Microsoft Graph API-integratie configureren met Cisco XDR

Inhoud

Inleiding

Voorwaarden

Integratiestappen

Onderzoeken uitvoeren

Verifiëren

Problemen oplossen

Inleiding

Dit document beschrijft de procedure voor het integreren van Microsoft Graph API met Cisco XDR en het type gegevens dat kan worden opgevraagd.

Voorwaarden

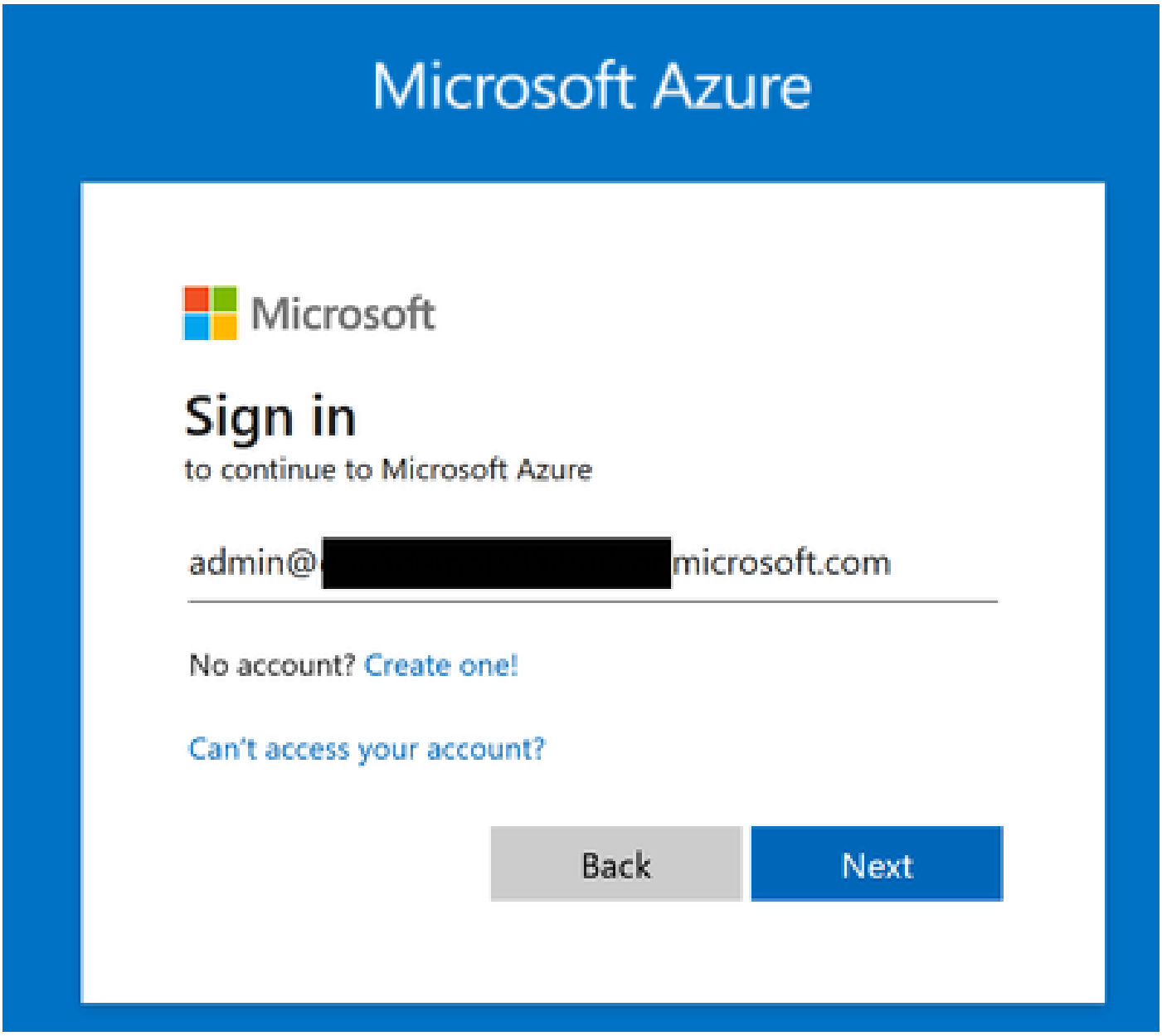
- Cisco XDR Admin-account
- Microsoft Azure-systeembeheerderaccount
- Toegang tot Cisco XDR

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Integratiestappen

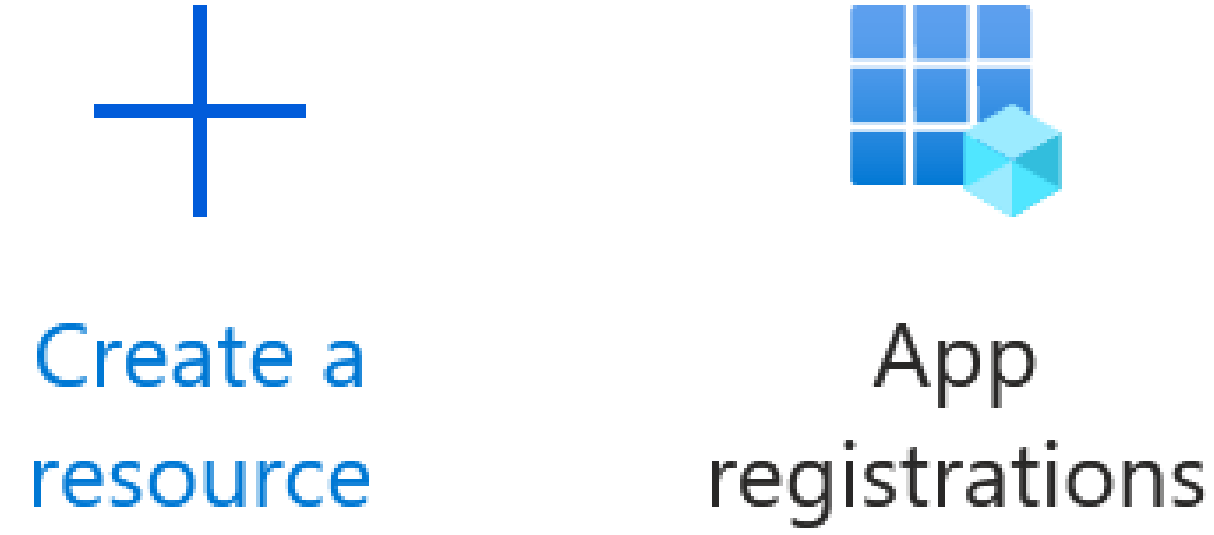
Stap 1.

Log in in Microsoft Azure als systeembeheerder.



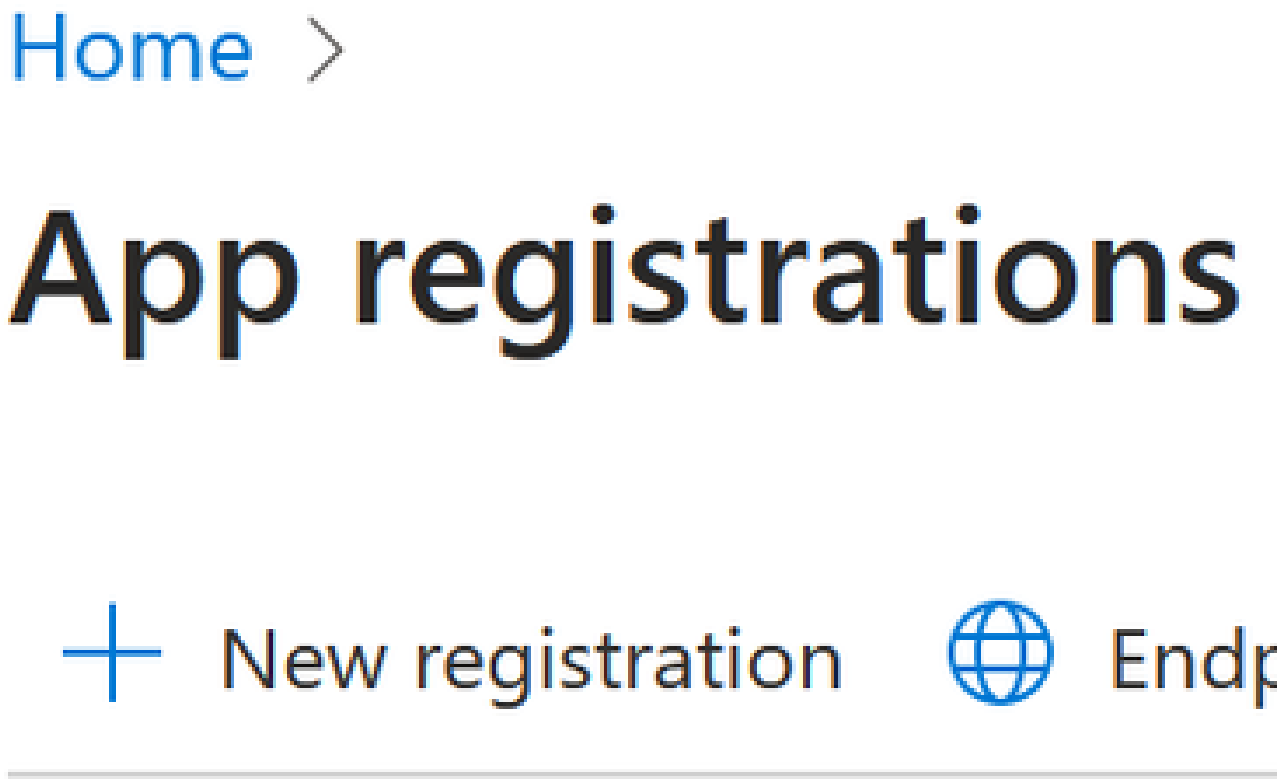
Stap 2.

Klik **App Registrations** op het Azure-serviceportal.



Stap 3.

Klik op de knop .New registration



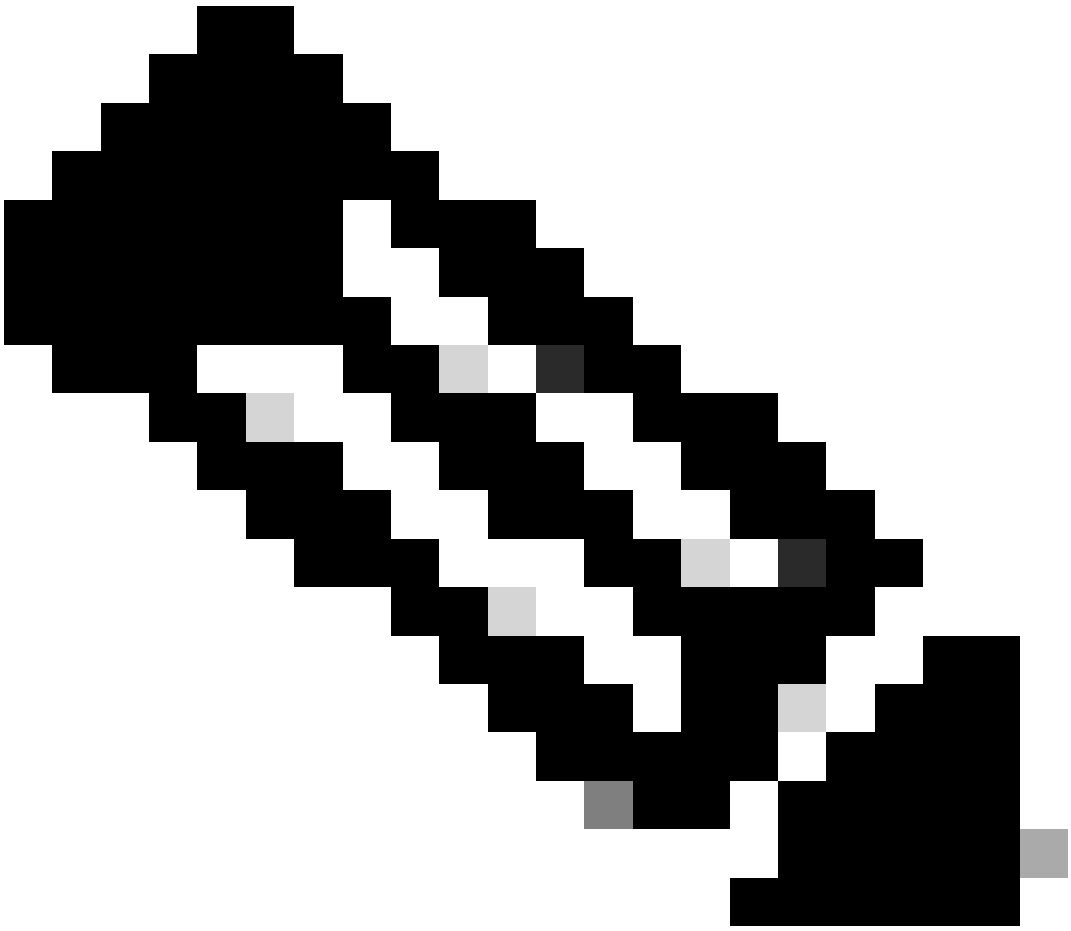
Stap 4.

Typ een naam om uw nieuwe app te identificeren.

* Name

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

SecureX - Graph API



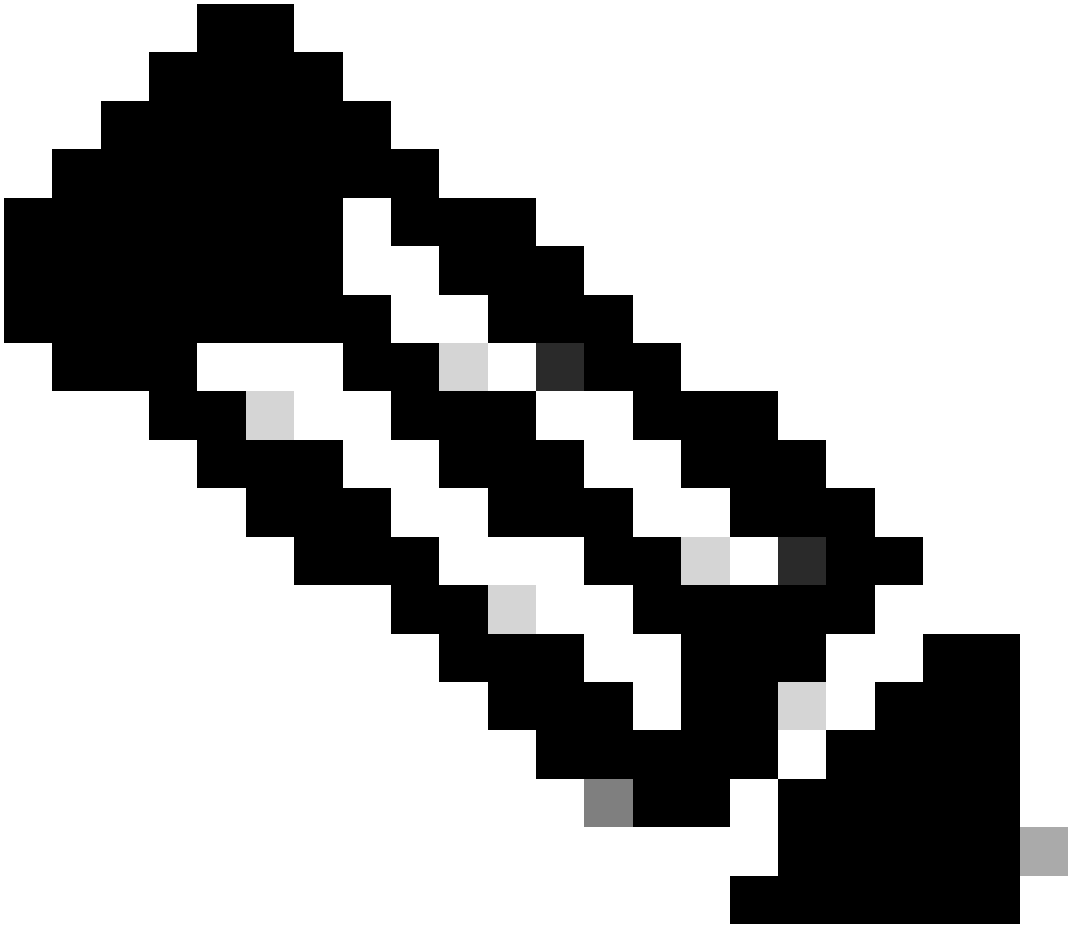
Opmerking: als de naam geldig is, wordt een groen vinkje weergegeven.

Kies de optie voor ondersteunde accounttypen **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



Opmerking: u hoeft geen Redirect URI te typen.

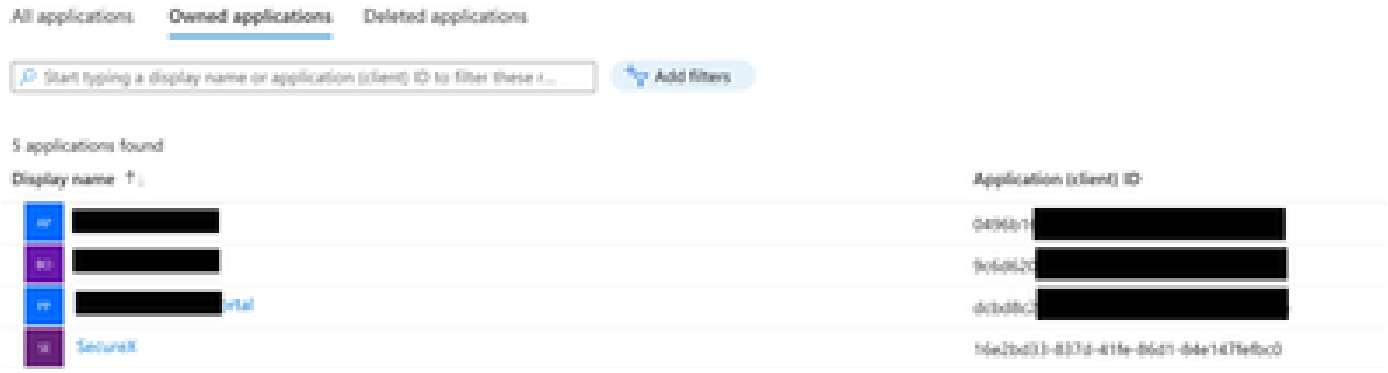
Stap 5.

Blader naar de onderkant van het scherm en klik op **Register**.

Stap 6.

Ga terug naar de Azure-servicepagina, klik op App Registrations > Owned Applications.

Identificeer uw app en klik op de naam. In dit voorbeeld is het dat wel SecureX.



Stap 7.

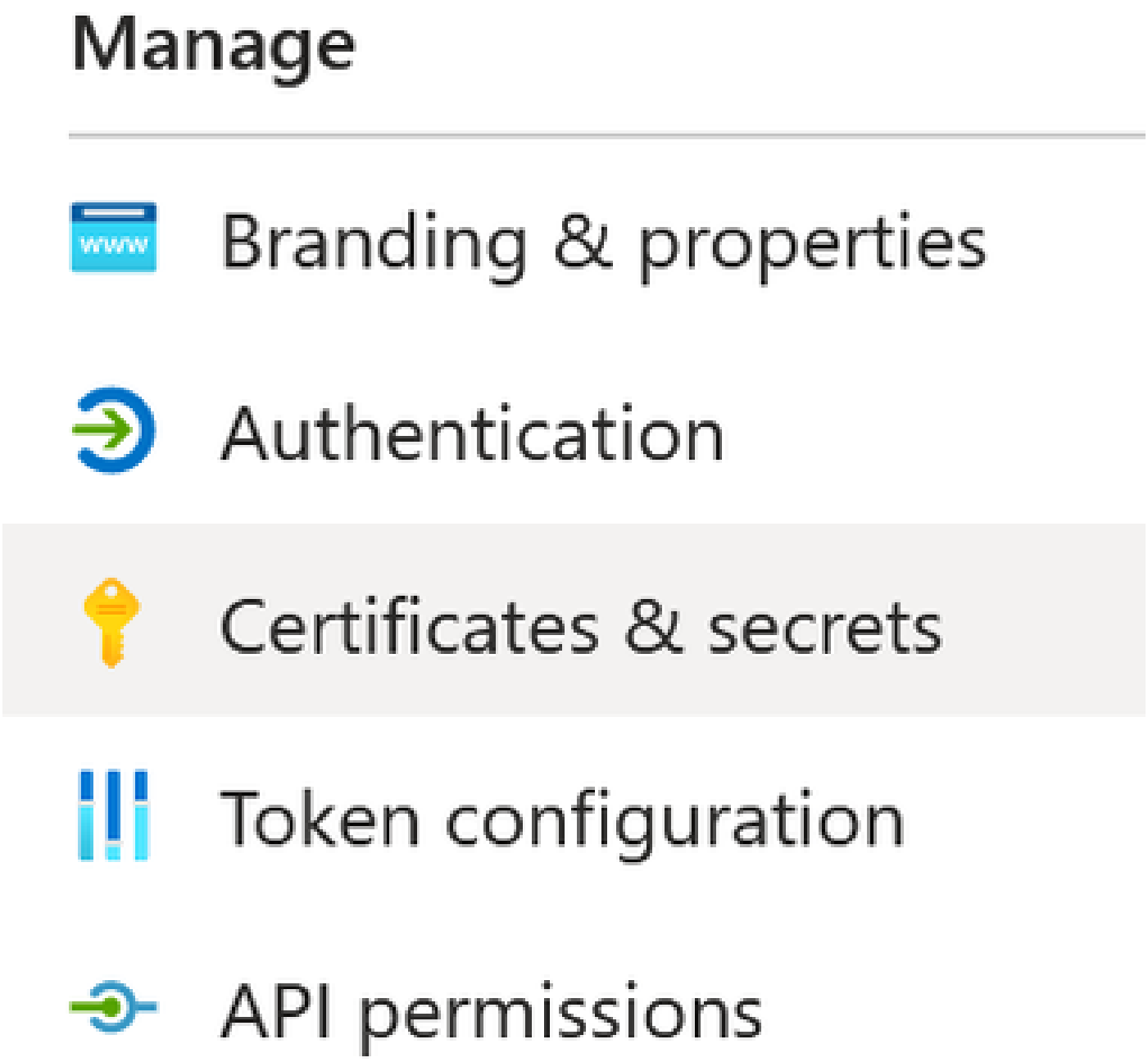
Er wordt een samenvatting van uw app weergegeven. Gelieve deze relevante gegevens te vermelden:

Applicatie (client)-ID:

Directory (tenant) ID:

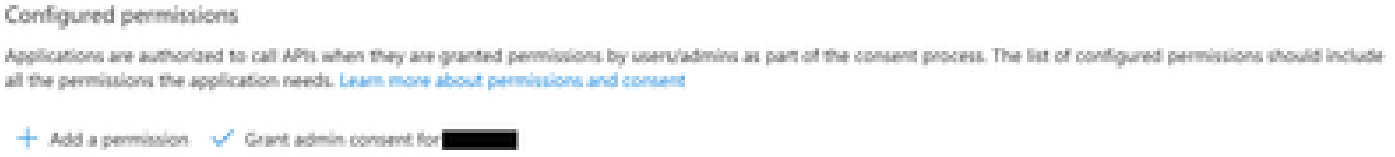
Stap 8.

Navigeer naar Manage Menu > API Permissions.



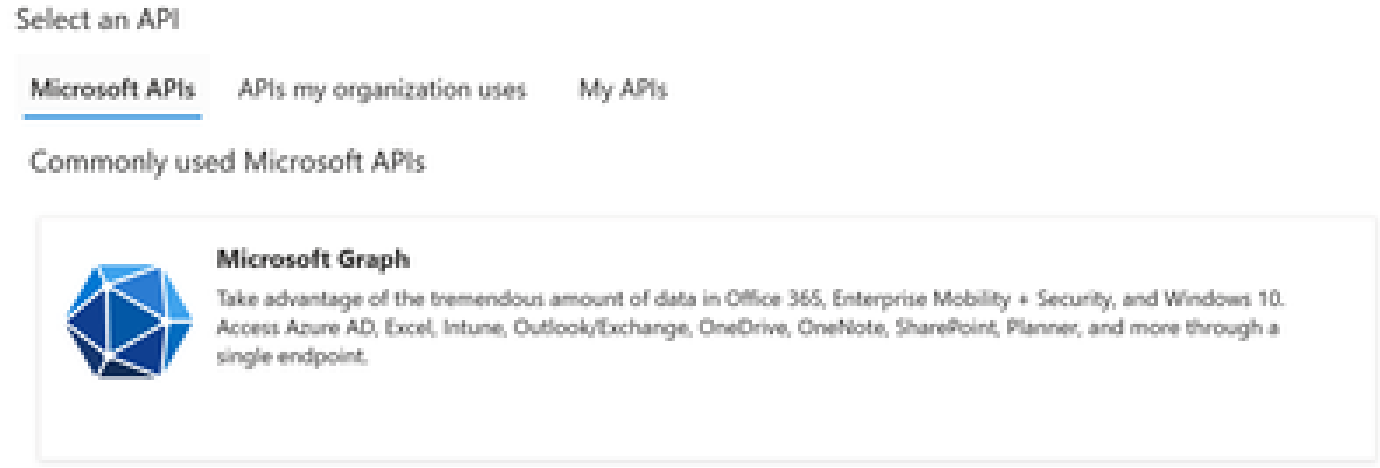
Stap 9.

Klik onder Configureerde toegangsrechten op Add a Permission.



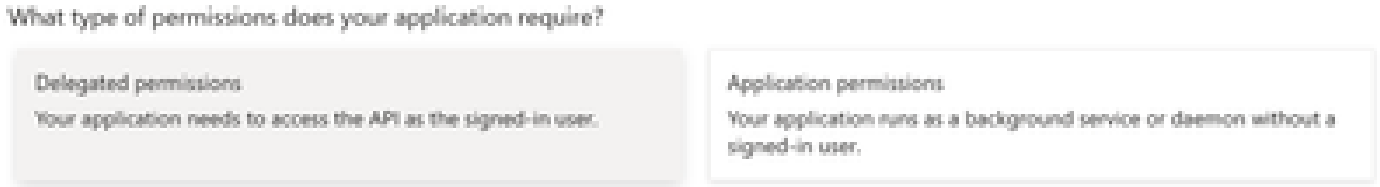
Stap 10.

Klik in de sectie API-toegangsrechten aanvragen op **Microsoft Graph**.



Stap 11.

Selecteer Application permissions.



In de zoekbalk, zoek naar Security. Uitvouwen **Security Actions** en selecteren

- **Read.All**
- **ReadWrite.All**

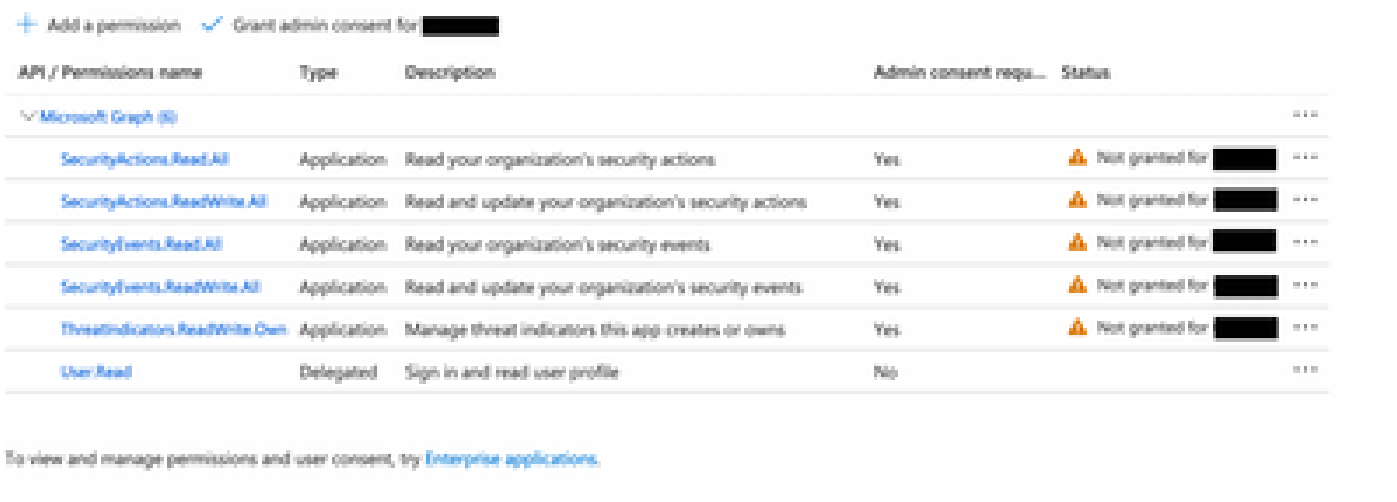
- **Security Events** en selecteer
  - **Read.All**
  - **ReadWrite.All**

- **Bedreigingsindicatoren** en selecteer
  - **ThreatIndicators.readWrite.OwnedBy**

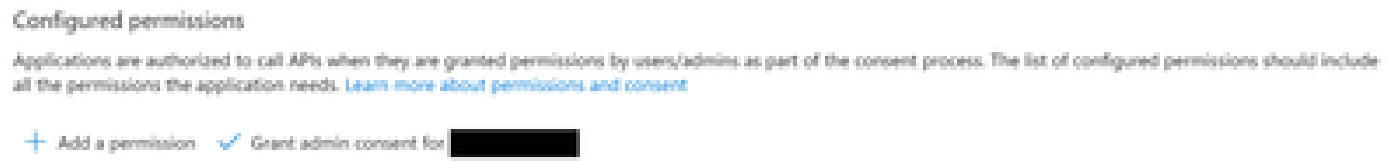
Klik op de knop .Add permissions

Stap 12.

Controleer de geselecteerde rechten.

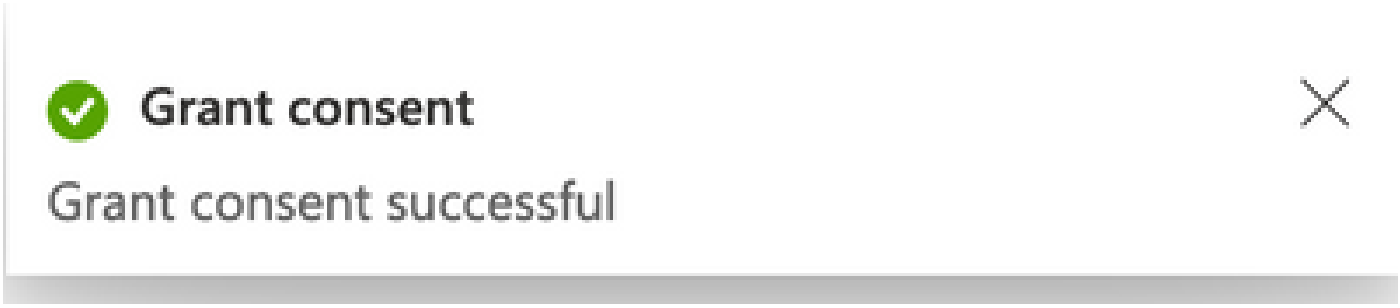


Klik **Grant Admin consent** voor uw organisatie.



Er verschijnt een prompt om te kiezen of u toestemming wilt verlenen voor alle machtigingen. Klik op de knop .Yes

Er verschijnt een soortgelijk popup zoals in deze afbeelding:



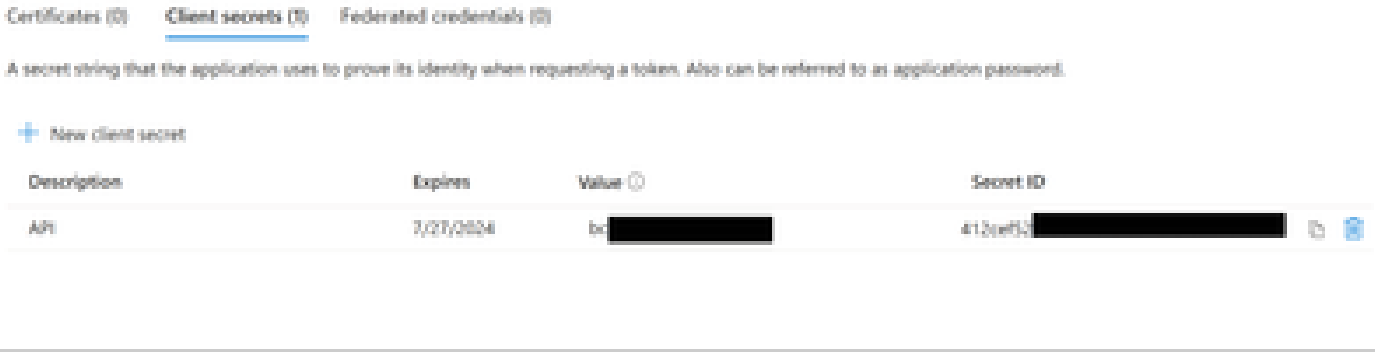
Stap 13.

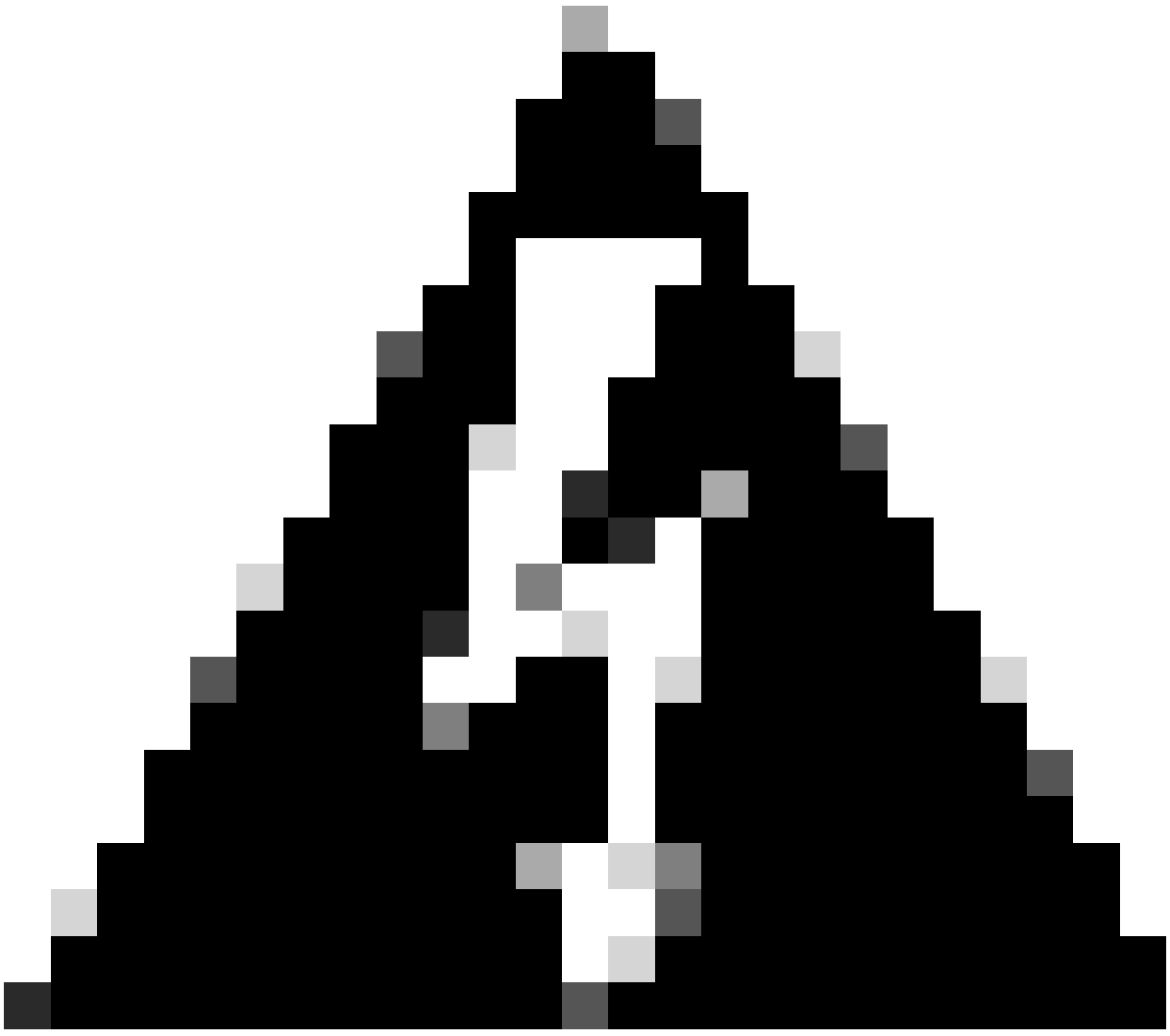
Navigeer naar Manage > Certificates & Secrets.

Klik op de knop .Add New Client Secret

Schrijf een korte beschrijving en selecteer een geldige Expires datum. Er wordt voorgesteld om een geldigheidsdatum van meer dan 6 maanden te selecteren om te voorkomen dat de API-sleutels verlopen.

Zodra gemaakt, kopieer en bewaar op een veilige plaats het deel dat zegt **Value**, zoals het wordt gebruikt voor de integratie.





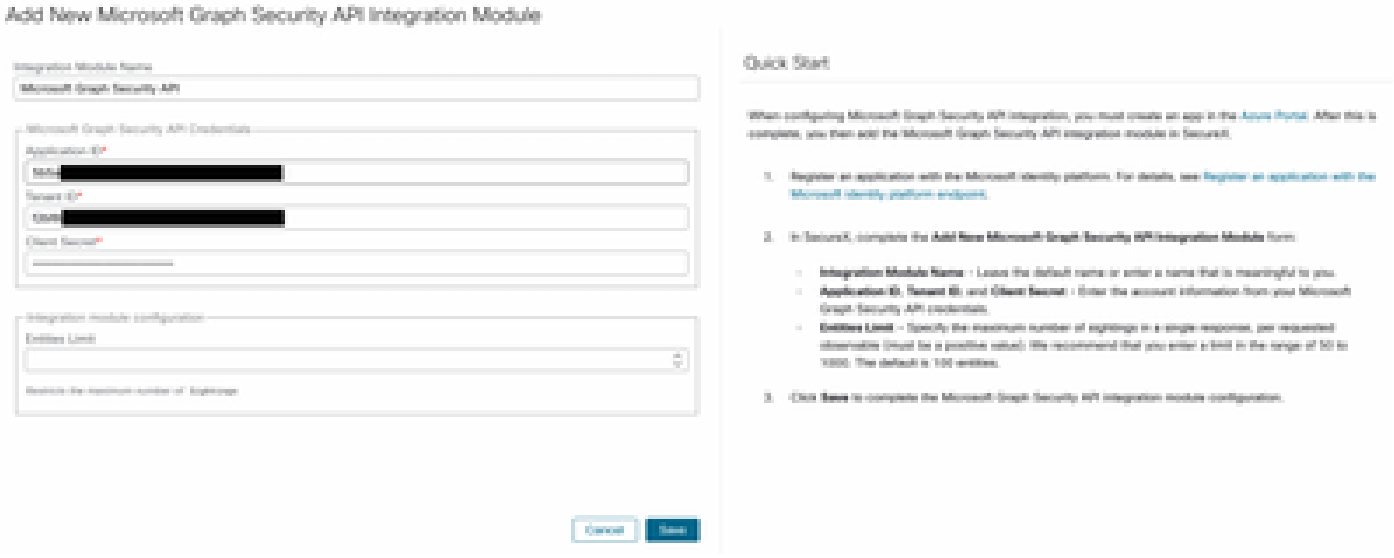
Waarschuwing: dit veld kan niet worden hersteld en u moet een nieuw geheim maken.

Zodra u over alle informatie beschikt, navigeer naar **Overview** en kopieer de waarden van uw App. Navigeer dan naar SecureX.

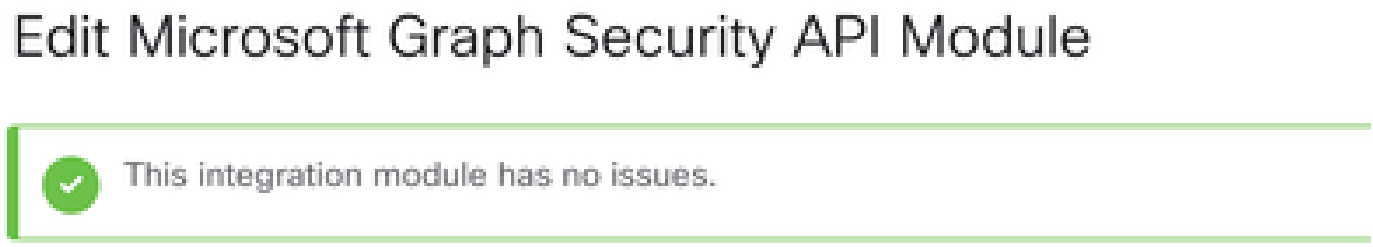
Stap 14.

Navigeer om te Integration Modules > Available Integration Modules > selecteren Microsoft Security Graph API, klik Add.

Wijs een naam toe en plak de waarden die u uit de Azure-portal hebt gekregen.



Klik op Save en wacht tot de gezondheidscontrole is geslaagd.



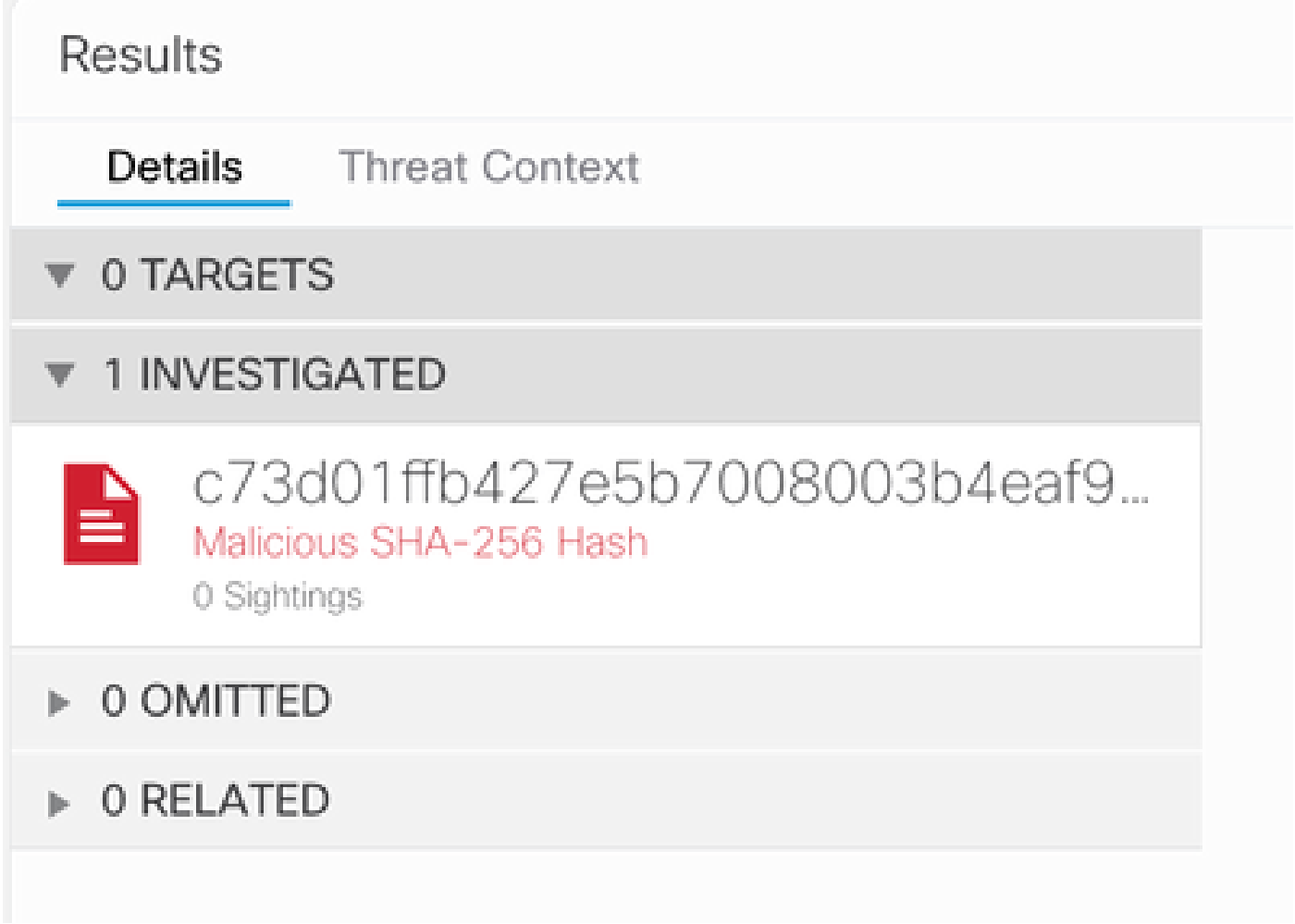
Onderzoeken uitvoeren

Op dit moment wordt het Cisco XDR Dashboard niet bevolkt door een timer met Microsoft Security Graph API. In plaats daarvan kan de informatie van uw Azure-portal worden opgevraagd bij het gebruik van Onderzoeken.

Houd in gedachten, de Grafiek API kan alleen worden opgevraagd voor:

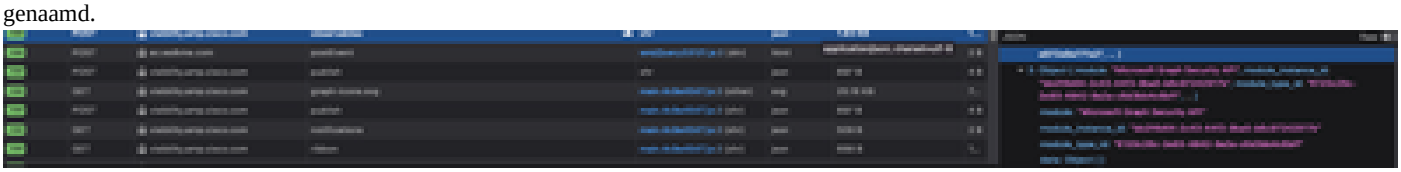
- ip
- domein
- hostnaam
- url
- bestand_naam
- bestand_pad
- sha256

In dit voorbeeld werd bij het onderzoek gebruik gemaakt van deze SHA c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148.



Zoals u kunt zien, heeft het 0 Sightings in de Lab Environment, dus hoe te testen als Grafiek API werkt?

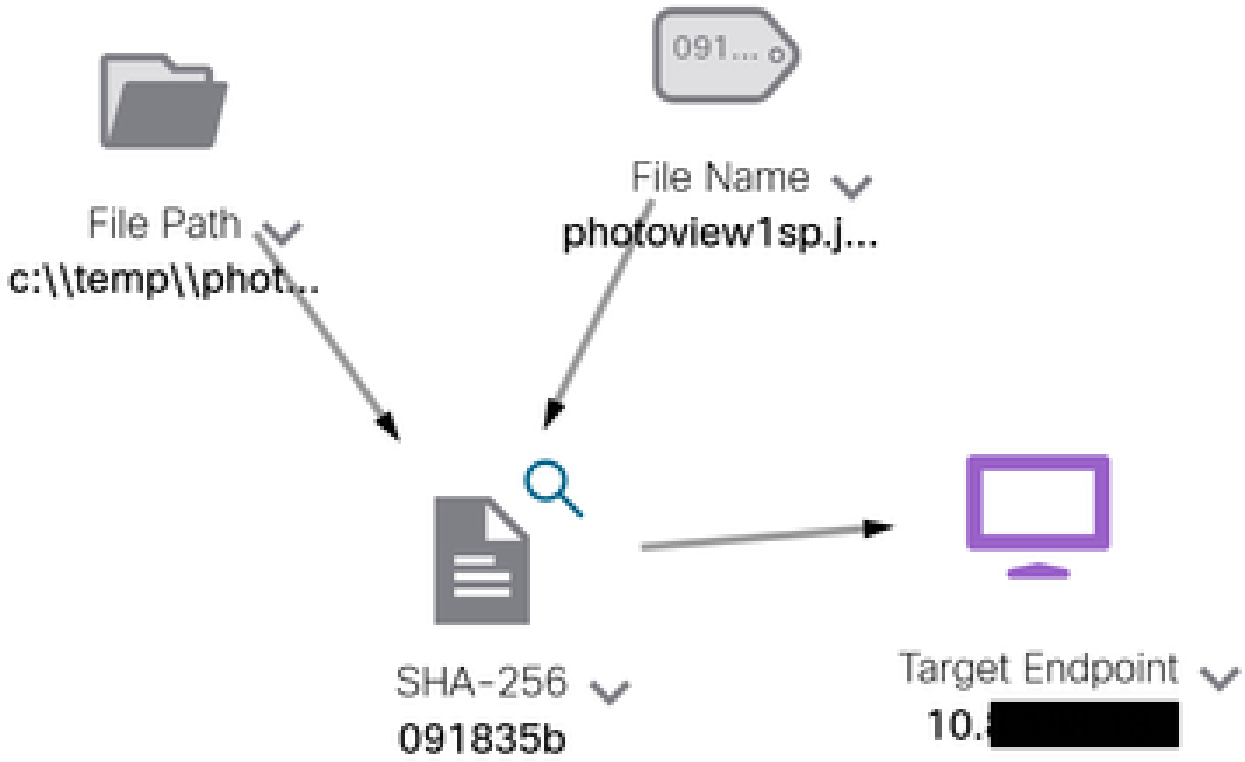
Open de WebDeveloper Tools, voer het onderzoek uit, vind een Post Event naar **zichtbaarheid.amp.cisco.com** het bestand Observables genaamd.



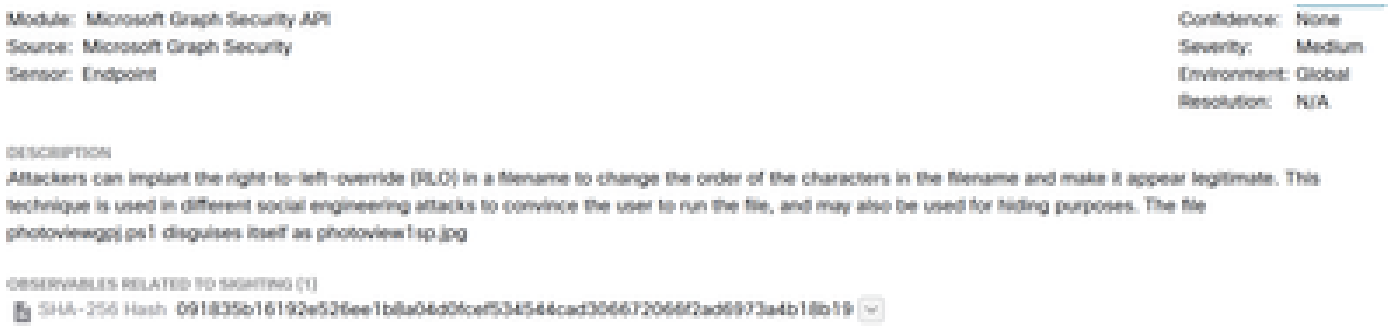
Verifiëren

U kunt deze link gebruiken: Microsoft grafiek security Snapshots voor een lijst van snapshots die u helpen om de respons te begrijpen die u kunt krijgen van elk type waarneembaar.

U kunt een voorbeeld zien zoals in deze afbeelding:



Breid het venster uit, kunt u de informatie zien die door de integratie wordt verstrekt:



Houd in gedachten dat gegevens moeten bestaan in uw Azure-portal, en Graph API werkt beter bij gebruik met andere Microsoft-oplossingen. Dit moet echter worden gevalideerd door Microsoft Support.

Problemen oplossen

- Bericht autorisatie is mislukt:
    - Zorg ervoor dat de waarden voor **Tenant ID** en Client ID correct zijn en nog steeds geldig zijn.

- Geen gegevens tijdens onderzoek:
    - Zorg ervoor dat u de juiste waarden voor **Tenant ID** en **Client ID**hebt gekopieerd en geplakt.
        - Zorg ervoor dat u de informatie uit het veld **Value** uit de Certificates & Secrets sectie hebt gebruikt.
        - Gebruik WebDeveloper tools om te bepalen of de Graph API wordt gevraagd wanneer er een onderzoek plaatsvindt.
        - Aangezien de Grafiek API gegevens van diverse Microsoft waakzame leveranciers samenvoegt, zorg ervoor dat OData voor de vraagfilters wordt gesteund. (Bijvoorbeeld Office 365 Security and Compliance en Microsoft Defender ATP).

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.