

Configurar a integração da API do Microsoft Graph com o Cisco XDR

Contents

[Introdução](#)

[Pré-requisitos](#)

[Etapas de integração](#)

[Executar investigações](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve o procedimento para integrar a API do Microsoft Graph com o Cisco XDR e o tipo de dados que podem ser consultados.

Pré-requisitos

- Conta de administrador do Cisco XDR
- Conta do Administrador de Sistema do Microsoft Azure
- Acesso ao Cisco XDR

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Etapas de integração

Etapa 1.

Faça logon no Microsoft Azure como um Administrador do Sistema.

Microsoft Azure



Sign in

to continue to Microsoft Azure

admin@[REDACTED]microsoft.com

No account? [Create one!](#)

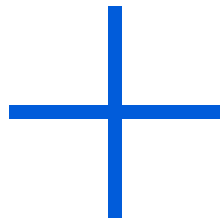
[Can't access your account?](#)

Back

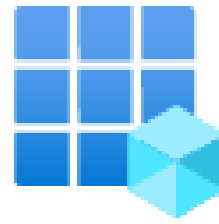
Next

Etapa 2.

Clique **App Registrations** no portal de serviços do Azure.



Create a
resource



App
registrations

Etapa 3.

Clique em New registration.

Home >

App registrations



New registration



Endp

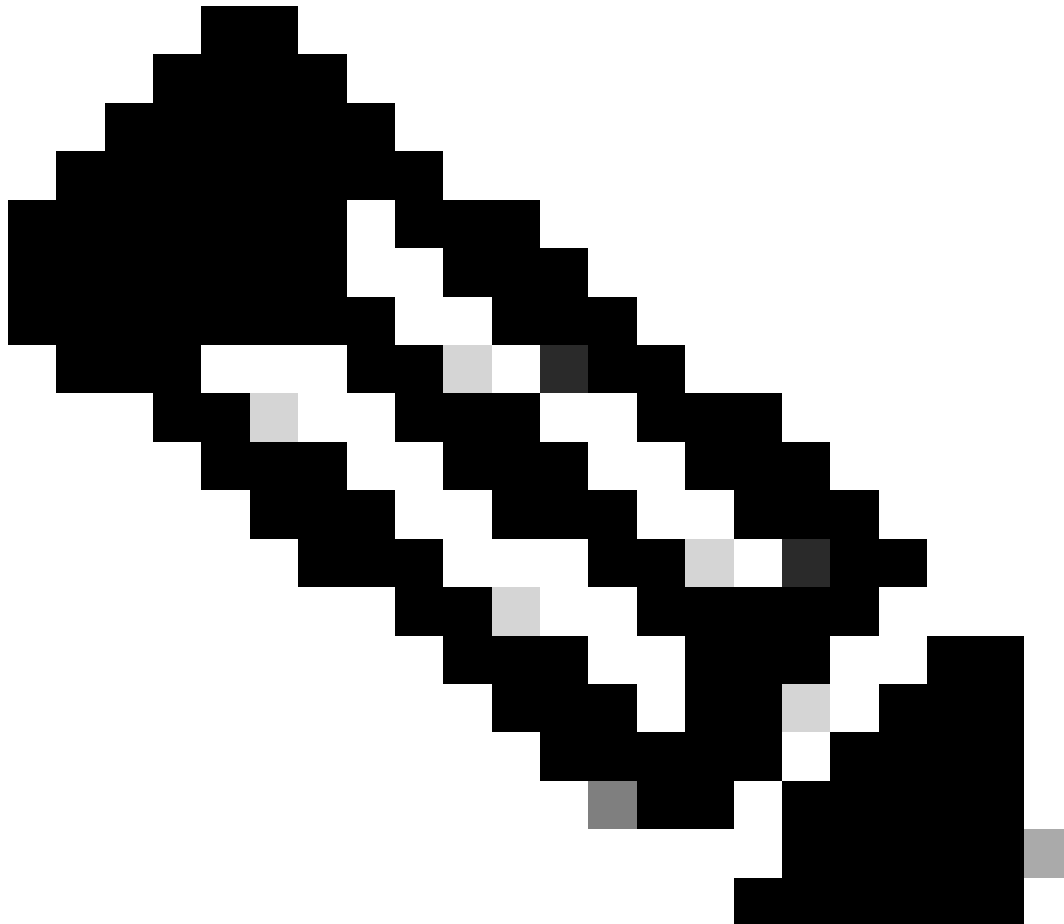
Etapa 4.

Digite um nome para identificar o novo Aplicativo.

▪ Name

The user-facing display name for this application (this can be changed later).

SecureX - Graph API



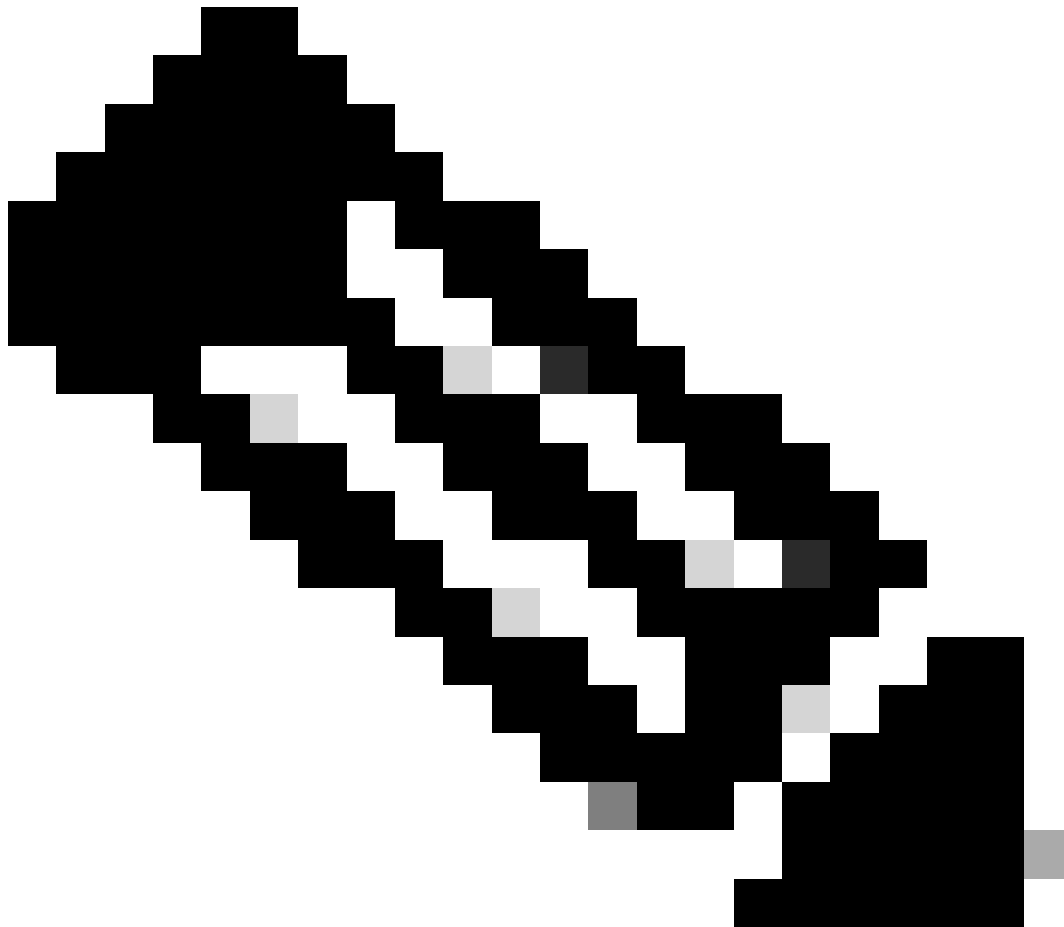
Observação: uma marca de seleção verde será exibida se o nome for válido.

Em Tipos de conta suportados, escolha a opção **Accounts in this organizational directory only**.

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (██████████ Single tenant)
 - Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 - Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 - Personal Microsoft accounts only
-



Observação: não é necessário digitar um URI de redirecionamento.

Role até a parte inferior da tela e clique em **Register**.

By proceeding, you agree to the Microsoft Platform Policies [↗](#)

Register

Etapa 6.





Volte para a página de serviços do Azure e clique em App Registrations > Owned Applications.

Identifique seu aplicativo e clique no nome. Neste exemplo, é SecureX.

All applications: Owned applications Deleted applications

[Add filters](#)

5 applications found

Display name ↑	Application (client) ID
 [Redacted]	049831 [Redacted]
 [Redacted]	9c660c [Redacted]
 [Redacted] Portal	6c3d8c [Redacted]
 SecureX	16e2bd33-8378-419e-86d7-64e1479fbc0

Passo 7.

Um resumo do seu aplicativo é exibido. Identifique estes detalhes relevantes:

ID do aplicativo (cliente):

Display name : [SecureX](#)

Application (client) ID : 16e2bd33-[Redacted]

ID do diretório (espaço):

Directory (tenant) ID : f2bf8cd3-[Redacted]

Etapa 8.

Navegue até Manage Menu > API Permissions.

Manage



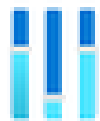
Branding & properties



Authentication



Certificates & secrets



Token configuration



API permissions

Etapa 9.

Em Permissões configuradas, clique em Add a Permission.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for ██████████

Etapa 10.

Na seção Solicitar permissões de API, clique em **Microsoft Graph**.

Select an API

Microsoft APIs

APIs my organization uses

My APIs

Commonly used Microsoft APIs



Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Etapa 11.

Selecione Application permissions.

What type of permissions does your application require?

Delegated permissions.

Your application needs to access the API as the signed-in user.

Application permissions.

Your application runs as a background service or daemon without a signed-in user.

Na barra Pesquisar, procure Security. Expandir **Security Actions** e selecionar

- **Ler.Tudo**
- **LeituraGravação.Tudo**

- **Eventos de segurança** e seleccione
 - **Ler.Tudo**
 - **LeituraGravação.Tudo**

- **Indicadores de ameaças** e seleccione
 - **IndicadoresDeAmeaças.LeituraGravação.PropriedadeDe**

Clique em Add permissions.

Etapa 12.

Revisar as permissões seleccionadas.

+ Add a permission ✓ Grant admin consent for [REDACTED]

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (5)				
SecurityActions.Read.All	Application	Read your organization's security actions	Yes	⚠ Not granted for [REDACTED]
SecurityActions.ReadWrite.All	Application	Read and update your organization's security actions	Yes	⚠ Not granted for [REDACTED]
SecurityEvents.Read.All	Application	Read your organization's security events	Yes	⚠ Not granted for [REDACTED]
SecurityEvents.ReadWrite.All	Application	Read and update your organization's security events	Yes	⚠ Not granted for [REDACTED]
ThreatIndicators.ReadWrite.Own	Application	Manage threat indicators this app creates or owns	Yes	⚠ Not granted for [REDACTED]
User.Read	Delegated	Sign in and read user profile	No	

To view and manage permissions and user consent, try [Enterprise applications](#).

Clique em **Grant Admin consent** para sua organização.

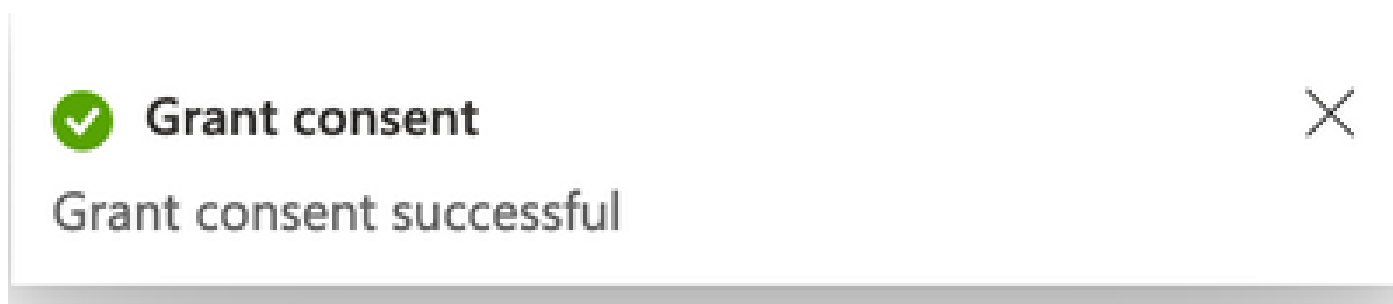
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for [REDACTED]

Um prompt para escolher se você deseja conceder consentimento para todas as permissões é exibido. Clique em Yes.

Um pop-up semelhante ao mostrado nesta imagem é exibido:



Etapa 13.

Navegue até Manage > Certificates & Secrets.

Clique em Add New Client Secret.

Escreva uma breve descrição e selecione uma data válidaExpires. Sugere-se selecionar uma data de validade de mais de 6 meses para evitar a expiração das chaves de API.

Depois de criada, copie e armazene em um local seguro a parte que diz **Value**, pois é usada para a integração.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
API	7/27/2024	bc [REDACTED]	412ref5 [REDACTED]

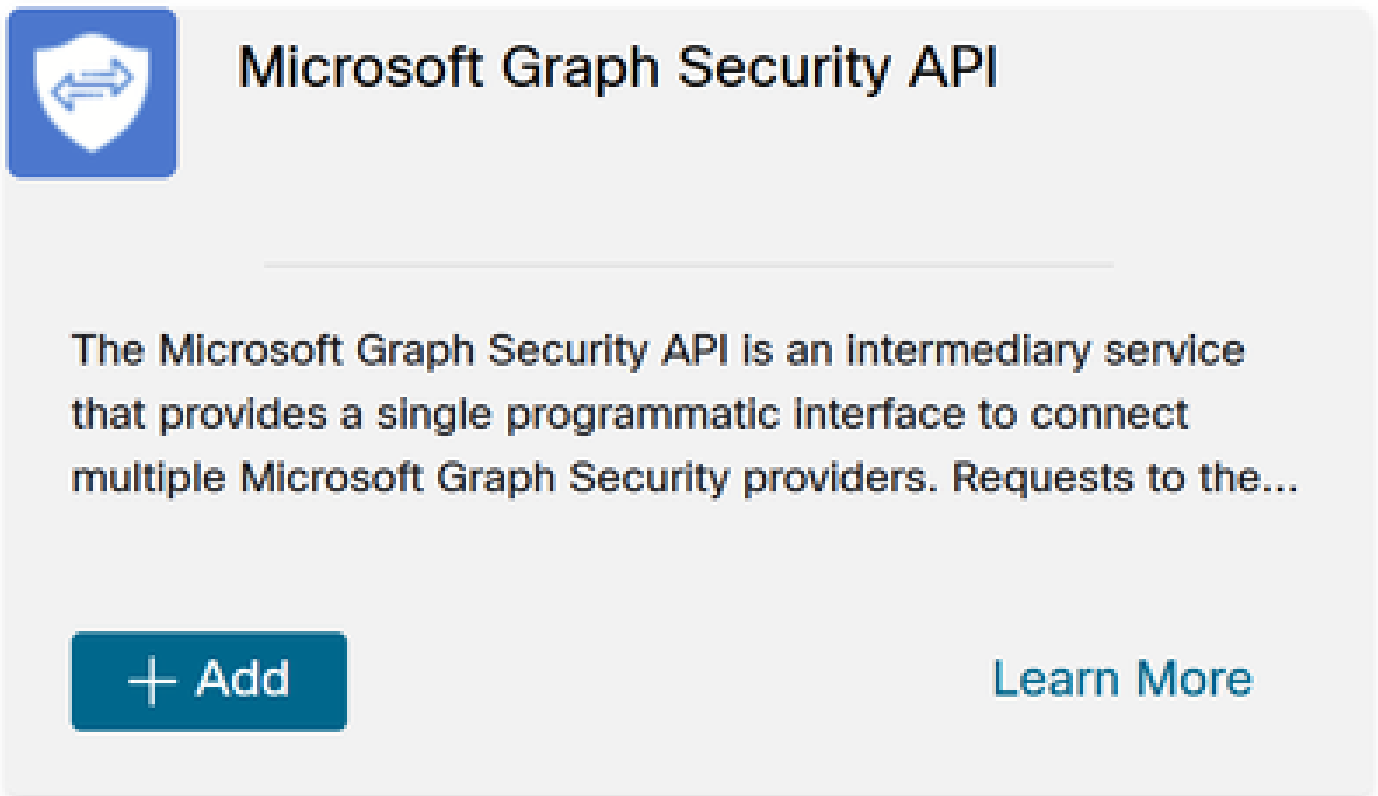


Aviso: este campo não pode ser recuperado e você deve criar um Novo Segredo.

Depois de ter todas as informações, navegue de volta **Overview** e copie os valores do seu aplicativo. Em seguida, navegue até SecureX.

Etapa 14.

Navegue para Integration Modules > Available Integration Modules > selecionar Microsoft Security Graph API e clique em Add.



The card features a blue shield icon with a white double-headed arrow. The title "Microsoft Graph Security API" is in a large, bold, black font. Below the title is a horizontal line. The main text describes the API as an intermediary service for connecting multiple providers. At the bottom left is a dark blue button with a white plus sign and the text "+ Add". At the bottom right is a blue link that says "Learn More".

Atribua um nome e cole os valores obtidos no portal do Azure.

Add New Microsoft Graph Security API Integration Module

Integration Module Name
Microsoft Graph Security API

Microsoft Graph Security API Credentials

Application ID
[Redacted]

Tenant ID
[Redacted]

Client Secret
[Redacted]

Integration Module configuration

Entities Limit
[Dropdown menu]

Specifies the maximum number of responses

Cancel Save

Quick Start

When configuring Microsoft Graph Security API integration, you must create an app in the [Azure Portal](#). After this is complete, you then add the Microsoft Graph Security API integration module in Secured.

1. Register an application with the Microsoft identity platform. For details, see [Register an application with the Microsoft identity platform endpoints](#).
2. In Secured, complete the [Add New Microsoft Graph Security API Integration Module](#) form.
 - **Integration Module Name** - Leave the default name or enter a name that is meaningful to you.
 - **Application ID**, **Tenant ID**, and **Client Secret** - Enter the account information from your Microsoft Graph Security API credentials.
 - **Entities Limit** - Specify the maximum number of responses in a single response, per requested identifiability (must be a positive value). We recommend that you enter a limit in the range of 50 to 1000. The default is 100 entities.
3. Click **Save** to complete the Microsoft Graph Security API integration module configuration.

Clique Save e aguarde a verificação de integridade ser bem-sucedida.

Edit Microsoft Graph Security API Module



This integration module has no issues.

Executar investigações

A partir de agora, a API do Microsoft Security Graph não preenche o painel do Cisco XDR com um bloco. Em vez disso, as informações do seu portal do Azure podem ser consultadas com o uso de Investigações.

Lembre-se de que a API do Graph só pode ser consultada para:

- ip
- domínio
- hostname
- url
- nome_do_arquivo
- caminho_do_arquivo
- sha256

Neste exemplo, a investigação usou este SHA `c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148`.

Results

Details

Threat Context

▼ 0 TARGETS

▼ 1 INVESTIGATED



c73d01ffb427e5b7008003b4eaf9...

Malicious SHA-256 Hash

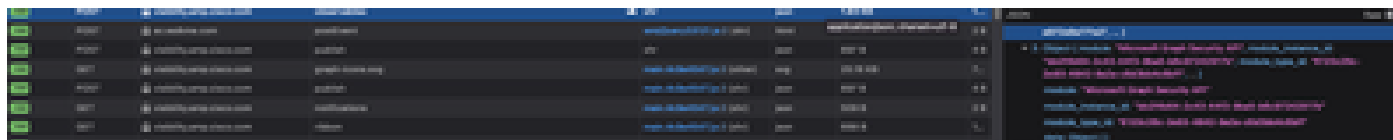
0 Sightings

▶ 0 OMITTED

▶ 0 RELATED

Como você pode ver, ele tem 0 pontos turísticos no ambiente de laboratório, então como testar se a API do Graph funciona?

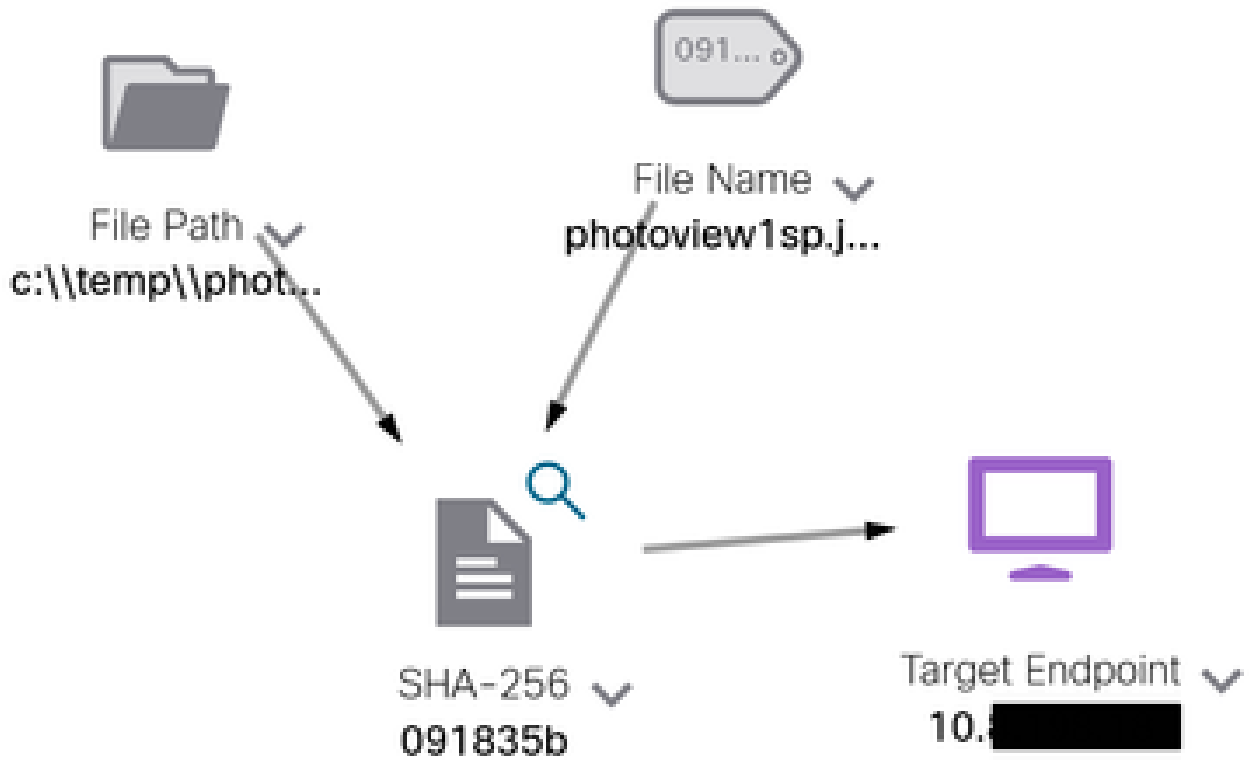
Abra o WebDeveloper Tools, execute a investigação, encontre um evento de postagem para **visibility.amp.cisco.com** no arquivo chamado Observables.



Verificar

Você pode usar este link: [Snapshots de segurança do gráfico da Microsoft](#) para obter uma lista de Snapshots que o ajudam a entender a resposta que você pode obter de cada tipo de item observável.

Você pode ver um exemplo como mostrado nesta imagem:



Expanda a janela, você poderá ver as informações fornecidas pela integração:

Module: Microsoft Graph Security API
 Source: Microsoft Graph Security
 Sensor: Endpoint

Confidence: None
 Severity: Medium
 Environment: Global
 Resolution: N/A

DESCRIPTION

Attackers can implant the right-to-left-override (RLO) in a filename to change the order of the characters in the filename and make it appear legitimate. This technique is used in different social engineering attacks to convince the user to run the file, and may also be used for hiding purposes. The file photoview[gg]ps1 disguises itself as photoview1sp.jpg

OBSERVABLES RELATED TO SIGHTING (1)

SHA-256 Hash: 091835b16193e536ee1bba04d0fceff534544cad306673066f3ad6973a4b18b19

Lembre-se de que os dados devem existir no portal do Azure, e a API do Graph funciona melhor quando usada com outras soluções da Microsoft. No entanto, isso deve ser validado pelo Suporte da Microsoft.

Troubleshooting

- Mensagem de falha de autorização:
 - Verifique se os valores para **Tenant ID** e Client ID estão corretos e se ainda são válidos.

- Nenhum dado aparece na investigação:
 - Certifique-se de ter copiado e colado os valores apropriados para **Tenant ID** e **Client ID**.
 - Certifique-se de ter usado as informações do campo **Value** da Certificates & Secrets seção.
 - Use as ferramentas do WebDeveloper para determinar se a API do Graph é consultada quando ocorre uma investigação.
 - À medida que a API do Graph mescla dados de vários provedores de alerta da Microsoft, certifique-se de que OData seja suportado para os filtros de consulta. (Por exemplo, Segurança e Conformidade do Office 365 e ATP do Microsoft Defender).

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.