CDO와 SecureX 통합

• SecureX 및 CDO, on page 1

SecureX 및 CDO

Cisco SecureX 플랫폼은 가시성을 통합하고 자동화를 가능하게 하며 네트워크, 엔드포인트, 클라우드 및 애플리케이션 전반에서 보안을 강화하는 일관된 경험을 위해 Cisco의 광범위한 통합 보안 포트폴리오와 고객의 인프라를 연결합니다. 통합 플랫폼에서 기술을 연결함으로써 SecureX는 측정 가능한 통찰력, 바람직한 결과 및 더할 나위 없는 팀 간 협업을 제공합니다. SecureX가 무엇이고 이 플랫폼이 제공하는 기능에 대한 자세한 내용은 SecureX 정보를 참조하십시오.

SecureX가 CDO 테넌트에 액세스하도록 허용하면 총 디바이스 수는 물론 오류가 있는 디바이스, 충돌이 있는 디바이스 및 현재 동기화되지 않을 수 있는 디바이스를 포함하여 디바이스 이벤트가 요약됩니다. 이벤트 요약은 또한 현재 적용된 정책 및 해당 정책과 관련된 개체를 집계하는 두 번째 창을 제공합니다. 정책은 디바이스 유형으로 정의되며 개체는 개체 유형을 통해 식별됩니다.

SecureX 대시보드에 CDO 모듈을 추가하려면 여러 단계가 필요합니다. 자세한 내용은 SecureX에 CDO 추가를 참조하십시오.

Warning CDO 및 SecureX 계정을 아직 병합하지 않은 경우, 온보딩된 모든 디바이스에 대한 이벤트가 표시되지 않을 수 있습니다. SecureX에서 CDO 모듈을 생성하기 전에 계정을 병합하는 것이 좋습니다. 자세한 내용은 CDO 및 SecureX 계정 병합을 참조하십시오.

SecureX 리본

SecureX 리본은 SecureX 계정 생성 여부와 상관없이 CDO에서 사용할 수 있습니다. 페이지 하단에 있는 SecureX 탭 

을 클릭하여 리본을 확장합니다.

리본을 사용하려면 SecureX 계정을 확인해야 합니다. SecureX에 액세스하는 데 사용하는 것과 동일한 인증 로그인을 사용하는 것이 좋습니다. 리본이 인증되면 CDO에서 직접 SecureX 기능을 활용할 수 있습니다.

자세한 내용은 SecureX 리본 설명서를 참조하십시오.

SecureX 문제 해결

이 경험에는 두 가지 제품이 포함됩니다. 발생할 수 있는 문제를 식별, 해결 또는 문의하는 데 도움이 되도록 SecureX 문제 해결을 참조하십시오.

관련 정보:

- SecureX 정보
- CDO 및 SecureX 계정 병합
- CDO에서 SecureX 연결, on page 3
- CDO에서 SecureX 연결 끊기, on page 4
- SecureX에 CDO 추가
- SecureX 문제 해결

CDO 및 SecureX 계정 병합

SecureX 또는 Cisco Threat Response(CTR) 계정이 이미 있는 경우, 디바이스를 SecureX에 등록하려면 CDO 계정과 SecureX/CTR 계정을 병합해야 합니다. 계정을 SecureX 포털에 병합할 수 있습니다. CDO 모듈을 만들기 전에 계정을 병합하는 것이 매우 좋습니다. 어카운트가 병합될 때까지 SecureX에서 디바이스의 이벤트를 보거나 다른 SecureX 기능을 활용할 수 없습니다.

지침은 SecureX의 계정 병합을 참조하십시오.

Note 둘 이상의 지역 클라우드에 계정이 있는 경우 각 지역 클라우드에 대해 별도로 계정을 병합해야 합니다.

관련 정보:

- SecureX 및 CDO
- SecureX에 CDO 추가
- SecureX 문제 해결

SecureX에 CDO 추가

SecureX가 등록된 디바이스에 액세스하도록 허용하고 SecureX 대시보드에 CDO 모듈을 추가하여 보안 포트폴리오의 다른 Cisco 플랫폼과 함께 디바이스 정책 및 개체 요약을 확인합니다.

시작하기 전에

CDO에서 SecureX를 연결하기 전에 다음 항목을 작업하는 것이 매우 좋습니다.

- SecureX 계정의 관리자 이상이어야 합니다.

- CO 테넌트에 대한 슈퍼 관리자 사용자 역할이 있어야 합니다.
- 테넌트 통신을 용이하게 하기 위해 보안 서비스 익스체인지에 테넌트 계정을 병합합니다. 자세한 내용은 CDO 및 SecureX 계정 병합을 참조하십시오.
- CDO 계정을 보안 서비스 익스체인지과 병합한 후, CDO 테넌트에서 로그아웃하고 다시 로그인해야 합니다.
- 아직 구성하지 않은 경우 Cisco Secure Sign-On을 MFA(Multi-Factor Authentication)용 SAML SSO(Single Sign-On IdP) 및 Duo Security로 구성합니다. CDO와 SecureX 모두 이를 인증 방법으로 사용합니다. 자세한 내용은 SAML Single Sign-On을 Cisco Defense Orchestrator와 통합을 참조하십시오.

Note 참고: 테넌트가 여러 개인 경우 SecureX에서 테넌트당 하나의 모듈을 생성해야 합니다. 각 테넌트는 인증을 위해 고유한 API 토큰이 필요합니다.

CDO에서 SecureX 연결

SecureX 및 CDO 계정을 병합한 후 두 플랫폼 간의 통신을 승인하고 수동으로 CDO 모듈을 SecureX 대시보드에 추가하도록 활성화해야 합니다. CDO UI를 통해 SecureX를 연결하고 보안 포트폴리오의 다른 Cisco 플랫폼과 함께 디바이스의 정책, 이벤트 유형, 개체 등에 대한 요약을 확인합니다.

Note SecureX 대시보드에 구성된 CDO 모듈이 이미 있는 경우 **Connect Tenant to SecureX** 옵션은 중복 CDO 모듈을 생성합니다. 이 문제가 발생하면 자세한 내용은 SecureX 문제 해결을 참조하십시오.

다음 절차를 사용하여 CDO에서 API 토큰을 조달하고 CDO 모듈을 SecureX에 추가합니다.

단계 **1** CDO에 로그인합니다.

단계 **2** 오른쪽 상단 모서리에 있는 사용자 메뉴에서 **Settings(**설정**)**을 선택합니다.

단계 **3** 창 왼쪽에서 **General Settings(**일반 설정**)** 탭을 선택합니다.

단계 **4** **Tenant Settings(**테넌트 설정**)** 섹션을 찾아 **Connect SecureX(SecureX** 연결**)**를 클릭합니다. 브라우저 창이 SecureX 로그인 페이지로 리디렉션됩니다. CDO 테넌트와 연결하려는 조직 자격 증명으로 SecureX에 로그인합니다.

단계 **5** SecureX에 성공적으로 로그인하면 브라우저가 자동으로 다시 CDO로 리디렉션됩니다. **General Settings(**일반 설정**)** 페이지의 **User Management (**사용자 관리**)** 탭에서 SecureX에 로그인한 조직의 이름을 포함하는 새 사용자를 볼 수 있습니다. 이 사용자는 읽기 전용이며 SecureX로 데이터를 보내는 데만 사용됩니다.

CDO에서 SecureX 연결 끊기

CDO와 SecureX 조직 간의 통신 요청 연결을 끊을 수 있습니다. 이 옵션은 SecureX에서 조직을 제거하지 않지만, CDO에서 읽기 전용 API 사용자를 제거하고 이전에 SecureX 조직과 연결된 테넌트는 이벤트 보고서 전송을 중지합니다.

이것은 CDO의 SecureX 리본에서 테넌트를 로그아웃하거나, 어떠한 방식으로든 리본을 비활성화하지 않습니다. 리본에서 로그아웃하려면 Support Case Manager(지원 사례 매니저)에서 사례를 열어 리본 로그인을 수동으로 재설정해야 합니다. 이 요청은 테넌트를 리본에서 로그아웃합니다.

단계 **1** CDO에 로그인합니다.

단계 **2** 오른쪽 상단 모서리에 있는 사용자 메뉴에서 **Settings(**설정**)**을 선택합니다.

단계 **3** 창 왼쪽에서 **General Settings(**일반 설정**)** 탭을 선택합니다.

단계 **4** **Tenant Settings(**테넌트 설정**)** 섹션을 찾아 **Disconnect SecureX(SecureX** 연결 끊기**)**를 클릭합니다. **General Settings(**일반 설정**)** 페이지의 **User Management(**사용자 관리**)** 탭에서, SecureX로 데이터를 보내기 위해 생성된 읽기 전용 사용자가 삭제됩니다.

SecureX에 CDO 타일 추가

CDO 모듈을 활성화한 후 이제 CDO 타일을 SecureX 대시보드에 추가할 수 있습니다. 제품의 모듈은 CDO의 상태 정보에 액세스하고 두 가지 가능한 타일 선택을 통해 대시보드에 데이터를 보고합니다.

SecureX 대시보드에 CDO 타일을 추가하려면 다음 절차를 따르십시오.

단계 **1** SecureX 대시보드 탭 

에서 **New Dashboard(**새 대시보드**)**를 클릭합니다. SecureX 대시보드에 처음 액세스하는 경우 **Add Tiles(**타일 추가**)**를 클릭할 수도 있습니다.

단계 **2** (선택 사항) 대시보드 이름을 변경합니다.

Tip 테넌트가 여러 개인 경우 이 이름 변경 옵션을 사용하여 CDO 타일이 연결된 테넌트를 식별합니다.

단계 **3** "Available Tiles(사용 가능한 타일)" 목록에서 **CDO**를 선택하고 옵션을 확장하여 사용 가능한 타일을 확인합니다. 대시보드에 포함하려는 모든 타일을 선택합니다.

- **CDO** 디바이스 요약. 이 타일에는 현재 CDO 테넌트에 온보딩된 모든 디바이스와 해당 상태가 나열됩니다.
- **CDO** 개체 및 정책. 이 타일에는 디바이스에 현재 적용된 모든 정책 및 해당 정책과 관련된 개체가 나열됩니다.

Note CDO가 나열되지 않으면, SecureX에 저장된 CDO의 유효한 API 토큰이 없는 것입니다. 자세한 내용은 CDO에 액세스하도록 SecureX에 CDO 타일 추가을 참조하십시오.

단계 **4** **Save(**저장**)**를 클릭합니다.

관련 정보**:**

- CDO 및 SecureX 계정 병합
- SecureX 문제 해결