配置Microsoft Graph API与Cisco XDR的集成

目录

简介

本文档介绍将Microsoft Graph API与Cisco XDR集成的过程以及可查询的数据类型。

先决条件

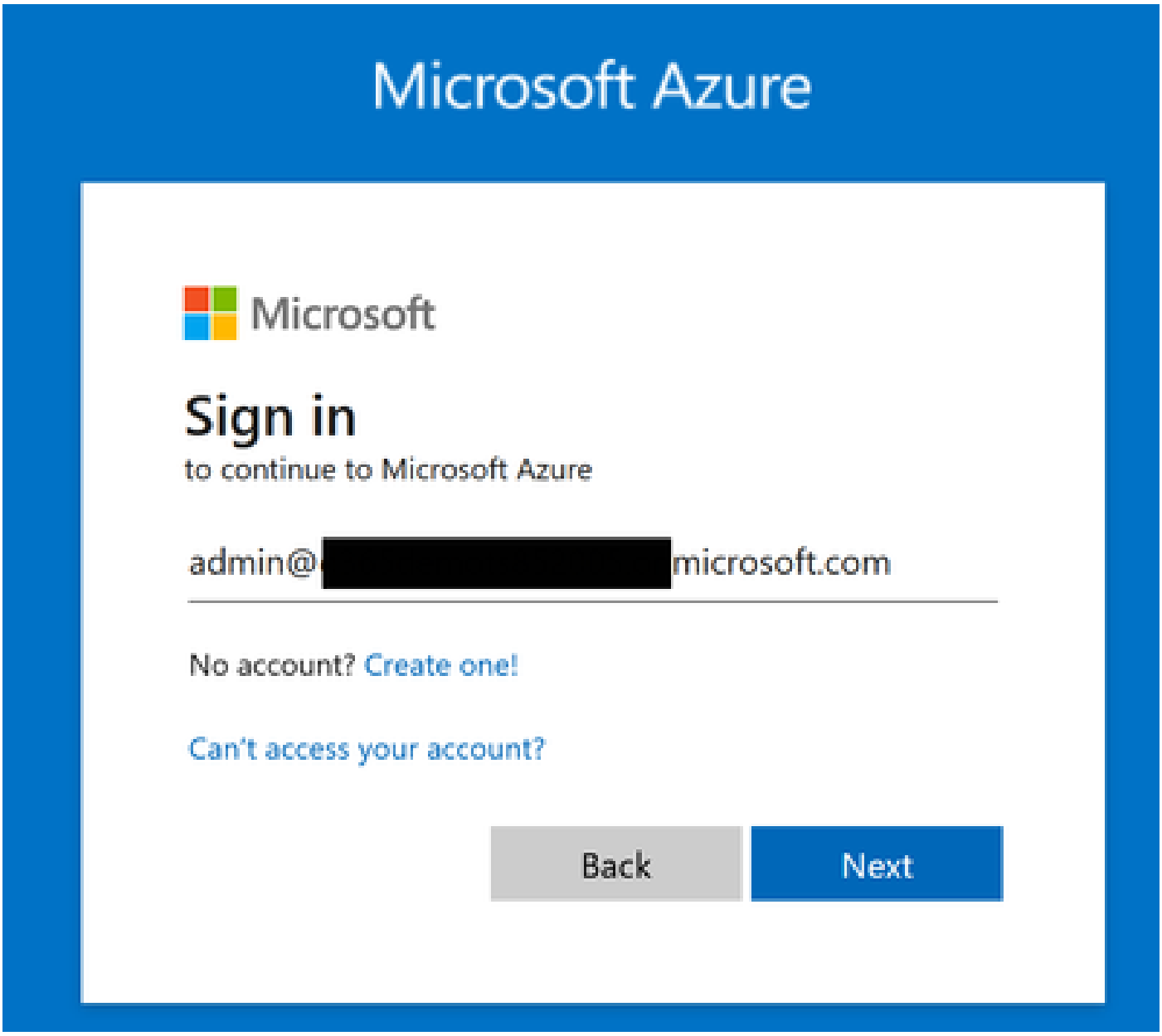
- Cisco XDR管理员帐户
- Microsoft Azure系统管理员帐户
- 访问Cisco XDR

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

集成步骤

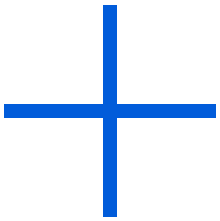
步骤1:

以系统管理员身份登录Microsoft Azure。

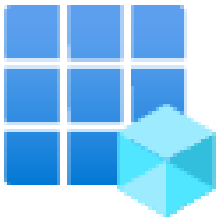


第二步：

点击Azure服务门户**App Registrations** 上的。



Create a resource



App registrations

第三步：

单击。New registration

Home >

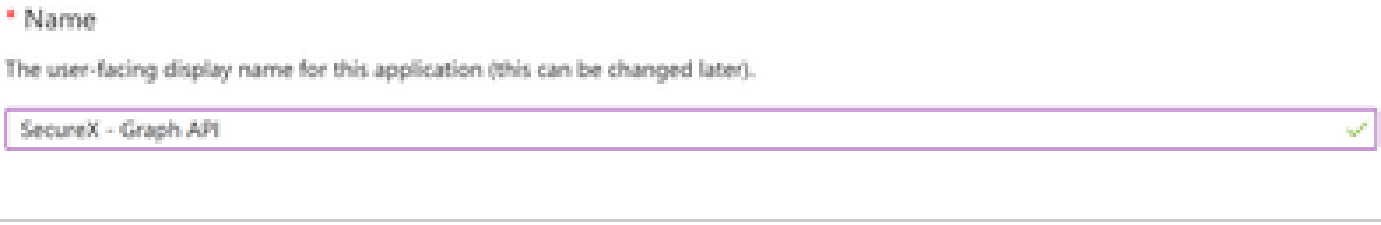
App registrations

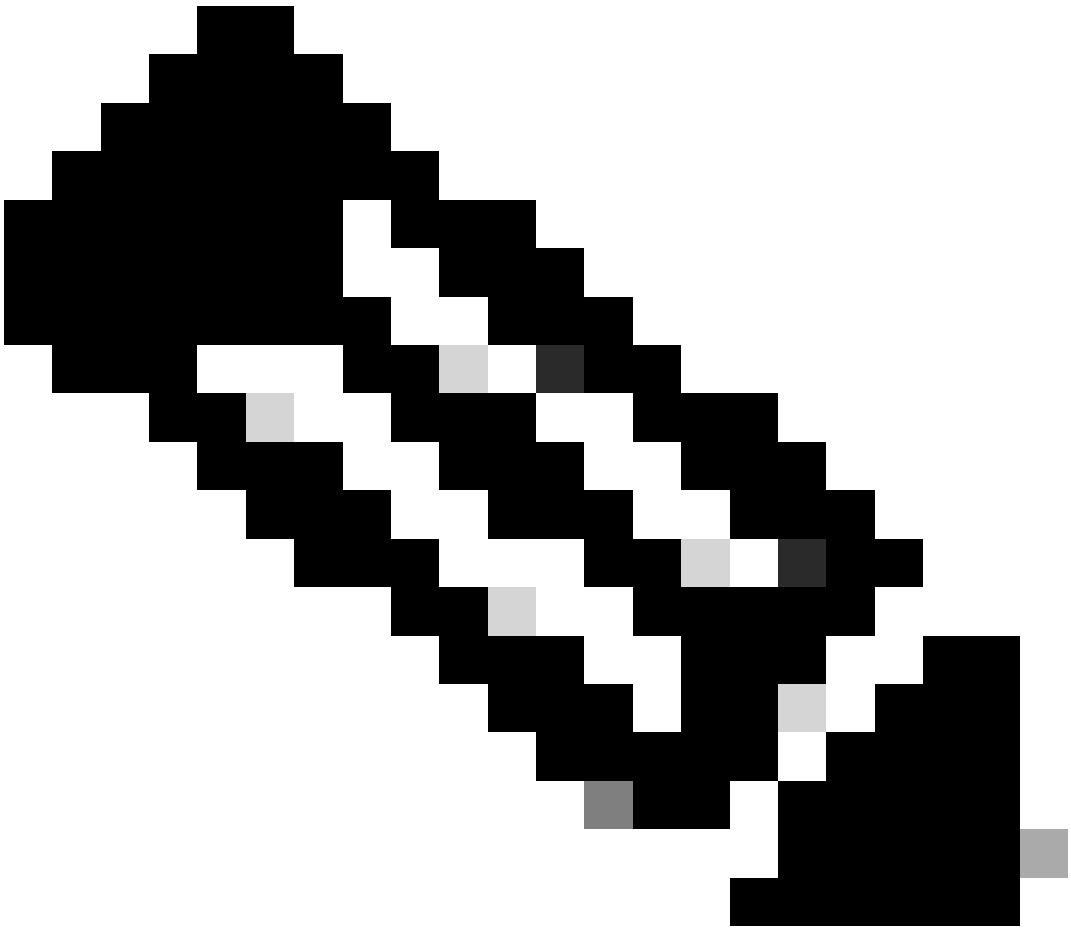
New registration

Endp

第四步：

键入名称以标识新应用。





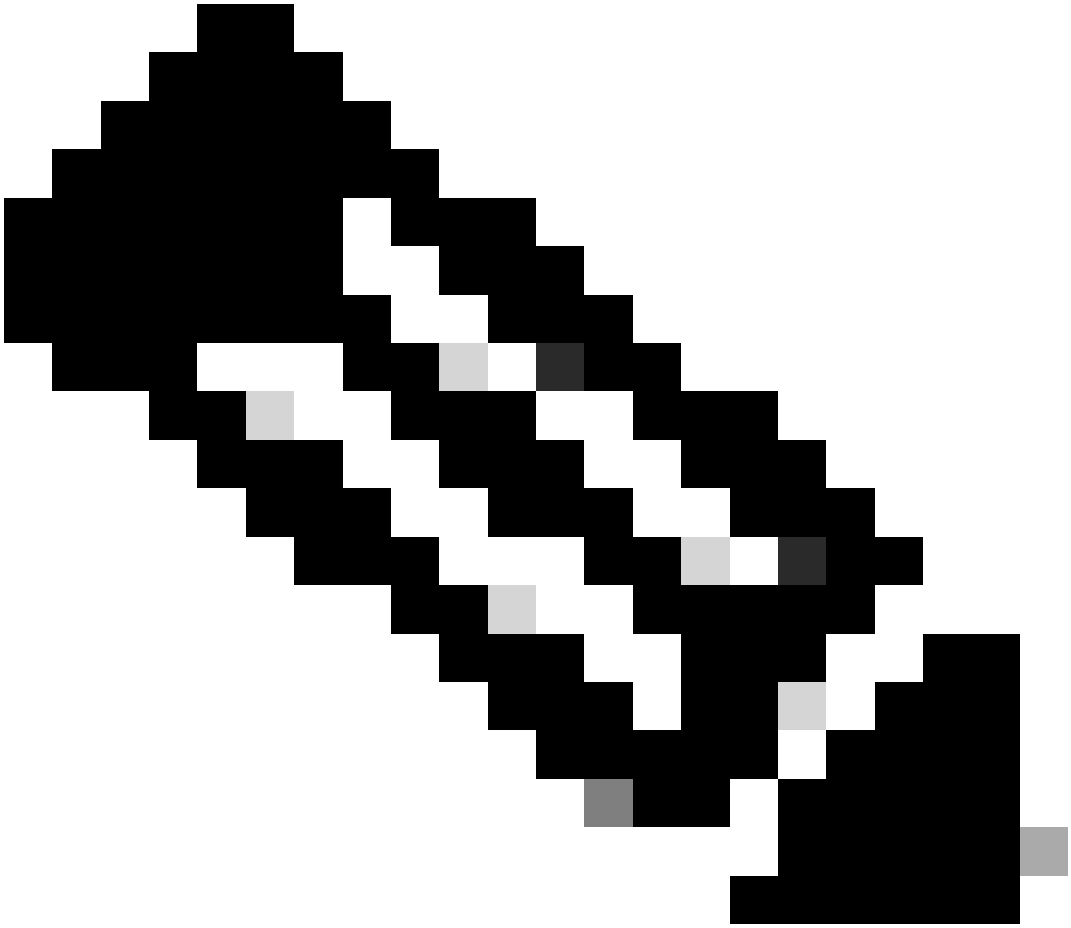
注意：如果名称有效，则会显示绿色的复选标记。

在支持的帐户类型上，选择选项 **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



注意：您不需要键入重定向URI。

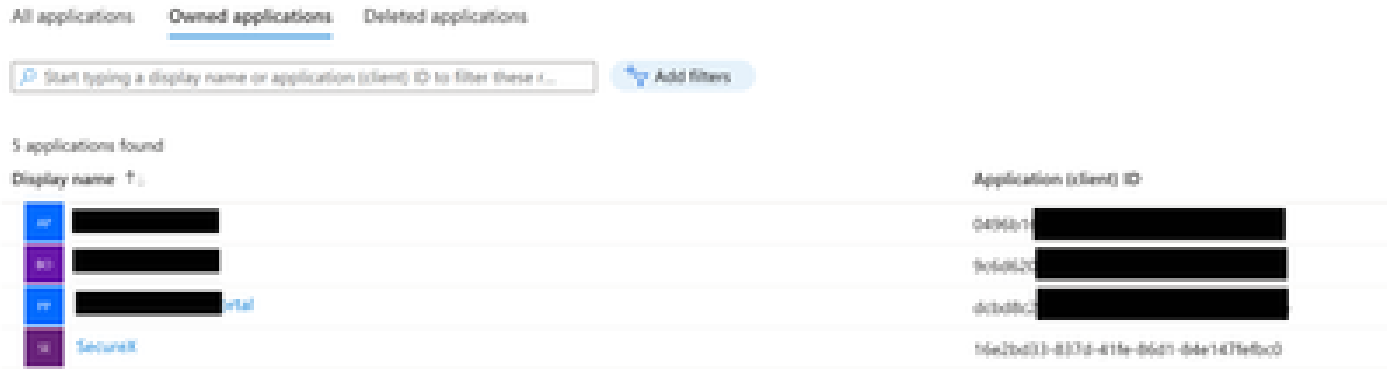
第五步：

滚动到屏幕底部并单击 **Register**。

第六步：

导航回Azure服务页面，点击App Registrations > Owned Applications。

识别您的应用并点击名称。在本例中为SecureX。



步骤 7.

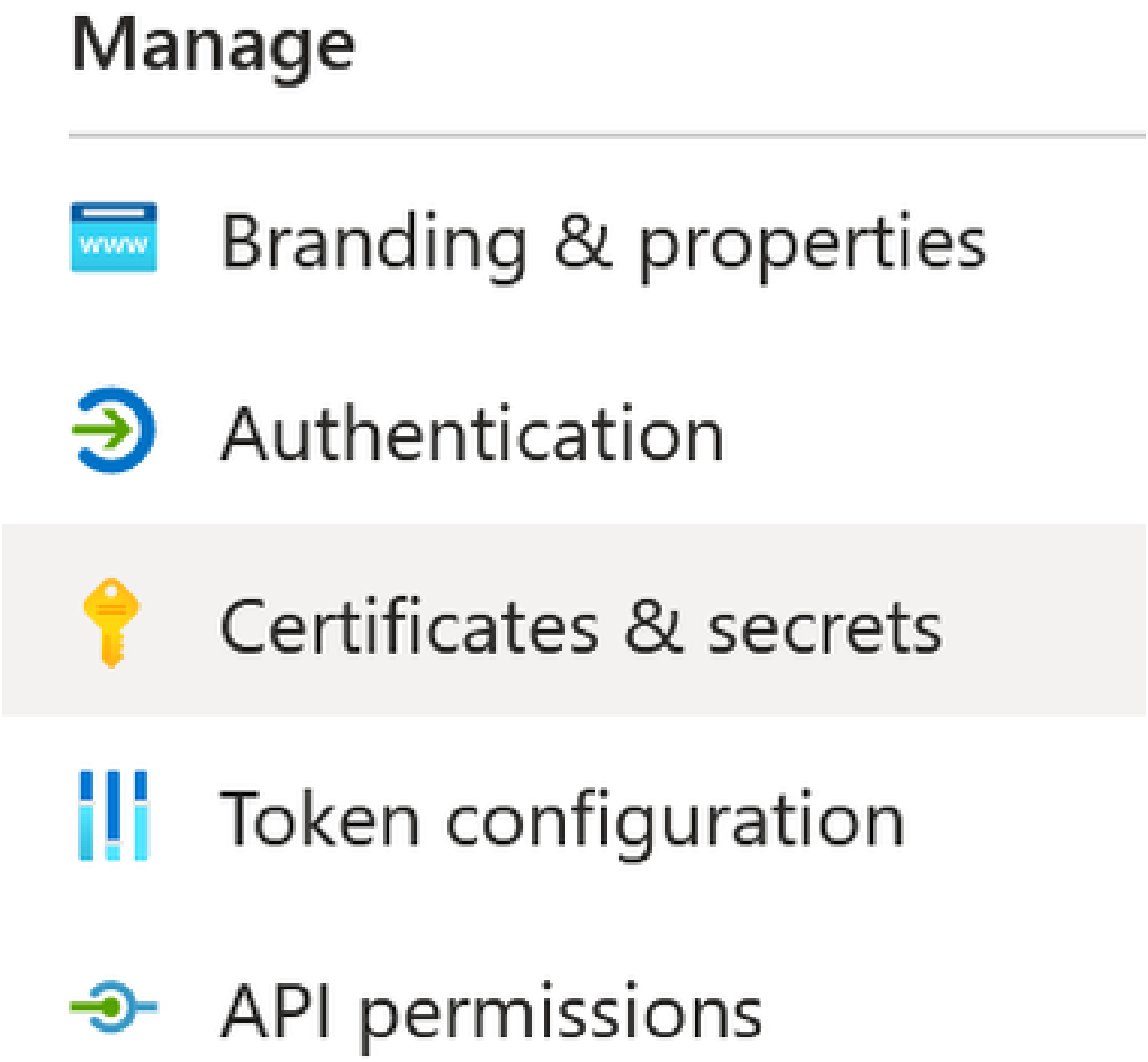
系统将显示您的应用的摘要。请确定以下相关详细信息：

应用程序（客户端）ID：

目录（租户）ID：

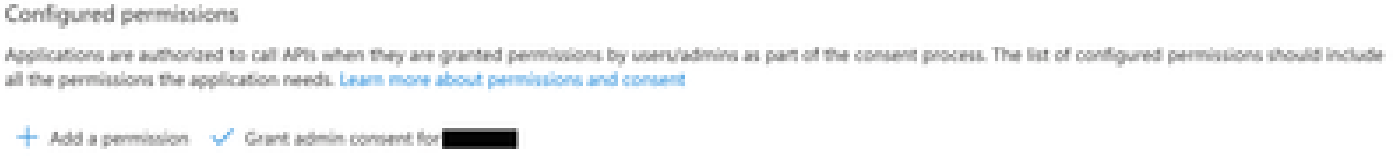
步骤 8

导航到Manage Menu > API Permissions。



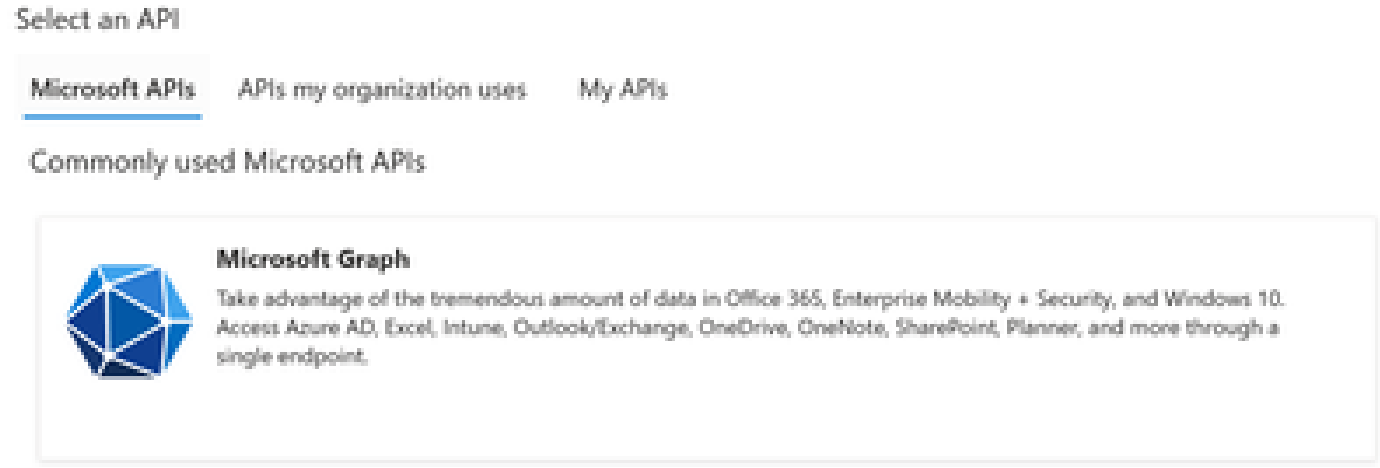
步骤 9

在“配置的权限”下，单击Add a Permission。



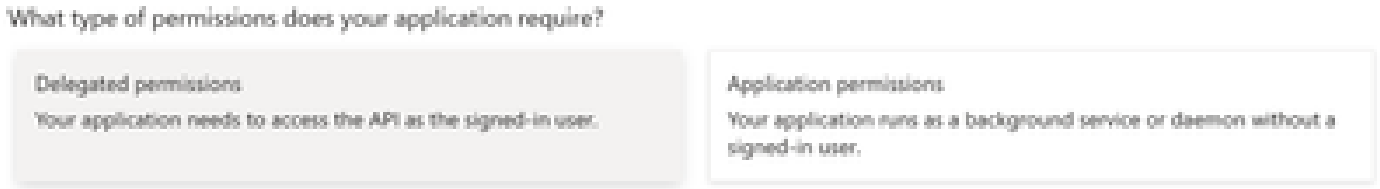
步骤 10

在“请求API权限”部分，单击 **Microsoft Graph**。



步骤 11

选择.Application permissions



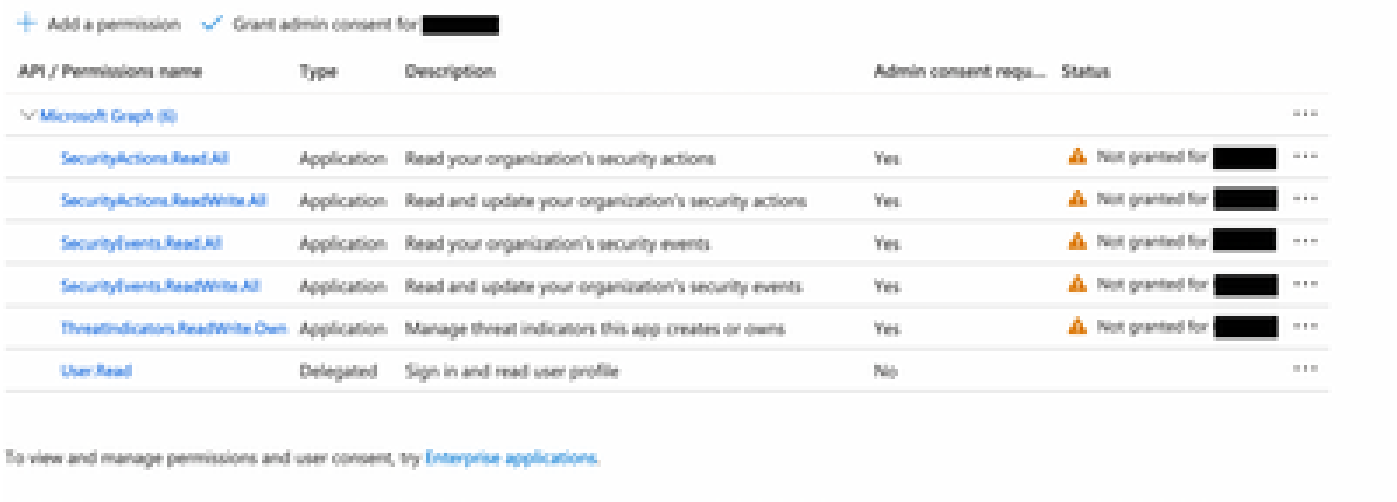
在搜索栏中，查找Security。展开 **Security Actions** 并选择

- **Read.All**
- **全部读**
- **安全事件**并选择
  - **Read.All**
  - **全部读**
- **威胁指示器**并选择
  - **ThreatIndicators.ReadWrite.OwnedBy**

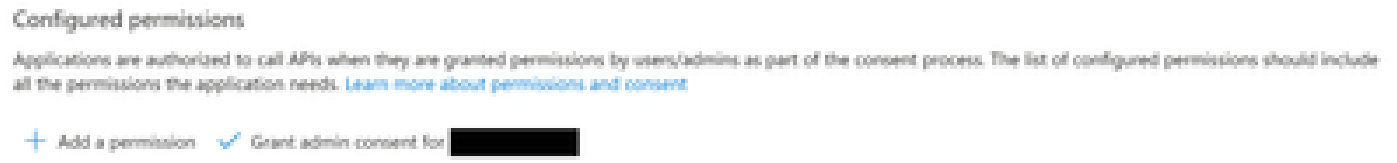
单击。Add permissions

步骤 12

检查您选择的权限。

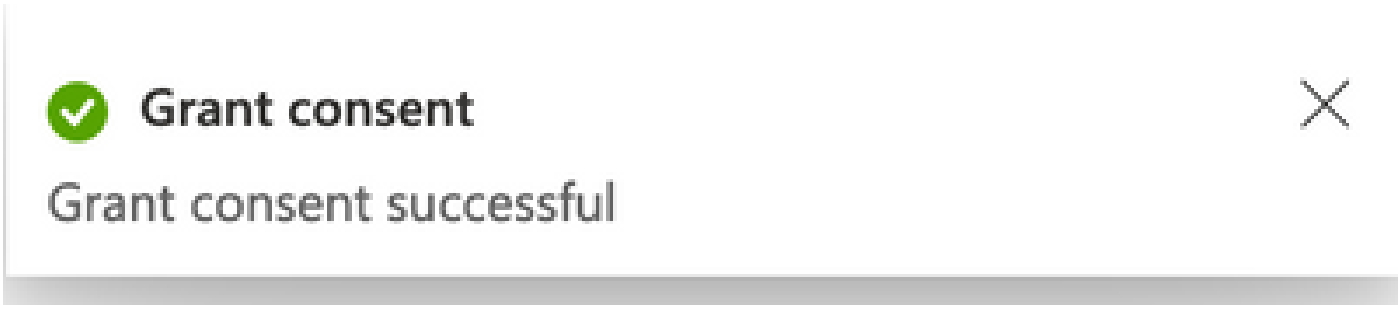


为您的组织点击 **Grant Admin consent** 。



系统将显示一个提示，提示您选择是否要同意所有权限。单击。Yes

此时将显示类似弹出窗口，如下图所示：



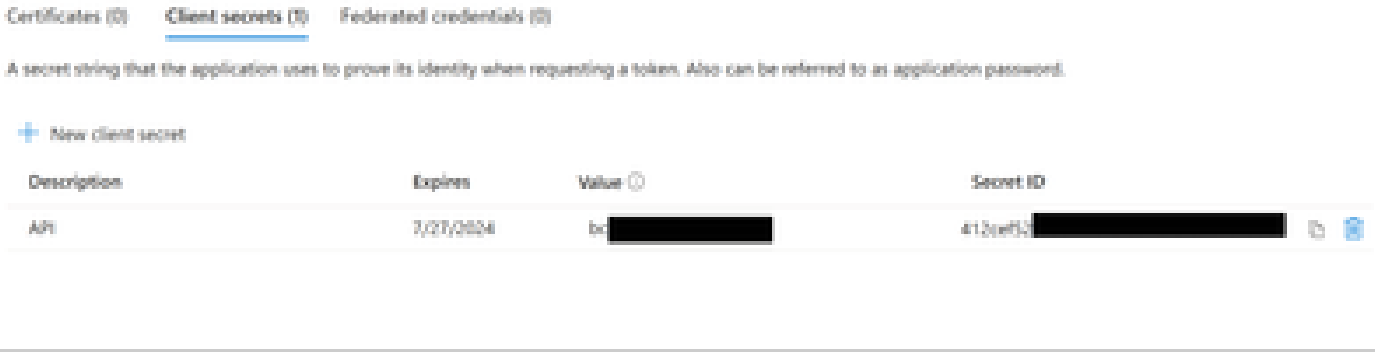
步骤 13

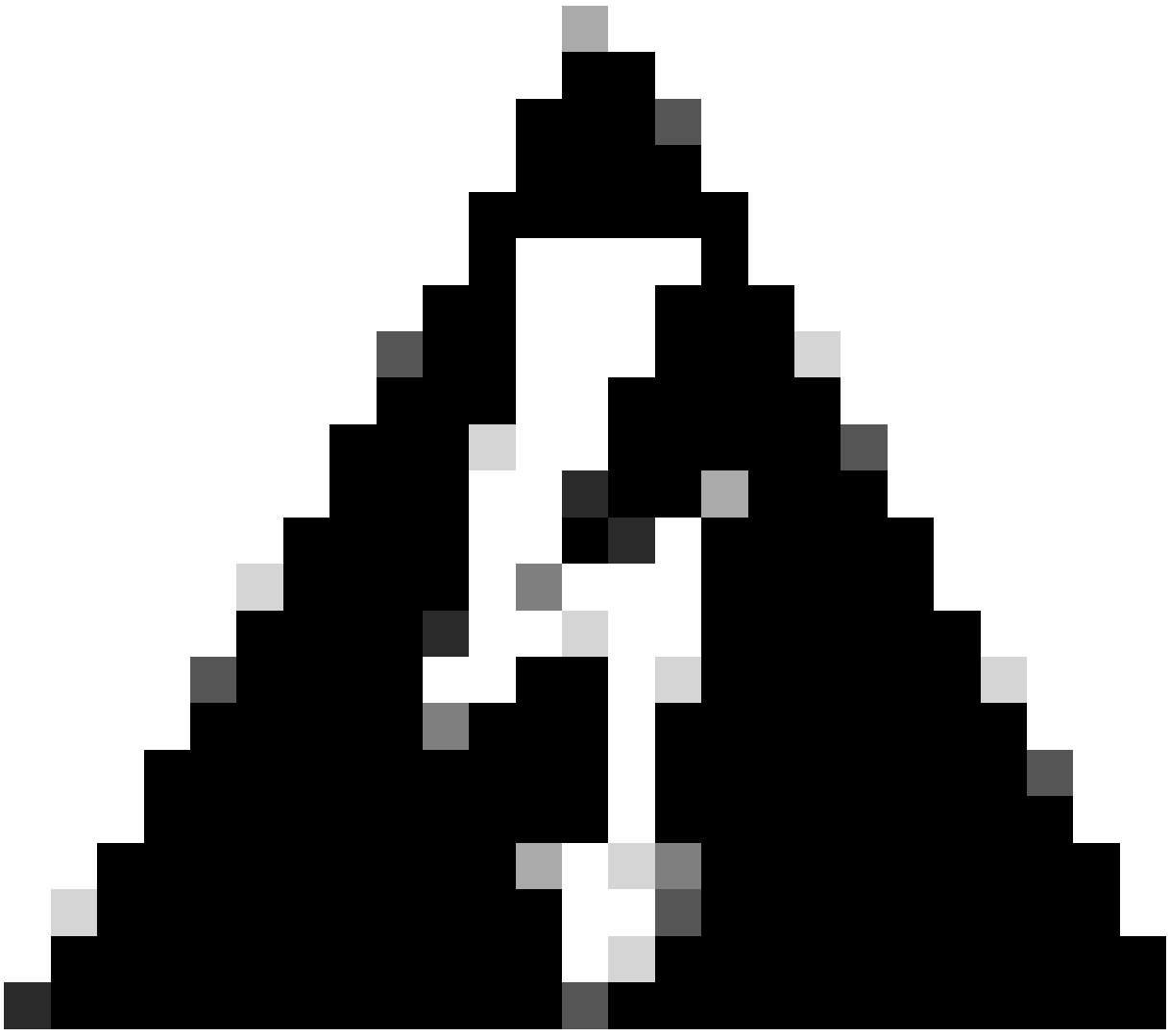
导航到Manage > Certificates & Secrets。

单击。Add New Client Secret

写下简要描述并选择有效的日期Expires。建议选择6个月以上的有效日期，以防止API密钥过期。

创建后，在用于集成的情况下，将 **Value**部分复制并存储在安全位置。





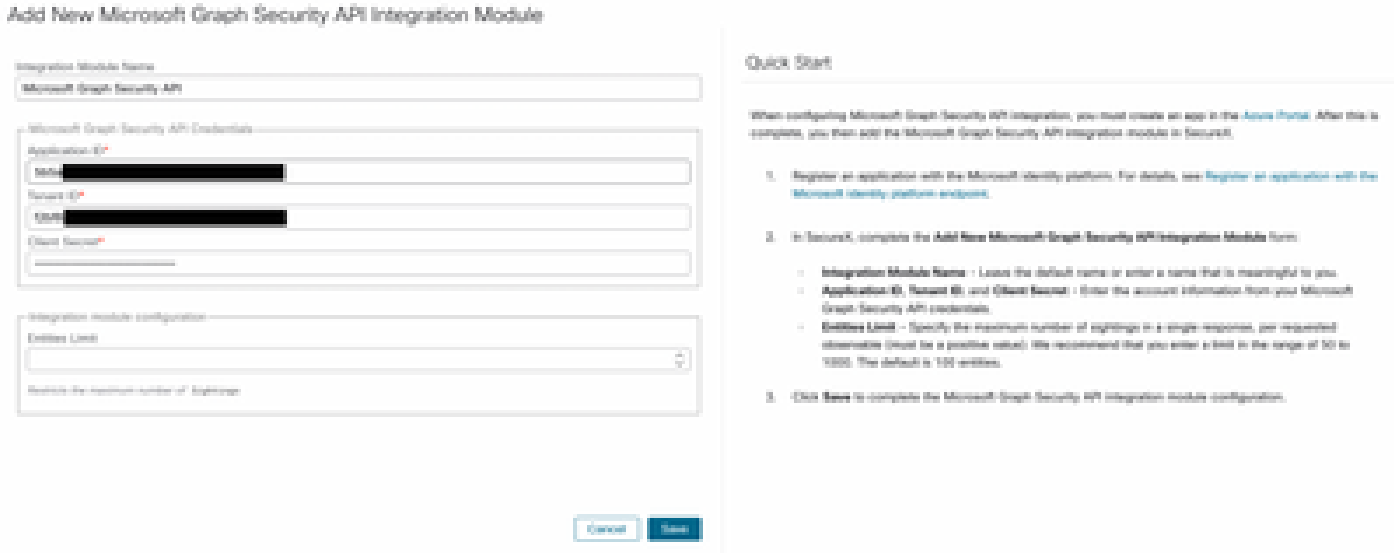
警告：此字段无法恢复，您必须创建新密钥。

获取所有信息后，导航回 **Overview** 并复制应用的值。然后导航到SecureX。

步骤 14

导航至Integration Modules > Available Integration Modules > 选择Microsoft Security Graph API，点击Add。

分配名称并粘贴从Azure门户获得的值。



单击Save，然后等待运行状况检查成功。

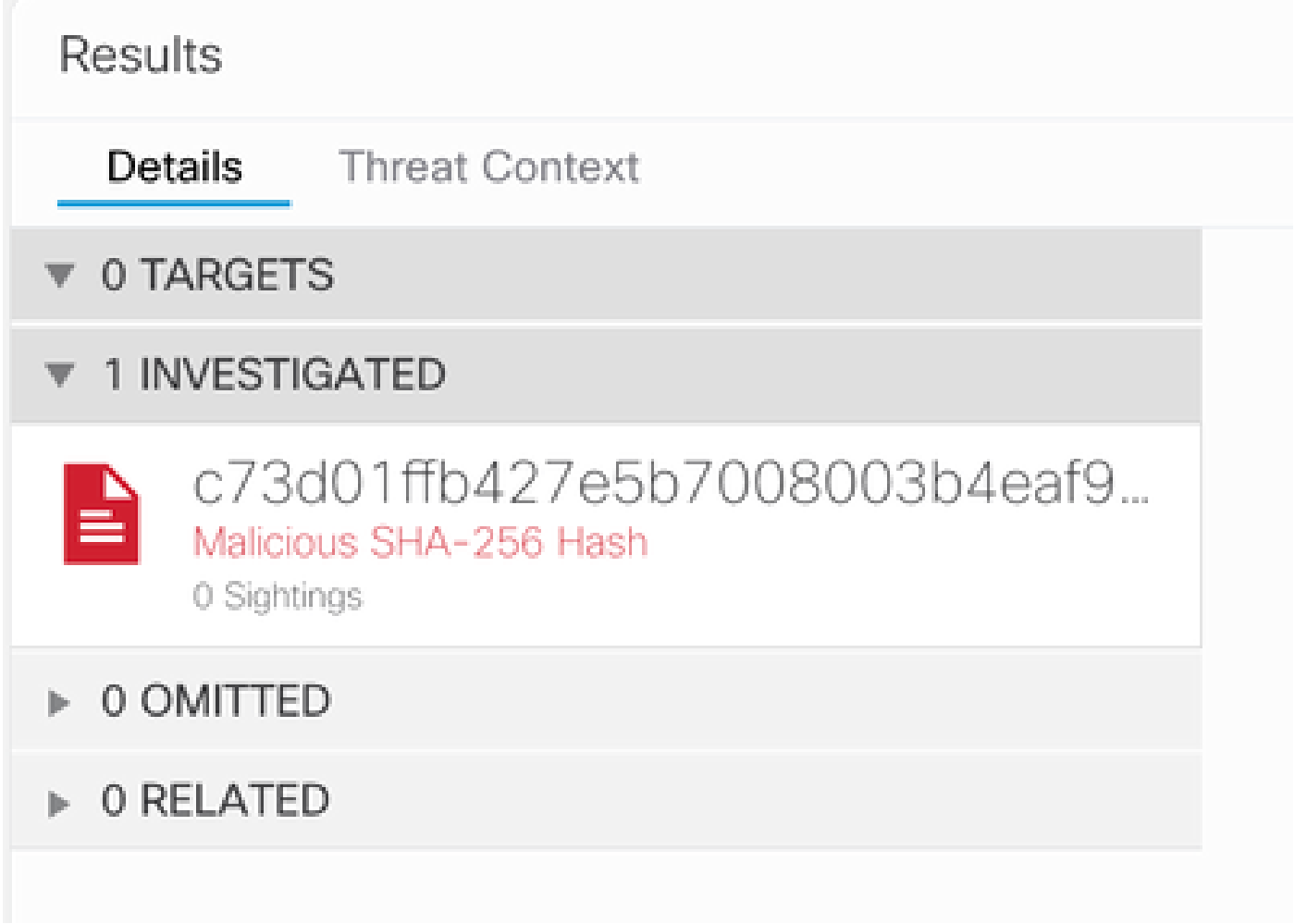
执行调查

到目前为止，Microsoft安全图API未使用磁贴填充Cisco XDR控制面板。相反，可以使用调查来查询Azure门户中的信息。

请记住，Graph API只能查询以下内容：

- ip
- 域
- 主机名
- url
- file_name
- file_path
- sha256

在本示例中，调查使用此SHA c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148。



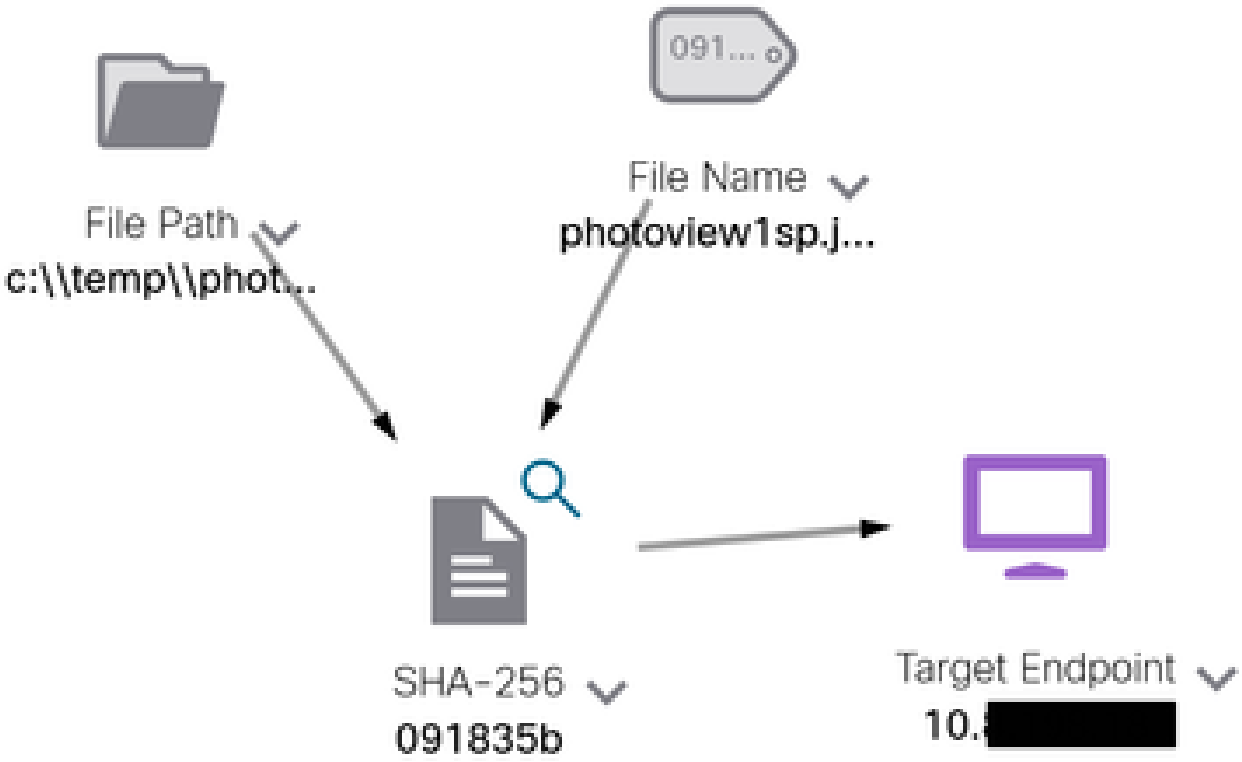
如您所见，它在实验室环境中有0次发现，那么如何测试Graph API是否有效？

打开WebDeveloper工具，运行调查，然后向**visibility.amp.cisco.com**查找帖子事件，并找到名为Observables的文件。

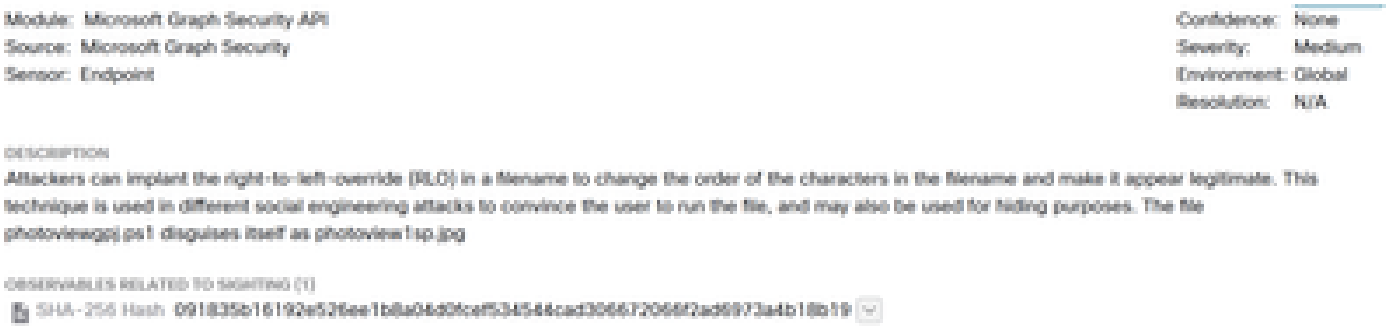
验证

您可以使用此链接：Microsoft图形安全快照获取快照列表，以帮助您了解可从每种可观察类型获得的响应。

您可以看到如下图所示的示例：



展开此窗口，您可以看到集成提供的信息：



请记住，数据必须存在于Azure门户中，Graph API在与其他Microsoft解决方案配合使用时效果更好。但是，这必须由Microsoft支持部门进行验证。

故障排除

- 授权失败消息：
    - 确保 **Tenant ID** 和Client ID的值正确并且仍然有效。

- 调查中未显示任何数据：
    - 确保复制并粘贴了 **Tenant ID** 和 **Client ID**的适当值。
        - 确保您使用了Certificates & Secrets部分 **Value** 的字段信息。
        - 使用WebDeveloper工具确定调查发生时是否查询图形API。
        - 当图形API合并来自各种Microsoft警报提供者的数据时，请确保查询过滤器支持OData。（例如，Office 365安全与合规性和Microsoft Defender ATP）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。