



Cisco Security Analytics and Logging

- Cisco Defense Orchestrator의 Security Analytics and Logging(SaaS) 정보, 2 페이지
- CDO의 이벤트 유형, 2 페이지
- ASA에 대한 SAL SaaS(Security Analytics and Logging) 정보, on page 9
- ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, 13 페이지
- CDO 매크로를 사용하여 Cisco Cloud로 ASA 시스템 로그 이벤트 전송, on page 15
- 명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송, on page 19
- ASA 디바이스용 NSEL(Network Security Event Logging), on page 25
- 구문 분석된 ASA 시스템 로그 이벤트, on page 38
- 클라우드 제공 Firewall Management Center 관리 디바이스에 대한 SAL(SaaS) 구현, 40 페이지
- SAL(SaaS) 통합의 요구사항, 지침 및 제한, 40 페이지
- 시스템 로그를 사용하여 SAL(SaaS)에 이벤트 전송, 41 페이지
- 직접 연결을 사용하여 SAL(SaaS)에 , 43 페이지
- 직접 연결을 사용하여 SAL(SaaS)에 이벤트 로그를 전송하기 위해 위협 방어 디바이스 활성화 또는 비활성화, 44 페이지
- 보안 이벤트 커넥터, 45 페이지
- 보안 이벤트 커넥터 설치, 46 페이지
- Cisco Security Analytics and Logging(SaaS) 프로비저닝, 66 페이지
- 보안 이벤트 커넥터 제거, 66 페이지
- Cisco Secure Cloud Analytics 포털 프로비저닝, on page 67
- Secure Cloud Analytics에서 센서 상태 및 CDO 통합 상태 검토, 68 페이지
- 전체 네트워크 분석 및 보고를 위한 **Cisco Secure Cloud Analytics** 센서 구축, on page 69
- CDO에서 Cisco Secure Cloud Analytics 알림 보기, on page 70
- Cisco Secure Cloud Analytics 및 동적 엔티티 모델링, on page 71
- 방화벽 이벤트 기반 알림 작업, on page 72
- 알림 우선순위 수정, 79 페이지
- 라이브 이벤트 보기, on page 79
- 이벤트 로깅 페이지의 열 표시 및 숨기기, on page 82
- 사용자 지정 가능한 이벤트 필터, on page 86
- Security Analytics and Logging의 이벤트 속성, on page 87
- 이벤트 로깅 페이지에서 이벤트 검색 및 필터링, 118 페이지

- 백그라운드 검색 다운로드, 128 페이지
- 데이터 스토리지 요금제, on page 128
- SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기, on page 130

Cisco Defense Orchestrator의 Security Analytics and Logging(SaaS) 정보

Cisco SAL(Security Analytics and Logging)을 사용하면 모든 ASA 및 Secure Firewall Threat Defense 디바이스에서 연결, 침입, 파일, 악성코드, 보안 인텔리전스, 시스템 로그 및 NSEL(Netflow Secure Event Logging) 이벤트를 캡처하여 CDO(Cisco Defense Orchestrator)에서 한꺼번에 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.

CDO의 이벤트 유형

SaaS(Secure Logging Analytics)에서 로깅한 ASA 및 Secure Firewall Threat Defense 이벤트를 필터링할 때 CDO가 지원하는 ASA 및 FTD 이벤트 유형 목록에서 선택할 수 있습니다. CDO 메뉴에서 **Analytics**(분석) > **Event Logging**(이벤트 로깅)으로 이동하고 필터 아이콘을 클릭하여 이벤트를 선택합니다. 이러한 이벤트 유형은 시스템 로그 ID의 그룹을 나타냅니다. 아래 표는 어떤 시스템 로그 ID가 어떤 이벤트 유형에 포함되어 있는지 보여줍니다. 특정 시스템 로그 ID에 대한 자세한 내용은 [Cisco ASA Series 시스템 로그 메시지](#) 또는 [Cisco Secure Firewall Threat Defense 시스템 로그 메시지 가이드](#)에서 검색할 수 있습니다.

일부 시스템 로그 이벤트에는 추가 속성 "EventName"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 EventName 속성을 통해 이벤트 테이블을 필터링해서 찾을 수 있습니다. [Syslog 이벤트에 대한 이벤트 이름 속성](#)을 참조하십시오.

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. 일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성을 참조하십시오.

NetFlow 이벤트는 시스템 로그 이벤트와 다릅니다. NetFlow 필터는 NSEL 레코드를 생성한 모든 NetFlow 이벤트 ID를 검색합니다. 이러한 NetFlow 이벤트 ID는 Cisco ASA NetFlow 구현 가이드에 정의되어 있습니다.

다음 테이블에서는 CDO가 지원하는 이벤트 유형을 설명하고 이벤트 유형에 해당하는 시스템 로그 또는 NetFlow 이벤트 번호를 나열합니다.

필터 이름	설명	해당 시스템 로그 이벤트 또는 NetFlow 이벤트
AAA	이는 AAA가 구성된 경우 네트워크의 리소스를 모두 사용하거나 권한을 부여하거나 인증하려는 시도가 실패 또는 잘못된 경우 시스템에서 생성하는 이벤트입니다.	109001-109035 113001-113027
봇넷	이러한 이벤트는 사용자가 악성 코드에 감염된 호스트(봇넷)를 포함할 수 있는 악의적인 네트워크에 액세스하려고 하거나 시스템이 동적 필터 차단 목록에서 도메인 또는 IP 주소와 주고받는 트래픽을 탐지하는 경우 로깅됩니다.	338001-338310
장애 조치	이러한 이벤트는 시스템이 스택이트폴 및 스택이트리스 페일오버 구성에서 오류를 탐지하거나 페일오버 발생 시 보조 방화벽 유닛에서 오류를 탐지하면 로깅됩니다.	101001-101005, 102001, 103001-103007, 104001-104004, 105001-105048 210001-210022 311001-311004 709001-709007

필터 이름	설명	해당 시스템 로그 이벤트 또는 NetFlow 이벤트
방화벽 거부됨	<p>이러한 이벤트는 방화벽 시스템이 다양한 이유로 네트워크 패킷의 트래픽을 거부할 때 발생하며, 이는 잠재적으로 네트워크에 대한 공격을 의미할 수 있습니다. 보안 정책으로 인해 패킷이 삭제되거나 시스템이 동일한 소스 IP와 대상 IP를 가진 패킷을 수신하여 패킷이 삭제되는 등 다양한 패킷 삭제 이유가 있을 수 있습니다.</p> <p>방화벽 거부됨 이벤트는 NetFlow에 포함될 수 있으며 NetFlow 이벤트 ID 및 시스템 로그 ID와 함께 보고될 수 있습니다.</p>	106001, 106007, 106012, 106013, 106015, 106016, 106017, 106020, 106021, 106022, 106023, 106025, 106027
방화벽 트래픽	<p>이는 네트워크에서의 다양한 연결 시도, 사용자 ID, 타임스탬프, 종료된 세션 등에 따라 로깅되는 이벤트입니다.</p> <p>방화벽 트래픽 이벤트는 NetFlow에 포함될 수 있으며 NetFlow 이벤트 ID 및 시스템 로그 ID와 함께 보고될 수 있습니다.</p>	<p>106001-106100, 108001-108007, 110002-110003</p> <p>201002-201013, 209003-209005, 215001</p> <p>302002-302304, 302022-302027, 303002-303005, 313001-313008, 317001-317006, 324000-324301, 337001-337009</p> <p>400001-400050, 401001-401005, 406001-406003, 407001-407003, 408001-408003, 415001-415020, 416001, 418001-418002, 419001-419003, 424001-424002, 431001-431002, 450001</p> <p>500001-500005, 508001-508002</p> <p>607001-607003, 608001-608005, 609001-609002, 616001</p> <p>703001-703003, 726001</p>
IPsec VPN	<p>IPsec 보안 연결의 불일치가 발생하거나 시스템이 수신하는 IPsec 패킷에서 오류를 탐지하면 IPsec VPN이 구성된 방화벽에 이러한 이벤트가 로깅됩니다.</p>	402001-402148, 602102-602305, 702304-702307

필터 이름	설명	해당 시스템 로그 이벤트 또는 NetFlow 이벤트
NAT	NAT 항목이 생성되거나 삭제된 경우, 그리고 NAT 풀의 모든 주소가 사용된 경우 NAT 구성 방화벽에 이러한 이벤트가 로깅됩니다.	201002-201013, 202001-202011, 305005-305012
SSL VPN	WebVPN 세션이 생성되거나 종료될 때, 사용자 액세스 오류 및 사용자 활동이 발생할 때 SSL VPN으로 구성된 방화벽에 이러한 이벤트가 로깅됩니다.	716001-716060, 722001-722053, 723001-723014, 724001-724004, 725001-725015
NetFlow	네트워크 패킷이 인터페이스를 오가는 IP 네트워크 트래픽, 타임스탬프, 사용자 ID 및 전송되는 데이터 양을 중심으로 이러한 이벤트가 로깅됩니다.	0, 1, 2, 3, 5

필터 이름	설명	해당 시스템 로그 이벤트 또는 NetFlow 이벤트
연결	<p>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.</p> <p>연결 이벤트에는 탐지된 세션에 관한 데이터가 포함되어 있습니다. 모든 개별 연결 이벤트에 대한 정보는 몇 가지 요소에 따라 가용성이 결정되지만, 일반적으로는 다음과 같습니다.</p> <ul style="list-style-type: none"> • 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 	430002, 430003

필터 이름	설명	해당 시스템 로그 이벤트 또는 NetFlow 이벤트
침입	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.	430001
파일	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.	430004

필터 이름	설명	해당 시스템 로그 이벤트 또는 NetFlow 이벤트
악성코드	<p>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.</p> <p>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.</p>	430005
보안 인텔리전스	<p>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.</p> <p>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.</p>	430002, 430003

ASA에 대한 SAL SaaS(Security Analytics and Logging) 정보

SaaS(Security Analytics and Logging)를 사용하면 ASA에서 모든 시스템 로그 이벤트 및 NSEL(Netflow Secure Event Logging)을 캡처하여 CDO(Cisco Defense Orchestrator)에서 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. **Logging and Troubleshooting**(기록 및 문제 해결) 패키지는 이러한 기능을 제공합니다.

시스템은 로깅 분석 및 탐지 패키지(이전 방화벽 분석 및 로깅 패키지)를 사용하여 FTD 이벤트에 Secure Cloud Analytics 동적 엔티티 모델링을 적용하고 행동 모델링 분석을 사용하여 Secure Cloud Analytics 관찰 및 알림을 생성할 수 있습니다. 전체 네트워크 분석 및 모니터링 패키지를 구입하는 경우 시스템은 FTD 이벤트와 네트워크 트래픽 모두에 동적 엔티티 모델링을 적용하고 관찰 및 알림을 생성합니다. Cisco SSO(Single Sign-On, 단일 인증)를 사용하여 CDO에서 사용자에게 프로비저닝된 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다.

CDO 이벤트 뷰어에 ASA 이벤트가 표시되는 방법

ASA에서 로깅이 활성화되고 네트워크 트래픽이 액세스 제어 규칙 기준과 일치하면 시스템 로그 이벤트 및 NSEL 이벤트가 생성됩니다. 이벤트가 Cisco Cloud에 저장되면 CDO에서 볼 수 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. 모든 SEC에 동일한 이벤트를 전달하지 마십시오. Cisco Cloud로 전송되는 이벤트를 복제하고 일일 수집 속도를 불필요하게 부풀릴 수 있습니다.

보안 이벤트 커넥터를 통해 ASA에서 Cisco Cloud로 시스템 로그 및 NSEL 이벤트를 전송하는 방법

기본 로깅 및 문제 해결 라이선스를 사용하는 경우 ASA 이벤트가 Cisco Cloud에 도달하는 방법은 다음과 같습니다.

1. 사용자 이름 및 비밀번호를 사용하여 CDO에 ASA를 온보딩합니다.
2. 시스템 로그 및 NSEL 이벤트를 시스템 로그 서버인 것처럼 SEC 중 하나에 전달하고 디바이스에서 로깅을 활성화하도록 ASA를 구성합니다.
3. SEC는 이벤트가 저장된 Cisco Cloud로 이벤트를 전달합니다.
4. CDO는 설정한 필터에 따라 Cisco Cloud의 이벤트를 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 클라우드에 저장된 ASA 시스템 로그 이벤트에 분석을 적용합니다.
2. 생성된 관찰 및 알림은 CDO 포털과 연결된 Secure Cloud Analytics 포털에서 액세스할 수 있습니다.

3. CDO 포털에서 Secure Cloud Analytics 포털을 교차 실행하여 이러한 관찰 및 알림을 검토할 수 있습니다.

솔루션에 사용된 구성 요소

SDC(Secure Device Connector) - SDC는 CDO를 ASA에 연결합니다. ASA에 대한 로그인 자격 증명은 SDC에 저장되지 않습니다. 자세한 내용은 [보안 디바이스 커넥터](#)를 참조하십시오.

SEC(Secure Event Connector) - SEC는 ASA에서 이벤트를 수신하여 Cisco Cloud로 전달하는 애플리케이션입니다. Cisco Cloud에 있으면 CDO의 Event Logging(이벤트 로깅) 페이지에서 이벤트를 보거나 Secure Cloud Analytics를 사용하여 분석할 수 있습니다. 환경에 따라 SEC는 보안 디바이스 커넥터(있는 경우)에 설치됩니다. 또는 네트워크에서 유지 관리하는 자체 CDO 커넥터 가상 머신에서 수행할 수 있습니다. 자세한 내용은 [보안 이벤트 커넥터](#), on page 45를 참조하십시오.

Adaptive Security Appliance (ASA)-ASA에서는 고급 스테이트풀 방화벽 및 VPN 집선 장치 기능을 제공하며 애드온 모듈과 통합된 서비스를 제공합니다. ASA에는 다중 보안 상황(가상 방화벽과 유사), 클러스터링(다중 방화벽을 단일 방화벽으로 통합), 투명(Layer 2) 방화벽 또는 라우팅(Layer 3) 방화벽 가동, 고급 검사 엔진, IPsec VPN, SSL VPN 및 클라이언트리스 SSL VPN 지원 등의 다양한 기능이 포함되어 있습니다.

Secure Cloud Analytics는 ASA 이벤트에 동적 엔티티 모델링을 적용하여 이 정보를 기반으로 탐지를 생성합니다. 이렇게 하면 네트워크에서 수집한 텔레메트리를 심층적으로 분석하여 추세를 식별하고 네트워크 트래픽의 이상 동작을 검사할 수 있습니다. **Logging Analytics and Detection**(로깅 분석 및 탐지) 또는 **Total Network Analytics and Monitoring**(총 네트워크 분석 및 모니터링) 라이선스가 있는 경우 이 서비스를 사용할 수 있습니다.

라이선싱

이 솔루션을 구성하려면 다음 계정 및 라이선스가 필요합니다.

- **Cisco Defense Orchestrator**. CDO 테넌트가 있어야 합니다.
- **Secure Device Connector**. 보안 디바이스 커넥터에 대한 별도의 라이선스는 없습니다.
- **Secure Event Connector**. 보안 이벤트 커넥터에 대한 별도의 라이선스는 없습니다.
- **Secure Logging Analytics(SaaS)**. [Security Analytics and Logging 라이선스 테이블](#)을 참조하십시오.
- **ASA(Adaptive Security Appliance)**. 기본 라이선스 이상

Security Analytics and Logging 라이선싱

SaaS(Security Analytics and Logging)를 구현하려면 다음 라이선스 중 하나를 구매해야 합니다.

라이선스 이름	제공된 기능	사용 가능한 라이선스 기간	기능 사전 요건
로깅 및 문제 해결	<ul style="list-style-type: none"> 라이브 피드 및 기록 보기로 CDO 내의 ASA 이벤트 및 이벤트 세부 정보 보기 	<ul style="list-style-type: none"> 1년 3년 5년 	<ul style="list-style-type: none"> CDO 소프트웨어 버전 9.6 이상을 실행하는 온프레미스 ASA 구축 Cisco Cloud에 ASA 이벤트를 전달하기 위한 하나 이상의 SEC 구축
로깅 분석 및 탐지(이전 이름 방화벽 분석 및 모니터링)	<p>로깅 및 문제 해결 기능 추가:</p> <ul style="list-style-type: none"> 이벤트에 동적 엔터티 모델링 및 행동 분석을 적용합니다. 이벤트 데이터를 기반으로 Secure Cloud Analytics에서 알림 열기, CDO 이벤트 뷰어에서 교차 실행 	<ul style="list-style-type: none"> 1년 3년 5년 	<ul style="list-style-type: none"> CDO 소프트웨어 버전 9.6 이상을 실행하는 온프레미스 ASA 구축 Cisco Cloud에 ASA 이벤트를 전달하기 위한 하나 이상의 SEC 구축 새로 프로비저닝된 또는 기존의 Cisco Secure Cloud Analytics 포털.

라이선스 이름	제공된 기능	사용가능한라이선스기간	기능 사전 요건
총 네트워크 분석 및 모니터링	<p>로깅 분석 및 탐지, 추가:</p> <ul style="list-style-type: none"> • ASA 이벤트, 온프레미스 네트워크 트래픽 및 클라우드 기반 네트워크 트래픽에 동적 엔티티 모델링 및 행동 분석을 적용합니다. • ASA 이벤트 데이터, Cisco Secure Cloud Analytics 센서에서 수집한 온프레미스 네트워크 트래픽 플로우 데이터 및 CDO 이벤트 뷰어에서 교차 실행되는 Cisco Secure Cloud Analytics에 전달된 클라우드 기반 네트워크 트래픽의 조합을 기반으로 하는 Cisco Secure Cloud Analytics의 공개 알림 	<ul style="list-style-type: none"> • 1년 • 3년 • 5년 	<ul style="list-style-type: none"> • CDO • 소프트웨어 버전 9.6 이상을 실행하는 온프레미스 ASA 구축 • Cisco Cloud에 이벤트를 전달하기 위한 하나 이상의 SEC 구축 • 네트워크 트래픽 플로우 데이터를 클라우드에 전달하기 위해 하나 이상의 Cisco Secure Cloud Analytics 센서 버전 4.1 이상을 구축하거나, 네트워크 트래픽 플로우 데이터를 Cisco Secure Cloud Analytics로 전달하기 위해 Cisco Secure Cloud Analytics를 클라우드 기반 구축과 통합합니다. • 새로 프로비저닝된 또는 기존의 Cisco Secure Cloud Analytics 포털.

데이터 요금제

Cisco Cloud가 온보딩된 ASA에서 매일 수신하는 이벤트 수를 반영하는 데이터 요금제를 구매해야 합니다. 이를 "일일 수집 속도"라고 합니다. [Logging Volume Estimator](#) 도구를 사용하여 일일 수집 속도를 예측할 수 있으며, 속도가 변경되면 데이터 요금제를 업데이트할 수 있습니다.

데이터 요금제는 일별 볼륨 1GB 단위로 제공되며 1년, 3년 또는 5년 단위로 제공됩니다. 데이터 요금제에 대한 자세한 내용은 [Secure Logging Analytics\(SaaS\) 주문 가이드](#)를 참조하십시오.



Note 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 **Monitoring**(모니터링) > **Event Logging**(이벤트 로깅) 탭으로 이동하여 30일 무료 평가판을 요청할 수 있습니다. 30일 평가판이 끝나면 [SaaS\(Secure Logging Analytics\) 주문 가이드](#)의 지침에 따라 CCW(Cisco Commerce Workspace)에서 서비스를 계속하기 위해 원하는 이벤트 데이터 볼륨을 주문할 수 있습니다.

다음 단계

[ASA 디바이스에 대한 SaaS\(Secure Logging Analytics\) 구현](#)으로 이동

ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현

시작하기 전에

- [ASA에 대한 SAL SaaS\(Security Analytics and Logging\) 정보](#)를 검토하여 다음에 대해 알아보십시오.
 - Cisco Cloud로 이벤트를 전송하는 방법
 - 솔루션의 애플리케이션
 - 필요한 라이선스
 - 필요한 데이터 요금제
- CDO 테넌트를 생성하기 위해 매니지드 서비스 제공자 또는 CDO 영업 담당자에게 문의했습니다.
- [보안 디바이스 커넥터](#)를 검토합니다. SDC를 사용하여 CDO를 ASA에 연결하는 것은 "모범 사례"로 간주되지만 필수 사항은 아닙니다.
- 네트워크에서 SDC를 구축하려는 경우 다음 방법 중 하나를 사용하여 설치할 수 있습니다.
 - 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.
 - [고유한 VM 이미지를 사용하여 보안 디바이스 커넥터 구축](#)을 사용합니다.

- **보안 이벤트 커넥터 설치**했으며 모든 ASA에서 테넌트에 온보딩된 SEC로 이벤트를 전송할 수 있습니다.
- 어카운트 사용자에게 대한 **이중 인증을 설정**했습니다.

Cisco SaaS(Security Analytics and Logging)를 구현하고 보안 이벤트 커넥터를 통해 **Cisco Cloud**로 이벤트를 전송하는 워크플로우

1. 위의 "시작하기 전에"를 검토하여 환경이 올바르게 구성되었는지 확인하십시오.
2. 사용자 이름 및 비밀번호를 사용하는 **ASA 디바이스 온보딩**
3. **명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송.**
4. **CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성.**
5. 이벤트가 CDO에 표시되는지 확인합니다. 탐색 막대에서 **Monitoring(모니터링)>Event Logging(이벤트 로깅)**을 선택합니다. 라이브 이벤트를 보려면 Live(라이브) 탭을 클릭합니다.
6. **Firewall Analytics and Monitoring(방화벽 분석 및 모니터링)** 또는 **Total Network Analytics and Monitoring(총 네트워크 분석 및 모니터링)** 라이선스가 있는 경우 다음 섹션인 **Cisco Secure Cloud Analytics**를 사용하여 이벤트 분석을 계속 진행합니다.

Cisco Secure Cloud Analytics를 사용하여 이벤트 분석

Firewall Analytics and Monitoring(방화벽 분석 및 모니터링) 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, 67 페이지.**
2. **Total Network Analytics 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, 69 페이지**의 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, 70 페이지**의 내용을 참조하십시오.
4. FTD 이벤트에서 생성된 Secure Cloud Analytics 알림을 모니터링하려면 CDO에서 Secure Cloud Analytics로 교차 실행합니다. **CDO에서 Cisco Secure Cloud Analytics 알림 보기, 70 페이지**의 내용을 참조하십시오.

CDO에서 교차 실행하여 Cisco Secure Cloud Analytics 알림 검토

Firewall Analytics and Monitoring(방화벽 분석 및 모니터링) 또는 **Total Network Analytics and Monitoring(총 네트워크 분석 및 모니터링)** 라이선스를 사용하면 CDO에서 Secure Cloud Analytics로 교차 실행하여 FTD 이벤트에 의해 생성된 알림을 검토할 수 있습니다.

자세한 내용은 다음 문서를 참조하십시오.

- CDO에 로그인
- CDO에서 Cisco Secure Cloud Analytics 알림 보기, 70 페이지
- Cisco Secure Cloud Analytics 및 동적 엔티티 모델링
- 방화벽 이벤트 기반 알림 작업

보안 이벤트 커넥터 문제 트러블슈팅

다음 문제 해결 항목을 사용하여 다음에 대한 상태 및 로깅 정보를 수집합니다.

- 보안 이벤트 커넥터 온보딩 실패 문제 해결
- 문제 해결 로그 파일 이벤트 로깅
- 상태 확인을 사용하여 보안 이벤트 커넥터의 상태 학습

워크플로

보안 및 분석 로깅 이벤트를 사용한 문제 해결에서는 Cisco Security Analytics 및 로깅에서 생성된 이벤트를 사용하여 사용자가 네트워크 리소스에 액세스할 수 없는 이유를 확인하는 방법을 설명합니다.

방화벽 이벤트 기반 알림 작업도 참조하십시오.

CDO 매크로를 사용하여 Cisco Cloud로 ASA 시스템 로그 이벤트 전송

명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송에 설명된 모든 명령을 사용하는 CDO 매크로를 생성하고 동일한 배치의 모든 ASA에서 해당 매크로를 실행하여 Cisco Cloud에 이벤트를 전송하도록 모든 ASA를 구성할 수 있습니다.

CDO의 매크로 툴을 사용하면 CLI 명령 목록을 어셈블하고, 명령 syntax(명령문)의 요소를 매개변수로 변환한 다음, 두 번 이상 사용 가능하게끔 명령 목록을 저장할 수 있습니다. 매크로는 한 번에 둘 이상의 디바이스에서 실행할 수도 있습니다.

검증된 매크로를 사용하면 디바이스 간의 컨피그레이션 일관성이 향상되고, 명령줄 인터페이스를 사용할 때 발생할 수 있는 syntax(명령문) 오류가 방지됩니다.

자세한 내용을 읽기 전에 이러한 항목을 검토하여 매크로 사용 메커니즘을 이해하십시오. 이 문서에서는 최종 매크로 어셈블에 대해서만 설명합니다.

- 디바이스 관리를 위한 CLI 매크로
- CLI 매크로 생성
- CLI 매크로 실행
- CLI 매크로 편집

- CLI 매크로 삭제

ASA SaaS(Security Analytics and Logging) 매크로 생성

다음 절차에서 볼 수 있는 서식에는 ASA CLI 명령과 매크로 형식의 두 가지 유형이 있습니다. ASA CLI 명령은 [ASA 구문 규칙](#)을 따르도록 작성되었습니다. 매크로 규칙은 [CLI 매크로 생성](#)에 설명되어 있습니다.

시작하기 전에 별도의 창에서 [명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송](#)을 열고 이 절차와 동시에 읽어보십시오. 그러면 매크로를 생성할 때 명령 설명을 읽을 수 있습니다.



Note 로깅 구성이 이미 ASA에 있는 경우 CDO에서 매크로를 실행해도 기존 로깅 구성이 모두 지워지지 않습니다. 대신, CDO 매크로에 정의된 설정이 이미 있는 것과 병합됩니다.

단계 1 일반 텍스트 편집기를 열고 아래의 지침 및 옵션에 따라 매크로로 변환할 명령 목록을 생성합니다. CDO는 매크로에 기록된 순서대로 명령을 실행합니다. 일부 명령에는 매크로를 실행할 때 입력하는 `{{parameters}}` 값이 있습니다.

단계 2 ASA가 시스템 로그 서버인 것처럼 **SEC**에 메시지를 보내도록 구성합니다.

메시지를 전송할 syslog 서버로 SEC를 지정하려면 **logging host** 명령을 사용합니다. 테넌트에 온보딩한 SEC 중 하나에 이벤트를 보낼 수 있습니다.

logging host 명령은 이벤트를 보낼 TCP 또는 UDP 포트를 지정합니다. 어떤 포트를 사용해야 하는지 확인하려면 [SaaS\(Secure Logging Analytics\)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기](#)를 참조하십시오.

logging host*interface_name***SEC_IP_address**{**tcp**/**port** | **udp**/**port**}

시스템 로그 이벤트를 SEC로 전송하는 데 사용하는 프로토콜에 따라 이 명령을 두 개의 서로 다른 매크로 중 하나로 설정합니다.

logging host `{{interface_name}}` `{{SEC_ip_address}}` tcp/`{{port_number}}`

logging host `{{interface_name}}` `{{SEC_ip_address}}` udp/`{{port_number}}`

(선택 사항) TCP를 사용하는 경우 매크로의 명령 목록에 이 명령을 추가할 수 있습니다. 매개변수가 필요하지 않습니다.

logging permit-hostdown

단계 3 어떤 **syslog** 메시지를 **syslog** 서버에 전송할지 지정합니다.

logging trap 명령을 사용하여 syslog 서버로 보내야 하는 syslog 메시지를 지정합니다.

logging trap {*severity_level* | *message_list*}

심각도 수준별로 SEC로 전송되는 이벤트를 정의하려면 명령을 다음 매크로로 전환합니다.

logging trap `{{severity_level}}`

메시지 목록의 일부인 SEC에 이벤트만 보내려면 명령을 다음 매크로로 변환합니다.

```
logging trap {{message_list_name}}
```

이전 단계에서 **logging trap message_list** 명령을 선택한 경우 메시지 목록에서 syslog를 정의해야 합니다. 매크로를 생성할 때 명령 설명을 읽을 수 있도록 **사용자 지정 이벤트 목록 생성**을 엽니다. 다음 명령으로 시작합니다.

```
logging listname {level level [class message_class] | message start_id [-end_id]}
```

이를 다음과 같이 분류합니다.

```
logging list {{message_list_name}} level {{security_level}}
```

```
logging list {{message_list_name}} level {{security_level}} class {{message_class}}
```

```
logging list {{message_list_name}} message {{syslog_range_or_number}}
```

마지막 변형에서는 메시지 파라미터 {{syslog_range_or_number}}를 단일 syslog ID(106023) 또는 범위(302013-302018)로 입력할 수 있습니다. 메시지 목록을 만들려면 원하는 만큼의 줄에서 하나 이상의 명령 변형을 사용합니다. 단일 매크로에서 동일한 이름의 모든 매개변수는 사용자가 입력한 것과 동일한 값을 사용한다는 점에 유의하십시오. CDO는 매개변수가 비어 있는 매크로를 실행하지 않습니다.

Important **logging list** 명령은 매크로에서 **logging trap** 명령 앞에 와야 합니다. 먼저 목록을 정의하면 **logging trap** 명령에서 사용할 수 있습니다. 아래의 **샘플 매크로**를 참조하십시오.

- 단계 4** (선택 사항) syslog 타임스탬프를 추가합니다. ASA에서 발생한 시스템 로그 메시지에 날짜와 시간을 추가하려면 이 명령을 추가합니다. 타임스탬프 값은 **SyslogTimestamp** 필드에 표시됩니다. 이 명령을 명령 목록에 추가합니다. 매개변수는 필요하지 않습니다.

logging timestamp

Note 버전 9.10(1)부터 ASA는 이벤트 시스템 로그에서 RFC 5424에 따라 타임스탬프를 활성화하는 옵션을 제공합니다. 이 옵션을 활성화하면 syslog 메시지의 모든 타임스탬프가 RFC 5424 형식에 따라 시간을 표시합니다. 다음은 RFC 5424 형식의 샘플 출력입니다.

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from
src interface :src IP/src port to dest IP/dest port
```

- 단계 5** (선택 사항) EMBLEM 형식이 아닌 syslog 메시지에 디바이스 ID를 포함합니다. 매크로를 생성할 때 명령 설명을 읽을 수 있도록 **디바이스 ID를 EMBLEM 이의 형식 Syslog 메시지에 포함**을 엽니다. 이는 매크로의 기반이 되는 CLI 명령입니다.

```
logging device-id {cluster-id | context-name | hostname | ipaddress interface_name [system] | string text}
```

이를 다음과 같이 분류합니다.

```
logging device-id cluster-id
```

```
logging device-id context-name
```

```
logging device-id hostname
```

```
logging device-id ipaddress {{interface_name}} system
```

```
logging device-id string {{text_16_char_or_less}}
```

- 단계 6** 로깅을 활성화합니다. 이 명령을 그대로 매크로에 추가합니다. 매개변수가 없습니다.

logging enable

단계 7 매크로의 마지막 줄에 쓰기 **write memory**를 추가하지 마십시오. 대신 **show running-config logging** 명령을 추가하여 ASA의 시작 구성에 커밋하기 전에 입력한 로깅 명령의 결과를 검토합니다.

show running-config logging

단계 8 구성이 변경되었다고 확인하는 경우 **write memory** 명령에 대한 별도의 매크로를 생성하거나 CDO의 **대량 명령 줄 인터페이스** 기능을 사용하여 매크로를 사용하여 구성된 모든 디바이스에 명령을 실행할 수 있습니다.

write memory

단계 9 (선택 사항) 액세스 제어 규칙 "permit" 이벤트에 대한 로깅을 활성화합니다. 이 단계는 **명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송** 절차에 설명되어 있지만 이 매크로에는 포함되어 있지 않습니다. 대신 CDO GUI에서 수행됩니다.

단계 10 매크로를 저장합니다.

Example

다음은 단일 매크로로 결합된 명령 목록의 샘플입니다.

```
logging host {{interface_name}} {{SEC_ip_address}} {{tcp_or_udp}}/{{port_number}}
logging permit-hostdown
logging list {{message_list_name}} level {{security_level}}
logging list {{message_list_name}} message {{syslog_range_or_number_1}}
logging list {{message_list_name}} message {{syslog_range_or_number_2}}
logging trap {{message_list_name}}
logging device-id cluster-id
logging enable
show running-config logging
```



Note 서로 다른 특정 syslog ID 또는 범위를 추가하는 몇 가지 **logging list** 명령이 있습니다. {{syslog_range_or_number_X}} 매개변수에는 숫자 또는 기타 구분자가 필요합니다. 그렇지 않으면 매크로가 채워질 때 값이 모두 동일하게 됩니다. 또한 모든 매개변수에 값이 지정되지 않은 경우 CDO는 매크로를 실행하지 않으므로 실행하려는 명령만 매크로에 포함해야 한다는 점에 유의하십시오. 모든 syslog ID가 동일한 목록에 포함되므로 event_list_name이 각 줄에서 동일하게 유지됩니다.

What to do next**매크로 실행**

ASA Security Analytics and Logging Macro(보안 분석 및 로깅 매크로)를 생성하고 저장한 후 매크로를 실행하여 ASA 시스템 로그 이벤트를 Cisco Cloud로 전송합니다.

명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송

이 절차에서는 ASA 시스템 로그 이벤트를 SEC(Secure Event Connector)에 전달한 다음 로깅을 활성화하는 방법을 설명합니다. 이러한 절차에서는 해당 워크플로우를 완료하는 데 필요한 사항만 설명합니다. ASA에서 로깅을 구성할 수 있는 모든 방법에 대한 자세한 내용은 [ASDM1: Cisco ASA 시리즈 일반 운영 ASDM 구성 가이드](#) 또는 [CLI 1권: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드](#)의 모니터링 장을 참조하십시오.

지원되는 ASA 명령에 대한 제한 사항

CDO는 아직 다음 Syslog 명령 또는 메시지 형식을 지원하지 않습니다.

- Syslog의 EMBLEM 형식
- 보안 Syslog

ASA용 CDO 명령줄 인터페이스

이 절차의 모든 작업은 ASA용 CDO의 명령줄 인터페이스에서 진행하게 됩니다. 명령줄 인터페이스 페이지를 열려면 다음을 수행합니다.

단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 로깅을 활성화할 ASA를 선택합니다.

단계 4 오른쪽의 Device Actions(디바이스 작업) 창에서 > **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 5 **Command Line Interface**(명령줄 인터페이스) 탭을 클릭합니다. 이제 프롬프트에서 아래에 설명된 명령을 입력할 준비가 되었습니다.

모든 명령을 입력한 후 **Send**(전송)를 클릭합니다. CDO의 CLI 인터페이스는 ASA에 직접 연결되므로 명령은 디바이스의 실행 중인 구성에 즉시 기록됩니다. ASA의 시작 구성에 변경 사항을 기록하려면 `write memory` 명령을 추가로 실행해야 합니다.

보안 이벤트 커넥터에 ASA Syslog 이벤트 전달

ASA 시스템 로그 이벤트를 온보딩한 SEC(Secure Event Connector) 중 하나로 전달한 다음 로깅을 활성화하려면 다음 절차에서 작업을 완료해야 합니다.

단계 1 ASA가 시스템 로그 서버인 것처럼 SEC에 메시지를 보내도록 구성합니다.

단계 2 SEC에 전송할 모든 로그의 심각도 레벨 또는 시스템 로그 이벤트 목록을 결정합니다.

단계 3 로깅을 활성화합니다.

단계 4 변경 사항을 ASA의 시작 구성에 저장합니다.

CLI를 사용하여 ASA 시스템 로그 이벤트를 Cisco 클라우드로 전송

단계 1 ASA가 시스템 로그 서버인 것처럼 SEC에 메시지를 보내도록 구성합니다.

ASA에서 Cisco Cloud로 시스템 로그 이벤트를 전송할 때 외부 시스템 로그 서버인 것처럼 SEC로 전달하면 SEC에서 Cisco Cloud로 메시지를 전달합니다.

syslog 메시지를 SEC에 보내려면 다음 단계를 수행합니다.

- a. TCP 또는 UDP를 사용하여 ASA가 시스템 로그 서버인 것처럼 SEC에 메시지를 전송하도록 ASA를 구성합니다. SEC는 IPv4 또는 IPv6 주소를 사용할 수 있습니다. TCP 또는 UDP 포트로 이벤트를 전송합니다. 어떤 포트를 사용해야 하는지 확인하려면 [SaaS\(Secure Logging Analytics\)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기](#)를 참조하십시오.

다음은 **logging host** 명령 구문의 예입니다.

```
logging host interface_name SEC_IP_address [[ tcp/port ] | [ udp/port ]]
```

예:

```
> logging host mgmt 192.168.1.5 tcp/10125
> logging host mgmt 192.168.1.5 udp/10025
> logging host mgmt 2002::1:1 tcp/10125
> logging host mgmt 2002::1:1 udp/10025
```

- **interface_name** 인수는 메시지가 시스템 로그 서버로 전송되는 ASA 인터페이스를 지정합니다. SDC와의 통신에 이미 사용 중인 동일한 ASA 인터페이스를 통해 SDC에 시스템 로그 메시지를 보내는 것이 "모범 사례"입니다.
- **SEC_IP_address** 인수는 SEC가 설치된 VM의 IP 주소를 포함해야 합니다.
- **tcp/port** 또는 **udp/port** 키워드-인수 쌍은 시스템 로그 메시지가 TCP 프로토콜 및 관련 포트 또는 UDP 프로토콜 및 관련 포트를 사용하여 전송되도록 지정합니다. UDP 또는 TCP를 사용하여 syslog 서버에 데이터를 전송하도록 ASA를 구성할 수 있지만 둘 다 사용할 수는 없습니다. 프로토콜을 지정하지 않으면 기본 프로토콜은 UDP입니다.

TCP를 지정한 경우 ASA는 시스템 로그 서버의 장애를 감지하고 보호 조치로서 ASA를 통한 새로운 연결을 차단합니다. TCP syslog 서버에 대한 연결에 관계없이 새 연결을 허용하려면 b 단계를 참조하십시오. UDP를 지정한 경우 ASA는 시스템 로그 서버의 작동 여부에 관계없이 새 연결을 계속 허용합니다. 유효한 값

Note 두 개의 개별 syslog 서버로 ASA 메시지를 전송하려는 경우, 다른 syslog 서버의 적절한 인터페이스, IP 주소, 프로토콜 및 포트를 사용하여 두 번째 logging host 명령을 실행할 수 있습니다.

- b. (선택 사항) TCP를 통해 이벤트를 SEC로 전송하는 경우 SEC가 중단되었거나 ASA의 로그 대기열이 꽉 차면 새 연결이 차단됩니다. syslog 서버가 백업되고 로그 대기열이 비워지면 새로운 연결이 다시 허용됩니다. TCP 시스템 로그 서버에 대한 연결에 관계없이 새 연결을 허용하려면 이 명령을 사용하여 TCP 연결 시스템 로그 서버가 다운될 때 새 연결을 차단하는 기능을 비활성화합니다.

logging permit-hostdown

예:

```
> logging permit-hostdown
```

단계 2 다음 명령으로 어떤 시스템 로그 메시지를 시스템 로그 서버에 전송할지 지정합니다.

logging trap { severity_level | message_list }

예:

```
> logging trap 3
> logging trap asa_syslogs_to_cloud
```

심각도 레벨 숫자(1~7) 또는 이름을 지정할 수 있습니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 레벨 3, 2, 1에 대해 syslog 메시지를 보냅니다.

message_list 인수는 사용자 지정 이벤트 목록을 생성한 경우 해당 목록의 이름으로 교체됩니다. 사용자 지정 이벤트 목록을 지정할 때는 해당 목록에 있는 시스템 로그 메시지만 보안 이벤트 커넥터로 전송합니다. 위의 예에서 asa_syslogs_to_cloud는 이벤트 목록의 이름입니다.

message_list를 사용하면 Cisco Cloud로 전송되는 syslog 메시지를 엄격하게 정의하여 비용을 절약할 수 있습니다.

message_list를 생성하려면 [사용자 지정 이벤트 목록 생성](#)을 참조하십시오. 데이터 수집 및 스토리지 비용에 대한 자세한 내용은 [데이터 스토리지 요금제](#)를 참조하십시오.

단계 3 (선택 사항) **syslog** 타임스탬프 추가

logging timestamp 명령을 사용하여 syslog 메시지가 ASA에서 생성된 날짜 및 시간을 메시지에 추가합니다. 타임스탬프 값은 **SyslogTimestamp** 필드에 표시됩니다.

예:

```
> logging timestamp
```

Note 버전 9.10(1)부터 ASA는 이벤트 시스템 로그에서 RFC 5424에 따라 타임스탬프를 활성화하는 옵션을 제공합니다. 이 옵션을 활성화하면 syslog 메시지의 모든 타임스탬프가 RFC 5424 형식에 따라 시간을 표시합니다. 다음은 RFC 5424 형식의 샘플 출력입니다.

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from src interface :src IP/src port to dest IP/dest port.
```

단계 4 (선택 사항) **EMBLEM** 형식이 아닌 **syslog** 메시지에 디바이스 ID 포함

디바이스 ID는 특정 ASA에서 전송된 모든 syslog 메시지를 쉽게 구분하는 데 도움이 되는 syslog 메시지에 삽입할 수 있는 ID입니다. 지침은 [디바이스 ID를 EMBLEM 이외 형식 Syslog 메시지에 포함](#)을 참조하십시오.

단계 5 (선택 사항) 액세스 제어 규칙 "**permit**" 이벤트에 대한 로깅 활성화

액세스 제어 규칙이 리소스에 대한 액세스를 거부하면 이벤트가 자동으로 로깅됩니다. 액세스 제어 규칙이 리소스에 대한 액세스를 허용할 때 생성되는 이벤트도 로깅하려면, 액세스 제어 규칙에 대한 로깅을 켜고 심각도 유형을

구성해야 합니다. 개별 네트워크 액세스 제어 규칙에 대한 로깅을 설정하는 방법에 대한 지침은 [Log Rule Activity\(규칙 활동 로깅\)](#)를 참조하십시오.

Note 액세스 제어 규칙 "permit" 이벤트에 대한 로깅을 활성화하면 일일 이벤트 수집 속도를 기반으로 하므로 구매한 데이터 플랜을 더 많이 사용하게 됩니다.

단계 6 로깅 활성화

명령 프롬프트에서 `logging enable`을 입력합니다. ASA에서 로깅은 개별 규칙이 아니라 전체 디바이스에 대해 활성화됩니다.

예:

```
> logging enable
```

Note 현재 CDO는 보안 로깅 활성화를 지원하지 않습니다.

단계 7 시작 구성에 변경 사항 저장

명령 프롬프트에서 `write memory`를 입력합니다. ASA에서 로깅은 개별 규칙이 아니라 전체 디바이스에 대해 활성화됩니다.

예:

```
> write memory
```

관련 정보:

- [SDC 가상 머신에 SEC\(Secure Event Connector\) 설치, on page 46](#)
- [CDO 이미지를 사용하여 SEC 설치](#)

사용자 지정 이벤트 목록 생성

다음 방법 중 하나를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트를 전송할 때 맞춤형 이벤트 목록을 생성합니다.

- [명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송](#)
- [CDO 매크로를 사용하여 Cisco Cloud로 ASA 시스템 로그 이벤트 전송](#)

다음 세 가지 기준에 따라 `message_list`라고도 하는 이벤트 목록을 생성할 수 있습니다.

- 이벤트 클래스
- 심각도
- 메시지 ID

특정 로깅 대상(예: syslog 서버 또는 Secure Event Connector)으로 보낼 사용자 지정 이벤트 목록을 생성하려면 다음 단계를 수행하십시오.

단계 1 **Inventory**(재고 목록) 페이지에서 **Devices**(디바이스) 탭을 클릭합니다.

단계 2 해당 탭을 클릭하고 맞춤형 이벤트 목록에 포함할 시스템 로그 메시지가 있는 **ASA**를 선택합니다.

단계 3 **Device Actions**(디바이스 작업) 창에서 **> Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 4 ASA에 **logging list** 명령을 실행하려면 이 명령 구문을 사용합니다.

```
logging list name { level level [ class message_class ] | message start_id [ -end_id ] }
```

name 인수는 목록의 이름을 지정합니다. *level level* 키워드 및 인수 쌍은 심각도 레벨을 지정합니다. *class message_class* 키워드-인수 쌍은 특정 메시지 클래스를 지정합니다. *message start_id [-end_id]* 키워드-인수 쌍은 개별 시스템 로그 메시지 숫자 또는 숫자 범위를 지정합니다.

Note 심각도 레벨 이름을 **syslog** 메시지 목록의 이름으로 사용하지 마십시오. 금지된 이름에는 긴급, 경고, 중요, 오류, 알림, 정보 및 디버깅이 포함됩니다. 마찬가지로 이벤트 목록 이름의 맨 앞에 이러한 단어의 처음 3개 글자를 사용하지 마십시오. 예를 들어 "err"로 시작하는 이벤트 목록 이름을 사용하지 마십시오.

- 심각도에 따라 이벤트 목록에 **syslog** 메시지를 추가합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 레벨 3, 2, 1에 대해 syslog 메시지를 보냅니다.

예:

```
> logging list asa_syslogs_to_cloud level 3
```

- 다른 기준에 따라 시스템 로그 메시지를 이벤트 목록에 추가합니다.

이전 단계와 동일한 명령을 입력하여 기존 메시지 목록의 이름과 추가 기준을 지정합니다. 목록에 추가할 각 기준에 대한 새로운 명령을 입력합니다. 예를 들어 다음과 같이 목록에 포함할 syslog 메시지에 대한 기준을 지정할 수 있습니다.

- 302013~302018 범위에 해당하는 시스템 로그 메시지 ID.
- 심각도 레벨이 중요 이상인 모든 syslog 메시지(긴급, 경고 또는 중요).
- 심각도 레벨이 경고 이상인 모든 HA 클래스 시스템 로그 메시지(긴급, 알림, 심각, 오류 또는 경고).

예:

```
> logging list asa_syslogs_to_cloud message 302013-302018
> logging list asa_syslogs_to_cloud level critical
> logging list asa_syslogs_to_cloud level warning class ha
```

Note 다음 조건을 하나라도 충족하면 syslog 메시지가 로깅됩니다. syslog 메시지가 조건을 둘 이상 충족하는 경우 메시지는 한 번만 로깅됩니다.

단계 5 시작 구성에 변경 사항 저장

명령 프롬프트에 **write memory**를 입력합니다.

예:

```
> write memory
```

디바이스 ID를 EMBLEM 이외 형식 Syslog 메시지에 포함

EMBLEM 형식이 아닌 시스템 로그 메시지에 디바이스 ID를 포함하도록 ASA를 구성할 수 있습니다. syslog 메시지에 대해 1가지 디바이스 ID 유형만 지정할 수 있습니다. 다음 절차에서 이 절차를 참조합니다.

- 명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송
- CDO 매크로를 사용하여 Cisco Cloud로 ASA 시스템 로그 이벤트 전송

이 디바이스 식별자는 Event Logging(이벤트 로깅) 페이지에 표시되는 시스템 로그 이벤트의 SensorID 필드에 반영됩니다.

단계 1 디바이스 ID를 할당하려는 시스템 로그 메시지가 있는 ASA를 선택합니다.

단계 2 Device Actions(디바이스 작업) 창에서 **>_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 3 디바이스에 **logging device-id** 명령을 실행하려면 이 명령 syntax(명령문)를 사용합니다.

logging device-id { **cluster-id** | **context-name** | **hostname** | **ipaddress***interface_name* [**system**] | **stringtext** }

예:

```
> logging device-id hostname
> logging device-id context-name
> logging device-id string Cambridge
```

context-name 키워드는 현재 컨텍스트의 이름을 디바이스 ID로 사용하도록 지정합니다(다중 컨텍스트 모드에만 적용). 다중 컨텍스트 모드에서 관리자 컨텍스트 모드를 위해 디바이스 ID 로깅을 활성화하는 경우 시스템 실행 공간에서 발생하는 메시지는 시스템의 디바이스 ID를 사용하고 관리자 컨텍스트에서 발생하는 메시지는 관리자 컨텍스트의 이름을 디바이스 ID로 사용합니다.

Note ASA 클러스터에서는 항상 선택된 인터페이스에 대해 기본 유닛 IP 주소를 사용합니다.

cluster-id 키워드는 클러스터에서 개별 ASA 유닛의 부트 구성 고유 이름을 디바이스 ID로 지정합니다.

hostname 키워드는 ASA의 호스트 이름을 디바이스 ID로 사용하도록 지정합니다.

ipaddress interface_name 키워드-인수 쌍은 *interface_name*으로 지정된 인터페이스 IP 주소를 디바이스 ID로 사용하도록 지정합니다. **ipaddress** 키워드를 사용하는 경우 시스템 로그 메시지가 전송되는 인터페이스에 관계없이 디바이스 ID가 지정된 ASA 인터페이스 IP 주소가 됩니다. 클러스터 환경에서 **system** 키워드는 디바이스 ID가 인터페이스의 시스템 IP 주소가 되도록 만듭니다. 이 키워드는 디바이스에서 전송되는 모든 syslog 메시지에 대해 하나의 일관된 디바이스 ID를 제공합니다.

string text 키워드-인수 쌍은 문자열이 디바이스 ID로 사용되도록 지정합니다. 문자열은 최대 16자를 포함할 수 있습니다.

공백 또는 다음 문자를 사용할 수 없습니다.

- &(앰퍼샌드)
- `(작은따옴표)
- "(큰따옴표)

- <(보다 작음)
- >(보다 큼)
- ?(물음표)

단계 4 시작 구성에 변경 사항 저장

명령 프롬프트에 **write memory**를 입력합니다.

예:

```
> write memory
```

ASA 디바이스용 NSEL(Network Security Event Logging)

ASA의 기본 시스템 로그 메시지는 ASA에서 보고한 이벤트가 위협을 나타내는지 여부를 Secure Cloud Analytics에서 판단하는 데 필요한 데이터가 많이 부족합니다. NSEL(Netflow Secure Event Logging)은 해당 데이터와 함께 Secure Cloud Analytics를 제공합니다.

"플로우는 네트워크 디바이스를 통과하는 몇 가지 공통 속성이 있는 패킷의 단방향 시퀀스로 정의됩니다. 이렇게 수집된 플로우는 외부 디바이스인 NetFlow 컬렉터로 내보내집니다. 네트워크 플로우는 매우 세분화됩니다. 예를 들어 플로우 레코드에는 IP 주소, 패킷 및 바이트 수, 타임스탬프, ToS(서비스 유형), 애플리케이션 포트, 입력 및 출력 인터페이스 등의 세부 정보가 포함됩니다."¹

Cisco ASA는 NetFlow 버전 9 서비스를 지원합니다. NSEL의 ASA 구현은 플로우에서 중요한 이벤트를 나타내는 레코드만 내보내는 스테이트풀 IP 플로우 추적 방법을 제공합니다. 스테이트풀 플로우 추적에서 추적된 플로우는 일련의 상태 변경을 거칩니다.

이 문서에서는 CDO 매크로를 사용하여 ASA에 대해 NetFlow를 구성하는 간단한 방법을 설명합니다. [Cisco ASA NetFlow 구현 가이드](#)는 ASA에서 NetFlow를 구성하는 방법에 대한 매우 자세한 설명을 제공하며, 이 콘텐츠와 함께 유용한 리소스를 찾을 수 있습니다.

향후 작업

[CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성](#)으로 이동합니다.

관련 문서

- [CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성](#)
- [ASA에서 NSEL\(NetFlow Secure Event Logging\) 구성 삭제](#)
- [ASA 전역 정책의 이름 확인](#)

1. ("Cisco Systems NetFlow 서비스 내보내기 버전 9." 인터넷 엔지니어링 태스크 포스, 네트워크 워킹 그룹, 코멘트 요청: 3954, 2004년 10월, B. Claise, Ed. <https://www.ietf.org/rfc/rfc3954.txt>)

CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성

ASA는 NSEL(NetFlow Secure Event Logging)을 사용하여 세부 연결 이벤트 데이터를 보고합니다. 양방향 플로우 통계를 포함하는 Secure Cloud Analytics를 이 연결 이벤트 데이터에 적용할 수 있습니다. 이 절차에서는 ASA 디바이스에서 NSEL을 구성하고 이러한 NSEL 이벤트를 플로우 컬렉터로 전송하는 방법을 설명합니다. 이 경우 플로우 컬렉터는 SEC(Secure Event Connector)입니다.

이 절차는 **NSEL** 구성 매크로를 참조합니다.

```

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate {{timeout_rate_in_mins}}
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
flow-export active refresh-interval {{refresh_interval_in_mins}}
class-map {{flow_export_class_name}}
  match {{add_this_traffic_to_class_map}}
policy-map {{global_policy_map_name}}
  class {{flow_export_class_name}}
    flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
service-policy {{global_policy_map_name}} global
logging flow-export-syslogs disable
show run flow-export
show run policy-map {{global_policy_map_name}}
show run class-map {{flow_export_class_name}}

```

다음은 모든 기본값, 클래스 맵의 일반 이름 및 `global_policy`에 추가된 클래스 맵이 포함된 Configure NSEL 매크로의 예입니다. 이러한 절차를 완료하면 매크로는 다음과 유사합니다.

```

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate 60
flow-export delay flow-create 55
flow-export active refresh-interval 1
class-map flow_export_class_map
  match any
policy-map global_policy
  class flow_export_class_map
    flow-export event-type all destination {{SEC_IPv4_address}}
logging flow-export-syslogs disable
show run flow-export
show run policy-map global_policy
show run class-map flow_export_class_map

```

시작하기 전에

다음 정보를 수집합니다.

- 이전에 CDO 매크로로 작업한 적이 없는 경우 다음 항목을 읽어보십시오.
 - [명령줄 인터페이스 매크로](#)
 - [CLI 매크로 편집](#)
 - [CLI 매크로 실행](#)
- ASA에서 데이터를 수신할 SEC의 IPv4 주소
- SEC에 데이터를 보낼 asa의 인터페이스

- NetFlow 이벤트 전송에 사용되는 UDP 포트 번호 SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기, on page 130의 내용을 참조하십시오.
- ASA 전역 정책의 이름 확인, on page 33

워크플로

이 워크플로우에 따라 CDO 매크로를 사용하여 ASA 디바이스에 대한 NSEL을 구성합니다. 각 단계를 수행해야 합니다.

1. NSEL 매크로 구성 열기, on page 27.
2. NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의, on page 28.
3. SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성, on page 29.
4. NSEL 이벤트에 대한 정책 맵 정의, on page 29.
5. 중복된 시스템 로그 메시지 비활성화, on page 30.
6. 매크로 검토 및 전송, on page 32.

향후 작업

NSEL 매크로 구성 열기, on page 27로 이동하여 위의 워크플로를 시작합니다.

NSEL 매크로 구성 열기

Before you begin

이는 더 긴 워크플로의 첫 번째 부분입니다. 시작하기 전에 [CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성](#), on page 26의 내용을 참조하십시오.

단계 1 **Inventory**(인벤토리) 페이지에서 **Devices**(장치) 탭을 클릭합니다.

단계 2 적절한 디바이스 유형 탭을 클릭하고 NSEL(NetFlow Secure Event Logging)을 구성할 ASA를 선택합니다.

단계 3 **Device Actions**(디바이스 작업) 창에서 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 4 Macro(매크로) 별  **Macros** 을 클릭하여 사용 가능한 매크로 목록을 표시합니다.

단계 5 매크로 목록에서 **Configuring NSEL**(NSEL 구성)을 선택합니다.

단계 6 Macro(매크로) 상자에서 **View Parameters**(매개변수 보기)를 클릭합니다.

What to do next

NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의, on page 28를 진행합니다.

NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의

NSEL 메시지는 테넌트에 온보딩한 SEC 중 하나로 전송할 수 있습니다. 이 지침은 매크로의 다음 섹션을 참조합니다.

```
flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate {{timeout_rate_in_mins}}
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
flow-export active refresh-interval {{refresh_interval_in_mins}}
```

Before you begin

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 [CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 26](#)의 내용을 참조하십시오.

단계 1 flow-export destination 명령은 NetFlow 패킷이 전송되는 컬렉터를 정의합니다. 이 경우 SEC로 전송됩니다. 다음 매개변수에 대한 필드를 입력합니다.

- **{{interface}}** - NetFlow 이벤트가 전송되는 ASA의 인터페이스 이름을 입력합니다.
- **{{SEC_IPv4_address}}** - SEC의 IPv4 주소를 입력합니다. SEC는 플로우 컬렉터 역할을 합니다.
- **{{SEC_NetFlow_port}}** - NetFlow 패킷이 전송되는 SEC의 UDP 포트 번호를 입력합니다.

단계 2 flow-export template timeout-rate 명령은 템플릿 레코드가 구성된 모든 출력 대상으로 전송되는 간격을 지정합니다.

- **{{timeout_rate_in_mins}}** - 템플릿을 재전송할 때까지의 시간(분)을 입력합니다. 60분 값을 사용하는 것이 좋습니다. SEC는 템플릿을 처리하지 않습니다. 숫자가 크면 SEC에 대한 트래픽이 줄어듭니다.

단계 3 flow-export delay flow-create 명령은 flow-create 이벤트의 전송을 지정된 시간(초)만큼 지연시킵니다. 이 값은 권장 Active Timeout(활성 시간 초과) 값과 일치하며 ASA에서 내보낸 플로우 이벤트 수를 줄입니다. 이 속도에서 NSEL 이벤트는 연결 종료 시 또는 연결 생성 후 55초 중 더 빠른 시점에 CDO에 처음 표시됩니다. 이 명령이 구성되지 않은 경우 지연이 없으며 플로우가 생성되는 즉시 flow-create 이벤트가 내보내집니다.

- **{{delay_flow_create_rate_in_secs}}** - 플로우 생성 이벤트 전송 간의 지연 시간(초)을 입력합니다. 55초 값을 사용하는 것이 좋습니다.

단계 4 flow-export active refresh-interval 명령은 수명이 긴 플로우에 대한 상태 업데이트가 ASA에서 전송되는 빈도를 정의합니다. 유효한 값은 1분~60분입니다. Flow Update Interval(플로우 업데이트 간격) 필드에서 **flow-export active refresh-interval**을 **flow-export delay flow-create** 간격보다 5초 이상 크게 구성하면 flow-update 이벤트가 flow-creation 이벤트보다 먼저 표시되지 않습니다.

- **{{refresh_interval_in_mins}}**-1분 값을 사용하는 것이 좋습니다. 유효한 값은 1분~60분입니다.

What to do next

SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성, on page 29를 진행합니다.

SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성

매크로의 다음 명령은 클래스의 모든 NSEL 이벤트를 그룹화한 다음 해당 클래스를 SEC(Secure Event Connector)로 내보냅니다. 이 지침은 매크로의 다음 섹션을 참조합니다.

```
class-map {{flow_export_class_name}}
match {{add_this_traffic_to_class_map}}
```

Before you begin

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 [CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 26](#)의 내용을 참조하십시오.

단계 1 class-map 명령은 SEC로 내보낼 NSEL 트래픽을 식별하는 클래스 맵의 이름을 지정합니다.

- **{{flow-export-class-name}}**- 클래스 맵의 이름을 입력합니다. 이름의 길이는 최대 40자입니다. "class-default"라는 이름 그리고 "_internal" 또는 "_default"로 시작하는 모든 이름은 예약되어 있습니다. 모든 유형의 클래스 맵은 동일한 네임스페이스를 사용하므로, 다른 클래스 맵 유형에서 사용된 이름을 재사용할 수 없습니다.

단계 2 클래스 맵과 연결될(일치하는) 트래픽을 식별합니다. **{{add_this_traffic_to_class_map}}**의 값에 대해 다음 옵션 중 하나를 선택합니다.

- **{{add_this_traffic_to_class_map}}** 필드에 **any**를 입력합니다. NSEL 트래픽에 대한 모든 트래픽 유형을 모니터링합니다. "any" 값을 사용하는 것이 좋습니다.
- **{{add_this_traffic_to_class_map}}** 필드에 **access-list name-of-access-list**를 입력합니다. 이렇게 하면 생성한 액세스 목록과 연결된 모든 트래픽이 연결됩니다. 자세한 내용은 [Cisco ASA NetFlow 구현 가이드](#)에서 [모듈러 정책 프레임워크를 통한 플로우 내보내기 구성](#)을 참조하십시오.

What to do next

NSEL 이벤트에 대한 정책 맵 정의, on page 29를 계속합니다.

NSEL 이벤트에 대한 정책 맵 정의

이 작업은 이전 작업에서 생성한 클래스에 NetFlow 내보내기 작업을 할당하고 새 정책 맵에 클래스를 할당합니다. 이 지침은 매크로의 다음 섹션을 참조합니다.

```
policy-map {{global_policy_map_name}}
class {{flow_export_class_name}}
flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
```

Before you begin

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 [CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성](#), [on page 26](#)의 내용을 참조하십시오.

단계 1 **policy-map** 명령은 policy-map을 생성합니다. 다음 작업에서는 이 정책 맵을 전역 정책과 연결합니다.

- **{{global_policy_map_name}}** - 정책 맵의 이름을 입력합니다. 방화벽의 기존 전역 정책 이름(있는 경우)을 사용하는 것이 좋습니다. 전역 정책의 기본 이름은 **global_policy**입니다. [ASA 전역 정책의 이름 확인](#)을 참조하십시오. [Cisco ASA NetFlow 구현 가이드의 Configure Flow-Export Actions Through Modular Policy Framework\(모듈형 정책 프레임워크를 통한 플로우 내보내기 작업 구성\)](#)에 따라 새 정책 맵을 생성하고 전역적으로 적용하는 경우 나머지 검사 정책은 비활성화됩니다.

단계 2 **class** 명령은 [SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성](#), [on page 29](#)에서 생성한 클래스 맵의 이름을 상속합니다.

단계 3 **flow-export event-type {{event-type}} destination {{IPv4_address}}** 명령은 플로우 컬렉터(이 경우 SEC)로 전송해야 하는 이벤트 유형을 정의합니다.

- **{{event-type}}** - event_type 키워드는 필터링되는 지원 이벤트의 이름입니다. **"all"** 값을 사용하는 것이 좋습니다.
- **{{SEC_IPv4_address}}** - SEC의 IPv4 주소입니다. 해당 값은 [NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의](#), [on page 28](#)에 입력한 값에서 상속됩니다.

What to do next

[중복된 시스템 로그 메시지 비활성화](#), [on page 30](#)를 계속합니다.

중복된 시스템 로그 메시지 비활성화

이 지침은 매크로의 이 섹션을 참조합니다. 명령을 수정할 필요가 없습니다.

```
logging flow-export-syslogs disable
```

NetFlow를 활성화하여 플로우 정보를 내보내면 다음 표의 시스템 로그 메시지가 중복됩니다. 동일한 정보를 NetFlow를 통해 내보내므로 성능을 위해 중복 시스템 로그 메시지를 비활성화하는 것이 좋습니다.



Note NSEL 및 시스템 로그 메시지가 모두 활성화된 경우 두 로깅 유형 간에 시간순으로 정렬되지 않습니다.

Syslog 메시지	설명	NSEL 이벤트 ID	NSEL 확장 이벤트 ID
106100	ACL(액세스 제어 규칙)이 발생할 때마다 생성됨	1 — 플로우가 생성됨 (ACL에서 플로우를 허용한 경우) 3 — 플로우가 거부됨 (ACL에서 플로우를 거부한 경우)	0 — ACL이 플로우를 허용한 경우 1001 — 인그레스 ACL에서 플로우를 거부함 1002 — 이그레스 ACL에서 플로우를 거부함
106015	첫 번째 패킷이 SYN 패킷이 아니므로 TCP 플로우가 거부됨	3 — 플로우가 거부됨	1004 — 첫 번째 패킷이 TCP SYN 패킷이 아니므로 플로우가 거부됨
106023	access-group 명령을 통해 인터페이스에 연결된 ACL에서 플로우를 거부한 경우	3 — 플로우가 거부됨	1001 — 인그레스 ACL에서 플로우를 거부함 1002 — 이그레스 ACL에서 플로우를 거부함
302013, 302015, 302017, 302020	TCP, UDP, GRE, ICMP 연결 생성	1 — 플로우가 생성됨	0 — 무시함
302014, 302016, 302018, 302021	TCP, UDP, GRE, ICMP 연결 해제	2 — 플로우가 삭제됨	0 — 무시함 >2000 — 플로우가 해제됨
313001	디바이스에 대한 ICMP 패킷이 거부됨	3 — 플로우가 거부됨	1003 — 구성으로 인해 To-the-box 플로우가 거부됨
313008	디바이스에 대한 ICMP v6 패킷이 거부됨	3 — 플로우가 거부됨	1003 — 구성으로 인해 To-the-box 플로우가 거부됨
710003	디바이스 인터페이스에 대한 연결 시도가 거부됨	3 — 플로우가 거부됨	1003 — 구성으로 인해 To-the-box 플로우가 거부됨

중복 시스템 로그 메시지를 비활성화하지 않으려면 이 매크로를 편집하고 이 줄만 삭제할 수 있습니다.

logging flow-export-syslogs disable

NetFlow 관련 시스템 로그 메시지 비활성화 및 다시 활성화의 절차에 따라 나중에 개별 시스템 로그 메시지를 활성화하거나 비활성화할 수 있습니다.

매크로 검토 및 전송

Before you begin

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 [CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 26](#)의 내용을 참조하십시오.

단계 1 매크로의 필드를 입력한 후 **Review**(검토)를 클릭하여 ASA로 전송되기 전에 명령을 검토합니다.

단계 2 명령에 대한 응답이 만족스러우면 **Send**(전송)를 클릭합니다.

단계 3 명령을 전송한 후 "일부 명령이 실행 중인 구성을 변경했을 수 있습니다."라는 메시지와 함께 두 개의 링크가 표시될 수 있습니다.

⚠ Some commands may have made changes to the running config

[Write to Disk](#) [Dismiss](#)

- **Write to Disk**(디스크에 쓰기)를 클릭하면 이 명령으로 수행한 변경 사항과 실행 중인 구성의 다른 모든 변경 사항이 디바이스의 시작 구성에 저장됩니다.
- **Dismiss**(해제)를 클릭하면 메시지가 사라집니다.

[CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 26](#)에 설명된 워크플로우를 완료했습니다.

ASA에서 NSEL(NetFlow Secure Event Logging) 구성 삭제

이 절차에서는 SEC(Secure Event Connector)를 NSEL 플로우 컬렉터로 지정하는 ASA에서 NSEL(NetFlow Secure Event Logging) 구성을 삭제하는 방법을 설명합니다. 이 절차에서는 [CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성](#)에 설명된 매크로를 반대로 수행합니다.

이 절차는 **DELETE NSEL** 매크로를 참조합니다.

```
policy-map {{flow_export_policy_name}}
no class {{flow_export_class_name}}
no class-map {{flow_export_class_name}}
no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}
no flow-export template timeout-rate {{timeout_rate_in_mins}}
no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
no flow-export active refresh-interval {{refresh_interval_in_mins}}
logging flow-export-syslogs enable
show run flow-export
show run policy-map {{flow_export_policy_name}}
show run class-map {{flow_export_class_name}}
```

DELETE-NSEL 매크로 열기

단계 1 **Inventory**(인벤토리) 페이지에서 **Devices**(장치) 탭을 클릭합니다.

단계 2 적절한 디바이스 유형 탭을 클릭하고 NSEL(NetFlow Secure Event Logging) 구성을 삭제할 ASA를 선택합니다.

단계 3 **Device Actions**(디바이스 작업) 창에서 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 4 매크로 별표(★ Macros)를 클릭하여 사용 가능한 매크로 목록을 표시합니다.

단계 5 매크로 목록에서 **DELETE-NSEL**을 선택합니다.

단계 6 Macro(매크로) 상자에서 **View Parameters**(매개변수 보기)를 클릭합니다.

매크로에 값을 입력하여 No 명령 완료

ASA CLI는 명령의 "no" 형식을 사용하여 삭제합니다. 매크로의 필드를 입력하여 명령의 "no" 형식을 완성합니다.

단계 1 `policy-map {{flow_export_policy_name}}`

- **{{flow_export_policy_name}}** - 정책 맵 이름의 값을 입력합니다.

단계 2 `no class {{flow_export_class_name}}`

- **{{flow_export_class_name}}** - 클래스 맵 이름의 값을 입력합니다.

단계 3 `no class-map {{flow_export_class_name}}`

- **{{flow_export_class_name}}** - 클래스 맵 이름의 값이 위의 단계에서 상속됩니다.

단계 4 `no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}`

- **{{interface}}** - NetFlow 이벤트가 전송된 ASA의 인터페이스 이름을 입력합니다.
- **{{IPv4_address}}** - SEC의 IPv4 주소를 입력합니다. SEC는 플로우 컬렉터 역할을 합니다.
- **{{NetFlow_port}}** - NetFlow 패킷이 전송되는 SEC의 UDP 포트 번호를 입력합니다.

단계 5 `no flow-export template timeout-rate {{timeout_rate_in_mins}}`

- **{{timeout_rate_in_mins}}** - flow-export 템플릿 제한 시간을 입력합니다.

단계 6 `no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}`

- **{{delay_flow_create_rate_in_secs}}** - flow-export 지연 흐름 생성 속도를 입력합니다.

단계 7 `no flow-export active refresh-interval {{refresh_interval_in_mins}}`

- **{{refresh_interval_in_mins}}** - flow-export 활성 새로 고침 간격을 입력합니다.

ASA 전역 정책의 이름 확인

ASA의 전역 정책 이름을 확인하려면 다음 절차를 수행합니다.

단계 1 **Inventory**(재고 목록) 페이지에서 전역 정책의 이름을 찾을 디바이스를 선택합니다.

단계 2 Device Actions(디바이스 작업) 창에서 **>_Command Reference**(명령 참조)를 선택합니다.

단계 3 Command Line Interface(명령줄 인터페이스) 창의 프롬프트에 다음을 입력합니다.

```
show running-config service-policy
```

아래 예의 출력에서 global_policy는 전역 정책의 이름입니다.

예:

```
> show running-config service-policy
```

```
service-policy global_policy global
```

NSEL 데이터 플로우 문제 해결

CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성을 했으면 다음 절차를 사용하여 NSEL 이벤트가 사용자 ASA에서 Cisco Cloud로 전송되고 Cisco Cloud가 이를 수신하는지 확인합니다.

ASA가 NSEL 이벤트를 SEC(보안 이벤트 커넥터)로 보낸 다음 Cisco Cloud로 보내도록 구성된 후에는 데이터가 즉시 흐르지 않습니다. NET에서 생성되는 NSEL 관련 트래픽이 있다고 가정하면 첫 번째 NSEL 패킷이 ASA에 도착하는 데 몇 분 정도 걸릴 수 있습니다.



Note 이 워크플로우는 "flow-export counters" 명령 및 "capture" 명령을 사용하여 NSEL 데이터 플로우 문제를 해결하는 방법을 보여줍니다. 이러한 명령 사용에 대한 자세한 내용은 [CLI Book 1: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드](#)의 "패킷 캡처" 및 [Cisco ASA NetFlow 구현 가이드](#)의 "NSEL 모니터링"을 참조하십시오.

다음 세 가지 작업을 수행합니다.

- NetFlow 패킷이 SEC로 전송되고 있는지 확인
- Cisco Cloud에서 NetFlow 패킷을 수신하고 있는지 확인

NSEL 이벤트가 SEC로 전송되고 있는지 확인

두 명령 중 하나를 사용하여 NSEL 패킷이 SEC로 전송되고 있는지 확인합니다.

- flow-export counters
- capture

"flow-export counters" 명령을 사용하여 전송되는 flow-export 패킷 및 NSEL 오류 확인

- NSEL 이벤트를 SEC로 전송하도록 ASA를 구성했는지 확인합니다 [CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성](#)을 참조하십시오.

- SEC IP 주소는 NSEL 이벤트의 플로우 컬렉터 주소입니다. 테넌트에 둘 이상의 SEC를 온보딩한 경우 올바른 IP 주소를 사용하고 있는지 확인합니다.
- NetFlow 이벤트를 전달하는 데 사용되는 UDP 포트 번호를 찾습니다. [SaaS\(Secure Logging Analytics\)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기](#)를 참조하십시오.
- NSEL 이벤트를 전송하는 ASA에서 권장되는 인터페이스는 관리 인터페이스입니다. 인터페이스가 다를 수 있습니다.

CDO의 [명령줄 인터페이스](#)를 사용하여 NSEL에 대해 구성된 ASA에 이러한 명령을 전송합니다.

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 적절한 디바이스 탭을 클릭하고 NSEL 이벤트를 SEC로 전송하도록 구성된 ASA를 선택합니다.

단계 4 **Device Actions**(장치 작업) 창에서 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 5 `clear flow-export counters` 명령을 실행하여 플로우 내보내기 카운터를 재설정합니다. 이렇게 하면 새 이벤트가 수신되는지 쉽게 확인할 수 있도록 `clear export flow` 카운터가 0으로 재설정됩니다.

예시:

```
> clear flow-export counters
```

```
Done!
```

단계 6 NSEL 패킷의 대상, 전송된 패킷 수 및 오류를 확인하려면 `show flow-export counters` 명령을 실행합니다.

예시:

```
>show flow-export counters
```

```
대상: management 209.165.200.225 10425
```

```
Statistics:
```

```
packets sent 25000
```

```
오류:
```

```
block allocation errors 0
```

```
invalid interface 0
```

```
template send failure 0
```

```
no route to collector 0
```

```
source port allocation 0
```

위의 출력에서 목적지 줄은 NSEL 이벤트가 전송된 ASA의 인터페이스, SEC의 IP 주소, SEC의 포트 10425를 보여줍니다. 또한 25000의 전송된 패킷도 표시 됩니다.

오류가 없고 패킷이 전송되는 경우 아래의 [Cisco Cloud에서 NetFlow 패킷을 수신하고 있는지 확인](#)으로 건너뛰십시오.

오류 설명:

- **block allocation errors**(블록 할당 오류) -블록 할당 오류가 수신되면 ASA가 플로우 익스포터에 메모리를 할당하지 않은 것입니다.
 - 복구 작업: Cisco TAC(Technical Assistance Center)에 문의합니다.
- **invalid interface**(잘못된 인터페이스) - NSEL 이벤트를 SEC로 전송하려고 하지만 플로우 내보내기에 대해 정의한 인터페이스가 전송하도록 구성되지 않았음을 나타냅니다.
 - 복구 작업: NSEL을 구성할 때 선택한 인터페이스를 검토합니다. 관리 인터페이스를 사용하는 것이 좋습니다. 사용자의 인터페이스는 다를 수 있습니다.
- **template send failure**(템플릿 전송 실패) - NSEL을 정의해야 하는 템플릿이 올바르게 구문 분석되지 않았습니니다.
 - 복구 작업: [Defense Orchestrator 지원에 문의하십시오.](#)
- **no route to collector**(컬렉터에 대한 경로 없음)-ASA에서 SEC로의 네트워크 경로가 없음을 나타냅니다
 - 복구 작업:
 - NSEL을 구성할 때 SEC에 사용한 IP 주소가 올바른지 확인합니다.
 - SEC의 상태가 Active(활성)이고 최근 하트비트를 전송했는지 확인합니다. [SDC에 연결할 수 없음](#)을 참조하십시오.
 - 보안 디바이스 커넥터의 상태가 Active(활성)이고 최근 하트비트를 전송했는지 확인합니다.
- **source port allocation**(소스 포트 할당) - ASA에 잘못된 포트가 있음을 나타낼 수 있습니다.

"capture" 명령을 사용하여 ASA에서 SEC로 전송된 NSEL 패킷 캡처

- NSEL 이벤트를 SEC로 전송하도록 ASA를 구성했는지 확인합니다 [CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성](#)을 참조하십시오.
- SEC IP 주소는 NSEL 이벤트의 플로우 컬렉터 주소입니다. 테넌트에 둘 이상의 SEC를 온보딩한 경우 올바른 IP 주소를 사용하고 있는지 확인합니다.
- NetFlow 이벤트를 전달하는 데 사용되는 UDP 포트 번호를 찾습니다. [SaaS\(Secure Logging Analytics\)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기](#)를 참조하십시오.
- NSEL 이벤트를 전송하는 ASA에서 권장되는 인터페이스는 관리 인터페이스입니다. 인터페이스가 다를 수 있습니다.

CDO의 [명령줄 인터페이스](#)를 사용하여 NSEL에 대해 구성한 ASA에 이러한 명령을 전송합니다.

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 NSEL 이벤트를 SEC로 전송하도록 구성된 ASA를 선택합니다.

단계 4 **Device Actions**(디바이스 작업) 창에서 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 5 명령 창에서 이 **capture** 명령을 실행합니다.

```
>capture capture_name interface interface_name match udp any host IP_of_SEC eq NetFlow_port
```

어디에서

- *capture_name*은 패킷 캡처의 이름입니다.
- *interface_name*은 NSEL 패킷이 ASA를 나가는 인터페이스의 이름입니다.
- *IP_of_SEC*는 SEC VM의 IP 주소입니다.
- *NetFlow_port*는 NSEL 이벤트가 전송되는 포트입니다.

이렇게 하면 패킷 캡처가 시작됩니다.

단계 6 캡처된 패킷을 보려면 **show capture** 명령을 실행합니다.

```
> show capture capture_name
```

여기서 *capture_name*은 이전 단계에서 정의한 패킷 캡처의 이름입니다.

다음은 캡처 시간, 패킷이 전송된 IP 주소, IP 주소 및 패킷이 전송된 포트를 표시하는 출력의 예입니다. 이 예에서 192.168.25.4는 SEC의 IP 주소이고 포트 10425는 NSEL 이벤트를 수신하는 SEC의 포트입니다.

캡처된 6개의 패킷

```
1: 14:23:51.706308 192.168.0.169.16431 > 192.168.25.4.10425: udp 476
2: 14:23:53.923017 192.168.0.169.16431 > 192.168.25.4.10425: udp 248
3: 14:24:07.411904 192.168.0.169.16431 > 192.168.25.4.10425: udp 1436
4: 14:24:07.411920 192.168.0.169.16431 > 192.168.25.4.10425: udp 1276
5: 14:24:21.021208 192.168.0.169.16431 > 192.168.25.4.10425: udp 112
6: 14:24:27.444755 192.168.0.169.16431 > 192.168.25.4.10425: udp 196
```

단계 7 패킷 캡처를 수동으로 중지하려면 **capture stop** 명령을 실행합니다.

```
> capture capture_name stop
```

여기서 *capture_name*은 이전 단계에서 정의한 패킷 캡처의 이름입니다.

Cisco Cloud에서 NetFlow 패킷을 수신하고 있는지 확인

시작하기 전에

NSEL 이벤트가 ASA에서 전송되고 있는지 확인합니다.

라이브 NSEL 이벤트 확인

라이브 이벤트와 기록 이벤트를 모두 확인합니다.

이 절차에서는 Cisco Cloud가 지난 1시간 내에 수신한 NSEL 이벤트를 필터링합니다.

단계 1 CDO 메뉴에서 분석 > 이벤트를 로깅을 선택합니다.

단계 2 **Live**(라이브) 탭을 클릭합니다.

단계 3 이벤트 필터를 고정으로 엽니다.

단계 4 ASA Events(이벤트) 섹션에서 NetFlow가 선택되어 있는지 확인합니다.

단계 5 NSEL 이벤트를 전송하도록 구성된 ASA의 IP 주소를 Sensor ID(센서 ID) 필드에 입력합니다.

단계 6 필터의 맨 아래에서 "Include NetFlow Events(NetFlow 이벤트 포함)"가 선택되어 있는지 확인합니다.

이전 NSEL 이벤트 확인

이 절차는 Cisco 클라우드가 지정한 기간 내에 수신한 NSEL 이벤트를 필터링합니다.

단계 1 CDO 메뉴에서 분석 > 이벤트를 로깅을 선택합니다.

단계 2 기록 탭을 클릭합니다.

단계 3 이벤트 필터를 고정으로 엽니다.

단계 4 ASA Events(이벤트) 섹션에서 NetFlow가 선택되어 있는지 확인합니다.

단계 5 CDO가 NSEL 이벤트를 수신한 적이 있는지 확인할 수 있도록 시작 시간을 충분히 이전으로 설정합니다.

단계 6 NSEL 이벤트를 전송하도록 구성된 ASA의 IP 주소를 Sensor ID(센서 ID) 필드에 입력합니다.

단계 7 필터의 맨 아래에서 "Include NetFlow Events(NetFlow 이벤트 포함)"가 선택되어 있는지 확인합니다.

구문 분석된 ASA 시스템 로그 이벤트

구문 분석된 시스템 로그 이벤트는 다른 시스템 로그 이벤트보다 더 많은 이벤트 속성을 포함하며, 구문 분석된 특정 필드에서 검색할 수 있습니다. SEC는 지정한 모든 ASA 이벤트를 Cisco Cloud로 전달하지만, 아래 테이블의 시스템 로그 메시지만 구문 애널리틱스됩니다. 구문 분석된 모든 시스템 로그 이벤트는 식별을 돕기 위해 이탤릭체로 표시됩니다.

시스템 로그에 대한 자세한 설명은 [Cisco ASA Series 시스템 로그 메시지](#)를 참조하십시오.

시스템 로그 ID	시스템 로그 범주	시스템 로그 메시지의 목적
106015	방화벽	상태가 잘못된 TCP 거부를 나타냅니다.

시스템 로그 ID	시스템 로그 범주	시스템 로그 메시지의 목적
106023	방화벽	실제 IP 패킷이 ACL에 의해 거부되었습니다. 이 메시지는 ACL에 대해 로그 옵션을 활성화하지 않은 경우에도 나타납니다.
106100	액세스 목록/사용자 세션	패킷이 ACL에 의해 허용되거나 거부되었습니다.
113019	사용자 인증	중요 AnyConnect
302013, 302015, 302017, 302020	사용자 세션	TCP, UDP, GRE 및 ICMP 연결 생성을 위한 연결 시작 및 종료 Syslog.
302014, 302016, 302018, 302021	사용자 세션	TCP, UDP, GRE 및 ICMP 연결 생성을 위한 연결 시작 및 종료 Syslog.
302020 - 302021	사용자 세션	ICMP 세션 설정 및 해제.
305006	사용자 세션/NAT 및 PAT	NAT 연결 실패
305011-305014	사용자 세션/NAT 및 PAT	NAT 빌드/해체 관련
313001, 313008	IP 스택	상자에 거부된 연결을 나타냅니다.
414004	시스템	중요 AnyConnect
609001 - 609002	방화벽	영역에 연결된 호스트 ip-address 에 대해 네트워크 상태 컨테이너가 예약/제거되었습니다.
710002, 710004 710005	사용자 세션	상자 연결 실패
710003	사용자 세션	상자에 거부된 연결을 나타냅니다.
746012, 746013	사용자 세션	중요 AnyConnect

관련 정보:

- 명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송
- 이벤트 로깅 페이지에서 이벤트 검색 및 필터링

클라우드 제공 Firewall Management Center 관리 디바이스에 대한 SAL(SaaS) 구현

이 통합을 구축하려면 시스템 로그 또는 직접 연결을 사용하여 SAL(SaaS)에서 이벤트 데이터 스토리지를 설정해야 합니다.

- 시스템 로그를 사용하여 SAL(SaaS)에 이벤트 전송, 41 페이지
- 직접 연결을 사용하여 SAL(SaaS)에 , 43 페이지

SAL(SaaS) 통합의 요구사항, 지침 및 제한

유형	설명
Cisco Secure Firewall Threat Defense	<ul style="list-style-type: none"> • CDO 관리 독립형 위협 방어 디바이스, 버전 7.2 이상. • 시스템 로그를 사용하여 이벤트를 전송하려면 위협 방어 버전 6.4 이상이 설치되어 있어야 합니다. • 이벤트를 직접 전송하려면 위협 방어 버전 7.2 이상이 설치되어 있어야 합니다. • 방화벽 시스템을 구축하고 이벤트를 성공적으로 생성해야 합니다.
지역 클라우드	<ul style="list-style-type: none"> • 이벤트를 전송할 지역 클라우드를 결정합니다. • 이벤트는 다른 지역 클라우드에서 보거나 이동할 수 없습니다. • Cisco SecureX 또는 Cisco SecureX 위협 방어와 통합하기 위해 클라우드에 이벤트를 전송하기 위해 직접 연결을 사용하는 경우 이 통합에 대해 동일한 클라우드 지역을 사용해야 합니다. • 이벤트를 직접 전송하는 경우 CDO에서 지정하는 지역 클라우드가 CDO 테넌트의 지역과 일치해야 합니다.
데이터 요금제	<ul style="list-style-type: none"> • Cisco Cloud가 매일 위협 방어 디바이스로부터 받는 이벤트 수를 반영하는 데이터 계획을 구입해야 합니다. 이를 일일 수집 속도라고 합니다. • 데이터 스토리지 요구 사항을 예측하려면 로그 볼륨 에스티메이터 툴을 사용합니다.

유형	설명
어카운트	이 통합을 위한 라이선스를 구매하면 통합을 지원하기 위한 CDO 테넌트 계정이 제공됩니다.

시스템 로그를 사용하여 SAL(SaaS)에 이벤트 전송

이 절차에서는 CDO에서 관리하는 디바이스에서 보안 이벤트(연결, 보안 인텔리전스, 침입, 파일 및 악성코드 이벤트)에 대한 시스템 로그 메시지를 전송하기 위한 구성에 대한 정보를 제공합니다.

시작하기 전에

- 보안 이벤트를 생성하도록 정책을 구성하고 표시될 것으로 예상되는 이벤트가 **Analysis(분석)** 메뉴의 해당 테이블에 표시되는지 확인합니다.
- 시스템 로그 서버 IP 주소, 포트 및 프로토콜(UDP 또는 TCP)과 관련된 정보를 수집합니다.
- 디바이스가 시스템 로그 서버에 연결할 수 있는지 확인합니다.

단계 1 CDO에 로그인합니다.

단계 2 CDO 메뉴에서 **Tools & Services(툴 및 서비스)** > **Firewall Management Center**를 클릭하여 **Services(서비스)** 페이지를 엽니다.

단계 3 **Cloud-Delivered FMC(클라우드 제공 FMC)**를 클릭하고 선택한 다음 **Configuration(구성)**을 클릭합니다.

단계 4 위협 방어 디바이스에 대한 시스템 로그 설정을 구성합니다.

- a) **Devices(디바이스)** > **Platform Settings(플랫폼 설정)**을 클릭하고 위협 방어 디바이스와 연결된 플랫폼 설정 정책을 편집합니다.
- b) 왼쪽 탐색 창에서 **Syslog(시스템 로그)**를 클릭하고 다음과 같이 시스템 로그 설정을 구성합니다.

UI 요소를 클릭합니다.	방법은 다음과 같습니다.
로깅 설정	로깅을 활성화하고 FTP 서버 설정 및 플래시 사용량을 지정합니다.
로그 대상	특정 대상에 대한 로깅을 활성화하고 메시지 심각도 수준, 이벤트 클래스 또는 사용자 지정 이벤트 목록에 대한 필터링을 지정합니다.
이메일 설정	이메일로 전송되는 시스템 로그 메시지의 소스 주소로 사용할 이메일 주소를 지정합니다.
이벤트 목록	이벤트 클래스, 심각도 레벨 및 이벤트 ID를 포함하는 사용자 지정 이벤트 목록을 정의합니다.

UI 요소를 클릭합니다.	방법은 다음과 같습니다.
속도 제한	구성된 모든 대상에 전송되는 메시지의 양을 지정하고 속도 제한을 할당할 메시지 심각도 레벨을 정의합니다.
Syslog 설정	로깅 기능을 지정하고 타임스탬프 추가를 활성화하며, 다른 설정을 활성화하여 서버를 시스템 로그 대상으로 설정합니다.
Syslog 서버	로깅 대상으로 지정된 시스템 로그 서버의 IP 주소, 사용된 프로토콜, 형식 및 보안 영역을 지정합니다.

c) **Save**(저장)를 클릭합니다.

단계 5 액세스 제어 정책(파일 및 악성코드 로깅 포함)에 대한 일반 로깅 설정을 구성합니다.

- Policies**(정책) > **Access Control**(액세스 제어)를 클릭한 다음 위협 방어 디바이스와 연결된 액세스 제어 정책을 편집합니다.
- More**(더 보기)를 클릭한 다음 **Logging**(로깅)을 선택합니다. 액세스 제어 정책(파일 및 악성코드 로깅 포함)에 대한 일반 로깅 설정을 다음과 같이 구성합니다.

UI 요소를 클릭합니다.	방법은 다음과 같습니다.
특정 시스템 로그 알림을 사용해 전송	미리 정의된 기존 경고 목록에서 시스템 로그 경고를 선택하거나 이름, 로깅 호스트, 포트, 기능 및 심각도를 지정하여 경고를 추가합니다.
디바이스에 구축된 FTD 플랫폼 설정 정책에 구성된 시스템 로그 설정을 사용합니다.	Platform Settings (플랫폼 설정)에서 구성하여 시스템 로그 구성을 통합하고 액세스 제어 정책에서 설정을 재사용합니다. 선택한 심각도는 모든 연결 및 침입 이벤트에 적용됩니다. 기본 심각도는 ALERT (알림)입니다.
IPS 이벤트에 대한 Syslog 메시지 보내기	이벤트를 시스템 로그 메시지로 전송합니다. 재정의하지 않는 한 기본 시스템 로그 설정이 사용됩니다.
파일 및 악성코드 이벤트에 대한 Syslog 메시지 전송	파일 및 악성코드 이벤트를 시스템 로그 메시지로 전송합니다. 재정의하지 않는 한 기본 시스템 로그 설정이 사용됩니다.

c) **Save**(저장)를 클릭합니다.

단계 6 액세스 제어 정책에 대한 보안 인텔리전스 이벤트에 대한 로깅을 활성화합니다.

- 동일한 액세스 제어 정책에서 **Security Intelligence**(보안 인텔리전스) 탭을 클릭합니다.
- Logging**(로깅)을 클릭하여 다음 기준을 바탕으로 보안 인텔리전스 로깅을 활성화합니다.
 - 도메인 이름 기준 - **DNS Policy**(DNS 정책) 드롭다운 목록 옆에 있는 로깅을 클릭합니다.
 - IP 주소 기준 - **Networks**(네트워크) 옆에 있는 로깅을 클릭합니다.
 - URL 기준 - **URLs** 옆에 있는 로깅을 클릭합니다.

c) **Save**(저장)를 클릭합니다.

단계 7 액세스 제어 정책에서 각 규칙에 대해 syslog 로깅을 활성화합니다.

a) 동일한 액세스 제어 정책에서 **Rules**(규칙) 탭을 클릭합니다.

b) 편집할 규칙을 클릭합니다.

c) 규칙에서 **Logging**(로깅) 탭을 클릭합니다.

d) **Log at beginning of connection**(연결 시작 시 로깅) 및 **Log at end of connection**(연결 종료 시 로깅) 체크 박스를 선택합니다.

e) 파일 이벤트를 로깅하려면 **Log Files**(로그 파일) 체크 박스를 선택합니다.

f) **Syslog Server**(시스템 로그 서버) 체크 박스를 선택합니다.

g) 규칙이 **Using default syslog configuration in Access Control Logging**(액세스 제어 기록에서 기본 시스템 로그 구성 사용)인지 확인합니다.

h) **Save**(저장)를 클릭합니다.

i) 정책의 각 규칙에 대해 7.a~7.h 단계를 반복합니다.

다음에 수행할 작업

필요한 모든 변경을 수행한 경우 매니지드 디바이스에 변경 사항을 구축합니다.

직접 연결을 사용하여 SAL(SaaS)에

SAL(SaaS)에 이벤트를 직접 전송하도록 클라우드 사용 Firewall Management Center를 구성합니다.

시작하기 전에

- 클라우드 제공 Firewall Management Center에 디바이스를 온보딩하고, 이러한 디바이스에 라이선스를 할당하고, 이벤트를 SAL(SaaS)로 직접 전송하도록 이러한 디바이스를 구성합니다.
- 규칙을 수정하고 **Log at Beginning of Connection**(연결 시작 시 로깅) 및 **Log at End of Connection**(연결 종료 시 로깅) 옵션을 선택하여 규칙별로 연결 로깅을 활성화합니다.

단계 1 CDO에 로그인합니다.

단계 2 CDO 메뉴에서 **Tools & Services**(툴 및 서비스) > **Firewall Management Center**를 클릭합니다.

단계 3 **Cloud-Delivered FMC**(클라우드 제공 FMC)를 클릭하고 오른쪽에 있는 **System**(시스템) 창에서 **Cisco Cloud Events**(Cisco 클라우드 이벤트)를 클릭합니다.

단계 4 **Configure Cisco Cloud Events**(Cisco 클라우드 이벤트 구성) 위젯에서 다음을 수행합니다.

1. **Send Events to the Cisco Cloud**(Cisco 클라우드로 이벤트 전송) 토글 버튼을 클릭하여 전체 구성을 활성화합니다.
2. 클라우드로 침입 이벤트를 전송하려면 **Send Intrusion Events to the cloud**(클라우드로 침입 이벤트 전송) 확인란을 선택합니다.

직접 연결을 사용하여 **SAL(SaaS)**에 이벤트 로그를 전송하기 위해 위협 방어 디바이스 활성화 또는 비활성화

3. 파일 및 악성코드 이벤트를 클라우드로 전송하려면 **Send File and Malware Events to the cloud**(파일 및 악성코드 이벤트를 클라우드로 전송) 확인란을 선택합니다.
4. 연결 이벤트를 클라우드로 보내는 옵션을 선택합니다.
 - 연결 이벤트를 클라우드로 전송하지 않으려면 **None**(없음) 라디오 버튼을 클릭합니다.
 - 보안 인텔리전스 이벤트만 클라우드로 전송하려면 **Security Events**(보안 이벤트) 라디오 버튼을 클릭합니다.
 - 모든 연결 이벤트를 클라우드로 전송하려면 **All**(모두) 라디오 버튼을 클릭합니다.
5. **Save**(저장)를 클릭합니다.

직접 연결을 사용하여 **SAL(SaaS)**에 이벤트 로그를 전송하기 위해 위협 방어 디바이스 활성화 또는 비활성화

클라우드 사용 Firewall Management Center에서 관리하는 FTD 디바이스를 활성화하거나 비활성화하여 이벤트를 SAL(SaaS)에 직접 전송합니다. 이러한 디바이스 레벨 제어를 사용하면 선택적으로 특정 FTD 디바이스를 이벤트 로그를 Cisco Cloud로 전송에서 제외하여 트래픽을 줄이거나 SAL 및 온프레미스 이벤트 로그 스토리지의 조합을 유지 관리할 수 있습니다.



참고

- FTD 디바이스에서 Cisco Cloud로 이벤트를 전송하거나 비활성화하려면 클라우드 사용 Firewall Management Center에서 Cisco Cloud 이벤트 전역 설정을 활성화합니다. Cisco 클라우드 이벤트 전역 설정 활성화에 대한 자세한 내용은 [직접 연결을 사용하여 SAL\(SaaS\)로 이벤트를 전송하도록 클라우드 제공 Firewall Management Center 구성](#)을 참조하십시오.

Cisco 클라우드 이벤트 전역 설정이 클라우드 사용 Firewall Management Center에서 활성화된 경우 모든 FTD 디바이스에 대해 Cisco Cloud로 이벤트 전송이 기본적으로 활성화됩니다.

- FTD 디바이스를 활성화하거나 비활성화하여 이벤트 로그를 클라우드로 전송하는 옵션은 FTD 버전 7.4.1 이상에서 지원됩니다.

시작하기 전에

- 클라우드 사용 Firewall Management Center에 디바이스를 온보딩하고, 이러한 디바이스에 라이선스를 할당하고, 이벤트를 SAL(SaaS)로 직접 전송하도록 이러한 디바이스를 구성합니다.
- 규칙을 수정하고 **Log at Beginning of Connection**(연결 시작 시 로깅) 및 **Log at End of Connection**(연결 종료 시 로깅) 옵션을 선택하여 규칙별로 연결 로깅을 활성화합니다.

단계 1 CDO에 로그인합니다.

단계 2 CDO 메뉴에서 **Inventory**(재고 목록)를 클릭합니다.

단계 3 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 4 **FTD** 탭을 클릭합니다.

단계 5 재고 목록에서 구성을 편집할 FTD 디바이스를 선택합니다.

단계 6 **Device Management**(디바이스 관리) 창에서 **Cloud Events**(클라우드 이벤트)를 클릭합니다.

단계 7 **Send Events to the Cisco Cloud**(Cisco 클라우드로 이벤트 전송) 토글 버튼을 클릭하여 구성을 활성화하거나 비활성화합니다.

단계 8 **Save**(저장)를 클릭합니다.

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:

- [ASA에 대한 SAL SaaS\(Security Analytics and Logging\) 정보](#)
- [SDC 가상 머신에 SEC\(Secure Event Connector\) 설치, 46 페이지](#)
- [VM 이미지를 사용하여 SEC 설치](#)
- [VM 이미지를 사용하여 SEC 설치](#)
- [Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치, 64 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, 56 페이지](#)
- [CDO 이미지를 사용하여 SEC 설치, 49 페이지](#)
- [Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치, 64 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, 49 페이지](#) 또는 [VM 이미지를 사용하여 SEC 설치, 56 페이지](#)의 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 로깅을 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 구성](#)이 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 활성화인지 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.

단계 1 CDO에 로그인합니다.

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

단계 3 과란색 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 복

Deploy an On-Premises Secure Event Connector

```
dRaU9pSmhNM1UxWTJVMFppMDNNakZrTFRSaFpUVXRPV013TkMweU5UZG10VE5oTWpnMU9HVW1MQ0pq
YkdsbGJuUmZhV1FpT21KaGNHa3RZMnhwW1c1ME1uMC5tTzh0bTZM1N6cjI4b1ZGZERqYjJNRzVqUE
ZmYTZQYzVsRjRITt1teVVEVzh2Qk5FWW44c3V0Z3NTQU00TH15N0xzVgSydEx4N05nbS00STB6SmZ6
aWdQTKRiV1RsRW1tcjI5SkFVZ2NBWEhySkdzckMREszUnJUM0hZU3JkZ21Hd1dGb3FwWUdZnkJHRU
VacmI0YVFLSjFTdnJ5RjVFZ2FqajZFZkNVaERNMUE3Q3c1Q0p1Sn1JMnFzbGpNUzBXeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXR1QTFsYmE3VkxN0Up4bk9RS1pqaW
1rdDNsYnRRbDNrTHMxeWduaXdVU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YwDpbmCuZGV2LmXvY2toYXJ0Lm
1vIgpDRE9fVEVQU5UPSJDRE9fY2lZy28tYW1hbGxpbYIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
0i8vc3RhZ21uZy5kZXlYubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2lZy28tYW1hbGxpbY
IKT05MWV9FVkvOVE10Rz0idHJ1ZSIK
```

[Copy CDO Bootstrap Data](#)

Step 2

Read the [instructions](#) about deploying the Secure Event Connector on vSphere.
Copy the bootstrap data below and paste it when prompted for "SEC bootstrap Data".

⚠ The SEC bootstrap data is valid until 10/13/2021, 10:44:14 AM

```
U1NFX0RFVklDRV9JRd0iZTBhZTJkNmMtMDdhYy00Y2JkLWEzNWQtOGYzZDJKMjQ1ZmU3IqPTU0VfRE
U0VFT1RQPSI5Y2IzNTI4ZWZlMzg0TQ2NjVjMDFkZmEyYjUyMGUxNSIKVEVOQU5UX05BTUU9IKNET1
9jaXNjby1hbWFSbG1vIg==
```

[Copy SEC Bootstrap Data](#)

Step 3

Verify the connection status of the new SEC by exiting this dialog and checking the "Last Heartbeat" information.

Cancel

OK

사합니다.

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

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

```
[sdc@sdcm-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
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUIhoJpojP9UOoiUY8VHHGFXREWRtygfhVjkhOuihIuyftyXtfcghvjbkhB=
```

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.

```

=====
Running SEC health check for tenant [redacted]
-----
SEC cloud URL [redacted] is: Reachable
-----
SEC Connector status: Active
-----
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
-----
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in
=====

```

등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 [보안 이벤트 커넥터 온보딩 장애 문제 해결](#)로 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](#), 61 페이지를 계속 진행합니다.
- CDO 이미지를 사용하여 SDC를 설치한 경우 "다음 작업"을 진행합니다.

다음에 수행할 작업

[ASA 디바이스에 대한 SaaS\(Secure Logging Analytics\) 구현](#), 13 페이지 으로 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(Secure Event Connector)는 ASA 및 FTD에서 Cisco Cloud로 이벤트를 전달하므로, 라이선싱에 따라 Event Logging(이벤트 로깅) 페이지에서 해당 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다.

테넌트에 두 개 이상의 SEC(Secure Event Connector)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.

SEC 설치는 2단계로 진행됩니다.

1. [CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치, 50 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, 62 페이지](#).



참고 고유한 VM을 생성하여 CDO 커넥터를 생성하려면 [생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성](#)을 참조하십시오.

다음 작업:

[CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치, 50 페이지](#)를 계속 진행합니다.

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

시작하기 전에

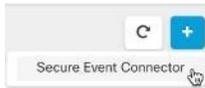
- Cisco Security and Analytics Logging, **Logging and Troubleshooting**(로깅 및 문제 해결) 라이선스를 구매하고, **Logging Analytics and Detection**(로깅 분석 및 탐지), **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수도 있습니다.
원하는 경우 CDO에 로그인하여 Security Analytics and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

단계 1 CDO 커넥터를 생성할 CDO 테넌트에 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 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 adm123입니다.

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

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

단계 12 프롬프트가 표시되면 **cdo** 사용자의 기본 비밀번호 adm123을 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 1 단계에서 CDO 부트스트랩 데이터를 복사합니

Deploy an On-Premises Secure Event Connector
✕

i
SEC will be deployed on a new VM

Step 1

Download the [CDO Connector VM](#) and follow the [documentation](#) to deploy the CDO VM on vSphere. You will be prompted for "CDO Bootstrap Data". Copy the data below and paste it into the CDO Bootstrap Data input field in vSphere.

CDO Bootstrap Data

```
Q0RPX1RPS0V0PSJ1eUpoYkdjaU9pS1NVekkxTm1Jc01uUjVjQ0k2SWtwWFZDSjkuZX1KM1pYSW1PaU
l3SWl3aWMyTnZjR1VpT2xzaWRISjFjM1FpTENKeVpXRmtJaXdPZDNKcGRHVWlMQ0poTTJVMVkyVTBa
aTAzTWpGa0xUUmhaVFV0T1dNd05DMHl0VGRpTlR0aE1qZzFPR1VpWFN3aVlXMXlJam9pYzJGdGJDSX
NjBkp2YkdWek1qcGJJbEpQVEVWZlUxv1FSVkpUUVST1NVNGlYU3dpYVh0ek1qb2lhWFJrSWl3aVky
eDFjM1Jsy2tsa0lqb2lNU0lzSW1sa0lqb2labVF3T0dReVpHVXRNMlZpT1MwMFPYzRMV0kwW1dNdF
pUWXh0V0UyWmpjNFkyUm1JaXdPZyZnWwFtVmpkRlI1Y0dVaU9pSjFjMlZ5SWl3aWFuUnBJam9pTURB
VacmI0YVFLSjFTdnJ5RjVfZ2FqaJZfZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZXlMT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXRlQTFSYmE3VkxNOUp4bk9RS1pqaW
1rdDNsYnRRbDnrTHMxeWduaXdVU1RuWkQxM0c5T2FJWEcCQ093T3NESGdNeHl6UU13ZWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWdpbmcuZGV2LmxvY2toYXJ0Lm
1vIgpDRE9fVEVOQU5UPSJDRE9fY2l2Y28tYW1hbGxpbyIKQ0RPX0JPT1RTVFJBUF9VUkw9Imh0dHBz
Oj8vc3RhZ2l2Zy5kZXUubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2l2Y28tYW1hbGxpby
IKT05MwV9FVkvOVE1ORz0idHJ1ZSIK
```

📄 Copy CDO Bootstrap Data
←

Cancel
OK

다.

단계 26 이 설정을 업데이트하시겠습니까?라는 메시지가 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, 54 페이지](#)를 진행합니다.

Please copy the bootstrap data from Setup Secure Event Connector page of CDO:

KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE

RtyFUiyIOHKnKJbKhvgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjkhOuihIuyftyXtfcghvjbkhB=

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.

```
=====
Running SEC health check for tenant [redacted]
=====
SEC cloud URL [redacted] is: Reachable
SEC Connector status: Active
=====
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
=====
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
=====
```

등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 [SEC 온보딩 실패 문제 해결](#)로 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

[ASA 디바이스에 대한 SaaS\(Secure Logging Analytics\) 구현, 13 페이지](#) 으로 돌아갑니다.

관련 정보:

- [보안 디바이스 커넥터 문제 해결](#)
- [보안 이벤트 커넥터 문제 해결](#)
- [SEC 온보딩 실패 문제 해결](#)

Ubuntu 가상 머신에 보안 이벤트 커넥터 구축

시작하기 전에

Ubuntu 가상 머신에서 보안 디바이스 커넥터 및 보안 이벤트 커넥터 구축에 설명된 대로 Ubuntu VM에 보안 디바이스 커넥터를 설치해야 합니다.

단계 1 CDO에 로그인합니다.

단계 2 **Tools & Services**(도구 및 서비스) > **Secure Connectors**(보안 커넥터)를 선택합니다.

단계 3 **Services**(서비스) 페이지에서 **Secure Connectors**(보안 커넥터) 탭을 선택하고 를 클릭한 후 **Secure Event Connector**(보안 이벤트 커넥터)를 선택합니다.

단계 4 창의 2단계에서 SEC 부트스트랩 데이터를 메모장에 복사합니다.

단계 5 다음 명령을 실행합니다.

```
[sdc@vm]:~$ sudo su sdc
```

```
sdc@vm:/home/user$ cd /usr/local/cdo/toolkit
```

메시지가 표시되면 복사한 SEC 부트스트랩 데이터를 입력합니다.

```
sdc@vm:~/toolkit$ ./sec.sh setup
```

```
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
Successfully on-boarded SEC
```

보안 이벤트 커넥터가 CDO에서 "활성" 상태가 될 때까지 몇 분 정도 걸릴 수 있습니다.

VM 이미지를 사용하여 SEC 설치

SEC(Secure Event Connector)는 ASA 및 FTD에서 Cisco Cloud로 이벤트를 전달하므로, 라이선싱에 따라 Event Logging(이벤트 로깅) 페이지에서 해당 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다.

테넌트에 두 개 이상의 SEC(Secure Event Connector)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, 56 페이지](#)
2. [생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 61 페이지](#)
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, 49 페이지](#)의 내용을 참조하십시오.

다음 작업:

[VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치, 56 페이지](#)를 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.

이 단계는 SEC(Secure Event Connector)를 설치하고 구성하기 위해 완료해야 하는 3단계 중 첫 번째 단계입니다. 이 절차 후에 다음 절차를 완료해야 합니다.

- [생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 61 페이지](#)

- CDO 커넥터 가상 머신에 보안 이벤트 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 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 연결**을 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 설치 는 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.

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 **sd**)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@sd-vm ~]# useradd cdo
[root@sd-vm ~]# useradd sd -d /usr/local/cdo
```

단계 13 **crontab**을 사용하도록 SDC 사용자를 구성합니다.

```
[root@sd-vm ~]# touch /etc/cron.allow
[root@sd-vm ~]# echo "sd" >> /etc/cron.allow
```

단계 14 **cdo** 사용자의 비밀번호를 생성합니다.

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

단계 15 **cdo** 사용자를 "Wheel" 그룹에 추가하여 관리(**sudo**) 권한을 부여합니다.

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

단계 16 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 **sd** 사용자를 이 그룹에 추가합니다.

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

단계 17 **/etc/docker/daemon.json** 파일이 없는 경우 파일을 생성하고 아래 내용을 입력합니다. 생성되면 **docker** 데몬을 다시 시작합니다.

참고 "group" 키에 입력한 그룹 이름이 [단계 16](#)과 일치하는지 확인합니다.

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

단계 18 현재 **vSphere** 콘솔 세션들 사용하는 경우 **SSH**로 전환하고 **cdo** 사용자로 로그인합니다. 로그인한 후에는 **sd** 사용자로 변경합니다. 암호를 묻는 메시지가 표시되면 **cdo** 사용자의 암호를 입력합니다.

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

단계 19 디렉토리를 **/usr/local/cdo**로 변경합니다.

단계 20 **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.

Deploy an On-Premises Secure Event Connector



i SEC will be deployed on a new VM

Step 1

Download the [CDO Connector VM](#) and follow the [documentation](#) to deploy the CDO VM on vSphere. You will be prompted for "CDO Bootstrap Data". Copy the data below and paste it into the CDO Bootstrap Data input field in vSphere.

CDO Bootstrap Data

```
Q0RPX1RPS0V0PSJ1eUp0YkdjaU9pS1NVekKxTm1Jc01uUjVjQ0k2SWtwWFZDSjkuZX1KM1pYSW1PaU
13SW13aWMYtnZjR1VpT2xzaWRISjFjM1FpTENKeVpXRmtJaXdpZDNKcGRHVW1MQ0poTTJVMVkyVTBa
aTAzTWpGa0xUUhmaVF0T1dNd05DMH10VGRpT1R0aE1qZzFPR1VpWFN3aV1XMX1Jam9pYzJGdGJDSX
NjBkp2YkdWek1qcGJJbEpQVEVWZ1UxV1FSVkpUUVVST1NVNG1YU3dpYVh0ek1qb21hWFJrSW13aVky
eDFjM1JsY2tsa01qb21NU01zSW1sa01qb21abVF3T0dReVpHVXRNM1ZpT1MwMFpEYzRMV0kwW1dNdF
pUWXh0V0UyWmpjNFkyUm1JaXdpYzNWaWFtVmpkR1I1Y0dVaU9pSjFjM1Z5SW13aWFuUnBJam9pTURB
VacmI0YVFLSjFtdnJ5RjVfZ2FqajZfZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBxeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXR1QTFsYmE3VksxNOUp4bk9RS1pqaW
1rdDNsYnRRbDNrTHMxeWduaXdVU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeh16UU13ZWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YwYwYwYwYwYwYwYwYwYwYwYwYw
1vIgpDRE9fVEV0QU5UPSJDRE9fY21zY28tYW1hbGxpbYIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
0i8vc3RhZ21uZy5kZXlYubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY21zY28tYW1hbGxpbY
IKT05MwV9FVkvOVE10Rz0idHJ1ZSIK
```

Copy CDO Bootstrap Data



Cancel

OK

단계 21 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_URL>/sdc/bootstrap/CDO_acm="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"

ONLY_EVENTING="true"
```

단계 22 다음 명령을 실행하여 디코딩된 부트스트랩 데이터의 섹션을 환경 변수로 내보냅니다.

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

단계 23 CDO에서 부트스트랩 번들을 다운로드합니다.

```
[sdc@sdc-vm ~]$ curl -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL" -o $CDO_TENANT.tar.gz
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$ ls -l /usr/local/cdo/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/cdo/CDO_<tenant_name>
```

단계 24 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, 61 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., 62 페이지. 이는 인바운드 이벤트 트래픽을 허용하는 보다 세부적인 접근 방식입니다.

시작하기 전에

이는 SEC를 설치하고 구성하기 위해 완료해야 하는 3단계 중 두 번째 단계입니다. 아직 완료하지 않았다면 이러한 구성을 변경하기 전에 VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치, 56 페이지를 완료합니다.

여기에 설명된 추가 구성 변경 중 하나를 완료한 후 CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치를 완료합니다.

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**를 계속합니다.

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

1. SDC VM의 CLI에 "cdo" 사용자로 로그인합니다.
2. 구성된 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 찾기](#)를 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 활성화 및 영구 규칙으로 설정합니다.

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

4. **CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치**를 계속합니다.

CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치

시작하기 전에

이 단계는 SEC(Secure Event Connector)를 설치하고 구성하기 위해 완료해야 하는 3단계 중 세 번째 단계입니다. 아직 수행하지 않은 경우 이 절차를 계속하기 전에 다음 두 가지 작업을 완료합니다.

- [VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치, 56 페이지](#)
- [생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 61 페이지](#)

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 2단계에서 링크를 클릭하여 **SEC** 부트스트랩 데이터를 복사합니다

Deploy an On-Premises Secure Event Connector



```
dRaU9pSmhNM1UxWTJVMFppMDNNakZrTFRSaFpUVXRPV013TkMweU5UZG10VE5oTWpnMU9HVW1MQ0pq
YkdsbGJuUmZhV1FpT2lKaGNHa3RZMnhwW1c1MEluMC5tTzh0bTZMZ1N6cjI4b1ZGZERqYjJNRzVqUE
ZmYTZYzVsRjRITt1teVVEVzh2Qk5FWW44c3V0Z3NTQUo0TH15N0xzVGsydEx4N05nbS00STB6SmZ6
aWdQTKrIv1RsRW1tcjI5SkFVZ2NBWEhySkdzcktMREszUnJUM0hZU3JkZ21Hd1dGb3FwWUdZnkJHRU
VacmI0YVFLSjFTdnJ5RjVFZ2FqajZFZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXR1QTFsYmE3VksN0Up4bk9RS1pqaW
1rdDNsYnRRbDNrTHMxeWduaXdvU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NFN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWdpbmcuZGV2LmxvY2toYXJ0Lm
1vIgpDRE9fVEV0QU5UPSJDRE9fY2lZy28tYW1hbGxpbYIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
0i8vc3RhZ2lZy5kZXYubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2lZy28tYW1hbGxpbY
IKT05MwV9FVkv0VE10Rz0idHJ1ZSIK
```

[Copy CDO Bootstrap Data](#)

Step 2

Read the [instructions](#) about deploying the Secure Event Connector on vSphere.
Copy the bootstrap data below and paste it when prompted for "SEC bootstrap Data".

⚠ The SEC bootstrap data is valid until 10/13/2021, 10:44:14 AM

```
U1NFx0RFVklDRV9JRD0iZTBhZTJkNmMtMDdhYv0Y2JkLWEzNWQt0GYzZDJkMiq1ZmU3IapTU0VfRE
U0Vft1RQPSI5Y2IzNTI4ZWZ1Mzg0TQ2NjViMDFkZmEyYjUyMGUxNSIKVEV0QU5UX05BTU09IKNET1
9jaXNjby1hbWFSbG1vIg==
```

[Copy SEC Bootstrap Data](#)

Step 3

Verify the connection status of the new SEC by exiting this dialog and checking the "Last Heartbeat" information.

Cancel

OK

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
RtyFUiyIOHKNkJbKhvghyRStwterTyufGUIhoJpojP9UOoiUY8VHGGFXREWRtygfhVjkhOuihIuyftyXtfcghvjbkbB=

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 정책으

```

=====
Running SEC health check for tenant [redacted]
-----
SEC cloud URL [redacted] is: Reachable
-----
SEC Connector status: Active
-----
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
-----
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
=====

```

로 표시됩니다.

등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 [보안 이벤트 커넥터 온보딩 장애 문제 해결](#)로 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. [ASA 디바이스에 대한 SaaS\(Secure Logging Analytics\) 구현, 13 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, 46 페이지](#)의 내용을 참조하십시오.
- SEC를 설치할 때 CDO 부트스트랩 데이터 및 SEC 부트스트랩 데이터를 적어 두십시오.

- 단계 1 Terraform 레지스트리의 [Secure Event Connector Terraform 모듈](#)로 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 3](#)의 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 추가](#)를 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)**를 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 Event Logging(이벤트 로깅) 페이지에서 ASA 또는 FTD 이벤트를 보거나 ASA 또는 FTD 이벤트 및 네트워크 플로우 데이터에 동적 엔터티 모델링 동작 애널리틱스를 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 문의](#)하십시오.

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, 66 페이지](#)의 내용을 참조하십시오.

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, 67 페이지](#)를 진행합니다.

## SDC에서 SEC 파일 제거

이는 SDC에서 보안 이벤트 커넥터를 제거하는 2단계 절차의 두 번째 부분입니다. 시작하기 전에 [보안 이벤트 커넥터 제거, 66 페이지](#)을 참조하십시오.

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.

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**(비밀 번호)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 70를 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 68에서 자세한 내용을 확인하십시오. Secure Cloud Analytics 포털에서 알림으로 작업하려는 경우 자세한 내용은 [CDO에서 Cisco Secure Cloud Analytics 알림 보기](#), on page 70 및 [방화벽 이벤트 기반 알림 작업](#)을 참조하십시오.
- **Total Network Analytics and Monitoring** 라이선스를 구매한 경우 내부 네트워크에 하나 이상의 Secure Cloud Analytics 센서를 구축하여 네트워크 플로우 데이터를 클라우드로 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 69를 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.

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 배포를 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 관리 Secure Firewall Threat Defense 디바이스가 NetFlow 데이터를 전달하도록 구성할 수 있습니다. 센서를 배포할 때, 이벤트 정보를 CDO로 전달하도록 구성된 FDM 관리 Secure Firewall Threat Defense 디바이스에서 NetFlow 데이터를 전달하도록 센서를 구성하지 마십시오.

센서 배포 지침 및 권장 사항은 [Secure Cloud Analytics 센서 설치 설명서](#)를 참조하십시오.

클라우드 기반 배포 구성 지침 및 권장 사항은 [Secure Cloud Analytics 퍼블릭 클라우드 모니터링 가이드](#)를 참조하십시오.



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

Secure Cloud Analytics에 대한 자세한 내용은 [Secure Cloud Analytics 무료 평가판 가이드](#)를 참조하십시오.

다음 단계

- CDO에서 [Cisco Secure Cloud Analytics 알림 보기](#), on page 70를 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 On](#)을 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.

---

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.

---

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 데이터뿐만 아니라 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 엔티티 모델링은 전송하는 트래픽 및 네트워크에서 수행하는 활동을 기반으로 엔티티에 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 엔티티의 최신 모델을 유지하기 위해 엔티티가 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. 엔티티는 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 엔티티와 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 엔티티에 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 73
2. 나중에 분석하기 위해 알림 일시 중지, on page 74
3. 추가 조사를 위해 알림 업데이트, on page 74
4. 알림 검토 및 조사 시작, on page 75
5. 엔터티 및 사용자 검사, on page 77
6. Secure Cloud Analytics를 사용하여 문제 해결, on page 77
7. 알림 업데이트 및 닫기, on page 78

## 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 보기](#)을 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 벗어났습니까?
- 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 알람인 경우 조사를 계속하기 전에 인터넷에서 엔터티를 격리하거나 연결을 닫는 것을 고려하십시오.

## 나중에 분석하기 위해 알람 일시 중지

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

알람 스누즈:

단계 1 **Close Alert**(알람 닫기)를 클릭합니다.

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

단계 3 **Save**(저장)를 클릭합니다.

### What to do next

이러한 알람을 검토할 준비가 되면 다시 알람을 해제할 수 있습니다. 이렇게 하면 상태가 Open(열림)으로 설정되고 다른 Open(열림) 알람과 함께 알람이 표시됩니다.

스누즈된 알람의 스누즈를 해제합니다.

- 스누즈된 알람에서 **Unsnaze Alert**(알람 스누즈 해제)를 클릭합니다.

## 추가 조사를 위해 알람 업데이트

알람 세부 정보를 엽니다.

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

단계 2 알람 유형 이름을 클릭합니다.

### What to do next

초기 분류 및 우선순위에 따라 알람을 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 Cloud**에서 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.

### SUMMARY STEPS

1. 알림 세부사항에서 관찰 유형 옆에 있는 화살표 아이콘(↕)을 클릭하여 해당 유형의 모든 로깅된 관찰을 확인합니다.
2. **All Observations for Network**(네트워크에 대한 모든 관찰) 옆에 있는 화살표 아이콘(↕)을 클릭하여 이 알림의 소스 엔터티에 대해 로깅된 모든 관찰을 확인합니다.

### DETAILED STEPS

**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 엔터티에 대해 로깅된 모든 관찰을 확인합니다.

이러한 관찰에 대한 추가 분석을 수행하려면 쉘표로 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 엔티티와 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 엔티티에 대한 정보를 검토합니다. 지리위치 정보를 검토하고 지리위치 데이터 또는 Umbrella 데이터가 악성 엔티티를 식별하는지 확인합니다. 이러한 엔티티에 의해 생성된 트래픽을 확인합니다. Talos, AbuseIPDB 또는 Google에 이러한 엔티티에 대한 정보가 있는지 확인합니다. 여러 날짜의 IP 주소를 찾고 외부 엔티티가 네트워크의 엔티티와 설정한 다른 유형의 연결을 확인합니다. 필요한 경우 이러한 내부 엔티티를 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 엔티티를 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 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 엔터티 또는 사용자가 네트워크 외부에서 로그인을 시도한 경우 엔터티 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 엔터티를 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 엔터티를 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 엔터티에 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.

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 필터링**과 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.

단계 1 탐색창에서 분석 > 이벤트 로깅을 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 80](#)
- [과거 이벤트 보기, on page 81](#)
- [이벤트 보기 사용자 지정, on page 81](#)

## 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.

### Events

| Date/Time                                        | Event Type |
|--------------------------------------------------|------------|
| ⚙️ Waiting for matching events after 1:38:40 PM. |            |
| May 31, 2019 1:33:35 PM                          | Connection |
| May 31, 2019 1:33:36 PM                          | Connection |
| May 31, 2019 1:33:44 PM                          | Connection |

## 과거 이벤트 보기

Live events(라이브 이벤트) 페이지에는 입력한 [이벤트 로깅 페이지에서 이벤트 검색 및 필터링](#)과 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:

단계 1 탐색창에서 분석 > 이벤트 로깅을 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 메시지](#)를 참조하십시오.
- ASA 이벤트 속성에 대한 전체 설명은 [Cisco ASA Series 시스템 로그 메시지](#)를 참조하십시오.

## 이벤트 보기 사용자 지정

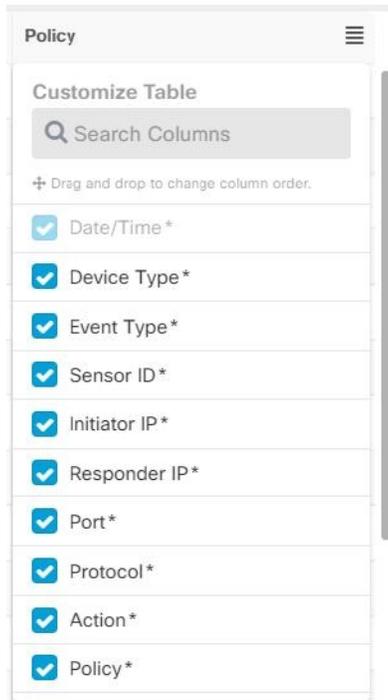
Event Logging(이벤트 로깅) 페이지에 대한 모든 변경 사항은 이 페이지에서 빠져나왔다가 나중에 다시 돌아올 때를 위해 자동으로 저장됩니다.



**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 시스템 로그 이벤트와 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.

단계 1 CDO 탐색 모음에서 분석 > 이벤트 로깅을 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 | ASA(Adaptive Security Appliance)<br>FTD(Firepower Threat Defense) |

| 열 헤더   | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 이벤트 유형 | <p>이 복합 열에는 다음 중 하나가 포함될 수 있습니다.</p> <ul style="list-style-type: none"> <li>• <b>FTD 이벤트 유형</b> <ul style="list-style-type: none"> <li>• <b>Connection(연결)</b> - 액세스 제어 규칙의 연결 이벤트를 표시합니다.</li> <li>• <b>File(파일)</b> - 액세스 제어 규칙의 파일 정책에 의해 보고된 이벤트를 표시합니다.</li> <li>• <b>Intrusion(침입)</b> - 액세스 제어 규칙의 침입 정책에 의해 보고된 이벤트를 표시합니다.</li> <li>• <b>Malware(악성코드)</b> - 액세스 제어 규칙의 악성코드 정책에 의해 보고된 이벤트를 표시합니다.</li> </ul> </li> <li>• <b>ASA Event Types(이벤트 유형)</b> - 이러한 이벤트 유형은 시스템 로그 또는 NetFlow 이벤트의 그룹을 나타냅니다. 어떤 Syslog ID 또는 어떤 NetFlow ID가 어떤 그룹에 포함되어 있는지에 대한 자세한 내용은 <a href="#">ASA 이벤트 유형</a>을 참조하십시오. <ul style="list-style-type: none"> <li>• <b>구문 분석된 이벤트</b> - 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.</li> <li>• <b>ASA NetFlow Event IDs(ASA NetFlow 이벤트 ID)</b>: ASA의 모든 <a href="#">Netflow(NSEL) 이벤트</a>가 여기에 표시됩니다.</li> </ul> </li> </ul> |
| 센서 ID  | <p>센서 ID는 이벤트가 보안 이벤트 커넥터로 전송되는 IP 주소입니다. 이는 일반적으로 Firepower Threat Defense 또는 ASA의 관리 인터페이스입니다.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| 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 responder가 사용하는 포트 또는 ICMP 코드 대상 포트의 값은 이벤트 세부사항의 ResponderPort 값에 해당합니다.                                                                                                             |
| 프로토콜   | 이벤트의 프로토콜을 나타냅니다.                                                                                                                                                                        |

| 열 헤더 | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 작업   | <p>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.</p> <ul style="list-style-type: none"> <li>• 연결 이벤트 유형의 경우 필터는 AC_RuleAction 특성에서 일치 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.</li> <li>• 파일 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.</li> <li>• 침입 이벤트 유형의 경우 필터는 InLineResult 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allowed(허용됨), Blocked(차단됨), Trusted(신뢰할 수 있음)일 수 있습니다.</li> <li>• 악성코드 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Cloud Lookup Timeout(클라우드 조회 시간 초과)일 수 있습니다.</li> <li>• Syslog 및 NetFlow 이벤트 유형의 경우 필터는 Action(작업) 속성에서 일치하는 항목을 검색합니다.</li> </ul> |
| 정책   | 이벤트를 트리거한 정책의 이름입니다. ASA 및 FDM 관리 디바이스마다 이름이 다릅니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

관련 정보:

[이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 118](#)

## 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.

단계 1 주 메뉴에서 분석 > 이벤트 로깅을(를) 선택합니다.

단계 2 모든 값의 Search(검색) 필드를 지웁니다.

단계 3 이벤트 테이블 위에서 과란색 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 118](#)의 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 82](#)의 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 118](#)의 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.

- ASA(Adaptive Security Appliance) 이벤트 속성에 대한 전체 설명은 [Cisco ASA Series 시스템 로그 메시지](#)를 참조하십시오.

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

- 구문 분석된 ASA 시스템 로그 이벤트
- 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 3자리)               |
|--------------|-------------------------------------------|----------------------------------------|
| 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 3자리)                                                                           |
|----------------|----------------------------------------|----------------------------------------------------------------------------------------------------|
| 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, 402, 404, 501, 602, 702, 713, 714, 715                                         |
| 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.

| Historical                                                                                                                                                                                                                                                                                                                                                                       |             | Live                                                                                                                                                                                                                                                       |           |                                                                                                                                                                                                                                                      |              |          |                      |                                                  |        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------|----------------------|--------------------------------------------------|--------|
| Date/Time                                                                                                                                                                                                                                                                                                                                                                        | Event Type  | Sensor ID                                                                                                                                                                                                                                                  | Initiator | Responder                                                                                                                                                                                                                                            | Port         | Protocol | Action               | Policy                                           |        |
| Aug 20, 2019 10:44:14 AM                                                                                                                                                                                                                                                                                                                                                         | Malware     | 192.168.20.53                                                                                                                                                                                                                                              |           |                                                                                                                                                                                                                                                      | 80           | tcp      | Cloud Lookup Timeout | BlockOfficeDocumentsPDFUpload_BlockMalwareOthers |        |
| <b>1</b> Date/Time<br><b>2</b> Application: HTTP<br>ClientApplication: Web browser<br>EventSecond: 1566312254<br>EventType: MalwareEvent<br>FileAction: Cloud Lookup Timeout<br>FileDirection: Download<br>FileName: eicar.com<br>FilePolicy: BlockOfficeDocumentsPDFUpload_BlockMalwareOthers<br>FileSHA256: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f   |             | <b>3</b> FileSize: 68<br>FileType: EICAR<br><b>4</b> FirstPacketSecond: Aug 20, 2019 10:44:08 AM<br>InitiatorIP: [redacted]<br><b>4</b> InitiatorPort: 65386<br>LastPacketSecond: Aug 20, 2019 10:44:14 AM<br>ResponderIP: [redacted]<br>ResponderPort: 80 |           | <b>5</b> SensorID: 192.168.20.53<br>SHA_Disposition: Unavailable<br>SperoDisposition: Spero detection not performed on file<br>ThreatName: Unknown<br>timestamp: Aug 20, 2019 10:44:14 AM<br>URI: /eicar.com<br>Username: No Authentication Required |              |          |                      |                                                  |        |
| Date/Time                                                                                                                                                                                                                                                                                                                                                                        | Device Type | Event Type                                                                                                                                                                                                                                                 | Sensor ID | Initiator IP                                                                                                                                                                                                                                         | Responder IP | Port     | Protocol             | Action                                           | Policy |
| Jun 12, 2020, 7:27:02 AM                                                                                                                                                                                                                                                                                                                                                         | ASA         | 302013                                                                                                                                                                                                                                                     | admin     | 192.168.25.4                                                                                                                                                                                                                                         | 192.168.0.68 | 443      | TCP                  | Built                                            |        |
| <b>6</b> Action: Built<br>ConnectionID: 1169028<br>DeviceType: ASA<br>Direction: inbound<br>EgressInterface: identity<br>EventGroup: session<br>EventGroupDefinition: User Session<br>EventName: Built TCP<br>Message: ASA-6-302013: Built inbound TCP connection 1169028 for management:192.168.25.4/36540 (192.168.25.4/36540) to identity:192.168.0.68/443 (192.168.0.68/443) |             | EventType: 302013<br>IngressInterface: management<br>InitiatorIP: 192.168.25.4<br>InitiatorPort: 36540<br>MappedInitiatorIP: 192.168.25.4<br>MappedInitiatorPort: 36540<br>MappedResponderIP: 192.168.0.68<br>MappedResponderPort: 443                     |           | Protocol: TCP<br>ResponderIP: 192.168.0.68<br>ResponderPort: 443<br>SensorID: admin<br>Severity: Informational<br><b>6</b> SyslogTimestamp: 2020-06-12 11:15:26 +0000 UTC<br>timestamp: Jun 12, 2020, 7:27:02 AM                                     |              |          |                      |                                                  |        |

| Date/Time                    | Device Type             | Event Type | Sensor ID                  | Initiator IP            | Responder IP  | Port                    | Protocol                | Action | Policy |
|------------------------------|-------------------------|------------|----------------------------|-------------------------|---------------|-------------------------|-------------------------|--------|--------|
| Jun 12, 2020, 7:27:13 AM     | ASA                     | 5          | 192.168.0.169              | 192.168.25.4            | 192.168.0.169 | 443                     | TCP                     | Update |        |
| <b>Action</b>                | Update                  |            | <b>InitiatorBytes</b>      | 0                       |               | <b>Protocol</b>         | TCP                     |        |        |
| <b>ConnectionID</b>          | 482168                  |            | <b>InitiatorIP</b>         | 192.168.25.4            |               | <b>ResponderBytes</b>   | 3581                    |        |        |
| <b>DeviceType</b>            | ASA                     |            | <b>InitiatorPackets</b>    | 0                       |               | <b>ResponderIP</b>      | 192.168.0.169           |        |        |
| <b>EgressInterface</b>       | 65535                   |            | <b>InitiatorPort</b>       | 38068                   |               | <b>ResponderPackets</b> | 33                      |        |        |
| <b>EventType</b>             | 5                       |            | <b>LastPacketSecond</b>    | Jun 12, 2020, 7:27:07 A |               | <b>ResponderPort</b>    | 443                     |        |        |
| <b>FirewallExtendedEvent</b> | 2034                    |            |                            | M                       |               | <b>SensorID</b>         | 192.168.0.169           |        |        |
| <b>FirstPacketSecond</b>     | Jun 12, 2020, 7:27:07 A |            | <b>MappedInitiatorIP</b>   | 192.168.25.4            |               | <b>Severity</b>         | Informational           |        |        |
|                              | M                       |            | <b>MappedInitiatorPort</b> | 38068                   |               | <b>timestamp</b>        | Jun 12, 2020, 7:27:13 A |        |        |
| <b>ICMPCode</b>              | 0                       |            | <b>MappedResponderIP</b>   | 192.168.0.169           |               |                         | M                       |        |        |
| <b>ICMPType</b>              | 0                       |            | <b>MappedResponderPort</b> | 443                     |               |                         |                         |        |        |
| <b>IngressInterface</b>      | 9                       |            | <b>NetFlowTimestamp</b>    | 1591961232              |               |                         |                         |        |        |

| 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.<br><br>FirstPacketSecond의 값은 LastPacketSecond에서 ConnectionDuration을 빼서 계산됩니다.<br><br>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. 알람과 함께 Secure Cloud Analytics는 알람을 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 엔티티 모델링은 전송하는 트래픽 및 네트워크에서 수행하는 활동을 기반으로 엔티티에 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 엔티티의 최신 모델을 유지하기 위해 엔티티가 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. 엔티티는 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 알람을 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 엔터티가 도메인 컨트롤러와 일치하는 트래픽을 전송하면 시스템은 해당 엔터티에 도메인 컨트롤러 역할을 할당합니다. 이후에 엔터티가 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 엔터티의 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 엔터티가 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.

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 73](#)
2. [나중에 분석하기 위해 알림 일시 중지, on page 74](#)
3. [추가 조사를 위해 알림 업데이트, on page 74](#)
4. [알림 검토 및 조사 시작, on page 75](#)
5. [엔터티 및 사용자 검사, on page 77](#)
6. [Secure Cloud Analytics를 사용하여 문제 해결, on page 77](#)
7. [알림 업데이트 및 닫기, on page 78](#)

## 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 보기](#)을 참조하십시오.

다음 질문을 합니다.

- 이 알림 유형을 높은 우선순위로 구성했습니까?
- 영향을 받는 서버넷에 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 벗어났습니까?
- 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 엔터티를 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(엔터티의 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:

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 **Unsnaze Alert**(알림 스누즈 해제)를 클릭합니다.

## 추가 조사를 위해 알림 업데이트

알림 세부 정보를 엽니다.

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.

- 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.

### SUMMARY STEPS

- 알림 세부사항에서 관찰 유형 옆에 있는 화살표 아이콘(↕)을 클릭하여 해당 유형의 모든 로깅된 관찰을 확인합니다.
- All Observations for Network**(네트워크에 대한 모든 관찰) 옆에 있는 화살표 아이콘(↕)을 클릭하여 이 알림의 소스 엔터티에 대해 로깅된 모든 관찰을 확인합니다.

### DETAILED STEPS

**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 엔터티에 대해 로깅된 모든 관찰을 확인합니다.

이러한 관찰에 대한 추가 분석을 수행하려면 쉘표로 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.

- 엔터티와 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 엔터티와 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 엔터티는 항상 네트워크 내부에 있습니다. 이를 방화벽 이벤트의 Initiator IP(이니시에이터 IP)와 비교해 보십시오. 이 IP는 연결을 시작한 엔터티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

관찰에서 다른 외부 엔터티에 대한 정보를 검토합니다. 지리위치 정보를 검토하고 지리위치 데이터 또는 Umbrella 데이터가 악성 엔터티를 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 엔터티가 연결을 설정한 외부 엔터티 IP 주소 또는 호스트 이름에 대한 컨텍스트를 검토합니다.

- 이 엔터티에 대한 최근 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **IP Traffic**(IP 트래픽)을 선택합니다.
- 이 엔터티에 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 엔터티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 AbuseIPDB를 선택합니다.
- Cisco Umbrella 웹사이트에서 이 엔터티에 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.

## 알림 업데이트 및 닫기

결과에 따라 태그를 추가합니다.

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, 126 페이지](#)
- [백그라운드에서 기록 이벤트 검색, 126 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, 119 페이지](#)
- [NetFlow 이벤트만 필터링, 121 페이지](#)
- [ASA 또는 FDM-관리 디바이스 시스템 로그 이벤트에 대한 필터링\(ASA NetFlow 이벤트 제외\), 121 페이지](#)
- [필터 요소 결합, 121 페이지](#)

## 라이브 또는 과거 이벤트 필터링

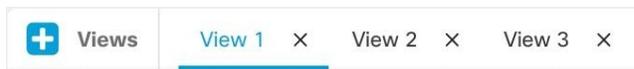
이 절차에서는 이벤트 필터링을 사용하여 Event Logging(이벤트 로깅) 페이지에서 이벤트의 하위 집합을 확인하는 방법을 설명합니다. 특정 필터 기준을 반복적으로 사용하는 경우 사용자 지정 필터를 생성하여 저장할 수 있습니다. 자세한 내용은 [사용자 지정 가능한 이벤트 필터](#)를 참조하십시오.

단계 1 탐색 모음에서 분석 > 이벤트 로깅을 선택합니다.

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

단계 3 필터 버튼 를 클릭합니다. 필터링 열은 고정 아이콘 을 클릭하여 열 수 있습니다.

단계 4 저장된 필터 요소가 없는 View(보기) 탭을 클릭합니다.



단계 5 필터링할 이벤트 세부 정보를 선택합니다.

### • FTD 이벤트

- 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 Events(ASA 이벤트) - 이러한 이벤트 유형은 시스템 로그 또는 NetFlow 이벤트의 그룹을 나타냅니다.

이벤트에 대한 자세한 내용은 [CDO의 이벤트 유형](#)을 참조하십시오.

- 구문 분석된 이벤트 - [구문 분석된 ASA 시스템 로그 이벤트](#)는 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.

- **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 세부정보의 InitiatorPort 값에 해당합니다. (범위 추가 - 시작 포트 종료 포트 및 이니시에이터와 응답자 사이 또는 둘 다 사이에 공백)
  - **Responder**(응답기)-세션 responder가 사용하는 포트 또는 ICMP 코드입니다. 대상 포트의 값은 이벤트 세부사항의 ResponderPort 값에 해당합니다.
- **NetFlow - ASA 디바이스용 NSEL(Network Security Event Logging)** 이벤트는 Syslog 이벤트와 다릅니다. NetFlow 필터는 NSEL 레코드를 생성한 모든 NetFlow 이벤트 ID를 검색합니다. 이러한 "NetFlow 이벤트 ID"는 [Cisco ASA NetFlow 구현 가이드](#)에 정의되어 있습니다.

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

## NetFlow 이벤트만 필터링

이 절차에서는 ASA NetFlow 이벤트만 찾습니다.

- 단계 1 CDO 메뉴 모음에서 분석 > 이벤트 로깅을 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.

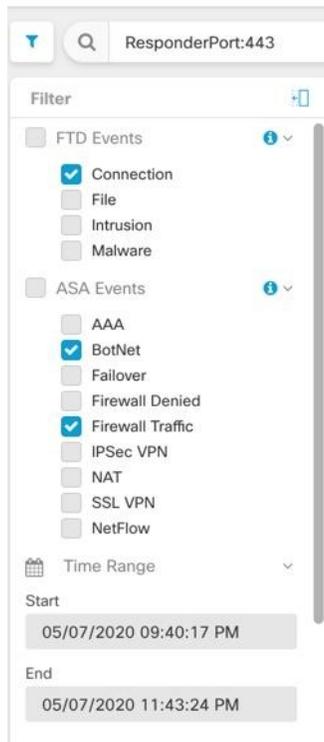
## ASA 또는 FDM-관리 디바이스 시스템 로그 이벤트에 대한 필터링(ASA NetFlow 이벤트 제외)

이 절차에서는 Syslog 이벤트만 찾습니다.

- 단계 1 CDO 메뉴 모음에서 분석 > 이벤트 로깅을 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(ASA 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 과란색으로 표시됩니다. 예를 들면 다음과 같습니다.

## Event Logging

Historical Live

Clear
Time Range After 05/03/2023 07:23:40 PM

+ Views
View 1

| Date/Time               | Device Type | Event Type | Sensor ID / Hostname | Initiator IP |
|-------------------------|-------------|------------|----------------------|--------------|
| May 3, 2023, 7:23:40 PM | ASA         | 3          |                      |              |

|                       |                                      |                     |
|-----------------------|--------------------------------------|---------------------|
| Action                | Deny                                 | IngressACLID        |
| ConnectorID           | 08c0a888-b619-4f1a-a655-d4bd005dd8c8 | IngressInterface    |
| DeviceType            | ASA                                  | InitiatorIP         |
| EgressInterface       | 4                                    | InitiatorPort       |
| EventType             | 3                                    | LastPacketSecond    |
| FirewallExtendedEvent | 1001                                 | MappedInitiatorIP   |
| ICMPCode              | 0                                    | MappedInitiatorPort |
| ICMPType              | 0                                    | MappedResponderIP   |

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 필터가 비어 있고 테이블에서 값을 마우스 오른쪽 버튼으로 클릭하면 다른 값이 없으므로 NOT만 사용할 수 있습니다.

The screenshot shows the 'Event Logging' interface. At the top, there are tabs for 'Historical' and 'Live'. A search bar contains the query: 'InitiatorIP: "10.10.11.11" AND EventType: "3"'. Below the search bar, there is a 'Time Range' filter set to 'After 05/03/2023 07:23:40 PM'. A 'Views' section shows 'View 1' selected. The main table displays event details for May 3, 2023, 7:23:40 PM on an ASA device. A dropdown menu is open over the search bar, showing logical operators: AND, OR, NOT, AND NOT, and OR NOT. The table columns are Date/Time, Device Type, Event Type, Sensor ID / Hostname, and Initiator IP. The table content includes fields like Action (Deny), ConnectorID, DeviceType (ASA), EgressInterface (4), EventType (3), FirewallExtendedEvent (1001), ICMPCode (0), and ICMPType (0). On the right side of the table, there are fields like IngressACLID, IngressInterface, InitiatorIP, InitiatorPort, LastPacketSecond, MappedInitiatorIP, MappedInitiatorPort, and MappedResponderIP.

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 NOT**은 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"
```

**NOT**과 **AND NOT**을 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

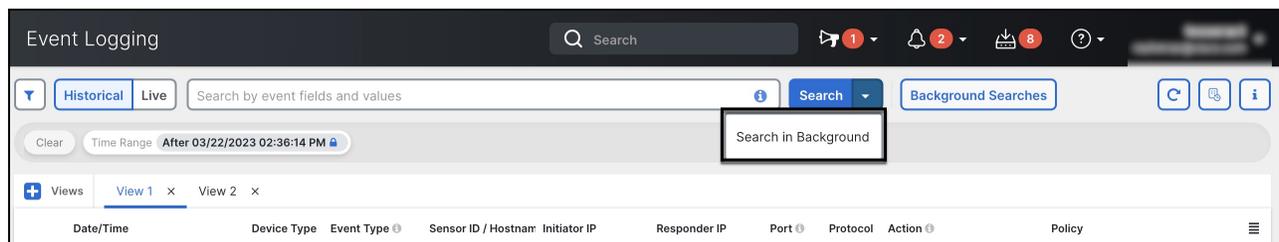
검색 및 백그라운드 검색 기능을 사용하여 Event Logging(이벤트 로깅) 페이지에서 로깅된 모든 이벤트를 볼 수 있습니다. 백그라운드 검색은 기록 이벤트에 대해서만 수행할 수 있습니다.

**단계 1** 탐색 모음에서 분석 > 이벤트 로깅을 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 ✕

[Start a Background Search](#)
[View Notification Settings](#)

| Search Name          | File Size | User              | Status                           | Run Time                                                    | Actions                                           |
|----------------------|-----------|-------------------|----------------------------------|-------------------------------------------------------------|---------------------------------------------------|
| Search_1679428080471 | 3.74 KB   | admin@example.com | Completed<br>(Expires in 5 days) | Started Mar 21, 2023, 3:48:03 PM<br>Completed in 2 seconds  | <a href="#">View</a> <a href="#">Download</a> ... |
| Search_1679428045727 | 3.74 KB   | admin@example.com | Completed<br>(Expires in 5 days) | Started Mar 21, 2023, 3:47:27 PM<br>Completed in 2 seconds  | <a href="#">View</a> <a href="#">Download</a> ... |
| Search_1679427993327 | 2.25 KB   | admin@example.com | Completed<br>(Expires in 5 days) | Started Mar 21, 2023, 3:46:35 PM<br>Completed in 2 seconds  | <a href="#">View</a> <a href="#">Download</a> ... |
| Search_167942230313  | 662 Bytes | admin@example.com | Completed<br>(Expires in 5 days) | Started Mar 21, 2023, 1:58:39 PM<br>Completed in 3 seconds  | <a href="#">View</a> <a href="#">Download</a> ... |
| Search_1679408015574 | 662 Bytes | admin@example.com | Completed<br>(Expires in 5 days) | Started Mar 21, 2023, 10:13:44 AM<br>Completed in 3 seconds | <a href="#">View</a> <a href="#">Download</a> ... |

[Close](#)

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.

다음에 수행할 작업

반복 쿼리가 필요한 경우, 모든 백그라운드 검색을 예약된 백그라운드 검색으로 전환할 수 있습니다. 자세한 내용은 [이벤트 뷰어에서 백그라운드 검색 예약, 127 페이지](#)를 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.

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

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.

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 1년, 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 가이드](#)를 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 **라이선싱**을 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.

단계 1 Cisco Commerce에 사용자 계정으로 로그인합니다.

단계 2 Cisco Defense Orchestrator PID를 선택합니다.

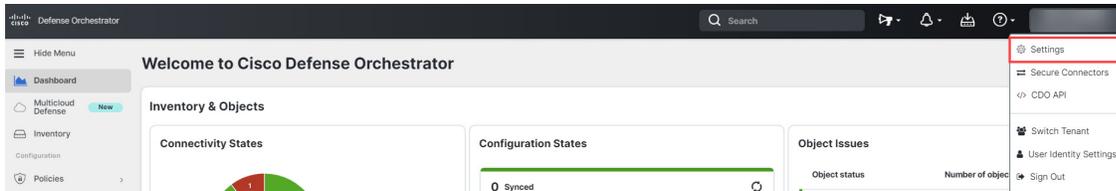
단계 3 프롬프트에 따라 스토리지 용량의 길이 또는 용량을 업그레이드합니다.

증가된 비용은 기존 라이선스의 남은 기간에 따라 비례 배분됩니다. 자세한 지침은 [Secure Logging Analytics\(SaaS\) 주문 가이드](#)를 참조하십시오.

## 보안 애널리틱스 및 로깅 데이터 계획 사용량 보기

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

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 디바이스의 이벤트를 SEC(Secure Event Connector)의 특정 UDP, TCP 또는 NSEL 포트에 전송할 수 있습니다. 그런 다음 SEC는 해당 이벤트를 Cisco 클라우드에 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

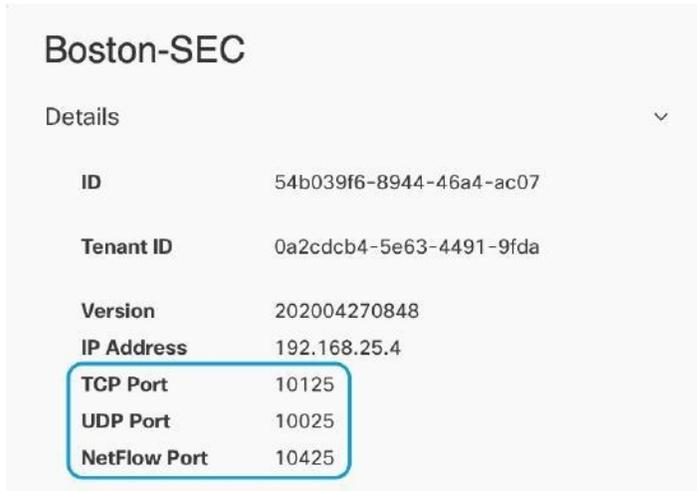
이러한 포트가 이미 사용 중인 경우 SaaS(Secure Logging Analytics)를 구성하기 전에 SEC 디바이스 세부 정보를 확인하여 실제로 이벤트를 수신하는 데 사용 중인 포트를 확인합니다.

SEC에서 사용하는 포트 번호를 찾으려면 다음을 수행합니다.

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.



| Boston-SEC             |                         |
|------------------------|-------------------------|
| Details <span>▼</span> |                         |
| ID                     | 54b039f6-8944-46a4-ac07 |
| Tenant ID              | 0a2cddb4-5e63-4491-9fda |
| Version                | 202004270848            |
| IP Address             | 192.168.25.4            |
| TCP Port               | 10125                   |
| UDP Port               | 10025                   |
| NetFlow Port           | 10425                   |



## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.