Secure Firewall Threat Defense와 Cisco XDR 통합 소개

Secure Firewall Threat Defense 및Cisco XDR 통합에 관한 정보

Secure Firewall Threat Defense를 Cisco Extended Detection and Response(Cisco XDR)와 통합하여 Cisco의 통합 보안 포트폴리오와 방화벽 구축을 연결하여 가시성을 통합하고 자동화를 가능하게 하며 네트워크 전반에서 보안을 강화하는 일관된 환경을 구축합니다.

Cisco XDR 정보

Cisco XDR는 여러 텔레메트리 소스에서 탐지를 상호 연결하여 가시성을 통합하는 클라우드 기반 솔루션 으로, 보안 팀이 가장 정교한 위협을 탐지하고 우선 순위를 정하고 이에 대응합니다.

방화벽 구축을 Cisco XDR와 통합하여 다음을 수행할 수 있습니다.

- 방화벽 이벤트를 상호 연결하고 분석하여 엔드 투 엔드 인시던트를 확인하고 위험을 기반으로 인시던트를 승격하므로 분석가가 시급하게 해결해야 하는 사항에 집중할 수 있습니다.
- 알림의 우선순위를 명확하게 지정하고 탐지부터 대응까지 최단 경로를 제공하여 위협 탐지 및 대응 기능을 향상합니다.
- 자동화와 가이드형 대응 권장 사항을 사용하여 자신 있게 위협을 해소합니다.

Cisco XDR에 대한 자세한 내용은 Cisco XDR 도움말 센터를 참조하십시오.

참고 Cisco XDR는 별도 라이선스 제품입니다. Cisco Secure Firewall 제품에 필요한 라이선스 외에 추가 구독이 필요합니다. 자세한 정보는 Cisco XDR 라이선스를 참고하십시오.

지역 클라우드

표 *1:* 지역 클라우드의 ***URL***

지역	클라우드에 연결	지원되는 통합 방법 및 **Threat Defense** 디바이스 버전
북미	• api-sse.cisco.com • mx*.sse.itd.cisco.com • eventing-ingest.sse.itd.cisco.com • defenseorchestrator.com • edge.us.cdo.cisco.com	• 직접 통합: 버전 6.4 이상 • 시스템 로그를 이용한 통합: 버전 6.3 이상
유럽	• api.eu.sse.itd.cisco.com • mx*.eu.sse.itd.cisco.com • eventing-ingest.eu.sse.itd.cisco.com • defenseorchestrator.eu • edge.eu.cdo.cisco.com	• 직접 통합: 버전 6.5 이상 • 시스템 로그를 이용한 통합: 버전 6.3 이상
아시아(APJC)	• api.apj.sse.itd.cisco.com • mx*.apj.sse.itd.cisco.com • eventing-ingest.apj.sse.itd.cisco.com • apj.cdo.cisco.com • edge.apj.cdo.cisco.com	• 직접 통합: 버전 6.5 이상 • 시스템 로그를 이용한 통합: 버전 6.3 이상
호주	• api.aus.sse.itd.cisco.com • mx*.aus.sse.itd.cisco.com • eventing-ingest.aus.sse.itd.cisco.com • aus.cdo.cisco.com	• 직접 통합: 버전 6.5 이상 • 시스템 로그를 이용한 통합: 버전 6.3 이상

지역	클라우드에 연결	지원되는 통합 방법 및 **Threat Defense** 디바이스 버전
인도	• api.in.sse.itd.cisco.com • mx*.in.sse.itd.cisco.com • eventing-ingest.in.sse.itd.cisco.com • in.cdo.cisco.com	• 직접 통합: 버전 6.5 이상 • 시스템 로그를 이용한 통합: 버전 6.3 이상

지역 클라우드 선택 지침 및 제한 사항

지역 클라우드를 선택할 때는 다음 사항을 염두에 두십시오.

- 지역 클라우드 선택은 Threat Defense 디바이스 버전 및 통합 방법(시스템 로그 또는 직접)에 따라 다릅니다.

  지역 클라우드 및 해당 URL의 목록은 지역 클라우드를 참조하십시오.

- 가능하다면 구축한 곳에서 가장 가까운 지역 클라우드를 사용하십시오.
- 다른 지역 클라우드에서는 데이터를 병합하거나 집계할 수 없습니다. 여러 지역의 데이터를 집계하려면 모든 지역의 디바이스가 동일한 지역 클라우드로 데이터를 전송해야 합니다.
- 각 지역 클라우드에서 어카운트를 만들 수 있으며 각 클라우드의 데이터는 별도로 유지됩니다.
- 선택한 지역 클라우드는 Cisco 지원 진단 및 Cisco 지원 네트워크 기능에도 사용됩니다. 이 설정은 Security Analytics and Logging(SaaS)를 사용하는 Secure Network Analytics 클라우드의 클라우드 영역에도 적용됩니다.

지원되는 이벤트 유형

Threat Defense 및 Cisco XDR 통합은 다음 이벤트 유형을 지원합니다.

표 ***2: Cisco Security Cloud***로 이벤트를 전송하기 위해 지원되는 이벤트 유형

이벤트 유형	직접 통합을 위한 지원되는 **Threat Defense** 디바이스 버전	시스템 로그 통합을 위한 지원되는 **Threat Defense** 디바이스 버전
침입 이벤트	6.4 이상	6.3 이상

이벤트 유형	직접 통합을 위한 지원되는 **Threat Defense** 디바이스 버전	시스템 로그 통합을 위한 지원되는 **Threat Defense** 디바이스 버전
높은 우선순위 연결 이벤트 수행: • 보안 관련 연결 이벤트. • 파일 및 악성코드 이벤트와 관련된 연결 이벤트. • 침입 이벤트와 관련된 연결 이벤트.	6.5 이상	지원되지 않음
파일 및 악성코드 이벤트	6.5 이상	지원되지 않음

이벤트를 클라우드로 전송하는 방법 비교

Threat Defense 디바이스는 시스템 로그를 이용하거나 직접 보안 서비스 익스체인지 포털을 통해 이벤트를 클라우드에 전송합니다.

직접 이벤트 전송	시스템 로그를 사용하여 이벤트 전송
지원되는 소프트웨어 버전을 실행하는 Threat Defense 디바이스만 지원합니다.	지원되는 소프트웨어 버전을 실행하는 모든 디바이스를 지원합니다.
버전 6.4 이상을 지원합니다.	버전 6.3 이상을 지원합니다.
나열된 모든 이벤트 유형을 지원합니다.	침입 이벤트만 지원합니다.
Threat defense 디바이스가 인터넷에 연결되어 있어야 합니다.	디바이스는 인터넷에 연결하지 않아도 됩니다.
구축에서는 Smart Software Manager 온 프레미스 서버(이전 명칭은 Smart Software Satellite Server)를 사용할 수 없습니다.	구축시 Smart Software Manager 온 프레미스 서버를 사용할 수 있습니다.
사내 프록시 서버를 설정하고 유지 관리하지 않아도 됩니다.	온프레미스 가상 Cisco Security Services 프록시 서버가 필요합니다. 이 프록시 서버에 대한 자세한 내용은 Cisco Security Services 프록시를 참조하십시오. 보안 서비스 익스체인지에 액세스하려면 Security Services Exchange 액세스를 참조하십시오.