Firepower 및 통합에 대한 중요 정보 SecureX

Firepower 정보 및 SecureX

Cisco 보안 제품 구매에 포함된 통합 포털인 SecureX을(를) 통해 모든 Cisco 보안 제품의 데이터를 볼 수 있습니다.

SecureX 는 Cisco의 통합 보안 포트폴리오를 기존 인프라와 연결하여 가시성을 통합하고 자동화를 지원하며 네트워크, 엔드포인트, 클라우드 및 애플리케이션 전반에서 보안을 강화하는 단순화된 플랫폼 환경입니다.

SecureX에 관한 자세한 내용은 https://www.cisco.com/c/en/us/products/security/securex/index.html의 내용을 참조하십시오.

SecureX 포털에서 Firepower 데이터를 보고 작업하려면 이 문서의 지침을 따르십시오.

SecureX 지역 클라우드

지역	클라우드에 연결	지원되는 **Firepower** 통합 방법
북미	https://securex.us.security.cisco.com	• 직접 통합: Firepower 릴리스 6.4 이상 • 시스템 로그를 통한 통합: Firepower 릴리스 6.3 이상

지역	클라우드에 연결	지원되는 Firepower 통합 방법
유럽	https://securex.eu.security.cisco.com	• 직접 통합: Firepower 릴리스 6.5 이상 • 시스템 로그를 통한 통합: Firepower 릴리스 6.3 이상
아시아(APJC)	https://securex.apjc.security.cisco.com	• 직접 통합: Firepower 릴리스 6.5 이상 • 시스템 로그를 통한 통합: Firepower 릴리스 6.3 이상

지역 클라우드 선택 지침 및 제한 사항

지역 클라우드를 선택하기 전에 다음 사항을 고려하십시오.

- Firepower 버전 및 통합 방법(syslog 또는 직접)이 선택에 영향을 미칩니다.

  자세한 내용은 SecureX 지역 클라우드, 1 페이지의 내용을 참조하십시오.

- 가능하다면 Firepower를 구축한 곳에서 가장 가까운 지역 클라우드를 사용하십시오.
- 다른 클라우드에 있는 데이터는 집계하거나 병합할 수 없습니다.
- 여러 지역의 데이터를 집계해야 한다면, 모든 지역의 디바이스는 동일한 지역 클라우드로 데이터를 전송해야 합니다.
- 각 지역별 클라우드에서 계정을 생성할 수 있습니다. 각 클라우드의 데이터는 분리됩니다.
- Firepower 제품에서 선택하는 지역은 Cisco Support Diagnostics 및 Cisco Support Network 기능(적용 가능하며 활성화된 경우)에도 사용됩니다. 자세한 내용은 Firepower 제품의 온라인 도움말을 참조하십시오.
- Firepower 구축이 Cisco Security Analytics and Logging(SaaS) / CDO 및 SecureX/Cisco SecureX Threat Response 모두와 직접 통합되는 경우 이러한 모든 통합은 동일한 지역 클라우드를 사용해야 합니다.

지원되는 이벤트 유형

Firepower 및 SecureX 통합은 다음 이벤트 유형을 지원합니다.

표 *1: Cisco Cloud*로의 이벤트 전송을 위한 *Firepower* 버전 지원

기능	**FMC** 버전에서 관리하는 디바이스 (직접 통합)	**FDM** 버전에서 관리하는 **FTD** 디바이스 (직접 통합)	시스템 로그
침입(IPS) 이벤트	6.3 이상(시스템 로그 이용) 6.4 이상(직접 연결 이용)	6.3 이상(시스템 로그 이용) 6.4 이상(직접 연결 이용)	지원
보안 인텔리전스 연결 이벤트	6.5 이상	6.5 이상	지원되지 않음
파일 및 악성코드 이벤트	6.5 이상	6.5 이상	지원되지 않음

이벤트를 클라우드로 전송하는 방법 비교

Firepower 디바이스는 이벤트를 보안 서비스 익스체인지 포털을 통해 SecureX에서 사용할 수 있도록 합니다(시스템 로그나 직접 연결 이용).

직접 전송	프록시를 사용하여 시스템 로그를 통해 전송
지원되는 Firepower 소프트웨어 버전을 실행하는 Firepower Threat Defense(NGFW) 장치만 지원	지원되는 Firepower 소프트웨어 버전을 실행하는 모든 디바이스 지원
Firepower 6.4 이상 지원	Firepower 6.3 이상 지원
지원되는 이벤트 유형, 2 페이지에 나열된 모든 이벤트 유형을 지원합니다.	침입 이벤트만 지원합니다.
Firepower Threat Defense 디바이스는 반드시 인터넷에 연결해야 합니다.	Firepower 디바이스는 인터넷에 연결하지 않아도 됩니다.
Firepower 구축에서는 Smart Software Manager 온프레미스 서버(이전 명칭은 Smart Software Satellite Server)를 사용할 수 없습니다.	구축시 Smart Software Manager 온 프레미스 서버를 사용할 수 있습니다.

직접 전송	프록시를 사용하여 시스템 로그를 통해 전송
사내 프록시 서버를 설정하고 유지 관리하지 않아도 됩니다.	사내 가상 Cisco Security Services Proxy(CSSP) 서버가 필요합니다. 이 프록시 서버에 대 한 자세한 내용은 SSE 보안 서비스 익스체인지(온라인 도움말)에서 확인할 수 있습니다. SSE에 액세스하는 방법은 Access(액세스) 보안 서비스 익스체인지의 내용을 참조하십시오.

모범 사례

참조하는 절차 항목의 요구 사항(Requirements) 항목 및 시작하기 전에(Before You Begin) 항목을 포함한, 다음 항목에 있는 가이드라인 및 설정 지침을 정확하게 따르십시오.

- 모든 통합의 경우:

  지역 클라우드 선택 지침 및 제한 사항, 2 페이지의 내용을 참조하십시오.

- 직접 통합:

  Cisco Cloud에 이벤트를 직접 전송하고 SecureX와 통합하는 방법의 내용을 참조하십시오.

- 시스템 로그를 이용한 통합:

  시스템 로그를 이용해 Cisco Cloud에 이벤트를 전송하는 방법의 내용을 참조하십시오.