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

Contents

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

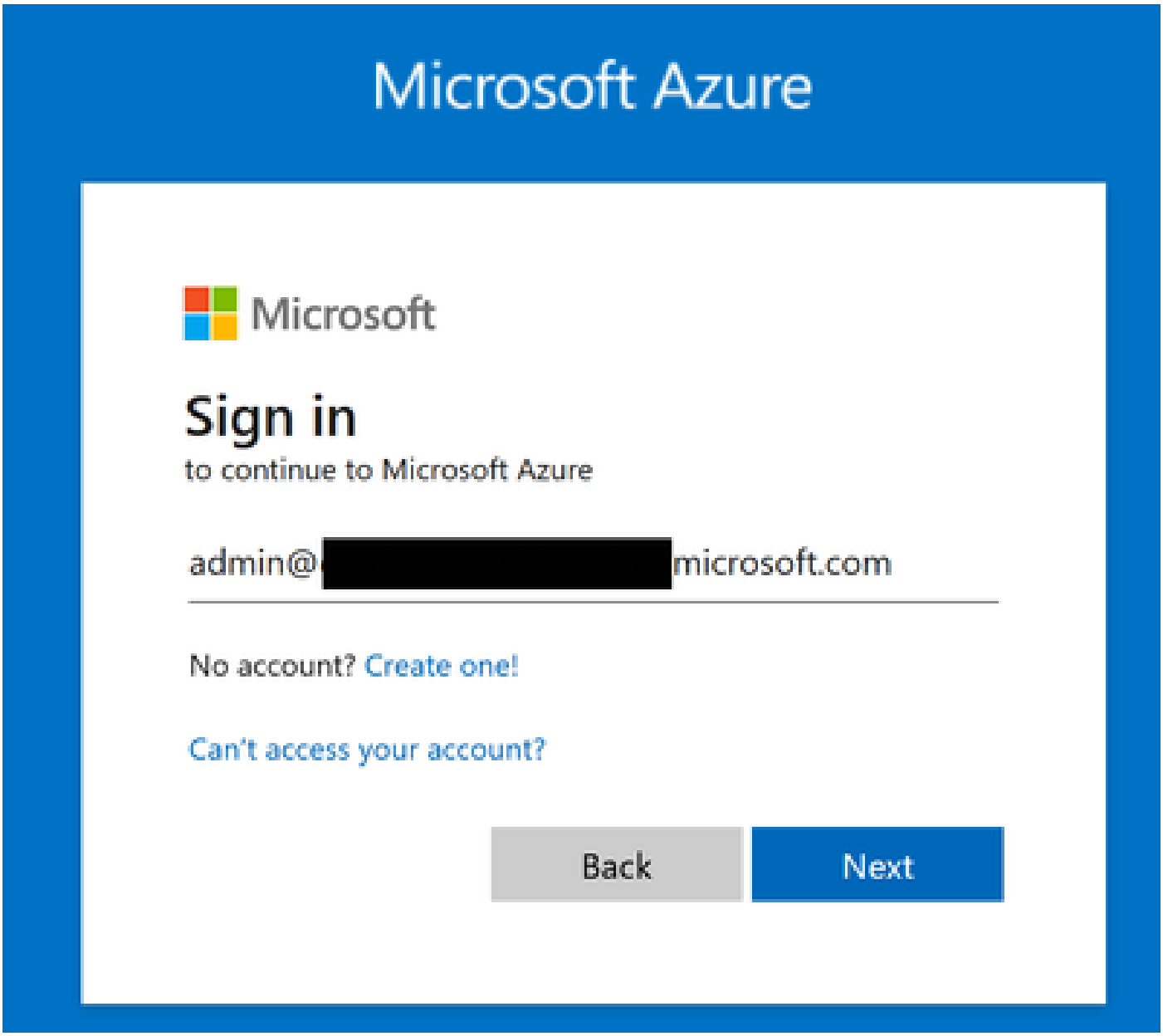
- Conta de administrador do Cisco XDR
- Conta do Administrador de Sistema do Microsoft Azure
- Acesso ao Cisco XDR

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

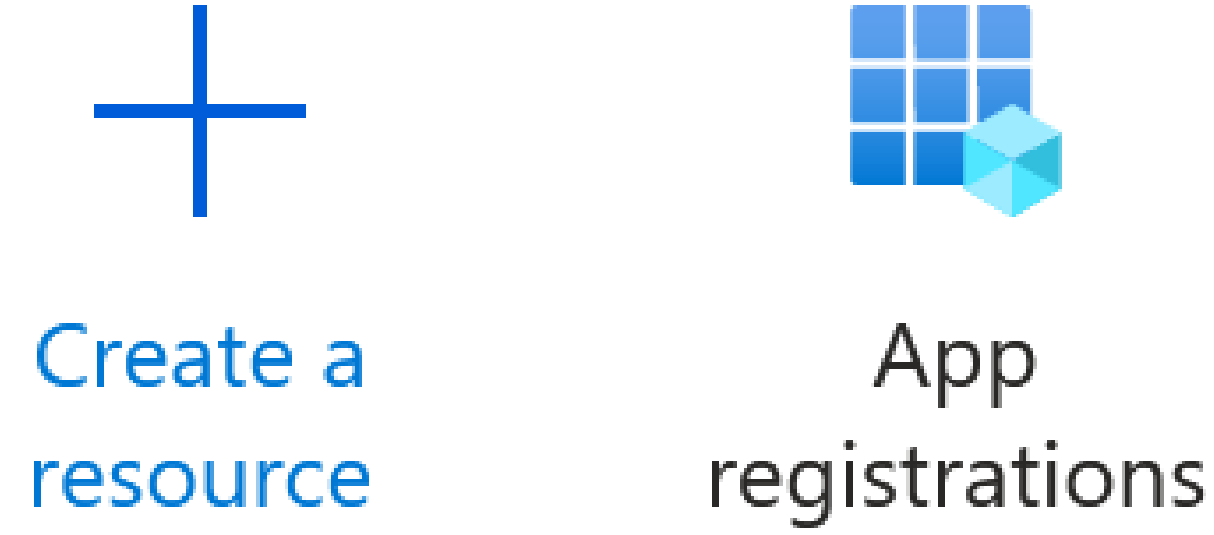
Etapa 1.

Faça logon no Microsoft Azure como um Administrador do Sistema.



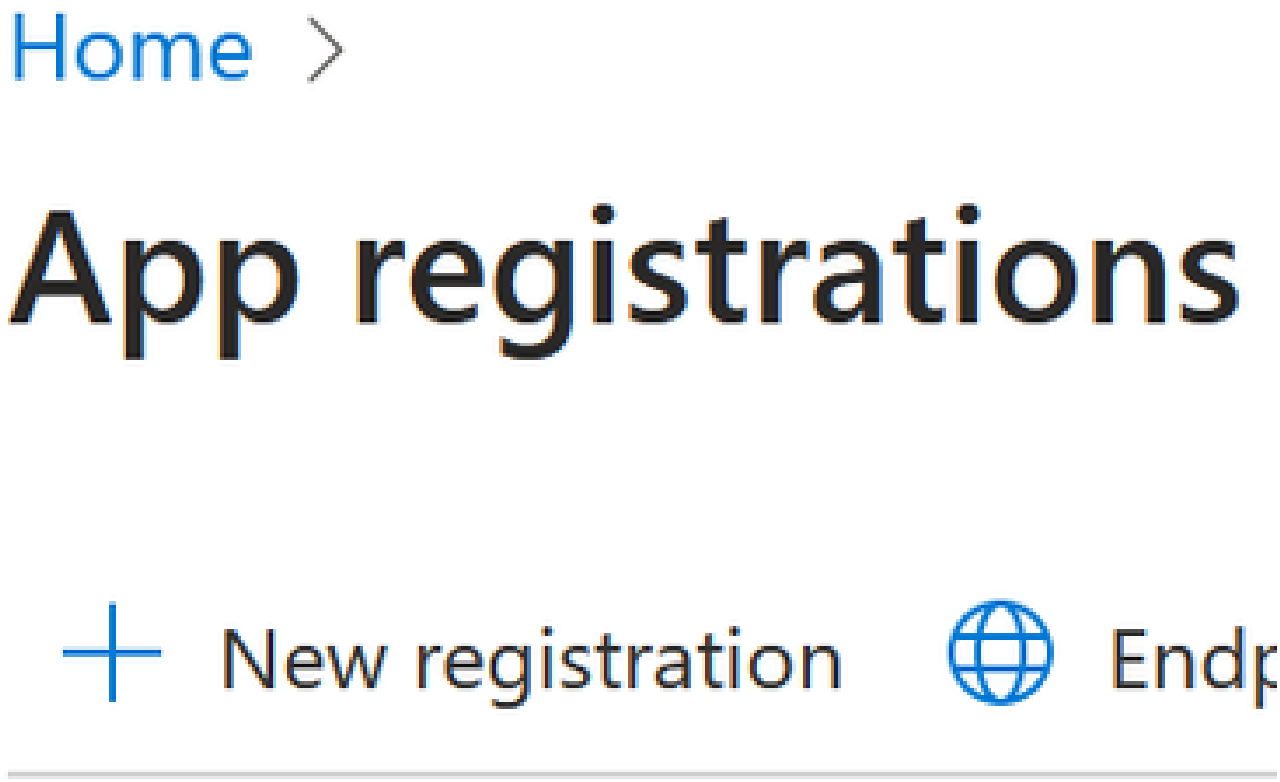
Etapa 2.

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



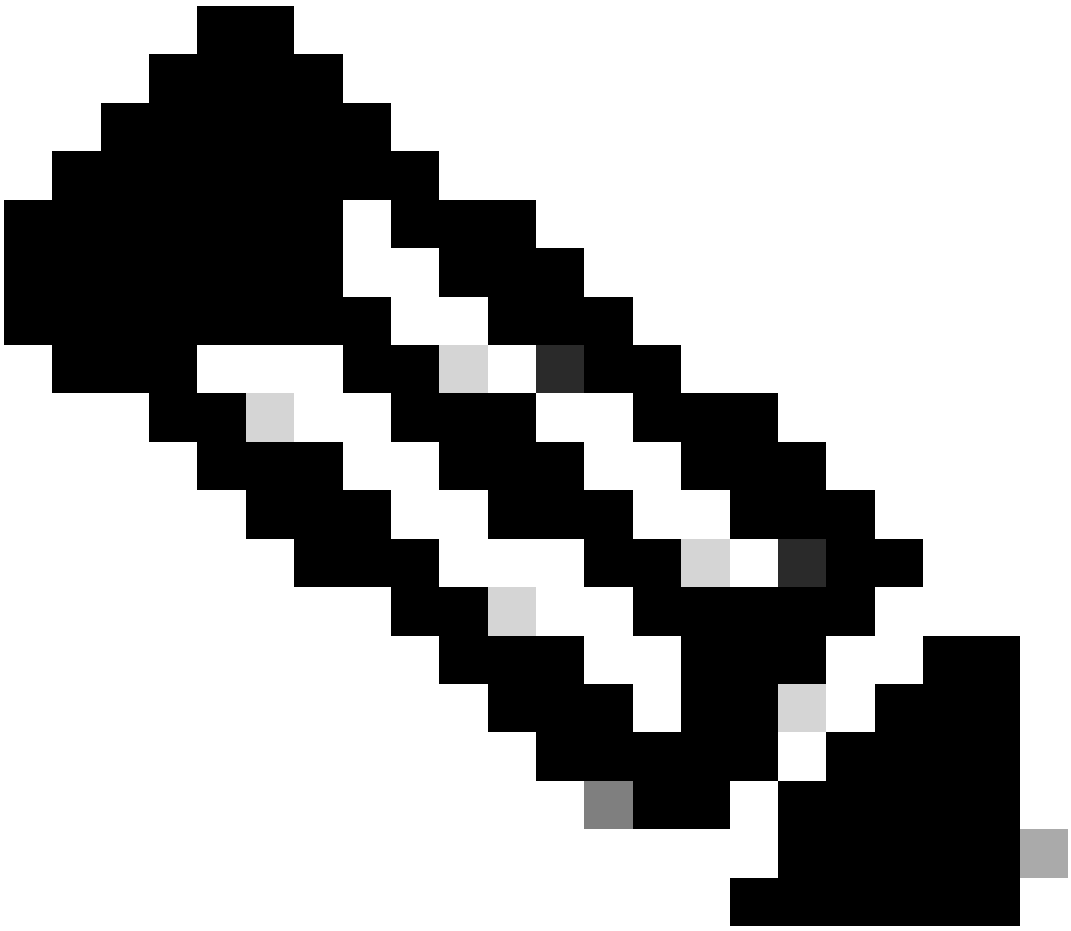
Etapa 3.

Clique em New registration.



Etapa 4.

Digite um nome para identificar o novo Aplicativo.



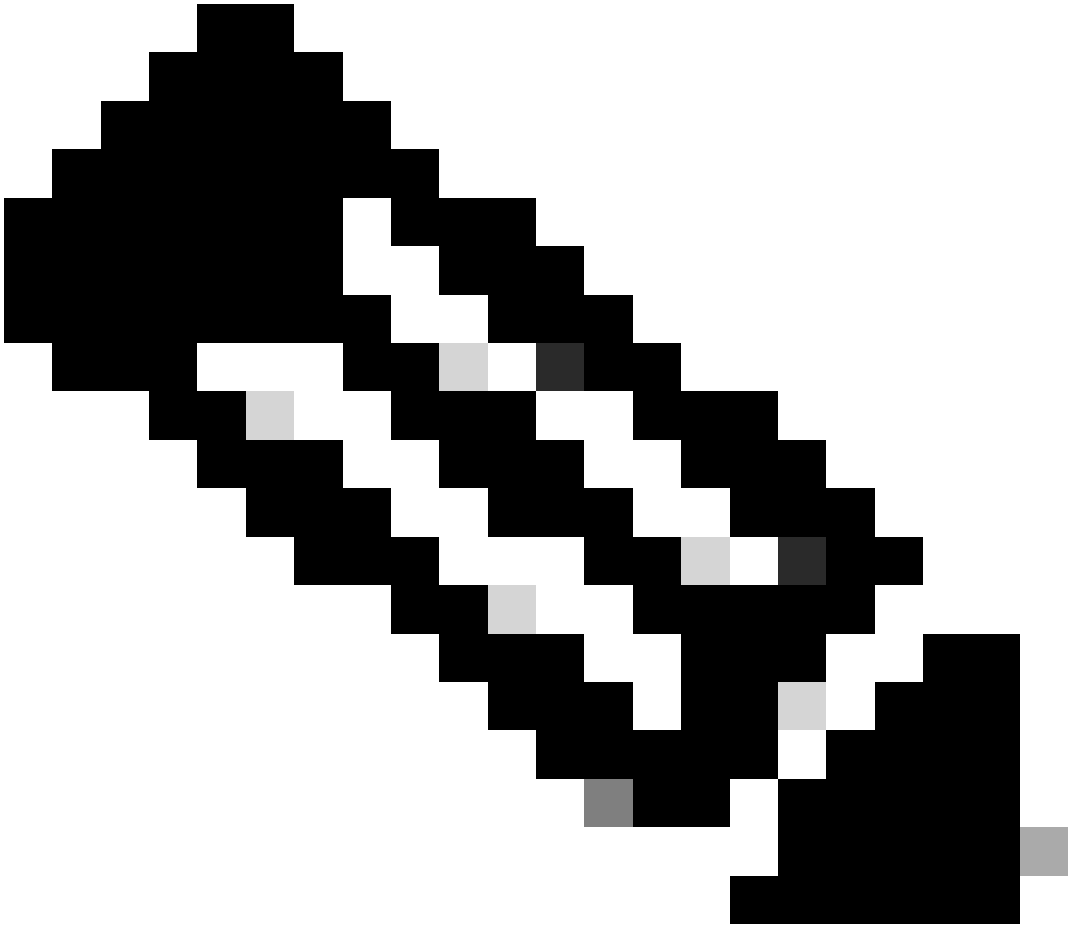
Observação: uma marca de seleção verde será exibida se o nome for válido.

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 ([redacted]: 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.

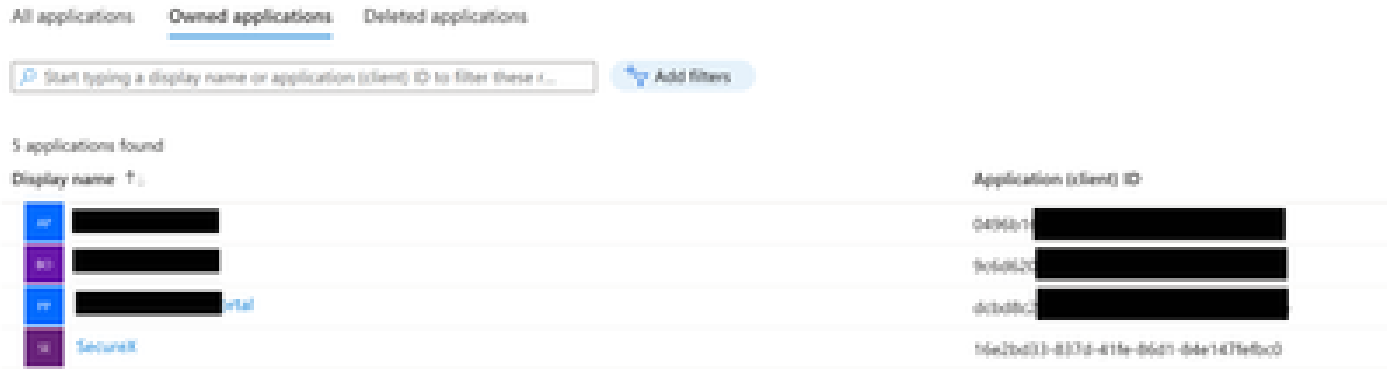
Etapa 5.

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



Passo 7.

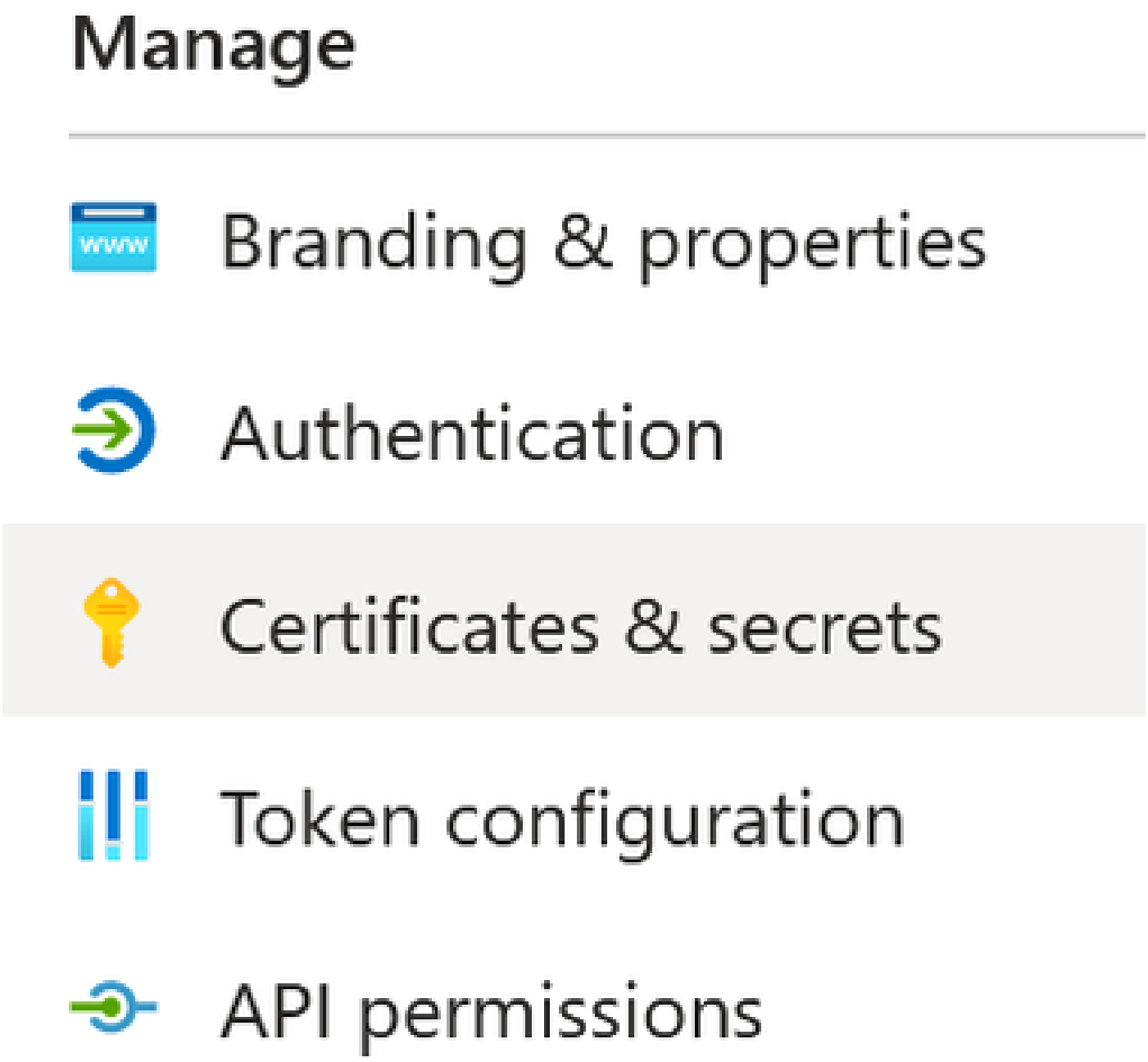
Um resumo do seu aplicativo é exibido. Identifique estes detalhes relevantes:

ID do aplicativo (cliente):

ID do diretório (espaço):

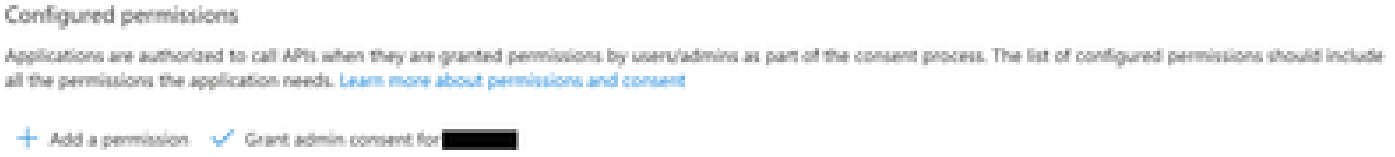
Etapa 8.

Navegue até Manage Menu > API Permissions.



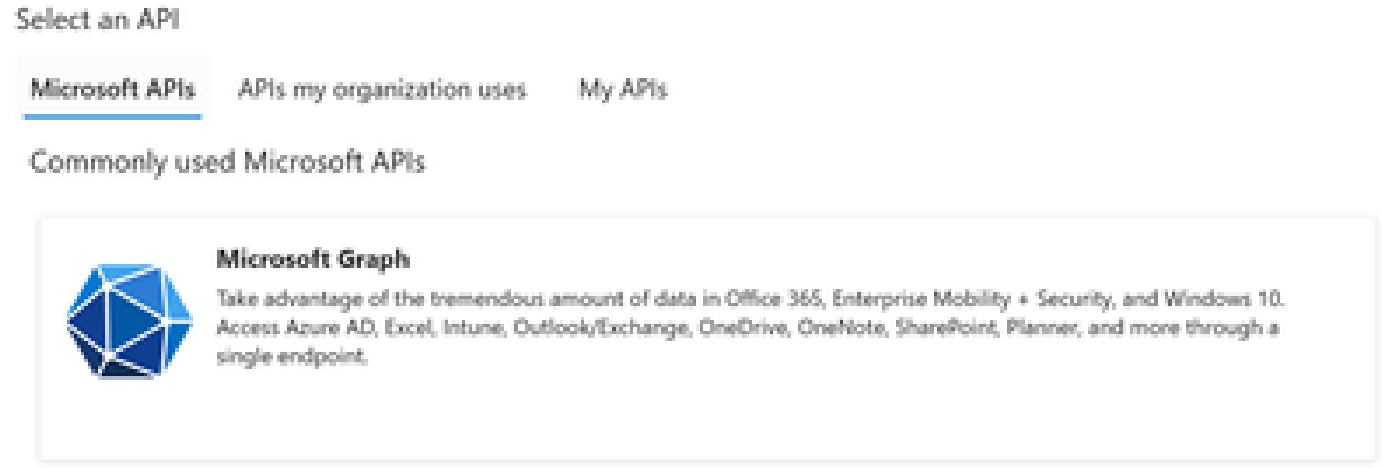
Etapa 9.

Em Permissões configuradas, clique em Add a Permission.



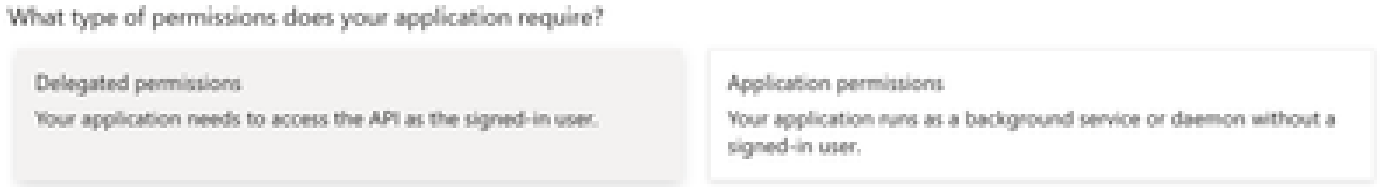
Etapa 10.

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



Etapa 11.

Selecione Application permissions.



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

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

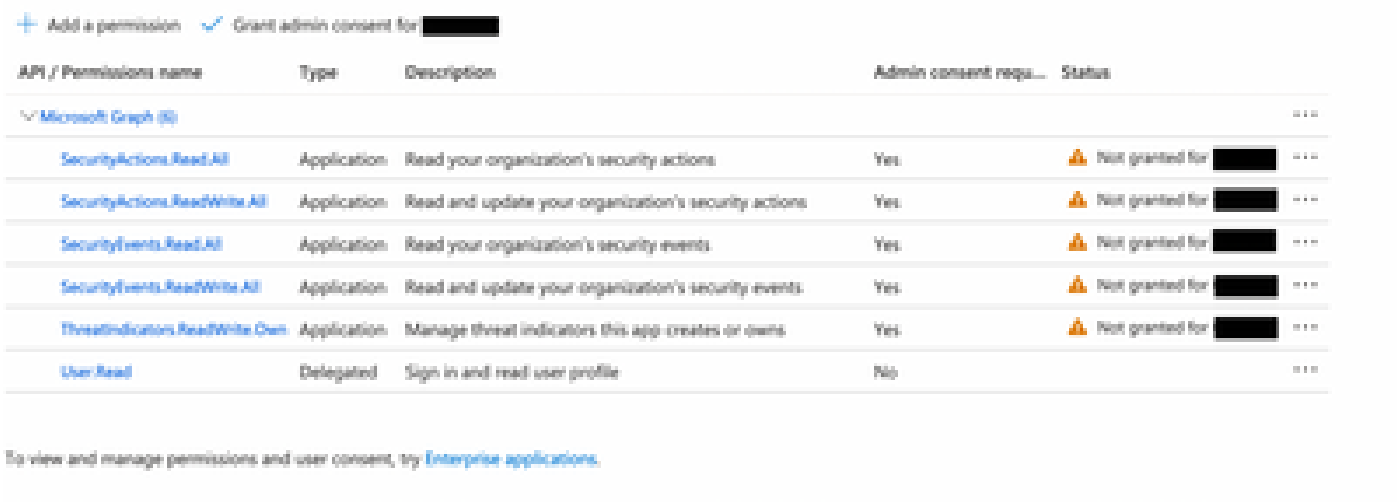
- **Eventos de segurança** e selecione
  - **Ler.Tudo**
  - **LeituraGravação.Tudo**

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

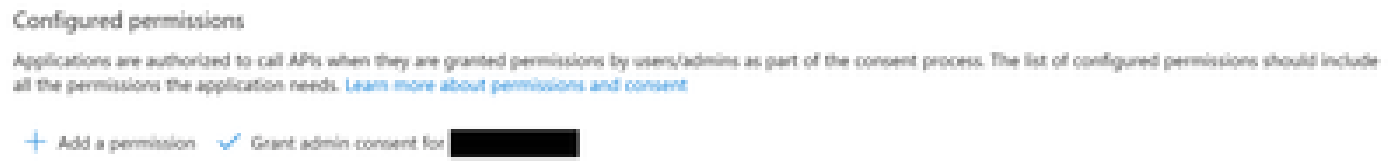
Clique em Add permissions.

Etapa 12.

Revisar as permissões selecionadas.

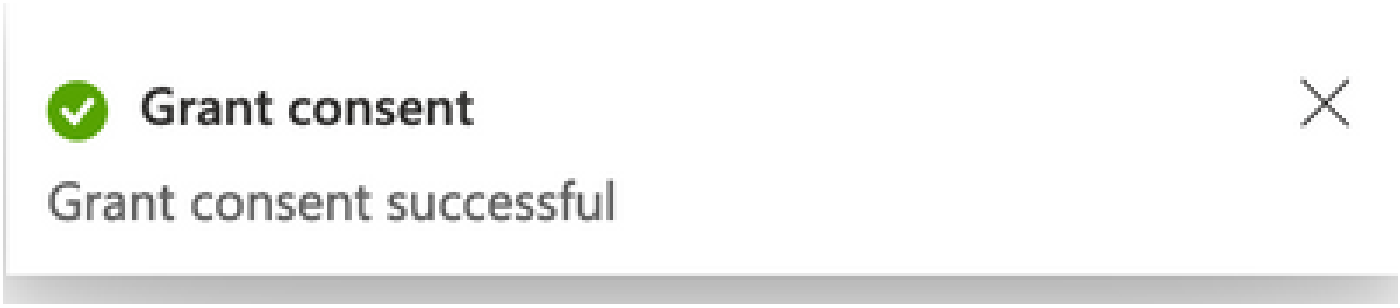


Clique em **Grant Admin consent** para sua organização.



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:



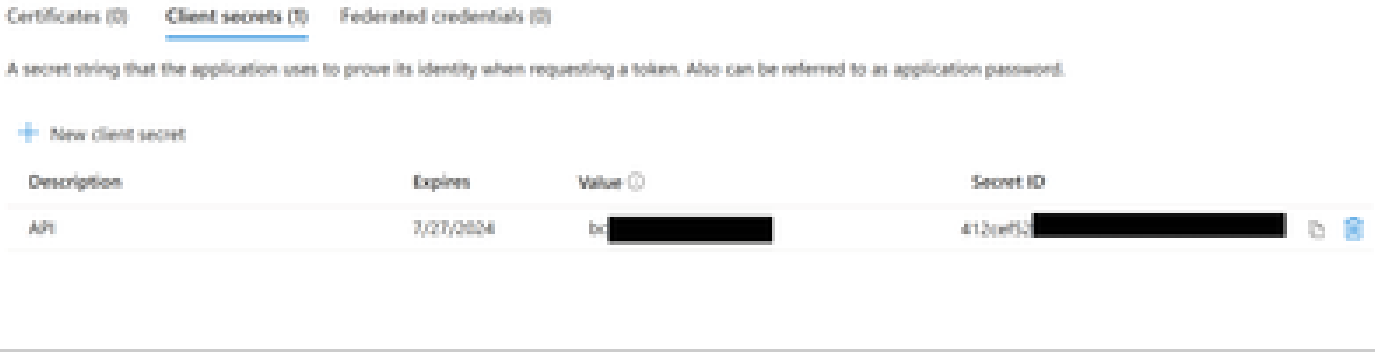
Etapa 13.

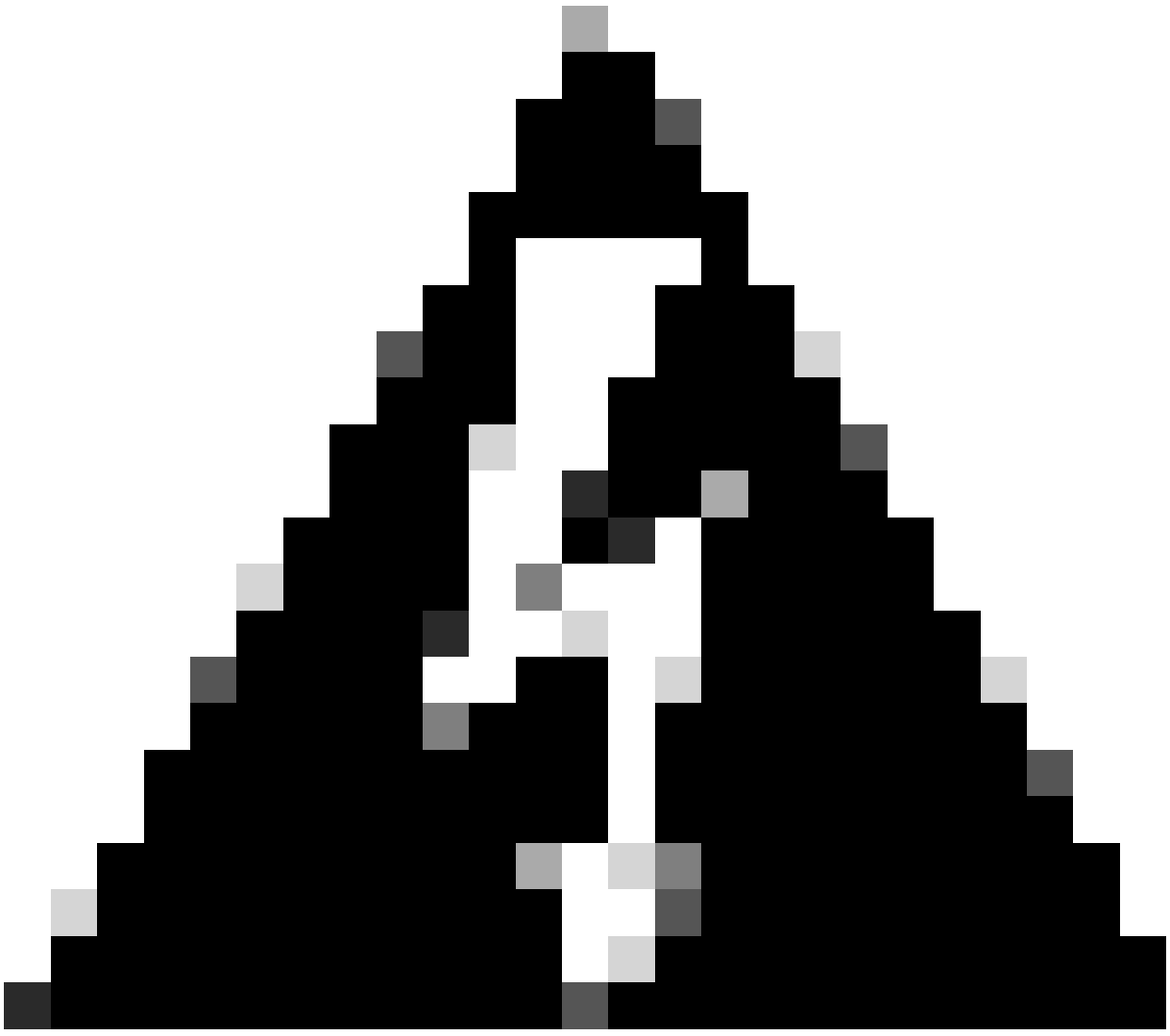
Navegue até Manage > Certificates & Secrets.

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.





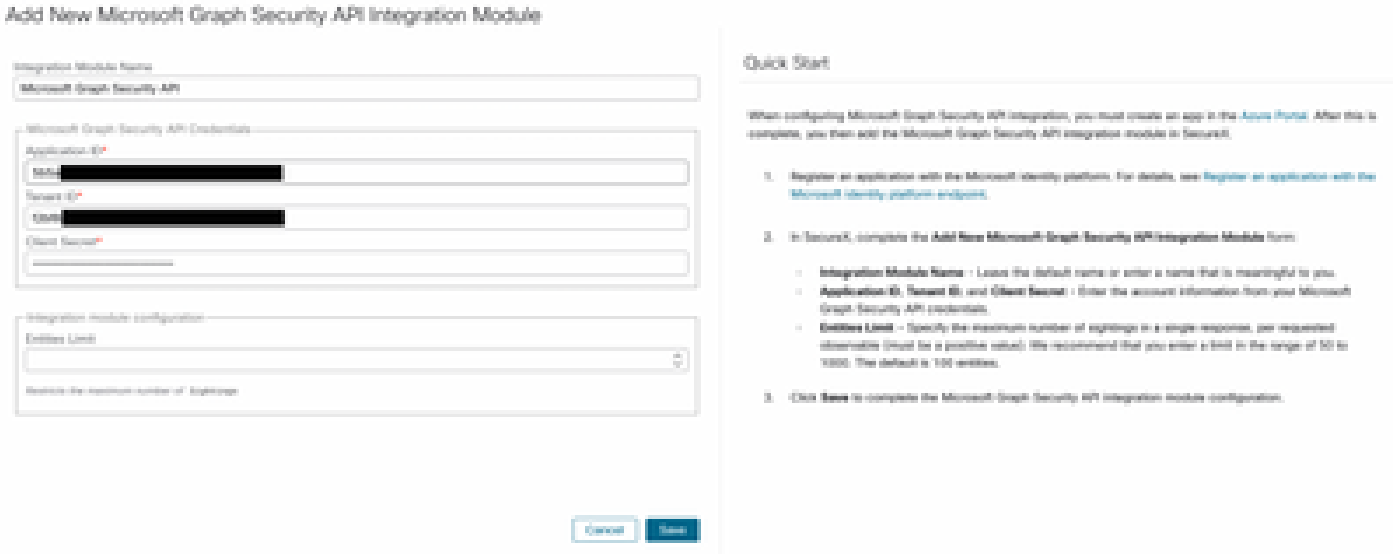
Aviso: este campo não pode ser recuperado e você deve criar um Novo Segredo.

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

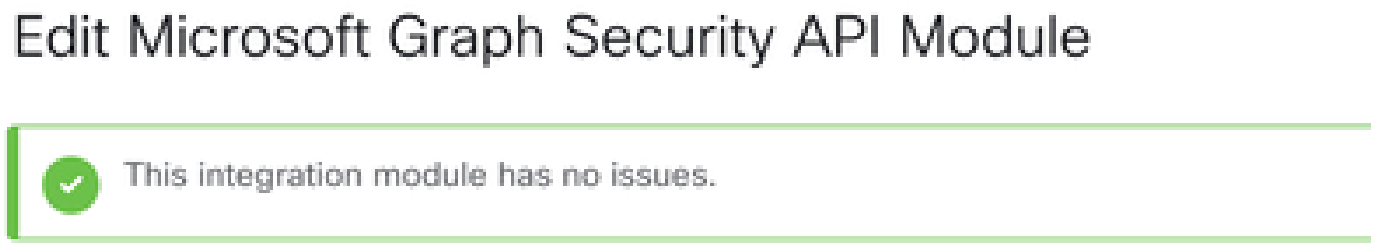
Etapa 14.

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

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



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



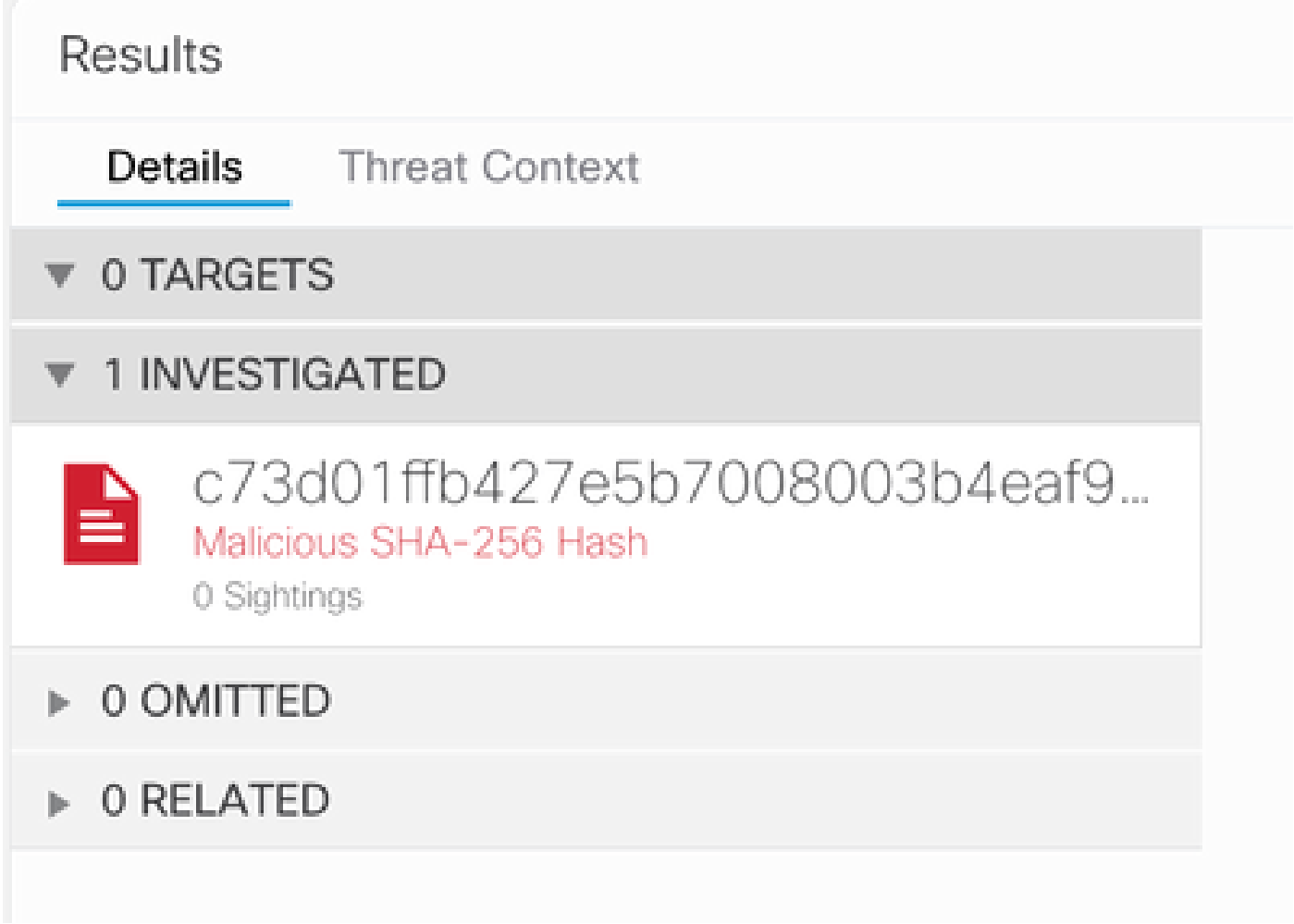
Executar investigações

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.



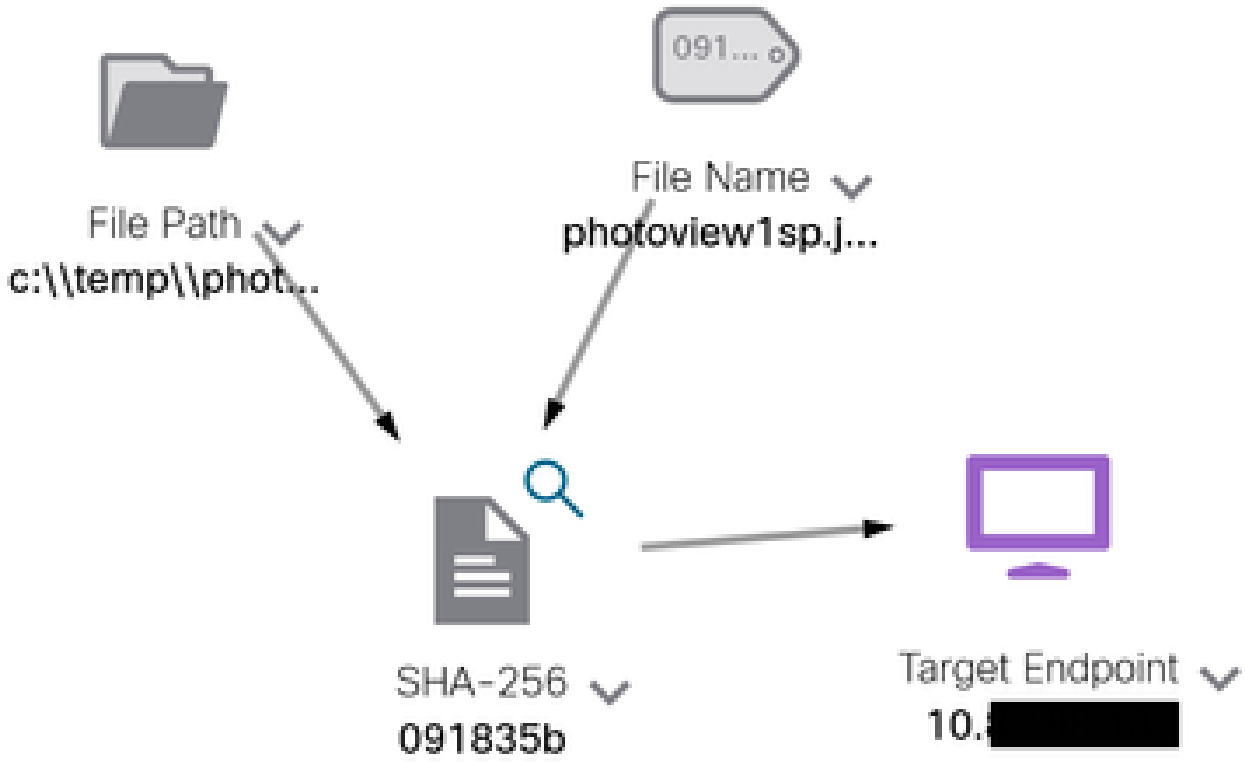
Como você pode ver, ele tem 0 pontos turísticos no ambiente de laboratório, então como testar se a API do Graph funciona?

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

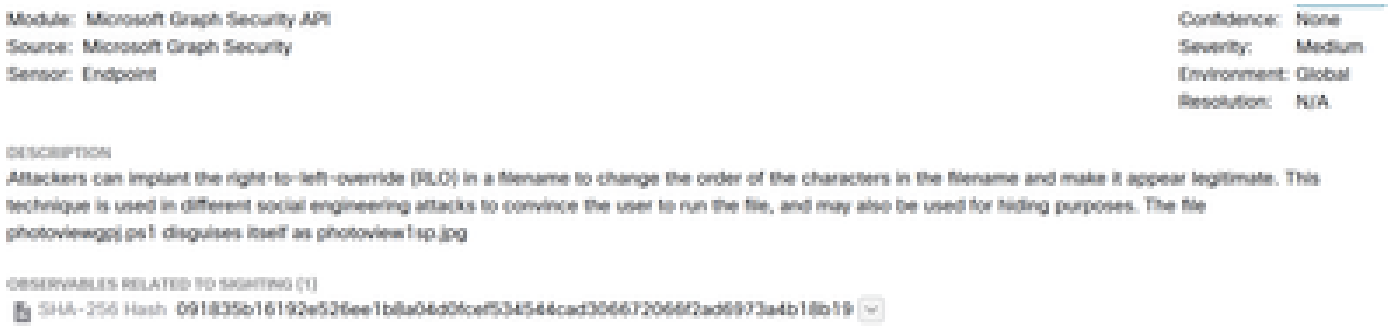
Verificar

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:



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.