

Configurer l'intégration de l'API Microsoft Graph avec Cisco XDR

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Étapes d'intégration](#)

[Effectuer des investigations](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit la procédure d'intégration de l'API Microsoft Graph avec Cisco XDR, et le type de données pouvant être interrogées.

Conditions préalables

- Compte d'administrateur Cisco XDR
- Compte d'administrateur système Microsoft Azure
- Accès à Cisco XDR

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Étapes d'intégration

Étape 1.

Connectez-vous à Microsoft Azure en tant qu'administrateur système.

Microsoft Azure



Sign in

to continue to Microsoft Azure

admin@[REDACTED]microsoft.com

No account? [Create one!](#)

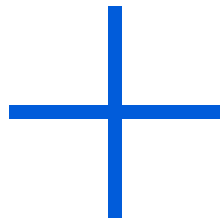
[Can't access your account?](#)

Back

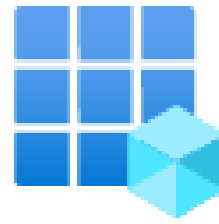
Next

Étape 2.

Cliquez **App Registrations** sur le portail des services Azure.



Create a
resource



App
registrations

Étape 3.

Cliquez sur New registration.

Home >

App registrations

+ New registration  Endp

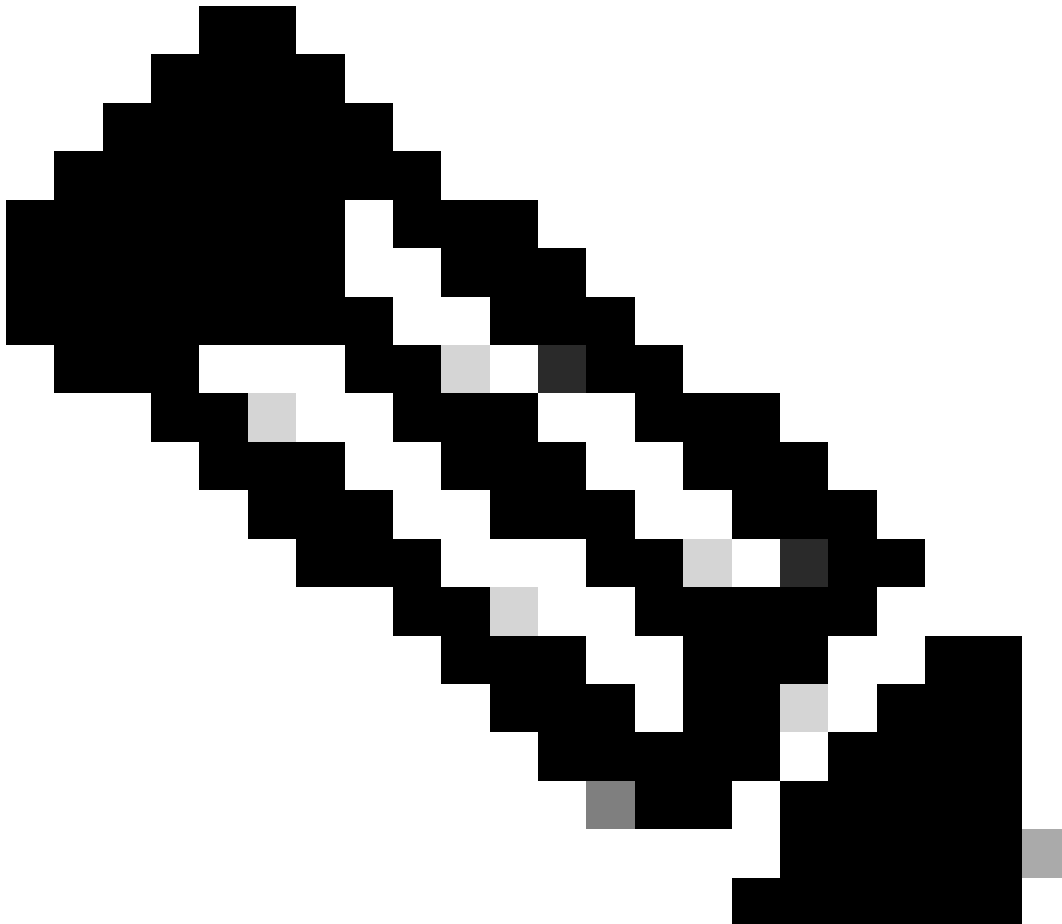
Étape 4.

Tapez un nom pour identifier votre nouvelle application.

▪ Name

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

SecureX - Graph API



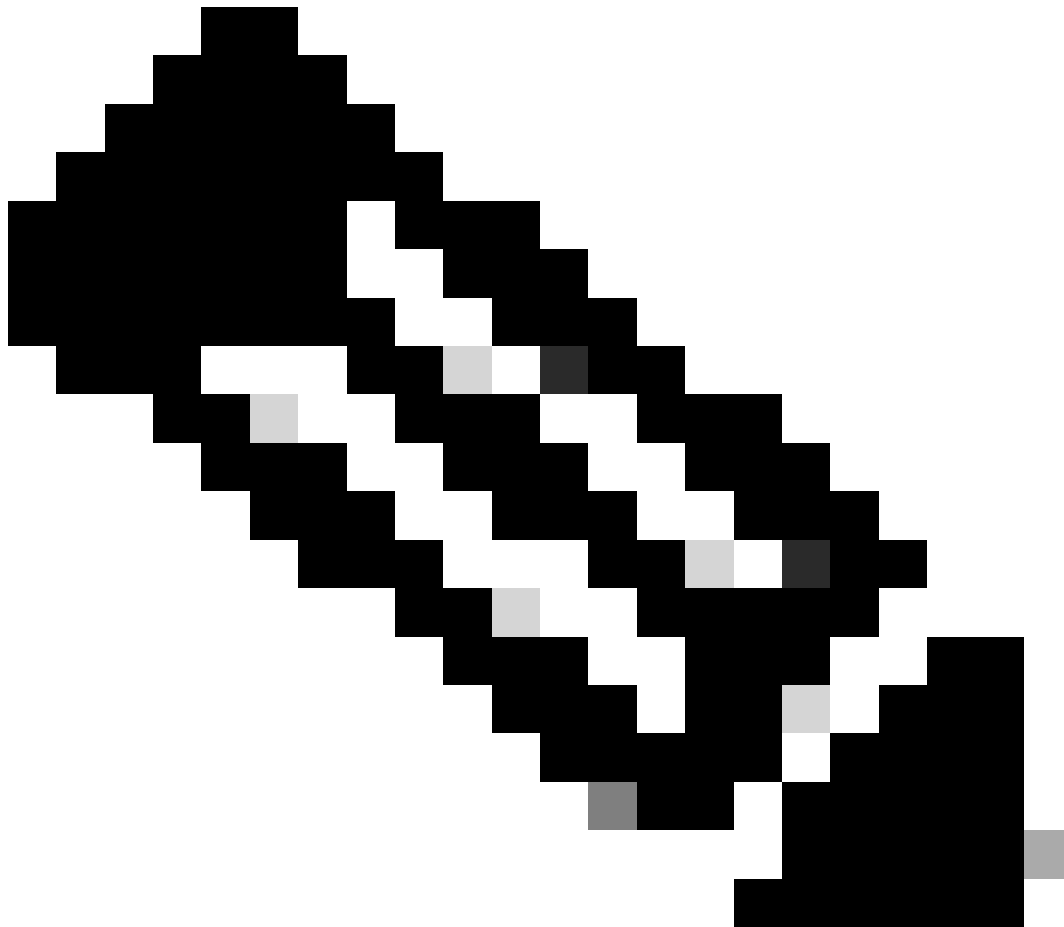
Remarque : une coche verte apparaît si le nom est valide.

Dans Types de comptes pris en charge, sélectionnez l'option **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
-



Remarque : il n'est pas nécessaire de taper un URI de redirection.

Faites défiler l'écran jusqu'en bas et cliquez sur **Register**.

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

Register

Étape 6.





Revenez à la page des services Azure, cliquez sur App Registrations > Owned Applications.

Identifiez votre application et cliquez sur son nom. Dans cet exemple, c'est 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	6c3d8b [Redacted]
 SecureX	16e2bd33-8378-419e-86d1-64e1479efc0

Étape 7.

Un résumé de votre application s'affiche. Veuillez indiquer les détails pertinents suivants :

ID de l'application (client) :

Display name : [SecureX](#)

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

ID du répertoire (locataire) :

Directory (tenant) ID : f2bf8cd3-[Redacted]

Étape 8.

Accédez à Manage Menu > API Permissions.

Manage



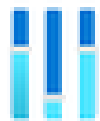
Branding & properties



Authentication



Certificates & secrets



Token configuration



API permissions

Étape 9.

Sous Autorisations configurées, cliquez sur 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 ██████████

Étape 10.

Dans la section Demander des autorisations API, cliquez sur **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.

Étape 11.

Sélectionnez 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.

Dans la barre de recherche, recherchez Security. Développez **Security Actions** et sélectionnez

- **Lire.Tout**
- **LectureÉcriture.Tout**
- **Événements de sécurité** et sélectionnez
 - **Lire.Tout**
 - **LectureÉcriture.Tout**
- **Indicateurs de menace** et sélectionnez
 - **IndicateursMenaces.LectureÉcriture.PropriétéDe**

Cliquez sur Add permissions.

Étape 12.

Vérifiez les autorisations que vous avez sélectionnées.

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

API / Permissions name	Type	Description	Admin consent reqa...	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](#).

Cliquez sur **Grant Admin consent** pour votre organisation.

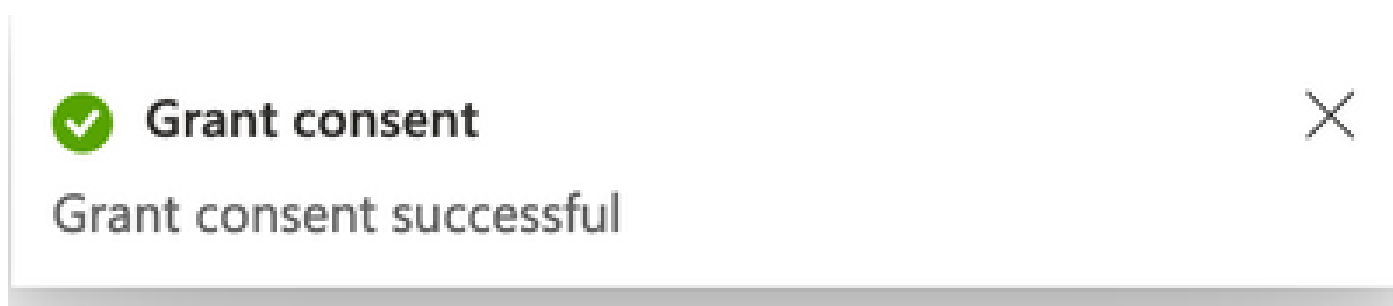
Configured permissions

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]

Une invite vous invitant à choisir si vous souhaitez accorder votre consentement pour toutes les autorisations s'affiche. Cliquez sur Yes.

Une fenêtre contextuelle similaire à celle illustrée dans cette image apparaît :



Étape 13.

Accédez à Manage > Certificates & Secrets.

Cliquez sur Add New Client Secret.

Rédigez une brève description et sélectionnez une date valide Expires. Il est conseillé de sélectionner une date de validité supérieure à 6 mois pour empêcher l'expiration des clés API.

Une fois créée, copiez et stockez dans un endroit sûr la partie qui indique **Value**, telle qu'elle est utilisée pour l'intégration.

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]

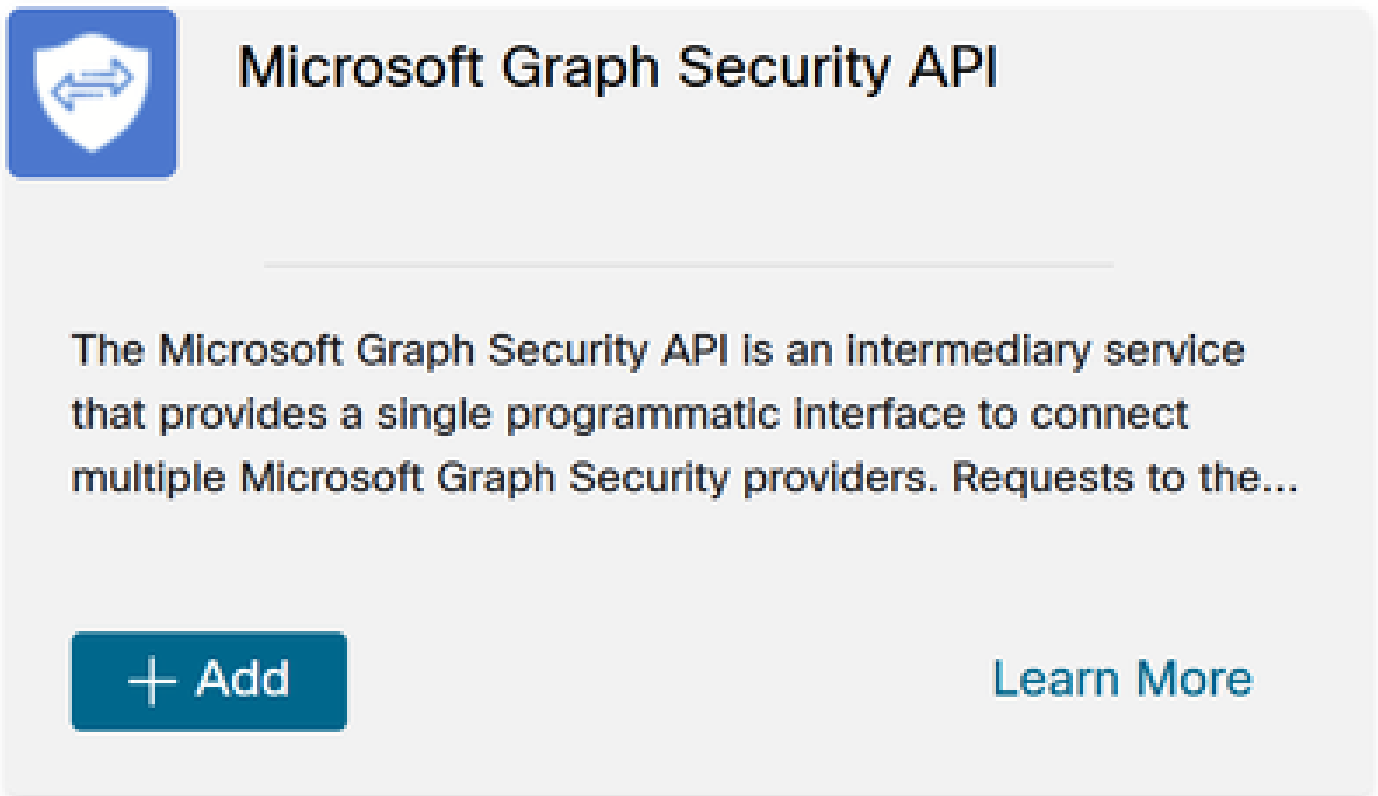


Avertissement : ce champ ne peut pas être récupéré et vous devez créer un nouveau secret.

Une fois que vous avez toutes les informations, revenez à **Overview** et copiez les valeurs de votre application. Accédez ensuite à SecureX.

Étape 14.

Naviguez pour Integration Modules > Available Integration Modules > sélectionner Microsoft Security Graph API, puis cliquez sur Add.



The card features a blue shield icon with a white double-headed arrow. The title "Microsoft Graph Security API" is in large, bold black font. Below the title is a horizontal line. The main text describes the service as an intermediary that connects 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 "Learn More".

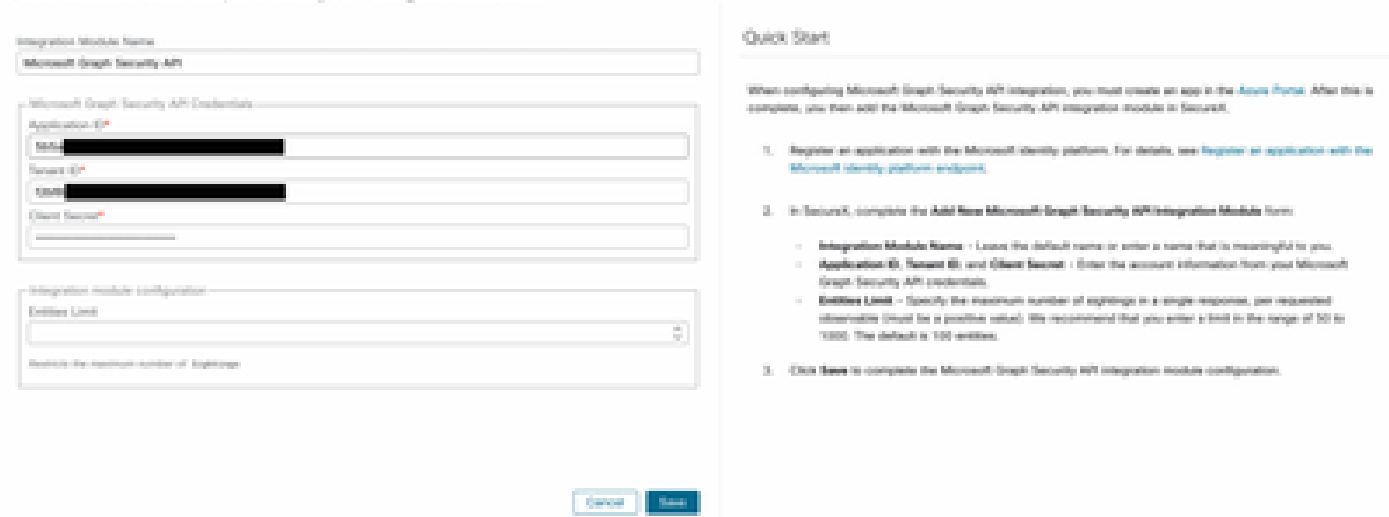
Microsoft Graph Security API

The Microsoft Graph Security API is an intermediary service that provides a single programmatic interface to connect multiple Microsoft Graph Security providers. Requests to the...

[+ Add](#) [Learn More](#)

Attribuez un nom et collez les valeurs obtenues à partir du portail Azure.

Add New Microsoft Graph Security API Integration Module



The screenshot shows a configuration form with three main sections: "Integration Module Name", "Microsoft Graph Security API Credentials", and "Integration Module Configuration".

- Integration Module Name:** A text input field containing "Microsoft Graph Security API".
- Microsoft Graph Security API Credentials:** A section with four input fields: "Application ID", "Tenant ID", "Client ID", and "Client Secret". The "Application ID" and "Client ID" fields contain redacted values.
- Integration Module Configuration:** A section with a dropdown menu for "Entries Limit" set to "1000". Below it is a note: "Specifies the maximum number of responses".

At the bottom right of the form are "Cancel" and "Save" buttons.

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 SecureX.

1. Register an application with the Microsoft identity platform. For details, see [Register an application with the Microsoft identity platform endpoints](#).
2. In SecureX, 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.
 - **Entries Limit** - Specify the maximum number of responses in a single response, per requested observable (must be a positive value). We recommend that you enter a limit in the range of 50 to 1000. The default is 100 entries.
3. Click [Save](#) to complete the Microsoft Graph Security API integration module configuration.

Cliquez sur Save et attendez que le contrôle d'intégrité réussisse.

Edit Microsoft Graph Security API Module



This integration module has no issues.

Effectuer des investigations

À ce jour, l'API Microsoft Security Graph ne remplit pas le tableau de bord Cisco XDR avec une vignette. Au contraire, les informations de votre portail Azure peuvent être interrogées à l'aide d'Investigations.

Gardez à l'esprit que l'API Graph ne peut être interrogée que pour :

- ip
- domaine
- nom de l'hôte
- url
- nom_fichier
- chemin_fichier
- sha256

Dans cet exemple, l'enquête a utilisé cette SHA `c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148`.

Results

Details

Threat Context

▼ 0 TARGETS

▼ 1 INVESTIGATED



c73d01ffb427e5b7008003b4eaf9...

Malicious SHA-256 Hash

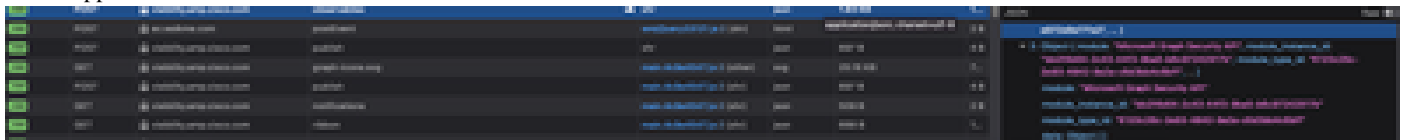
0 Sightings

▶ 0 OMITTED

▶ 0 RELATED

Comme vous pouvez le voir, il a 0 Sightings dans l'environnement de laboratoire, alors comment tester si l'API Graph fonctionne ?

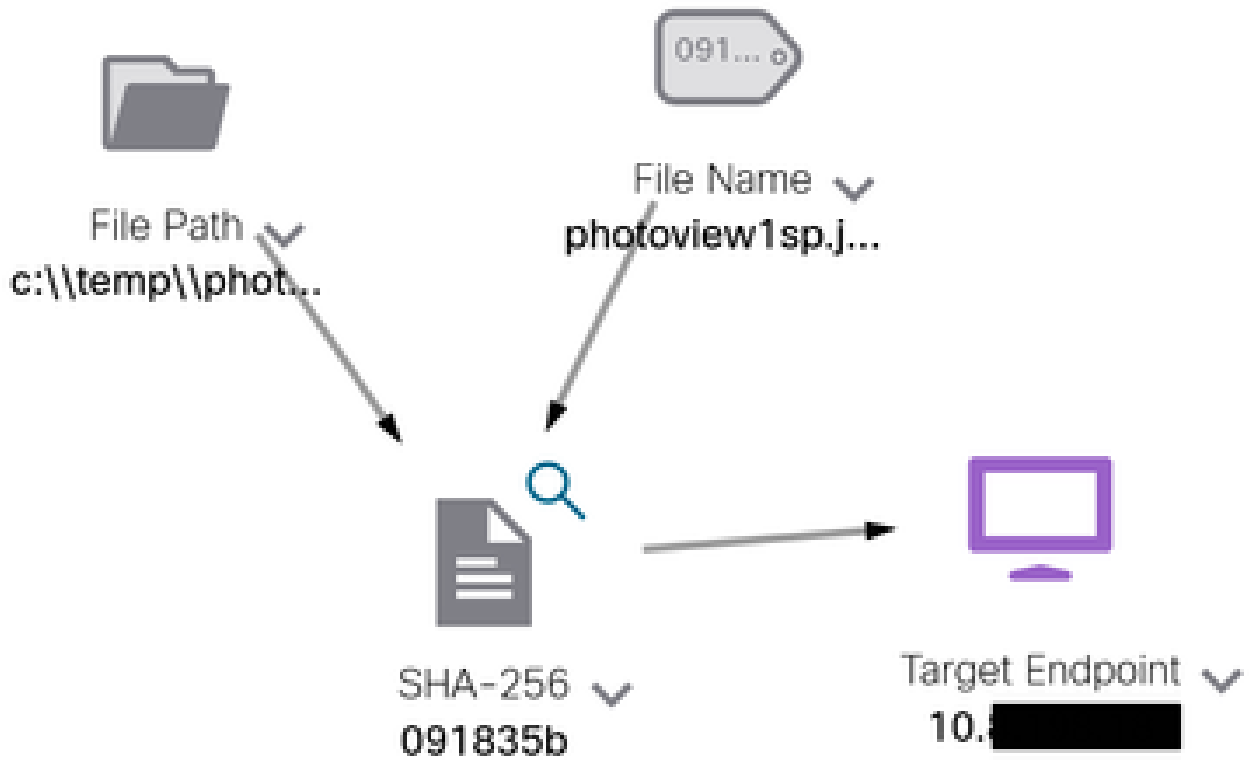
Ouvrez les Outils de développement Web, exécutez l'investigation, recherchez un événement de publication sur **visibilité.amp.cisco.com** dans le fichier appelé Observables.



Vérifier

Vous pouvez utiliser ce lien : [Microsoft graph security Snapshots](#) pour une liste de Snapshots qui vous aident à comprendre la réponse que vous pouvez obtenir de chaque type de observable.

Vous pouvez voir un exemple comme illustré dans cette image :



Développez la fenêtre, vous pouvez voir les informations fournies par l'intégration :

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 091835b16193e53bee1bba04d0fceff534544cad306673066f3ad6973a4b18b19

Gardez à l'esprit que les données doivent exister dans votre portail Azure et que l'API Graph fonctionne mieux lorsqu'elle est utilisée avec d'autres solutions Microsoft. Cependant, cela doit être validé par le support technique de Microsoft.

Dépannage

- Message Échec d'autorisation :
 - Vérifiez que les valeurs de **Tenant ID** et Client ID sont correctes et qu'elles sont toujours valides.

- Aucune donnée n'apparaît dans Investigation :
 - Veillez à copier et coller les valeurs appropriées pour **Tenant ID** et **Client ID**.
 - Assurez-vous que vous avez utilisé les informations du champ **Value** de la Certificates & Secrets section.
 - Utilisez les outils WebDeveloper pour déterminer si l'API Graph est interrogée lors d'une investigation.
 - À mesure que l'API graphique fusionne les données de divers fournisseurs d'alertes Microsoft, assurez-vous que OData est pris en charge pour les filtres de requête. (Par exemple, Sécurité et conformité Office 365 et Microsoft Defender ATP).

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.