Configurazione dell'integrazione dell'API di Microsoft Graph con Cisco XDR

Sommario

Introduzione

Questo documento descrive la procedura per integrare l'API di Microsoft Graph con Cisco XDR e il tipo di dati su cui è possibile eseguire una query.

Prerequisiti

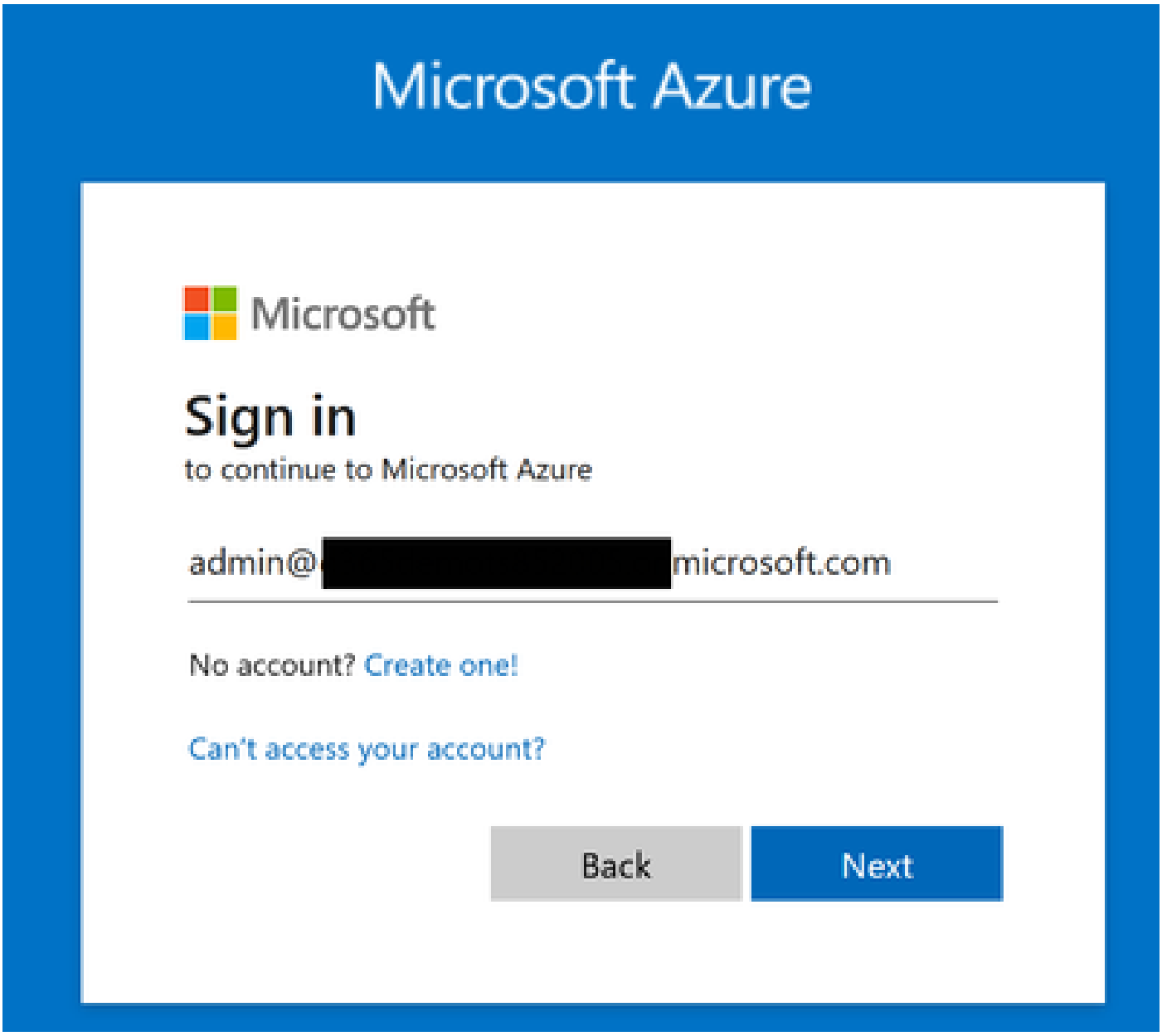
- Account Cisco XDR Admin
- Account amministratore di sistema di Microsoft Azure
- Accesso a Cisco XDR

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Fasi di integrazione

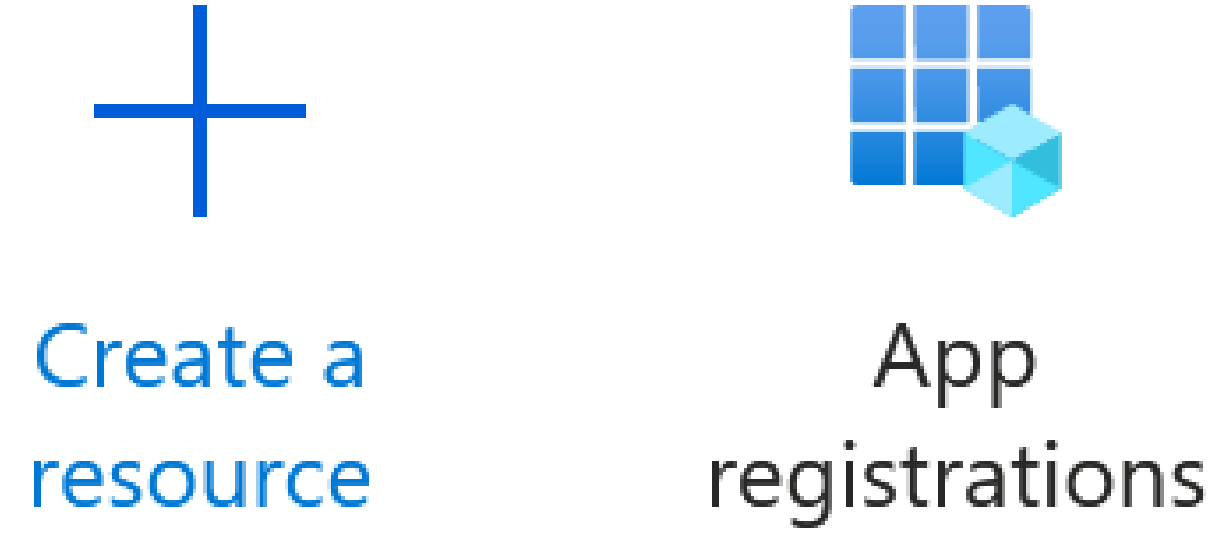
Passaggio 1.

Accedere a Microsoft Azure come amministratore di sistema.



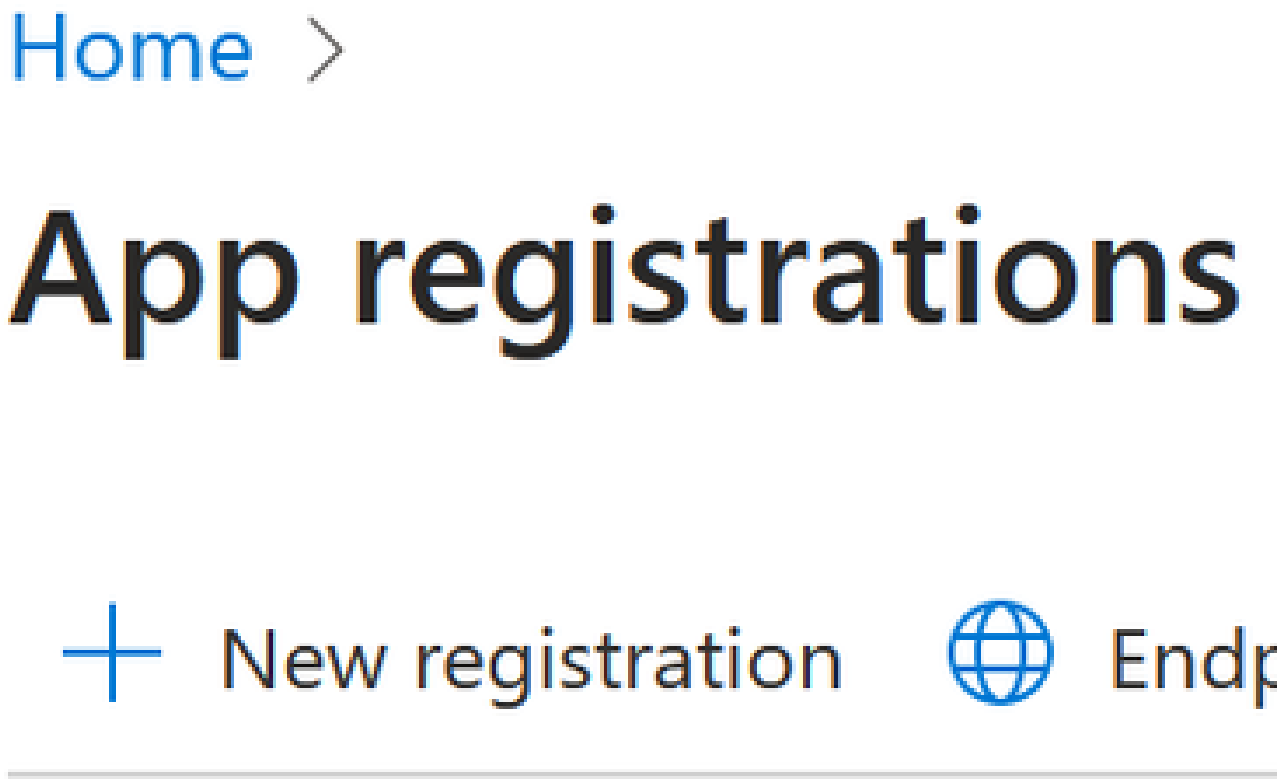
Passaggio 2.

Fare clic **App Registrations** sul portale dei servizi di Azure.



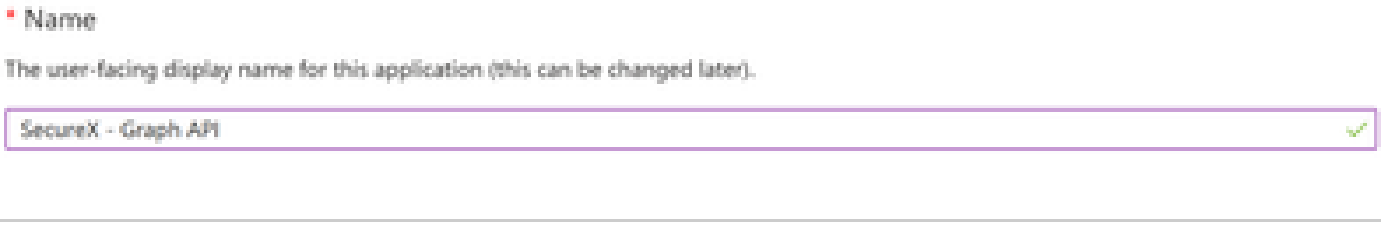
Passaggio 3.

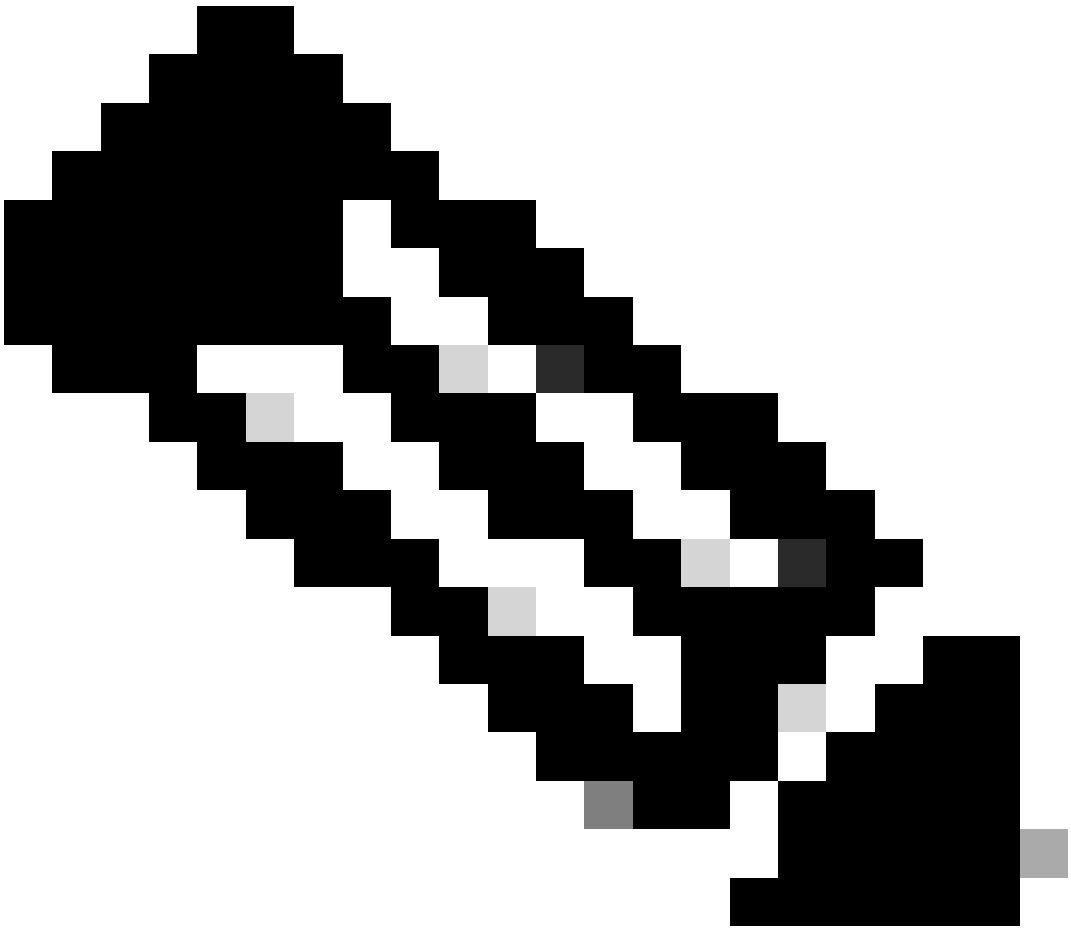
Fare clic su .New registration



Passaggio 4.

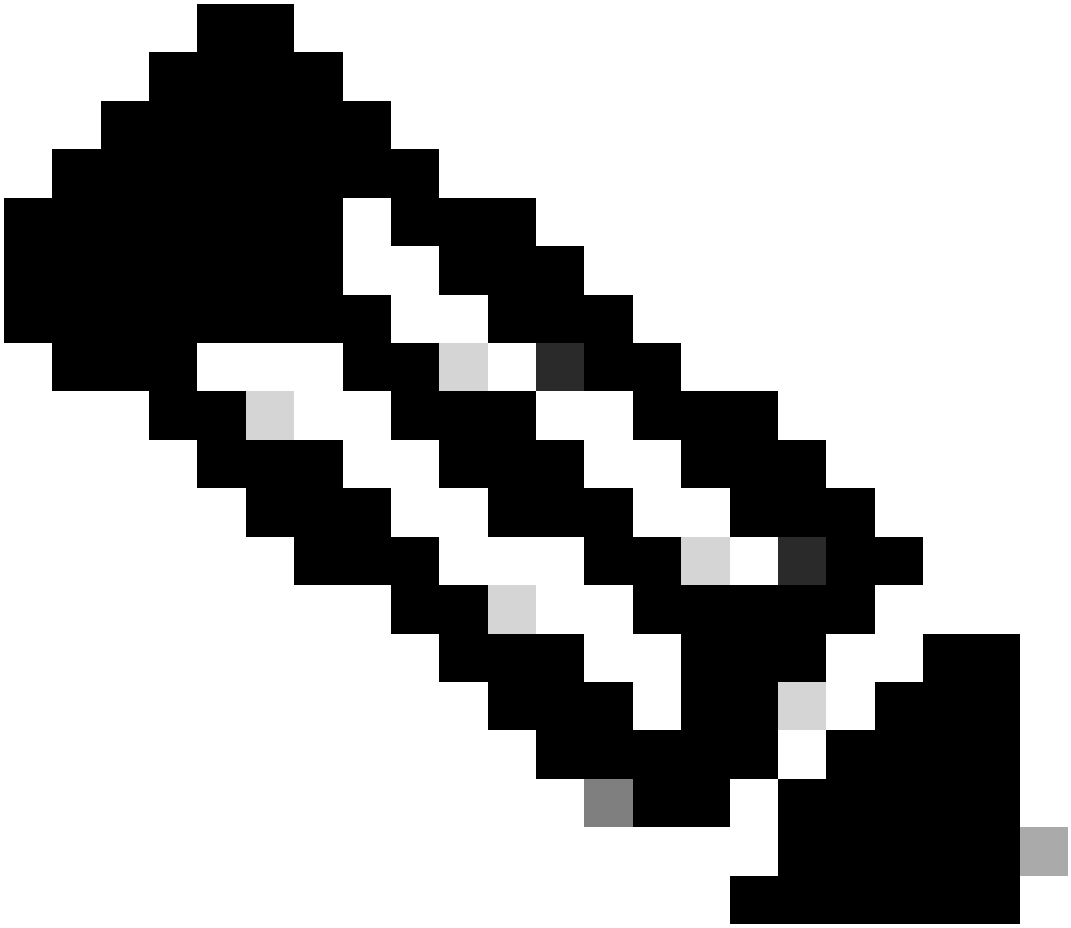
Digitare un nome per identificare la nuova app.





Nota: se il nome è valido, viene visualizzato un segno di spunta verde.

In Tipi di conto supportati, scegliere l'opzione **Accounts in this organizational directory only**.



Nota: non è necessario digitare un URI di reindirizzamento.

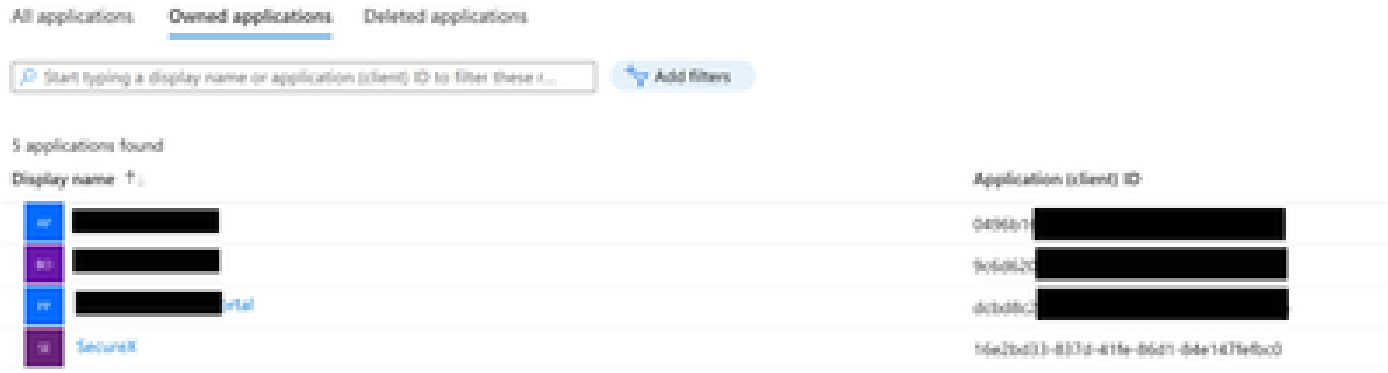
Passaggio 5.

Scorrere fino alla parte inferiore dello schermo e fare clic su **Register**.

Passaggio 6.

Tornare alla pagina dei servizi di Azure e fare clic su App Registrations > Owned Applications.

Identificare l'app e fare clic sul nome. Nell'esempio, questo valore è SecureX.



Passaggio 7.

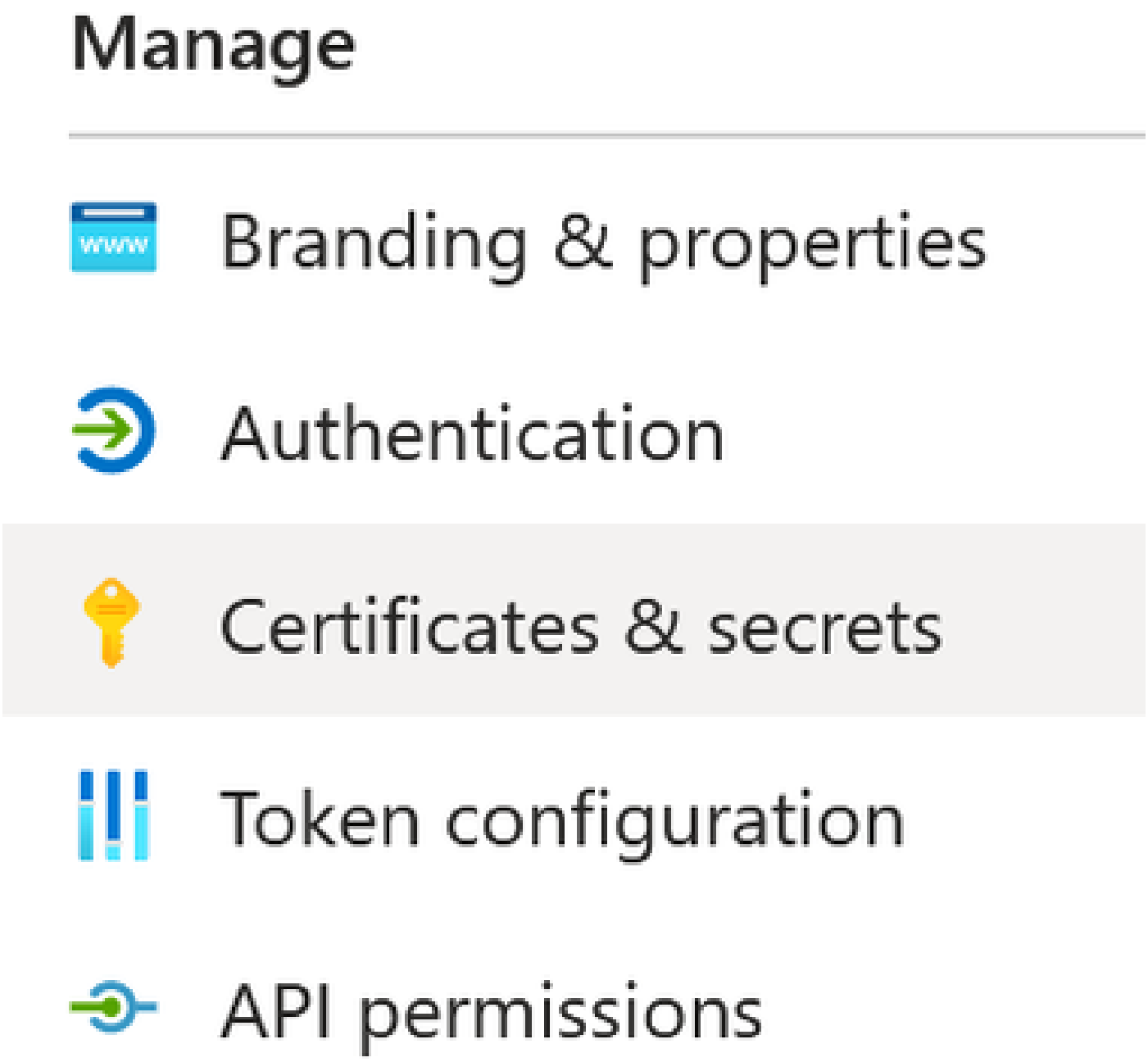
Verrà visualizzato un riepilogo dell'app. Indicare le informazioni pertinenti:

ID applicazione (client):

ID directory (tenant):

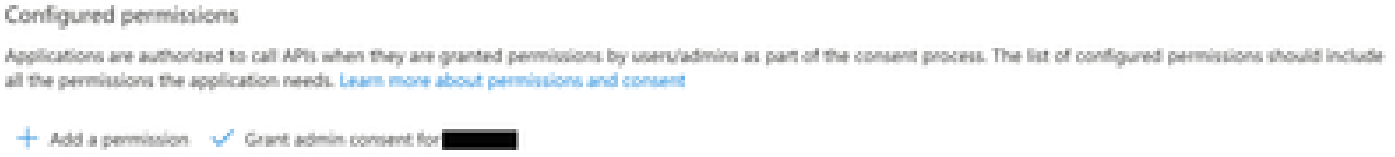
Passaggio 8.

Passare a Manage Menu > API Permissions.



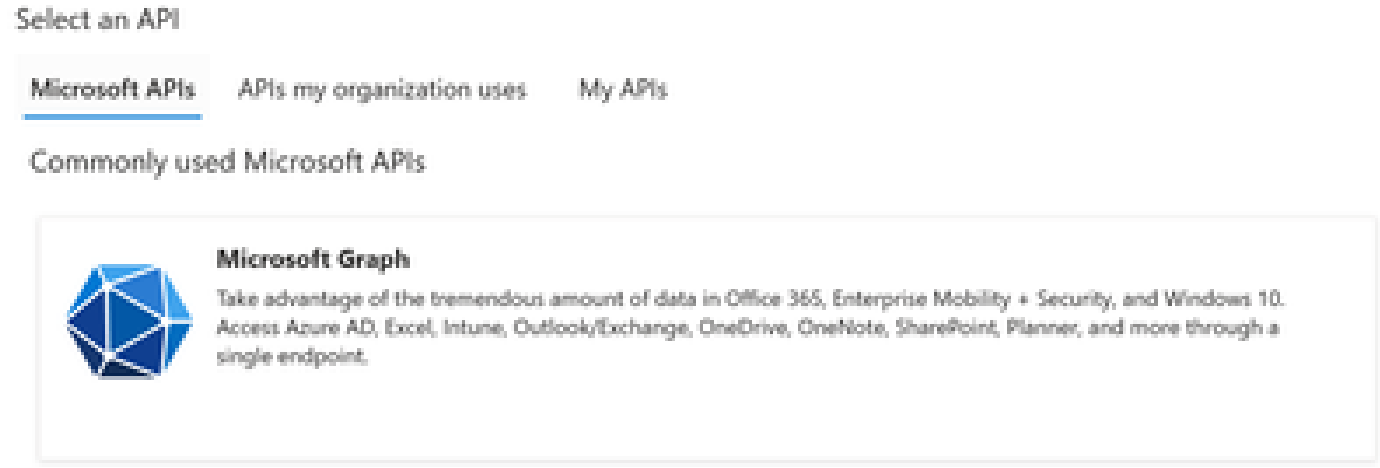
Passaggio 9.

In Autorizzazioni configurate fare clic su Add a Permission.



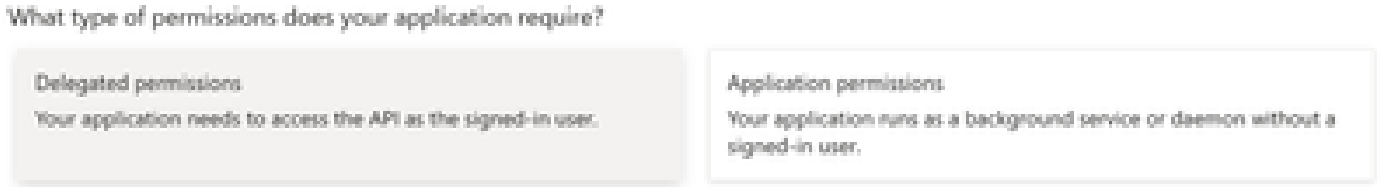
Passaggio 10.

Nella sezione Richiedi autorizzazioni API, fare clic su **Microsoft Graph**.



Passaggio 11.

Selezionare Application permissions.



Nella barra di ricerca, cercare Security. Espandi **Security Actions** e seleziona

- **Leggi.Tutto**
- **ReadWrite.All**

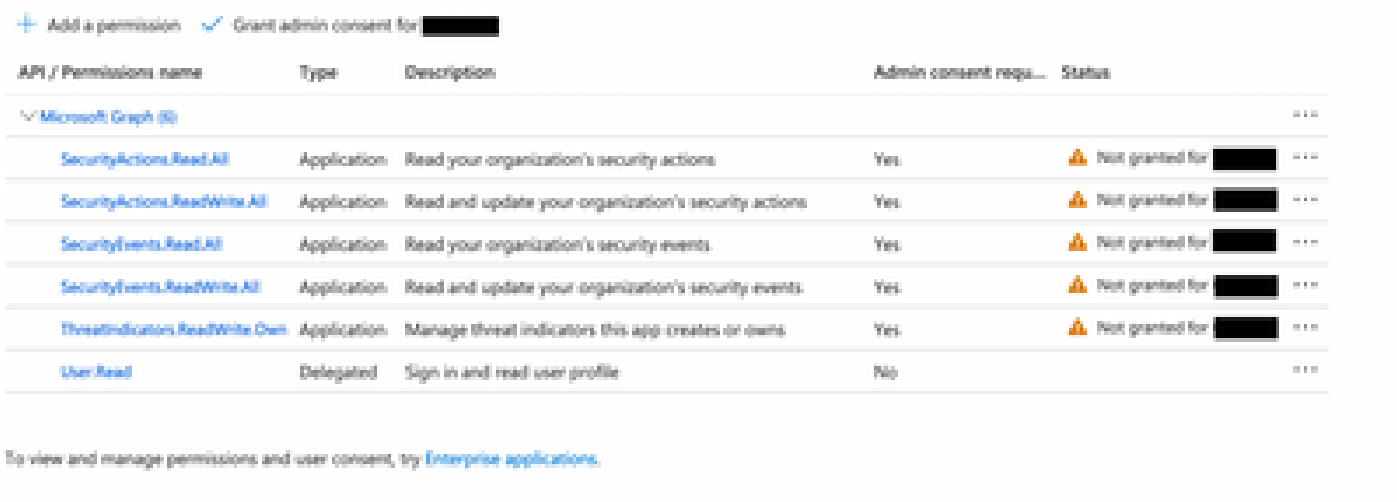
- **Eventi di protezione** e selezionare
  - **Leggi.Tutto**
  - **ReadWrite.All**

- **Indicatori di minaccia** e selezione
  - **IndicatoriMinacce.ReadWrite.OwnedBy**

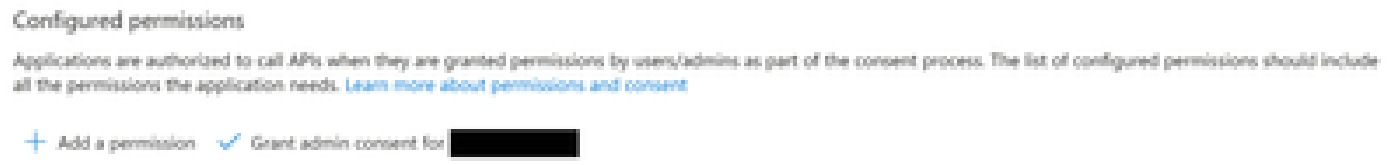
Fare clic su .Add permissions

Passaggio 12.

Rivedere le autorizzazioni selezionate.

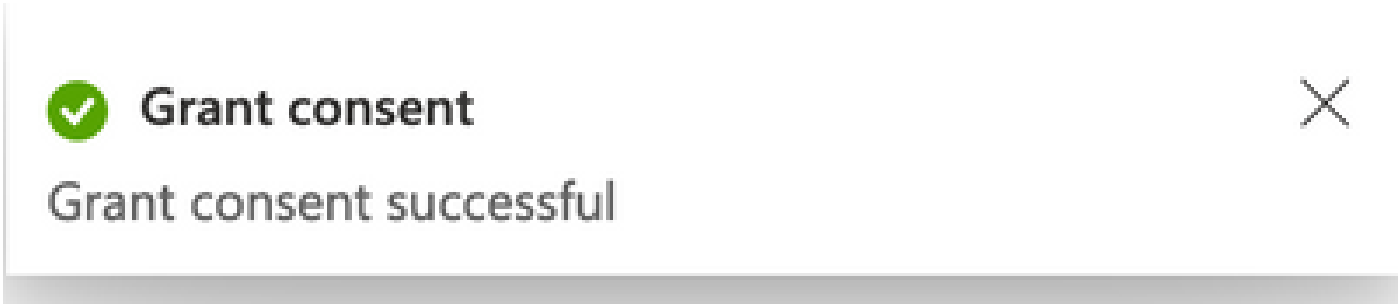


Fare clic su **Grant Admin consent** per l'organizzazione.



Viene visualizzato un prompt che richiede se si desidera concedere il consenso per tutte le autorizzazioni. Fare clic su .Yes

Viene visualizzato un popup simile a quello mostrato nell'immagine:



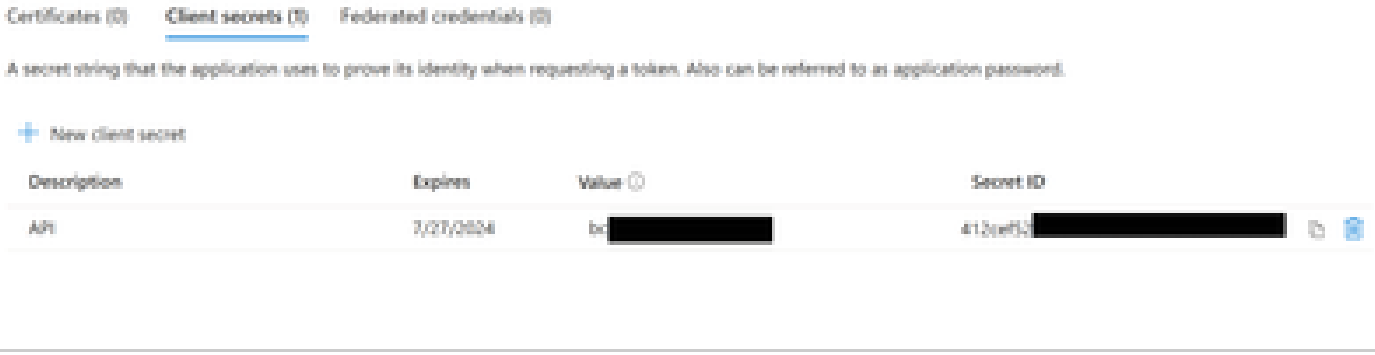
Passaggio 13.

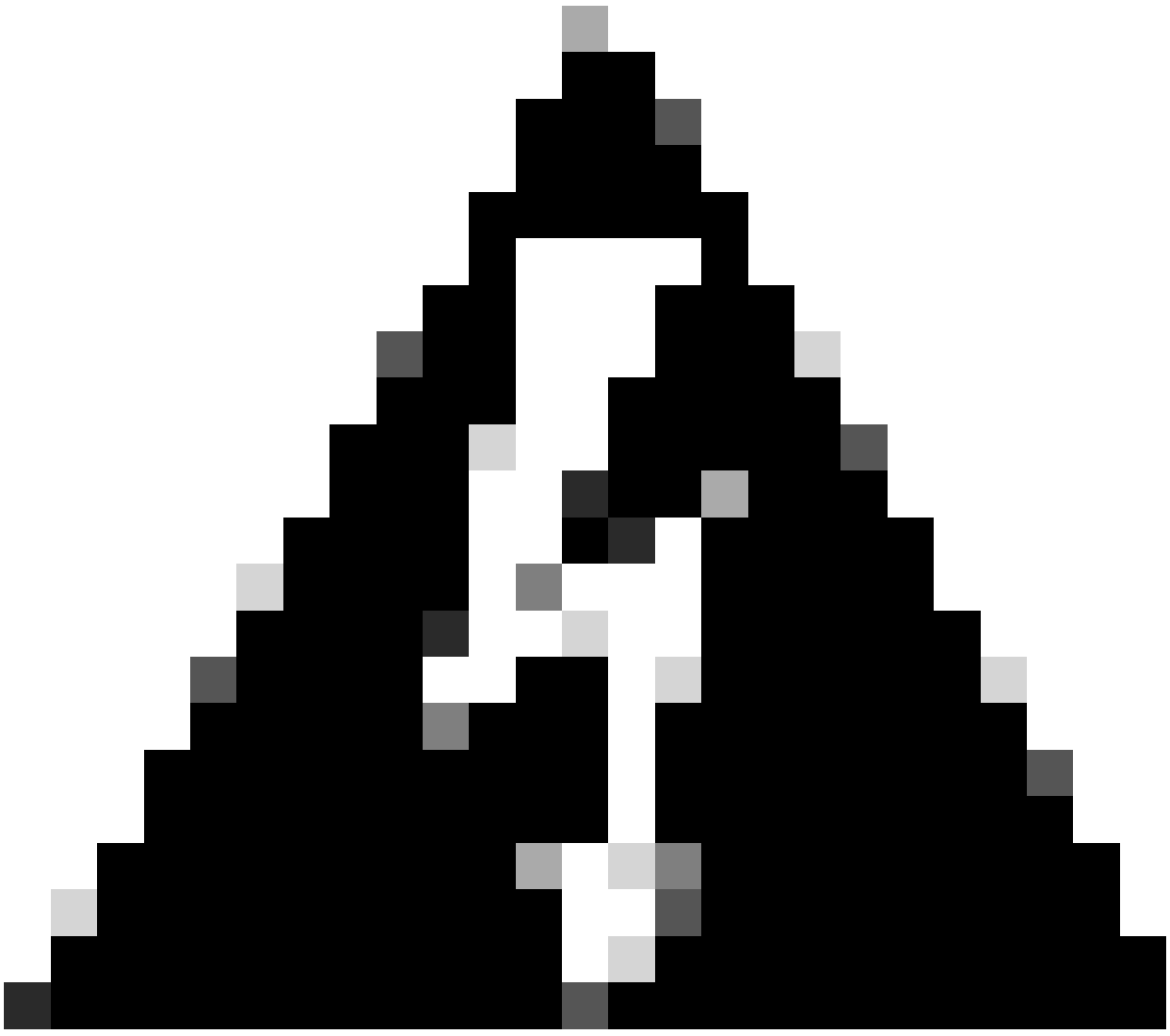
Passare a Manage > Certificates & Secrets.

Fare clic su .Add New Client Secret

Scrivere una breve descrizione e selezionare una data validaExpires. Si consiglia di selezionare una data di validità superiore a 6 mesi per evitare la scadenza delle chiavi API.

Una volta creata, copiare e conservare in un luogo sicuro la parte che dice **Value**, così come viene utilizzata per l'integrazione.





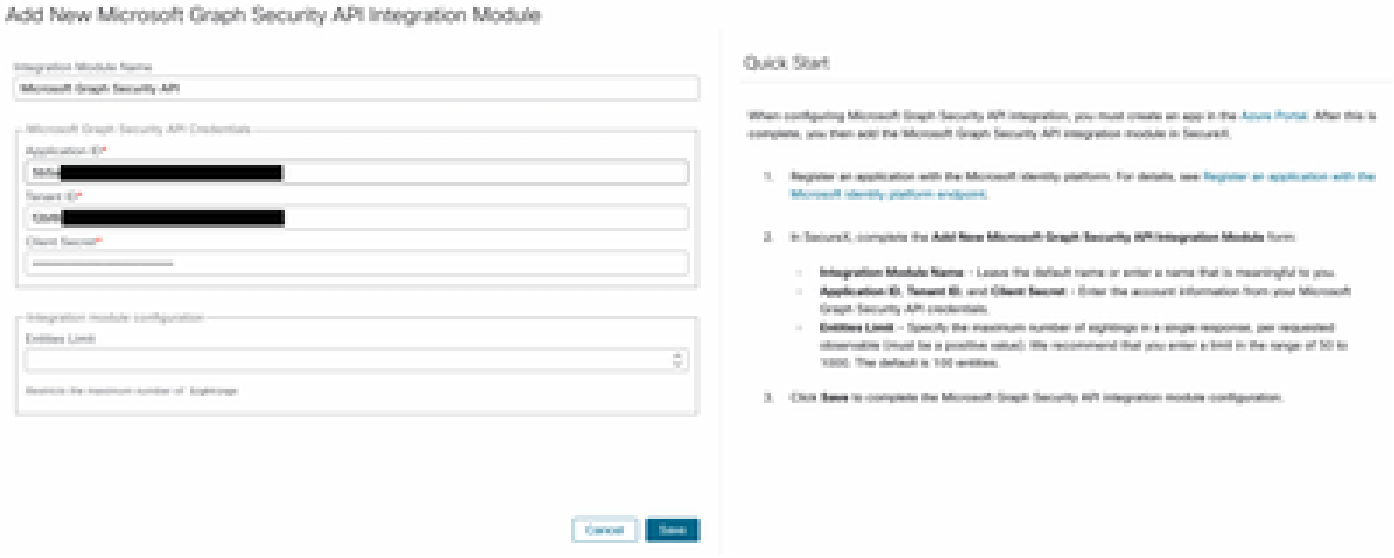
Avviso: questo campo non può essere recuperato ed è necessario creare un nuovo segreto.

Dopo aver ottenuto tutte le informazioni, tornare ai valori dell'App **Overview** e copiarli. Passare quindi a SecureX.

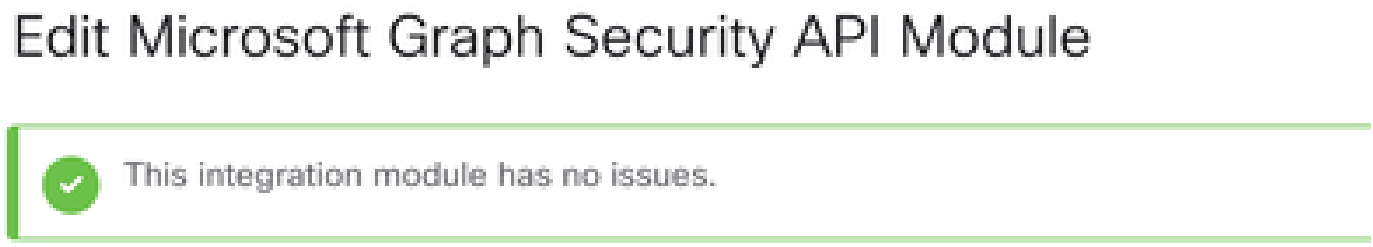
Passaggio 14.

Passare alla sezione Integration Modules > Available Integration Modules > SelezionaMicrosoft Security Graph API, quindi fare clic su Add.

Assegnare un nome e incollare i valori ottenuti dal portale di Azure.



Fare clic su Save e attendere il completamento del controllo di integrità.



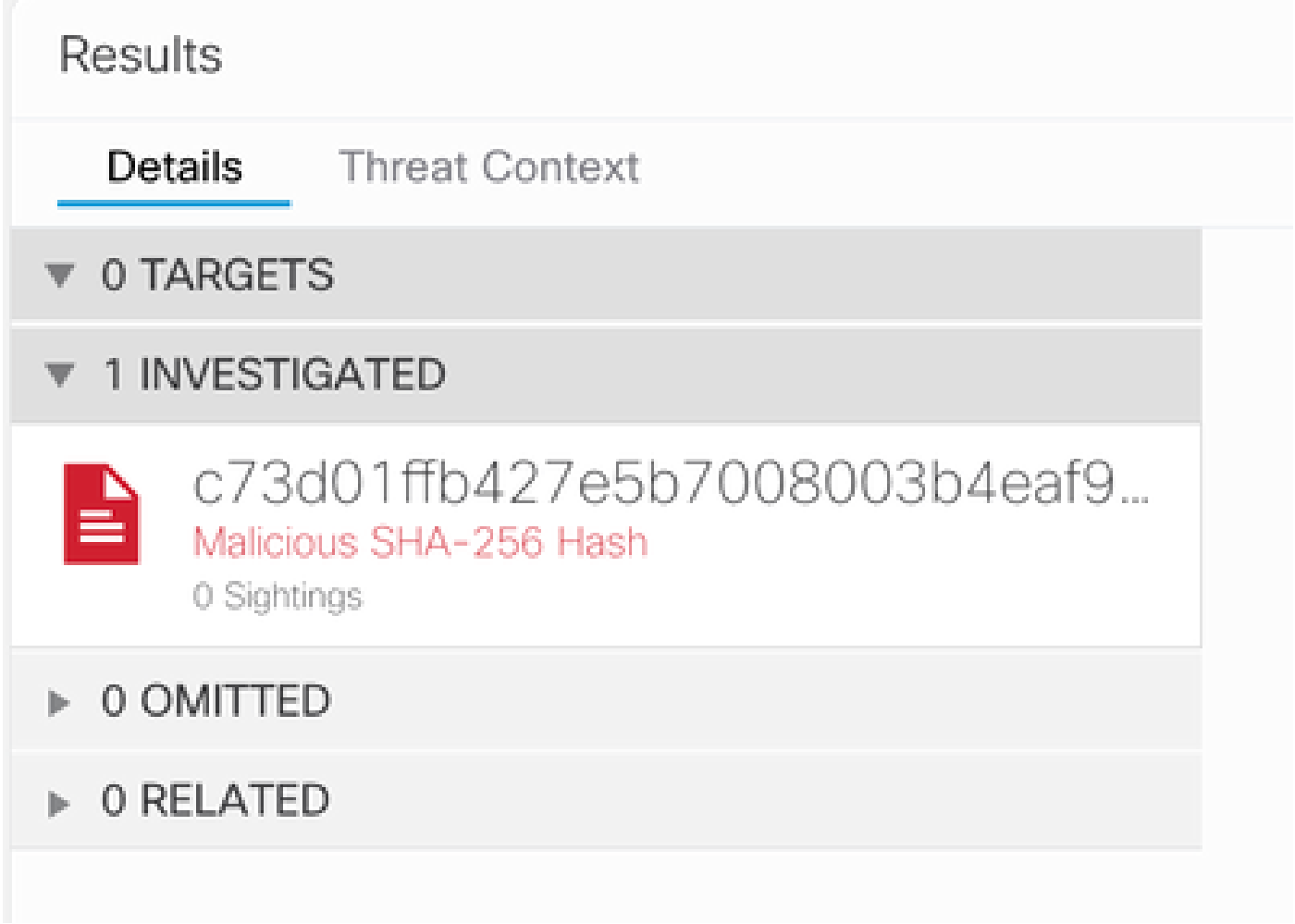
Esegui indagini

Al momento, l'API di Microsoft Security Graph non popola Cisco XDR Dashboard con una tessera. Le informazioni del portale di Azure possono invece essere richieste tramite le indagini.

Tenete presente che è possibile eseguire una query sull'API Graph solo per:

- ip
- dominio
- nome host
- url
- file
- percorso
- sha256

In questo esempio, l'indagine ha utilizzato questo Agente integrità sistema c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148.



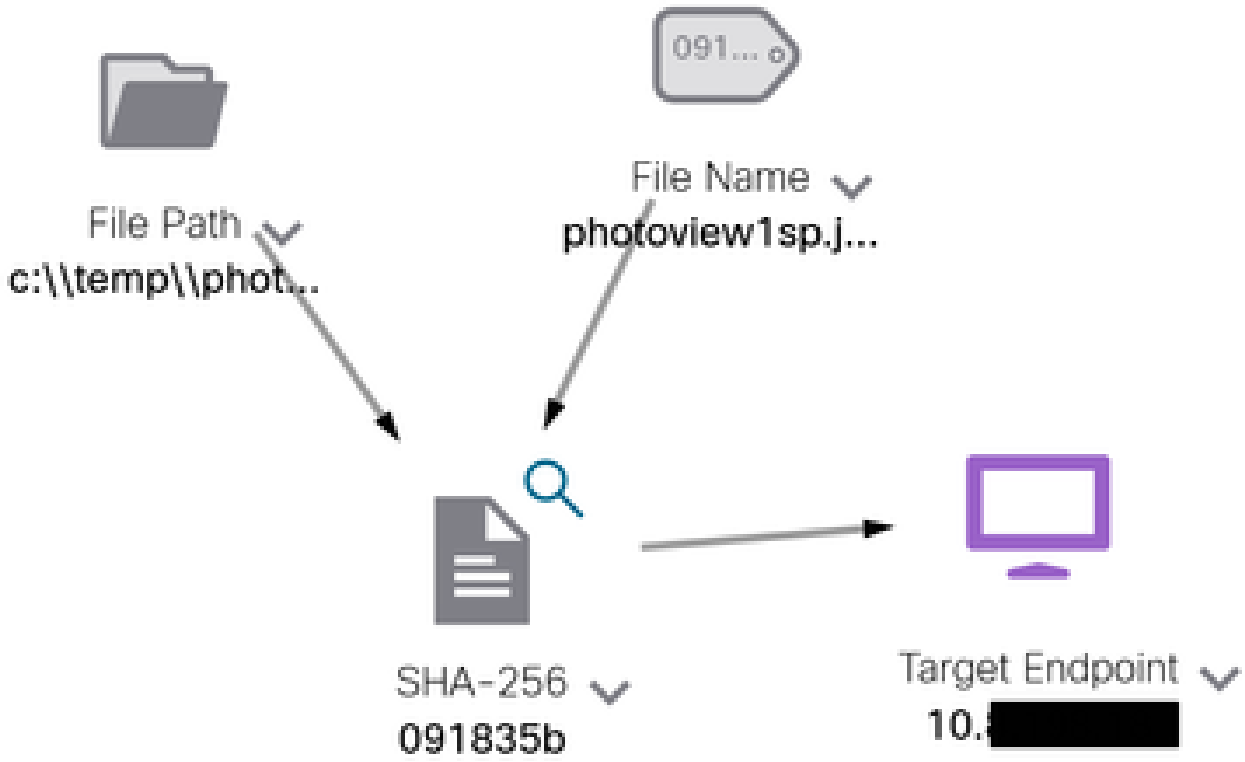
Come potete vedere, ha 0 Avvistamenti nell'ambiente Lab, quindi come verificare se l'API di Graph funziona?

Aprire WebDeveloper Tools, eseguire l'indagine, trovare un evento post per **visibility.amp.cisco.com** il file chiamato Observables.

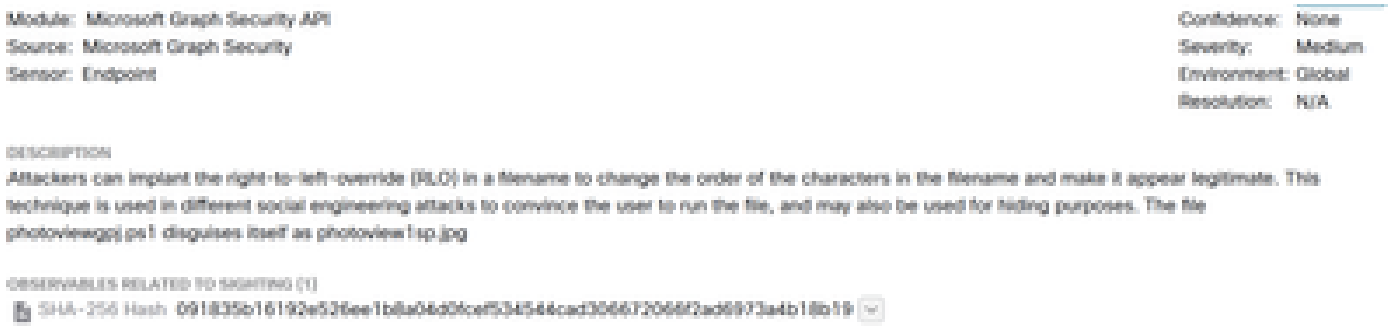
Verifica

È possibile utilizzare questo collegamento: Microsoft graph security Snapshots per un elenco di Snapshot che aiutano a comprendere la risposta che si può ottenere da ogni tipo di osservabile.

Di seguito è riportato un esempio:



Espandere la finestra per visualizzare le informazioni fornite dall'integrazione:



Tenere presente che i dati devono esistere nel portale di Azure e che l'API Graph funziona meglio se utilizzata con altre soluzioni Microsoft. Tuttavia, questa condizione deve essere convalidata dal supporto tecnico Microsoft.

Risoluzione dei problemi

- Messaggio Autorizzazione Non Riuscita:
    - Verificare che i valori di **Tenant ID** e Client ID siano corretti e che siano ancora validi.

- Nessun dato visualizzato nell'investigazione:
    - Assicurarsi di aver copiato e incollato i valori appropriati per **Tenant ID** e **Client ID**.
        - Assicurarsi di aver utilizzato le informazioni del campo **Value** della Certificates & Secrets sezione.
        - Utilizzare gli strumenti di WebDeveloper per determinare se viene eseguita una query sull'API Graph quando viene eseguita un'indagine.
        - Quando l'API Graph unisce i dati provenienti da vari provider di avvisi Microsoft, verificare che OData sia supportato per i filtri query. (ad esempio, Office 365 Security and Compliance e Microsoft Defender ATP).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).