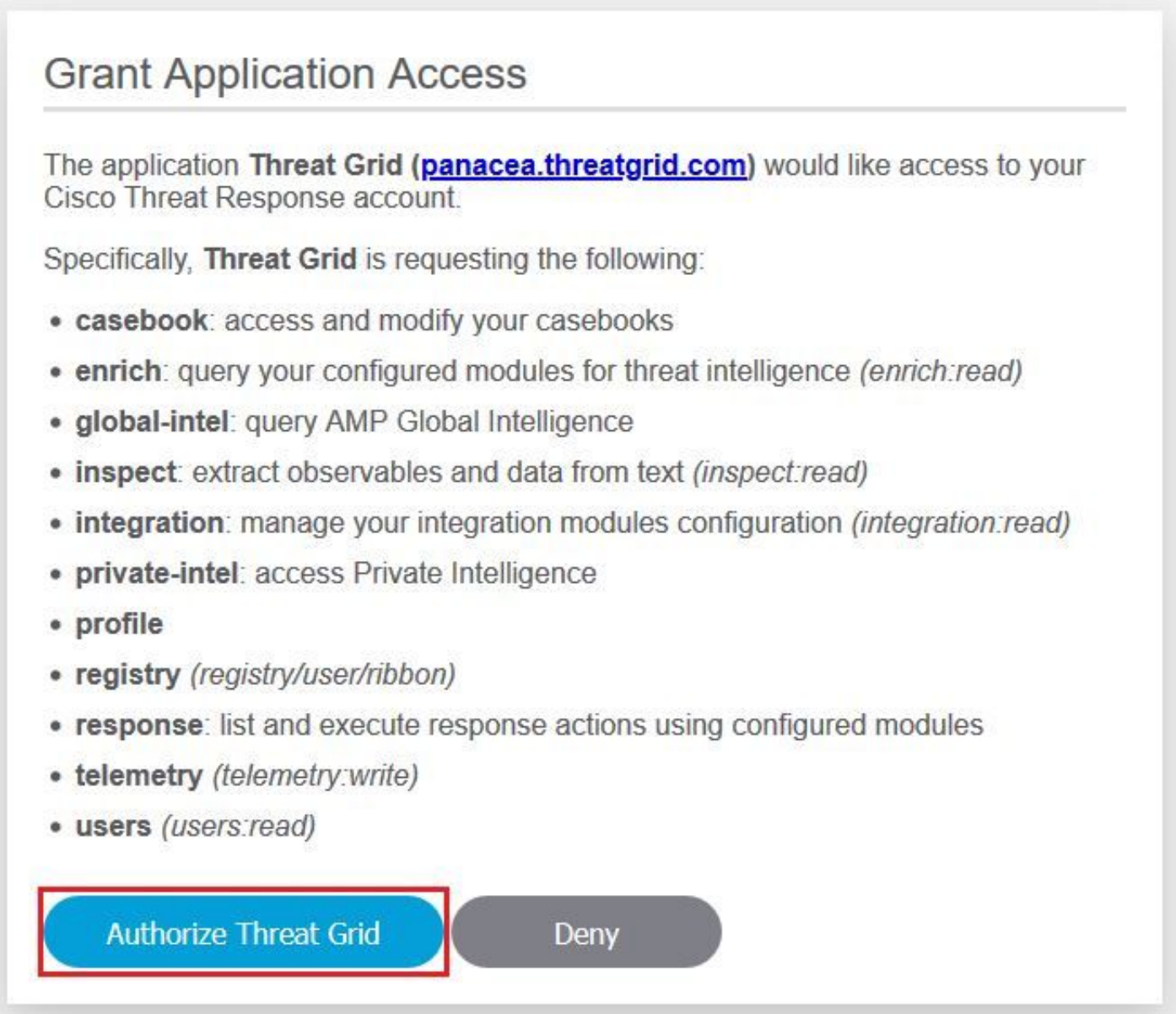


Etapa 3. Navegue até a seção **Conexões** e selecione a opção **Conectar resposta a ameaças**, conforme mostrado na imagem.

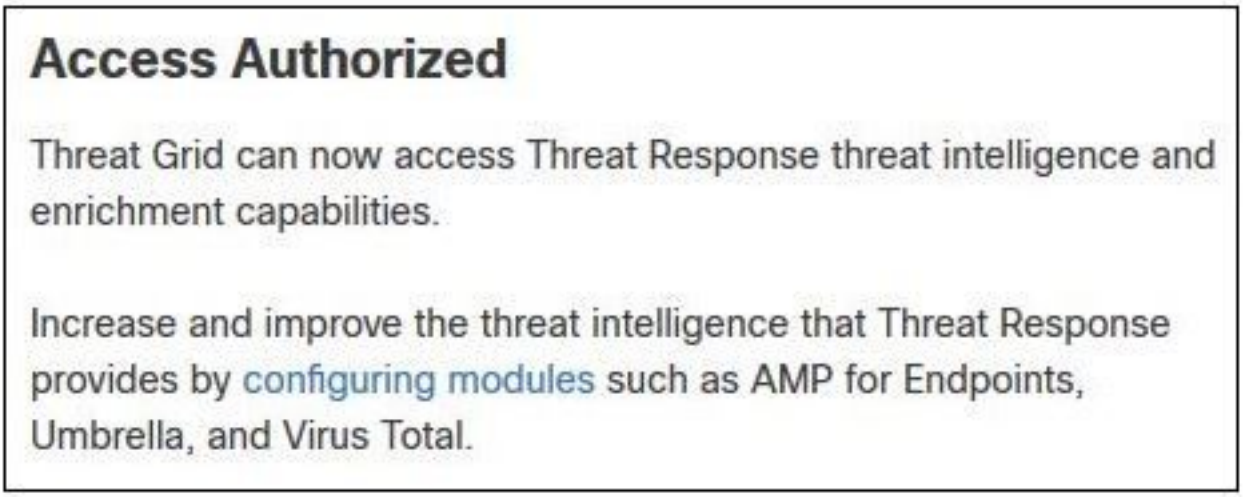


Etapa 4. Selecione a opção **Autorizar** para permitir que o Threat Grid acesse o Cisco Threat Response, como mostrado na imagem.

Etapa 5. Selecione a opção **Autorizar Grade de Ameaças** para conceder acesso ao aplicativo, como mostrado na imagem.



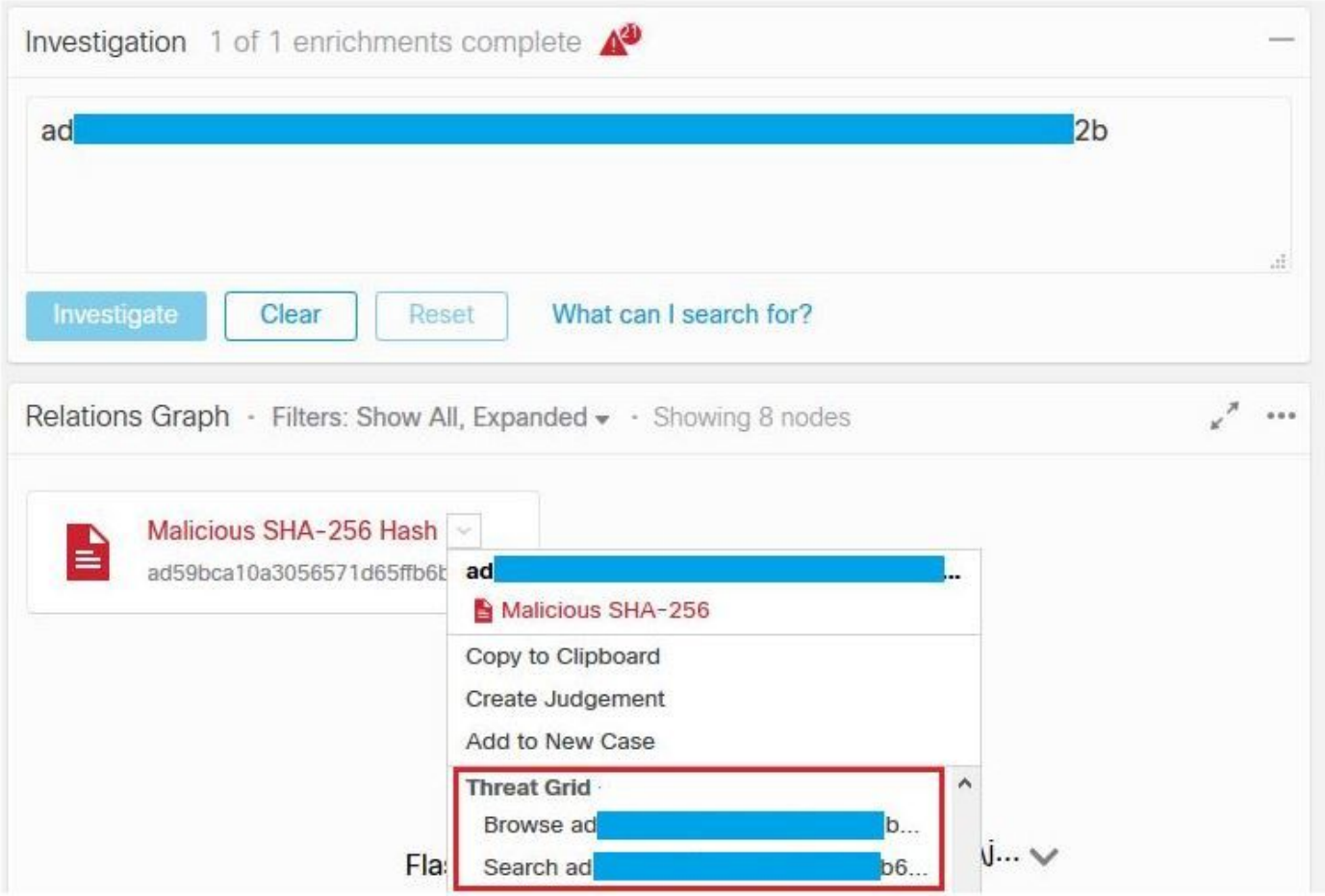
Etapa 6. A mensagem Access Authorized (Acesso autorizado) parece verificar se o Threat Grid tem acesso à inteligência de ameaças de resposta a ameaças e aos recursos de enriquecimento, como mostrado na imagem.



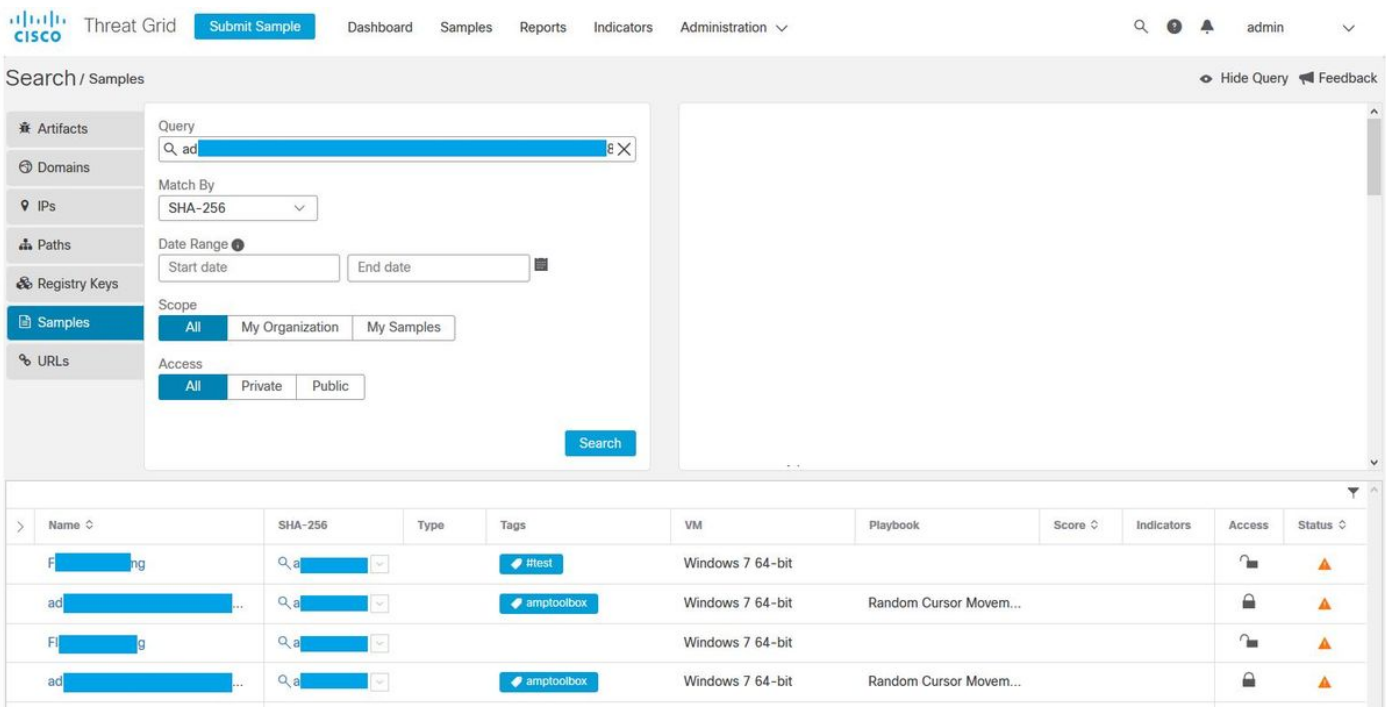
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para verificar a Integração CTR e TG, você pode fazer uma **Investigação** no console CTR, quando todos os detalhes da **Investigação** forem exibidos, você poderá ver a opção Threat Grid, como mostrado na imagem.



Você pode selecionar a opção Procurar ou Pesquisar o Threat Grid e ele é redirecionado para o Threat Grid Portal para coletar informações adicionais sobre arquivos / hashes / IPs / domínios / URLs no repositório de conhecimento do Threat Grid, como mostrado na imagem.


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...