Cisco Security Analytics and Logging

Security Analytics and Logging(SaaS) 정보

Cisco SAL(Security Analytics and Logging)을 사용하면 모든 FDM 관리 디바이스에서 연결, 침입, 파일, 맬웨어 및 보안 인텔리전스 이벤트와 ASA에서 모든 syslog 이벤트 및 NSEL(Netflow Secure Event Logging) 이벤트를 캡처하고 CDO(Cisco Defense Orchestrator)의 한 곳에서 볼 수 있습니다. 이벤트는 Cisco 클라우드에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 이 페이지에서 이벤트를 필터링하고 검토하여 네트워크에서 트리거되는 보안 규칙을 명확하게 파악할 수 있습니다.

추가 라이선싱을 사용하면 이러한 이벤트를 캡처한 후 CDO에서 프로비저닝된 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다. Secure Cloud Analytics는 이벤트 및 네트워크 플로우 데이터에 대한 행동 분석을 수행하여 네트워크의 상태를 추적하는 SaaS(Software as a Service) 솔루션입니다. 방화벽 이벤트 및 네트워크 플로우 데이터를 비롯한 소스에서 네트워크 트래픽에 대한 정보를 수집하여 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. Secure Cloud Analytics는 Talos와 같은 위협 인텔리전스의 다른 소스와 결합된 이 정보를 사용하여 본질적으로 악의적인 행동이 있음을 나타내는 경고를 생성합니다. 알림과 함께 Secure Cloud Analytics는 알림을 조사하고 악의적인 동작의 소스를 찾기 위한 더 나은 기반을 제공하기 위해 수집한 네트워크 및 호스트 가시성 및 상황 정보를 제공합니다.

용어 참고: 이 설명서에서는 Cisco Security Analytics and Logging을 Secure Cloud Analytics 포털(Software as a Service 제품)과 함께 사용하는 경우 이러한 통합을 Cisco Security Analytics and Logging(SaaS) 또는 SAL(SaaS)이라고 합니다.

FDM-관리 디바이스에 대한 보안 로깅 분석

Cisco SaaS(Security Analytics and Logging)를 사용하면 모든 FDM 관리 디바이스에서 연결, 침입, 파일, 맬웨어 및 보안 인텔리전스 이벤트를 캡처하고, Cisco Defense Orchestrator의 한 곳에서 볼 수 있습니다.

이벤트는 Cisco Cloud에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 여기에서 이벤트를 필터링하고 검토하여 네트워크에서 어떤 보안 규칙이 트리거되고 있는지 명확하게 이해할 수 있습니다. **Logging and Troubleshooting(**기록 및 문제 해결**)** 패키지는 이러한 기능을 제공합니다.

Logging Analytics and Detection(로그 분석 및 탐지**)** 패키지(이전의 **Firewall Analytics and Logging(**방화벽 분석 및 로그**)** 패키지)를 통해 시스템은 Secure Cloud Analytics 동적 엔터티 모델링을 FDM 관리 디바이스 이벤트에 적용하고 동작 모델링 분석을 사용하여 Secure Cloud Analytics 관찰 및 경고를 생성할 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 패키지를 보유한 경우, 시스템은 FDM 관리 디바이스 이벤트와 네트워크 트래픽 모두에 동적 엔터티 모델링을 적용하고, 관찰 및 경고를 생성합니다. Cisco Single Sign-On을 사용하여 CDO에서 사용자를 위해 프로비저닝된 Cisco Secure Cloud Analytics 포털로 교차 실행할 수 있습니다.

FDM 이벤트가 CDO 이벤트 뷰어에 표시되는 방법

개별 규칙이 이벤트를 로깅하도록 구성되고 네트워크 트래픽이 규칙 기준과 일치하면 연결, 침입, 파일, 악성코드 및 보안 인텔리전스 이벤트가 생성됩니다. 이벤트가 Cisco cloud에 저장되면 CDO에서 볼 수 있습니다. 이벤트를 Cisco cloud로 보내도록 FDM 관리 디바이스를 구성하는 방법에는 두 가지가 있습니다.

- 모든 디바이스에서 여러 SEC(Secure Event Connector)를 설치하고 규칙에 의해 생성된 이벤트를 마치 시스템 로그 서버인 것처럼 SEC로 전송할 수 있습니다. 그런 다음 SEC는 Cisco Cloud에 이벤트를 전달합니다.
- FDM 관리 디바이스가 등록 키를 사용하도록 CDO에 온보딩된 경우, Secure Firewall device manager의 컨트롤을 사용하여 이벤트를 Cisco cloud로 직접 보낼 수 있습니다.

보안 이벤트 커넥터를 사용하여 Cisco Cloud로 이벤트를 전송하는 방법

Logging and Troubleshooting(기본 로그 및 문제 해결 **)** 라이선스를 사용하여, Secure Firewall device manager이벤트가 Cisco cloud에 도달하는 방법은 다음과 같습니다.

1. 사용자 이름과 암호를 사용하거나 등록 키를 사용하여 FDM 관리 디바이스를 CDO에 온보딩합니다.
2. 액세스 제어 규칙, 보안 인텔리전스 규칙 및 SSL 암호 해독 규칙과 같은 개별 규칙을 구성하여 마치 Syslog 서버인 것처럼 SEC 중 하나로 이벤트를 전달합니다. 액세스 제어 규칙에서 파일 및 악성코드 정책과 침입 정책을 활성화하고 해당 정책에 의해 생성된 이벤트를 SEC에 전달할 수도 있습니다.
3. 파일 이벤트에 대한 **System Settings(**시스템 설정**)** > **Logging(**기록**)**에서 파일/악성코드 로깅을 구성합니다.
4. 침입 이벤트에 대한 **System Settings(**시스템 설정**)** > **Logging(**기록**)**에서 침입 기록을 구성합니다.
5. SEC는 이벤트가 저장된 Cisco Cloud로 이벤트를 전달합니다.
6. CDO은 설정한 필터에 따라 이벤트 로그 페이지에 Cisco cloud의 이벤트가 표시됩니다.

Logging Analytics and Detection(로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 사용하면 다음 작업도 수행됩니다.

1. Cisco Secure Cloud Analytics는 Cisco cloud에 저장된 Secure Firewall device manager 연결 이벤트에 분석을 적용합니다.
2. 생성된 관찰 및 경고는 CDO 포털과 연결된 Secure Cloud Analytics 포털에서 액세스할 수 있습니다.
3. CDO 포털에서 Secure Cloud Analytics 포털을 교차 실행하여 이러한 관찰 및 경고를 검토할 수 있습니다.

Secure Firewall device manager에서 **Cisco Cloud**로 이벤트가 직접 전송되는 방식

기본 로그 및 문제 해결 라이센스를 사용하면 다음과 같이 Secure Firewall device manager 이벤트가 Cisco cloud에 도달합니다.

1. 등록 토큰을 사용하여 FDM 관리 디바이스를 CDO에 온보딩합니다.
2. 액세스 제어 규칙, 보안 인텔리전스 규칙, SSL 암호 해독 규칙 등의 개별 규칙을 구성하여 이벤트를 로깅하지만 이벤트를 전송할 Syslog 서버는 지정하지 않습니다. 액세스 제어 규칙에서 파일 및 악성코드 정책과 침입 정책을 활성화하고 해당 정책에 의해 생성된 이벤트를 Cisco Cloud로 전달할 수도 있습니다.
3. 파일 및 악성코드 정책과 침입 정책이 연결 이벤트를 로깅하도록 액세스 제어 규칙에 구성된 경우 파일 이벤트 및 침입 이벤트가 Cisco Cloud로 전송됩니다.
4. Secure Firewall device manager에서 Cloud Logging을 활성화하면 다양한 규칙에 기록된 이벤트가 Cisco cloud로 전송됩니다.
5. CDO은 설정한 필터를 기반으로 Cisco cloud에서 이벤트를 가져와 이벤트 뷰어에 표시합니다.

Logging Analytics and Detection(로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 사용하면 다음 작업도 수행됩니다.

1. Cisco Secure Cloud Analytics는 Cisco cloud에 저장된 Secure Firewall device manager 연결 이벤트에 분석을 적용합니다.
2. 생성된 관찰 및 경고는 CDO 포털과 연결된 Secure Cloud Analytics 포털에서 액세스할 수 있습니다.
3. CDO 포털에서 Secure Cloud Analytics 포털을 교차 실행하여 이러한 관찰 및 경고를 검토할 수 있습니다.

구성 비교

다음은 SEC를 통해 Cisco cloud로 이벤트를 보내는 것과 Cisco cloud로 직접 이벤트를 보내는 것 사이의 CDO 구성 차이점에 대한 요약입니다.

FDM-관리 디바이스 구성	**SEC(**보안 이벤트 커넥터**)**를 통해 이벤트를 전송하는 경우	이벤트를 **Cisco Cloud**에 직접 전송하는 경우
FDM-관리 디바이스에 대한CDO 온보딩 방법	자격 증명(사용자 이름 및 비밀번호) 등록 토큰	등록 토큰 일련 번호
버전 지원	버전 6.4+	등록 토큰 - 버전 6.5+ 일련 번호 - 버전 6.7+

FDM-관리 디바이스 구성	**SEC**(보안 이벤트 커넥터)를 통해 이벤트를 전송하는 경우	이벤트를 **Cisco Cloud**에 직접 전송하는 경우
Cisco Security Analytics and Logging (SaaS) 라이선스	로깅 및 문제 해결 로깅 분석 및 탐지(선택 사항) 총 네트워크 분석 및 모니터링(선택 사항)	로깅 및 문제 해결 로깅 분석 및 탐지(선택 사항) 총 네트워크 분석 및 모니터링(선택 사항)
라이선스	라이선스 -침입 규칙, 파일 제어 규칙 또는 보안 인텔리전스 필터링에서 연결 이벤트를 수집하려는 경우. 맬웨어 -파일 제어 규칙에서 연결 이벤트를 수집하려는 경우.	라이선스 -침입 규칙, 파일 제어 규칙 또는 보안 인텔리전스 필터링에서 연결 이벤트를 수집하려는 경우. 맬웨어 -파일 제어 규칙에서 연결 이벤트를 수집하려는 경우.
보안 이벤트 커넥터	필수	해당 없음
데이터 압축*	이벤트가 압축됨*	이벤트가 압축되지 않음*
데이터 요금제	필수	필수

참고 데이터 서브스크립션 및 과거 월간 사용량은 사용하는 압축되지 않은 데이터의 양을 기준으로 합니다.

솔루션의 구성 요소

Cisco SaaS(Security Analytics and Logging)는 이러한 구성 요소를 사용하여 CDO에 다음 이벤트를 전달합니다.

보안 디바이스 커넥터**(SDC)**- SDC는 CDO를 FDM 관리 디바이스에 연결합니다. FDM 관리 디바이스의 로그인 자격 증명은 SDC에 저장됩니다. 자세한 내용은 SDC(Secure Device Connector)을 참조하십시오.

보안 이벤트 커넥터**(SEC)**-SEC는 FDM 관리 디바이스에서 이벤트를 수신하여 Cisco cloud로 전달하는 애플리케이션입니다. Cisco cloud에 있으면 CDO의 Event Logging 페이지에서 이벤트를 보거나 Cisco Secure Cloud Analytics로 분석할 수 있습니다. 테넌트와 연결된 SEC가 하나 이상 있을 수 있습니다. 환경에 따라 보안 디바이스 커넥터 또는 CDO 커넥터 VM에 보안 이벤트 커넥터를 설치합니다.

Secure Firewall device manager- FDM 관리 디바이스는 Cisco의 차세대 방화벽입니다. 네트워크 트래픽 및 액세스 제어에 대한 상태 저장 검사 외에도, FDM 관리 디바이스는 맬웨어 및 애플리케이션 계층 공격으로부터 보호, 통합 침입 방지 및 클라우드 제공 위협 인텔리전스와 같은 기능을 제공합니다.

Logging Analytics and Detection(로깅 분석 및 탐지) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스가 있는 경우 Cisco SaaS(Security Analytics and Logging)는 Cisco Secure Cloud Analytics를 사용하여 CDO에 전달된 이벤트를 추가로 분석합니다.

Cisco Secure Cloud Analytics-Secure Cloud Analytics는 이벤트에 동적 엔터티 모델링을 적용하여 이 정보를 기반으로 탐지를 생성합니다. 이렇게 하면 네트워크에서 수집한 텔레메트리를 심층적으로 분석하여 추세를 식별하고 네트워크 트래픽의 이상 동작을 검사할 수 있습니다.

라이선싱

이 솔루션을 구성하려면 다음 계정 및 라이선스가 필요합니다.

Cisco Defense Orchestrator. CDO 테넌트가 있어야 합니다.

Secure Device Connector. SDC에 대한 별도의 라이선스는 없습니다.

Secure Event Connector. SEC에 대한 별도의 라이선스는 없습니다.

Secure Logging Analytics(SaaS). **Logging and Troubleshooting** 라이선스를 구매해야 합니다. 이 패키지의 목표는 온보딩 FDM 관리 디바이스에서 파생된 실시간 및 기록 이벤트를 네트워크 운영 팀에 제공하여 네트워크의 트래픽 문제를 해결하고 분석하는 것입니다.

또한 **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매하여 Cisco Secure Cloud Analytics를 적용할 수 있습니다. 이 패키지의 목표는 네트워크 운영 팀에 이벤트(및 Total Network Analytics 및 Monitoring 라이선스가 있는 네트워크 트래픽)에 대한 추가 통찰력을 제공하여 가능한 비정상적인 동작을 더 잘 식별하고 이에 대응하는 것입니다.

라이선스 이름	제공된 기능	사용가능한라이선스기간	기능 사전 요건
로깅 및 문제 해결	CDO에서 라이브 피드 및 기록 보기로 이벤트 및 이벤트 세부 정보 보기	• 1년 • 3년 • 5년	• CDO • 버전 6.4 이상을 실행하는 온프레미스 배포 . • 이벤트를 클라우드로 전달하기 위해 하나 이상의 SEC 배포

라이선스 이름	제공된 기능	사용 가능한 라이선스 기간	기능 사전 요건
로깅 분석 및 탐지(이전 이름 방화벽 분석 및 모니터링)	로깅 및 문제 해결 기능 추가: • FDM 관리 디바이스 이벤트에 동적 엔터티 모델링 및 동작 분석을 적용합니다 • CDO 이벤트 뷰어에서 교차 실행하여 이벤트 데이터를 기반으로 Secure Cloud Analytics에서 알림을 엽니다.	• 1년 • 3년 • 5년	• CDO • 버전 6.4 이상을 실행하는 온프레미스 배포. • 이벤트를 클라우드로 전달하기 위해 하나 이상의 SEC 배포. • 새로 프로비저닝된 또는 기존의 Secure Cloud Analytics 포털.

라이선스 이름	제공된 기능	사용가능한라이선스기간	기능 사전 요건
총 네트워크 분석 및 모니터링	로깅 분석 및 탐지, 추가: • 이벤트, 온프레미스 네트워크 트래픽 및 클라우드 기반 네트워크 트래픽에 동적 엔터티 모델링 및 동작 분석을 적용합니다. • 이벤트 데이터, Secure Cloud Analytics 센서에서 수집한 온프레미스 네트워크 트래픽 플로우 데이터, Secure Cloud Analytics로 전달된 클라우드 기반 네트워크 트래픽의 조합을 기반으로 Secure Cloud Analytics에서 경고를 열고, CDO 이벤트 뷰어에서 교차 실행합니다.	• 1년 • 3년 • 5년	• CDO • 버전 6.4 이상을 실행하는 온프레미스 배포 . • 이벤트를 클라우드로 전달하기 위해 하나 이상의 SEC 배포 . • 네트워크 트래픽 플로우 데이터를 클라우드에 전달하기 위해 하나 이상의 Secure Cloud Analytics 센서 버전 4.1 이상을 배포하거나, 네트워크 트래픽 플로우 데이터를 Secure Cloud Analytics로 전달하기 위해 Secure Cloud Analytics를 클라우드 기반 배포과 통합합니다. • 새로 프로비저닝된 또는 기존의 Secure Cloud Analytics 포털.

FDM-관리 장치. FDM 관리 디바이스를 실행하고 보안 이벤트를 생성하는 규칙을 생성하려면 다음 라이선스가 있어야 합니다.

라이선스	기간	부여된 기능
Essentials(이센셜)(자동 포함)	영구	선택적 기간 라이선스가 적용되지 않는 모든 기능. 이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능을 허용할지도 지정해야 합니다. 현재 거주 국가가 내보내기 제어 표준을 충족하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션은 고급 암호화 사용과 고급 암호화를 필요로 하는 기능 사용을 제어합니다.
	기간 기준	침입 탐지 및 방지 - 침입 정책은 침입 및 익스플로잇의 트래픽을 분석하고, 선택적으로 문제가 되는 패킷을 삭제할 수 있습니다. 파일 제어 - 파일 정책은 사용자가 특정 유형의 파일을 업로드(전송)하거나 다운로드(수신)하는 것을 탐지하고, 선택적으로 차단할 수 있습니다. 맬웨어 라이선스가 필요한 AMP for Firepower를 사용하면, 맬웨어가 포함된 파일을 검사하고 차단할 수 있습니다. 모든 유형의 파일 정책을 사용하려면 Threat(위협) 라이선스가 있어야 합니다. 보안 인텔리전스 필터링 - 트래픽이 액세스 제어 규칙을 기준으로 분석 대상이 되기 전에 선택한 트래픽을 삭제합니다. 동적 피드를 사용하면 최신 인텔리전스를 기반으로 연결을 즉시 삭제할 수 있습니다.

라이선스	기간	부여된 기능
맬웨어	기간 기준	악성코드를 확인하는 파일 정책으로서 Cisco AMP(Advanced Malware Protection)를 AMP for Firepower(네트워크 기반 Advanced Malware Protection) 및 Cisco Threat Grid와 함께 사용합니다. 파일 정책은 네트워크를 통해 전송된 파일에서 악성코드를 탐지하고 차단할 수 있습니다.

데이터 요금제

Cisco cloud가 온보딩 FDM 관리 디바이스에서 매일 수신하는 이벤트 수를 반영하는 데이터 스토리지 플랜을 구매해야 합니다. 수집 속도를 결정하는 가장 좋은 방법은 SaaS(Secure Logging Analytics)를 구매하기 전에 무료 평가판에 참여하는 것입니다. 이를 통해 이벤트 볼륨을 적절하게 예측할 수 있습니다. 또한 Logging Volume Estimator Tool을 사용할 수 있습니다.

주의 이벤트를 Cisco cloud로 직접 전송하거나 SEC를 통해 동시에 전송하도록 FDM 관리 디바이스를 구성할 수 있습니다. 이렇게 하면 동일한 이벤트가 두 번 "수집"되고 데이터 요금제에 대해 두 번 계산되지만 Cisco Cloud에는 한 번만 저장됩니다. 불필요한 요금이 발생하지 않도록 한 가지 방법 또는 다른 방법을 사용하여 Cisco Cloud에 이벤트를 전송해야 합니다.

데이터 요금제는 일별 볼륨 1GB 단위로 제공되며 1년, 3년 또는 5년 단위로 제공됩니다. 데이터 요금제에 대한 자세한 내용은 Secure Logging Analytics(SaaS) 주문 가이드를 참조하십시오.

참고 Security Analytics and Logging 라이선스 및 데이터 요금제를 보유하고 있는 경우 나중에 다른 라이선스를 취득할 수 있으며, 이것만 있으면 다른 데이터 요금제를 구매할 필요가 없습니다. 네트워크 트래픽 처리량이 변경되어 다른 데이터 플랜을 취득하는 경우에는 다른 Security Analytics and Logging 라이선스를 구입하지 않아도 됩니다.

30일 무료 평가판

CDO에 로그인하고 분석 > 이벤트 로깅로 이동하여 30일 위험 부담 없는 평가판을 요청할 수 있습니다. 30일 평가판이 끝나면 SaaS(Secure Logging Analytics) 주문 가이드의 지침에 따라 CCW(Cisco Commerce Workspace)에서 서비스를 계속하기 위해 원하는 이벤트 데이터 볼륨을 주문할 수 있습니다.

다음 작업**?**

FDM-관리 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, 11 페이지를 계속 진행합니다.

FDM-관리 디바이스에 대한 SaaS(Secure Logging Analytics) 구현

시작하기 전에

- 다음에 대한 자세한 사항은 FDM-관리 디바이스에 대한 보안 로깅 분석, on page 2의 내용을 검토합니다.
  - Cisco Cloud로 이벤트를 전송하는 방법
  - 솔루션의 애플리케이션
  - 필요한 라이선스
  - 필요한 데이터 요금제
- 매니지드 서비스 제공자 또는 Cisco Defense Orchestrator 영업 담당자에게 문의했으며 CDO 테넌트가 있습니다.
- 테넌트는 CDO가 FDM 관리 디바이스와 연결하는 데 SDC(Secure Device Connector)를 사용하거나 사용하지 않을 수 있습니다. 디바이스 자격 증명을 사용하여 온보딩하는 FDM 관리 디바이스에 대해 테넌트에 SDC가 설치되어 있어야 하며, 이는 모범 사례로 간주됩니다. 등록 키 또는 일련 번호를 사용하여 FDM 관리 디바이스를 온보딩하는 경우 SDC가 필요하지 않습니다.
- 테넌트에 대한 SDC를 설치한 경우 SDC 상태가 **Active(**활성**)**이고 최근 하트비트를 기록했는지 확인합니다.
- SDC를 설치하는 경우 다음 방법 중 하나를 사용하여 설치합니다.
  - CDO의 준비된 VM 이미지를 사용하여 SDC를 설치하려면 Deploy a secure device connector using CDO's VM image(CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축)를 사용합니다. 이는 SDC를 구축하는 가장 쉬운 방법입니다.
  - Deploy a secure device connector using your own VM(사용자 고유의 VM을 사용하여 보안 디바이스 커넥터 구축)을 사용합니다.
- 테넌트에 대해 CDO 이미지를 사용하여 SEC 설치할 수 있으며, 임의의 Firewall Device Manager에서 테넌트에 온보딩된 하나의 SEC로 이벤트를 전송할 수 있습니다.
- firewall device manager에서 Cisco 클라우드로 이벤트를 직접 전송하는 경우 관리 인터페이스의 포트 443에서 아웃바운드 액세스를 연 것입니다.
- 어카운트 사용자에 대한 이중 인증을 설정했습니다.

SaaS(Secure Logging Analytics)를 구현하고 보안 이벤트 커넥터를 통해 **Cisco Cloud**로 이벤트를 전송하는 새로운 **CDO** 고객 워크플로우

1. FDM 관리 디바이스 온보딩 관리자 사용자 이름 및 비밀번호 또는 등록 토큰을 사용하여 디바이스를 온보딩할 수 있습니다.
2. SaaS(Secure Logging Analytics)용 시스템 로그 서버 개체를 생성합니다.
3. 연결 이벤트를 기록하도록 FDM 관리 장치 정책을 구성합니다.
4. Cisco Defense Orchestrator 이벤트 로깅에 FDM 이벤트 전송하도록 FDM 관리 디바이스를 구성합니다.
5. 이벤트가 CDO에 표시되는지 확인합니다. 내비게이션 바에서 분석 > 이벤트 로깅을 선택합니다. 라이브 이벤트를 보려면 Live(라이브) 탭을 클릭합니다.
6. **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 Cisco Secure Cloud Analytics에서 이벤트 분석을 계속 진행합니다.

SaaS(Secure Logging Analytics)를 구현하고 **Cisco Cloud**에 직접 이벤트를 전송하는 새로운 **CDO** 고객 워크플로우

1. FDM 관리 디바이스 온보딩 등록 키만 사용할 수 있습니다.
2. 연결 이벤트를 기록하도록 FDM 관리 장치 정책을 구성합니다.
3. FDM-관리 이벤트를 Cisco Cloud에 직접 전송하도록 FDM 관리 디바이스를 구성합니다.
4. 이벤트가 CDO에 표시되는지 확인합니다. 내비게이션 바에서 분석 > 이벤트 로깅을 선택합니다. 라이브 이벤트를 보려면 Live(라이브) 탭을 클릭합니다.
5. **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 Cisco Secure Cloud Analytics에서 이벤트 분석을 계속 진행합니다.

SaaS(Secure Logging Analytics)를 구현하고 보안 이벤트 커넥터를 통해 **Cisco Cloud**로 이벤트를 전송하는 기존 **CDO** 고객 워크플로우

1. FDM 관리 디바이스 온보딩 관리자 사용자 이름 및 비밀번호 또는 등록 토큰을 사용하여 디바이스를 온보딩할 수 있습니다.
2. SaaS(Secure Logging Analytics)용 시스템 로그 서버 개체.
3. 연결 이벤트를 기록하도록 FDM 관리 장치 정책을 구성합니다.
4. Cisco Defense Orchestrator 이벤트 로깅에 FDM 이벤트 전송.
5. 이벤트가 CDO에 표시되는지 확인합니다. 내비게이션 바에서 분석 > 이벤트 로깅을 선택합니다. 라이브 이벤트를 보려면 Live(라이브) 탭을 클릭합니다.

6. **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 Cisco Secure Cloud Analytics에서 이벤트 분석을 계속 진행합니다.

SaaS(Secure Logging Analytics)를 구현하고 **Cisco Cloud**에 직접 이벤트를 전송하는 기존 **CDO** 고객 워크플로우

1. FDM 관리 디바이스 온보딩 등록 키만 사용할 수 있습니다.
2. 연결 이벤트를 기록하도록 FDM 관리 장치 정책을 구성합니다.
3. FDM-관리 이벤트를 Cisco Cloud에 직접 전송하도록 FDM 관리 디바이스를 구성합니다.
4. 이벤트가 CDO에 표시되는지 확인합니다. 내비게이션 바에서 분석 > 이벤트 로깅을 선택합니다. 라이브 이벤트를 보려면 Live(라이브) 탭을 클릭합니다.
5. **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 Cisco Secure Cloud Analytics에서 이벤트 분석을 계속 진행합니다.

Cisco Secure Cloud Analytics에서 이벤트 분석

Logging Analytics and Detection(로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 이전 단계와 함께 다음을 수행합니다.

1. Cisco Secure Cloud Analytics 포털 프로비저닝, on page 38.
2. **Total Network and Monitoring** 라이선스를 구매한 경우 하나 이상의 Secure Cloud Analytics 센서를 내부 네트워크에 구축합니다. 전체 네트워크 분석 및 보고를 위한 Cisco Secure Cloud Analytics 센서 구축, on page 40의 내용을 참조하십시오.
3. Cisco SSO(Single Sign-On) 자격 증명에 연결된 Secure Cloud Analytics 사용자 어카운트를 생성하도록 사용자를 초대합니다. CDO에서 Cisco Secure Cloud Analytics 알림 보기, on page 41의 내용을 참조하십시오.
4. firewall device manager 이벤트에서 생성된 Secure Cloud Analytics 알림을 모니터링하려면 CDO에서 Secure Cloud Analytics를 교차 실행합니다. CDO에서 Cisco Secure Cloud Analytics 알림 보기, on page 41의 내용을 참조하십시오.

CDO에서 교차 실행하여 **Secure Cloud Analytics** 알림 검토

Logging Analytics and Detection(로깅 애널리틱스 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 애널리틱스 및 모니터링**)** 라이선스를 사용하면 CDO에서 Secure Cloud Analytics로 교차 실행하여 firewall device manager 이벤트를 기반으로 Secure Cloud Analytics에서 생성된 알림을 검토할 수 있습니다.

자세한 내용은 다음 문서를 참조하십시오.

- CDO에 로그인

- CDO에서 Cisco Secure Cloud Analytics 알림 보기, on page 41
- Cisco Secure Cloud Analytics 및 동적 엔티티 모델링, on page 42
- 방화벽 이벤트 기반 알림 작업

SaaS(Secure Analytics and Logging) 워크플로우

보안 및 분석 로깅 이벤트를 사용한 문제 해결에서는 SaaS(Secure Logging Analytics)에서 생성된 이벤트를 사용하여 사용자가 네트워크 리소스에 액세스할 수 없는 이유를 확인하는 방법을 설명합니다.

방화벽 이벤트 기반 알림 작업도 참고합니다.

Cisco Defense Orchestrator 이벤트 로깅에 FDM 이벤트 전송

이벤트 로깅 뷰어에서 액세스 제어 규칙, 보안 인텔리전스 규칙 및 SSL 암호 해독 규칙의 FDM 관리 이벤트를 보려면 먼저 해당 이벤트를 Cisco 클라우드로 전송해야 합니다.

- 액세스 제어 규칙. 네트워크 연결의 시작 또는 종료 시 FDM-관리 이벤트 유형를 로깅할 수 있습니다. 이 규칙 유형에 대한 로깅 구성에 대한 자세한 내용은 FDM 액세스 제어 정책 구성 및 FDM 액세스 제어 규칙의 로깅 설정을 참조하십시오.
- 보안 인텔리전스 규칙. 보안 인텔리전스 규칙에 의해 생성된 FDM-관리 이벤트 유형를 로깅할 수 있습니다. 로깅을 활성화하면 차단 목록 항목과 일치하는 항목이 로깅됩니다. 로깅이 활성화된 상태에서 제외된 연결이 액세스 제어 규칙과 일치하는 경우에는 로그 메시지를 받더라도 예외 항목과 일치하는 항목은 로깅되지 않습니다. 로깅 구성에 대한 자세한 내용은 Firepower 보안 인텔리전스 정책 구성을 참조하십시오.
- **SSL** 암호 해독 규칙. SSL 암호 해독 규칙에 의해 생성된 FDM-관리 이벤트 유형를 로깅할 수 있습니다.

파일 및 악성코드 이벤트 또는 침입 이벤트를 Cisco Cloud로 전송하고 보안 이벤트 커넥터를 사용하는 경우 디바이스에 대한 로깅 설정을 구성해야 합니다.

관련 정보:

- SaaS(Secure Logging Analytics)를 위한 시스템 로그 서버 개체 생성

FDM-관리 이벤트를 Cisco Cloud에 직접 전송

Firewall Device Manager 버전 6.5부터는 연결 이벤트, 침입, 파일 및 악성코드 이벤트를 FDM 관리 디바이스에서 Cisco Cloud로 직접 전송할 수 있습니다. Cisco Cloud에 있으면 Cisco Defense Orchestrator(CDO)로 모니터링하고 Cisco Secure Cloud Analytis로 분석할 수 있습니다. 이 방법에서는 SDC(보안 디바이스 커넥터) 가상 머신에 SEC(보안 이벤트 커넥터) 컨테이너를 설치할 필요가 없습니다.

Before you begin

다음 항목을 검토합니다.

- FDM-관리 디바이스에 대한 보안 로깅 분석, on page 2
- FDM-관리 디바이스에 대한 SaaS(Secure Logging Analytics) 구현

Procedure

단계 **1** Cisco Cloud로 이벤트를 전송하려는 디바이스의 Firewall Device Manager에 로그온합니다.

단계 **2** 이렇게 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)**를 선택합니다.

단계 **3** Send Events to the Cisco Cloud(Cisco cloud로 이벤트 전송) 창에서 **Enable(**활성화**)**를 클릭합니다.

FDM-관리 이벤트 유형

이벤트 유형

시스템은 다음 이벤트 유형을 생성할 수 있습니다. 모니터링 대시보드에서 관련된 통계를 확인하려면 이러한 이벤트를 생성해야 합니다.

데이터(진단) 이벤트

데이터 기록에서는 디바이스 및 시스템 상태, 네트워크 구성 관련 이벤트에 대한 syslog 메시지를 제공합니다. 이러한 이벤트는 연결과 관련이 없습니다. 개별 액세스 제어 규칙 내에서 연결 로깅을 구성합니다.

데이터 기록에서는 데이터 플레인에서 실행되는 기능, 즉 **show running-config** 명령으로 볼 수 있는 CLI 구성에 정의된 기능에 대해 메시지를 생성합니다. 여기에는 라우팅, VPN, 데이터 인터페이스, DHCP 서버, NAT 등과 같은 기능이 포함됩니다.

연결 이벤트

사용자가 시스템을 통과하는 트래픽을 생성할 때 연결에 대한 이벤트를 생성할 수 있습니다. 액세스 규칙에서 연결 로깅을 활성화하여 이러한 이벤트를 생성합니다. 보안 인텔리전스 정책과 SSL 암호 해독 규칙에서 로깅을 활성화하여 연결 이벤트를 생성할 수도 있습니다.

연결 이벤트에는 탐지된 세션에 관한 데이터가 포함되어 있습니다. 모든 개별 연결 이벤트에 대한 정보는 몇 가지 요소에 따라 가용성이 결정되지만, 일반적으로는 다음과 같습니다.

- 기본 연결 속성: 타임 스탬프, 소스 및 대상 IP 주소, 인그레스 및 이그레스 영역, 연결을 처리한 디바이스 등
- 시스템에서 검색하거나 유추한 추가 연결 속성: 애플리케이션, 요청된 URL 또는 연결과 관련된 사용자 등

- 연결이 로깅된 사유에 대한 메타데이터: 어떤 설정이 트래픽을 처리했는지, 연결이 허용 또는 차단되었는지, 암호화 및 해독된 연결에 대한 상세정보 등

침입 이벤트

시스템은 호스트 및 호스트 데이터의 가용성, 무결성 및 기밀성에 영향을 미칠 수 있는 악성 활동 탐지를 위해 네트워크를 통과하는 패킷을 검토합니다. 시스템은 침입 가능성을 식별하는 경우 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 상황 정보의 레코드인 침입 이벤트를 생성합니다. 침입 이벤트는 호출하는 액세스 제어 규칙의 로깅 컨피그레이션과 관계없이 차단하거나 알리도록 설정된 모든 침입 규칙에 대해 생성됩니다.

파일 이벤트

파일 이벤트는 파일 정책을 기준으로 하여 시스템이 네트워크 트래픽에서 탐지하고 선택적으로 차단한 파일을 나타냅니다. 이러한 이벤트를 생성하려면 파일 정책을 적용하는 액세스 규칙에 대해 파일 로깅을 활성화해야 합니다.

시스템이 파일 이벤트를 생성하는 경우 호출하는 액세스 제어 규칙의 로깅 컨피그레이션과 관계없이 시스템은 관련 연결의 종료도 로깅합니다.

악성코드 이벤트

시스템은 전체적인 액세스 제어 컨피그레이션의 일부로 네트워크 트래픽에서 악성코드를 탐지할 수 있습니다. AMP for Firepower는 결과 이벤트의 상태와 악성코드가 탐지된 방법, 위치, 시간에 대한 상황 데이터를 포함하는 악성코드 이벤트를 생성할 수 있습니다. 이러한 이벤트를 생성하려면 파일 정책을 적용하는 액세스 규칙에 대해 파일 로깅을 활성화해야 합니다.

파일 상태는 변경될 수 있습니다(예: 정상에서 악성코드로 또는 악성코드에서 정상으로). AMP for Firepower가 AMP 클라우드에 파일에 대해 쿼리하고, 쿼리한지 일주일 이내에 상태가 변경되었음을 클라우드에서 확인하는 경우, 시스템에서는 회귀적 악성코드 이벤트를 생성합니다.

보안 인텔리전스 이벤트

보안 인텔리전스 이벤트는 정책에 따라 차단되거나 또는 모니터링된 각 연결의 보안 인텔리전스 정책에 의해 생성된 연결 이벤트 유형입니다. 모든 보안 인텔리전스 이벤트에는 내용이 채워진 Security Intelligence Category(보안 인텔리전스 카테고리) 필드가 있습니다.

이러한 각 이벤트에는 해당하는 "일반" 연결 이벤트가 있습니다. 보안 인텔리전스 정책은 액세스 제어를 비롯한 다른 많은 보안 정책보다 먼저 평가되기 때문에 보안 인텔리전스에 의해 연결이 차단된 경우, 그 결과로 생성된 이벤트에는 시스템이 후속 평가를 통해 수집했을 수 있는 정보(예: 사용자 ID)가 포함되지 않습니다.

보안 이벤트 커넥터

SEC(Secure Event Connector)는 보안 분석 및 로깅 SaaS 솔루션의 구성 요소입니다. ASA 및 FDM 관리 디바이스에서 이벤트를 수신하여 Cisco Cloud에 전달합니다. CDO는 관리자가 해당 페이지에서 또는

Cisco Secure Cloud Analytics를 사용하여 이벤트를 분석할 수 있도록 Event Logging(이벤트 로깅) 페이지에 이벤트를 표시합니다.

SEC는 네트워크 또는 AWS Virtual Private Cloud(VPC)에 구축된 보안 디바이스 커넥터 또는 네트워크에 구축된 자체 CDO 커넥터 가상 머신에 설치됩니다.

보안 이벤트 커넥터 ID

Cisco TAC(Technical Assistance Center) 또는 기타 CDO 지원과 협력할 때는 SEC의 ID가 필요할 수 있습니다. 이 ID는 CDO의 Secure Connector(보안 커넥터) 페이지에 있습니다. SEC ID를 찾으려면 다음을 수행합니다.

1. 왼쪽의 CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.
2. 식별할 SEC를 클릭합니다.
3. SEC ID는 Details(세부 정보) 창의 Tenant ID(테넌트 ID) 위에 나열되는 ID입니다.

관련 정보:

- FDM-관리 디바이스에 대한 보안 로깅 분석
- SDC 가상 머신에 SEC(Secure Event Connector) 설치, 18 페이지
- VM 이미지를 사용하여 SEC 설치
- VM 이미지를 사용하여 SEC 설치
- Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치, 35 페이지
- 보안 이벤트 커넥터 제거
- Cisco Security Analytics and Logging(SaaS) 프로비저닝

보안 이벤트 커넥터 설치

SEC(보안 이벤트 커넥터)는 SDC가 있거나 없는 테넌트에 설치할 수 있습니다.

보안 디바이스 커넥터(있는 경우)와 동일한 가상 머신에 하나의 SEC를 설치할 수 있습니다. 또는 네트워크에서 유지 관리하는 자체 CDO 커넥터 가상 머신에 SEC를 설치할 수 있습니다.

다양한 설치 사례를 설명하는 다음 항목을 참조하십시오.

- VM 이미지를 사용하여 SEC 설치, 27 페이지
- CDO 이미지를 사용하여 SEC 설치, 21 페이지
- Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치, 35 페이지

SDC 가상 머신에 SEC(Secure Event Connector) 설치

SEC(Secure Event Connector)는 ASA 및 FDM 관리 디바이스에서 이벤트를 수신하여 Cisco Cloud에 전달합니다. CDO는 관리자가 해당 페이지에서 또는 Cisco Secure Cloud Analytics를 사용하여 이벤트를 분석할 수 있도록 Event Logging(이벤트 로깅) 페이지에 이벤트를 표시합니다.

보안 디바이스 커넥터(있는 경우)와 동일한 가상 머신에 하나의 SEC를 설치할 수 있습니다. 또는 네트워크에서 유지 관리하는 자체 CDO 커넥터 가상 머신에 SEC를 설치할 수 있습니다.

이 문서에서는 SDC와 동일한 가상 머신에 SEC를 설치하는 방법을 설명합니다. 더 많은 SEC를 설치하려면 CDO 이미지를 사용하여 SEC 설치, 21 페이지 또는 VM 이미지를 사용하여 SEC 설치, 27 페이지의 내용을 참조하십시오.

시작하기 전에

- Cisco Security and Analytics 로깅, 로깅 및 트러블슈팅 라이선스를 구매합니다. 또는 Cisco Security and Analytics 로그아웃을 먼저 시도하려면 CDO에 로그인하고 기본 탐색 모음에서 분석 > 이벤트 로깅를 선택하고 **Request Trial(**평가판 요청**)**을 클릭합니다. 또한 **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 및 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수 있습니다.
- SDC가 설치되었는지 확인합니다. SDC를 설치해야 하는 경우 다음 절차 중 하나를 수행합니다.
  - CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축
  - 자체 VM을 사용하여 보안 디바이스 커넥터 구축

참고 자체 VM에 온프레미스 SDC를 설치한 경우 이벤트가 SDC에 도달하도록 허용하려면 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성이 필요합니다.

- SDC가 CDO와 통신하는지 확인합니다.
  1. CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.
  2. SDC의 마지막 하트비트가 SEC 설치 전 10분 미만이었으며 SDC의 상태가 활성인지 확인합니다.
- 시스템 요구 사항 - SDC를 실행하는 가상 머신에 추가 CPU 및 메모리를 할당합니다.
  - CPU: 총 6개의 CPU를 만들기 위해 SEC를 수용할 수 있도록 추가로 4개의 CPU를 할당합니다.
  - 메모리: 총 10GB의 메모리를 만들려면 SEC에 8GB의 메모리를 추가로 할당합니다.

    SEC를 수용하도록 VM의 CPU와 메모리를 업데이트한 후 VM의 전원을 켜고 Secure Connector(보안 커넥터) 페이지에 SDC가 "Active(활성)" 상태로 표시되는지 확인합니다.

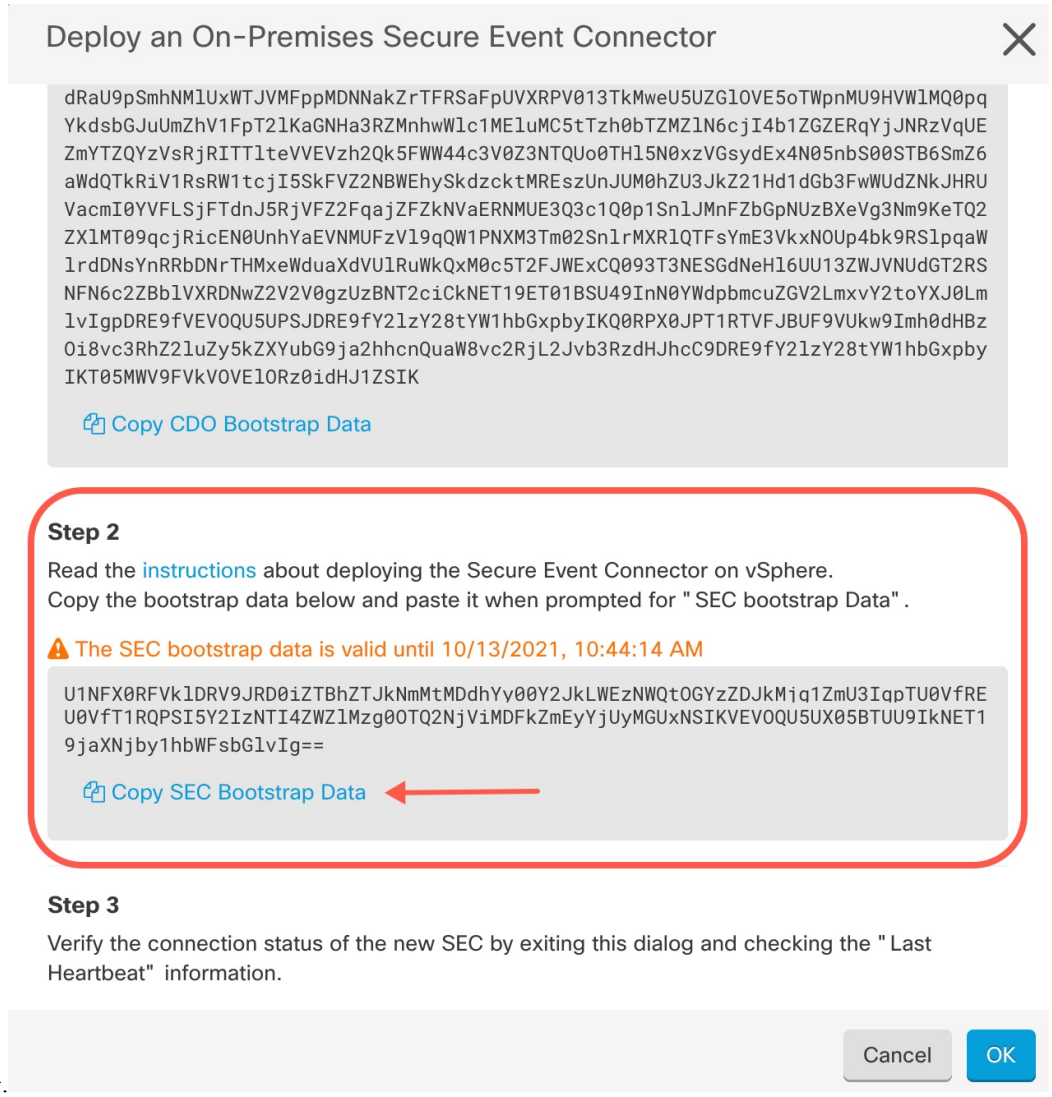
프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **3** 파란색 더하기 버튼을 클릭하고 **Secure Event Connector(**보안 이벤트 커넥터**)**를 클릭합니다.

단계 **4** 마법사의 1단계를 건너뛰고 2단계로 이동합니다. 마법사 2단계에서 링크를 클릭하여 **SEC** 부트스트랩 데이터를 복사합니



다.

단계 **5** 터미널 창을 열고 SDC에 "cdo" 사용자로 로그인합니다.

단계 **6** 로그인한 후에는 "sdc" 사용자로 전환합니다. 암호를 묻는 메시지가 표시되면 "cdo" 사용자의 암호를 입력합니다. 다음은 이러한 명령의 예입니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

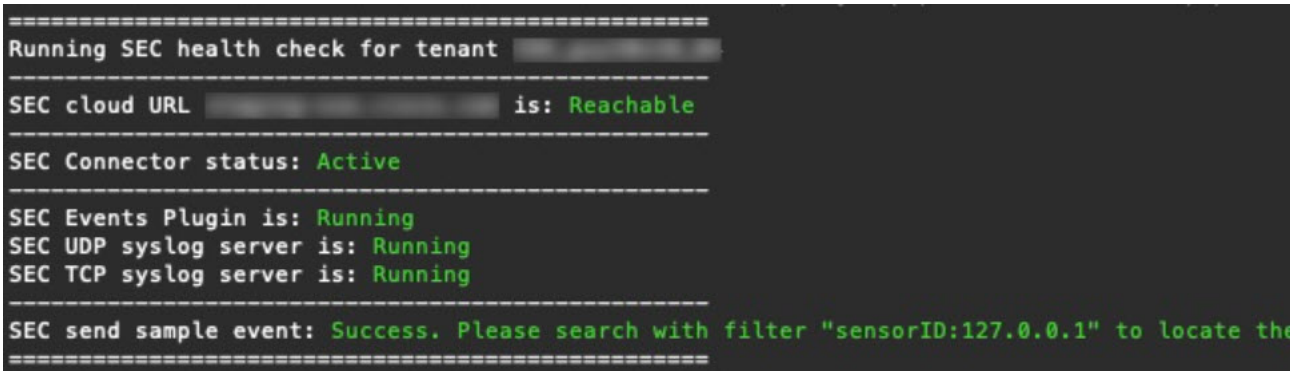
단계 **7** 프롬프트에서 **sec.sh** 설정 스크립트를 실행합니다.

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

단계 **8** 프롬프트 끝에 4단계에서 복사한 부트스트랩 데이터를 붙여넣고 **Enter** 키를 누릅니다.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC가 온보딩되면 sec.sh는 SEC의 상태를 확인하는 스크립트를 실행합니다. 모든 상태 확인이 "녹색"인 경우 상태 확인은 이벤트 로그에 샘플 이벤트를 전송합니다. 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.



등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 보안 이벤트 커넥터 온보딩 장애 문제 해결로 이동하십시오.

단계 **9** SDC 및 SEC가 실행 중인 VM에 추가 구성이 필요한지 확인합니다.

- 자체 가상 머신에 SDC를 설치한 경우 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 32 페이지을 계속 진행합니다.
- CDO 이미지를 사용하여 SDC를 설치한 경우 "다음 작업"을 진행합니다.

다음에 수행할 작업

FDM-관리 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, 11 페이지으로 돌아갑니다.

관련 정보:

- 보안 디바이스 커넥터 문제 해결
- 보안 이벤트 커넥터 트러블슈팅
- SEC 온보딩 장애 문제 해결
- 보안 이벤트 커넥터 등록 실패 문제 해결

CDO 이미지를 사용하여 SEC 설치

SEC(보안 이벤트 커넥터)는 ASA 및 FTD에서 Cisco cloud로 이벤트를 전달하므로 라이선스에 따라 Event Logging 페이지에서 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다.

테넌트에 두 개 이상의 SEC(보안 이벤트 커넥터)를 설치하고ASAs 및 FDM 관리 디바이스의 이벤트를 설치한 SEC로 보낼 수 있습니다. 여러 SEC를 사용하면 서로 다른 위치에 SEC를 설치하고 Cisco Cloud에 이벤트를 전송하는 작업을 배포할 수 있습니다.

SEC 설치는 2단계로 진행됩니다.

1. CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치, 21 페이지 설치하는 모든 SEC에 대해 하나의 CDO 커넥터가 필요합니다. CDO 커넥터는 SDC(보안 디바이스 커넥터)와 다릅니다.
2. CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치, 33 페이지.

참고 고유한 VM을 생성하여 CDO 커넥터를 생성하려면 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성를 참조하십시오.

다음 작업:

CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치, 21 페이지를 계속 진행합니다.

CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치

시작하기 전에

- Cisco Security and Analytics Logging, **Logging and Troubleshooting(**로깅 및 문제 해결**)** 라이선스를 구매하고, **Logging Analytics and Detection(**로깅 분석 및 탐지**)**, **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수도 있습니다.

  원하는 경우 CDO에 로그인하여 Security Analytics and Logging(보안 분석 및 로깅) 평가판을 요청하고 기본 내비게이션 바에서 분석 > 이벤트 로깅을 선택하고 **Request Trial(**평가판 요청**)**을 클릭합니다.

- CDO는 엄격한 인증서 확인이 필요하며 CDO 커넥터와 인터넷 간의 웹/콘텐츠 프록시 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 CDO 커넥터와 CDO 간의 트래픽 검사를 비활성화합니다.
- 이 프로세스에서 설치된 **CDO** 커넥터는 **TCP** 포트 **443**에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다**.**
- Connect to Cisco Defense Orchestrator using Secure Device Connector(보안 디바이스 커넥터를 사용하여 Cisco Defense Orchestrator에 연결)를 검토하여 **CDO** 커넥터에 대한 적절한 네트워크 액세스를 확인합니다.

- CDO는 vSphere 웹 클라이언트 또는 ESXi 웹 클라이언트를 사용한 CDO 커넥터 VM OVF 이미지 설치를 지원합니다.
- CDO는 VM vSphere 데스크톱 클라이언트를 사용한 CDO 커넥터 VM OVF 이미지 설치를 지원하지 않습니다.
- ESXi 5.1 하이퍼바이저.
- CDO 커넥터 및 SEC만 호스팅하는 VM의 시스템 요구 사항:
  - VMware ESXi 호스트에는 vCPU 4개가 필요합니다.
  - VMware ESXi 호스트에는 최소 8GB의 메모리가 필요합니다.
  - VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다.
- 설치를 시작하기 전에 다음 정보를 수집하십시오.
  - CDO 커넥터 VM에 사용할 고정 IP 주소.
  - 설치 프로세스 중 생성하는 **root** 및 **cdo** 사용자의 비밀번호.
  - 조직에서 사용하는 DNS 서버의 IP 주소
  - SDC 주소가 있는 네트워크의 게이트웨이 IP 주소
  - 시간 서버의 FQDN 또는 IP 주소.
- CDO 커넥터 가상 머신은 보안 패치를 정기적으로 설치하도록 구성되며, 이를 위해서는 포트 80 아웃바운드를 열어야 합니다.

프로시저

단계 **1** CDO 커넥터를 생성할 CDO 테넌트에 로그온합니다.

단계 **2** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **3** 파란색 더하기 버튼을 클릭하고 **Secure Event Connector(**보안 이벤트 커넥터**)**를 클릭합니다.

단계 **4** 1단계에서 **Download the CDO Connector VM image(CDO** 커넥터 **VM** 이미지 다운로드**)**를 클릭합니다. 이는 SEC를 설치하는 특수 이미지입니다. 최신 이미지를 사용하려면 항상 CDO 커넥터 VM을 다운로드하십시오.

단계 **5** .zip 파일의 모든 파일을 추출합니다. 다음과 같이 표시됩니다.

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

단계 **6** vSphere 웹 클라이언트를 사용하여 VMware 서버에 관리자로 로그인합니다.

참고 VM vSphere 데스크톱 클라이언트를 사용하지 마십시오.

단계 **7** 지시에 따라 OVF 템플릿에서 온프레미스 CDO 커넥터 가상 머신을 구축합니다. (템플릿을 구축하려면 .ovf, .mf 및 .vdk 파일이 필요합니다.)

단계 **8** 설정이 완료되면 VM의 전원을 켭니다.

단계 **9** 새 CDO 커넥터 VM의 콘솔을 엽니다.

단계 **10** **cdo** 사용자로 로그인합니다. 기본 암호는 `adm123`입니다.

단계 **11** 프롬프트에 `sudo sdc-onboard setup`을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

단계 **12** 프롬프트가 표시되면 cdo 사용자의 기본 비밀번호 `adm123`을 입력합니다.

단계 **13** 지시에 따라 **root** 사용자의 새 암호를 생성합니다.

단계 **14** 지시에 따라 **cdo** 사용자의 새 암호를 생성합니다.

단계 **15** 지시에 따라 Cisco Defense Orchestrator 도메인 정보를 입력합니다.

단계 **16** CDO 커넥터 VM에 사용할 고정 IP 주소를 입력합니다.

단계 **17** CDO 커넥터 VM이 설치된 네트워크의 게이트웨이 IP 주소를 입력합니다.

단계 **18** CDO 커넥터의 NTP 서버 주소 또는 FQDN을 입력합니다.

단계 **19** Docker 브리지 정보를 묻는 프롬프트가 표시되면 정보를 입력하거나 해당되지 않는 경우 비워두고 <Enter> 키를 누릅니다.

단계 **20** 입력을 확인합니다.

단계 **21** "지금 SDC를 설정하시겠습니까?"라는 프롬프트가 나타나면 **n**을 입력합니다.

단계 **22** **cdo** 사용자로 로그인하여 CDO 커넥터에 대한 SSH 연결을 생성합니다.

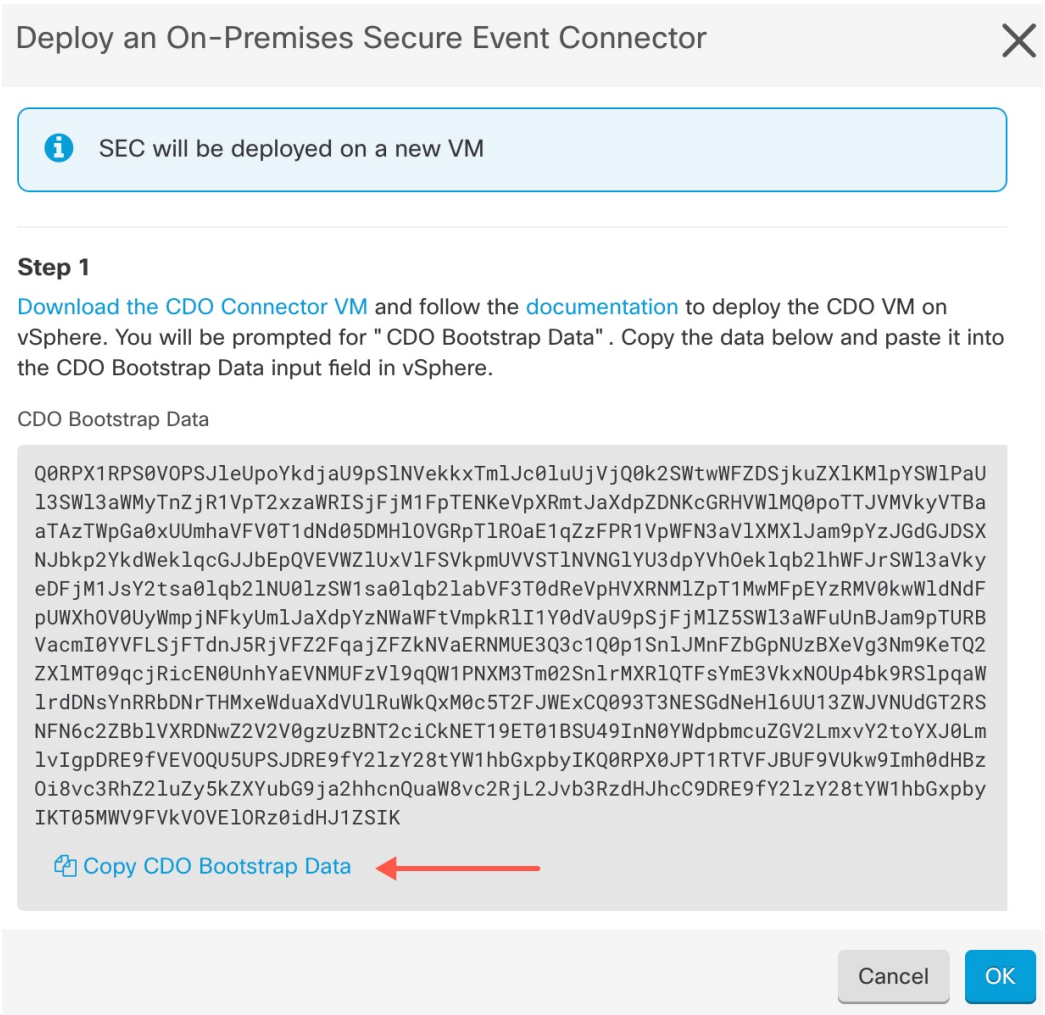
단계 **23** 프롬프트에 **`sudo sdc-onboard bootstrap`**을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

단계 **24** 프롬프트가 표시되면 cdo 사용자의 비밀번호를 입력합니다.

단계 **25** 프롬프트가 표시되면 CDO로 돌아가 CDO 부트스트랩 데이터를 복사한 다음 SSH 세션에 붙여넣습니다. CDO 부트스트랩 데이터를 복사하려면 다음을 수행합니다.

1. CDO에 로그인합니다.
2. CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.
3. 온보딩을 시작한 보안 이벤트 커넥터를 선택합니다. 상태가 "Onboarding(온보딩)"으로 표시되어야 합니다.
4. Actions(작업) 창에서 **Deploy an On-Premises Secure Event Connector(**온프레미스 보안 디바이스 커넥터 구축**)**를 클릭합니다.
5. 대화 상자의 1단계에서 CDO 부트스트랩 데이터를 복사합니



다.

단계 **26** 이 설정을 업데이트하시겠습니까**?**라는메시지가 표시되면 **n**을 입력합니다.

단계 **27** CDO의 Deploy an On-Premises Secure Event Connector(온프레미스 보안 이벤트 커넥터 구축) 대화 상자로 돌아가 **OK(**확인**)**를 클릭합니다. Secure Connector(보안 커넥터) 페이지에서 Secure Event Connector(보안 이벤트 커넥터)가 노란색 Onboarding(온보딩) 상태로 표시됩니다.

다음에 수행할 작업

CDO 커넥터 VM에 보안 이벤트 커넥터 설치, 25 페이지를 진행합니다.

CDO 커넥터 VM에 보안 이벤트 커넥터 설치

시작하기 전에

CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치, 21 페이지에 설명된 대로 CDO 커넥터 VM을 설치해야 합니다.

프로시저

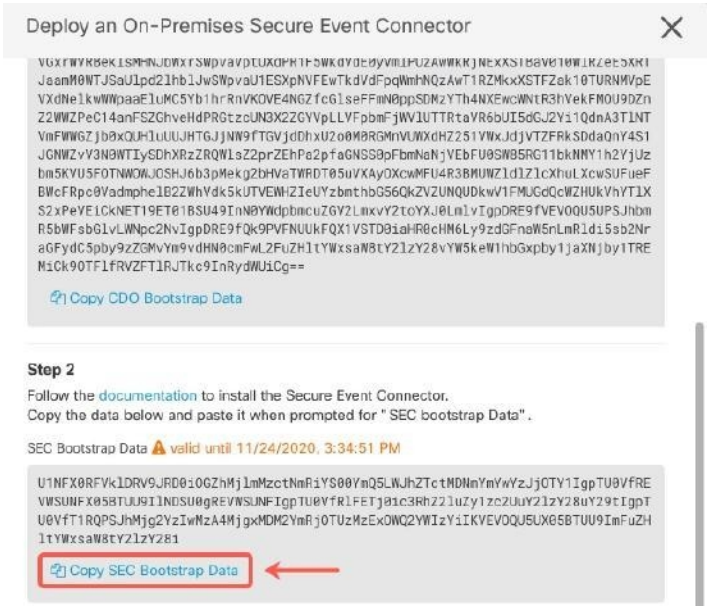
단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **3** 위에서 온보딩한 CDO 커넥터를 선택합니다. Secure Connector(보안 커넥터) 테이블에서는 이를 보안 이벤트 커넥터(보안 이벤트 커넥터)라고 하며 여전히 "Onboading(온보딩)" 상태여야 합니다.

단계 **4** 오른쪽의 작업 창에서 **Deploy an On-Premises Secure Event Connector(**온프레미스 보안 디바이스 커넥터 구축**)**를 클릭합니다.

단계 **5** 마법사 **2**단계에서 링크를 클릭하여 **SEC** 부트스트랩 데이터를 복사합니다.



단계 **6** CDO 커넥터에 대한 SSH 연결을 생성하고 **cdo** 사용자로 로그인합니다.

단계 **7** 로그인한 후에는 **sdc** 사용자로 전환합니다. 암호를 묻는 메시지가 표시되면 "cdo" 사용자의 암호를 입력합니다. 다음은 이러한 명령의 예입니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
 [sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

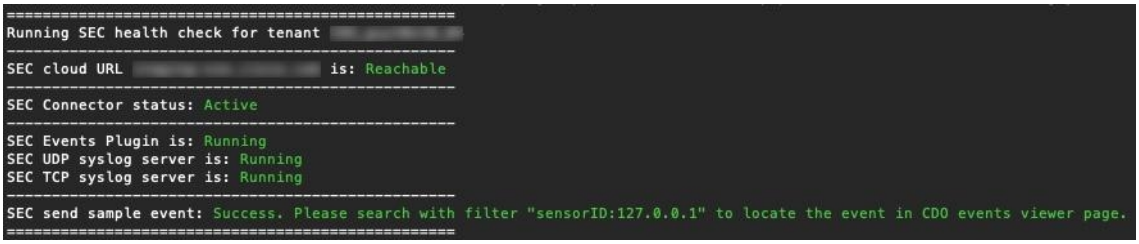
단계 **8** 프롬프트에서 sec.sh 설정 스크립트를 실행합니다.

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

단계 **9** 프롬프트 끝에 4단계에서 복사한 부트스트랩 데이터를 붙여넣고 **Enter** 키를 누릅니다.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
 RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC가 온보딩되면 sec.sh는 SEC의 상태를 확인하는 스크립트를 실행합니다. 모든 상태 확인이 "녹색"인 경우 상태 확인은 이벤트 로그에 샘플 이벤트를 전송합니다. 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.



등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 SEC 온보딩 실패 문제 해결로 이동하십시오.

성공 메시지가 표시되면 CDO로 돌아가고 **Deploy on-Premise Secure Event Connector(**온프레미스 보안 이벤트 커넥터 구축**)** 대화 상자에서 Done(완료)를 클릭합니다.

단계 **10** "**What to do next(**다음 작업**)**로 계속합니다."

다음에 수행할 작업

FDM-관리 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, 11 페이지으로 돌아갑니다.

관련 정보**:**

- 보안 디바이스 커넥터 문제 해결
- 보안 이벤트 커넥터 문제 해결
- SEC 온보딩 실패 문제 해결

VM 이미지를 사용하여 SEC 설치

SEC(보안 이벤트 커넥터)는 ASA 및 FTD에서 Cisco cloud로 이벤트를 전달하므로 라이선스에 따라 Event Logging 페이지에서 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다.

테넌트에 두 개 이상의 SEC(보안 이벤트 커넥터)를 설치하고 ASA 및 FDM 매니지드 디바이스의 이벤트를 설치한 SEC로 보낼 수 있습니다. 여러 SEC를 사용하면 서로 다른 위치에 SEC를 설치하고 Cisco Cloud에 이벤트를 전송하는 작업을 배포할 수 있습니다.

자체 VM 이미지를 사용하여 여러 SEC를 설치하는 작업은 3단계로 진행됩니다. 다음 각 단계를 수행해야 합니다.

1. VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치, 27 페이지
2. 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 32 페이지를 사용하여 VM에 대한 몇 가지 추가 구성 단계를 수행합니다.
3. CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치

참고 CDO 커넥터용 CDO VM 이미지를 사용하는 것이 가장 쉽고 정확하며 선호되는 CDO 커넥터 설치 방법입니다. 이 방법을 사용하려면 CDO 이미지를 사용하여 SEC 설치, 21 페이지의 내용을 참조하십시오.

다음 작업:

VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치, 27 페이지를 계속합니다.

VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치

CDO 커넥터 VM은 SEC를 설치하는 가상 머신입니다. CDO 커넥터의 목적은 Cisco SaaS(Security Analytics and Logging) 고객을 위한 SEC를 지원하는 것입니다.

시작하기 전에

- Cisco Security and Analytics Logging, **Logging and Troubleshooting(**로깅 및 문제 해결**)** 라이선스를 구매하고, **Logging Analytics and Detection(**로깅 분석 및 탐지**)**, **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수도 있습니다.

  원하는 경우 CDO에 로그인하여 Security Analytics and Logging(보안 분석 및 로깅) 평가판을 요청하고 기본 탐색 모음에서 분석 > 이벤트 로깅을 선택하고 **Request Trial(**평가판 요청**)**를 클릭합니다.

- CDO는 엄격한 인증서 확인이 필요하며 CDO 커넥터와 인터넷 간의 웹/콘텐츠 프록시를 지원하지 않습니다.
- **CDO** 커넥터는 **TCP** 포트 **443**에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다.

- 보안 디바이스 커넥터를 사용하여 Cisco Defense Orchestrator에 연결을 검토하여 **CDO** 커넥터에 대한 적절한 네트워크 액세스를 확인합니다**.**
- vCenter 웹 클라이언트 또는 ESXi 웹 클라이언트와 함께 설치된 VMware ESXi 호스트

참고 vSphere 데스크톱 클라이언트를 사용한 설치는 지원되지 않습니다.

- ESXi 5.1 하이퍼바이저.
- Cent OS 7 게스트 운영체제.
- CDO 커넥터 및 SEC만 호스팅하는 VM의 시스템 요구 사항:
  - CPU: SEC를 수용할 수 있도록 4개의 CPU를 할당합니다.
  - 메모리: SEC에 대해 8GB의 메모리를 할당합니다.
  - 디스크 공간: 64GB
- 이 절차를 수행하는 사용자는 Linux 환경에서 작업하고 파일 편집을 위해 **vi** 시각적 편집기를 사용하는 데 익숙해야 합니다.
- CentOS 가상 머신에 CDO Connector를 설치하는 경우 정기적으로 Yum 보안 패치를 설치하는 것이 좋습니다. Yum 구성에 따라 Yum 업데이트를 가져오려면 포트 80 및 443에서 아웃바운드 액세스를 열어야 할 수 있습니다. 또한 업데이트를 예약하려면 yum-cron 또는 crontab을 구성해야 합니다. 보안 운영 팀과 함께 Yum 업데이트를 받기 위해 변경해야 하는 보안 정책이 있는지 확인합니다.
- 설치를 시작하기 전에 다음 정보를 수집하십시오.
  - CDO 커넥터에 사용할 고정 IP 주소.
  - 설치 프로세스 중 생성하는 **root** 및 **cdo** 사용자의 비밀번호.
  - 조직에서 사용하는 DNS 서버의 IP 주소
  - CDO 커넥터 주소가 있는 네트워크의 게이트웨이 IP 주소
  - 시간 서버의 FQDN 또는 IP 주소.
- CDO 커넥터 가상 머신은 보안 패치를 정기적으로 설치하도록 구성되며, 이를 위해서는 포트 80 아웃바운드를 열어야 합니다.
- 시작하기 전에: 이 절차의 명령을 복사하여 터미널 창에 붙여넣지 말고 대신 입력하십시오. 일부 명령에는 "n-대시"가 포함되며, 잘라내기 및 붙여넣기 프로세스에서 이러한 명령은 "m-대시"로 적용되어 명령이 실패할 수 있습니다.

프로시저

단계 **1** 보안 디바이스 커넥터 페이지에서 파란색 플러스 버튼  을 클릭하고 보안 이벤트 커넥터(보안 이벤트 커넥터)를 클릭합니다.

단계 **2** 제공된 링크를 사용하여 "Deploy an On-Premises 보안 이벤트 커넥터(온프레미스 보안 이벤트 커넥터 배포)" 창의 2단계에서 SEC 부트스트랩 데이터를 복사합니다.

단계 **3** 이 절차의 사전 요구 사항에 나와 있는 메모리, CPU 및 디스크 공간 이상으로 CentOS 7 가상 머신(http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-Minimal-1804.iso)을 설치합니다.

단계 **4** 설치가 완료되면 CDO 커넥터의 IP 주소, 서브넷 마스크 및 게이트웨이를 지정하는 등의 기본 네트워킹을 구성합니다.

단계 **5** DNS(Domain Name Server) 서버를 구성합니다.

단계 **6** NTP(Network Time Protocol) 서버를 구성합니다.

단계 **7** CDO 커넥터의 CLI와의 손쉬운 상호 작용을 위해 CentOS에 SSH 서버를 설치합니다.

단계 **8** Yum 업데이트를 실행한 후 **open-vm-tools**, **nettools** 및 **bind-utils** 패키지를 설치합니다.

```
[root@sdc-vm ~]# yum update -y
[root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

단계 **9** **AWS CLI package(AWS CLI** 패키지**)** (https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html)를 설치합니다.

참고 `--user` 플래그를 사용하지 마십시오.

단계 **10** **Docker CE packages(Docker CE** 패키지**)** (https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce)를 설치합니다.

참고 "저장소를 사용하여 설치" 방법을 사용합니다.

단계 **11** Docker 서비스를 시작하고 부팅 시 시작되도록 활성화합니다.

```
[root@sdc-vm ~]# systemctl start docker
 [root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
/usr/lib/systemd/system/docker.service.
```

단계 **12** 두 사용자(**cdo** 및 **sdc**)를 생성합니다. cdo 사용자는 관리 기능을 실행하기 위해 로그인하는 사용자이며(루트 사용자를 직접 사용할 필요가 없음), sdc 사용자는 CDO 커넥터 도커 컨테이너를 실행하는 사용자입니다.

```
[root@sdc-vm ~]# useradd cdo
 [root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```

단계 **13** cdo 사용자의 비밀번호를 생성합니다.

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

단계 **14** cdo 사용자를 "Wheel" 그룹에 추가하여 관리(sudo) 권한을 부여합니다.

```
[root@sdc-vm ~]# usermod -aG wheel cdo
 [root@sdc-vm ~]#
```

단계 **15** Docker가 설치되면 사용자 그룹이 생성됩니다. CentOS/Docker 버전에 따라 "docker" 또는 "dockerroot"라고 부를 수 있습니다. /etc/group 파일을 확인하여 어떤 그룹이 생성되었는지 확인한 다음 sdc 사용자를 이 그룹에 추가합니다.

```
 [root@sdc-vm ~]# grep docker /etc/group
docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

단계 **16** `/etc/docker/daemon.json` 파일이 없는 경우 파일을 생성하고 아래 내용을 입력합니다. 생성되면 docker 데몬을 다시 시작합니다.

참고 "group" 키에 입력한 그룹 이름이 단계 15과 일치하는지 확인합니다.

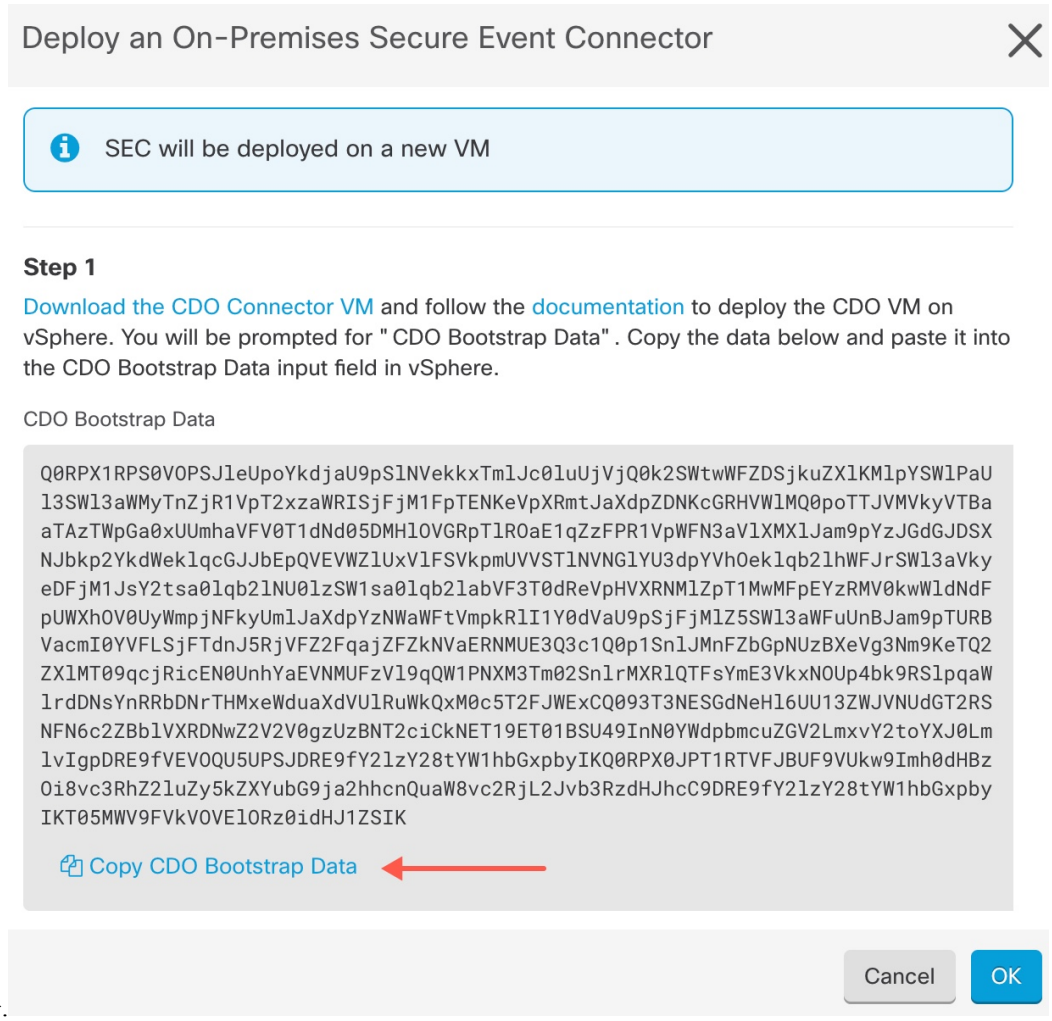
```
 [root@sdc-vm ~]# cat /etc/docker/daemon.json
{
 "live-restore": true,
 "group": "docker"
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

단계 **17** 현재 vSphere 콘솔 세션를 사용하는 경우 SSH로 전환하고 **cdo** 사용자로 로그인합니다. 로그인한 후에는 **sdc** 사용자로 변경합니다. 암호를 묻는 메시지가 표시되면 **cdo** 사용자의 암호를 입력합니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

단계 **18** 디렉터리를 **/usr/local/cdo**로 변경합니다.

단계 **19** **bootstrapdata**라는 새 파일을 생성하고 배포 마법사 1단계의 부트스트랩 데이터를 이 파일에 붙여넣습니다. 파일을 **Save(**저장**)**합니다. **vi** 또는 **nano**를 사용하여 파일을 생성할 수 있습니다.



다.

단계 **20** 부트스트랩 데이터는 base64로 인코딩됩니다. 이를 디코딩하고 **extractedbootstrapdata**라는 파일로 내보냅니다.

```
 [sdc@sdc-vm ~]$ base64 -d /usr/local/cdo/bootstrapdata >
/usr/local/cdo/extractedbootstrapdata
[sdc@sdc-vm ~]$
```

cat 명령을 실행하여 디코딩된 데이터를 확인합니다. 명령 및 디코딩된 데이터는 다음과 같이 표시됩니다.

```
[sdc@sdc-vm ~]$ cat /usr/local/cdo/extractedbootstrapdata
CDO_TOKEN="<token string>"
CDO_DOMAIN="www.defenseorchestrator.com"
CDO_TENANT="<tenant-name>"
CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"

ONLY_EVENTING="true"
```

단계 **21** 다음 명령을 실행하여 디코딩된 부트스트랩 데이터의 섹션을 환경 변수로 내보냅니다.

```
 [sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
[sdc@sdc-vm ~]$
```

단계 **22** CDO에서 부트스트랩 번들을 다운로드합니다.

```
 [sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL"
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$ ls -l /usr/local/cdo/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/cdo/tenant-name-SDC
```

단계 **23** CDO 커넥터 tarball을 추출하고 bootstrap_sec_only.sh 파일을 실행하여 CDO 커넥터 패키지를 설치합니다.

```
 [sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
<snipped – extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/cdo/toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/cdo/toolkit/es_toolkit.sh es_maintenance 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

다음에 수행할 작업

생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 32 페이지를 계속합니다.

생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성

자체 CentOS 7 가상 머신에 CDO 커넥터를 설치한 경우, 이벤트가 SEC에 도달하도록 허용하려면 다음 추가 구성 절차 중 하나를 수행해야 합니다.

- CentOS 7 VM에서 firewalld 서비스를 비활성화합니다.. 이는 Cisco 제공 SDC VM의 구성과 일치합니다.
- firewalld 서비스가 실행되도록 허용하고 방화벽 규칙을 추가하여 이벤트 트래픽이 SEC에 도달하도록 허용합니다., 33 페이지. 이는 인바운드 이벤트 트래픽을 허용하는 보다 세부적인 접근 방식입니다.

CentOS 7 VM에서 **firewalld** 서비스를 비활성화합니다.

1. SDC VM의 CLI에 "cdo" 사용자로 로그인합니다.

2. firewalld 서비스를 중지한 다음, 이후에 VM을 재부팅할 때 비활성화된 상태로 유지되는지 확인합니다. 메시지가 표시되면 **cdo** 사용자의 비밀번호를 입력합니다.

```
[cdo@SDC-VM ~]$ sudo systemctl stop firewalld
cdo@SDC-VM ~]$ sudo systemctl disable firewalld
```

3. Docker 서비스를 다시 시작하여 Docker 관련 항목을 로컬 방화벽에 다시 삽입합니다.

```
[cdo@SDC-VM ~]$ sudo systemctl restart docker
```

4. CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치, 33 페이지를 진행합니다.

firewalld 서비스가 실행되도록 허용하고 방화벽 규칙을 추가하여 이벤트 트래픽이 **SEC**에 도달하도록 허용합니다.

1. SDC VM의 CLI에 "cdo" 사용자로 로그인합니다.
2. 구성한 TCP, UDP 또는 NSEL 포트에서 SEC로 수신되는 트래픽을 허용하도록 로컬 방화벽 규칙을 추가합니다. SEC에서 사용하는 포트에 대해서는 SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오. 메시지가 표시되면 **cdo** 사용자의 비밀번호를 입력합니다. 다음은 이러한 명령의 예입니다. 다른 포트 값을 지정해야 할 수 있습니다.

```
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10125/tcp
cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10025/udp
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10425/udp
```

3. firewalld 서비스를 다시 시작하여 새 로컬 방화벽 규칙을 활성 및 영구 규칙으로 설정합니다.

```
[cdo@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치, 33 페이지를 진행합니다.

CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치

시작하기 전에

다음 두 가지 작업을 수행합니다.

- VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치, 27 페이지
- 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 32 페이지

프로시저

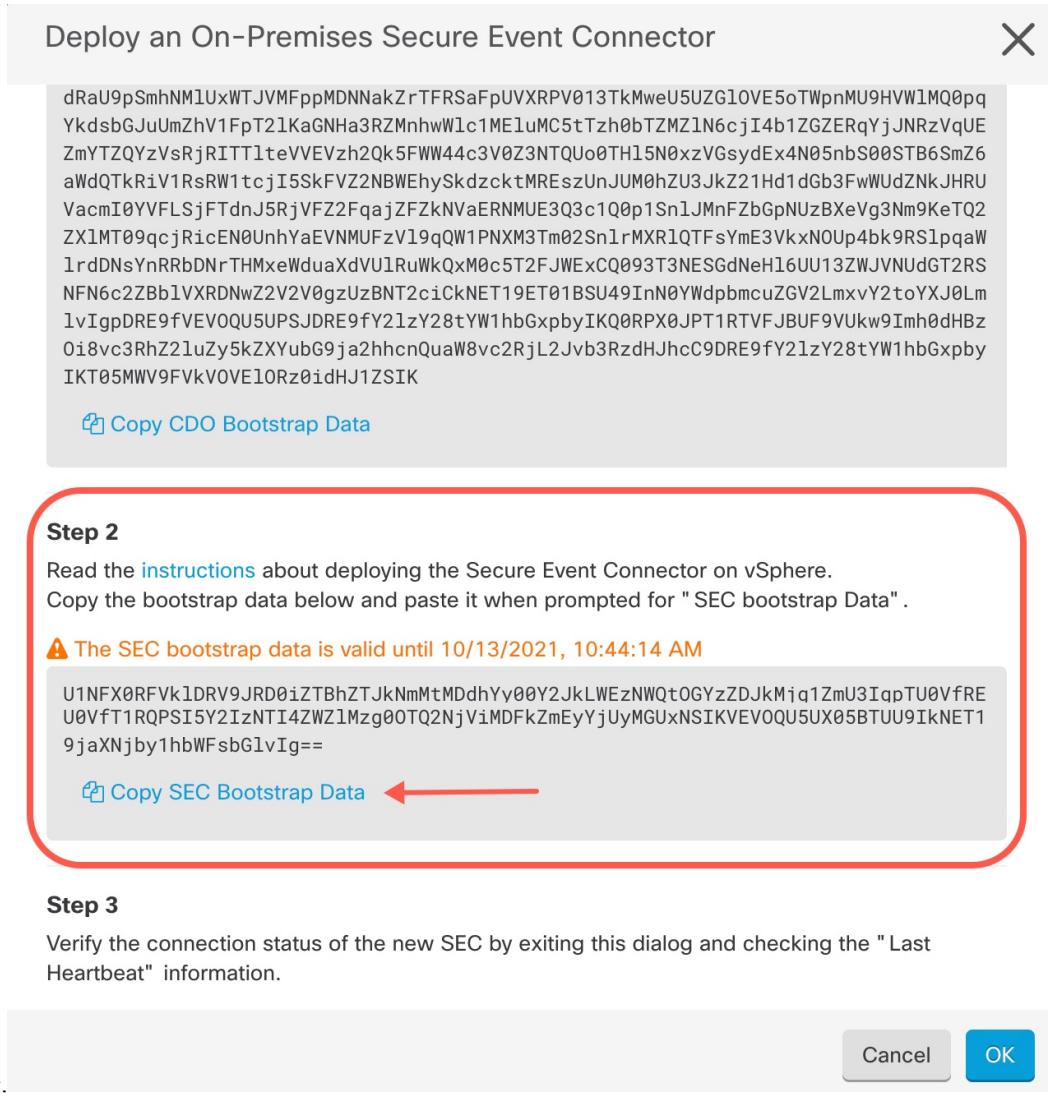
단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **3** 위의 사전 요구 사항에 있는 절차를 사용하여 설치한 CDO 커넥터를 선택합니다. Secure Connector(보안 커넥터) 테이블에서는 이를 보안 이벤트 커넥터(보안 이벤트 커넥터)라고 합니다.

단계 **4** 오른쪽의 작업 창에서 **Deploy an On-Premises Secure Event Connector(**온프레미스 보안 디바이스 커넥터 구축**)**를 클릭합니다.

단계 **5** 마법사 **2**단계에서 링크를 클릭하여 **SEC** 부트스트랩 데이터를 복사합니



다.

단계 **6** SSH를 사용하여 Secure Connector에 연결하고 **cdo** 사용자로 로그인합니다.

단계 **7** 로그인한 후에는 **sdc** 사용자로 전환합니다. 암호를 묻는 메시지가 표시되면 "cdo" 사용자의 암호를 입력합니다. 다음은 이러한 명령의 예입니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

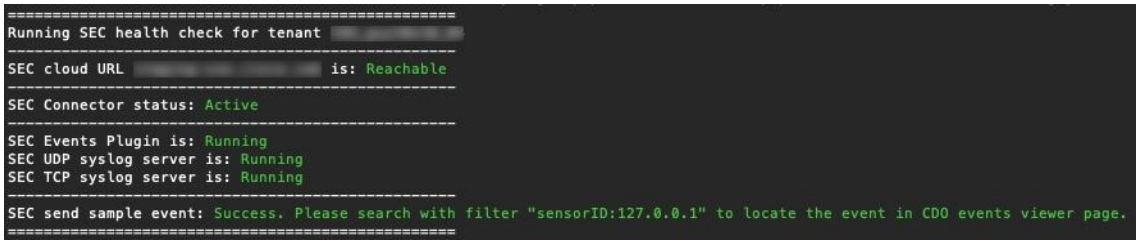
단계 **8** 프롬프트에서 sec.sh 설정 스크립트를 실행합니다.

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

단계 **9** 프롬프트 끝에 4단계에서 복사한 부트스트랩 데이터를 붙여넣고 **Enter** 키를 누릅니다.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
 KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC가 온보딩되면 sec.sh는 SEC의 상태를 확인하는 스크립트를 실행합니다. 모든 상태 확인이 "녹색"인 경우 상태 확인은 이벤트 로그에 샘플 이벤트를 전송합니다. 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.



등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 보안 이벤트 커넥터 온보딩 장애 문제 해결로 이동하십시오.

성공 메시지가 표시되면 **Deploy an ON-Premise Secure Event Connector(**온프레미스 보안 이벤트 커넥터 구축**)** 대화 상자에서 **Done(**완료**)**를 클릭합니다. VM 이미지에 SEC 설치를 완료했습니다.

단계 **10** "다음 작업"을 계속합니다.

다음에 수행할 작업

SAL SaaS의 구현을 계속하려면 이 절차로 돌아가십시오. FDM-관리 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, 11 페이지.

관련 정보**:**

- 보안 디바이스 커넥터 문제 해결
- 보안 이벤트 커넥터 트러블슈팅
- SEC 온보딩 장애 문제 해결
- SEC 등록 실패 문제 해결

Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치

시작하기 전에

- 이 작업을 수행하려면 CDO 테넌트에서 SAL을 활성화해야 합니다. 이 섹션에서는 SAL 라이선스가 있다고 가정합니다. 라이선스가 없는 경우 Cisco 보안 및 분석 로깅, 로깅 및 문제 해결 라이선스를 구매합니다.
- 새 SEC가 설치되어 있는지 확인합니다. 새 SEC를 생성하려면 SDC 가상 머신에 SEC(Secure Event Connector) 설치, 18 페이지의 내용을 참조하십시오.
- SEC를 설치할 때 CDO 부트스트랩 데이터 및 SEC 부트스트랩 데이터를 적어 두십시오.

프로시저

단계 1 Terraform 레지스트리의 Secure Event Connector Terraform 모듈로 이동하고 지침에 따라 SEC Terraform 모듈을 Terraform 코드에 추가합니다.

단계 2 Terraform 코드를 적용합니다.

단계 3 `instance_id` 및 `sec_fqdn` 출력은 나중에 절차에서 필요하므로 인쇄해야 합니다.

참고 SEC 문제를 해결하려면 AWS Systems Manager Session Manager(SSM)를 사용하여 SEC 인스턴스에 연결해야 합니다. SSM을 사용하여 인스턴스에 연결하는 방법에 대한 자세한 내용은 AWS Systems Manager Session Manager 설명서를 참조하십시오.

SSH를 사용하여 SDC 인스턴스에 연결하는 포트는 보안상의 이유로 노출되지 않습니다.

단계 4 ASA에서 SEC로 로그를 전송하려면 생성한 SEC의 인증서 체인을 가져와 단계 3의 출력과 함께 다음 명령을 실행하여 리프 인증서를 제거합니다.

```
rm -f /tmp/cert_chain.pem && openssl s_client -showcerts -verify 5 -connect <FQDN>:10125 <
 /dev/null | awk '/BEGIN CERTIFICATE/,/END CERTIFICATE/{ if(/BEGIN CERTIFICATE/){a++};
out="/tmp/cert_chain.pem"; if(a > 1) print >>out}'
```

단계 5 `/tmp/cert_chain.pem`의 내용을 클립보드에 복사합니다.

단계 6 다음 명령을 사용하여 SEC의 IP 주소를 기록해 둡니다.

```
nslookup <FQDN>
```

단계 7 CDO에 로그인하고 새 트러스트 포인트 개체 추가를 시작합니다. 자세한 내용은 신뢰할 수 있는 CA 인증서 개체 추가를 참조하십시오. **Add(추가)**를 클릭하기 전에 **Other Options(기타 옵션)**에서 **Enable CA flag in basic constraints extension(기본 제약 조건 확장에서 CA 플래그 활성화)** 확인란의 선택을 취소해야 합니다.

단계 8 **Add(추가)**를 클릭하고 **Install Certificate(인증서 설치)** 페이지의 CDO에서 생성한 CLI 명령을 복사한 다음 **Cancel(취소)**을 클릭합니다.

단계 9 `enrollment terminal(등록 터미널)` 아래 텍스트 클립보드에 `no ca-check`를 추가합니다.

단계 10 SSH로 ASA 디바이스에 연결하거나 CDO에서 ASA CLI 옵션을 사용하고 다음 명령을 실행합니다.

```
DataCenterFW-1> en
Password: ****************
DataCenterFW-1# conf t
DataCenterFW-1(config)# <paste your modified ASA CLIs here and press Enter>
DataCenterFW-1(config)# wr mem
Building configuration...
Cryptochecksum: 6634f35f 4c5137f1 ab0c5cdc 9784bdb6
```

다음에 수행할 작업

SEC가 AWS SSM을 사용하여 패킷을 수신하고 있는지 확인할 수 있습니다.

다음과 유사한 로그가 표시됩니다.

```
time="2023-05-10T17:13:46.135018214Z" level=info msg="[ip-10-100-5-19.ec2.internal][util.go:67
 plugin.createTickers:func1] Events - Processed - 6/s, Dropped - 0/s, Queue size - 0"
```

Cisco Security Analytics and Logging(SaaS) 프로비저닝

Cisco SaaS(Security Analytics and Logging) 유료 라이선스가 만료되도록 허용하는 경우 90일의 유예 기간이 제공됩니다. 이 유예 기간 동안 유료 라이선스를 갱신하는 경우 서비스가 중단되지 않습니다.

그렇지 않고 90일의 유예 기간이 경과하도록 허용하면 시스템은 모든 고객 데이터를 비웁니다. 더 이상 이벤트 로깅 페이지에서 ASA 또는 FTD 이벤트를 보거나 ASA 또는 FTD 이벤트 및 네트워크 플로우 데이터에 동적 엔터티 모델링 동작 분석을 적용할 수 없습니다.

보안 이벤트 커넥터 제거

경고: 이 절차는 보안 디바이스 커넥터에서 보안 이벤트 커넥터를 삭제합니다. 이렇게 하면 SaaS(Secure Logging Analytics)를 사용할 수 없습니다. 이는 되돌릴 수 없습니다. 질문이나 우려 사항이 있는 경우 이 작업을 수행하기 전에 CDO 지원에 문의하십시오.

보안 디바이스 커넥터에서 보안 이벤트 커넥터를 제거하는 작업은 다음의 2단계 프로세스입니다.

1. CDO에서 SEC 제거
2. SDC에서 SEC 파일 제거.

후속 작업:CDO에서 SEC 제거 계속

CDO에서 SEC 제거

시작하기 전에

보안 이벤트 커넥터 제거, 37 페이지의 내용을 참조하십시오.

프로시저

단계 1 CDO에 로그인합니다.

단계 2 CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 3 디바이스 유형인 보안 이벤트 커넥터가 있는 행을 선택합니다.

경고: 주의하십시오. 보안 디바이스 커넥터를 선택하지 마십시오.

단계 4 Actions(작업) 창에서 **Remove(제거)**를 클릭합니다.

단계 5 **OK(확인)**를 클릭하여 보안 이벤트 커넥터 삭제를 확인합니다.

다음에 수행할 작업

SDC에서 SEC 파일 제거, 38 페이지를 진행합니다.

SDC에서 SEC 파일 제거

이는 SDC에서 보안 이벤트 커넥터를 제거하는 2단계 절차의 두 번째 부분입니다. 시작하기 전에 보안 이벤트 커넥터 제거, 37 페이지을 참조하십시오.

프로시저

단계 **1** 가상 머신 하이퍼바이저를 열고 SDC에 대한 콘솔 세션을 시작합니다.

단계 **2** SDC 사용자로 전환합니다.

```
[cdo@tenant toolkit]$sudo su sdc
```

단계 **3** 프롬프트에서 다음 명령 중 하나를 입력합니다.

- 자체 테넌트만 관리하는 경우:

  ```
  [sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove
  ```

- 둘 이상의 테넌트를 관리하는 경우 테넌트 이름의 시작 부분에 CDO_를 추가합니다. 예를 들면 다음과 같습니다.

  ```
  [sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove CDO_[tenant_name]
  ```

단계 **4** SEC 파일을 제거할 것인지 확인합니다.

Cisco Secure Cloud Analytics 포털 프로비저닝

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Logging Analytics and Detection(로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매한 경우, SEC(Secure Event Connector)를 구축하고 구성한 후 Secure Cloud Analytics 포털을 CDO 포털에 연결해야 Secure Cloud Analytics 알림을 볼 수 있습니다. 기존 Secure Cloud Analytics 포털이 있는 경우 라이선스를 구매할 때 Secure Cloud Analytics 포털 이름을 제공하고 CDO 포털에 즉시 연결할 수 있습니다.

그렇지 않은 경우 CDO UI에서 새 Secure Cloud Analytics 포털을 요청할 수 있습니다. Secure Cloud Analytics 알림에 처음 액세스하면 시스템은 Secure Cloud Analytics 포털을 요청할 수 있는 페이지로 이동합니다. 이 포털을 요청하는 사용자에게는 포털에서 관리자 권한이 부여됩니다.

Procedure

단계 **1** CDO 메뉴에서 분석 > **Secure Cloud Analytics**를 선택하여 새 창에서 Secure Cloud Analytics UI를 엽니다.

단계 **2** **Start Free Trial(**무료 평가판 시작**)**을 클릭하여 Secure Cloud Analytics 포털을 프로비저닝하고 CDO 포털과 연결합니다.

Note 포털을 요청한 후 프로비저닝에 몇 시간이 걸릴 수 있습니다.

다음 단계로 이동하기 전에 포털이 프로비저닝되었는지 확인합니다.

1. CDO 메뉴에서 분석 > **Secure Cloud Analytics**를 선택하여 새 창에서 Secure Cloud Analytis UI를 엽니다.
2. 다음 옵션을 이용할 수 있습니다.
   - Secure Cloud Analytics 포털을 요청했는데 시스템에서 포털을 프로비저닝하는 중이라고 표시되면 기다렸다가 나중에 알림에 액세스해 보십시오.
   - Secure Cloud Analytics 포털이 프로비저닝된 경우 **Username(**사용자 이름**)** 및 **Password(**비밀번호**)**를 입력하고 **Sign in(**로그인**)**을 클릭합니다.

Note 관리자 사용자는 다른 사용자를 초대하여 Secure Cloud Analytis 포털 내에서 계정을 생성할 수 있습니다. 자세한 내용은 CDO에서 Cisco Secure Cloud Analytics 알림 보기, on page 41를 참조하십시오.

What to do next

- **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 라이선스를 구매한 경우 구성이 완료된 것입니다. Secure Cloud Analytics 포털 UI에서 CDO 통합 또는 센서 상태를 보려면 Secure Cloud Analytics에서 센서 상태 및 CDO 통합 상태 검토, on page 39에서 자세한 내용을 확인하십시오. Secure Cloud Analytics 포털에서 알림으로 작업하려는 경우 자세한 내용은 CDO에서 Cisco Secure Cloud Analytics 알림 보기, on page 41 및 방화벽 이벤트 기반 알림 작업을 참조하십시오.
- **Total Network Analytics and Monitoring** 라이선스를 구매한 경우 내부 네트워크에 하나 이상의 Secure Cloud Analytics 센서를 구축하여 네트워크 플로우 데이터를 클라우드에 전달합니다. 클라우드 기반 네트워크 플로우 데이터를 모니터링하려면 플로우 데이터를 Secure Cloud Analytics로 전달하도록 클라우드 기반 구축을 구성합니다. 자세한 내용은 전체 네트워크 분석 및 보고를 위한 Cisco Secure Cloud Analytics 센서 구축, on page 40를 참조하십시오.

Secure Cloud Analytics에서 센서 상태 및 CDO 통합 상태 검토

센서 상태

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Secure Cloud Analytis 웹 UI의 Sensor List(센서 목록) 페이지에서 CDO 통합 상태 및 구성된 센서를 볼 수 있습니다. CDO 통합은 읽기 전용 연결 이벤트 센서입니다. Stelathwatch Cloud는 기본 메뉴에서 센서의 전반적인 상태를 제공합니다.

- 녹색 클라우드 아이콘() - 모든 센서와 연결 설정됨, 구성된 경우 CDO
- 노란색 클라우드 아이콘() - 일부 센서 또는 CDO(구성된 경우)와의 연결이 설정되었으며 하나 이상의 센서가 제대로 구성되지 않음
- 빨간색 클라우드 아이콘() - 구성된 모든 센서 및 CDO(구성된 경우)와의 연결 끊김

센서 또는 CDO 통합에서 녹색 아이콘은 설정된 연결을 나타내고, 빨간색 아이콘은 연결 끊김을 나타냅니다.

프로시저

단계 **1** 1. Secure Cloud Analytis 포털 UI에서 **Settings(**설정**)(** **) > Sensors(**센서**)**를 선택합니다.

단계 **2** **Sensor List(**센서 목록**)**를 선택합니다.

전체 네트워크 분석 및 보고를 위한 **Cisco Secure Cloud Analytics** 센서 구축

Secure Cloud Analytics 센서 개요 및 배포

필수 라이선스: 전체 네트워크 분석 및 모니터링

Total Network Analytics and Monitoring(전체 네트워크 분석 및 모니터링**)** 라이선스를 취득한 경우 Secure Cloud Analytics 포털을 프로비저닝한 후 다음을 수행할 수 있습니다.

- 분석을 위해 네트워크 플로우 데이터를 클라우드에 전달하기 위해 온프레미스 네트워크 내에 Secure Cloud Analytics 센서를 배포하고 구성합니다.
- 분석을 위해 네트워크 플로우 로그 데이터를 Secure Cloud Analytics에 전달하도록 클라우드 기반 배포을 구성합니다.

네트워크 경계의 방화벽은 내부 네트워크와 외부 네트워크 간의 트래픽에 대한 정보를 수집하는 반면, Secure Cloud Analytics 센서는 내부 네트워크 내의 트래픽에 대한 정보를 수집합니다.

Note FDM 관리Secure Firewall Threat Defense 디바이스가 NetFlow 데이터를 전달하도록 구성할 수 있습니다. 센서를 배포할 때, 이벤트 정보를 CDO로 전달하도록 구성한 FDM 관리Secure Firewall Threat Defense 디바이스에서 NetFlow 데이터를 전달하도록 센서를 구성하지 마십시오.

센서 배포 지침 및 권장 사항은 Secure Cloud Analytics 센서 설치 설명서를 참조하십시오.

클라우드 기반 배포 구성 지침 및 권장 사항은 Secure Cloud Analytics 퍼블릭 클라우드 모니터링 가이드를 참조하십시오.

Note Secure Cloud Analytics 포털 UI의 지침을 검토하여 센서 및 클라우드 기반 배포을 구성할 수도 있습니다.

Secure Cloud Analytics에 대한 자세한 내용은 Secure Cloud Analytics 무료 평가판 가이드를 참조하십시오.

다음 단계

- CDO에서 Cisco Secure Cloud Analytics 알림 보기, on page 41를 계속 진행합니다.

CDO에서 Cisco Secure Cloud Analytics 알림 보기

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Events logging(이벤트 로깅) 페이지에서 방화벽 이벤트를 검토할 수 있지만 CDO 포털 UI에서 Cisco Secure Cloud Analytics 알림을 검토할 수는 없습니다. Security Analytics(보안 분석) 메뉴 옵션을 사용하여 CDO에서 Secure Cloud Analytics 포털로 교차 실행하고, 방화벽 이벤트 데이터(전체 네트워크 분석 및 모니터링을 활성화한 경우 네트워크 플로우 데이터)에서 생성된 알림을 볼 수 있습니다. Security Analytics(보안 분석) 메뉴 옵션은 하나 이상의 열려 있는 워크플로우 상태의 Secure Cloud Analytics 알림 수와 함께 배지를 표시합니다.

Security Analytics and Logging(보안 분석 및 로깅) 라이선스를 사용하여 Secure Cloud Analytics 알림을 생성하고 새 Secure Cloud Analytics 포털을 프로비저닝한 경우, CDO에 로그인한 다음 Cisco Secure Cloud Sign-On을 사용하여 Secure Cloud Analytics를 교차 실행합니다. URL을 통해 Secure Cloud Analytics 포털에 직접 액세스할 수도 있습니다.

자세한 내용은 Cisco Security Cloud Sign On을 참조하십시오.

Secure Cloud Analytics 포털에 사용자 초대

Secure Cloud Analytics 포털 프로비저닝을 요청하는 초기 사용자는 Secure Cloud Analytics 포털에서 관리자 권한을 갖습니다. 해당 사용자는 이메일로 다른 사용자를 초대하여 포털에 참여할 수 있습니다. 이러한 사용자에게 Cisco Secure Cloud Sign-On 자격증명이 없는 경우 초대 이메일의 링크를 사용하여 생성할 수 있습니다. 그러면 사용자는 Cisco Secure Cloud Sign-On 자격증명을 사용하여 CDO에서 Secure Cloud Analytics로 교차 실행하는 동안 로그인할 수 있습니다.

이메일로 다른 사용자를 Secure Cloud Analytics 포털에 초대하려면 다음을 수행합니다.

Procedure

단계 **1** Secure Cloud Analytics 포털에 관리자로 로그인합니다.

단계 **2** **Settings(**설정**)** > **Account Management(**계정 관리**)** > **User Management(**사용자 관리**)**를 선택합니다.

단계 **3** 이메일 주소를 입력합니다.

단계 **4** **Invite(**초대**)**를 클릭합니다.

CDO에서 Secure Cloud Analytics로 교차 실행

CDO에서 보안 알림을 보려면 다음을 수행합니다.

Procedure

단계 **1** CDO 포털에 로그인합니다.

단계 **2** CDO 메뉴에서 분석 > **Secure Cloud Analytics**를 선택합니다.

단계 **3** Secure Cloud Analytics 인터페이스에서 **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.

Cisco Secure Cloud Analytics 및 동적 엔티티 모델링

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Secure Cloud Analytics는 온프레미스 및 클라우드 기반 네트워크 구축을 모니터링하는 SaaS(Software as a Service) 솔루션입니다. 방화벽 이벤트 및 네트워크 플로우 데이터를 비롯한 소스에서 네트워크 트래픽에 대한 정보를 수집하여 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. Secure Cloud Analytics는 Talos와 같은 위협 인텔리전스의 다른 소스와 결합된 이 정보를 사용하여 본질적으로 악의적인 행동이 있음을 나타내는 경고를 생성합니다. 알림과 함께 Secure Cloud Analytics는 알림을 조사하고 악의적인 동작의 소스를 찾기 위한 더 나은 기반을 제공하기 위해 수집한 네트워크 및 호스트 가시성 및 상황 정보를 제공합니다.

동적 엔티티 모델링

동적 엔티티 모델링은 방화벽 이벤트 및 네트워크 플로우 데이터에 대한 동작 분석을 수행하여 네트워크의 상태를 추적합니다. Secure Cloud Analytics의 컨텍스트에서 엔티티는 네트워크의 호스트 또는 엔드포인트와 같이 시간이 지남에 따라 추적할 수 있는 항목입니다. 동적 엔터티 모델링은 전송하는 트래픽 및 네트워크에서 수행하는 활동을 기반으로 엔터티에 대한 정보를 수집합니다. **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 라이선스와 통합된 Secure Cloud Analytics는 엔티티가 일반적으로 전송하는 트래픽 유형을 확인하기 위해 방화벽 이벤트 및 기타 트래픽 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매한 경우 Secure Cloud Analytics는 엔티티 트래픽 모델링에 NetFlow 및 기타 트래픽 정보도 포함할 수 있습니다. Secure Cloud Analytics는 각 엔터티의 최신 모델을 유지하기 위해 엔터티가 계속해서 트래픽을 전송하고 잠재적으로 다른 트래픽을 전송하므로 시간이 지남에 따라 이러한 모델을 업데이트합니다. 이 정보에서 Secure Cloud Analytics는 다음을 식별합니다.

- 엔티티의 역할 - 엔티티가 일반적으로 수행하는 작업을 설명합니다. 예를 들어 엔티티가 일반적으로 이메일 서버와 연결된 트래픽을 전송하는 경우, Secure Cloud Analytics는 엔티티를 이메일

서버 역할로 할당합니다. 엔터티는 여러 역할을 수행할 수 있으므로 역할/엔티티 관계는 다대일일 수 있습니다.

- 엔티티에 대한 관찰 - 외부 IP 주소와의 하트비트 연결 또는 다른 엔티티와 설정된 원격 액세스 세션과 같이 네트워크에서의 엔티티 동작에 대한 팩트입니다. CDO와 통합하는 경우 방화벽 이벤트에서 이러한 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스도 구매한 경우, 시스템은 NetFlow에서 팩트를 가져오고 방화벽 이벤트와 NetFlow 모두에서 관찰을 생성할 수 있습니다. 관찰 자체는 관찰이 나타내는 것 이상의 의미를 전달하지 않습니다. 일반적인 고객은 수천 개의 관찰 및 몇 가지 알림을 가질 수 있습니다.

알림 및 분석

역할, 관찰 및 기타 위협 인텔리전스의 조합을 기반으로 Secure Cloud Analytics는 시스템에서 식별한 가능한 악의적인 행동을 나타내는 실행 가능한 항목인 알림을 생성합니다. 하나의 알림이 여러 관찰을 나타낼 수 있습니다. 방화벽이 동일한 연결 및 엔터티와 관련된 여러 연결 이벤트를 로깅하는 경우 하나의 알림만 생성될 수 있습니다.

예를 들어, 새 내부 디바이스 관찰 자체는 악의적인 행동을 구성하지 않습니다. 그러나 시간이 지남에 따라 엔티티가 도메인 컨트롤러와 일치하는 트래픽을 전송하면 시스템은 해당 엔티티에 도메인 컨트롤러 역할을 할당합니다. 이후에 엔티티가 비정상적인 포트를 사용하여 이전에 연결을 설정하지 않은 외부 서버에 연결하고 대량의 데이터를 전송하는 경우, 시스템은 새로운 대규모 연결(외부) 관찰 및 예외적인 도메인 컨트롤러 관찰을 로깅합니다. 해당 외부 서버가 Talos 감시 목록에 있는 것으로 식별된 경우, 이 모든 정보의 조합으로 인해 Secure Cloud Analytics가 이 엔티티의 동작에 대한 알림을 생성하고, 악성 동작을 조사하고 교정하기 위한 추가 작업을 수행하라는 메시지가 표시됩니다.

Secure Cloud Analytics 웹 포털 UI에서 알림을 열면 시스템이 알림을 생성하도록 유도한 지원 관찰을 볼 수 있습니다. 이러한 관찰을 통해 관련 엔터티에 대한 추가 컨텍스트(전송한 트래픽 포함) 및 외부 위협 인텔리전스(사용 가능한 경우)도 볼 수 있습니다. 또한 엔티티가 관련된 다른 관찰 및 알림을 보고 이 동작이 다른 잠재적인 악의적인 동작과 관련이 있는지 확인할 수 있습니다.

Secure Cloud Analytics에서 알림을 보고 닫을 때는 Secure Cloud Analytics UI의 트래픽을 허용하거나 차단할 수 없습니다. 디바이스를 액티브 모드로 구축한 경우에는 트래픽을 허용하거나 차단하도록 방화벽 액세스 제어 규칙을 업데이트하고, 패시브 모드에서 디바이스를 구축한 경우에는 방화벽 액세스 제어 규칙을 업데이트해야 합니다.

방화벽 이벤트 기반 알림 작업

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

알림 워크플로우

알림의 워크플로우는 상태를 기반으로 합니다. 시스템에서 알림을 생성할 때 기본 상태는 Open(열림)이며 사용자가 할당되지 않습니다. Alerts(알림) 요약을 볼 때 즉시 문제가 되는 모든 열린 알림이 기본적으로 표시됩니다.

참고: **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 알림은 NetFlow에서 생성된 관찰, 방화벽 이벤트에서 생성된 관찰 또는 두 데이터 소스의 관찰을 기반으로 할 수 있습니다.

알림 요약을 검토할 때 알림에 대한 상태를 초기 분류로 할당, 태그 지정 및 업데이트할 수 있습니다. 필터 및 검색 기능을 사용하여 특정 알림을 찾거나, 다른 상태의 알림을 표시하거나, 다른 태그 또는 담당자와 연결할 수 있습니다. 알림의 상태를 스누즈로 설정할 수 있습니다. 이 경우 스누즈 기간이 경과할 때까지 미해결 알림 목록에 다시 나타나지 않습니다. 알림에서 스누즈 상태를 제거하여 미해결 알림으로 다시 표시할 수도 있습니다. 알림을 검토할 때 자신 또는 시스템의 다른 사용자에게 할당할 수 있습니다. 사용자는 사용자 이름에 할당된 모든 알림을 검색할 수 있습니다.

Alerts(알림) 요약에서 알림 상세정보 페이지를 볼 수 있습니다. 이 페이지에서는 이 알림을 생성한 지원 관찰에 대한 추가 컨텍스트 및 이 알림과 관련된 엔터티에 대한 추가 컨텍스트를 검토할 수 있습니다. 이 정보는 네트워크에서 문제를 추가로 조사하고 잠재적으로 악의적인 동작을 해결하기 위해 실제 문제를 정확히 찾아내는 데 도움이 될 수 있습니다.

Stealthwatch Cloud 웹 포털 UI, CDO 및 네트워크에서 조사할 때 결과를 설명하는 알림과 함께 코멘트를 남길 수 있습니다. 이렇게 하면 나중에 참조할 수 있는 연구 기록을 만드는 데 도움이 됩니다.

분석을 완료한 경우 상태를 Closed(닫힘)로 업데이트하고 더 이상 기본적으로 미결 알림으로 표시되지 않도록 할 수 있습니다. 상황이 바뀌면 나중에 닫힌 알림을 다시 열 수도 있습니다.

다음은 지정된 알림을 조사하는 방법에 대한 일반적인 지침 및 제안 사항입니다. Stealthwatch Cloud는 알림을 로깅할 때 추가 컨텍스트를 제공하므로 이 컨텍스트를 조사에 활용할 수 있습니다.

이러한 단계는 포괄적이거나 모든 것을 포함하지 않습니다. 이는 알림 조사를 시작하는 데 사용할 수 있는 일반적인 프레임워크를 제공할 뿐입니다.

일반적으로 알림을 검토할 때 다음 단계를 수행할 수 있습니다.

1. 열린 알림 분류, on page 44
2. 나중에 분석하기 위해 알림 일시 중지, on page 45
3. 추가 조사를 위해 알림 업데이트, on page 46
4. 알림 검토 및 조사 시작, on page 46
5. 엔터티 및 사용자 검사, on page 48
6. Secure Cloud Analytics를 사용하여 문제 해결, on page 48
7. 알림 업데이트 및 닫기, on page 49

열린 알림 분류

특히 둘 이상의 알림이 아직 조사되지 않은 경우, 미해결 알림을 분류합니다.

- CDO에서 SWC로 교차 실행하고 알림을 보는 방법에 대한 자세한 내용은 CDO에서 Cisco Secure Cloud Analytics 알림 보기을 참조하십시오.

다음 질문을 합니다.

- 이 알림 유형을 높은 우선순위로 구성했습니까?
- 영향을 받는 서브넷에 대해 높은 감도를 설정했습니까?
- 네트워크의 새 엔터티에서 발생하는 비정상적인 동작입니까?
- 엔터티의 일반적인 역할은 무엇이며 이 알림의 동작이 해당 역할과 어떻게 일치합니까?
- 이 엔터티의 정상적인 동작에서 예외적으로 벗어났습니다.
- 사용자가 관련된 경우, 이는 사용자의 예상된 동작입니까, 아니면 예외적인 것입니까?
- 보호되거나 민감한 데이터가 손상될 위험이 있습니까?
- 이 동작이 계속 허용되는 경우 네트워크에 미치는 영향은 어느 정도입니까?
- 외부 엔터티와 통신하는 경우, 이러한 엔터티가 과거에 네트워크의 다른 엔터티와 연결을 설정했습니까?

우선순위가 높은 알림인 경우 조사를 계속하기 전에 인터넷에서 엔티티를 격리하거나 연결을 닫는 것을 고려하십시오.

나중에 분석하기 위해 알림 일시 중지

다른 알림에 비해 우선 순위가 낮은 알림을 스누즈합니다. 예를 들어 조직에서 이메일 서버를 FTP 서버로 용도를 변경하고 시스템에서 긴급 프로파일 알림(엔티티의 현재 트래픽이 이전에 일치하지 않았던 행동 프로파일과 일치함을 나타냄)을 생성하는 경우 이 알림을 나중에 다시 확인할 수 있습니다. 스누즈된 알림은 열린 알림과 함께 표시되지 않습니다. 이러한 스누즈된 알림을 검토하려면 특별히 필터링해야 합니다.

알림 스누즈:

Procedure

단계 **1** **Close Alert(**알림 닫기**)**를 클릭합니다.

단계 **2** Snooze this alert(이 알림 스누즈) 창의 드롭다운에서 스누즈 기간을 선택합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

What to do next

이러한 알림을 검토할 준비가 되면 다시 알림을 해제할 수 있습니다. 이렇게 하면 상태가 Open(열림)으로 설정되고 다른 Open(열림) 알림과 함께 알림이 표시됩니다.

스누즈된 알림의 스누즈를 해제합니다.

- 스누즈된 알림에서 **Unsnooze Alert(**알림 스누즈 해제**)**를 클릭합니다.

추가 조사를 위해 알림 업데이트

알림 세부 정보를 엽니다.

Procedure

단계 **1** **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.

단계 **2** 알림 유형 이름을 클릭합니다.

What to do next

초기 분류 및 우선순위에 따라 알림을 할당하고 태그를 지정합니다.

1. **Assignee(**담당자**)** 드롭다운에서 사용자를 선택하여 알림을 할당하면 사용자가 조사를 시작할 수 있습니다.
2. 드롭다운에서 하나 이상의 **Tags(**태그**)**를 선택하여 알림에 태그를 추가하여 향후 식별을 위해 알림을 더 잘 분류하고 알림에서 장기적 패턴을 설정합니다.
3. 이 알림에 대한 코멘트를 입력한 다음 **Comment(**코멘트**)**를 클릭하여 초기 결과를 추적하고 알림에 할당된 사람을 지원하는 데 필요한 코멘트를 남깁니다. 알림은 시스템 코멘트와 사용자 코멘트를 모두 추적합니다.

알림 검토 및 조사 시작

할당된 알림을 검토하는 경우 알림 세부 정보를 검토하여 Stealthwatch Cloud에서 알림을 생성한 이유를 파악합니다. 지원 관찰을 검토하여 이러한 관찰이 소스 엔터티에 미치는 영향을 파악합니다.

경고가 방화벽 이벤트를 기반으로 생성된 경우, 시스템은 방화벽 구축이 이 경고의 소스임을 인식하지 않습니다.

이 소스 엔터티에 대한 모든 지원 관찰을 확인하여 일반 동작 및 패턴을 파악하고 이 활동이 더 긴 추세의 일부일 수 있는지 확인합니다.

프로시저

단계 **1** 알림 세부사항에서 관찰 유형 옆에 있는 화살표 아이콘(➔)을 클릭하여 해당 유형의 모든 로깅된 관찰을 확인합니다.

단계 **2** **All Observations for Network(**네트워크에 대한 모든 관찰**)** 옆에 있는 화살표 아이콘(➔)을 클릭하여 이 알림의 소스 엔티티에 대해 로깅된 모든 관찰을 확인합니다.

이러한 관찰에 대한 추가 분석을 수행하려면 쉼표로 구분된 값 파일로 지원 관찰을 다운로드합니다.

- 알림 세부 정보의 Supporting Observations(지원 관찰) 창에서 **CSV**를 클릭합니다.

관찰 결과에서 소스 엔터티 동작이 악의적인 동작을 나타내는지 확인합니다. 소스 엔터티가 여러 외부 엔터티와의 연결을 설정한 경우, 외부 엔터티가 어떤 식으로든 관련이 있는지 확인합니다(예: 모든 엔터티가 유사한 지리위치 정보를 가지고 있거나 해당 IP 주소가 동일한 서브넷에 있는지 여부).

소스 엔터티 IP 주소 또는 호스트 이름에서 소스 엔터티와 관련된 추가 컨텍스트를 확인합니다. 여기에는 관련될 수 있는 기타 알림 및 관찰, 디바이스 자체에 대한 정보, 전송 중인 세션 트래픽 유형이 포함됩니다.

- 엔티티와 관련된 모든 알림을 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Alerts(**알림**)**를 선택합니다.
- IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Observations(**관찰**)**를 선택하여 엔티티와 관련된 모든 관찰을 확인합니다.
- 디바이스에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Device(**디바이스**)**를 선택합니다.
- 이 엔터티와 관련된 세션 트래픽을 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic(**세션 트래픽**)**을 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy(**복사**)**를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 소스 엔티티는 항상 네트워크 내부에 있습니다. 이를 방화벽 이벤트의 Initiator IP(이니시에이터 IP)와 비교해 보십시오. 이 IP는 연결을 시작한 엔티티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

관찰에서 다른 외부 엔터티에 대한 정보를 검토합니다. 지리위치 정보를 검토하고 지리위치 데이터 또는 Umbrella 데이터가 악성 엔티티를 식별하는지 확인합니다. 이러한 엔터티에 의해 생성된 트래픽을 확인합니다. Talos, AbuseIPDB 또는 Google에 이러한 엔터티에 대한 정보가 있는지 확인합니다. 여러 날짜의 IP 주소를 찾고 외부 엔터티가 네트워크의 엔터티와 설정한 다른 유형의 연결을 확인합니다. 필요한 경우 이러한 내부 엔터티를 찾아 보안 침해 또는 의도하지 않은 행동의 증거가 있는지 확인합니다.

소스 엔티티가 연결을 설정한 외부 엔티티 IP 주소 또는 호스트 이름에 대한 컨텍스트를 검토합니다.

- 이 엔티티에 대한 최근 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **IP Traffic(IP** 트래픽**)**을 선택합니다.
- 이 엔티티에 대한 최근 세션 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic(**세션 트래픽**)**을 선택합니다.
- **AbuseIPDB**웹사이트에서 이 엔티티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 AbuseIPDB를 선택합니다.
- Cisco Umbrella 웹사이트에서 이 엔티티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Cisco Umbrella**를 선택합니다.
- Google에서 이 IP 주소를 검색하려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Google Search(Google** 검색**)**를 선택합니다.

- Talos 웹사이트에서 이 정보에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Talos Intelligence**를 선택합니다.
- IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Add IP to watchlist(**감시 목록에 **IP** 추가**)**를 선택하여 이 엔터티를 감시 목록에 추가합니다.
- 이 엔터티의 지난 달 트래픽을 검색하려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Find IP on multiple days(**여러 날짜의 **IP** 찾기**)**를 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy(**복사**)**를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 연결된 엔터티는 항상 네트워크 외부에 있습니다. 이를 방화벽 이벤트의 Responder IP(응답자 IP)와 비교해 보십시오. 이는 연결 요청에 응답한 엔터티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

엔터티 및 사용자 검사

Stealthwatch Cloud 포털 UI에서 알림을 검토한 후 소스 엔터티, 이 알림과 관련되었을 수 있는 사용자 및 기타 관련 엔터티에 대해 직접 추가 검사를 수행할 수 있습니다.

- 소스 엔터티가 물리적으로 또는 클라우드에서 네트워크의 어느 위치에 있는지 확인하고 직접 액세스합니다. 이 엔터티에 대한 로그 파일을 찾습니다. 네트워크의 물리적 엔터티인 경우 디바이스에 액세스하여 로그 정보를 검토하고 이 동작의 원인에 대한 정보가 있는지 확인합니다. 가상 엔터티이거나 클라우드에 저장된 경우 로그에 액세스하여 이 엔터티와 관련된 항목을 검색합니다. 무단 로그인, 승인되지 않은 구성 변경 등에 대한 자세한 내용은 로그를 검사합니다.
- 엔터티를 검사합니다. 엔터티 자체에서 악성코드 또는 취약성을 식별할 수 있는지 확인합니다. 조직에서 승인하지 않은 USB 스틱과 같이 디바이스에 대한 물리적 변경이 있는지를 포함하여 악의적인 변경이 있는지 확인합니다.
- 네트워크의 사용자 또는 네트워크 외부의 사용자가 관련되었는지 확인합니다. 가능한 경우 사용자에게 무엇을 하고 있었는지 물어봅니다. 사용자가 사용할 수 없는 경우, 액세스 권한이 있어야 했는지, 그리고 퇴사한 직원이 퇴사 전에 외부 서버에 파일을 업로드하는 등의 상황이 발생했는지 확인합니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

Secure Cloud Analytics를 사용하여 문제 해결

악의적인 행동으로 인해 알림이 발생한 경우 악의적인 행동을 교정합니다. 예를 들면 다음과 같습니다.

- 악의적인 엔티티 또는 사용자가 네트워크 외부에서 로그인을 시도한 경우 엔티티 또는 사용자가 네트워크에 액세스하지 못하도록 방화벽 규칙 및 방화벽 구성을 업데이트합니다.
- 엔터티가 무단 도메인 또는 악의적인 도메인에 액세스하려고 시도한 경우 영향을 받는 엔터티를 검사하여 악성코드가 원인인지 확인합니다. 악의적인 DNS 리디렉션이 있는 경우 네트워크의 다른 엔터티 또는 봇넷의 일부가 영향을 받는지 확인합니다. 사용자가 이러한 작업을 수행하려는 경우 방화벽 설정을 테스트하는 등 합법적인 이유가 있는지 확인합니다. 도메인에 대한 추가 액세스를 방지하려면 방화벽 규칙 및 방화벽 구성을 업데이트합니다.
- 엔터티가 기록 엔터티 모델 동작과 다른 동작을 보이는 경우 동작 변경이 의도된 것인지 확인합니다. 의도하지 않은 작업인 경우 네트워크의 다른 권한이 있는 사용자가 변경을 담당하는지 확인합니다. 의도하지 않은 동작이 네트워크 외부의 엔터티와의 연결과 관련된 경우 이를 해결하기 위해 방화벽 규칙 및 방화벽 구성을 업데이트합니다.
- 취약성 또는 익스플로잇을 식별한 경우, 영향을 받는 엔티티를 업데이트 또는 패치하여 취약성을 제거하거나 무단 액세스를 방지하도록 방화벽 구성을 업데이트합니다. 네트워크의 다른 엔터티가 유사하게 영향을 받을 수 있는지 확인하고 해당 엔터티에 동일한 업데이트 또는 패치를 적용합니다. 현재 취약성 또는 익스플로잇에 수정 사항이 없는 경우 해당 벤더에 문의하십시오.
- 악성코드가 확인되면 엔티티를 격리하고 악성코드를 제거합니다. 방화벽 파일 및 악성코드 이벤트를 검토하여 네트워크의 다른 엔터티가 위험에 노출되어 있는지 확인하고, 이 악성코드가 확산되지 않도록 엔터티를 격리 및 업데이트합니다. 이 악성코드 또는 이 악성코드를 유발한 엔티티에 대한 정보로 보안 인텔리전스를 업데이트합니다. 향후 이 악성코드가 네트워크를 감염시키는 것을 방지하려면 방화벽 액세스 제어와 파일 및 악성코드 규칙을 업데이트하십시오. 필요에 따라 벤더에 알립니다.
- 악의적인 행동으로 인해 데이터가 유출된 경우 무단 소스로 전송되는 데이터의 특성을 확인합니다. 무단 데이터 유출에 대한 조직의 프로토콜을 따르십시오. 이 소스에 의한 향후 데이터 유출 시도를 방지하려면 방화벽 구성을 업데이트하십시오.

알림 업데이트 및 닫기

결과에 따라 태그를 추가합니다.

Procedure

단계 **1** Secure Cloud Analytics 포털 UI에서 **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.

단계 **2** 드롭다운에서 하나 이상의 **Tags(**태그**)**를 선택합니다.

조사 결과 및 수행한 교정 단계를 설명하는 최종 코멘트를 추가합니다.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

알림을 닫고 유용하거나 도움이 되지 않음으로 표시합니다.

1. 알림 세부 정보에서 **Close Alert(**알림 닫기**)**를 클릭합니다.

2. 알림이 도움이 되었으면 **Yes(**예**)**를 선택하고, 알림이 도움이 되지 않았다면 **No(**아니요**)**를 선택합니다. 이는 알림이 악의적인 행동으로 인해 발생했음을 의미하는 것이 아니라 해당 알림이 조직에 도움이 되었음을 의미합니다.
3. **Save(**저장**)**를 클릭합니다.

What to do next

종료된 알림 다시 열기

종료된 알림과 관련된 추가 정보를 발견하거나 알림과 관련된 코멘트를 더 추가하려는 경우 알림을 다시 열어 상태를 Open(열림)으로 변경할 수 있습니다. 그런 다음 필요에 따라 알림을 변경한 다음 추가 조사가 완료되면 알림을 닫을 수 있습니다.

종료된 알림을 다시 엽니다.

- 닫힌 알림의 세부 사항에서 **Reopen Alert(**알림 다시 열기**)**를 클릭합니다.

알림 우선순위 수정

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

알림 유형은 기본 우선순위와 함께 제공되며, 이는 시스템이 이 유형의 알림 생성에 대한 민감도에 영향을 미칩니다. 알림은 기본적으로 Cisco 인텔리전스 및 기타 요인에 따라 낮음 또는 보통으로 설정됩니다. 네트워크 환경에 따라 알림 유형의 우선순위를 다시 지정하여 우려되는 특정 알림을 강조할 수 있습니다. 모든 알림 유형을 낮음, 보통 또는 높음 우선순위로 구성할 수 있습니다.

- **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.
- Settings(설정) 드롭다운 아이콘()을 클릭한 다음 **Alert Types and Priorities(**알림 유형 및 우선순위**)**를 선택합니다.
- 알림 유형 옆에 있는 편집 아이콘()을 클릭하고 낮음, 중간 또는 높음을 선택하여 우선순위를 변경합니다.

라이브 이벤트 보기

Live events(라이브 이벤트) 페이지에는 입력한 이벤트 로깅 페이지에서 이벤트 검색 및 필터링과 일치하는 최신 500개의 이벤트가 표시됩니다. 라이브 이벤트 페이지에 최대 500개의 이벤트가 표시되고 더 많은 이벤트가 스트리밍되는 경우, CDO는 최신 라이브 이벤트를 표시하고 가장 오래된 라이브 이벤트를 기록 이벤트 페이지로 전송하여 총 라이브 이벤트 수를 500개로 유지합니다. 이 전송을 수행하는 데 약 1분이 걸립니다. 필터링 기준이 추가되지 않은 경우, 이벤트를 로깅하도록 구성된 규칙에 의해 생성된 모든 최신 라이브 500 이벤트가 표시됩니다.

이벤트의 타임스탬프는 이벤트를 보는 CDO 관리자의 현지 시간으로 표시됩니다.

라이브 이벤트가 재생 중인지 일시 중지되었는지에 상관없이 필터링 기준을 변경하면 이벤트 화면이 지워지고 수집 프로세스가 다시 시작됩니다.

CDO 이벤트 뷰어에서 라이브 이벤트를 보려면 다음을 수행합니다.

Procedure

단계 **1** 탐색창에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** **Live(**라이브**)** 탭을 클릭합니다.

What to do next

이벤트를 재생하고 일시 중지하는 방법을 참조하십시오.

관련 정보**:**

- 라이브 이벤트 재생/일시 중지, on page 51
- 과거 이벤트 보기, on page 52
- 이벤트 보기 사용자 지정, on page 52

라이브 이벤트 재생/일시 중지

라이브 이벤트가 스트리밍될 때 라이브 이벤트를 "재생" ▶ 또는 "일시 중지" ⏸ 할 수 있습니다. 라이브 이벤트가 "재생" 중인 경우 CDO는 이벤트 뷰어에 지정된 필터링 기준과 일치하는 이벤트를 수신된 순서대로 표시합니다. 이벤트가 일시 중지된 경우 CDO는 라이브 이벤트 재생을 다시 시작할 때까지 라이브 이벤트 페이지를 업데이트하지 않습니다. 이벤트 재생을 다시 시작하면 CDO는 이벤트 재생을 다시 시작한 시점부터 Live(라이브) 페이지에 이벤트를 채우기 시작합니다. 누락된 항목은 다시 채우지 않습니다.

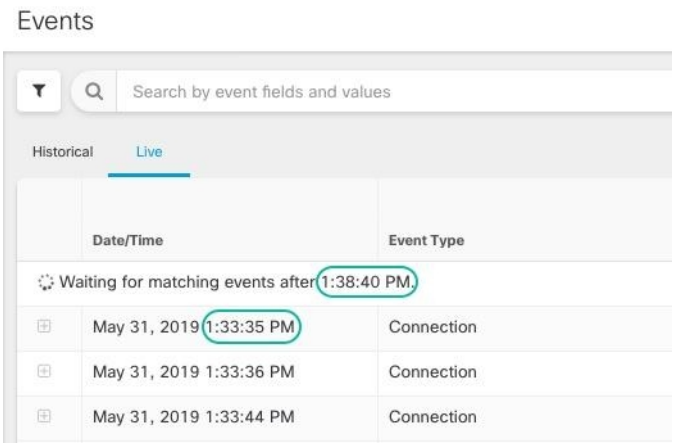
라이브 이벤트 스트리밍을 재생하거나 일시 중지했는지 여부에 관계없이 CDO가 수신한 모든 이벤트를 보려면 Historical(기록) 탭을 클릭합니다.

라이브 이벤트 자동 일시 중지

약 5분 동안 이벤트를 표시한 후 CDO는 라이브 이벤트의 스트림을 일시 중지한다고 경고합니다. 이때 링크를 클릭하여 다른 5분 동안 라이브 이벤트 스트리밍을 계속하거나 스트림을 중지할 수 있습니다. 준비가 되면 라이브 이벤트 스트림을 다시 시작할 수 있습니다.

이벤트 수신 및 보고

라이브 이벤트 뷰어에서 SEC(Secure Event Connector) 수신 이벤트와 CDO 게시 이벤트 사이에 약간의 지연이 발생할 수 있습니다. Live(라이브) 페이지에서 간격을 볼 수 있습니다. 이벤트의 타임스탬프는 SEC에서 이벤트를 수신한 시간입니다.



과거 이벤트 보기

Live events(라이브 이벤트) 페이지에는 입력한 이벤트 로깅 페이지에서 이벤트 검색 및 필터링과 일치하는 최신 500개의 이벤트가 표시됩니다. 가장 최근의 500개 이벤트보다 오래된 이벤트는 기록 이벤트 테이블로 전송됩니다. 이 전송을 수행하는 데 약 1분이 걸립니다. 그런 다음 저장한 모든 이벤트를 필터링하여 원하는 이벤트를 찾을 수 있습니다.

과거 이벤트를 보려면:

Procedure

단계 **1** 탐색창에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** 기록 탭을 클릭합니다. 기본적으로 기록 이벤트 테이블을 열면 지난 1시간 내에 수집된 이벤트가 표시되도록 필터가 설정됩니다.

이벤트 속성은 FDM(Firepower Device Manager) 또는 ASDM(Adaptive Security Device Manager)에서 보고하는 것과 거의 동일합니다.

- Firepower Threat Defense 이벤트 속성에 대한 전체 설명은 Cisco FTD 시스템 로그 메시지를 참조하십시오.
- ASA 이벤트 속성에 대한 전체 설명은 Cisco ASA Series 시스템 로그 메시지를 참조하십시오.

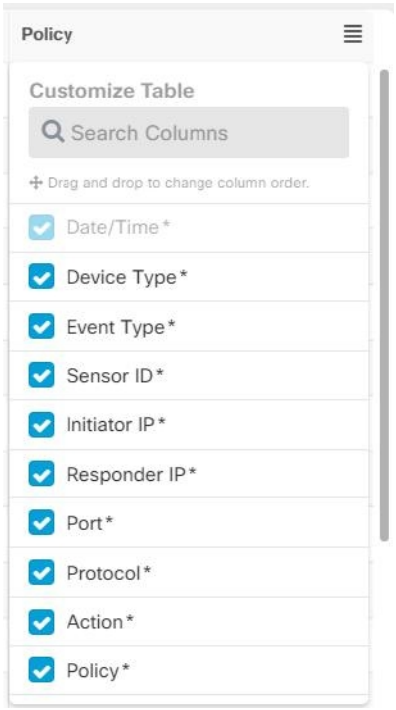
이벤트 보기 사용자 지정

Event Logging(이벤트 로깅) 페이지에 대한 모든 변경 사항은 이 페이지에서 빠져나왔다가 나중에 다시 돌아올 때를 위해 자동으로 저장됩니다.

Note 라이브 및 기록 이벤트 보기의 구성은 동일합니다. 이벤트 보기를 사용자 정의하면 이러한 변경 사항이 Live(라이브) 및 Historical(기록) 보기에 모두 적용됩니다.

열

원하는 보기에 적용되는 열 헤더만 포함하도록 라이브 및 기록 이벤트에 대한 이벤트 보기를 수정할 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘 을 클릭하고 원하는 열을 선택하거나 선택 취소합니다.



별표가 있는 열은 언제든지 제거할 수 있지만 기본적으로 이벤트 테이블 내에 제공됩니다. 검색 창을 사용하여 포함할 추가 열에 대한 키워드를 수동으로 검색합니다.

순서

Events(이벤트) 보기의 열 순서를 바꿀 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘 을 클릭하여 선택한 열 목록을 확장하고 원하는 순서로 열을 수동으로 끌어서 놓습니다. 여기서 드롭다운 메뉴의 목록 맨 위에 있는 열은 이벤트 보기에서 맨 왼쪽에 있는 열입니다.

관련 정보:

- 이벤트 로깅 페이지에서 이벤트 검색 및 필터링
- Security Analytics and Logging의 이벤트 속성

이벤트 로깅 페이지의 열 표시 및 숨기기

Event Logging(이벤트 로깅) 페이지에는 구성된 ASA 및 FDM 관리 디바이스에서 Cisco Cloud로 전송된 ASA 및 FTD Syslog 이벤트 및 ASA NSEL(NetFlow Secure Event Logging) 이벤트가 표시됩니다.

테이블과 함께 Show/Hide(표시/숨기기) 위젯을 사용하여 Event Logging(이벤트 로깅) 페이지에서 열을 표시하거나 숨길 수 있습니다.

Procedure

단계 **1** CDO 탐색 모음에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** 테이블의 맨 오른쪽으로 스크롤하여 **Show/Hide Columns(**열 표시/숨기기**)** 버튼 ≡를 클릭합니다.

단계 **3** 표시하려는 열을 선택하고, 숨기려는 열을 선택 취소합니다.

단계 **4** Show/Hide Columns(열 표시/숨기기) 드롭다운 메뉴의 열 이름 위에 마우스를 올려 놓고 회색 십자 표시를 눌러 열 순서를 다시 정렬합니다.

테넌트에 로그인하는 다른 사용자는 열이 다시 표시되거나 숨겨질 때까지 표시하도록 선택한 것과 동일한 열을 볼 수 있습니다.

이 표에서는 열 헤더에 대해 설명합니다.

열 헤더	설명
날짜/시간	디바이스가 이벤트를 생성한 시간 시간은 컴퓨터의 로컬 시간으로 표시됩니다.
디바이스 유형	또는 FTD(Firepower Threat Defense)

열 헤더	설명
이벤트 유형	이 복합 열에는 다음 중 하나가 포함될 수 있습니다. • **FTD** 이벤트 유형 • Connection(연결) - 액세스 제어 규칙의 연결 이벤트를 표시합니다. • File(파일) - 액세스 제어 규칙의 파일 정책에 의해 보고된 이벤트를 표시합니다. • Intrusion(침입) - 액세스 제어 규칙의 침입 정책에 의해 보고된 이벤트를 표시합니다. • Malware(악성코드) - 액세스 제어 규칙의 악성코드 정책에 의해 보고된 이벤트를 표시합니다. • ASA**Event Types(**이벤트 유형**)** -이러한 이벤트 유형은 Syslog 또는 NetFlow 이벤트의 그룹을 나타냅니다. 어떤 Syslog ID 또는 어떤 NetFlow ID가 어떤 그룹에 포함되어 있는지에 대한 자세한 내용은 ASA 이벤트 유형을 참조하십시오. • 구문 분석된 이벤트 - 구문 분석된 Syslog 이벤트는 다른 Syslog 이벤트보다 더 많은 이벤트 속성을 포함하며, CDO는 이러한 속성을 기반으로 더 빠르게 검색 결과를 반환할 수 있습니다. 구문 분석된 이벤트는 필터링 카테고리가 아닙니다. 그러나 구문 분석된 이벤트 ID는 Event Types(이벤트 유형) 열에 기울임꼴로 표시됩니다. 기울임꼴로 표시되지 않은 이벤트 ID는 구문 분석되지 않습니다. • ASA NetFlow Event IDs(NetFlow 이벤트 ID): ASA의 모든 Netflow(NSEL) 이벤트가 여기에 표시됩니다.
센서 ID	센서 ID는 이벤트가 보안 이벤트 커넥터로 전송되는 IP 주소입니다. 이는 일반적으로 Firepower Threat Defense 또는 ASA의 관리 인터페이스입니다.

열 헤더	설명
초기자 IP	이는 네트워크 트래픽 소스의 IP 주소입니다. Initiator address(이니시에이터 주소) 필드의 값은 이벤트 세부사항의 InitiatorIP(이니시에이터 IP) 필드 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.
응답기 IP	이것은 패킷의 대상 IP 주소입니다. Destination address(대상 주소) 필드의 값은 이벤트 세부사항의 ResponderIP 필드에 있는 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.
포트	세션 **responder**가 사용하는 포트 또는 ICMP 코드 대상 포트의 값은 이벤트 세부사항의 **ResponderPort** 값에 해당합니다.
프로토콜	이벤트의 프로토콜을 나타냅니다.

열 헤더	설명
작업	규칙에 의해 정의된 보안 작업을 지정합니다. 입력하는 값은 찾으려는 값과 정확히 일치해야 합니다. 그러나 대/소문자는 중요하지 않습니다. 연결, 파일, 침입, 악성코드, Syslog 및 NetFlow 이벤트 유형에 대해 서로 다른 값을 입력합니다. • 연결 이벤트 유형의 경우 필터는 AC_RuleAction 특성에서 일치 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다. • 파일 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다. • 침입 이벤트 유형의 경우 필터는 InLineResult 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allowed(허용됨), Blocked(차단됨), Trusted(신뢰할 수 있음)일 수 있습니다. • 악성코드 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Cloud Lookup Timeout(클라우드 조회 시간 초과)일 수 있습니다. • Syslog 및 NetFlow 이벤트 유형의 경우 필터는 Action(작업) 속성에서 일치하는 항목을 검색합니다.
정책	이벤트를 트리거한 정책의 이름입니다. ASA 및 FDM 관리디바이스의 이름은 다릅니다.

관련 정보:

이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 89

사용자 지정 가능한 이벤트 필터

SaaS(Secure Logging Analytics) 고객은 자주 사용하는 맞춤형 필터를 생성하고 저장할 수 있습니다.

필터의 요소는 구성할 때 필터 탭에 저장됩니다. Event Logging(이벤트 로깅) 페이지로 돌아갈 때마다 이러한 검색을 사용할 수 있습니다. 테넌트의 다른 CDO 사용자는 사용할 수 없습니다. 둘 이상의 테넌트를 관리하는 경우 다른 테넌트에서는 사용할 수 없습니다.

Note 필터 탭에서 작업할 때 필터 기준을 수정하면 해당 변경 사항이 사용자 지정 필터 탭에 자동으로 저장됩니다.

Procedure

단계 **1** 주 메뉴에서 분석 > 이벤트 로깅을(를) 선택합니다.

단계 **2** 모든 값의 Search(검색) 필드를 지웁니다.

단계 **3** 이벤트 테이블 위에서 파란색 더하기 버튼을 클릭하여 View(보기) 탭을 추가합니다. 필터 보기에는 이름을 지정할 때까지 "View 1", "View 2", "View 3" 등의 레이블이 지정됩니다.

단계 **4** View(보기) 탭을 선택합니다.

단계 **5** 필터 표시줄을 열고 맞춤형 필터에서 원하는 필터 속성을 선택합니다. 이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 89의 내용을 참조하십시오. 필터 특성만 맞춤형 필터에 저장됩니다.

단계 **6** 이벤트 로깅 테이블에 표시할 열을 사용자 정의합니다. 열 표시 및 숨기기에 대한 설명은 이벤트 로깅 페이지의 열 표시 및 숨기기, on page 54의 내용을 참조하십시오.

단계 **7** "View X" 레이블이 있는 필터 탭을 두 번 클릭하고 이름을 바꿉니다.

단계 **8** (선택 사항) 맞춤형 필터를 생성했으므로 이제 Search(검색) 필드에 검색 기준을 추가하여 맞춤형 필터를 변경하지 않고도 Event Logging(이벤트 로깅) 페이지에 표시되는 결과를 미세 조정할 수 있습니다. 이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 89의 내용을 참조하십시오.

Security Analytics and Logging의 이벤트 속성

이벤트 속성 설명

CDO에서 사용하는 이벤트 속성은 FDM(Firepower Device Manager) 또는 ASDM(Adaptive Security Device Manager)에서 보고하는 것과 거의 동일합니다.

- FDM 매니지드 디바이스 이벤트 속성에 대한 전체 설명은 Cisco Firepower Threat Defense 시스로그 메시지를 참조하십시오.

일부 ASA 시스템 로그 이벤트는 "구문 분석"되며, 다른 이벤트에는 속성:값 쌍을 사용하여 이벤트 로깅 테이블의 내용을 필터링할 때 사용할 수 있는 추가 속성이 있습니다. 시스템 로그 이벤트의 다른 중요한 속성은 다음 추가 항목을 참조하십시오.

- 일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성
- Syslog 이벤트에 대한 이벤트 이름 속성

• 시스템 로그 이벤트의 시간 속성

일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성

일부 시스템 로그 이벤트에는 추가 속성 "EventGroup" 및 "EventGroupDefinition"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 이러한 추가 속성을 사용하여 이벤트 테이블을 필터링할 수 있습니다. 예를 들어 Event Logging(이벤트 로깅) 테이블의 검색 필드에 `apfw:415*`를 입력하여 애플리케이션 방화벽 이벤트를 필터링할 수 있습니다.

Syslog 메시지 클래스와 연결된 메시지 **ID** 번호

EventGroup	**EventGroupDefinition**	시스템 로그 메시지 **ID** 번호**(**처음 **3**자리**)**
aaa/auth	사용자 인증	109, 113
acl/session	액세스 목록/사용자 세션	106
apfw	애플리케이션 방화벽	415
bridge	투명한 방화벽	110, 220
ca	PKI 인증 기관	717
citrix	Citrix 클라이언트	723
clst	클러스터링	747
cmgr	카드 관리	323
config	CLI(Command Line Interface)	111, 112, 208, 308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	Dynamic Access Policy	734
eap, eapoudp	Network Admission Control용 EAPoUDP 또는 EAP	333, 334
eigrp	EIGRP 라우팅	336
email	이메일 프록시	719
ipaa/envmon	환경 모니터링	735
HA	페일오버	101, 102, 103, 104, 105, 210, 311, 709
idfw	ID 기반 방화벽	746
ids	Intrusion Detection System(침입 탐지 시스템)	733

EventGroup	**EventGroupDefinition**	시스템 로그 메시지 **ID** 번호**(**처음 **3**자리**)**
ids/ips	침입 탐지 시스템/침입 방지 시스템	400
ikev2	IKEv2 툴킷	750, 751, 752
ip	IP 스택	209, 215, 313, 317, 408
ipaa	IP 주소 할당	735
ips	Intrusion Protection System(침입 방지 시스템)	401, 420
ipv6	IPv6	325
l4tm	차단 목록, 허용 목록, 그레이리스트	338
lic	라이선싱	444
mdm-proxy	MDM 프록시	802
nac	NAC(Network Admission Control)	731, 732
vpn/nap	IKE 및 IPsec/네트워크 액세스 포인트	713
np	네트워크 프로세서	319
ospf	OSPF 라우팅	318, 409, 503, 613
passwd	비밀번호 암호화	742
PP	전화 프록시	337
rip	RIP 라우팅	107, 312
rm	리소스 관리자	321
sch	Smart Call Home	120
session	사용자 세션	108, 201, 202, 204, 302, 303, 304, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
session/natpat	사용자 세션/NAT 및 PAT	305
snmp	SNMP	212
ssafe	ScanSafe	775
ssl/np ssl	SSL 스택/NP SSL	725
svc	SSL VPN 클라이언트	722

EventGroup	EventGroupDefinition	시스템 로그 메시지 ID 번호(처음 3자리)
sys	시스템	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711, 741
tre	트랜잭션 규칙 엔진	780
ucime	UC-IME	339
tag-switching	서비스 태그 스위칭	779
td	위협 탐지	733
VM	VLAN 매핑	730
vpdn	PPTP 및 L2TP 세션	213, 403, 603
vpn	IKE 및 IPSEC	316, 320, 404, 501, 602, 402
vpnc	VPN 클라이언트	611
vpnfo	VPN 페일오버	720
vpnlb	VPN 로드 밸런싱	718
vxlan	VXLAN	778
webfo	WebVPN 페일오버	721
webvpn	WebVPN 및 AnyConnect Client	716
session/natpat	사용자 세션/NAT 및 PAT	305

Syslog 이벤트에 대한 이벤트 이름 속성

일부 시스템 로그 이벤트에는 추가 속성 "EventName"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 EventName 특성을 사용하여 이벤트 테이블을 필터링하여 찾을 수 있습니다. 예를 들어 Event Logging(이벤트 로깅) 테이블의 검색 필드에 **EventName:"Denied IP Packet"**을 입력하여 "Denied IP packet(거부된 IP 패킷)"에 대한 이벤트를 필터링할 수 있습니다.

시스템 로그 이벤트 **ID** 및 이벤트 이름 테이블

- AAA 시스템 로그 이벤트 ID 및 이벤트 이름
- 봇넷 시스템 로그 이벤트 ID 및 이벤트 이름
- 페일오버 시스템 로그 이벤트 ID 및 이벤트 이름
- 방화벽 거부 시스템 로그 이벤트 ID 및 이벤트 이름
- 방화벽 트래픽 시스템 로그 이벤트 ID 및 이벤트 이름
- ID 기반 방화벽 시스템 로그 이벤트 ID 및 이벤트 이름

- IPSec 시스템 로그 이벤트 ID 및 이벤트 이름
- NAT 시스템 로그 이벤트 ID 및 이벤트 이름
- SSL VPN 시스템 로그 이벤트 ID 및 이벤트 이름

AAA 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 **ID**	이벤트 이름
109001	AAA Begin
109002	AAA Failed
109003	AAA Server Failed
109005	Authentication Success
109006	Authentication Failed
109007	Authorization Success
109008	Authorization Failed
109010	AAA Pending
109011	AAA Session Started
109012	AAA Session Ended
109013	AAA
109014	AAA Failed
109016	AAA ACL not found
109017	AAA Limit Reach
109018	AAA ACL Empty
109019	AAA ACL error
109020	AAA ACL error
109021	AAA error
109022	AAA HTTP limit reached
109023	AAA auth required
109024	Authorization Failed
109025	Authorization Failed
109026	AAA error
109027	AAA Server error

이벤트 **ID**	이벤트 이름
109028	AAA Bypassed
109029	AAA ACL error
109030	AAA ACL error
109031	Authentication Failed
109032	AAA ACL error
109033	Authentication Failed
109034	Authentication Failed
109035	AAA Limit Reach
113001	AAA Session limit reach
113003	AAA overridden
113004	AAA Successful
113005	Authorization Rejected
113006	AAA user locked
113007	AAA User unlocked
113008	AAA successful
113009	AAA retrieved
113010	AAA Challenge received
113011	AAA retrieved
113012	Authentication Successful
113013	AAA error
113014	AAA error
113015	Authentication Rejected
113016	AAA Rejected
113017	AAA Rejected
113018	AAA ACL error
113019	AAA Disconnected
113020	AAA error
113021	AAA Logging Fail

이벤트 **ID**	이벤트 이름
113022	AAA Failed
113023	AAA reactivated
113024	AAA Client certification
113025	AAA Authentication fail
113026	AAA error
113027	AAA error

봇넷 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 **ID**	이벤트 이름
338001	Botnet Source Block List
338002	Botnet Destination Block List
338003	Botnet Source Block List
338004	Botnet Destination Block List
338101	Botnet Source Allow List
338102	Botnet destination Allow List
338202	Botnet destination Grey
338203	Botnet Source Grey
338204	Botnet Destination Grey
338301	Botnet DNS Intercepted
338302	Botnet DNS
338303	Botnet DNS
338304	Botnet Download successful
338305	Botnet Download failed
338306	Botnet Authentication failed
338307	Botnet Decrypt failed
338308	Botnet Client
338309	Botnet Client
338310	Botnet dyn filter failed

페일오버 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 **ID**	이벤트 이름
101001	Failover Cable OK
101002	Failover Cable BAD
101003	Failover Cable not connected
101004	Failover Cable not connected
101005	Failover Cable reading error
102001	Failover Power failure
103001	No response from failover mate
103002	Failover mate interface OK
103003	Failover mate interface BAD
103004	Failover mate reports failure
103005	Failover mate reports self failure
103006	Failover version incompatible
103007	Failover version difference
104001	Failover role switch
104002	Failover role switch
104003	Failover unit failed
104004	Failover unit OK
106100	Permit/Denied by ACL
210001	Stateful Failover error
210002	Stateful Failover error
210003	Stateful Failover error
210005	Stateful Failover error
210006	Stateful Failover error
210007	Stateful Failover error
210008	Stateful Failover error
210010	Stateful Failover error
210020	Stateful Failover error

이벤트 **ID**	이벤트 이름
210021	Stateful Failover error
210022	Stateful Failover error
311001	Stateful Failover update
311002	Stateful Failover update
311003	Stateful Failover update
311004	Stateful Failover update
418001	Denied Packet to Management
709001	Failover replication error
709002	Failover replication error
709003	Failover replication start
709004	Failover replication complete
709005	Failover receive replication start
709006	Failover receive replication complete
709007	Failover replication failure
710003	Denied access to Device

방화벽 거부 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 **ID**	이벤트 이름
106001	Denied by Security Policy
106002	Outbound Deny
106006	Denied by Security Policy
106007	Denied Inbound UDP
106008	Denied by Security Policy
106010	Denied by Security Policy
106011	Denied Inbound
106012	Denied due to Bad IP option
106013	Dropped Ping to PAT IP
106014	Denied Inbound ICMP

이벤트 **ID**	이벤트 이름
106015	Denied by Security Policy
106016	Denied IP Spoof
106017	Denied due to Land Attack
106018	Denied outbound ICMP
106020	Denied IP Packet
106021	Denied TCP
106022	Denied Spoof packet
106023	Denied IP Packet
106025	Dropped Packet failed to Detect context
106026	Dropped Packet failed to Detect context
106027	Dropped Packet failed to Detect context
106100	Permit/Denied by ACL
418001	Denied Packet to Management
710003	Denied access to Device

방화벽 트래픽 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 **ID**	이벤트 이름
108001	Inspect SMTP
108002	Inspect SMTP
108003	Inspect ESMTP Dropped
108004	Inspect ESMTP
108005	Inspect ESMTP
108006	Inspect ESMTP Violation
108007	Inspect ESMTP
110002	No Router found
110003	Failed to Find Next hop
209003	Fragment Limit Reach
209004	Fragment invalid Length

이벤트 **ID**	이벤트 이름
209005	Fragment IP discard
302003	H245 Connection Start
302004	H323 Connection start
302009	Restart TCP
302010	Connection USAGE
302012	H225 CALL SIGNAL CONN
302013	Built TCP
302014	Teardown TCP
302015	Built UDP
302016	Teardown UDP
302017	Built GRE
302018	Teardown GRE
302019	H323 Failed
302020	Built ICMP
302021	Teardown ICMP
302022	Built TCP Stub
302023	Teardown TCP Stub
302024	Built UDP Stub
302025	Teardown UDP Stub
302026	Built ICMP Stub
302027	Teardown ICMP Stub
302033	Connection H323
302034	H323 Connection Failed
302035	Built SCTP
302036	Teardown SCTP
303002	FTP file download/upload
303003	Inspect FTP Dropped
303004	Inspect FTP Dropped

이벤트 **ID**	이벤트 이름
303005	Inspect FTP reset
313001	ICMP Denied
313004	ICMP Drop
313005	ICMP Error Msg Drop
313008	ICMP ipv6 Denied
324000	GTP Pkt Drop
324001	GTP Pkt Error
324002	Memory Error
324003	GTP Pkt Drop
324004	GTP Version 지원하지 않음
324005	GTP Tunnel Failed
324006	GTP Tunnel Failed
324007	GTP Tunnel Failed
337001	Phone Proxy SRTP Failed
337002	Phone Proxy SRTP Failed
337003	Phone Proxy SRTP Auth Fail
337004	Phone Proxy SRTP Auth Fail
337005	Phone Proxy SRTP no Media Session
337006	Phone Proxy TFTP Unable to Create File
337007	Phone Proxy TFTP Unable to Find File
337008	Phone Proxy Call Failed
337009	Phone Proxy Unable to Create Phone Entry
400000	IPS IP options-Bad Option List
400001	IPS IP options-Record Packet Route
400002	IPS IP options-Timestamp
400003	IPS IP options-Security
400004	IPS IP options-Loose Source Route
400005	IPS IP options-SATNET ID

이벤트 **ID**	이벤트 이름
400006	IPS IP options-Strict Source Route
400007	IPS IP Fragment Attack
400008	IPS IP Impossible Packet
400009	IPS IP Fragments Overlap
400010	IPS ICMP Echo Reply
400011	IPS ICMP Host Unreachable
400012	IPS ICMP Source Quench
400013	IPS ICMP Redirect
400014	IPS ICMP Echo Request
400015	IPS ICMP Time Exceeded for a Datagram
400017	IPS ICMP Timestamp Request
400018	IPS ICMP Timestamp Reply
400019	ICMP Information Request
400020	IPS ICMP Information Reply
400021	ICMP Address Mask Request
400022	ICMP Address Mask Request
400023	IPS Fragmented ICMP Traffic
400024	IPS Large ICMP Traffic
400025	IPS Ping of Death Attack
400026	IPS TCP NULL flags
400027	IPS TCP SYN+FIN flags
400028	IPS TCP FIN only flags
400029	IPS FTP Improper Address Specified
400030	IPS FTP Improper Port Specified
400031	IPS UDP Bomb attack
400032	IPS UDP Snork attack
400033	IPS UDP Chargen DoS attack
400034	IPS DNS HINFO Request

이벤트 **ID**	이벤트 이름
400035	IPS DNS Zone Transfer
400036	IPS DNS Zone Transfer from High Port
400037	IPS DNS Request for All Records
400038	IPS RPC Port Registration
400039	IPS RPC Port Unregistration
400040	IPS RPC Dump
400041	IPS Proxied RPC Request
400042	IPS YP server Portmap Request
400043	IPS YP bind Portmap Request
400044	IPS YP password Portmap Request
400045	IPS YP update Portmap Request
400046	IPS YP transfer Portmap Request
400047	IPS Mount Portmap Request
400048	IPS Remote execution Portmap Request
400049	IPS Remote execution Attempt
400050	IPS Statd Buffer Overflow
406001	Inspect FTP Dropped
406002	Inspect FTP Dropped
407001	Host Limit Reach
407002	Embryonic limit Reached
407003	Established limit Reached
415001	Inspect Http Header Field Count
415002	Inspect Http Header Field Length
415003	Inspect Http body Length
415004	Inspect Http content-type
415005	Inspect Http URL length
415006	Inspect Http URL Match
415007	Inspect Http Body Match

이벤트 **ID**	이벤트 이름
415008	Inspect Http Header match
415009	Inspect Http Method match
415010	Inspect transfer encode match
415011	Inspect Http Protocol Violation
415012	Inspect Http Content-type
415013	Inspect Http Malformed
415014	Inspect Http Mime-Type
415015	Inspect Http Transfer-encoding
415016	Inspect Http Unanswered
415017	Inspect Http Argument match
415018	Inspect Http Header length
415019	Inspect Http status Matched
415020	Inspect Http non-ASCII
416001	Inspect SNMP dropped
419001	Dropped packet
419002	Duplicate TCP SYN
419003	Packet modified
424001	Denied IP Packet
424002	Dropped Packet
431001	Dropped RTP
431002.	Dropped RTCP
500001	Inspect ActiveX
500002	Inspect Java
500003	Inspect TCP Header
500004	Inspect TCP Header
500005	Inspect Connection Terminated
508001	Inspect DCERPC Dropped
508002	Inspect DCERPC Dropped

이벤트 ID	이벤트 이름
509001	Prevented No Forward Cmd
607001	Inspect SIP
607002	Inspect SIP
607003	Inspect SIP
608001	Inspect Skinny
608002	Inspect Skinny dropped
608003	Inspect Skinny dropped
608004	Inspect Skinny dropped
608005	Inspect Skinny dropped
609001	Built Local-Host
609002	Teardown Local Host
703001	H225 Unsupported Version
703002	H225 Connection
726001	Inspect Instant Message

ID 기반 방화벽 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 ID	이벤트 이름
746001	Import started
746002	Import complete
746003	Import failed
746004	Exceed user group limit
746005	AD Agent down
746006	AD Agent out of sync
746007	Netbios response failed
746008	Netbios started
746009	Netbios stopped
746010	Import user failed
746011	Exceed user limit

이벤트 **ID**	이벤트 이름
746012	User IP add
746013	User IP delete
746014	FQDN Obsolete
746015	FQDN resolved
746016	DNS lookup failed
746017	Import user issued
746018	Import user done
746019	Update AD Agent failed

IPSec 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 **ID**	이벤트 이름
402114	Invalid SPI received
402115	Unexpected protocol received
402116	Packet doesn't match identity
402117	Non-IPSEC packet received
402118	Invalid fragment offset
402119	Anti-Replay check failure
402120	Authentication failure
402121	Packet dropped
426101	cLACP Port Bundle
426102	cLACP Port Standby
426103	cLACP Port Moved To Bundle From Standby
426104	cLACP Port Unbundled
602103	Path MTU updated
602104	Path MTU exceeded
602303	New SA created
602304	SA deleted
702305	SA expiration - Sequence rollover
702307	SA expiration - Data rollover

NAT 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 **ID**	이벤트 이름
201002	Max connection Exceeded for host
201003	Embryonic limit exceed
201004	UDP connection limit exceed
201005	FTP connection failed
201006	RCMD connection failed
201008	New connection Disallowed
201009	Connection Limit exceed
201010	Embryonic Connection limit exceeded
201011	Connection Limit exceeded
201012	Per-client embryonic connection limit exceeded
201013	Per-client connection limit exceeded
202001	Global NAT exhausted
202005	Embryonic connection error
202011	Connection Limit exceeded
305005	No NAT group found
305006	Translation failed
305007	Connection dropped
305008	NAT allocation issue
305009	NAT Created
305010	NAT teardown
305011	PAT created
305012	PAT teardown
305013	Connection denied

SSL VPN 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 **ID**	이벤트 이름
716001	WebVPN Session Started
716002	WebVPN Session Terminated
716003	WebVPN User URL access
716004	WebVPN User URL access denied
716005	WebVPN ACL error
716006	WebVPN User Disabled

이벤트 **ID**	이벤트 이름
716007	WebVPN Unable to Create
716008	WebVPN Debug
716009	WebVPN ACL error
716010	WebVPN User access network
716011	WebVPN User access
716012	WebVPN User Directory access
716013	WebVPN User file access
716014	WebVPN User file access
716015	WebVPN User file access
716016	WebVPN User file access
716017	WebVPN User file access
716018	WebVPN User file access
716019	WebVPN User file access
716020	WebVPN User file access
716021	WebVPN user access file denied
716022	WebVPN Unable to connect proxy
716023	WebVPN session limit reached
716024	WebVPN User access error
716025	WebVPN User access error
716026	WebVPN User access error
716027	WebVPN User access error
716028	WebVPN User access error
716029	WebVPN User access error
716030	WebVPN User access error
716031	WebVPN User access error
716032	WebVPN User access error
716033	WebVPN User access error
716034	WebVPN User access error
716035	WebVPN User access error
716036	WebVPN User login successful
716037	WebVPN User login failed
716038	WebVPN User Authentication Successful

이벤트 ID	이벤트 이름
716039	WebVPN User Authentication Rejected
716040	WebVPN User logging denied
716041	WebVPN ACL hit count
716042	WebVPN ACL hit
716043	WebVPN Port forwarding
716044	WebVPN Bad Parameter
716045	WebVPN Invalid Parameter
716046	WebVPN connection terminated
716047	WebVPN ACL usage
716048	WebVPN memory issue
716049	WebVPN Empty SVC ACL
716050	WebVPN ACL error
716051	WebVPN ACL error
716052	WebVPN Session Terminated
716053	WebVPN SSO Server added
716054	WebVPN SSO Server deleted
716055	WebVPN Authentication Successful
716056	WebVPN Authentication Failed
716057	WebVPN Session terminated
716058	WebVPN Session lost
716059	WebVPN Session resumed
716060	WebVPN Session Terminated
722001	WebVPN SVC Connect request error
722002	WebVPN SVC Connect request error
722003	WebVPN SVC Connect request error
722004	WebVPN SVC Connect request error
722005	WebVPN SVC Connect update issue
722006	WebVPN SVC Invalid address
722007	WebVPN SVC Message
722008	WebVPN SVC Message
722009	WebVPN SVC Message
722010	WebVPN SVC Message

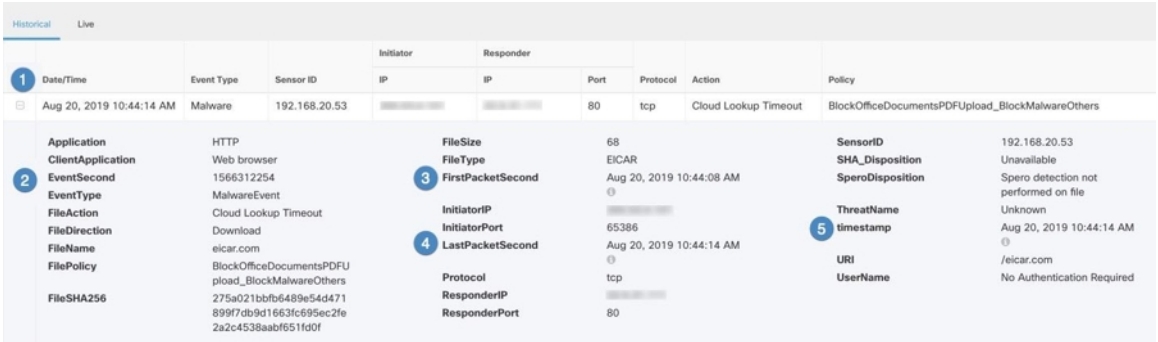
이벤트 **ID**	이벤트 이름
722011	WebVPN SVC Message
722012	WebVPN SVC Message
722013	WebVPN SVC Message
722014	WebVPN SVC Message
722015	WebVPN SVC invalid frame
722016	WebVPN SVC invalid frame
722017	WebVPN SVC invalid frame
722018	WebVPN SVC invalid frame
722019	WebVPN SVC Not Enough Data
722020	WebVPN SVC no address
722021	WebVPN Memory issue
722022	WebVPN SVC connection established
722023	WebVPN SVC connection terminated
722024	WebVPN Compression Enabled
722025	WebVPN Compression Disabled
722026	WebVPN Compression reset
722027	WebVPN Decompression reset
722028	WebVPN Connection Closed
722029	WebVPN SVC Session terminated
722030	WebVPN SVC Session terminated
722031	WebVPN SVC Session terminated
722032	WebVPN SVC connection Replacement
722033	WebVPN SVC Connection established
722034	WebVPN SVC New connection
722035	WebVPN Received Large packet
722036	WebVPN transmitting Large packet
722037.	WebVPN SVC connection closed
722038	WebVPN SVC session terminated
722039	WebVPN SVC invalid ACL
722040	WebVPN SVC invalid ACL
722041	WebVPN SVC IPv6 not available
722042	WebVPN invalid protocol

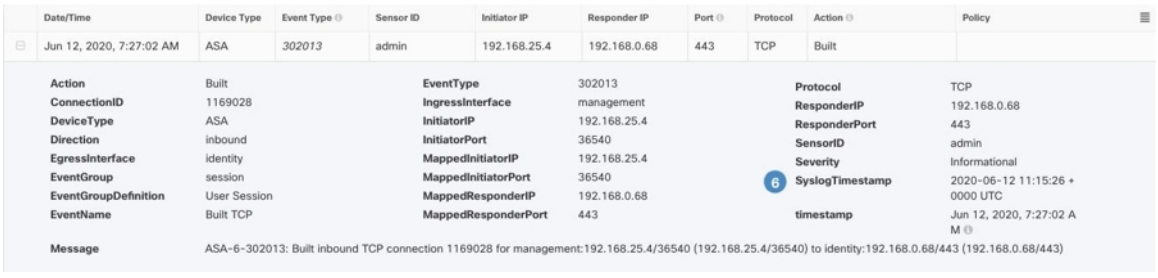
이벤트 **ID**	이벤트 이름
722043	WebVPN DTLS disabled
722044	WebVPN unable to request address
722045	WebVPN Connection terminated
722046	WebVPN Session terminated
722047	WebVPN Tunnel terminated
722048	WebVPN Tunnel terminated
722049	WebVPN Session terminated
722050	WebVPN Session terminated
722051	WebVPN address assigned
722053	WebVPN Unknown client
723001	WebVPN Citrix connection Up
723002	WebVPN Citrix connection Down
723003	WebVPN Citrix no memory issue
723004	WebVPN Citrix bad flow control
723005	WebVPN Citrix no channel
723006	WebVPN Citrix SOCKS error
723007	WebVPN Citrix connection list broken
723008	WebVPN Citrix invalid SOCKS
723009	WebVPN Citrix invalid connection
723010	WebVPN Citrix invalid connection
723011	WebVPN citrix Bad SOCKS
723012	WebVPN Citrix Bad SOCKS
723013	WebVPN Citrix invalid connection
723014	WebVPN Citrix connected to Server
724001	WebVPN Session not allowed
724002	WebVPN Session terminated
724003	WebVPN CSD
724004	WebVPN CSD
725001	SSL handshake Started
725002	SSL Handshake completed
725003	SSL Client session resume
725004	SSL Client request Authentication

이벤트 **ID**	이벤트 이름
725005	SSL Server request authentication
725006	SSL Handshake failed
725007	SSL Session terminated
725008	SSL Client Cipher
725009	SSL Server Cipher
725010	SSL Cipher
725011	SSL Device choose Cipher
725012	SSL Device choose Cipher
725013	SSL Server choose cipher
725014.	SSL LIB error
725015	SSL client certificate failed

시스템 로그 이벤트의 시간 속성

Event Logging(이벤트 로깅) 페이지에서 다양한 타임스탬프의 목적을 이해하면 원하는 이벤트를 필터링하고 찾을 수 있습니다.





번호	라벨	설명
1	날짜/시간	SEC(Secure Event Connector)가 이벤트를 처리한 시간. 방화벽이 해당 트래픽을 검사한 시간과 다를 수 있습니다. 타임스탬프와 동일한 값입니다.
2	EventSecond	LastPacketSecond와 같음.
3	FirstPacketSecond	연결이 열린 시간입니다. 이때 방화벽은 패킷을 검사합니다. FirstPacketSecond의 값은 LastPacketSecond에서 ConnectionDuration을 빼서 계산됩니다. 연결 시작 시 로깅된 연결 이벤트의 경우 FirstPacketSecond, LastPacketSecond 및 EventSecond 값은 모두 동일합니다.
4	LastPacketSecond	연결이 닫힌 시간입니다. 연결 종료 시 로깅된 연결 이벤트의 경우, LastPacketSecond 및 EventSecond는 동일합니다.
5	timestamp	SEC(Secure Event Connector)가 이벤트를 처리한 시간. 방화벽이 해당 트래픽을 검사한 시간과 다를 수 있습니다. 날짜/시간과 동일한 값입니다.
6	시스템 로그 타임스탬프	'logging timestamp'가 사용되는 경우 시스템 로그가 시작된 시간을 나타냅니다. 시스템 로그에 이 정보가 없으면 SEC가 이벤트를 수신한 시간이 반영됩니다.

번호	라벨	설명
7	NetflowTimeStamp	ASA에서 NetFlow 패킷을 채운 다음 플로우 컬렉터로 전송할 충분한 플로우 레코드/이벤트 수집을 완료한 시간입니다.

Cisco Secure Cloud Analytics 및 동적 엔티티 모델링

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Secure Cloud Analytics는 온프레미스 및 클라우드 기반 네트워크 구축을 모니터링하는 SaaS(Software as a Service) 솔루션입니다. 방화벽 이벤트 및 네트워크 플로우 데이터를 비롯한 소스에서 네트워크 트래픽에 대한 정보를 수집하여 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. Secure Cloud Analytics는 Talos와 같은 위협 인텔리전스의 다른 소스와 결합된 이 정보를 사용하여 본질적으로 악의적인 행동이 있음을 나타내는 경고를 생성합니다. 알림과 함께 Secure Cloud Analytics는 알림을 조사하고 악의적인 동작의 소스를 찾기 위한 더 나은 기반을 제공하기 위해 수집한 네트워크 및 호스트 가시성 및 상황 정보를 제공합니다.

동적 엔티티 모델링

동적 엔티티 모델링은 방화벽 이벤트 및 네트워크 플로우 데이터에 대한 동작 분석을 수행하여 네트워크의 상태를 추적합니다. Secure Cloud Analytics의 컨텍스트에서 엔티티는 네트워크의 호스트 또는 엔드포인트와 같이 시간이 지남에 따라 추적할 수 있는 항목입니다. 동적 엔터티 모델링은 전송하는 트래픽 및 네트워크에서 수행하는 활동을 기반으로 엔터티에 대한 정보를 수집합니다. **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 라이선스와 통합된 Secure Cloud Analytics는 엔티티가 일반적으로 전송하는 트래픽 유형을 확인하기 위해 방화벽 이벤트 및 기타 트래픽 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매한 경우 Secure Cloud Analytics는 엔티티 트래픽 모델링에 NetFlow 및 기타 트래픽 정보도 포함할 수 있습니다. Secure Cloud Analytics는 각 엔터티의 최신 모델을 유지하기 위해 엔터티가 계속해서 트래픽을 전송하고 잠재적으로 다른 트래픽을 전송하므로 시간이 지남에 따라 이러한 모델을 업데이트합니다. 이 정보에서 Secure Cloud Analytics는 다음을 식별합니다.

- 엔티티의 역할 - 엔티티가 일반적으로 수행하는 작업을 설명합니다. 예를 들어 엔티티가 일반적으로 이메일 서버와 연결된 트래픽을 전송하는 경우, Secure Cloud Analytics는 엔티티를 이메일 서버 역할로 할당합니다. 엔터티는 여러 역할을 수행할 수 있으므로 역할/엔티티 관계는 다대일일 수 있습니다.
- 엔티티에 대한 관찰 - 외부 IP 주소와의 하트비트 연결 또는 다른 엔티티와 설정된 원격 액세스 세션과 같이 네트워크에서의 엔티티 동작에 대한 팩트입니다. CDO와 통합하는 경우 방화벽 이벤트에서 이러한 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스도 구매한 경우, 시스템은 NetFlow에서 팩트를 가져오고 방화벽 이벤트와 NetFlow 모두에서 관찰을 생성할 수 있습니다. 관찰 자체는 관찰이 나타내는 것 이상의 의미를 전달하지 않습니다. 일반적인 고객은 수천 개의 관찰 및 몇 가지 알림을 가질 수 있습니다.

알림 및 분석

역할, 관찰 및 기타 위협 인텔리전스의 조합을 기반으로 Secure Cloud Analytics는 시스템에서 식별한 가능한 악의적인 행동을 나타내는 실행 가능한 항목인 알림을 생성합니다. 하나의 알림이 여러 관찰을 나타낼 수 있습니다. 방화벽이 동일한 연결 및 엔터티와 관련된 여러 연결 이벤트를 로깅하는 경우 하나의 알림만 생성될 수 있습니다.

예를 들어, 새 내부 디바이스 관찰 자체는 악의적인 행동을 구성하지 않습니다. 그러나 시간이 지남에 따라 엔티티가 도메인 컨트롤러와 일치하는 트래픽을 전송하면 시스템은 해당 엔티티에 도메인 컨트롤러 역할을 할당합니다. 이후에 엔티티가 비정상적인 포트를 사용하여 이전에 연결을 설정하지 않은 외부 서버에 연결하고 대량의 데이터를 전송하는 경우, 시스템은 새로운 대규모 연결(외부) 관찰 및 예외적인 도메인 컨트롤러 관찰을 로깅합니다. 해당 외부 서버가 Talos 감시 목록에 있는 것으로 식별된 경우, 이 모든 정보의 조합으로 인해 Secure Cloud Analytics가 이 엔티티의 동작에 대한 알림을 생성하고, 악성 동작을 조사하고 교정하기 위한 추가 작업을 수행하라는 메시지가 표시됩니다.

Secure Cloud Analytics 웹 포털 UI에서 알림을 열면 시스템이 알림을 생성하도록 유도한 지원 관찰을 볼 수 있습니다. 이러한 관찰을 통해 관련 엔터티에 대한 추가 컨텍스트(전송한 트래픽 포함) 및 외부 위협 인텔리전스(사용 가능한 경우)도 볼 수 있습니다. 또한 엔티티가 관련된 다른 관찰 및 알림을 보고 이 동작이 다른 잠재적인 악의적인 동작과 관련이 있는지 확인할 수 있습니다.

Secure Cloud Analytics에서 알림을 보고 닫을 때는 Secure Cloud Analytics UI의 트래픽을 허용하거나 차단할 수 없습니다. 디바이스를 액티브 모드로 구축한 경우에는 트래픽을 허용하거나 차단하도록 방화벽 액세스 제어 규칙을 업데이트하고, 패시브 모드에서 디바이스를 구축한 경우에는 방화벽 액세스 제어 규칙을 업데이트해야 합니다.

방화벽 이벤트 기반 알림 작업

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

알림 워크플로우

알림의 워크플로우는 상태를 기반으로 합니다. 시스템에서 알림을 생성할 때 기본 상태는 Open(열림)이며 사용자가 할당되지 않습니다. Alerts(알림) 요약을 볼 때 즉시 문제가 되는 모든 열린 알림이 기본적으로 표시됩니다.

참고: **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 알림은 NetFlow에서 생성된 관찰, 방화벽 이벤트에서 생성된 관찰 또는 두 데이터 소스의 관찰을 기반으로 할 수 있습니다.

알림 요약을 검토할 때 알림에 대한 상태를 초기 분류로 할당, 태그 지정 및 업데이트할 수 있습니다. 필터 및 검색 기능을 사용하여 특정 알림을 찾거나, 다른 상태의 알림을 표시하거나, 다른 태그 또는 담당자와 연결할 수 있습니다. 알림의 상태를 스누즈로 설정할 수 있습니다. 이 경우 스누즈 기간이 경과할 때까지 미해결 알림 목록에 다시 나타나지 않습니다. 알림에서 스누즈 상태를 제거하여 미해결 알림으로 다시 표시할 수도 있습니다. 알림을 검토할 때 자신 또는 시스템의 다른 사용자에게 할당할 수 있습니다. 사용자는 사용자 이름에 할당된 모든 알림을 검색할 수 있습니다.

Alerts(알림) 요약에서 알림 상세정보 페이지를 볼 수 있습니다. 이 페이지에서는 이 알림을 생성한 지원 관찰에 대한 추가 컨텍스트 및 이 알림과 관련된 엔터티에 대한 추가 컨텍스트를 검토할 수 있습

니다. 이 정보는 네트워크에서 문제를 추가로 조사하고 잠재적으로 악의적인 동작을 해결하기 위해 실제 문제를 정확히 찾아내는 데 도움이 될 수 있습니다.

Stealthwatch Cloud 웹 포털 UI, CDO 및 네트워크에서 조사할 때 결과를 설명하는 알림과 함께 코멘트를 남길 수 있습니다. 이렇게 하면 나중에 참조할 수 있는 연구 기록을 만드는 데 도움이 됩니다.

분석을 완료한 경우 상태를 Closed(닫힘)로 업데이트하고 더 이상 기본적으로 미결 알림으로 표시되지 않도록 할 수 있습니다. 상황이 바뀌면 나중에 닫힌 알림을 다시 열 수도 있습니다.

다음은 지정된 알림을 조사하는 방법에 대한 일반적인 지침 및 제안 사항입니다. Stealthwatch Cloud는 알림을 로깅할 때 추가 컨텍스트를 제공하므로 이 컨텍스트를 조사에 활용할 수 있습니다.

이러한 단계는 포괄적이거나 모든 것을 포함하지 않습니다. 이는 알림 조사를 시작하는 데 사용할 수 있는 일반적인 프레임워크를 제공할 뿐입니다.

일반적으로 알림을 검토할 때 다음 단계를 수행할 수 있습니다.

1. 열린 알림 분류, on page 44
2. 나중에 분석하기 위해 알림 일시 중지, on page 45
3. 추가 조사를 위해 알림 업데이트, on page 46
4. 알림 검토 및 조사 시작, on page 46
5. 엔터티 및 사용자 검사, on page 48
6. Secure Cloud Analytics를 사용하여 문제 해결, on page 48
7. 알림 업데이트 및 닫기, on page 49

열린 알림 분류

특히 둘 이상의 알림이 아직 조사되지 않은 경우, 미해결 알림을 분류합니다.

- CDO에서 SWC로 교차 실행하고 알림을 보는 방법에 대한 자세한 내용은 CDO에서 Cisco Secure Cloud Analytics 알림 보기을 참조하십시오.

다음 질문을 합니다.

- 이 알림 유형을 높은 우선순위로 구성했습니까?
- 영향을 받는 서브넷에 대해 높은 감도를 설정했습니까?
- 네트워크의 새 엔터티에서 발생하는 비정상적인 동작입니까?
- 엔터티의 일반적인 역할은 무엇이며 이 알림의 동작이 해당 역할과 어떻게 일치합니까?
- 이 엔터티의 정상적인 동작에서 예외적으로 벗어났습니다.
- 사용자가 관련된 경우, 이는 사용자의 예상된 동작입니까, 아니면 예외적인 것입니까?
- 보호되거나 민감한 데이터가 손상될 위험이 있습니까?
- 이 동작이 계속 허용되는 경우 네트워크에 미치는 영향은 어느 정도입니까?

- 외부 엔터티와 통신하는 경우, 이러한 엔터티가 과거에 네트워크의 다른 엔터티와 연결을 설정했습니까?

우선순위가 높은 알림인 경우 조사를 계속하기 전에 인터넷에서 엔티티를 격리하거나 연결을 닫는 것을 고려하십시오.

나중에 분석하기 위해 알림 일시 중지

다른 알림에 비해 우선 순위가 낮은 알림을 스누즈합니다. 예를 들어 조직에서 이메일 서버를 FTP 서버로 용도를 변경하고 시스템에서 긴급 프로파일 알림(엔티티의 현재 트래픽이 이전에 일치하지 않았던 행동 프로파일과 일치함을 나타냄)을 생성하는 경우 이 알림을 나중에 다시 확인할 수 있습니다. 스누즈된 알림은 열린 알림과 함께 표시되지 않습니다. 이러한 스누즈된 알림을 검토하려면 특별히 필터링해야 합니다.

알림 스누즈:

Procedure

단계 **1** **Close Alert(**알림 닫기**)**를 클릭합니다.

단계 **2** Snooze this alert(이 알림 스누즈) 창의 드롭다운에서 스누즈 기간을 선택합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

What to do next

이러한 알림을 검토할 준비가 되면 다시 알림을 해제할 수 있습니다. 이렇게 하면 상태가 Open(열림)으로 설정되고 다른 Open(열림) 알림과 함께 알림이 표시됩니다.

스누즈된 알림의 스누즈를 해제합니다.

- 스누즈된 알림에서 **Unsnooze Alert(**알림 스누즈 해제**)**를 클릭합니다.

추가 조사를 위해 알림 업데이트

알림 세부 정보를 엽니다.

Procedure

단계 **1** **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.

단계 **2** 알림 유형 이름을 클릭합니다.

What to do next

초기 분류 및 우선순위에 따라 알림을 할당하고 태그를 지정합니다.

1. **Assignee(**담당자**)** 드롭다운에서 사용자를 선택하여 알림을 할당하면 사용자가 조사를 시작할 수 있습니다.
2. 드롭다운에서 하나 이상의 **Tags(**태그**)**를 선택하여 알림에 태그를 추가하여 향후 식별을 위해 알림을 더 잘 분류하고 알림에서 장기적 패턴을 설정합니다.
3. 이 알림에 대한 코멘트를 입력한 다음 **Comment(**코멘트**)**를 클릭하여 초기 결과를 추적하고 알림에 할당된 사람을 지원하는 데 필요한 코멘트를 남깁니다. 알림은 시스템 코멘트와 사용자 코멘트를 모두 추적합니다.

알림 검토 및 조사 시작

할당된 알림을 검토하는 경우 알림 세부 정보를 검토하여 Stealthwatch Cloud에서 알림을 생성한 이유를 파악합니다. 지원 관찰을 검토하여 이러한 관찰이 소스 엔터티에 미치는 영향을 파악합니다.

경고가 방화벽 이벤트를 기반으로 생성된 경우, 시스템은 방화벽 구축이 이 경고의 소스임을 인식하지 않습니다.

이 소스 엔터티에 대한 모든 지원 관찰을 확인하여 일반 동작 및 패턴을 파악하고 이 활동이 더 긴 추세의 일부일 수 있는지 확인합니다.

프로시저

단계 **1** 알림 세부사항에서 관찰 유형 옆에 있는 화살표 아이콘(➔)을 클릭하여 해당 유형의 모든 로깅된 관찰을 확인합니다.

단계 **2** **All Observations for Network(**네트워크에 대한 모든 관찰**)** 옆에 있는 화살표 아이콘(➔)을 클릭하여 이 알림의 소스 엔티티에 대해 로깅된 모든 관찰을 확인합니다.

이러한 관찰에 대한 추가 분석을 수행하려면 쉼표로 구분된 값 파일로 지원 관찰을 다운로드합니다.

- 알림 세부 정보의 Supporting Observations(지원 관찰) 창에서 **CSV**를 클릭합니다.

관찰 결과에서 소스 엔터티 동작이 악의적인 동작을 나타내는지 확인합니다. 소스 엔터티가 여러 외부 엔터티와의 연결을 설정한 경우, 외부 엔터티가 어떤 식으로든 관련이 있는지 확인합니다(예: 모든 엔터티가 유사한 지리위치 정보를 가지고 있거나 해당 IP 주소가 동일한 서브넷에 있는지 여부).

소스 엔터티 IP 주소 또는 호스트 이름에서 소스 엔터티와 관련된 추가 컨텍스트를 확인합니다. 여기에는 관련될 수 있는 기타 알림 및 관찰, 디바이스 자체에 대한 정보, 전송 중인 세션 트래픽 유형이 포함됩니다.

- 엔티티와 관련된 모든 알림을 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Alerts(**알림**)**를 선택합니다.
- IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Observations(**관찰**)**를 선택하여 엔티티와 관련된 모든 관찰을 확인합니다.
- 디바이스에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Device(**디바이스**)**를 선택합니다.

- 이 엔터티와 관련된 세션 트래픽을 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic(**세션 트래픽**)**을 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy(**복사**)**를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 소스 엔티티는 항상 네트워크 내부에 있습니다. 이를 방화벽 이벤트의 Initiator IP(이니시에이터 IP)와 비교해 보십시오. 이 IP는 연결을 시작한 엔티티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

관찰에서 다른 외부 엔터티에 대한 정보를 검토합니다. 지리위치 정보를 검토하고 지리위치 데이터 또는 Umbrella 데이터가 악성 엔티티를 식별하는지 확인합니다. 이러한 엔터티에 의해 생성된 트래픽을 확인합니다. Talos, AbuseIPDB 또는 Google에 이러한 엔터티에 대한 정보가 있는지 확인합니다. 여러 날짜의 IP 주소를 찾고 외부 엔터티가 네트워크의 엔터티와 설정한 다른 유형의 연결을 확인합니다. 필요한 경우 이러한 내부 엔터티를 찾아 보안 침해 또는 의도하지 않은 행동의 증거가 있는지 확인합니다.

소스 엔티티가 연결을 설정한 외부 엔티티 IP 주소 또는 호스트 이름에 대한 컨텍스트를 검토합니다.

- 이 엔티티에 대한 최근 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **IP Traffic(IP** 트래픽**)**을 선택합니다.
- 이 엔티티에 대한 최근 세션 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic(**세션 트래픽**)**을 선택합니다.
- **AbuseIPDB**웹사이트에서 이 엔티티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 AbuseIPDB를 선택합니다.
- Cisco Umbrella 웹사이트에서 이 엔티티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Cisco Umbrella**를 선택합니다.
- Google에서 이 IP 주소를 검색하려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Google Search(Google** 검색**)**를 선택합니다.
- Talos 웹사이트에서 이 정보에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Talos Intelligence**를 선택합니다.
- IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Add IP to watchlist(**감시 목록에 **IP** 추가**)**를 선택하여 이 엔터티를 감시 목록에 추가합니다.
- 이 엔티티의 지난 달 트래픽을 검색하려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Find IP on multiple days(**여러 날짜의 **IP** 찾기**)**를 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy(**복사**)**를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 연결된 엔터티는 항상 네트워크 외부에 있습니다. 이를 방화벽 이벤트의 Responder IP(응답자 IP)와 비교해 보십시오. 이는 연결 요청에 응답한 엔티티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

엔터티 및 사용자 검사

Stealthwatch Cloud 포털 UI에서 알림을 검토한 후 소스 엔터티, 이 알림과 관련되었을 수 있는 사용자 및 기타 관련 엔터티에 대해 직접 추가 검사를 수행할 수 있습니다.

- 소스 엔터티가 물리적으로 또는 클라우드에서 네트워크의 어느 위치에 있는지 확인하고 직접 액세스합니다. 이 엔터티에 대한 로그 파일을 찾습니다. 네트워크의 물리적 엔티티인 경우 디바이스에 액세스하여 로그 정보를 검토하고 이 동작의 원인에 대한 정보가 있는지 확인합니다. 가상 엔터티이거나 클라우드에 저장된 경우 로그에 액세스하여 이 엔터티와 관련된 항목을 검색합니다. 무단 로그인, 승인되지 않은 구성 변경 등에 대한 자세한 내용은 로그를 검사합니다.
- 엔터티를 검사합니다. 엔터티 자체에서 악성코드 또는 취약성을 식별할 수 있는지 확인합니다. 조직에서 승인하지 않은 USB 스틱과 같이 디바이스에 대한 물리적 변경이 있는지를 포함하여 악의적인 변경이 있는지 확인합니다.
- 네트워크의 사용자 또는 네트워크 외부의 사용자가 관련되었는지 확인합니다. 가능한 경우 사용자에게 무엇을 하고 있었는지 물어봅니다. 사용자가 사용할 수 없는 경우, 액세스 권한이 있어야 했는지, 그리고 퇴사한 직원이 퇴사 전에 외부 서버에 파일을 업로드하는 등의 상황이 발생했는지 확인합니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

알림 업데이트 및 닫기

결과에 따라 태그를 추가합니다.

Procedure

단계 **1** Secure Cloud Analytics 포털 UI에서 **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.

단계 **2** 드롭다운에서 하나 이상의 **Tags(**태그**)**를 선택합니다.

조사 결과 및 수행한 교정 단계를 설명하는 최종 코멘트를 추가합니다.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

알림을 닫고 유용하거나 도움이 되지 않음으로 표시합니다.

1. 알림 세부 정보에서 **Close Alert(**알림 닫기**)**를 클릭합니다.
2. 알림이 도움이 되었으면 **Yes(**예**)**를 선택하고, 알림이 도움이 되지 않았다면 **No(**아니요**)**를 선택합니다. 이는 알림이 악의적인 행동으로 인해 발생했음을 의미하는 것이 아니라 해당 알림이 조직에 도움이 되었음을 의미합니다.

3. **Save(**저장**)**를 클릭합니다.

What to do next

종료된 알림 다시 열기

종료된 알림과 관련된 추가 정보를 발견하거나 알림과 관련된 코멘트를 더 추가하려는 경우 알림을 다시 열어 상태를 Open(열림)으로 변경할 수 있습니다. 그런 다음 필요에 따라 알림을 변경한 다음 추가 조사가 완료되면 알림을 닫을 수 있습니다.

종료된 알림을 다시 엽니다.

- 닫힌 알림의 세부 사항에서 **Reopen Alert(**알림 다시 열기**)**를 클릭합니다.

알림 우선순위 수정

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

알림 유형은 기본 우선순위와 함께 제공되며, 이는 시스템이 이 유형의 알림 생성에 대한 민감도에 영향을 미칩니다. 알림은 기본적으로 Cisco 인텔리전스 및 기타 요인에 따라 낮음 또는 보통으로 설정됩니다. 네트워크 환경에 따라 알림 유형의 우선순위를 다시 지정하여 우려되는 특정 알림을 강조할 수 있습니다. 모든 알림 유형을 낮음, 보통 또는 높음 우선순위로 구성할 수 있습니다.

- **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.
- Settings(설정) 드롭다운 아이콘(⚙)을 클릭한 다음 **Alert Types and Priorities(**알림 유형 및 우선순위**)**를 선택합니다.
- 알림 유형 옆에 있는 편집 아이콘(✎)을 클릭하고 낮음, 중간 또는 높음을 선택하여 우선순위를 변경합니다.

이벤트 로깅 페이지에서 이벤트 검색 및 필터링

특정 이벤트에 대한 기록 및 라이브 이벤트 테이블을 검색하고 필터링하는 것은 CDO에서 다른 정보를 검색하고 필터링할 때와 동일한 방식으로 작동합니다. 필터 기준을 추가하면 CDO가 Events(이벤트) 페이지에 표시되는 내용을 제한하기 시작합니다. 검색 필드에 검색 기준을 입력하여 특정 값의 이벤트를 찾을 수도 있습니다. 필터링 및 검색 메커니즘을 결합하는 경우, 검색은 이벤트를 필터링한 후 표시된 결과 중에서 입력한 값을 찾으려고 시도합니다.

다음은 이벤트 로그 검색을 수행하는 옵션입니다.

- 이벤트 로깅 페이지에서 이벤트 검색, 97 페이지
- 백그라운드에서 기록 이벤트 검색, 97 페이지

필터링은 라이브 이벤트를 시간 기준으로 필터링할 수 없다는 점을 제외하고 기록 이벤트와 동일한 방식으로 라이브 이벤트에 대해 작동합니다.

이러한 필터링 방법에 대해 알아보십시오.

라이브 또는 과거 이벤트 필터링

이 절차에서는 이벤트 필터링을 사용하여 Event Logging(이벤트 로깅) 페이지에서 이벤트의 하위 집합을 확인하는 방법을 설명합니다. 특정 필터 기준을 반복적으로 사용하는 경우 사용자 지정 필터를 생성하여 저장할 수 있습니다. 자세한 내용은 사용자 지정 가능한 이벤트 필터를 참조하십시오.

Procedure

단계 **1** 탐색 모음에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** Historical(기록) 또는 Live(라이브) 탭을 클릭합니다.

단계 **3** 필터 버튼를 클릭합니다. 필터링 열은 고정 아이콘을 클릭하여 열 수 있습니다.

단계 **4** 저장된 필터 요소가 없는 View(보기) 탭을 클릭합니다.

단계 **5** 필터링할 이벤트 세부 정보를 선택합니다.

- **FTD** 이벤트 유형
  - Connection(연결) - 액세스 제어 규칙의 연결 이벤트를 표시합니다.
  - File(파일) - 액세스 제어 규칙의 파일 정책에 의해 보고된 이벤트를 표시합니다.
  - Intrusion(침입) - 액세스 제어 규칙의 침입 정책에 의해 보고된 이벤트를 표시합니다.
  - Malware(악성코드) - 액세스 제어 규칙의 악성코드 정책에 의해 보고된 이벤트를 표시합니다.

  이러한 이벤트 유형에 대한 자세한 내용은 FDM-관리 이벤트 유형을 참조하십시오.
- ASA**Event Types(**이벤트 유형**)** -이러한 이벤트 유형은 Syslog 또는 NetFlow 이벤트의 그룹을 나타냅니다.
- **Time Range(**시간 범위**)** - 표시할 기간의 시작과 끝을 선택하려면 Start(시작) 또는 End(종료) 시간 필드를 클릭합니다. 타임스탬프는 컴퓨터의 로컬 시간으로 표시됩니다.
- **Action(**작업**)** - 규칙에 의해 정의된 보안 작업을 지정합니다. 입력하는 값은 찾으려는 값과 정확히 일치해야 합니다. 그러나 대/소문자는 중요하지 않습니다. 연결, 파일, 침입, 악성코드, Syslog 및 NetFlow 이벤트 유형에 대해 서로 다른 값을 입력합니다.

- 연결 이벤트 유형의 경우 필터는 AC_RuleAction 특성에서 일치 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.
- 파일 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.
- 침입 이벤트 유형의 경우 필터는 InLineResult 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allowed(허용됨), Blocked(차단됨), Trusted(신뢰할 수 있음)일 수 있습니다.
- 악성코드 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Cloud Lookup Timeout(클라우드 조회 시간 초과)일 수 있습니다.
- Syslog 및 NetFlow 이벤트 유형의 경우 필터는 Action(작업) 속성에서 일치하는 항목을 검색합니다.

- 센서 **ID** - 센서 ID는 이벤트가 보안 이벤트 커넥터로 전송되는 관리 IP 주소입니다.

  FDM 관리 디바이스의 경우 센서 ID는 일반적으로 디바이스 관리 인터페이스의 IP 주소입니다.

- **IP** 주소
  - 이니시에이터 - 네트워크 트래픽 소스의 IP 주소입니다. Initiator address(이니시에이터 주소) 필드의 값은 이벤트 세부사항의 InitiatorIP(이니시에이터 IP) 필드 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.
  - 응답자 - 패킷의 대상 IP 주소입니다. Destination address(대상 주소) 필드의 값은 이벤트 세부사항의 ResponderIP 필드에 있는 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.

- 포트
  - 이니시에이터-세션 이니시에이터가 사용하는 포트 또는 ICMP 유형입니다. 소스 포트의 값은 이벤트 세부 정보의 InitiatorPort 값에 해당합니다. (범위 추가 - 시작 포트 종료 포트 및 이니시에이터와 응답자 사이 또는 둘 다 사이에 공백)
  - **Reponder(**응답기**)-**세션 responder가 사용하는 포트 또는 ICMP 코드입니다. 대상 포트의 값은 이벤트 세부사항의 ResponderPort 값에 해당합니다.

단계 **6** (선택 사항) View(보기) 탭에서 클릭하여 필터를 사용자 지정 필터로 저장합니다.

NetFlow 이벤트만 필터링

이 절차에서는 ASA NetFlow 이벤트만 찾습니다.

Procedure

단계 **1** CDO 메뉴 모음에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** Filter(필터) 아이콘 을 클릭하고 필터를 열린 상태로 고정합니다.

단계 **3** **Netflow** ASA 이벤트 필터를 확인합니다.

단계 **4** 다른 모든 ASA 이벤트 필터를 지웁니다.

ASA NetFlow 이벤트만 Event Logging(이벤트 로깅) 테이블에 표시됩니다.

ASA 또는 FDM-관리 장치 syslog 이벤트에 대한 필터링(ASA NetFlow 이벤트 제외)

이 절차에서는 Syslog 이벤트만 찾습니다.

Procedure

단계 **1** CDO 메뉴 모음에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** Filter(필터) 아이콘 을 클릭하고 필터를 열린 상태로 고정합니다.

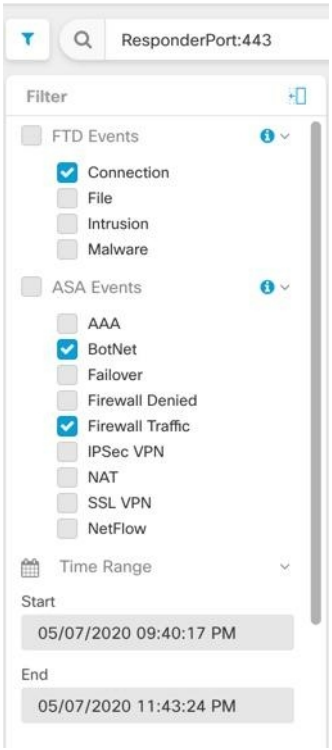
단계 **3** 필터 표시줄의 맨 아래로 스크롤하여 **Include NetFlow Events(NetFlow** 이벤트 포함**)** 필터가 선택 취소되었는지 확인합니다.

단계 **4** ASA Events(이벤트) 필터 트리로 다시 스크롤하여 **NetFlow** 상자가 선택 취소되었는지 확인합니다.

단계 **5** ASA 또는 FTD 필터 기준의 나머지를 선택합니다.

필터 요소 결합

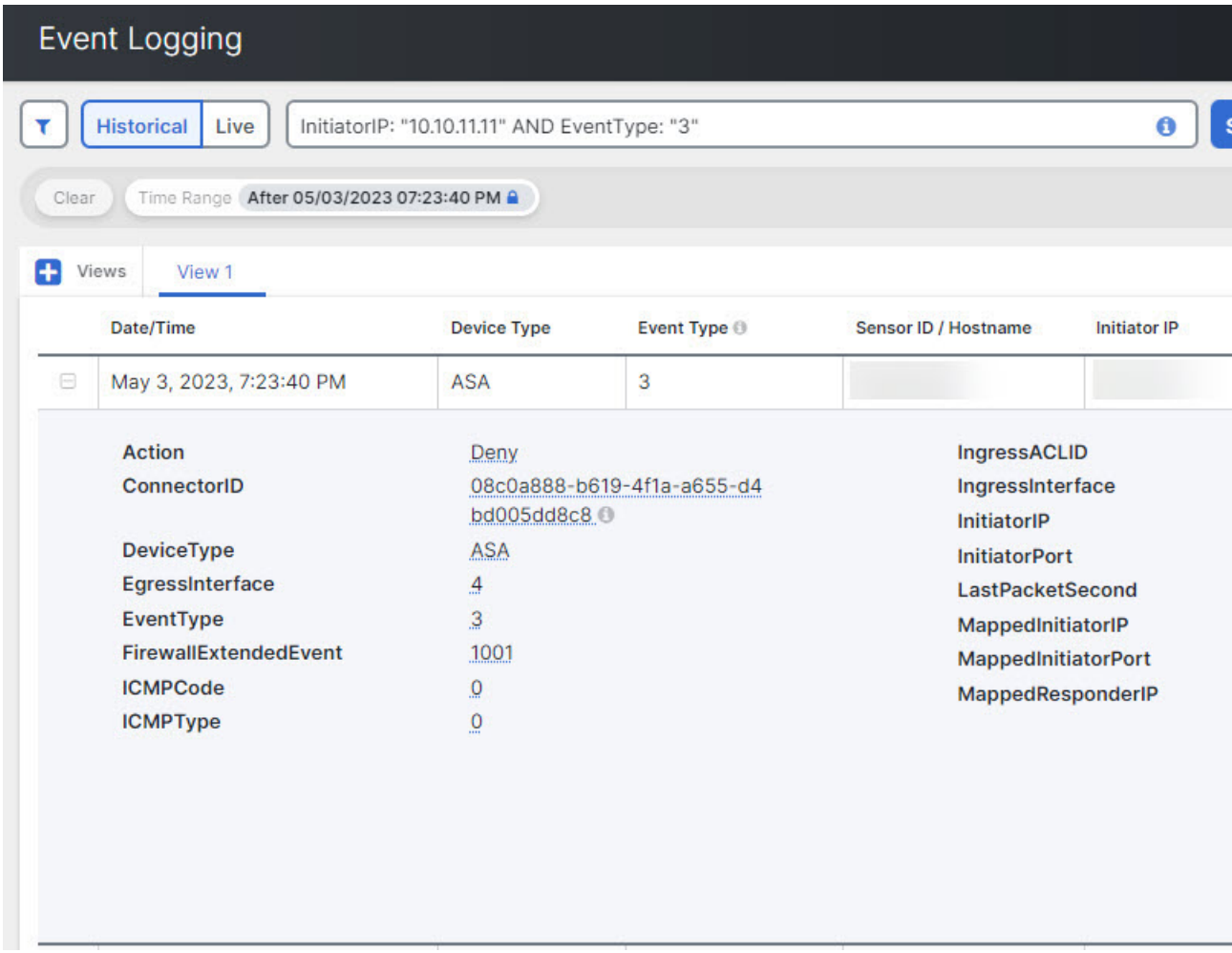
필터링 이벤트는 일반적으로 CDO의 표준 필터링 규칙을 따릅니다. 필터링 범주는 "AND"되고 범주 내의 값은 "OR"됩니다. 필터를 사용자 고유의 검색 기준과 결합할 수도 있습니다. 이벤트 필터의 경우 그러나 디바이스 이벤트 필터도 "OR"됩니다. 예를 들어 필터에서 다음 값을 선택한 경우,



이 필터를 사용하면 CDO는 위협 방어 디바이스 연결 이벤트 또는 ASA BotNet 또는 방화벽 트래픽 이벤트 및 시간 범위의 두 번 사이에 발생한 이벤트 및 ResponderPort 443도 포함하는 이벤트를 표시합니다. 시간 범위 내의 기록 이벤트를 기준으로 필터링할 수 있습니다. 라이브 이벤트 페이지에는 항상 최신 이벤트가 표시됩니다.

특정 속성: 값 쌍 검색

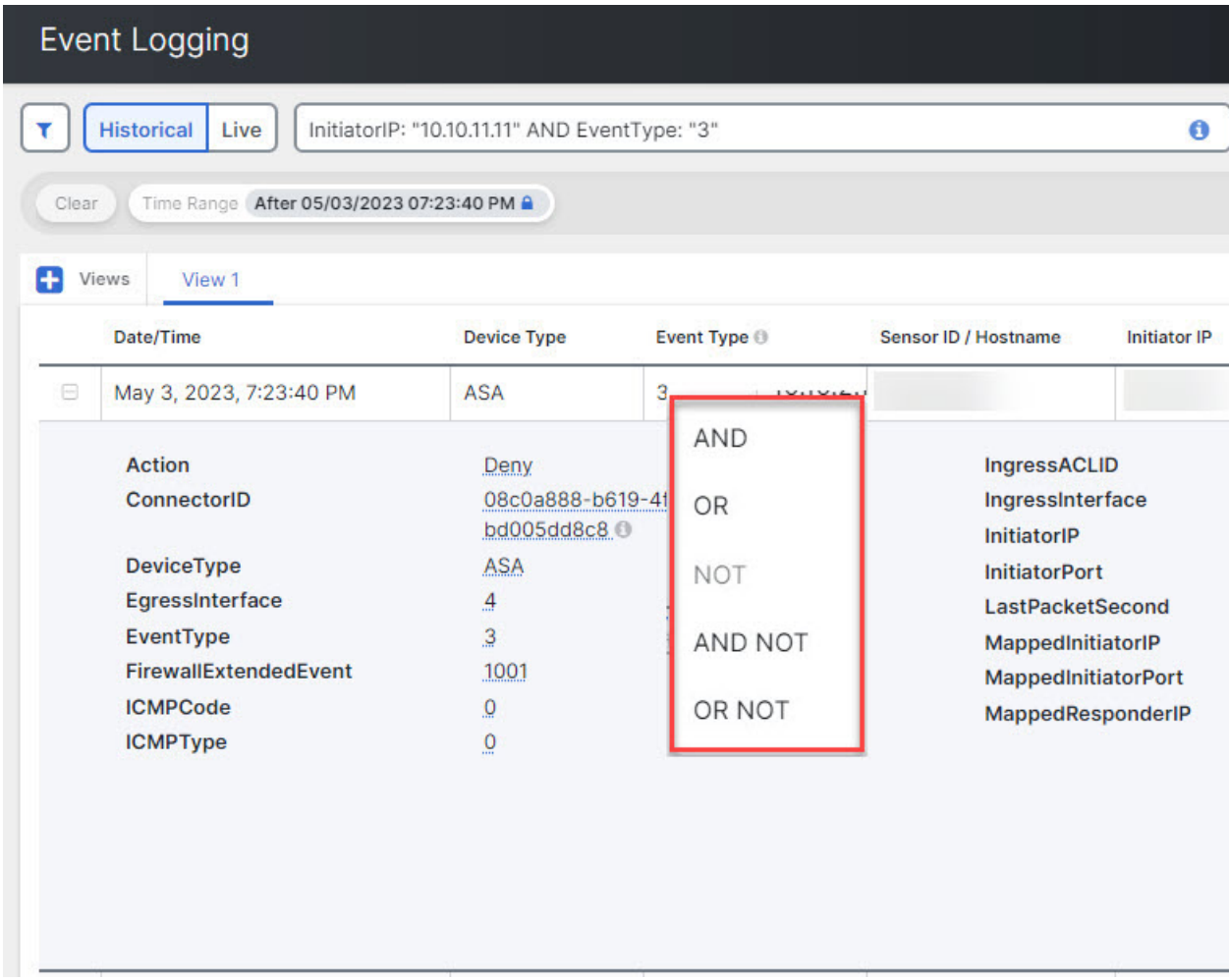
검색 필드에 이벤트 속성 및 값을 입력하여 라이브 또는 기록 이벤트를 검색할 수 있습니다. 이 작업을 수행하는 가장 쉬운 방법은 검색하려는 Event Logging(이벤트 로깅) 테이블의 속성을 클릭하는 것입니다. 그러면 CDO가 Search(검색) 필드에 해당 속성을 입력합니다. 롤오버하면 클릭할 수 있는 이벤트가 파란색으로 표시됩니다. 예를 들면 다음과 같습니다.



이 예에서는 InitiatorIP 값 10.10.11.11을 롤오버하고 이를 클릭하여 검색을 시작했습니다. 이니시에이터 IP 및 해당 값이 검색 문자열에 추가되었습니다. 다음으로, Event Type(이벤트 유형) 3를 클릭하여 검색 문자열에 추가하고 CDO에서 AND를 추가했습니다. 따라서 이 검색의 결과는 10.10.11.11에서 시작된 이벤트 및 3 이벤트 유형의 목록이 됩니다.

위의 예에서 값 3 옆에 돋보기가 있습니다. 돋보기를 롤오버하는 경우 AND, OR, AND NOT, OR NOT 연산자를 선택하여 검색에 추가할 값을 입력할 수도 있습니다.

아래 예에서는 "OR"가 선택되었습니다. 이 검색의 결과는 10.10.11.11에서 시작된 이벤트 또는 106023 이벤트 유형의 목록이 됩니다. 검색 필드가 비어 있고 테이블에서 값을 마우스 오른쪽 버튼으로 클릭하면 다른 값이 없으므로 NOT만 사용할 수 있습니다.



값을 롤오버하고 파란색으로 강조 표시되면 해당 값을 검색 문자열에 추가할 수 있습니다.

AND, OR, NOT, AND NOT, OR NOT 필터 연산자

검색 문자열에서 사용되는 "AND", "OR", "NOT", "AND NOT" 및 "OR NOT"의 동작은 다음과 같습니다.

AND

필터 문자열에서 AND 연산자를 사용하여 모든 특성을 포함하는 이벤트를 찾습니다. AND 연산자는 검색 문자열을 시작할 수 없습니다.

예를 들어 아래의 검색 문자열은 이니시에이터IP 주소 10.10.10.43에서 시작되고 이니시에이터 포트 59614에서 전송된 TCP 프로토콜 AND를 포함하는 이벤트를 검색합니다. 각 추가 AND 문을 사용하여 기준을 충족하는 이벤트의 수가 점점 더 적을 것으로 예상됩니다.

```
Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"
```

또는

필터 문자열에서 OR 연산자를 사용하여 특성을 포함하는 이벤트를 찾습니다. OR 연산자는 검색 문자열을 시작할 수 없습니다.

예를 들어 아래의 검색 문자열은 TCP 프로토콜을 포함하는 이벤트를 포함하는 이벤트, 또는 이니시에이터 IP 주소 10.10.10.43에서 시작된 또는 이니시에이터 포트 59614에서 전송된 이벤트를 표시합니다. 각 추가 OR 문에서 기준을 충족하는 이벤트의 수가 점점 더 커질 것으로 예상됩니다.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

NOT

특정 속성이 있는 이벤트를 제외하려면 검색 문자열의 시작 부분에만 이를 사용하십시오. 예를 들어 이 검색 문자열은 InitiatorIP 192.168.25.3인 이벤트를 결과에서 제외합니다.

```
 NOT InitiatorIP: "192.168.25.3"
```

AND NOT

특정 특성을 포함하는 이벤트를 제외하려면 필터 문자열에서 AND NOT 연산자를 사용합니다. AND NOT은 검색 문자열의 시작 부분에 사용할 수 없습니다.

예를 들어 이 필터 문자열은 InitiatorIP 192.168.25.3인 이벤트를 표시하지만 ResponderIP 주소가 10.10.10.1인 이벤트는 표시하지 않습니다.

```
 InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

NOT과 AND NOT을 조합하여 여러 속성을 제외할 수도 있습니다. 예를 들어 이 필터 문자열은 InitiatorIP 192.168.25.3의 이벤트 및 ResponderIP 10.10.10.1의 이벤트를 제외합니다.

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

OR NOT

특정 요소를 제외하는 검색 결과를 포함하려면 OR NOT 연산자를 사용합니다. OR NOT 연산자는 검색 문자열의 시작 부분에 사용할 수 없습니다.

예를 들어 이 검색 문자열은 프로토콜이 TCP인 이벤트 또는 InitiatorIP가 10.10.10.43인 이벤트 또는 InitiatorPort 59614가 아닌 이벤트를 찾습니다.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

(프로토콜: "tcp") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614")를 검색할 수도 있습니다.

와일드카드 검색

이벤트 내에서 결과를 찾으려면 **attribute:value** 검색의 value 필드에서 와일드카드를 나타내려면 별표(*)를 사용합니다. 예를 들어, 이 필터 문자열

```
 URL:*feedback*
```

은 문자열 **feedback**을 포함하는 이벤트의 URL 특성 필드에서 문자열을 찾습니다.

관련 정보**:**

- 이벤트 로깅 페이지의 열 표시 및 숨기기
- Security Analytics and Logging의 이벤트 속성

백그라운드에서 기록 이벤트 검색

CDO는 검색 기준을 정의하고 정의된 검색 기준에 따라 이벤트 로그를 검색하는 기능을 제공합니다. 백그라운드 검색 기능을 사용하여 백그라운드에서 이벤트 로그 검색을 수행하고 백그라운드 검색이 완료되면 검색 결과를 볼 수도 있습니다.

구성한 구독 알림 및 서비스 통합을 기반으로 백그라운드 검색이 완료되면 알림을 받습니다.

백그라운드 검색 페이지에서 직접 검색 결과를 보거나 다운로드하거나 삭제할 수 있습니다. 또한 백그라운드 검색이 일회성 이벤트에 대해 실행되도록 예약하거나 반복 일정을 예약할 수도 있습니다. 알림 설정 페이지로 이동하여 구독 옵션을 보거나 수정합니다.

이벤트 로깅 페이지에서 이벤트 검색

검색 및 백그라운드 검색 기능을 사용하여 Event Logging(이벤트 로깅) 페이지에서 로깅된 모든 이벤트를 볼 수 있습니다. 백그라운드 검색은 기록 이벤트에 대해서만 수행할 수 있습니다.

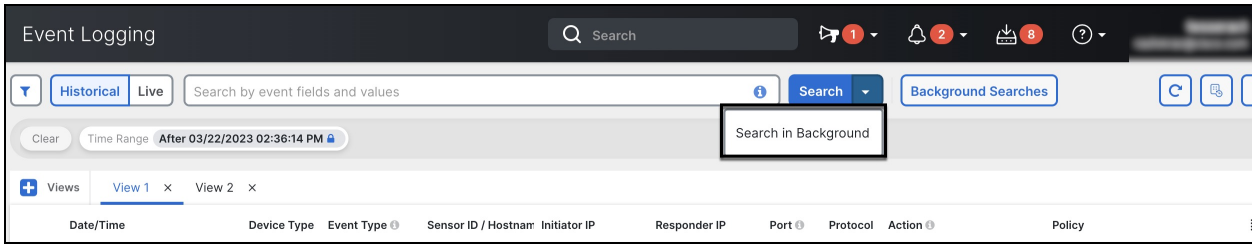
프로시저

단계 **1** 탐색 모음에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** **Historical(**기록**)** 또는 **Live(**라이브**)** 탭을 클릭합니다.

단계 **3** 내비게이션 창으로 이동하여 검색식을 입력하고 **Search(**검색**)** 버튼을 입력하여 검색을 실행합니다. 절대 시간 범위 또는 상대 시간 범위를 사용하여 검색을 좁히거나 확장할 수 있습니다.

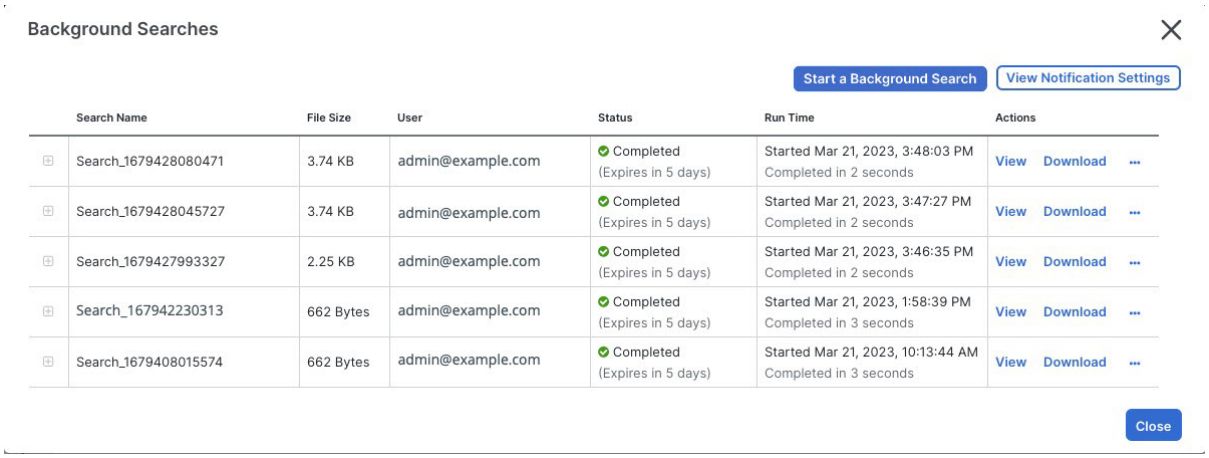
또는 **Search(**검색**)** 드롭다운 목록에서 **Search in Background(**백그라운드에서 검색**)**를 선택하여 검색 페이지에서 벗어나 있는 동안 백그라운드에서 검색을 실행합니다. 검색 결과가 준비되면 알림이 표시됩니다.



Search(검색**)** 버튼을 클릭하면 결과가 Event Logging(이벤트 로깅) 보기에 직접 나타납니다. 특정 검색 결과를 선택하면 쉽게 참조할 수 있도록 검색 기준이 검색 창에 나타납니다.

백그라운드에서 검색을 실행하도록 선택하면 검색 작업이 대기열에 추가되고 검색이 완료되면 알림이 표시됩니다. 백그라운드에서 여러 검색 쿼리를 실행할 수 있습니다.

단계 **4** **Background Searches(**백그라운드 검색**)** 버튼을 클릭하여 Background Searches(백그라운드 검색) 페이지를 봅니다.



Background Searches(백그라운드 검색) 페이지에 검색 결과 목록이 표시됩니다. 검색 결과를 보거나, 다운로드하거나, 삭제할 수 있습니다. 알림 설정 페이지로 이동하여 구독 옵션을 보거나 편집할 수도 있습니다. 이 페이지에서 검색을 시작하려면 **Start a Background Search(**백그라운드 검색 시작**)** 버튼을 선택합니다.

구독 옵션을 보거나 수정하는 방법에 대한 정보는 알림 설정을 참조하십시오.

다음에 수행할 작업

반복 쿼리가 필요한 경우, 모든 백그라운드 검색을 예약된 백그라운드 검색으로 전환할 수 있습니다. 자세한 내용은 이벤트 뷰어에서 백그라운드 검색 예약, 98 페이지를 참조하십시오.

이벤트 뷰어에서 백그라운드 검색 예약

이벤트 뷰어 페이지에서 백그라운드에서 반복 쿼리를 예약합니다. 검색은 기록 이벤트에 대해서만 예약할 수 있습니다. 예약된 검색은 언제든지 수정하거나 취소할 수 있습니다. 기존 쿼리를 반복 검색으로 수정할 수도 있습니다.

참고 시작, 완료 또는 실패한 검색에 대한 알림을 수신하도록 선택할 수 있습니다. 자세한 내용은 알림 설정를 참조하십시오.

기록 이벤트에 대해서만 백그라운드 검색을 예약할 수 있습니다. 예약 백그라운드 검색을 생성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 탐색 모음에서 **Analytics(**애널리틱스**)** > **Event Logging(**이벤트 로깅**)**를 선택합니다.

단계 **2** **Historical(**기록**)** 토글을 클릭하여 선택합니다. 기록 이벤트에 대한 백그라운드 검색만 예약할 수 있습니다.

단계 **3** 검색창에 검색하려는 검색 표현식을 입력합니다. **Search(**검색**)** 드롭다운 버튼을 클릭하고 **Search in background(**백그라운드에서 검색**)**를 선택합니다.

단계 **4** (선택 사항) 검색 이름을 변경합니다.

단계 **5** 기본적으로 **Search Now(**지금 검색**)** 확인란이 선택되어 있습니다. 선택된 경우, 저장 시 검색이 시작됩니다. 이 확인란을 선택하지 않으면 백그라운드 쿼리가 향후 검색으로서만 실행됩니다.

단계 **6** **Setup recurring schedule(**설정 반복 예약**)**을 확인하고 다음 설정을 구성합니다.

- **Search Logs for the Last(**마지막 검색 로그**) -** 얼마나 이전까지 검색하고자 하는지입니다.
- **Frequency(**빈도**) -** 예약 검색을 얼마나 자주 수행할지 선택합니다.

단계 **7** 창 하단에서 예약된 검색 기준을 확인합니다. **Schedule and Search Now(**지금 예약 및 검색**)**를 선택합니다. 또는 즉시 검색을 시작하도록 선택하지 않은 경우 버튼이 **Schedule Search(**검색 예약**)**로 표시됩니다.

다음에 수행할 작업

예약된 백그라운드 검색의 결과는 CDO에서 자동으로 삭제하기 전 최대 7일 동안 검토할 수 있습니다.

백그라운드 검색 다운로드

검색 결과 및 일정 쿼리는 CDO가 자동으로 제거하기 전까지 7일 동안 저장됩니다. 과거 이벤트에 대해 수행된 백그라운드 검색의 CSV 복사본을 다운로드합니다.

프로시저

단계 **1** 내비게이션 바에서 **Analytics(**분석**)** > **Event Logging(**이벤트 로깅**)**으로 이동합니다.

단계 **2** **Background Searches(**백그라운드 검색**)** > **Actions(**작업**)** > **Download(**다운로드**)**를 클릭합니다.

단계 **3** 검색을 찾습니다. 예약된 검색은 **Queries(**쿼리**)** 탭에 저장됩니다.

단계 **4** **Download(**다운로드**)**를 클릭합니다. .CSV 파일은 로컬 드라이브의 기본 스토리지 위치에 자동으로 다운로드됩니다.

데이터 스토리지 요금제

Cisco Cloud가 온보딩된 ASA 및 FDM 매니지드 디바이스에서 매일 수신하는 이벤트 수를 반영하는 데이터 스토리지 요금제를 구매해야 합니다. 이를 "일일 수집 속도"라고 합니다. 데이터 요금제는 1

년, 3년 또는 5년 단위의 GB/일 단위로 제공됩니다. 수집 속도를 결정하는 가장 좋은 방법은 Secure Logging Analytics(SaaS)를 구매하기 전에 무료 평가판에 참여하는 것입니다. 이를 통해 이벤트 볼륨을 적절하게 예측할 수 있습니다.

고객은 90일의 롤링 데이터 스토리지를 자동으로 수신합니다. 즉, 최근 90일간의 이벤트가 Cisco Cloud에 저장되고 91일이 되면 삭제됩니다.

고객은 기본 90일 이상의 추가 이벤트 보존으로 업그레이드하거나 기존 구독에 변경 주문을 통해 일일 볼륨(GB/일)을 추가할 수 있으며, 남은 구독 기간에 대해서만 일할 계산하여 청구됩니다.

데이터 요금제에 대한 자세한 내용은 Secure Logging Analytics(SaaS) 주문 가이드를 참조하십시오.

Note Security Analytics and Logging 라이선스 및 데이터 요금제를 보유하고 있는 경우 나중에 다른 Security Analytics and Logging 라이선스를 취득할 수 있으며, 다른 데이터 요금제를 구매할 필요가 없습니다. 네트워크 트래픽 처리량이 변경되어 다른 데이터 플랜을 취득하는 경우에는 다른 Security Analytics and Logging 라이선스를 구입하지 않아도 됩니다.

내 할당량에 대해 어떤 데이터가 계산됩니까**?**

보안 이벤트 커넥터로 전송된 모든 이벤트는 Secure Logging Analytics(SaaS) 클라우드에 누적되며 데이터 할당량에 포함됩니다.

이벤트 뷰어에 표시되는 내용을 필터링해도 Secure Logging Analytics(SaaS) 클라우드에 저장된 이벤트 수는 줄어들지 않으며, 이벤트 뷰어에서 볼 수 있는 이벤트 수는 줄어듭니다.

이벤트는 90일 동안 Secure Logging Analytics(SaaS) 클라우드에 저장됩니다. 그 후에는 제거됩니다.

스토리지 할당량을 빠르게 사용하고 있습니다**.** 어떻게 해야 합니까**?**

이 문제를 해결하는 두 가지 방법은 다음과 같습니다.

- 추가 스토리지를 요청합니다. 필요한 것을 과소 평가했을 수 있습니다.
- 이벤트를 로깅하는 규칙의 수를 줄입니다. SSL 정책 규칙, 보안 인텔리전스 규칙, 액세스 제어 규칙은 물론 침입 정책, 파일 및 악성코드 정책에서도 이벤트를 로깅할 수 있습니다. 로깅 대상을 확인합니다. 생각보다 많은 규칙 및 정책에서 이벤트를 로깅해야 합니까?

이벤트 스토리지 기간 연장 및 이벤트 스토리지 용량 늘리기

Security Analytics and Logging(보안 분석 및 로깅) 고객은 이러한 라이선싱를 구매할 때 90일의 이벤트 스토리지를 받게 됩니다.

- 로깅 및 문제 해결
- 로깅 분석 및 탐지
- 총 네트워크 분석 및 모니터링

라이선스를 처음 구매할 때 또는 라이선스 기간 중 언제든지 1년, 2년 또는 3년치 롤링 이벤트 스토리지로 업그레이드하도록 선택할 수 있습니다.

Security Analytics and Logging 라이선스를 처음 구매할 때 스토리지 용량을 업그레이드할지 묻는 메시지가 표시됩니다. "예"라고 답하면 구매 중인 PID 목록에 추가 PID(Product Identifier)가 추가됩니다.

라이선스 기간 중간에 롤링 이벤트 스토리지를 연장하거나 이벤트 클라우드 스토리지의 양을 늘리기로 결정한 경우 다음을 수행할 수 있습니다.

프로시저

단계 **1** Cisco Commerce에 사용자 계정으로 로그인합니다.

단계 **2** Cisco Defense Orchestrator PID를 선택합니다.

단계 **3** 프롬프트에 따라 스토리지 용량의 길이 또는 용량을 업그레이드합니다.

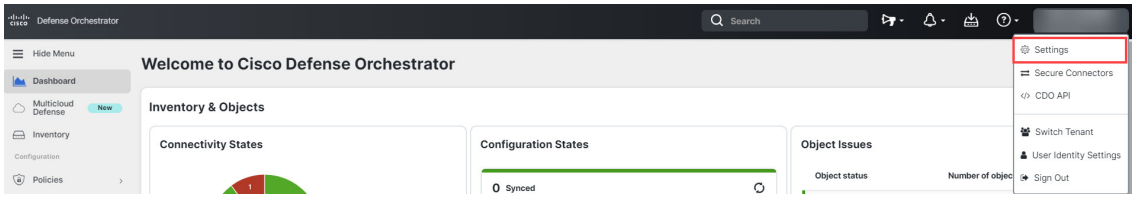
증가된 비용은 기존 라이선스의 남은 기간에 따라 비례 배분됩니다. 자세한 지침은 Secure Logging Analytics(SaaS) 주문 가이드를 참조하십시오.

보안 애널리틱스 및 로깅 데이터 계획 사용량 보기

월별 로깅 제한, 사용한 스토리지의 양, 사용 기간이 0으로 재설정된 경우를 확인하려면 다음을 수행합니다.

Procedure

단계 **1** 테넌트를 클릭하고 **Settings(**설정**)**를 선택합니다.



단계 **2** **Logging Settings(**로깅 설정**)**를 클릭합니다.

단계 **3** **View Historical Usage(**기록 사용량 보기**)**를 클릭하여 최근 12개월까지의 스토리지 사용량을 확인할 수도 있습니다.

SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기

SaaS(Secure Logging Analytics)를 사용하면 ASA 또는 FDM 관리 디바이스에서 SEC(Secure Event Connector)의 특정 UDP, TCP 또는 NSEL 포트로 이벤트를 보낼 수 있습니다. 그런 다음 SEC는 해당 이벤트를 Cisco 클라우드로 전달합니다.

이러한 포트가 아직 사용 중이 아닌 경우, SEC는 이벤트를 수신하는 데 포트를 제공하며, SaaS(Secure Logging Analytics) 설명서에서는 기능을 구성할 때 포트 사용을 권장합니다.

- TCP: 10125
- UDP: 10025
- NSEL: 10425

이러한 포트가 이미 사용 중인 경우 SaaS(Secure Logging Analytics)를 구성하기 전에 SEC 디바이스 세부 정보를 확인하여 실제로 이벤트를 수신하는 데 사용 중인 포트를 확인합니다.

SEC에서 사용하는 포트 번호를 찾으려면 다음을 수행합니다.

Procedure

단계 **1** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **2** Secure Connector(보안 커넥터) 페이지에서 이벤트를 전송할 SEC를 선택합니다.

단계 **3** Details(세부 정보) 창에 이벤트를 전송해야 하는 TCP, UDP 및 NetFlow(NSEL) 포트가 표시됩니다.