Microsoft Graph API와 Cisco XDR의 통합 구성

목차

소개

이 문서에서는 Microsoft Graph API를 Cisco XDR과 통합하는 절차와 쿼리할 수 있는 데이터 유형에 대해 설명합니다.

사전 요구 사항

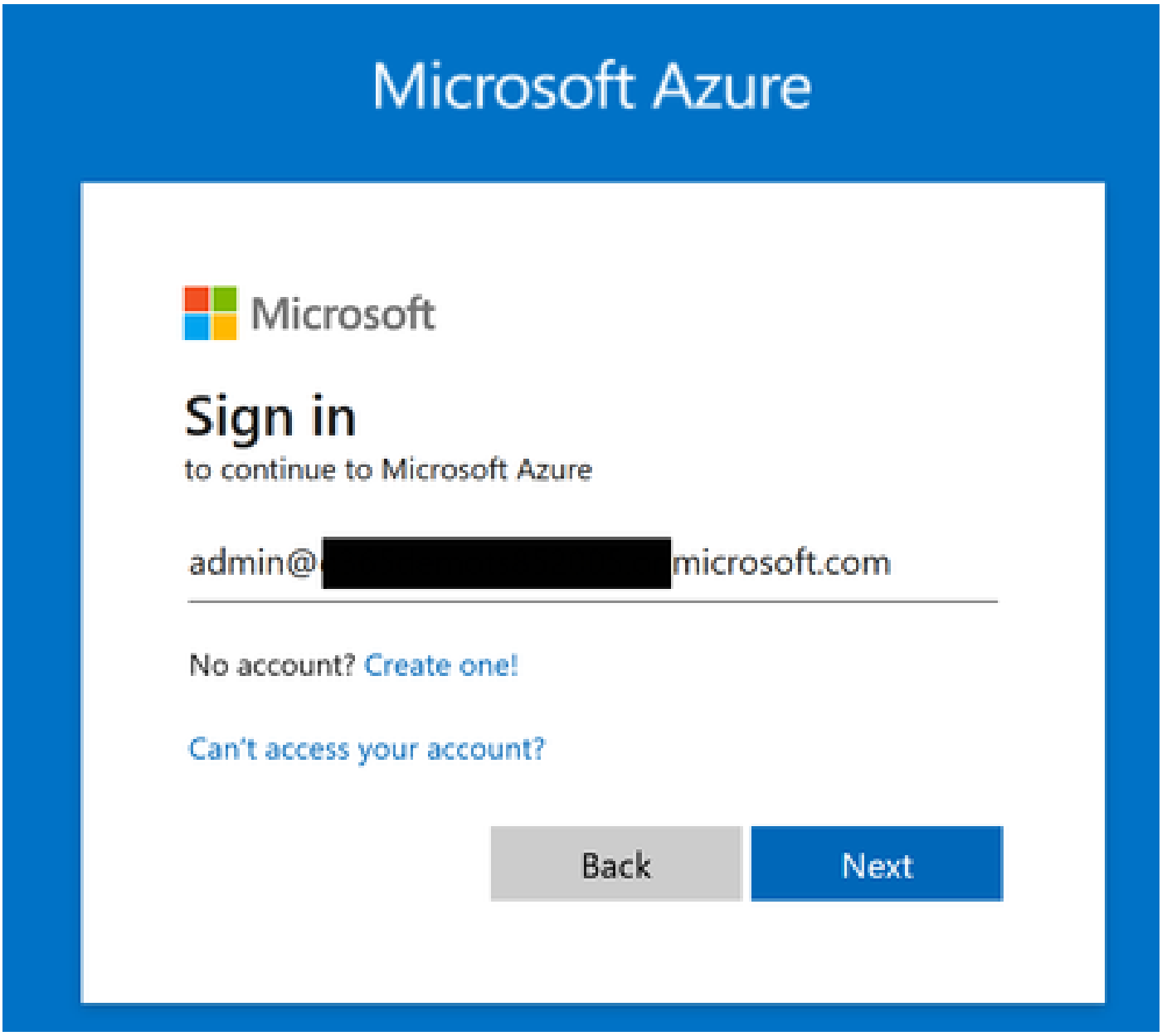
- Cisco XDR 관리 계정
- Microsoft Azure 시스템 관리자 계정
- Cisco XDR 액세스

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

통합 단계

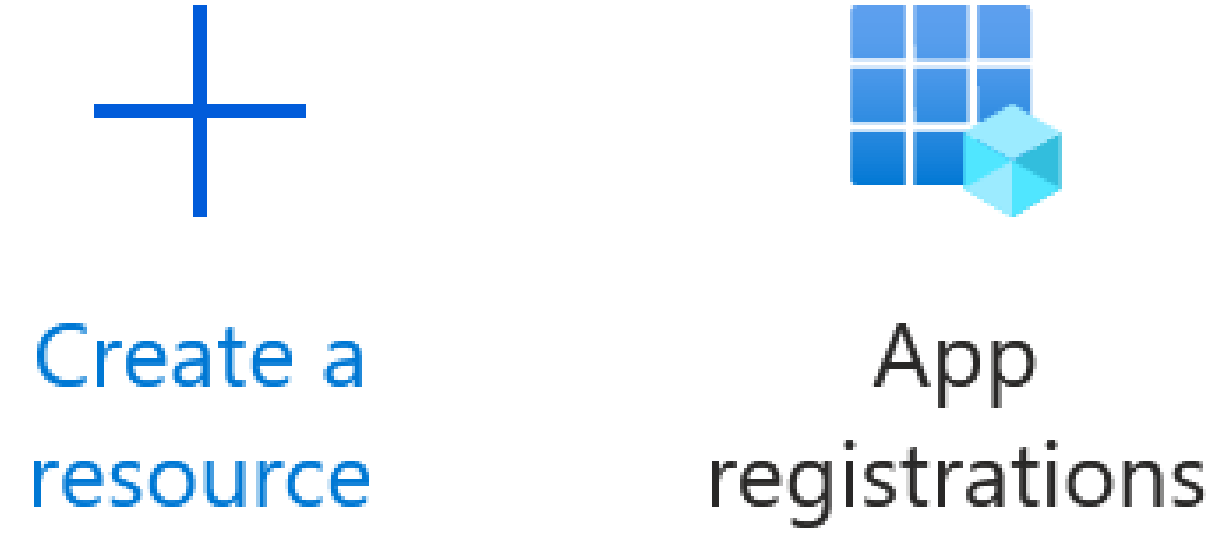
1단계.

시스템 관리자로 Microsoft Azure에 로그인합니다.



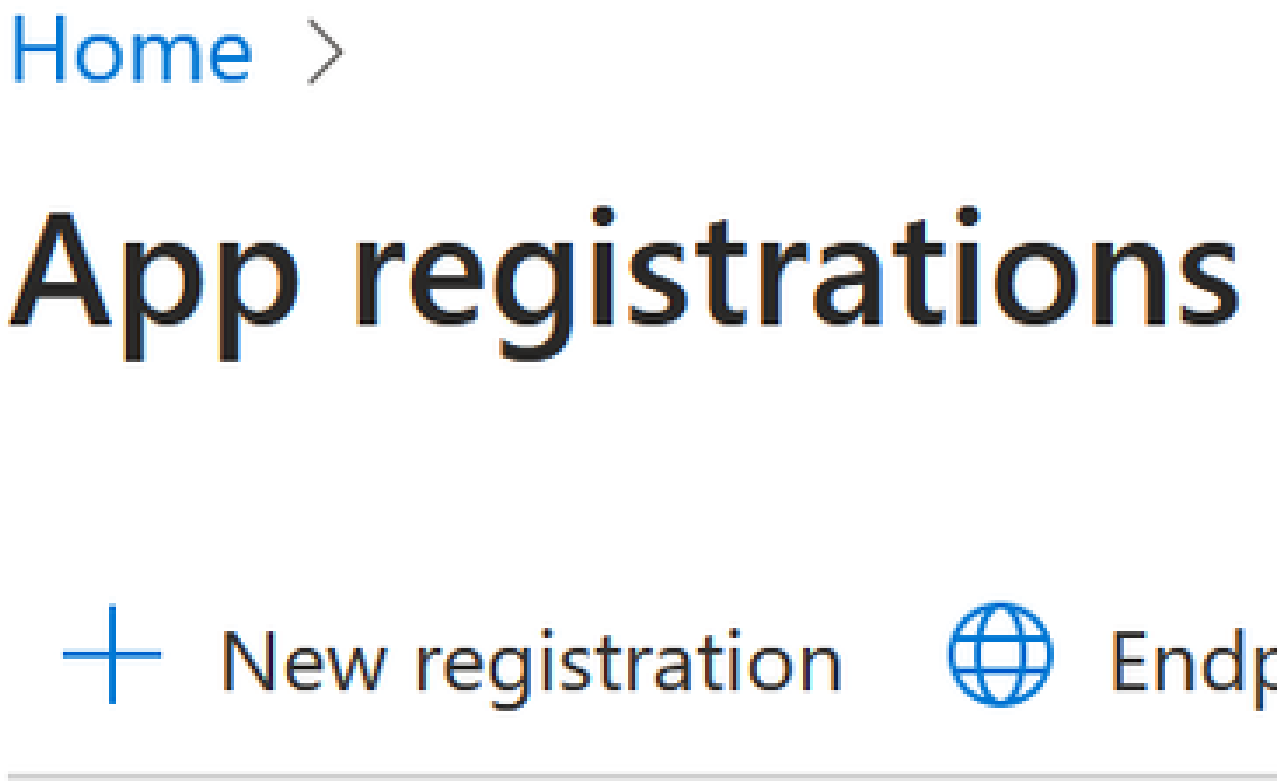
2단계.

Azure 서비스 포털**App Registrations** 을 클릭합니다.



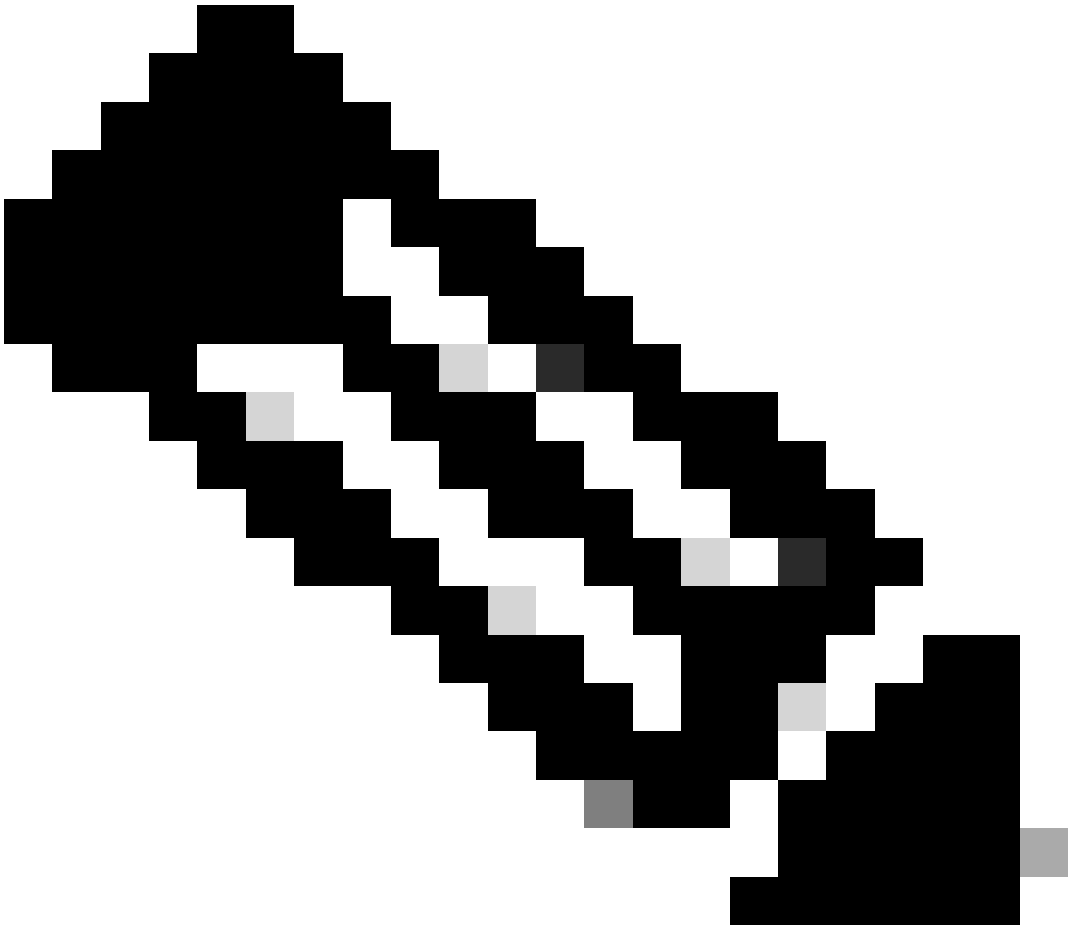
3단계.

를 New registration 클릭합니다.



4단계.

새 앱을 식별할 이름을 입력하세요.



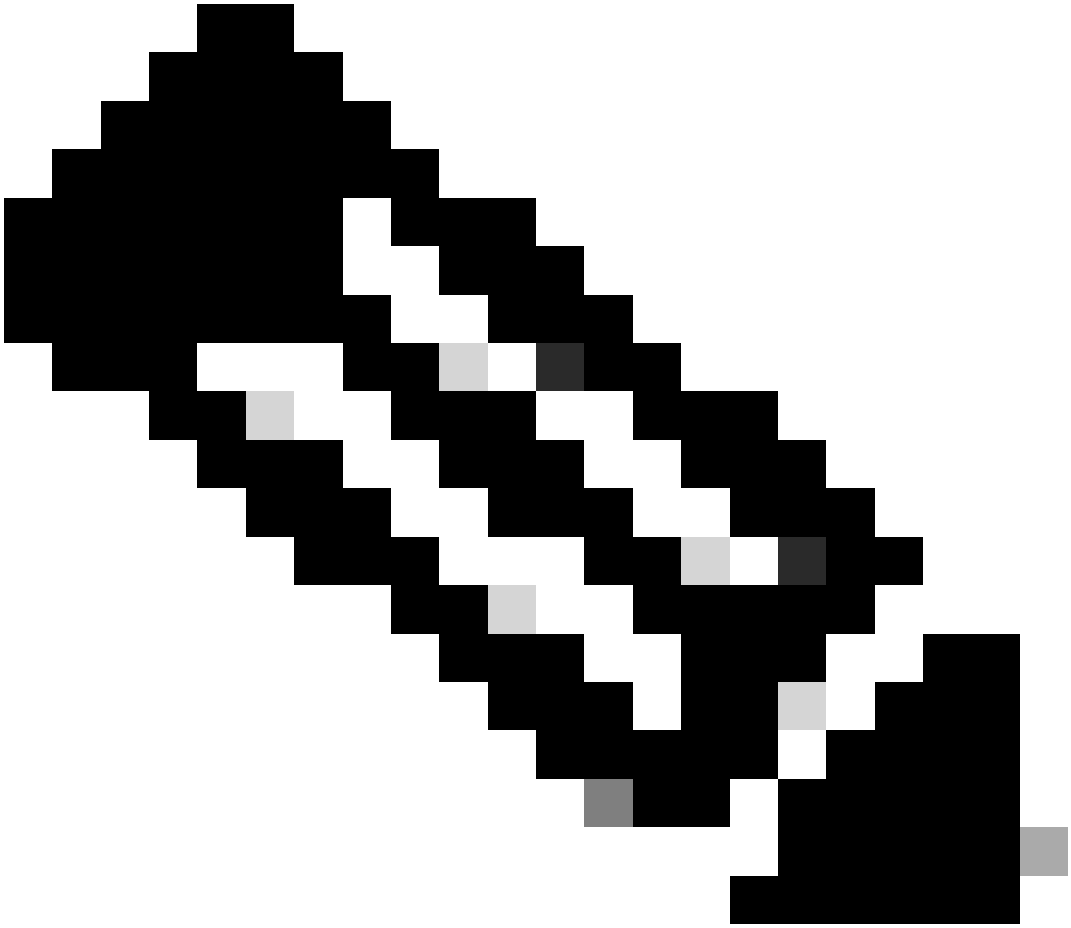
참고: 이름이 유효한 경우 녹색 확인 표시가 나타납니다.

지원되는 계정 유형에서 옵션을 선택합니다 **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



참고: 리디렉션 URI를 입력할 필요가 없습니다.

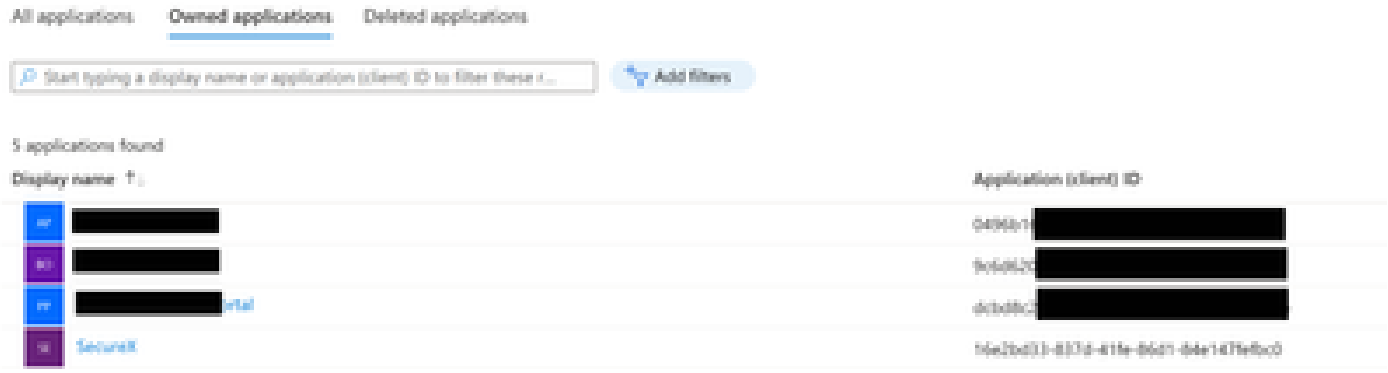
5단계.

화면 아래쪽으로 스크롤하고 을 **Register**클릭합니다.

6단계.

Azure 서비스 페이지로 다시 이동하여 을 클릭합니다App Registrations > Owned Applications.

앱을 식별하고 이름을 클릭합니다. 이 예에서는 SecureX입니다.



7단계.

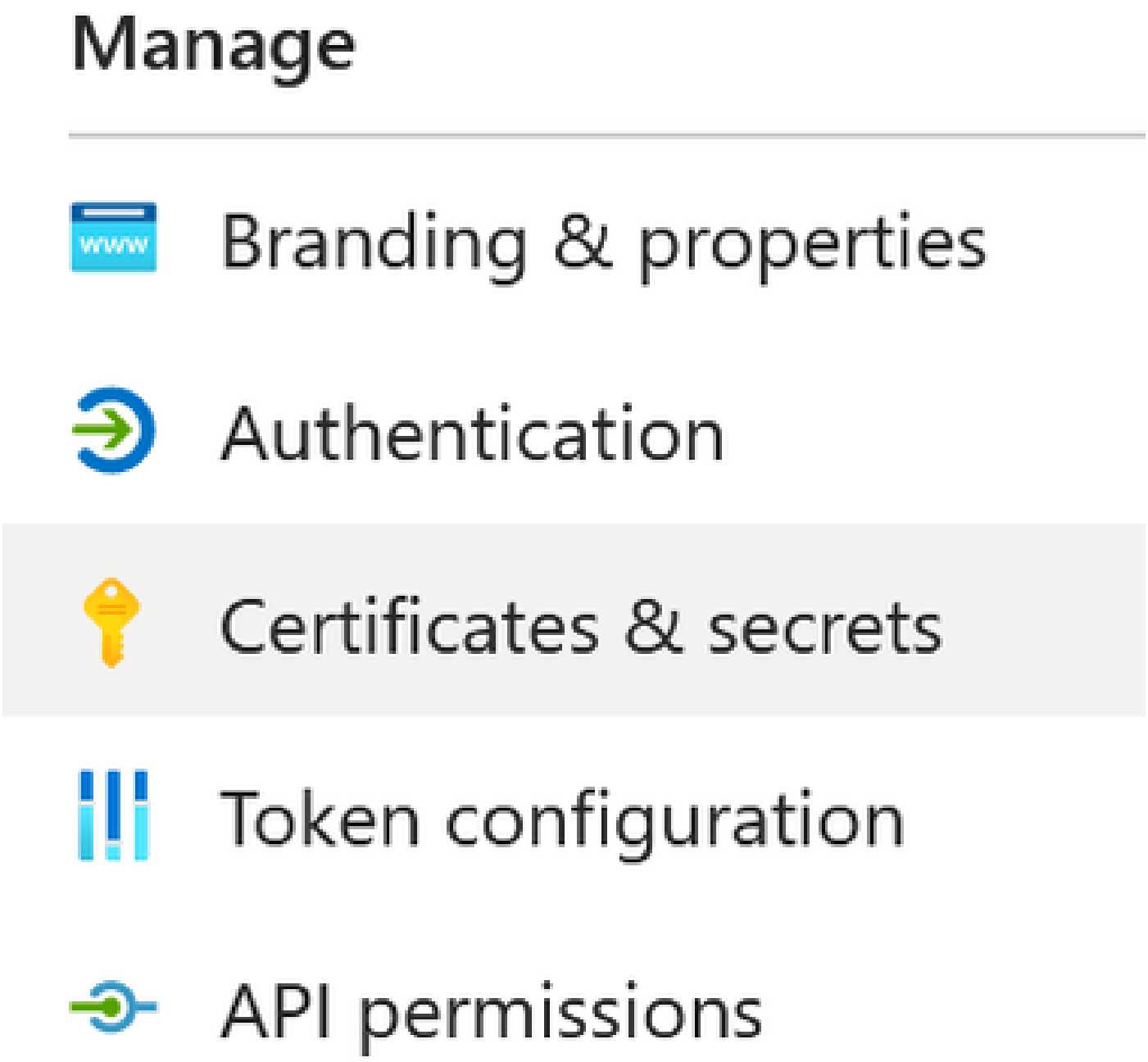
앱의 요약이 나타납니다. 관련 세부 정보를 확인하십시오.

애플리케이션(클라이언트) ID:

디렉터리(테넌트) ID:

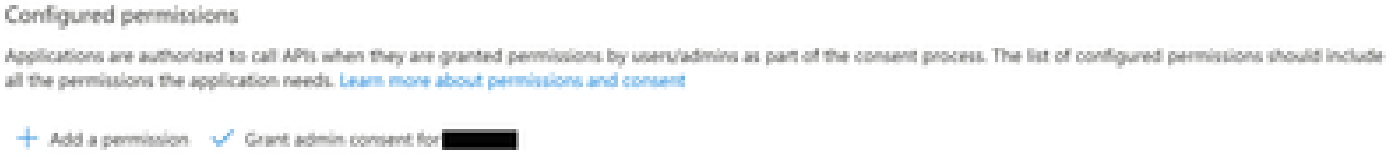
8단계.

로 Manage Menu > API Permissions 이동합니다.



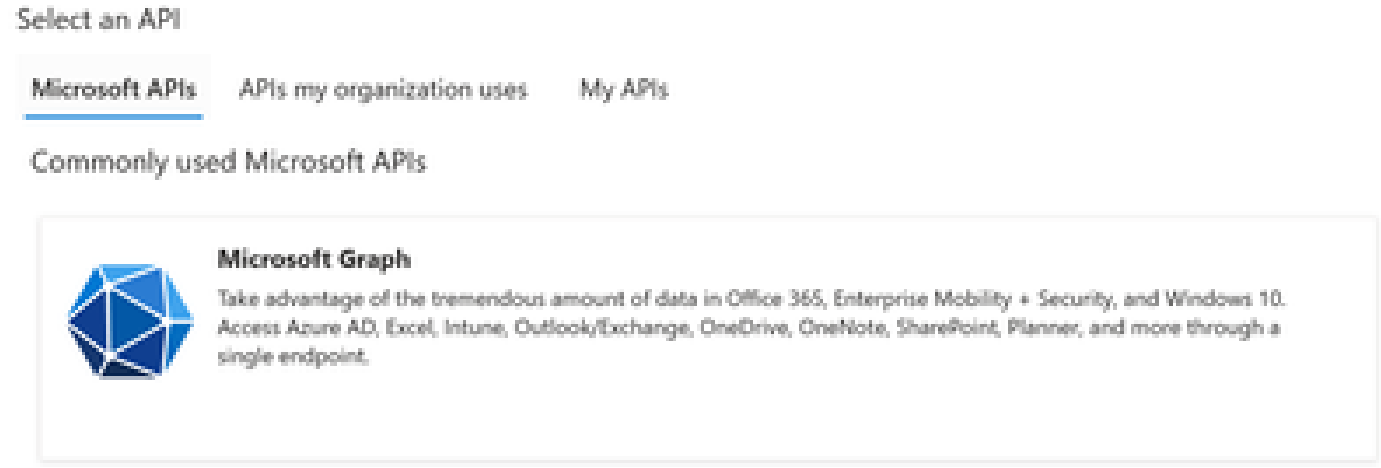
9단계.

Configured Permissions(구성된 권한)에서 을 클릭합니다Add a Permission.



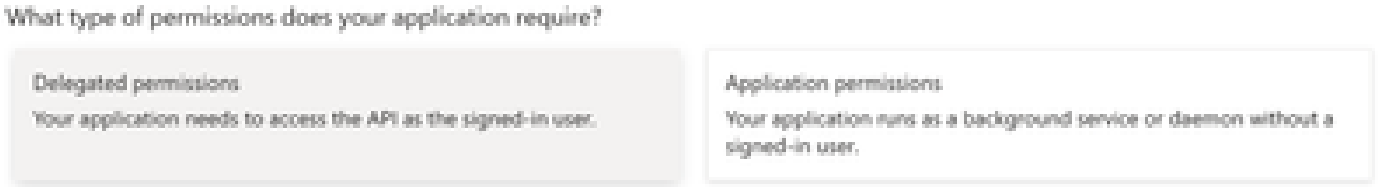
10단계.

Request API Permissions(API 권한 요청) 섹션에서 을 **Microsoft Graph**클릭합니다.



11단계.

를 Application permissions선택합니다.



검색 표시줄에서 를 Security 찾습니다. 확장 **Security Actions** 및 선택

- **모두 읽기**
- **읽기/쓰기.모두**

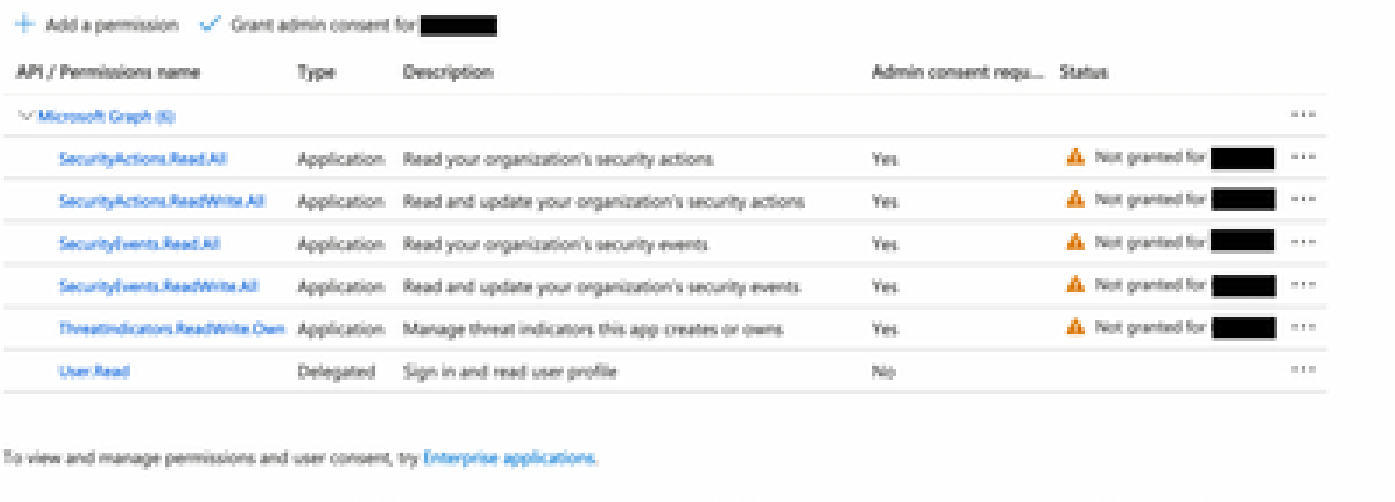
- **보안 이벤트** 및
  - **모두 읽기**
  - **읽기/쓰기.모두**

- **위협 지표** 및
  - **ThreatIndicators.ReadWrite.Owned사용자**

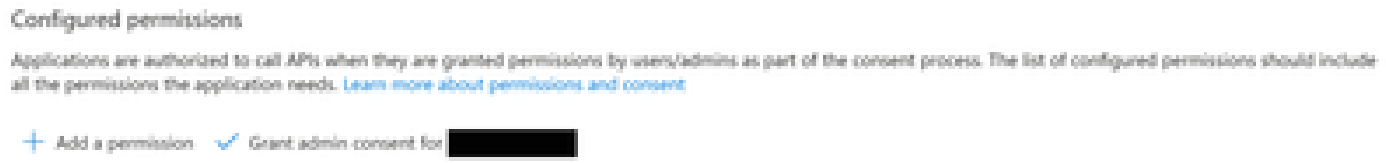
를 Add permissions 클릭합니다.

12단계.

선택한 사용 권한을 검토합니다.

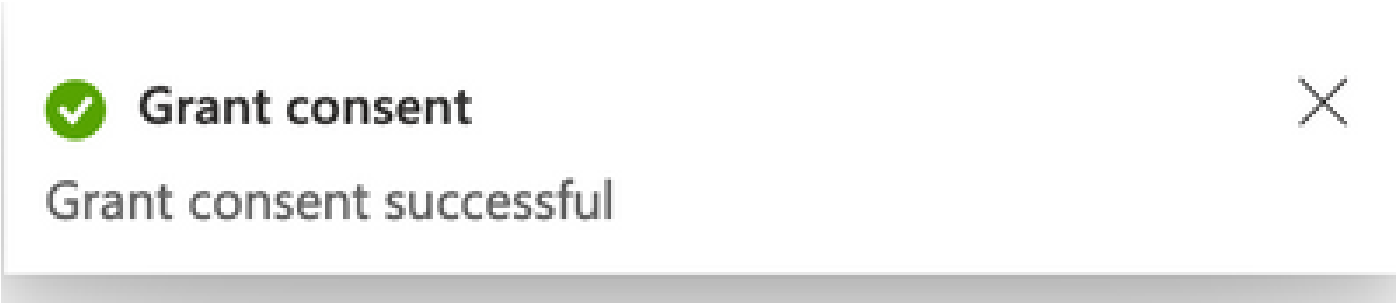


조직 **Grant Admin consent** 을 클릭합니다.



모든 권한에 대한 동의를 부여할지 여부를 선택하는 프롬프트가 나타납니다. 를 Yes 클릭합니다.

이 이미지에 표시된 것과 유사한 팝업이 나타납니다.



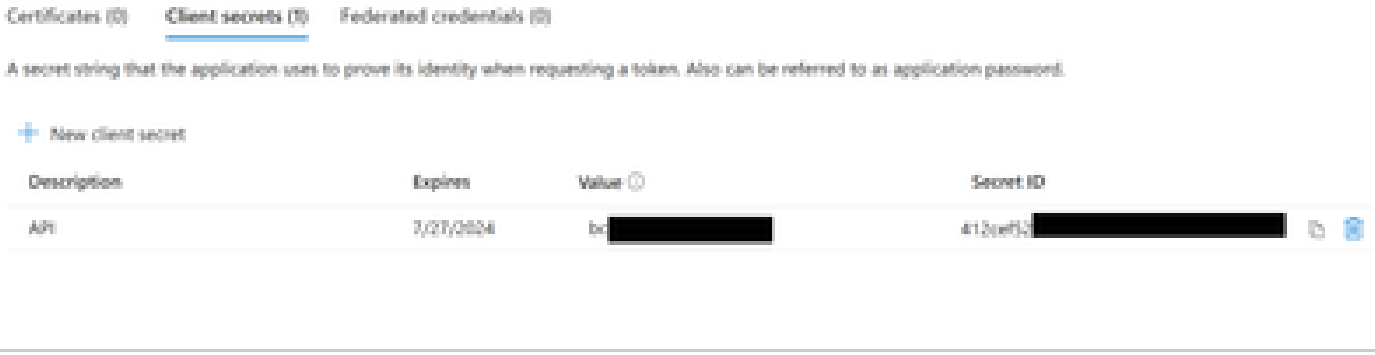
13단계.

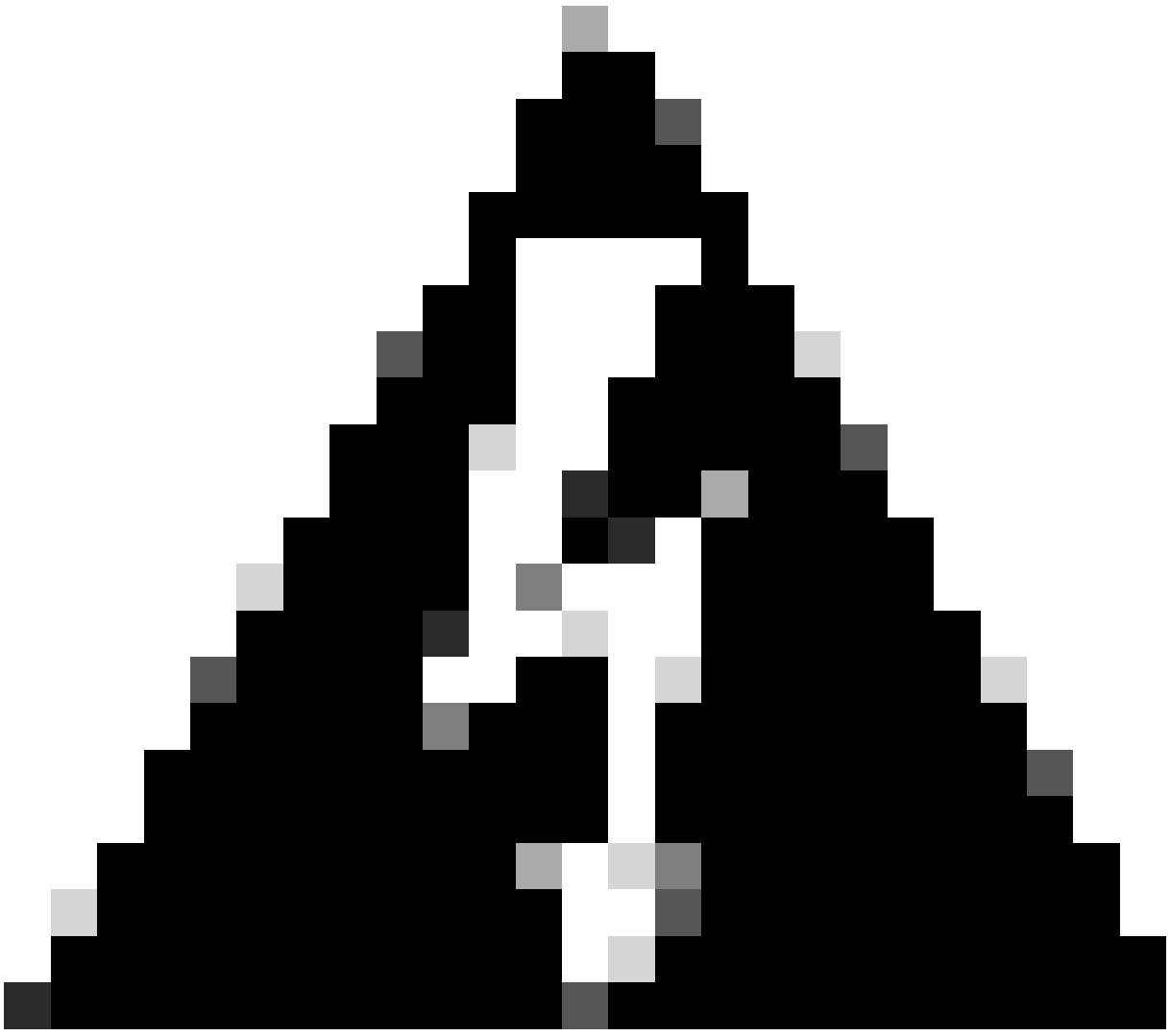
로 Manage > Certificates & Secrets 이동합니다.

를 Add New Client Secret 클릭합니다.

간단한 설명을 작성하고 유효한 날짜를 Expires 선택합니다. API 키의 만료를 막기 위해 유효 기간을 6개월 이상으로 선택하는 것이 좋습니다.

일단 생성되면, 그 부분이 통합에 사용되는 **Value**것처럼, 그 부분을 복사하여 안전한 장소에 보관한다.





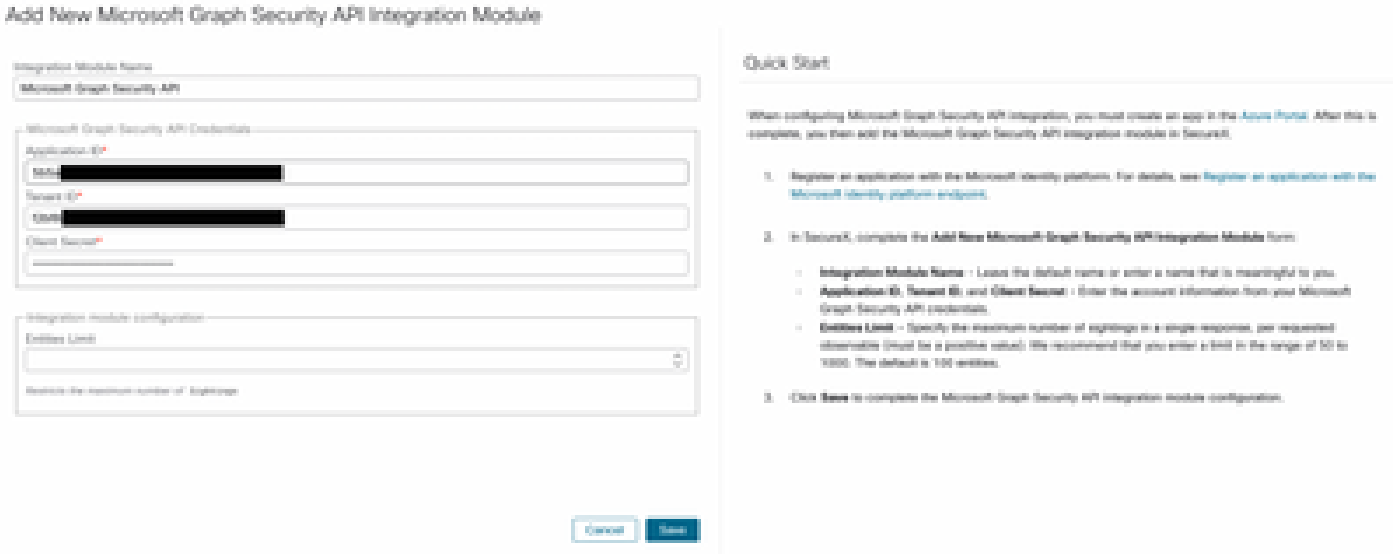
경고: 이 필드는 복구할 수 없으며 새 암호를 만들어야 합니다.

모든 정보를 얻은 후에는 앱으로 다시 **Overview** 이동하여 앱 값을 복사합니다. 그런 다음 로 SecureX 이동합니다.

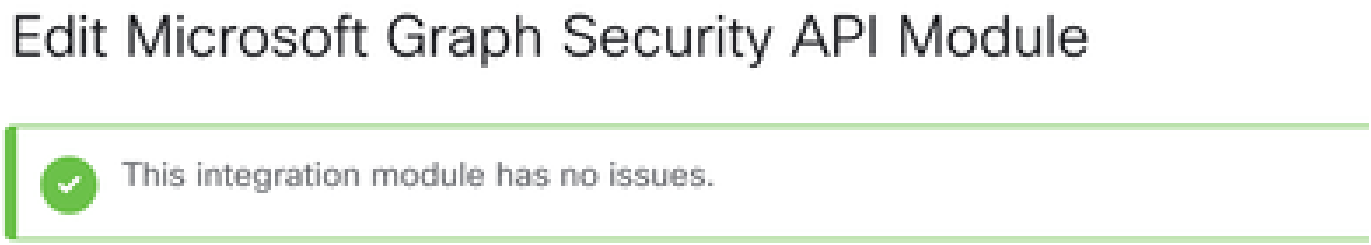
14단계.

선택으로 Integration Modules > Available Integration Modules > 이동하고 Microsoft Security Graph API 를 클릭합니다Add.

이름을 할당하고 Azure 포털에서 가져온 값을 붙여넣습니다.



을 Save 클릭하고 상태 검사가 성공할 때까지 기다립니다.



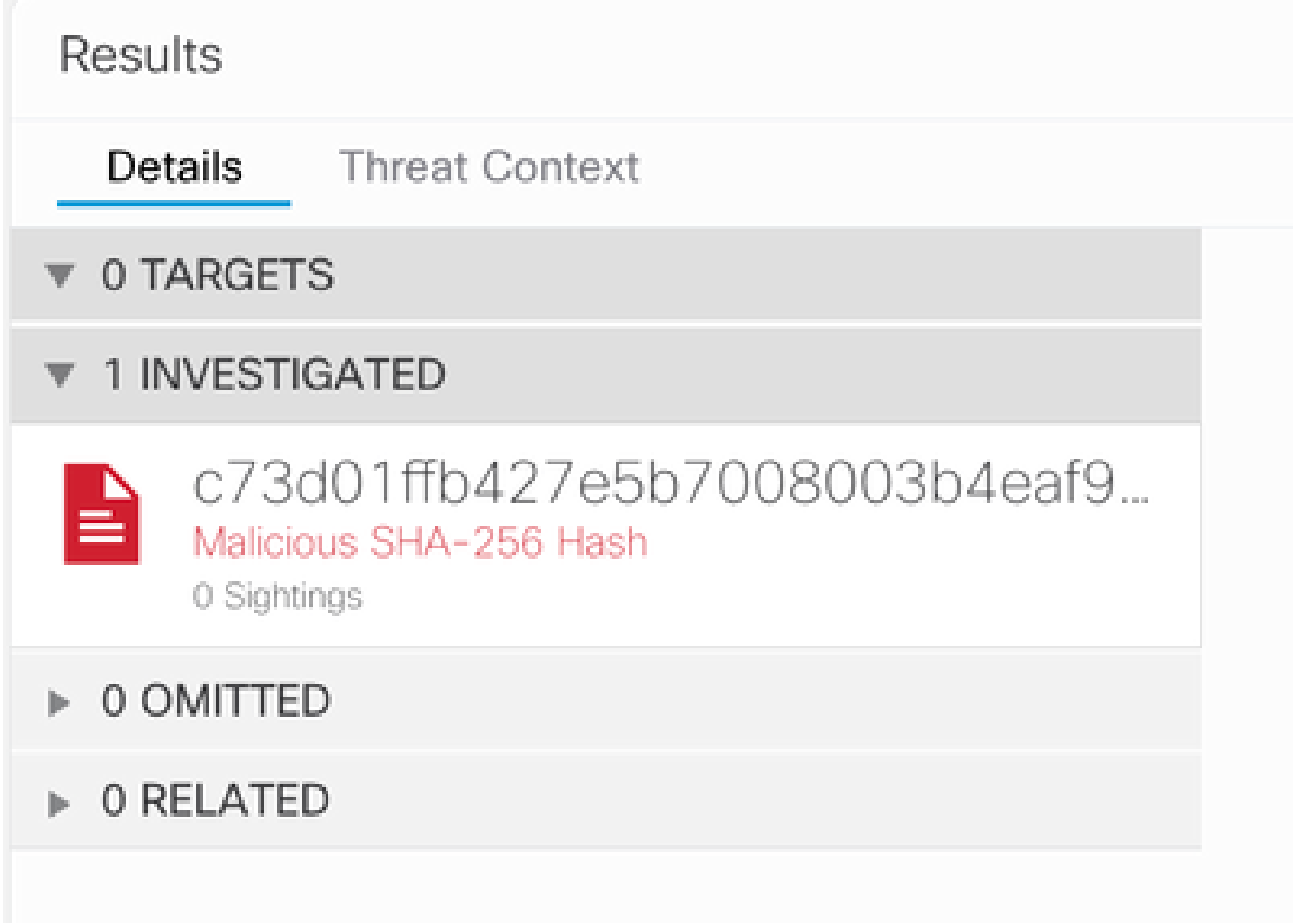
조사 수행

현재로서는 Microsoft Security Graph API가 Cisco XDR 대시보드에 타일로 채워지지 않습니다. 조사 기능을 사용하여 Azure 포털의 정보를 쿼리할 수 있습니다.

Graph API는 다음에만 쿼리할 수 있습니다.

- ip
- 도메인
- 호스트 이름
- url
- 파일_이름
- 파일 경로
- sha256

이 예에서는 조사 시 이 SHA가 c73d01ffb427e5b7008003b4eaf9303c1febd883100bf81752ba71f41c701148 사용되었습니다.



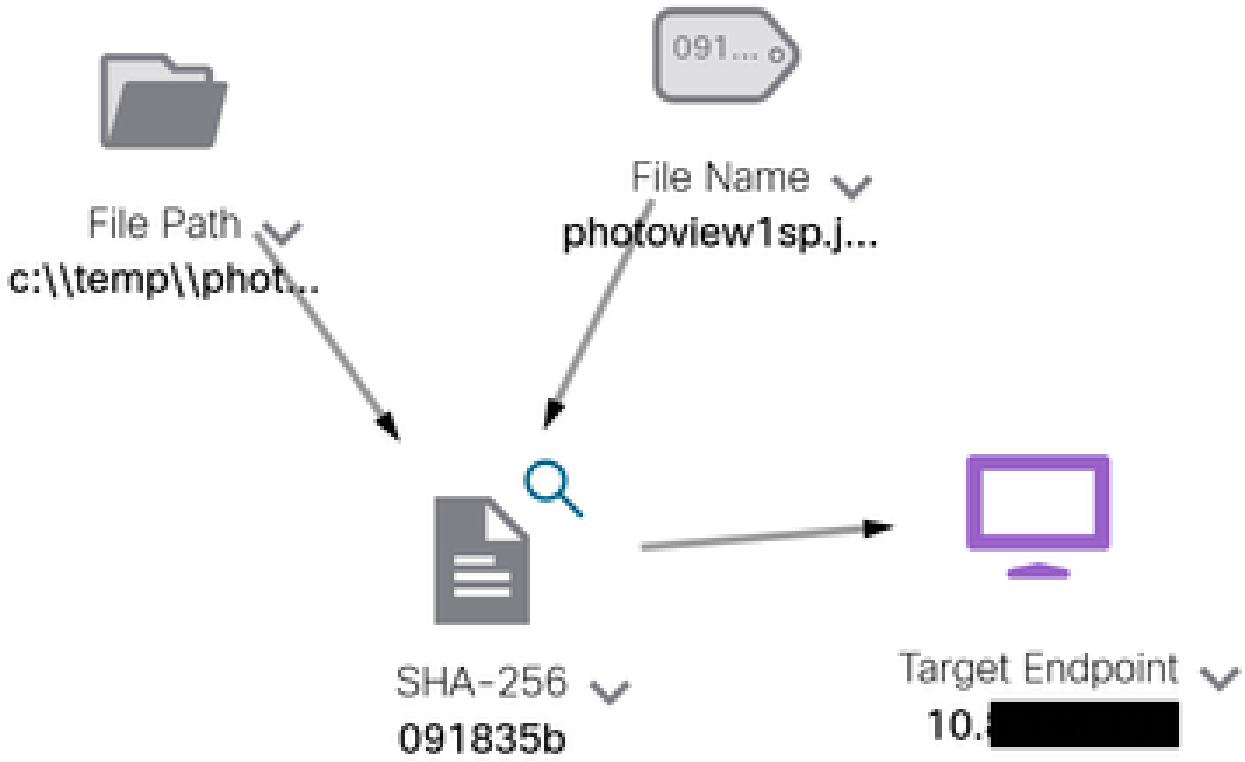
보시다시피 Lab Environment에서는 Sightings 0개가 표시되는데, Graph API가 작동하는지 테스트하는 방법은 무엇입니까?

WebDeveloper Tools를 열고, 조사를 실행하고, visibility**.amp.cisco.com**에 대한 Post Event(사후 이벤트)를 찾은 다음 라는 파일을 Observables찾습니다.

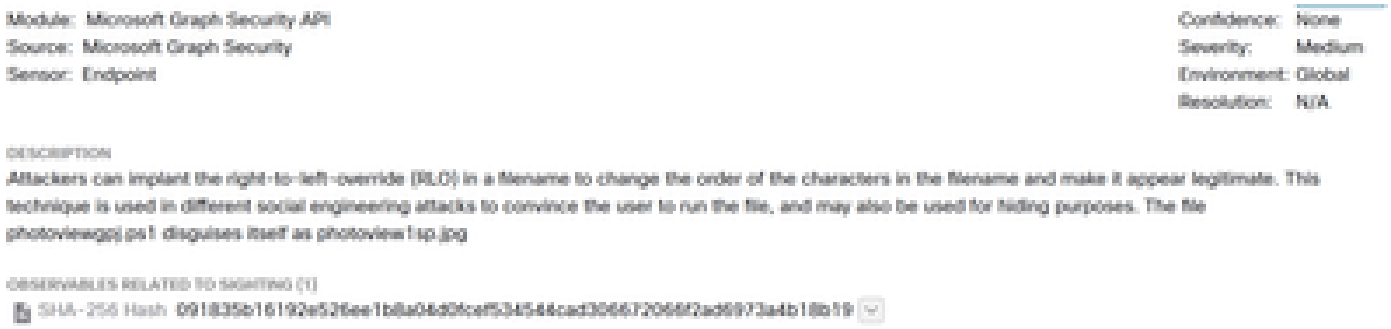
다음을 확인합니다.

이 링크를 사용할 수 있습니다. 관찰 가능한 각 유형에서 얻을 수 있는 응답을 이해하는 데 도움이 되는 스냅샷 목록에 대한 Microsoft graph security Snapshots

이 그림과 같은 예를 볼 수 있습니다.



창을 확장하면 통합에서 제공하는 정보를 볼 수 있습니다.



데이터는 Azure 포털에 있어야 하며 Graph API는 다른 Microsoft 솔루션과 함께 사용할 때 더 잘 작동합니다. 그러나 이는 Microsoft 지원에서 검증해야 합니다.

문제 해결

- 권한 부여 실패 메시지:
    - 및 의 **Tenant ID** 값이 정확하고Client ID 여전히 유효한지 확인합니다.

- Investigation에 데이터가 표시되지 않음:

  - 및 의 적절한 값을 복사하여 붙여 넣었는지 **Tenant ID** 확인합니다 **Client ID**.

    - 섹션의 필드 정보를 **Value** 사용했는지 Certificates & Secrets 확인합니다.

    - WebDeveloper 툴을 사용하여 조사가 수행될 때 Graph API를 쿼리할지 여부를 확인합니다.

    - Graph API가 다양한 Microsoft 알림 공급자의 데이터를 병합할 때 쿼리 필터에 대해 OData가 지원되는지 확인합니다. (예: Office 365 보안 및 규정 준수, Microsoft Defender ATP).

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.