

Cisco Secure Cloud Analytics

Cisco XDR 통합 가이드



목차

Cisco Secure Cloud Analytics 통합 Cisco XDR	3
Secure Cloud Analytics 타일, Cisco XDR	4
Secure Cloud Analytics	6
Secure Cloud Analytics	6
Secure Cloud Analytics 및 Cisco XDR	6
사용: Secure Cloud Analytics	6
사용: Cisco XDR	8
알림을 다음에 게시: Cisco XDR	10
알림 유형 게시 활성화	10
알림 인스턴스를 인시던트로 수동 승격	10
추가 리소스	11
지원 팀에 문의	12
변경 기록	13

Cisco Secure Cloud Analytics 통합 Cisco XDR

Cisco XDR 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 Cisco XDR는 측정 가능한 통찰력, 바람직한 결과 및 더할 나위 없는 팀 간 협업을 제공합니다.

Cisco Secure Cloud Analytics을(를) Cisco XDR과(와) 통합하여 Cisco XDR 대시보드에서 Secure Cloud Analytics 구축에 대한 추가 정보를 보고 Secure Cloud Analytics 웹 포털 내에서 Cisco XDR 리본을 사용할 수 있습니다.

Cisco XDR 리본에 로그인한 경우에는 알림을 기반으로 Cisco XDR 위협 대응 인시던트를 생성하고 IP 주소에서 다른 Cisco XDR 제품 통합으로 피벗할 수 있습니다. 이러한 기능의 사용에 대한 자세한 내용은 [Secure Cloud Analytics 초기 구축 가이드](#)를 참조하십시오.

Secure Cloud Analytics 무료 평가판 설정에 대한 자세한 내용은 [Secure Cloud Analytics](#) 웹 페이지를 참조하십시오.

Cisco XDR 어카운트를 생성한 후 리본에 대한 자세한 내용은 <https://docs.xdr.security.cisco.com/Content/Ribbon/ribbon.htm>을 참조하십시오.

Secure Cloud Analytics 타일, Cisco XDR

Secure Cloud Analytics Secure Cloud Analytics는 온프레미스 및 클라우드 기반 네트워크 구축을 모니터링하는 SaaS(Software as a Service) 솔루션입니다. 네트워크 트래픽에 대한 정보를 수집하여 네트워크에서의 동작에 대한 사실인 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. 관찰 자체는 관찰이 나타내는 것 이상의 의미를 전달하지 않습니다. 관찰, 역할 및 기타 위협 인텔리전스의 조합을 기반으로 Secure Cloud Analytics는 시스템에서 식별한 가능한 악의적인 행동을 나타내는 실행 가능한 항목인 알림을 생성합니다.

Secure Cloud Analytics 또한 웹 포털 UI에서 검토할 수 있는 흥미로운 동작의 관찰(강조 표시된 관찰)을 식별합니다. 이러한 관찰 자체가 악의적인 행동을 의미하지는 않지만, 네트워크에서 중요한 트래픽을 나타낼 수 있습니다.

다음에서는 Secure Cloud Analytics 결과를 나타내는 Cisco XDR 대시보드에 표시할 수 있는 Secure Cloud Analytics 타일에 대해 설명합니다.

알림 개요 차트

알림 개요 차트 타일은 선택한 프레임에 따라 바깥쪽 고리 안에 다단계 원형 차트를 표시합니다.

- 시간 프레임 내에 생성된 새 Secure Cloud Analytics 알림
- 시간 프레임 이전에 생성되어 시간 프레임 내에 아직 종료되지 않은 Secure Cloud Analytics 알림 열기
- 닫힌 Secure Cloud Analytics 알림이 시간 프레임 동안 종료됨

및 내부 원에 있음:

- 할당된 Secure Cloud Analytics 알림
- 할당되지 않은 Secure Cloud Analytics 알림

알림 빠른 보기

알림 빠른 보기 타일은 열려 있는 Secure Cloud Analytics 알림 및 할당되지 않은 Secure Cloud Analytics 알림의 현재 수를 표시합니다.

디바이스 수 차트

디바이스 수 차트 타일은 지정된 시간 프레임 동안 네트워크에서 전송 트래픽을 Secure Cloud Analytics에서 탐지한 고유한 엔티티의 수를 세로 막대그래프로 표시합니다.

관찰 수

관찰 수 타일은 지정된 시간 프레임에 Secure Cloud Analytics에서 생성된 총 관찰 수와 해당 시간 프레임에 강조 표시된 총 관찰 수를 표시합니다. 관찰 및 강조 표시된 관찰 링크를 통해 이러한 관찰에 대한 자세한 정보를 볼 수 있는 포털 UI로 이동합니다.

Cisco Secure Cloud Analytics 센서 상태

Cisco Secure Cloud Analytics 센서상태 타일은 구성된 Cisco Secure Cloud Analytics 센서의 목록과 활성/비활성 여부를 표시합니다.

시간대별 트래픽 차트

시간대별 트래픽 차트 타일은 선택한 시간 프레임 동안 Secure Cloud Analytics에서 모니터링 한 인바운드 트래픽, 인바운드 암호화 트래픽, 아웃바운드 트래픽 및 아웃바운드 암호화 트래픽의 양을 나타내는 누적 막대그래프를 표시합니다.

Secure Cloud Analytics

와 Cisco XDR 통합 구성

Cisco XDR 통합을 구성하려면 다음을 완료하십시오.

- Secure Cloud Analytics에서 Cisco XDR 사용자 통합을 활성화하여 Cisco XDR 리본을 Secure Cloud Analytics에 표시할 수 있습니다.
- Cisco XDR에서 Secure Cloud Analytics(으)로의 포털 통합을 활성화합니다.

Cisco XDR 어카운트가 있어야 합니다. 자세한 내용은 [Cisco Security Cloud Sign On 가이드](#)를 참조하십시오.

Secure Cloud Analytics

에서 Cisco XDR에 대한 액세스 권한 부여

Cisco XDR 액세스를 승인하면 Secure Cloud Analytics의 리본이 활성화됩니다.

절차

1. Secure Cloud Analytics 웹 포털에 로그인합니다.
2. 페이지 하단에 있는 리본에서 **+**을 클릭하여 확장합니다.
3. **Get Cisco XDR(Cisco XDR 가져오기)**을 클릭한 다음 지침에 따라 액세스를 승인합니다.

Secure Cloud Analytics 및 Cisco XDR

간 통합 활성화

[Secure Cloud Analytics 웹 포털](#) 또는 [Cisco XDR](#)에서 Cisco XDR 통합을 활성화할 수 있습니다.

사전 요건

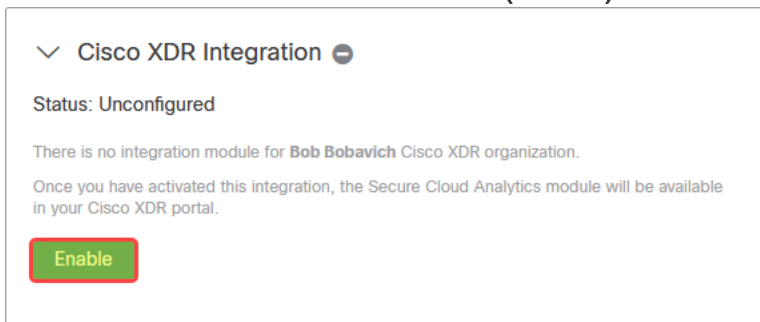
- 사용자는 Secure Cloud Analytics의 사이트 관리자입니다.
- 사용자는 Cisco XDR의 조직 관리자입니다.

이 두 가지 역할에 모두 속하지 않으면 Cisco XDR을 활성화할 수 없습니다.

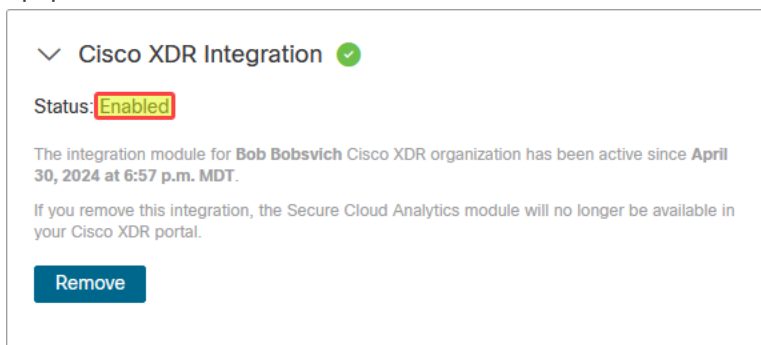
사용: Secure Cloud Analytics

1. **Secure Cloud Analytics** 웹 포털에 사이트 관리자로 로그인합니다.
2. **Settings(설정) > Integrations(통합) > XDR**로 이동합니다.
그러면 **Secure Cloud Analytics** 임플란트에 포함할 수 있는 통합이 표시됩니다.

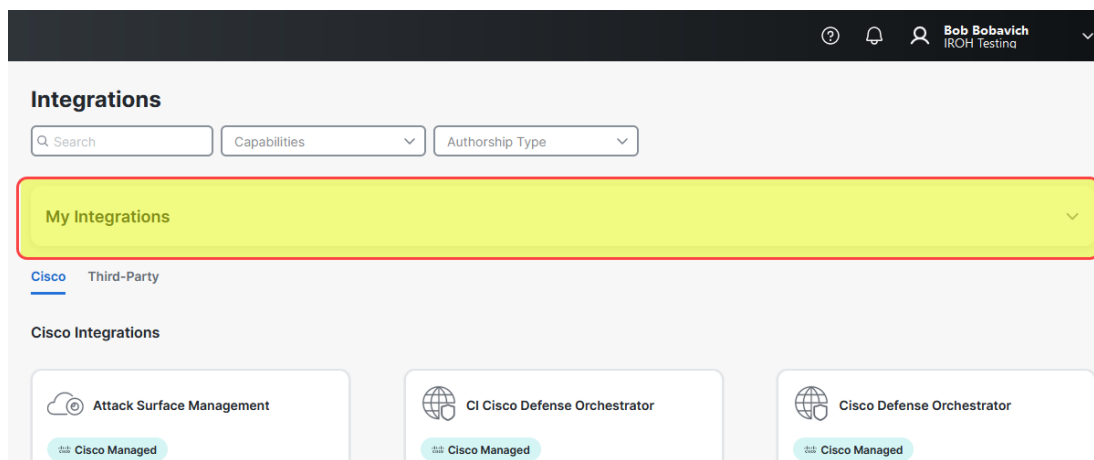
3. 아래 그림에 표시된 것과 같이 **Enable(활성화)**을 클릭합니다.



아래 그림에 표시된 것과 같이 Cisco XDR 모듈 상태가 **Enabled(활성화됨)**로 업데이트됩니다.



4. Cisco XDR로 진행합니다.
 5. **Administration(관리) > Integrations(통합)**로 이동하여 Secure Cloud Analytics 모듈을 봅니다.
 6. 아래 그림과 같이 **My Integrations(내 통합)** 드롭다운을 클릭합니다.




7. 드롭다운에서 아래로 스크롤하여 Secure Cloud Analytics 모듈을 찾습니다. 예제는 아래 그림에 나와 있습니다.


Bob Bobavich IROH Testing			
Orbital Ramya1	Orbital	Connected	Cisco Managed
OrbitalRuslan1	Orbital	Connected	Cisco Managed
SG-Orbital	Orbital	Connected	Cisco Managed
SG-Orbital-Jan31-1458	Orbital	Connected	Cisco Managed
SGOrbitalJan31	Orbital	Connected	Cisco Managed
[object Object]	Orbital	Connected	Cisco Managed
obsrvbl-staging	Secure Cloud Analytics	Connected	Cisco Managed

사용: Cisco XDR

1. Cisco XDR에 로그인합니다.
2. **Administration(관리)**으로 이동합니다.
3. **Integration(통합)**으로 이동합니다.
4. **Cisco** 탭에서 **Secure Cloud Analytics** 모듈을 찾습니다.
5. **Enable(활성화)**을 클릭합니다.



Secure Cloud Analytics

 **Cisco Managed**

Gain the visibility and continuous threat detection needed to secure your public cloud, private network, and hybrid environments.

[Free Trial](#)
[+ Enable](#)

Secure Cloud Analytics의 Cisco XDR 통합 페이지로 자동 리디렉션됩니다.



여러 Secure Cloud Analytics 포털이 있는 경우 Cisco XDR 리본에 연결한 포털을 선택해야 합니다.

Cisco XDR 모듈 상태가 *Enabled*(활성화됨)로 변경됩니다.

▼ Cisco XDR Integration ✔

Status: Enabled

The integration module for **Bob Bobsvich** Cisco XDR organization has been active since **April 30, 2024 at 6:57 p.m. MDT**.

If you remove this integration, the Secure Cloud Analytics module will no longer be available in your Cisco XDR portal.

[Remove](#)

그러면 **Cisco XDR > Integration Modules(통합 모듈) > My Integration Modules(내 통합 모듈)**로 자동 리디렉션됩니다.

 ? 🔔 👤 Bob Bobsvich IROH Testing 			
Orbital Ramya1	Orbital	✔ Connected	Cisco Managed
OrbitalRuslan1	Orbital	✔ Connected	Cisco Managed
SG-Orbital	Orbital	✔ Connected	Cisco Managed
SG-Orbital-Jan31-1458	Orbital	✔ Connected	Cisco Managed
SGOrbitalJan31	Orbital	✔ Connected	Cisco Managed
[object Object]	Orbital	✔ Connected	Cisco Managed
obsrvbi-staging	Secure Cloud Analytics	✔ Connected	Cisco Managed

알림을 다음에 게시: Cisco XDR

Secure Cloud Analytics 웹 포털에서 **게시** Cisco XDR 기능을 사용하여 알림 콘텐츠를 전송할 수 있습니다. 이렇게 하면 다음을 포함하여 Cisco XDR에서 Secure Cloud Analytics 알림 데이터의 전체 보기가 제공됩니다.

- 알림 유형
- Secure Cloud Analytics 알림 ID
- Secure Cloud Analytics 알림에 대한 참조
- 여러 Secure Cloud Analytics 포털을 Cisco XDR와 통합하는 경우, 알림이 발생한 Secure Cloud Analytics 테넌트
- 세부 설명
- 다음 단계
- 알림 업데이트 타임스탬프
- 알림 시점에 알려진 IP 주소 및 호스트 이름
- 해당되는 경우 MITER ATT&CK 전술 및 기술
- 알림 담당자
- 알림 우선순위
- 알림과 관련된 사용자 태그

알림 유형 게시 활성화



- Talos 인텔리전스 감시 목록 적중 알림은 Cisco XDR에 게시되도록 자동으로 활성화됩니다.
- 알림 유형이 비활성화된 경우, 해당 알림을 Cisco XDR에 게시할 수 없습니다.

1. Secure Cloud Analytics 웹 포털에 로그인합니다.
2. **Settings(설정)** → **Alerts(알림)**를 선택합니다.
3. Cisco XDR(으)로 전송할 알림 유형을 찾고 **Cisco XDR** 옆에서 (토글) 아이콘을(를) 클릭합니다.

알림 인스턴스를 인시던트로 수동 승격

1. Secure Cloud Analytics 웹 포털에 로그인합니다.
2. **Monitor(모니터링)** > **Alerts(알림)**로 이동합니다.
3. 원하는 알림으로 이동합니다.
4. 원하는 알림을 클릭합니다.
5. **Post to Cisco XDR(Cisco XDR에 게시)** 버튼으로 스크롤합니다.
6. **Post to Cisco XDR(Cisco XDR에 게시)**을 클릭합니다.

추가 리소스

Secure Cloud Analytics에 대한 자세한 정보는 다음을 참조하십시오.

- 일반 개요: <https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html>
- 설명서 리소스: <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html>
- Secure Cloud Analytics 초기 구축 가이드를 비롯한 설치 및 구성 가이드: <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html>

지원 팀에 문의

기술 지원이 필요하면 다음 방법 중 하나를 선택하십시오.

- 현지 Cisco 파트너에게 문의합니다.
- Cisco 지원팀에 문의
- 웹에서 사례를 확인하려면 <http://www.cisco.com/c/en/us/support/index.html>을 참조합니다.
- 이메일로 사례를 확인하려면 tac@cisco.com을 이용합니다.
- 전화 지원: 1-800-553-2447(미국)
- 월드와이드 지원 번호: <https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

변경 기록

수정	개정일	설명
1.0	2020년 6월 24일	최초 버전
1.1	2020년 12월 10일	추가 Cisco XDR 통합 정보로 업데이트되었습니다.
2.0	2021년 11월 3일	제품 브랜딩이 업데이트되었습니다.
3.0	2022년 2월 15일	구성 단계가 업데이트되었습니다.
4.0	2022년 7월 20일	Cisco XDR에 알림 게시 및 지원 문의 섹션을 추가했습니다.
5.0	2024년 6월 21일	브랜딩을 SecureX에서 Cisco XDR로 변경했습니다. 일부 절차를 명확하게 했습니다. 알림 유형 게시 활성화 항목을 생성했습니다.

저작권 정보

Cisco 및 Cisco 로고는 미국과 기타 국가에서 Cisco 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 <https://www.cisco.com/go/trademarks>로 이동하십시오. 언급된 제3자 상표는 해당 소유자의 재산입니다. '파트너'라는 용어의 사용이 Cisco와 다른 회사 간의 파트너십 관계를 의미하는 것은 아닙니다. (1721R)