XDR 분석에 대한 NVM 트러블슈팅 및 활성화

목차

소개

이 문서에서는 Cisco XDR Analytics for Cisco eExtended Detection and Response (XDR) / Network Visibility Module (NVM) 문제를 해결하는 방법에 대해 설명합니다

사전 요구 사항

XDR 통합이 포함된 활성 XDR 분석 포털

요구 사항

단일 XDR 통합으로 XDR 분석 계정 실행

사용되는 구성 요소

- XDR 분석
- XDR
- NVM 센서
- Secure Client(버전 5.0 이상)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

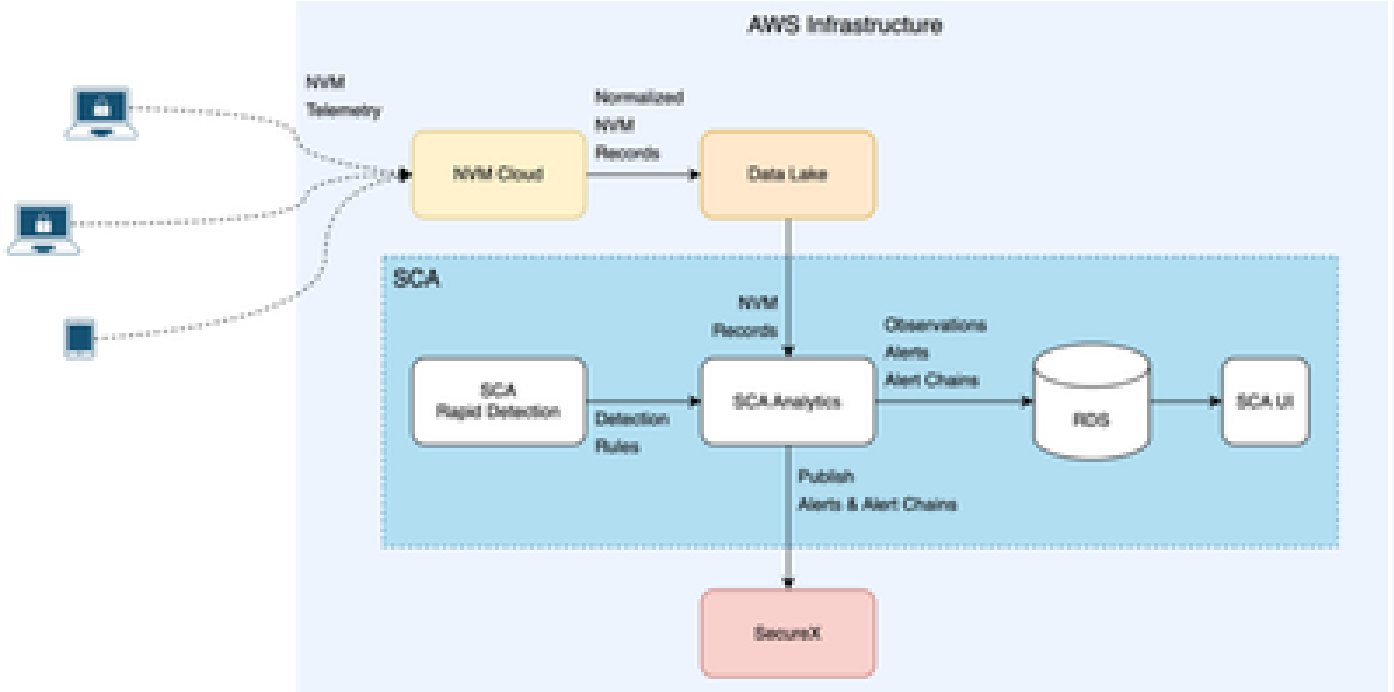
XDR 분석 NVM 흐름

XDR 분석에서 NVM 원격 분석 사용
텔레메트리는 Cisco Secure Client의 NVM 구성 요소에 의해 생성됩니다.

NVM은 사용자 행동, 네트워크 통신, 프로세스를 포함한 향상된 네트워크 가시성을 제공하여 인시던트 조사 시간을 줄이고 엔드포인트 가시성의 공백을 채웁니다

https://docs.xdr.security.cisco.com/Content/Help-Resources/nvm-resources.htm

NVM 데이터 흐름 - XDR 분석



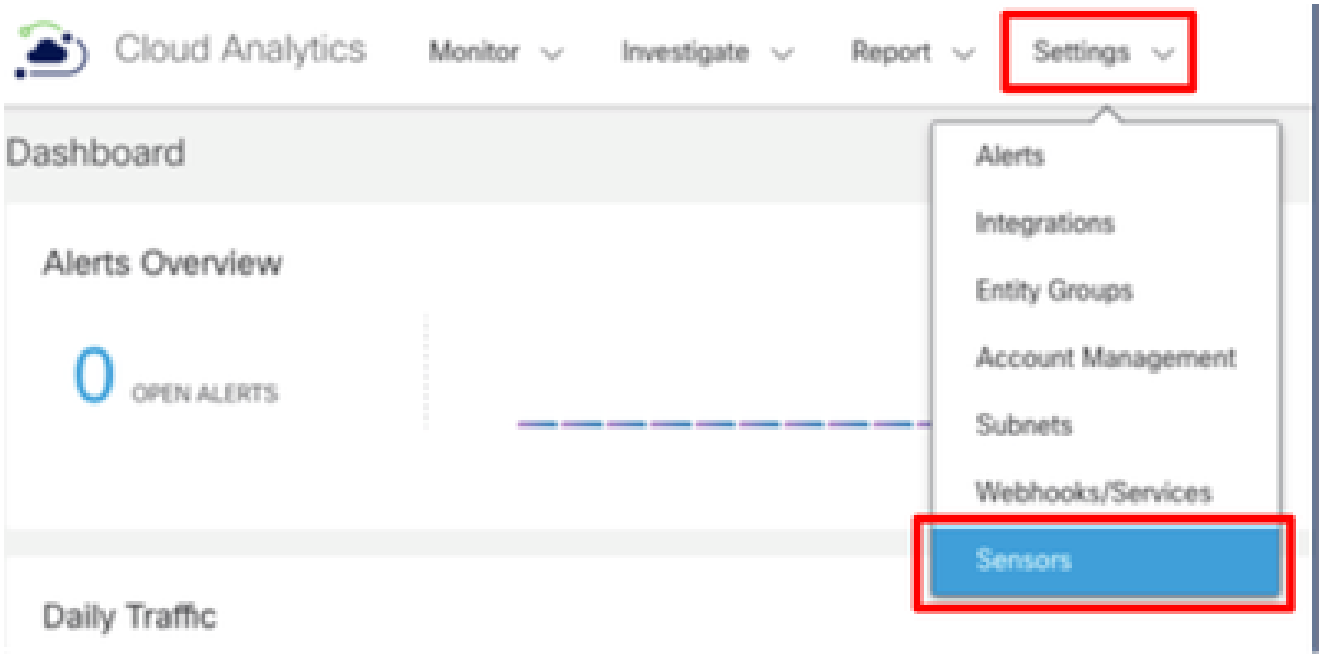
- 항상 Secure Client 버전을 최신 상태로 유지하는 것이 좋습니다. 이 워크플로에서는 Secure Client 버전 5.0 이상을 사용해야 합니다.
  https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html
- 최신 Secure Client 버전 및 Deployment Pro의 업데이트 유지 관리
  file: https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm
- NVM Cloud는 텔레메트리 볼륨을 처리하여 데이터 레이크가 텔레메트리를 수집하고 이를 표준화하여 효율적인 스토리지를 제공합니다
- XDR Analytics는 탐지 생성 - 관찰 및 알림을 위해 정기적으로(10분) NVM 레코드를 처리합니다.
- 신속한 탐지를 통해 구성을 사용하여 간단한 관찰 및 알림을 신속하게 추가할 수 있습니다.

- XDR Analytics는 알림을 공격 체인(이전의 알림 체인)과 연결

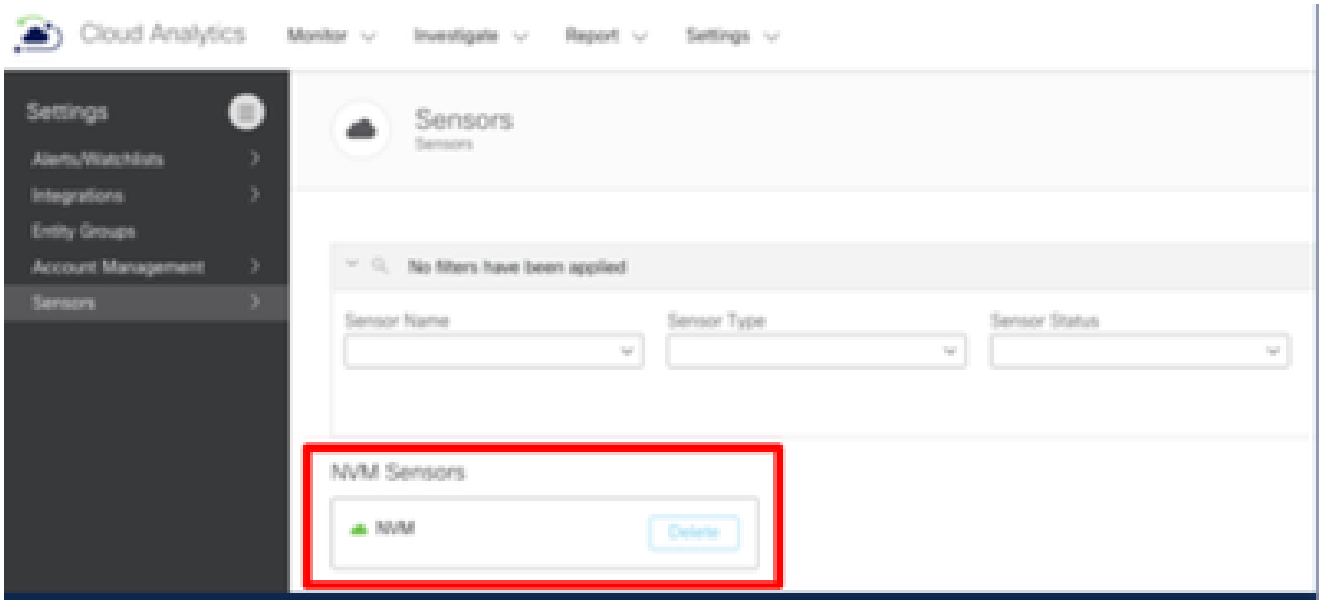
- 사용자는 경고 및 공격 체인을 XDR에 게시할 수 있습니다.

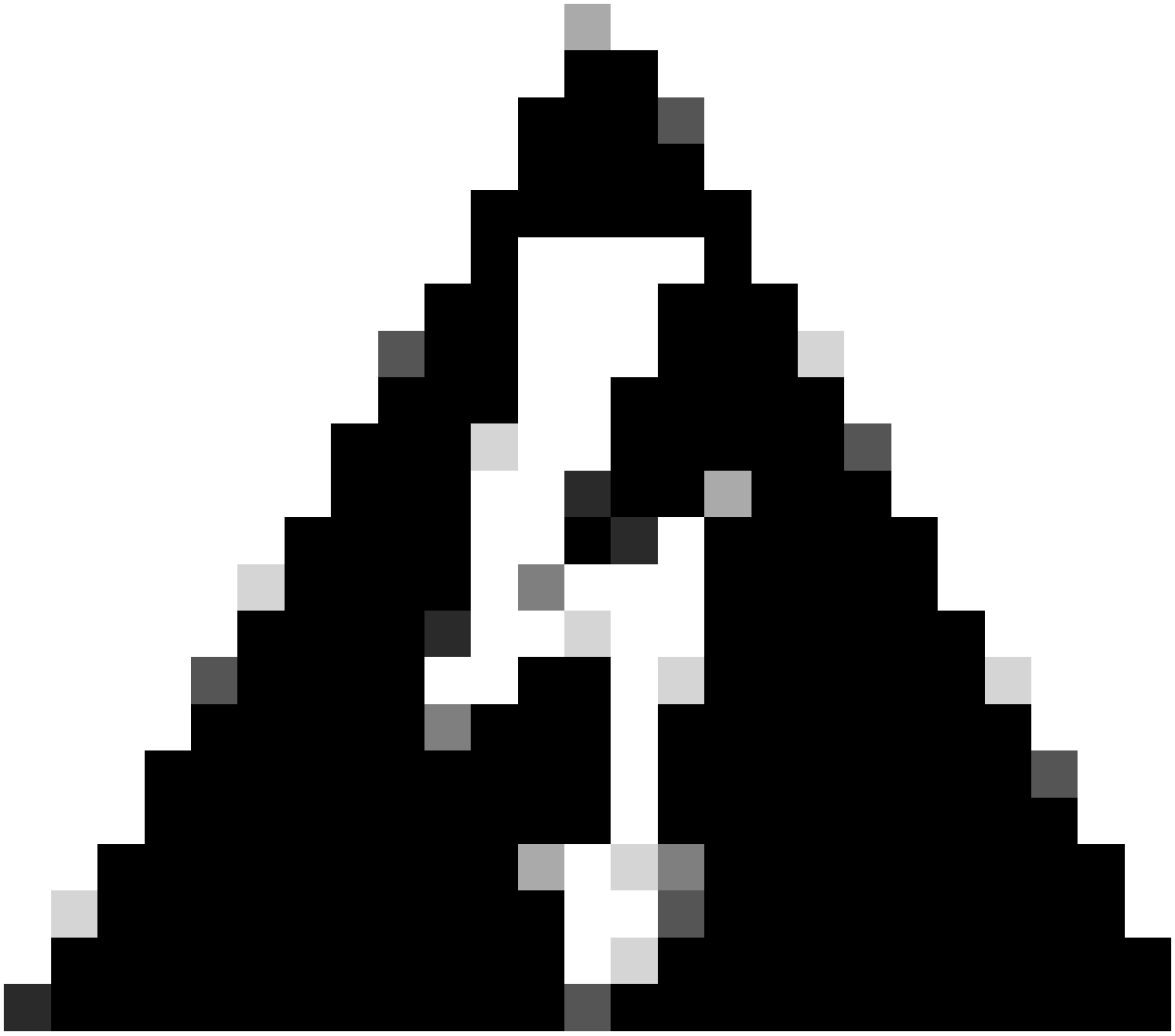
NVM 센서 상태

- NVM 센서 생성 확인:- XDR 분석 대시보드에서 settings(설정) > Sensors(센서)로 이동합니다.



- 그런 다음 NVM 센서를 센서 목록에서 사용할 수 있는지 확인합니다





경고: XDR 분석 포털에는 최대 하나의 XDR 테넌트/조직이 연결되어 있어야 합니다.

NVM 조직 ID

- NVM 클라이언트의 API 엔드포인트에서 표시되는 조직 ID가 동일한지 확인합니다. https://XDR Analytics_PORTAL_URL/api/v3/integrations/securex/orgs/

NVM Data Lake 프로비저닝 상태

- 데이터 레이크가 제대로 온보딩되었는지 확인하기 위한 API 엔드포인트는 다음 API 엔드포인트를 사용하여 연결을 확인할 수 있습니다.https://XDR Analytics_Portal_URL/api/v3/integrations/securex/orgs/onboard_datake/

- 포털을 통해 액세스 권한을 부여받은 모든 사용자가 이러한 엔드포인트(포털 관리자, TAC, 엔지니어링)에 도달할 수 있습니다.

디버깅

- 디버깅 응답 코드:

응답 코드	필요한 조치
DataLake가 프로비전되었습니다.	이벤트 뷰어를 통해 NVM 흐름 검증
데이터 레이크를 프로비전할 수 없습니다. XDR 조직이 검색되지 않았습니다.	XDR 원클릭 통합을 사용하여 XDR 및 XDR 분석을 연결합니다
데이터 팩을 프로비전할 수 없습니다. 여러 XDR 조직에서	TAC에 지원을 요청하세요

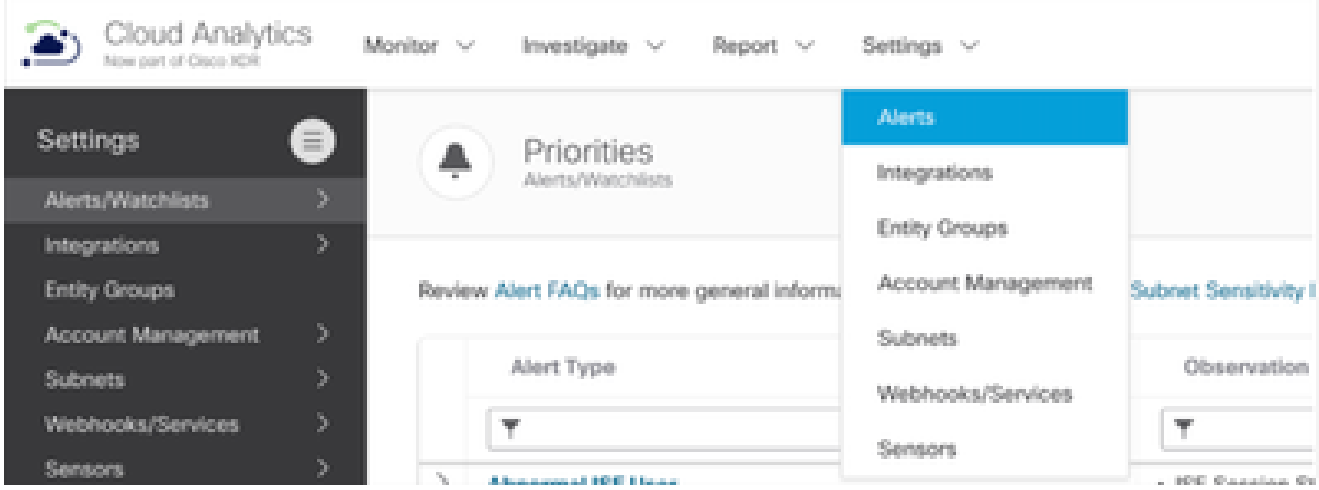
- 이 단계 중 하나라도 실패할 경우 Secure Client 인터페이스에서 DART(Secure Client Diagnostics And Reporting Tool)를 실행하여 문제를 진단합니다(항상 DART가 관리자로 실행되도록 요청)
  Secure Client용 DART 번들 수집

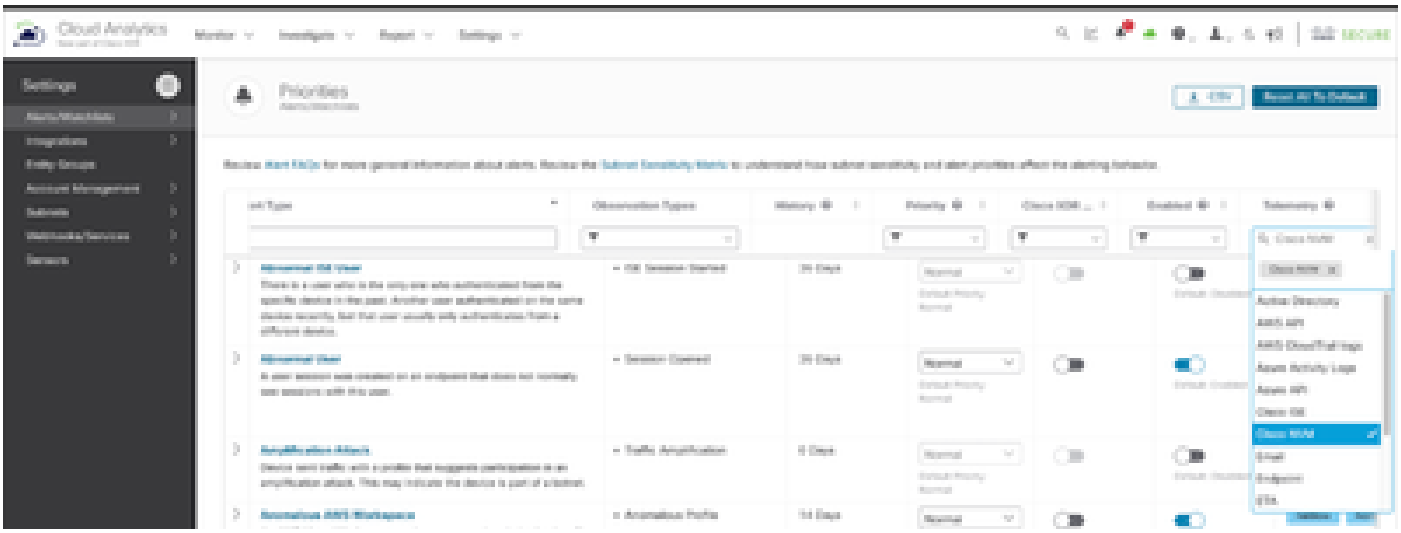
관찰 및 알림

NVM 경고

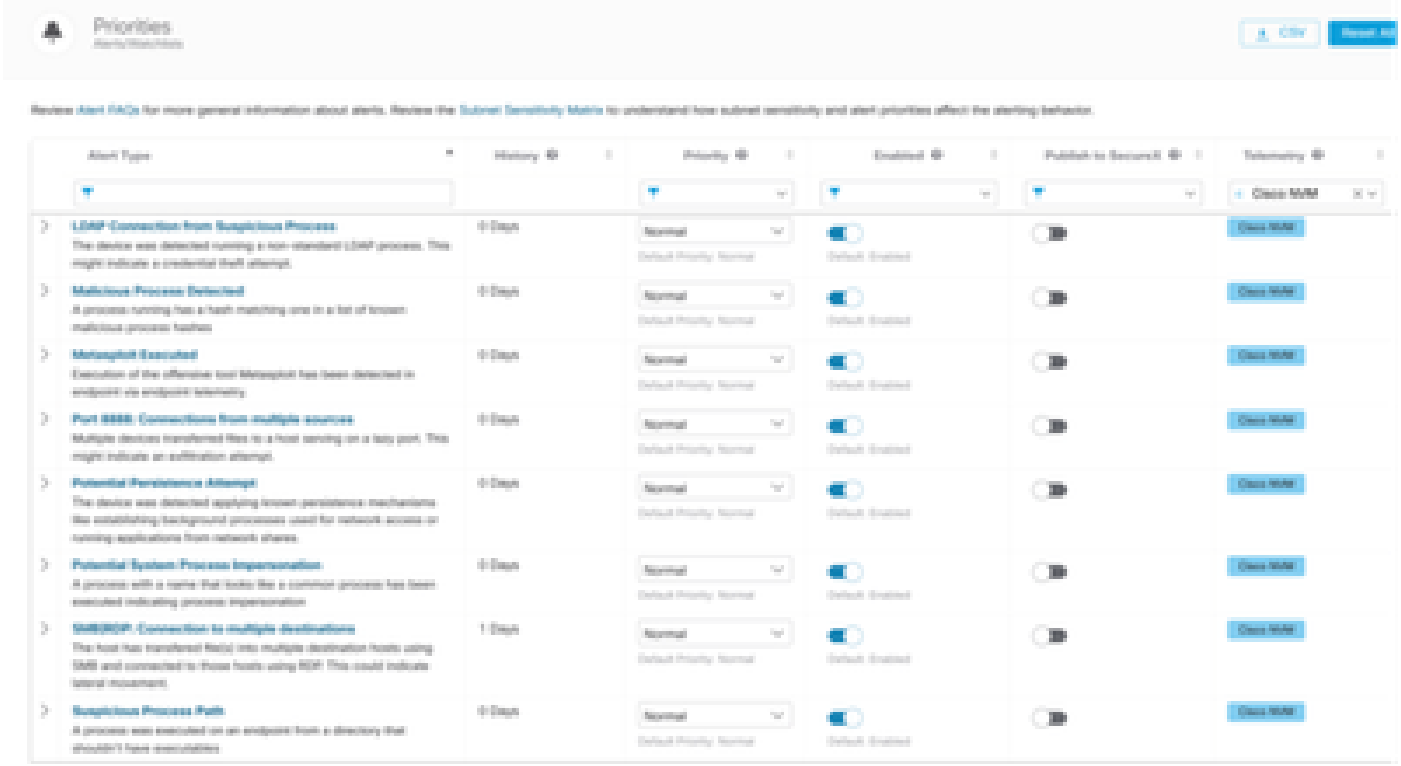
- XDR 분석 포털에 로그인
- Settings(설정) > Alerts(알림)Telemetry(원격 분석) > Cisco NVM

- 텔레메트리 > Cisco NVM


Cloud Analytics
Monitor
Investigate
Report
Settings
Settings
Alerts/Watchlists
Integrations
Entity Groups
Account Management
Subnets
Webhooks/Services
Sensors
Priorities
Alerts/Watchlists
Alerts
Integrations
Entity Groups
Account Management
Subnets
Webhooks/Services
Sensors
Review Alert FAQs for more general inform
Subnet Sensitivity
Alert Type
Observation

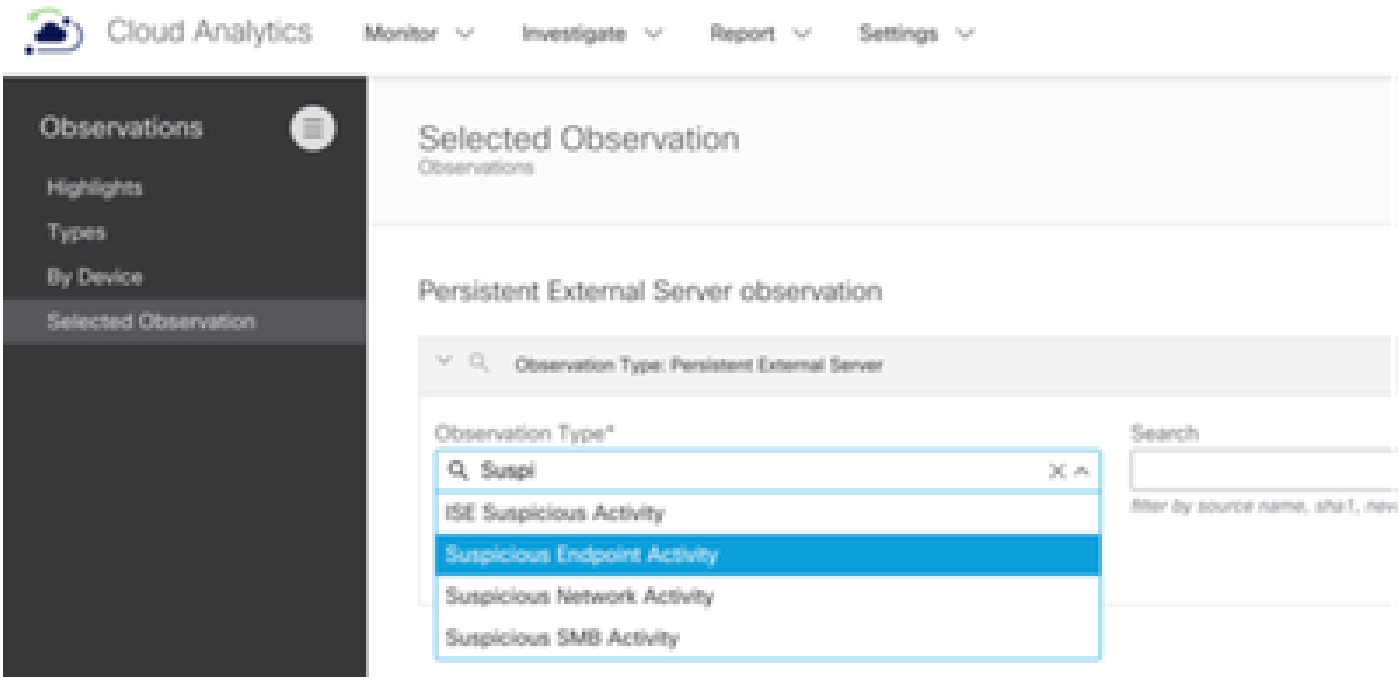


NVM 경고 설정



NVM 관찰

- 의심스러운 엔드포인트 활동
- XDR 분석 포털
- Monitor(모니터링) > Observations(관찰)
- 선택한 관찰
- 의심스러운 엔드포인트 활동 필터링



NVM 탐지 주의 사항

- NVM은 연결된 네트워크 연결이 있는 프로세스 및 플로우 데이터만 캡처합니다.
- NVM은 기본적으로 흐름 종료 시에만 흐름 데이터를 보고하도록 구성됨

결론

이 단계에서는 NVM 정보를 사용한 관찰 및 알림을 활성화하고 워크플로 문제를 해결하기 위해 XDR 분석을 탐색하는 데 도움이 됩니다.

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.