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

Table des matières

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

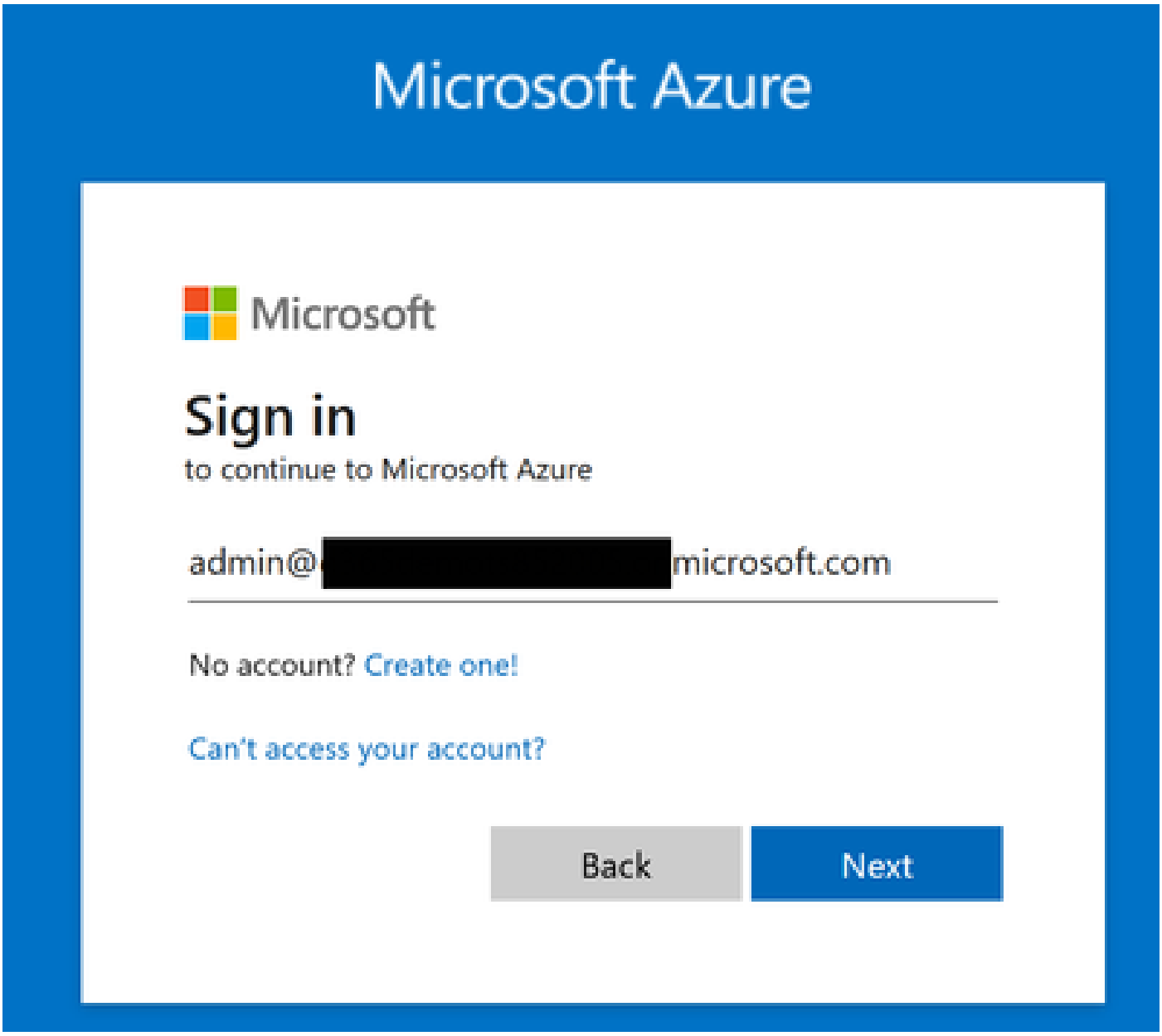
- Compte d'administrateur Cisco XDR
- Compte d'administrateur système Microsoft Azure
- Accès à Cisco XDR

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

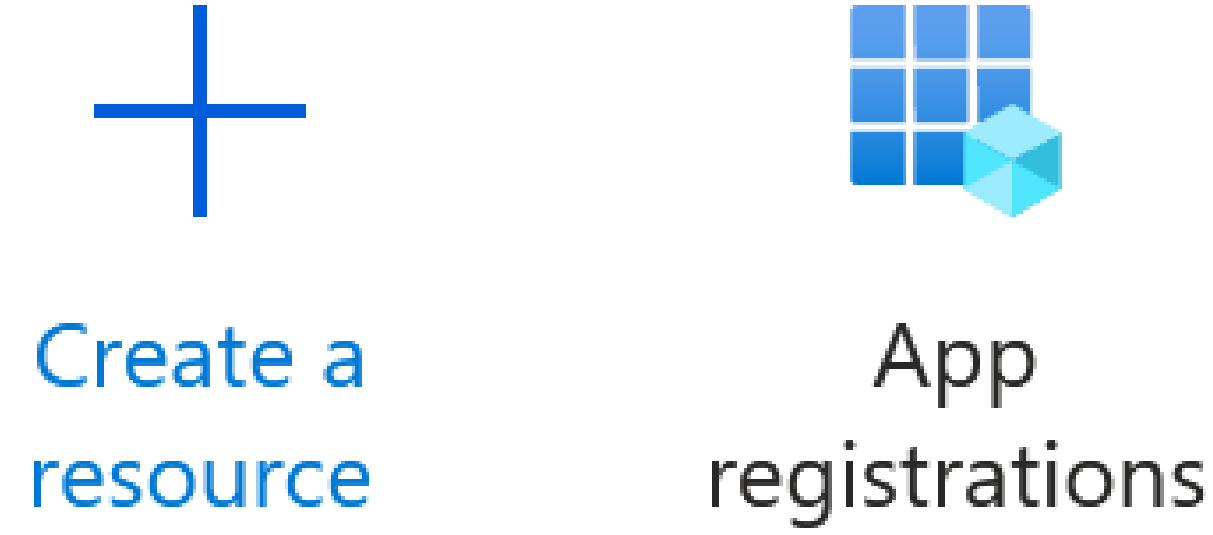
Étape 1.

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



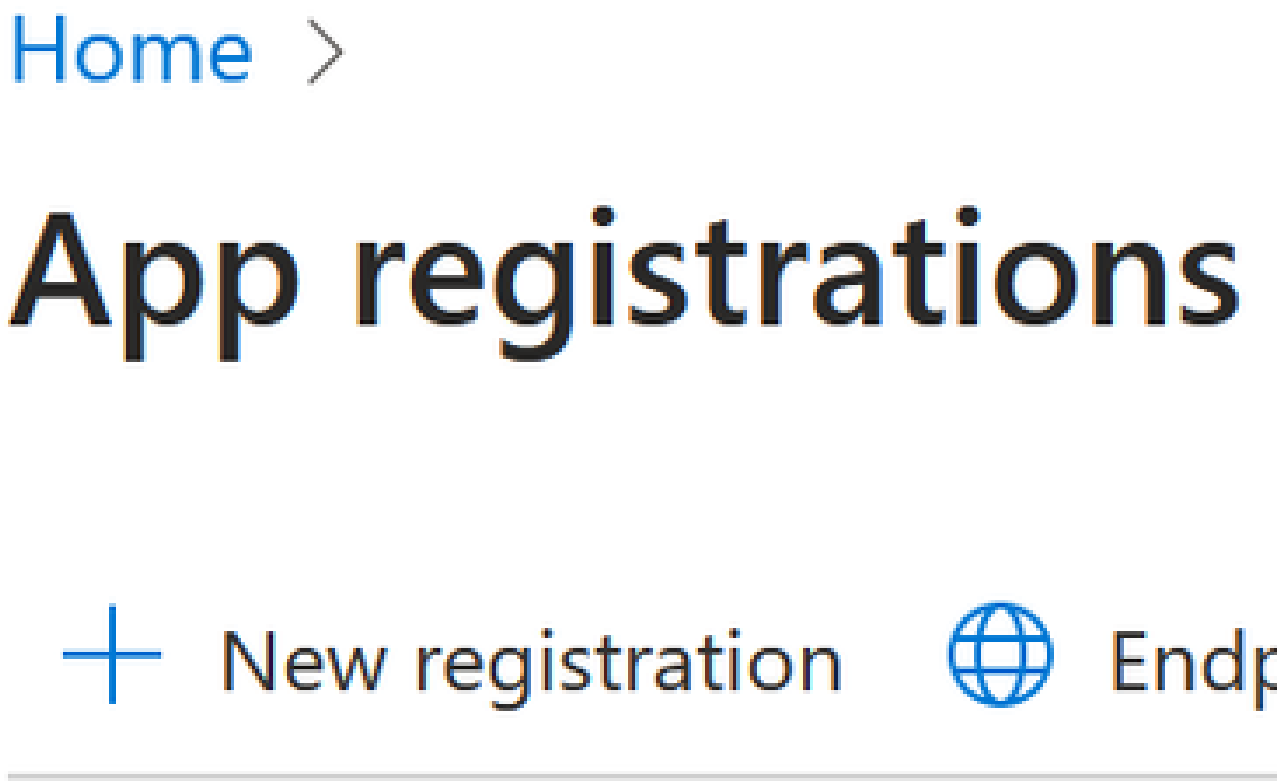
Étape 2.

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



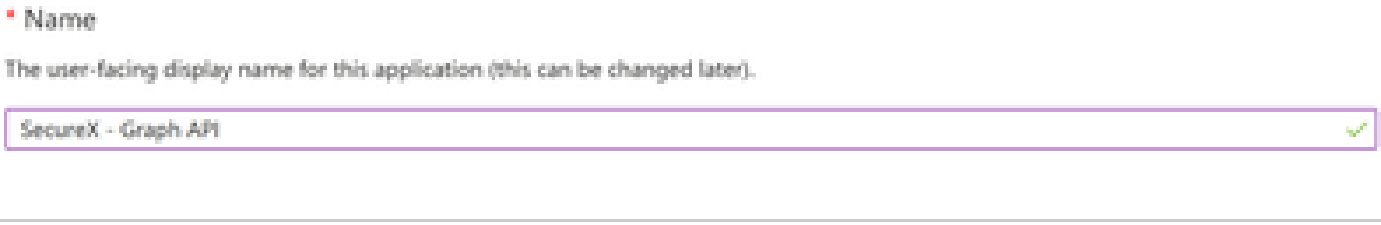
Étape 3.

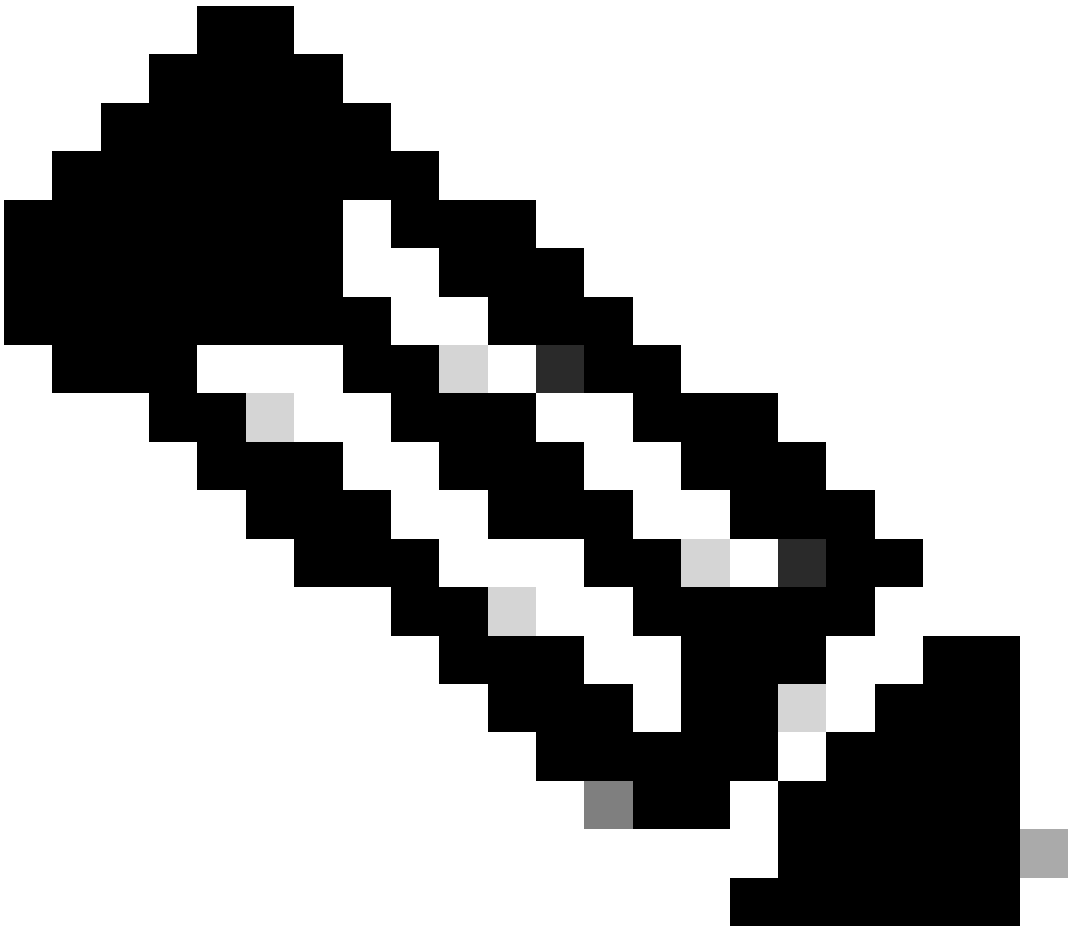
Cliquez sur New registration.



Étape 4.

Tapez un nom pour identifier votre nouvelle application.





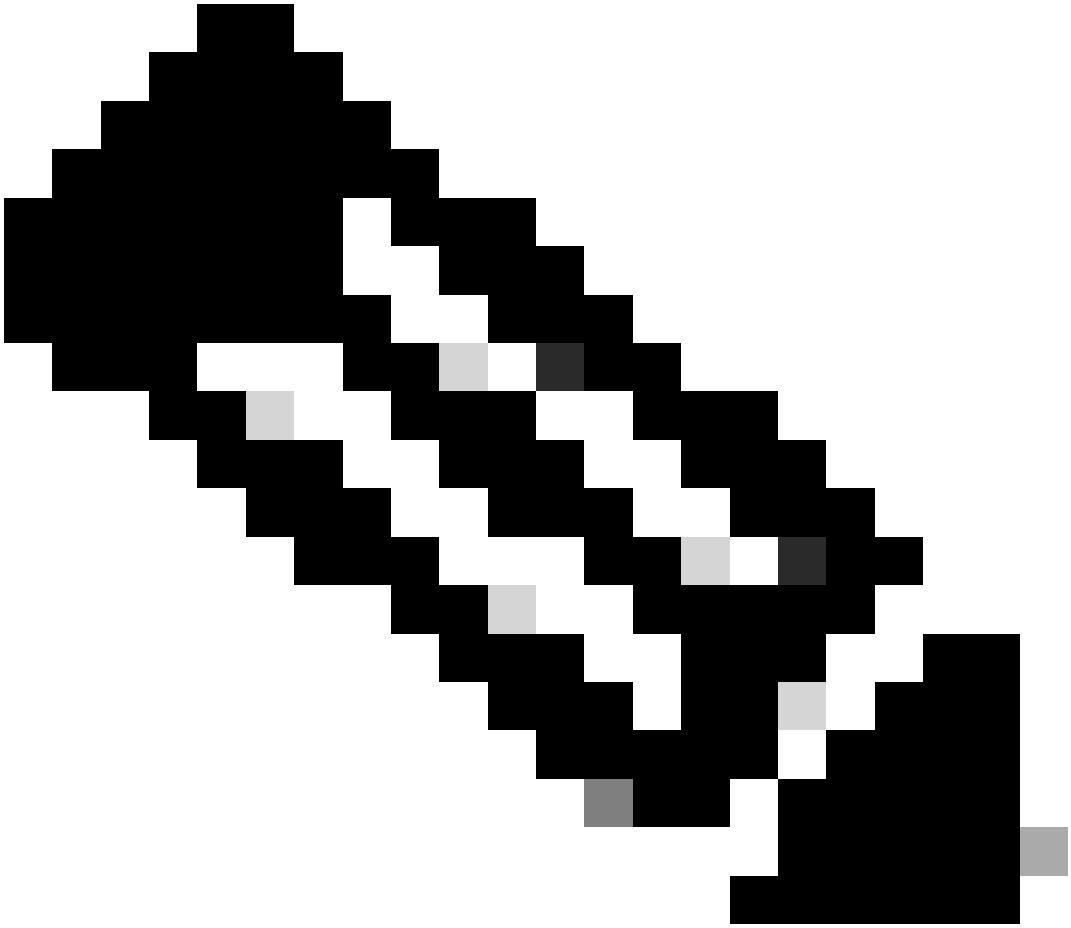
Remarque : une coche verte apparaît si le nom est valide.

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 ([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



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

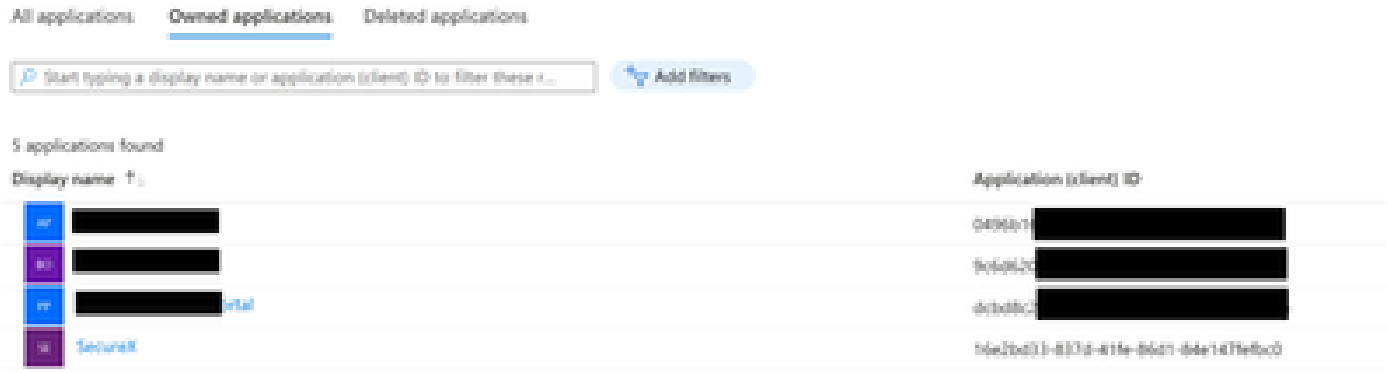
Étape 5.

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



Étape 7.

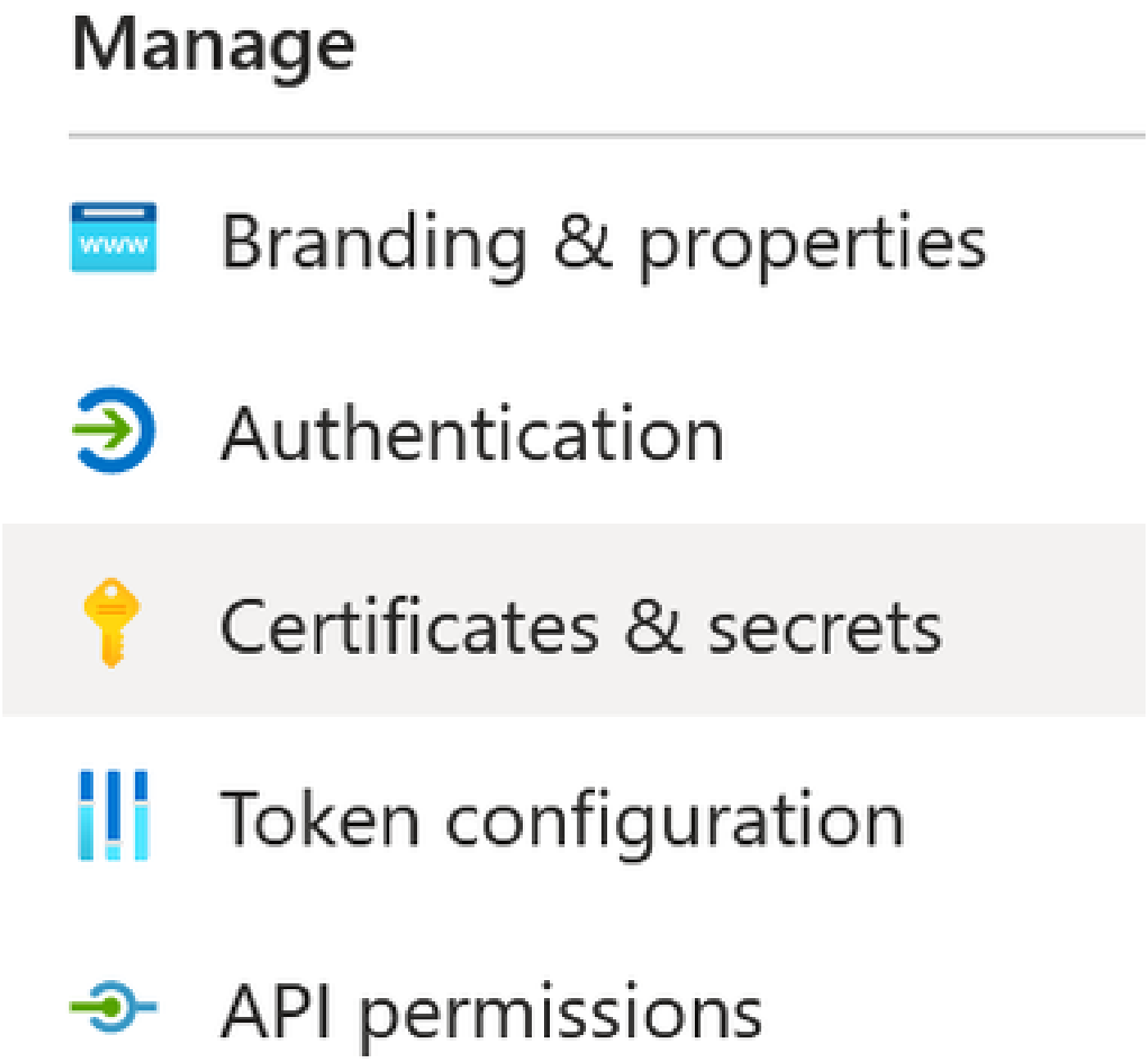
Un résumé de votre application s'affiche. Veuillez indiquer les détails pertinents suivants :

ID de l'application (client) :

ID du répertoire (locataire) :

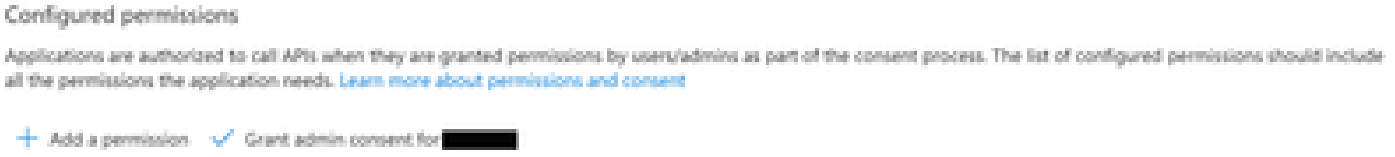
Étape 8.

Accédez à Manage Menu > API Permissions.



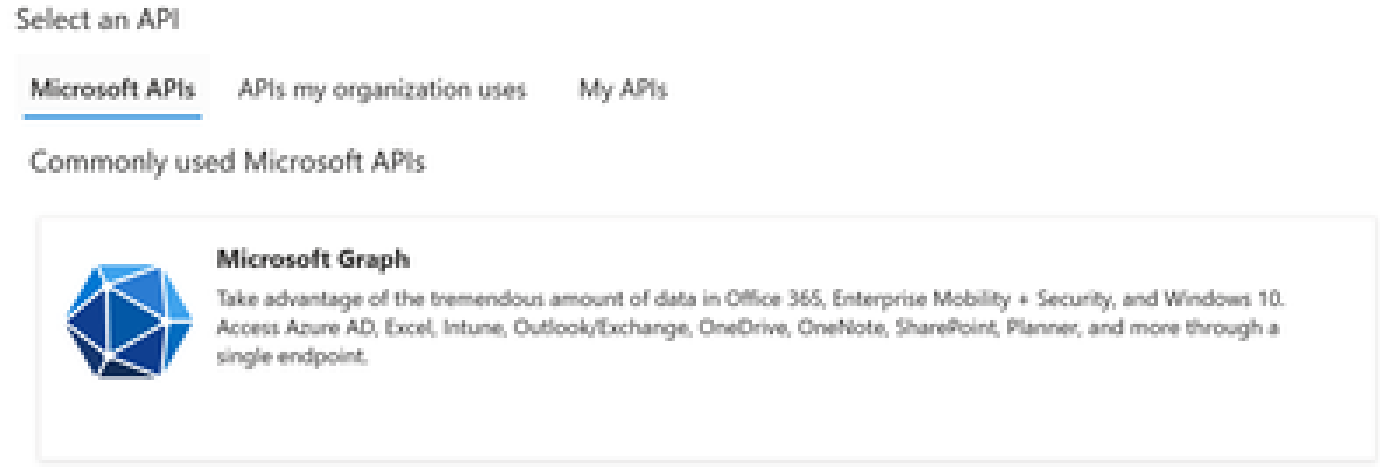
Étape 9.

Sous Autorisations configurées, cliquez sur Add a Permission.



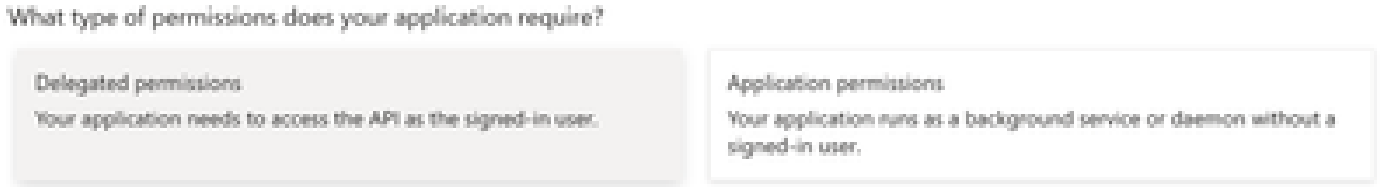
Étape 10.

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



Étape 11.

Sélectionnez Application permissions.



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

- **Lire.Tout**
- **LectureÉcriture.Tout**

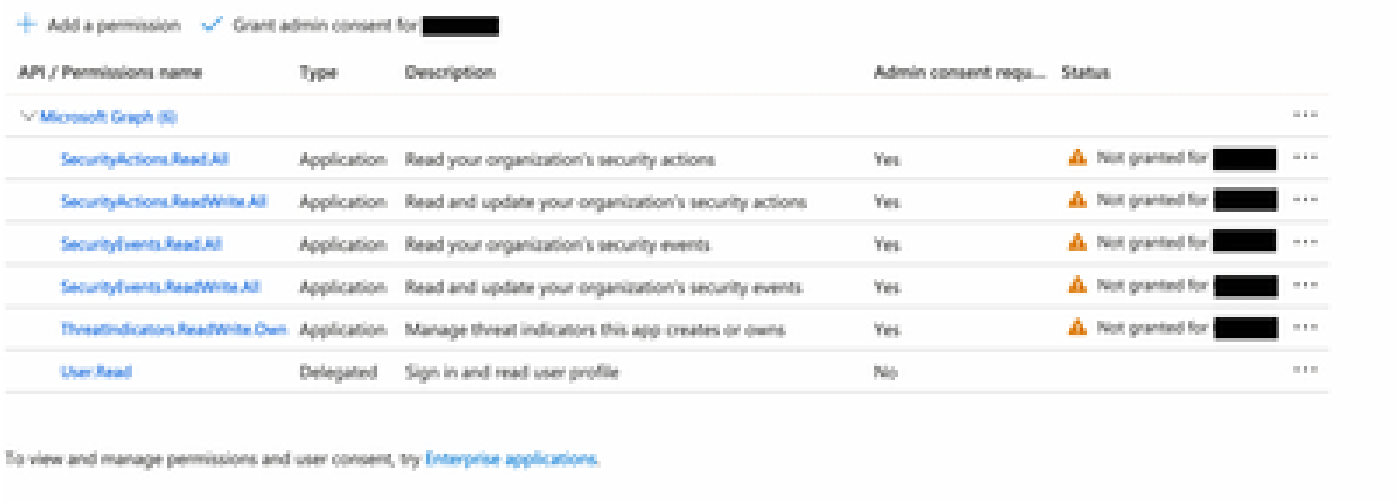
- **Evénements de sécurité** et sélectionnez
  - **Lire.Tout**
  - **LectureÉcriture.Tout**

- **Indicateurs de menace** et sélectionnez
  - **IndicateursMenaces.LectureÉcriture.PropriétéDe**

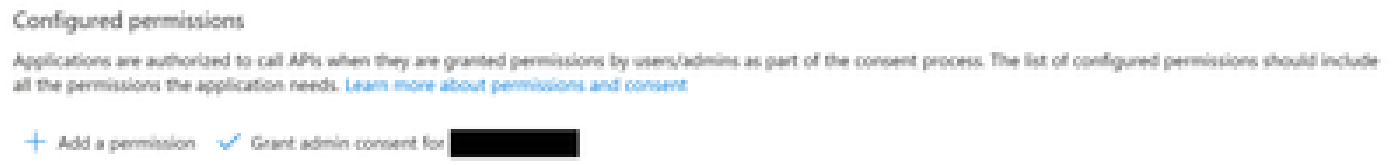
Cliquez sur Add permissions.

Étape 12.

Vérifiez les autorisations que vous avez sélectionnées.

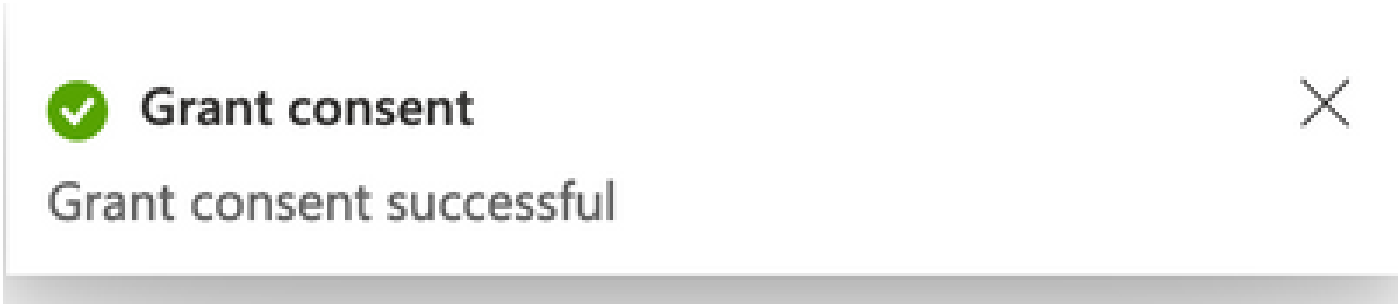


Cliquez sur **Grant Admin consent** pour votre organisation.



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 :



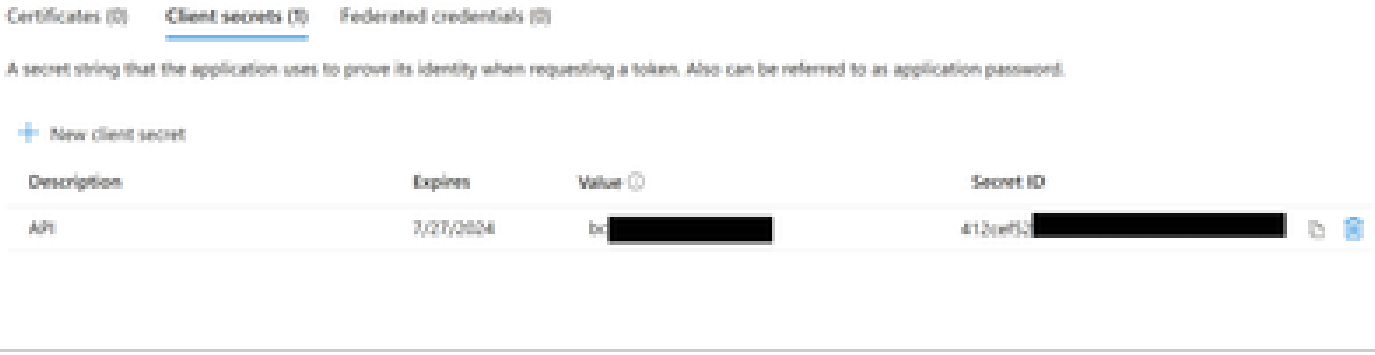
Étape 13.

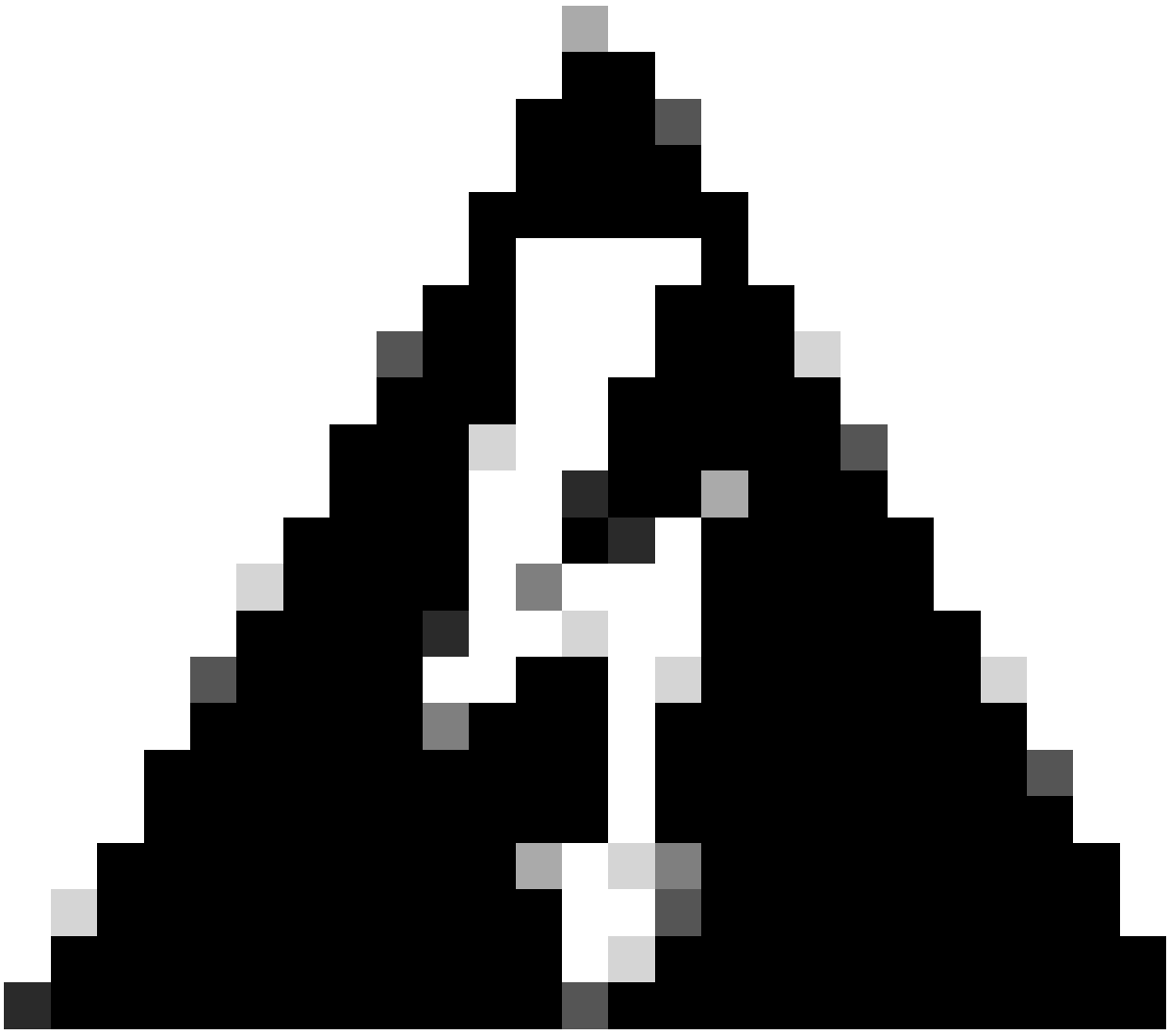
Accédez à Manage > Certificates & Secrets.

Cliquez sur Add New Client Secret.

Rédigez une brève description et sélectionnez une date valideExpires. 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.





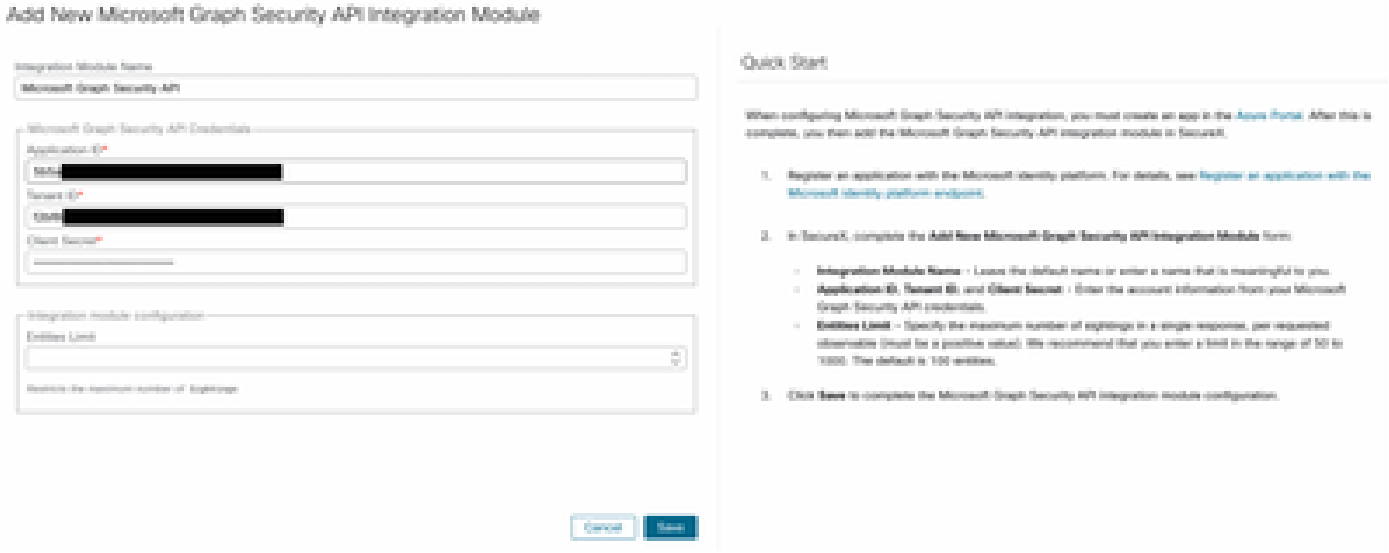
Avertissement : ce champ ne peut pas être récupéré et vous devez créer un nouveau secret.

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.

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



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

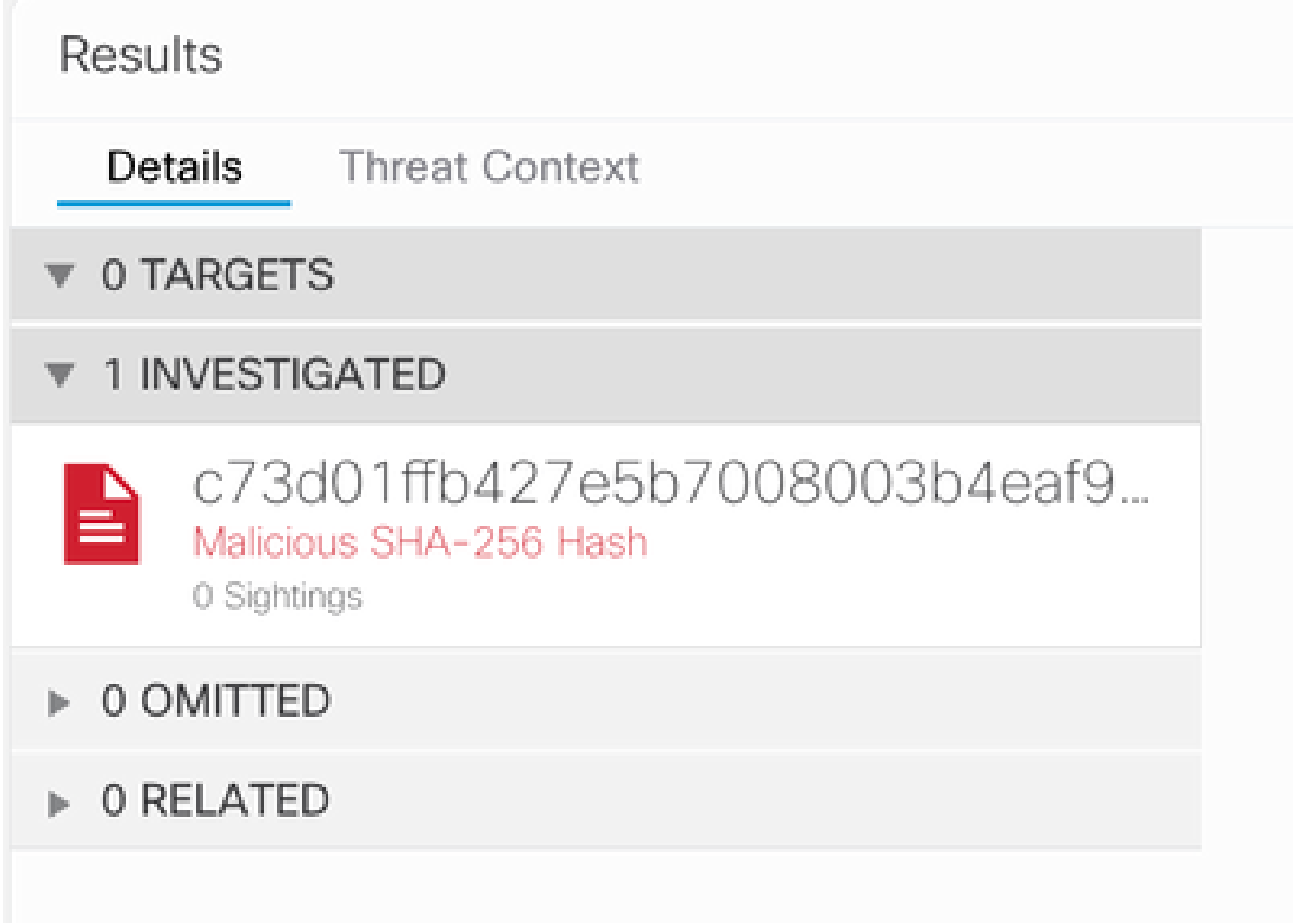
Effectuer des investigations

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 :

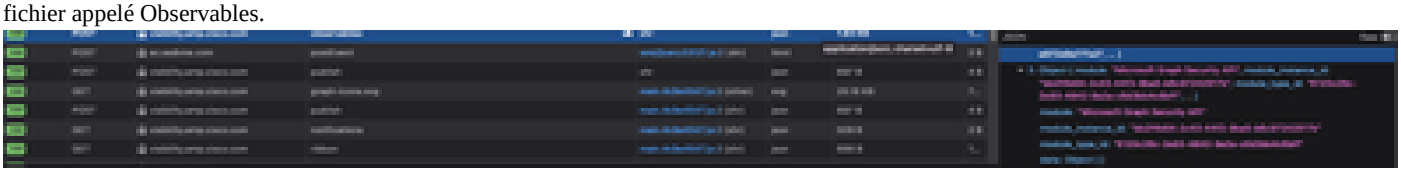
- ip
- domaine
- nom de l'hôte
- url
- nom_fichier
- chemin_fichier
- sha256

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



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

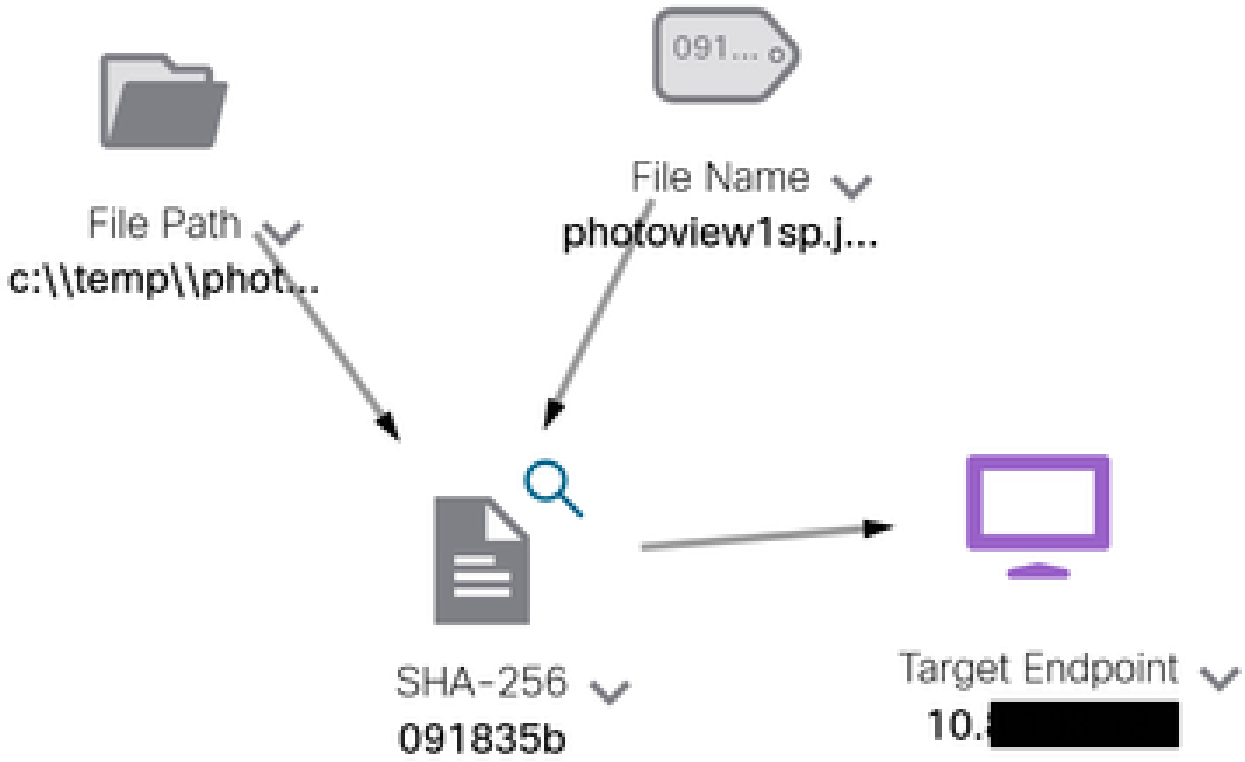
Ouvrez les Outils de développement Web, exécutez l'investigation, recherchez un événement de publication sur **visibilité.amp.cisco.com** dans le fichier appelé Observables.



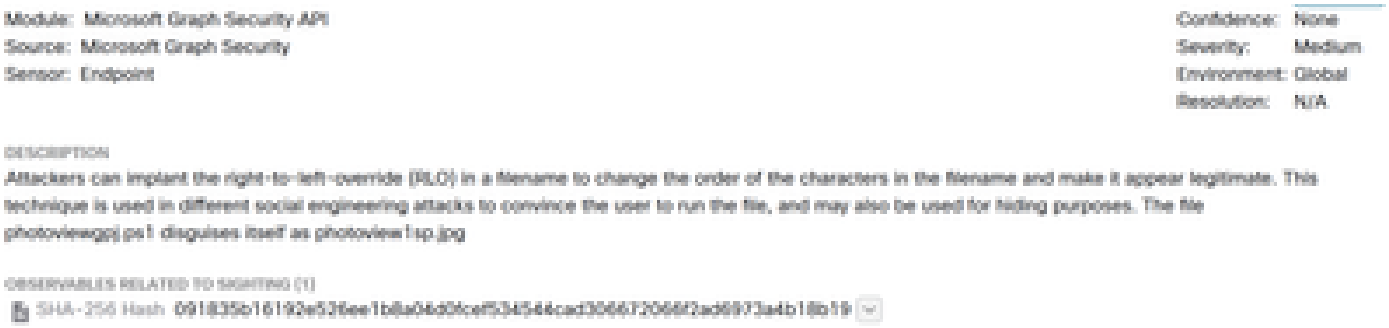
Vérifier

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 :



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.