Konfigurieren der Integration der Microsoft Graph API mit Cisco XDR

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Integration der Microsoft Graph-API in Cisco XDR sowie der Typ der abfragbaren Daten beschrieben.

Voraussetzungen

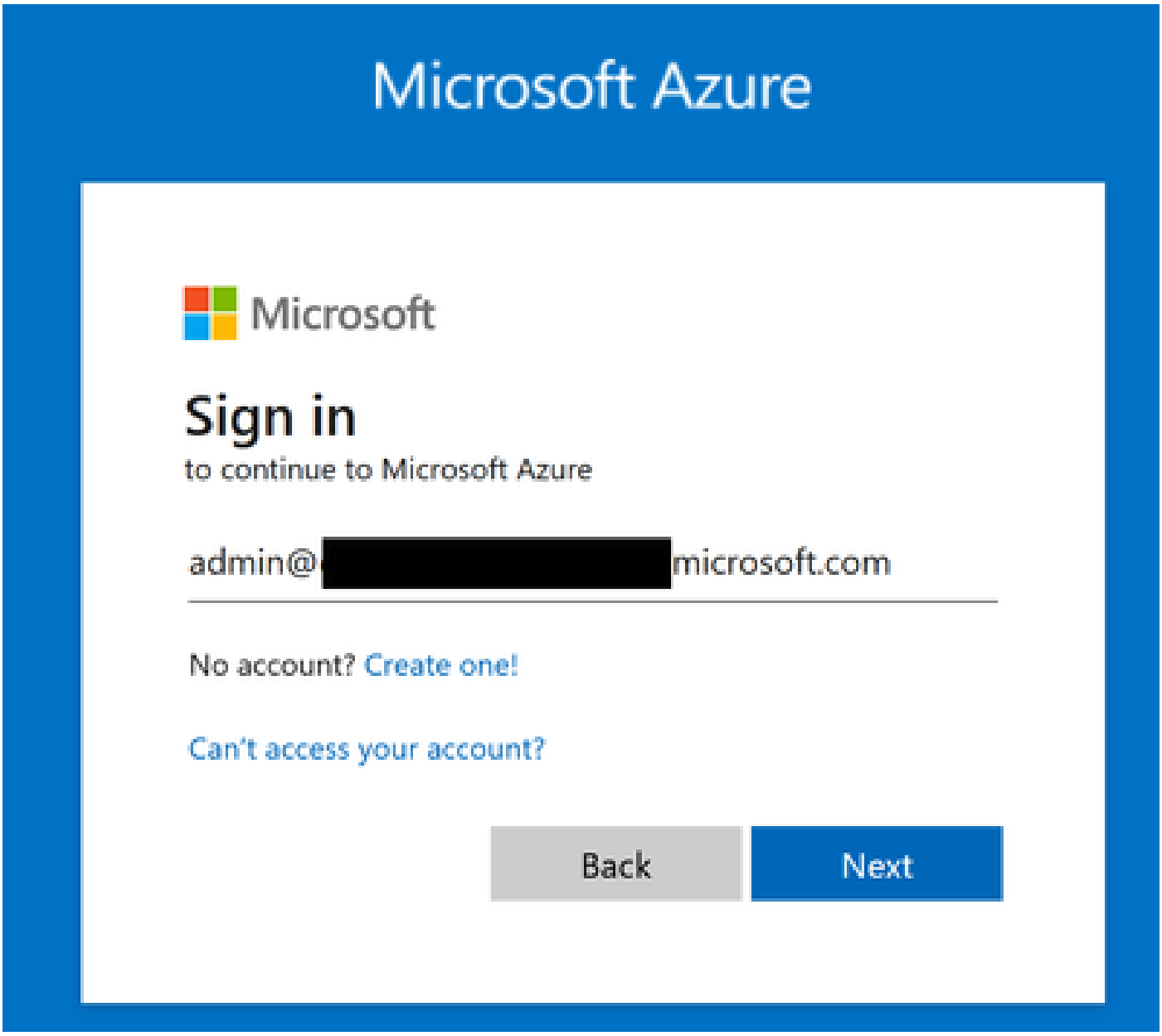
- Cisco XDR-Administratorkonto
- Microsoft Azure-Systemadministratorkonto
- Zugriff auf Cisco XDR

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Integrationsschritte

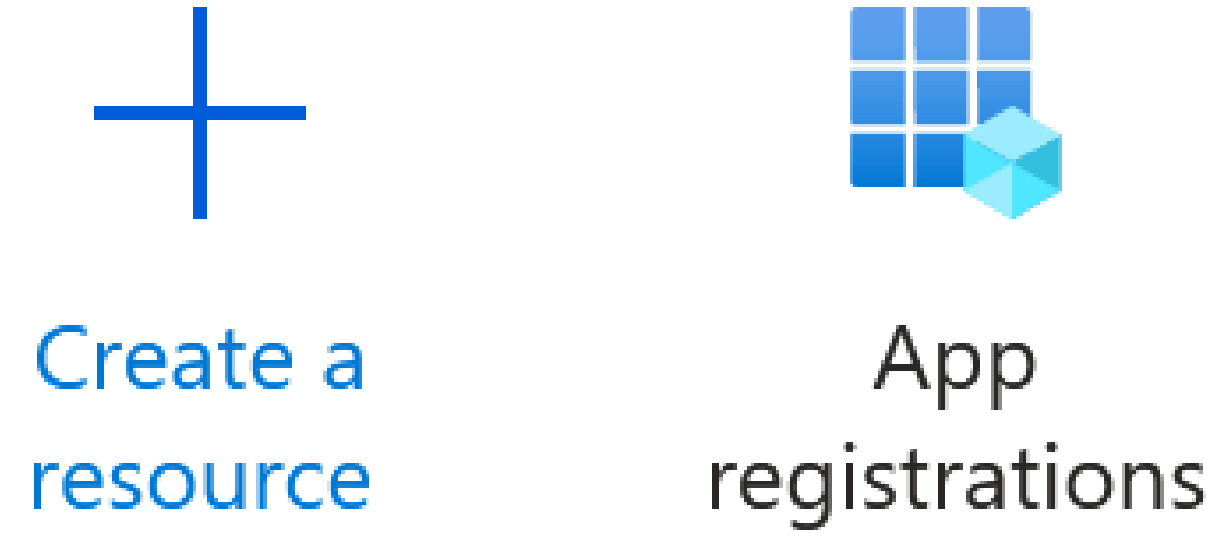
Schritt 1:

Melden Sie sich als Systemadministrator bei Microsoft Azure an.



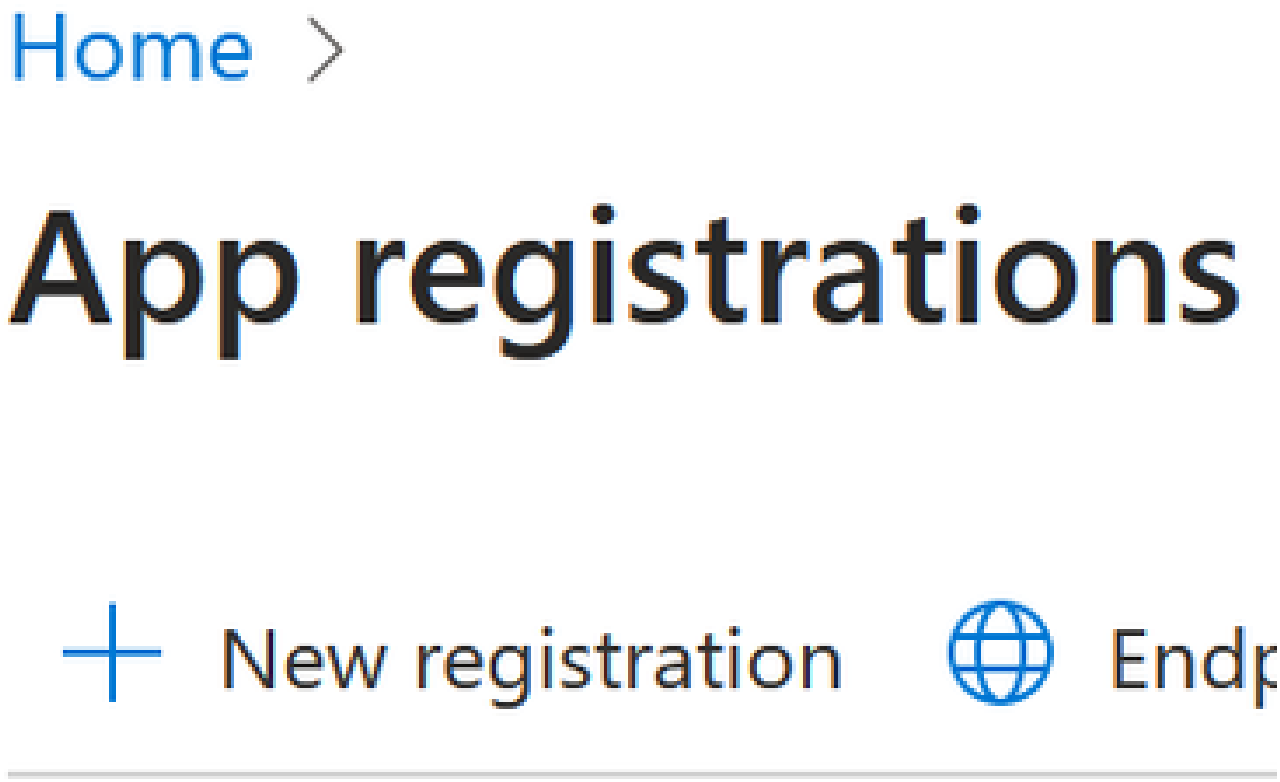
Schritt 2:

Klicken Sie **App Registrations** auf das Azure-Serviceportal.



Schritt 3:

Klicken Sie auf .New registration



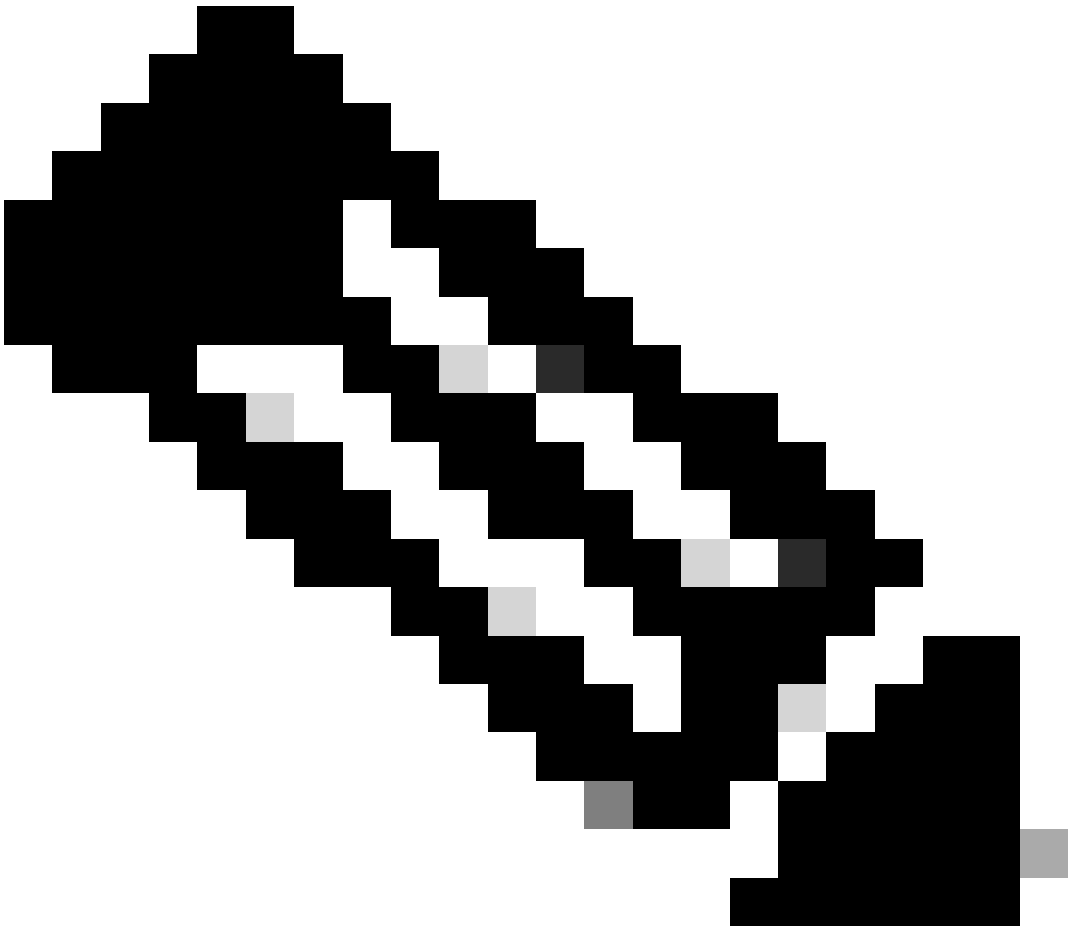
Schritt 4:

Geben Sie einen Namen ein, um Ihre neue App zu identifizieren.

* Name

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

SecureX - Graph API



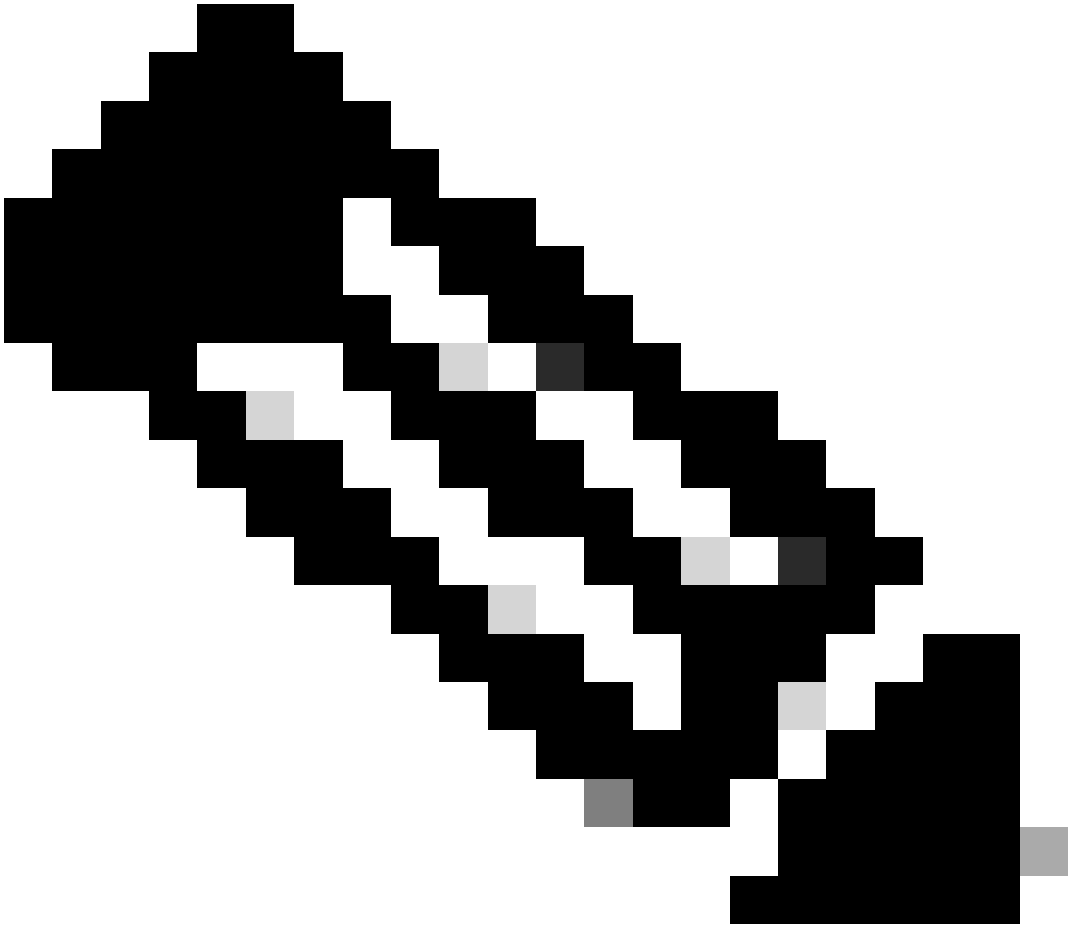
Hinweis: Wenn der Name gültig ist, wird ein grünes Häkchen angezeigt.

Wählen Sie für unterstützte Kontotypen die 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



Hinweis: Sie müssen keinen Umleitungs-URI eingeben.

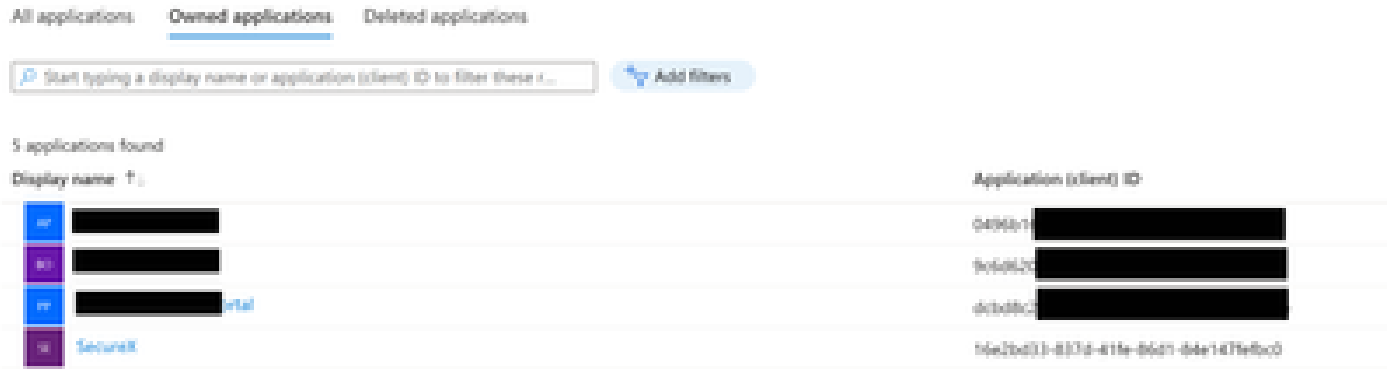
Schritt 5:

Blättern Sie zum unteren Bildschirmrand, und klicken Sie auf **Register**.

Schritt 6:

Navigieren Sie zurück zur Azure-Dienstseite, und klicken Sie auf App Registrations > Owned Applications.

Identifizieren Sie Ihre App, und klicken Sie auf den Namen. In diesem Beispiel ist dies der FallSecureX.



Schritt 7.

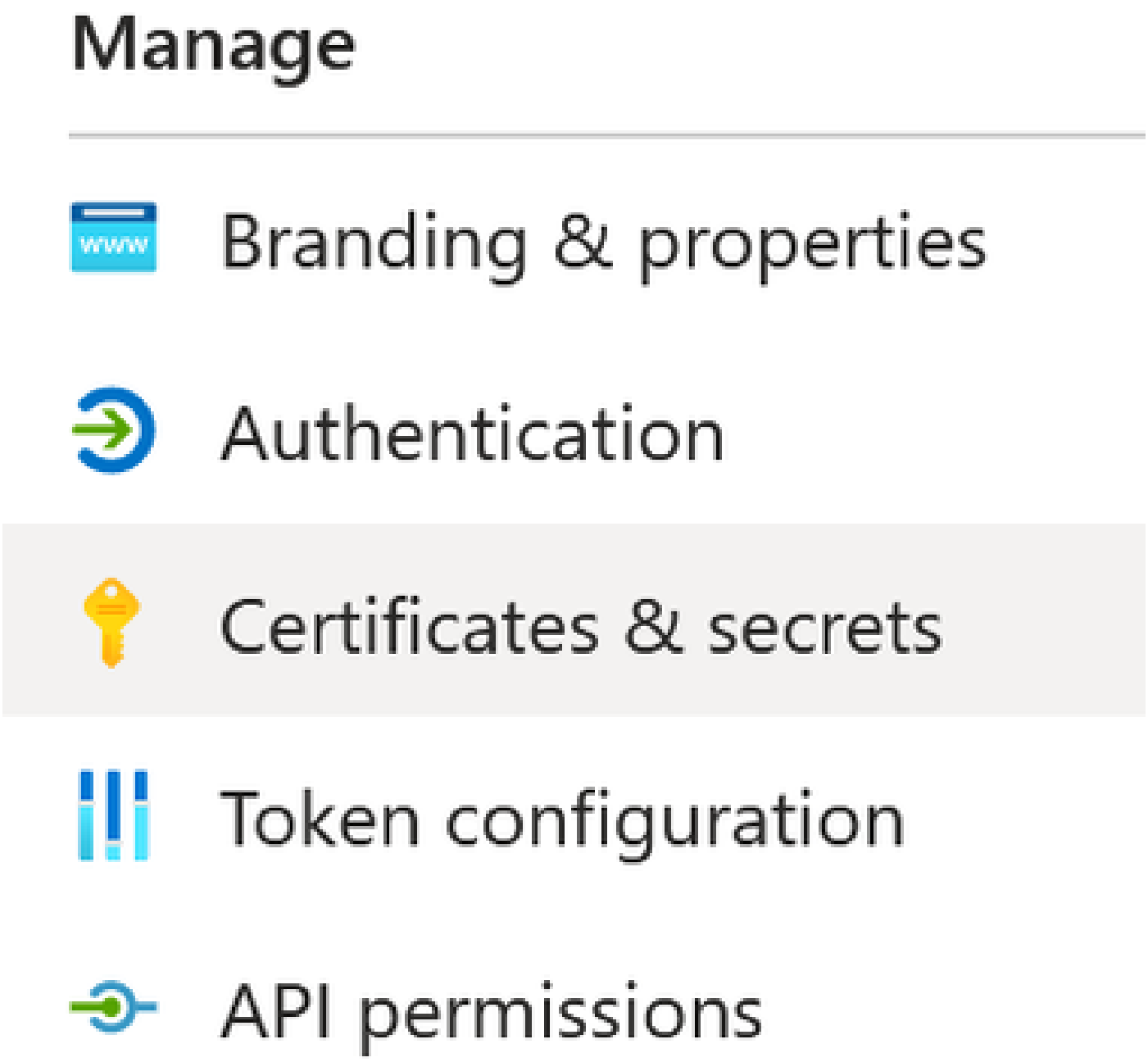
Eine Zusammenfassung Ihrer App wird angezeigt. Bitte geben Sie die folgenden relevanten Details an:

Anwendungs-ID (Client):

Verzeichnis-ID (Tenant):

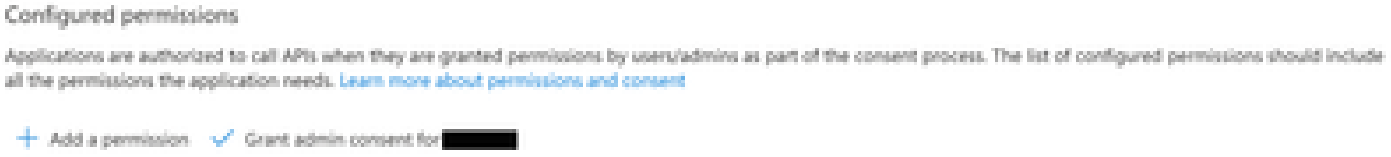
Schritt 8:

Navigieren Sie zu Manage Menu > API Permissions.



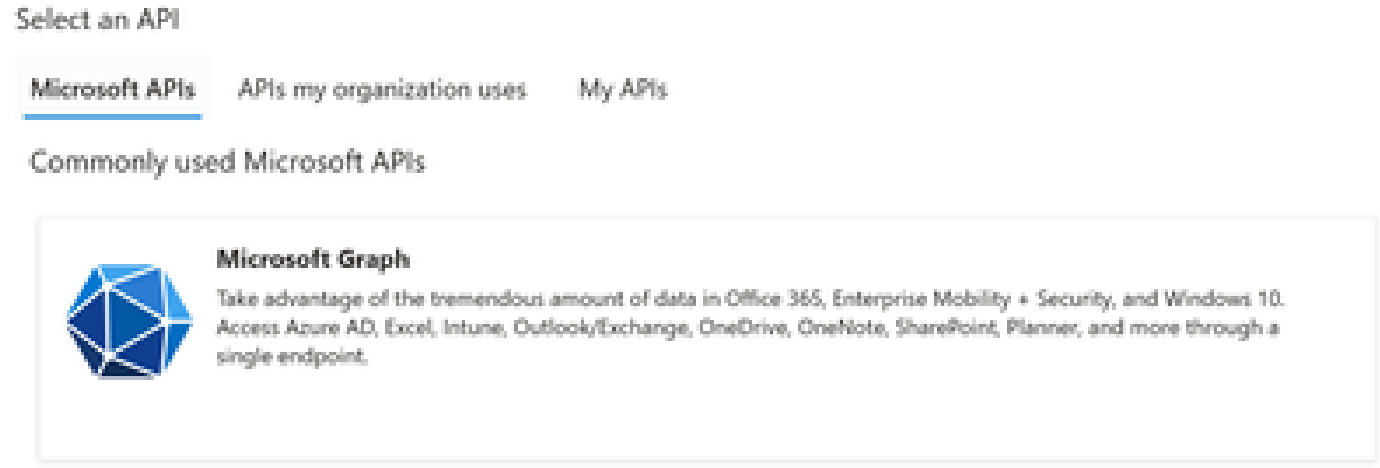
Schritt 9.

Klicken Sie unter Konfigurierte Berechtigungen auf Add a Permission.



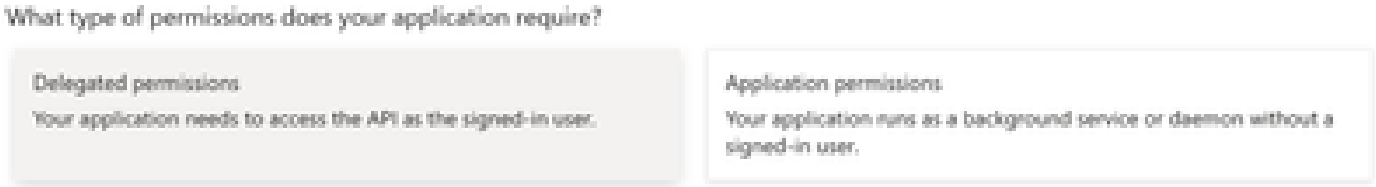
Schritt 10.

Klicken Sie im Abschnitt Anfordern von API-Berechtigungen auf **Microsoft Graph**.



Schritt 11.

Auswählen Application permissions.



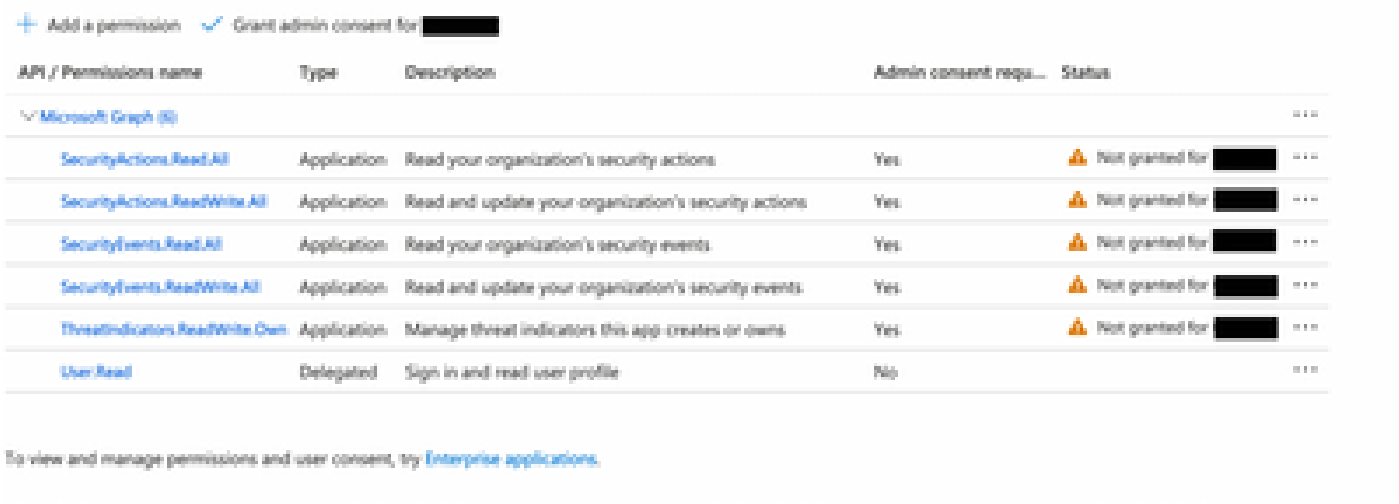
Suchen Sie in der Suchleiste nach Security. Erweitern **Security Actions** und auswählen

- **Lesen.Alle**
- **LesenSchreiben.Alle**
- **Sicherheitsereignisse** auswählen und
  - **Lesen.Alle**
  - **LesenSchreiben.Alle**
- **Bedrohungsindikatoren anzeigen** und auswählen
  - **ThreatIndicators.ReadWrite.OwnedBy**

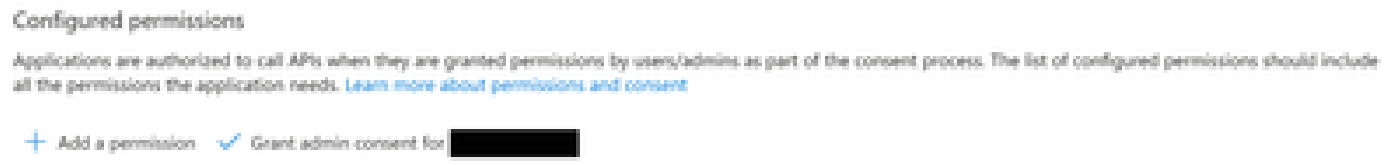
Klicken Sie auf .Add permissions

Schritt 12:

Überprüfen Sie die ausgewählten Berechtigungen.

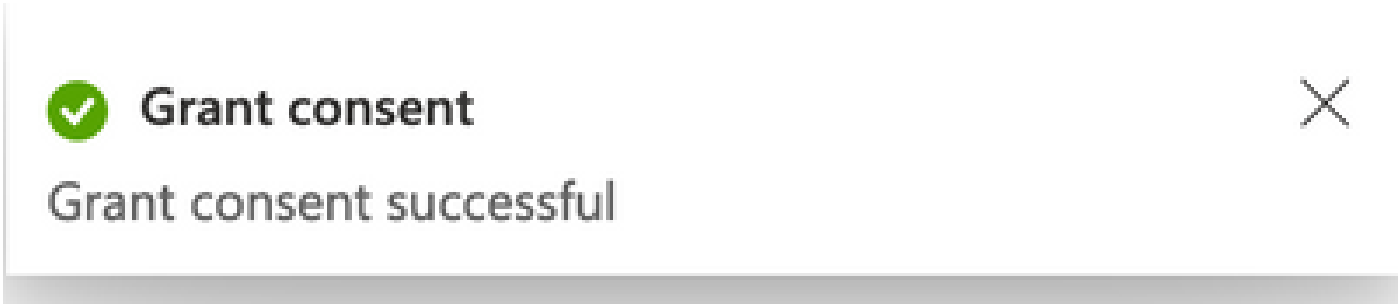


Klicken Sie hier **Grant Admin consent** für Ihre Organisation.



Sie werden aufgefordert, auszuwählen, ob Sie die Zustimmung für alle Berechtigungen erteilen möchten. Klicken Sie auf .Yes

Ein ähnliches Popup-Fenster wird angezeigt, wie in dieser Abbildung dargestellt:



Schritt 13:

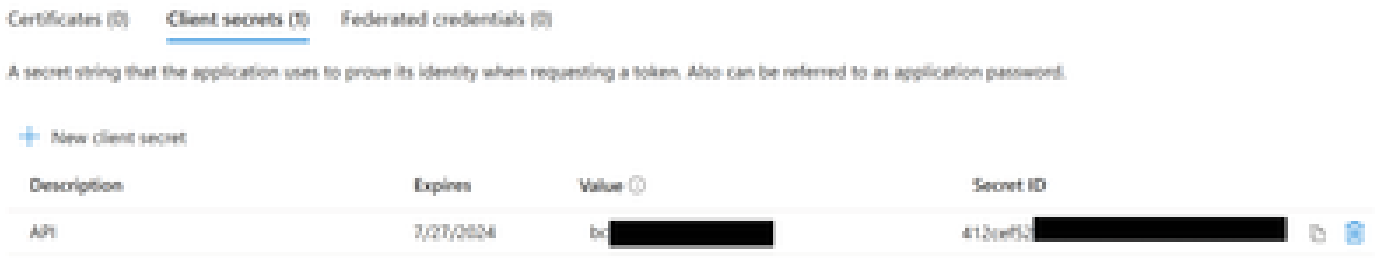
Navigieren Sie zu Manage > Certificates & Secrets.

Klicken Sie auf .Add New Client Secret

Schreiben Sie eine kurze Beschreibung, und wählen Sie ein gültiges Expires Datum aus. Es wird empfohlen, ein Gültigkeitsdatum von mehr als 6 Monaten zu wählen, um zu verhindern, dass die API-Schlüssel ablaufen.

Nach der Erstellung können Sie den Abschnitt, der Ihnen sagt, **Value**wie er für die Integration verwendet wird, kopieren und an einem sicheren

Ort speichern.



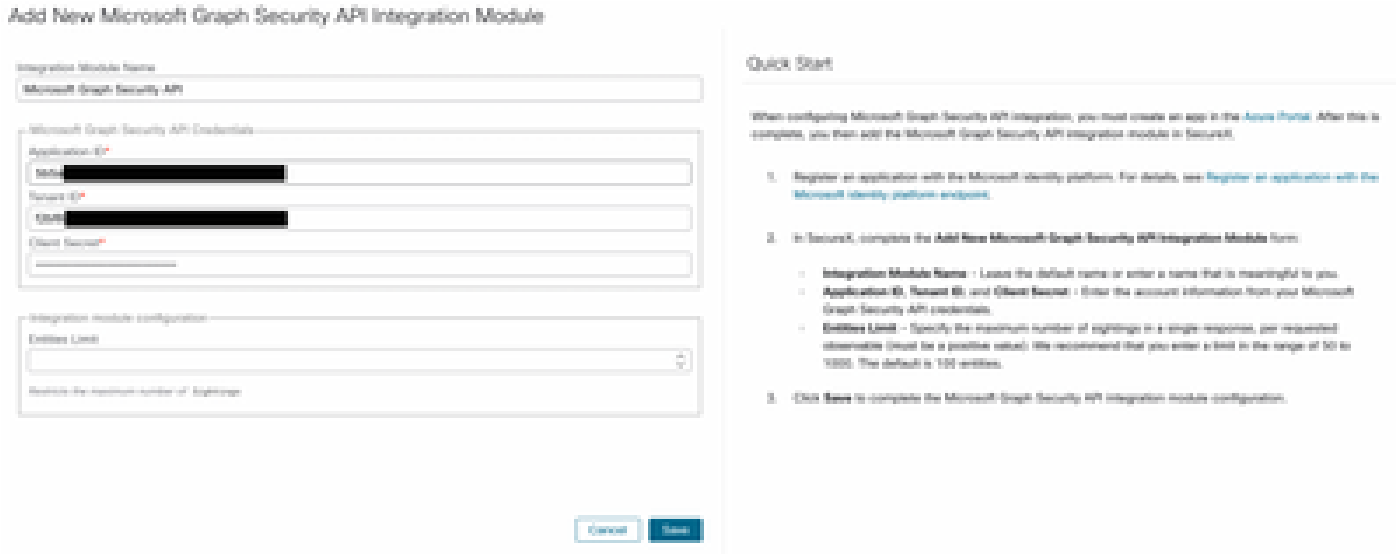
Warnung: Dieses Feld kann nicht wiederhergestellt werden, und Sie müssen einen neuen Schlüssel erstellen.

Sobald Sie alle Informationen haben, navigieren Sie zurück zu **Overview** und kopieren Sie die Werte Ihrer App. Navigieren Sie anschließend zu SecureX.

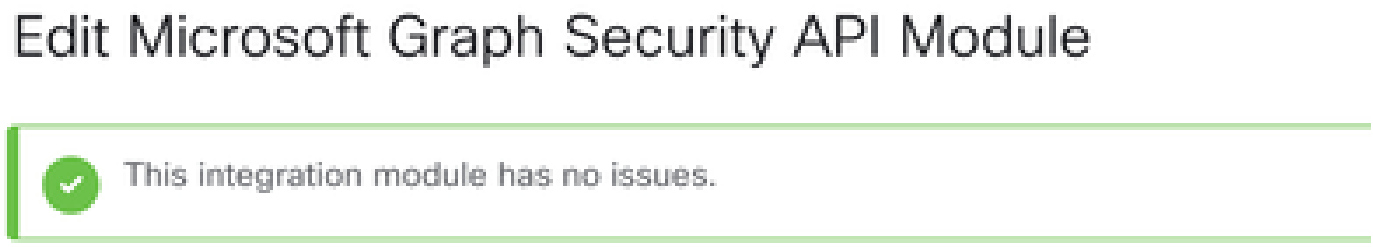
Schritt 14:

Navigieren Sie zur Integration Modules > Available Integration Modules > Option Microsoft Security Graph API, und klicken Sie auf Add.

Weisen Sie einen Namen zu, und fügen Sie die Werte ein, die Sie aus dem Azure-Portal erhalten haben.



Klicken Sie Save, und warten Sie, bis der Statuscheck erfolgreich ist.



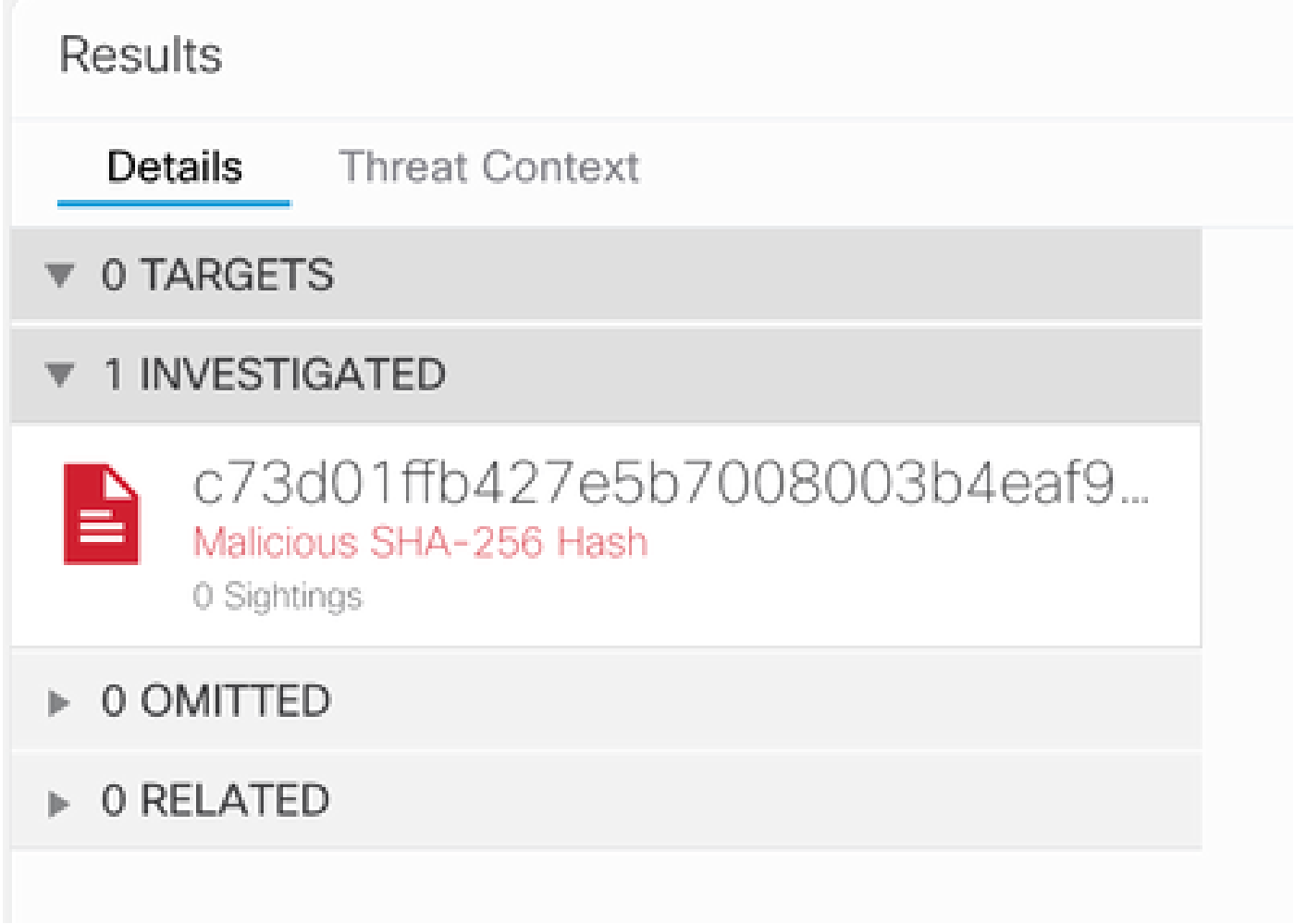
Durchführung von Untersuchungen

Bislang wird im Cisco XDR Dashboard mit der Microsoft Security Graph API keine Kachel angezeigt. Stattdessen können die Informationen aus Ihrem Azure-Portal mithilfe von Investigations abgefragt werden.

Beachten Sie, dass die Graph-API nur abgefragt werden kann für:

- ip
- Domäne
- hostname
- url
- Dateiname
- Dateipfad
- SHA256

In diesem Beispiel wurde diese SHA c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148 verwendet.



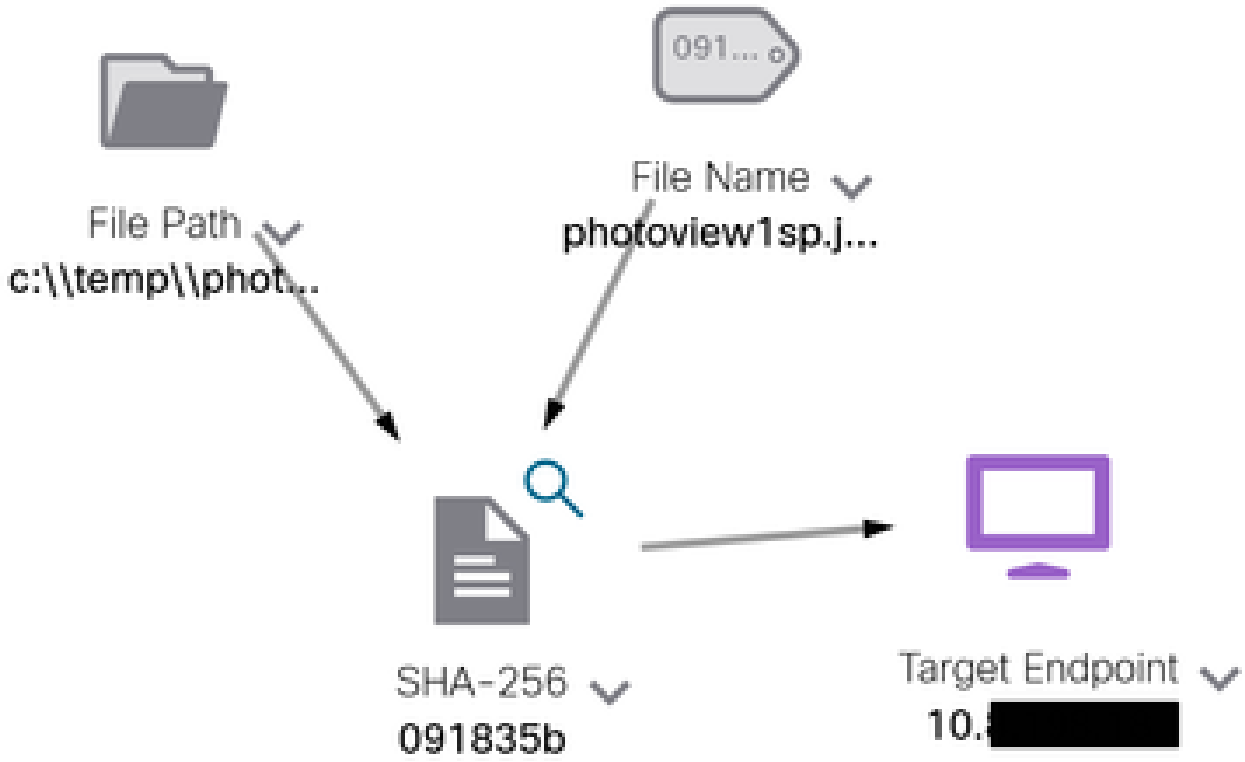
Wie Sie sehen können, hat es 0 Sichtungen in der Lab-Umgebung, wie also zu testen, ob Graph API funktioniert?

Öffnen Sie die WebDeveloper-Tools, führen Sie die Untersuchung aus, suchen Sie nach einem Post Event, um **visibility.amp.cisco.com** die Datei mit dem Namen Observables.

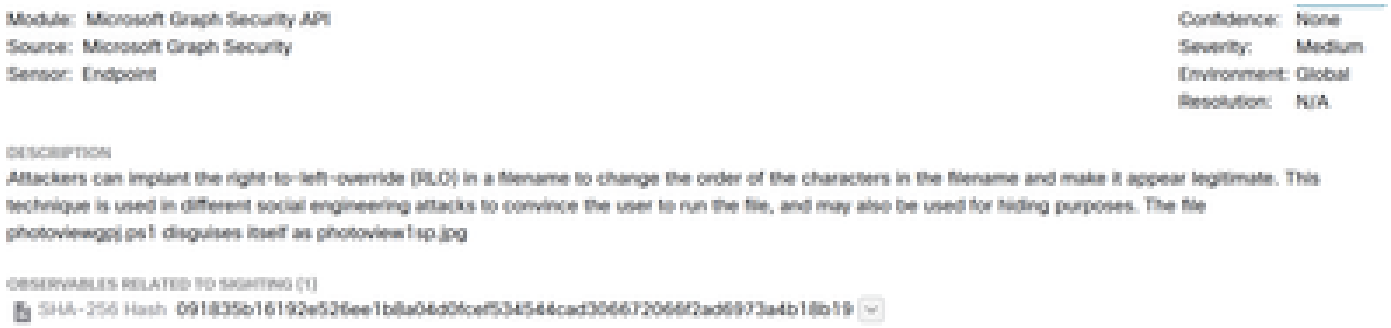
Überprüfung

Sie können diesen Link verwenden: Microsoft Graph Sicherheit Snapshots für eine Liste von Snapshots, die Ihnen helfen zu verstehen, die Antwort, die Sie von jeder Art von beobachtbaren erhalten können.

Sie können ein Beispiel sehen, wie in der folgenden Abbildung dargestellt:



Erweitern Sie das Fenster, können Sie die Informationen sehen, die durch die Integration bereitgestellt werden:



Beachten Sie, dass Daten in Ihrem Azure-Portal vorhanden sein müssen, und die Graph-API funktioniert besser, wenn sie mit anderen Microsoft-Lösungen verwendet wird. Dies muss jedoch vom Microsoft Support validiert werden.

Fehlerbehebung

- Meldung "Autorisierung fehlgeschlagen":
    - Stellen Sie sicher, dass die Werte für **Tenant ID** und Client ID korrekt sind und dass sie weiterhin gültig sind.

- Keine Daten werden in der Untersuchung angezeigt:
    - Stellen Sie sicher, dass Sie die entsprechenden Werte für **Tenant ID** und **Client ID**kopiert und eingefügt haben.
    - Stellen Sie sicher, dass Sie die Informationen aus dem Feld **Value** aus dem Certificates & Secrets Abschnitt verwendet haben.
    - Verwenden Sie WebDeveloper-Tools, um festzustellen, ob die Graph-API bei einer Untersuchung abgefragt wird.
    - Wenn die Graph-API Daten von verschiedenen Microsoft-Warnungsanbietern zusammenführt, stellen Sie sicher, dass OData für die Abfragefilter unterstützt wird. (z. B. Office 365 Security and Compliance und Microsoft Defender ATP).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.