보안 방화벽 콘텐츠 업데이트 예약 모범 사례

문제

FMC(Firewall Management Center)를 사용하여 FTD(Firewall Threat Defense) 디바이스를 관리하는 조직은 보안 및 콘텐츠 업데이트 적용 모범 사례에 대한 지침을 필요로 합니다. 특히 서로 다른 업데이트 유형을 얼마나 자주 적용해야 하는지, 업데이트를 즉시 적용하지 않고 예약할 수 있는지, 이러한 업데이트의 운영 영향은 무엇인지에 대해서는 불확실성이 있습니다. Cisco에서 자주, 때로는 매주 콘텐츠 업데이트를 릴리스하므로, 관리자는 이러한 업데이트를 릴리스할 때 즉시 적용해야 하는지 또는 조직의 유지 관리 창 및 변경 관리 정책에 따라 예약할 수 있는지를 파악해야 하기 때문에 이러한 문제가 발생합니다.

환경

- Cisco 보안 방화벽 Firepower, 모든 버전
- Firepower Management Center, 모든 버전

해결

이 표에서는 Firepower의 각 업데이트 유형의 용도를 보여 줍니다.

업데이트 유형	목적	참고
SRU/LSP	침입 규칙 업데이트(각각 Snort 2 및 Snort 3)	침입 탐지/방지 규칙 유지
지역 DB	IP 주소에 대한 지오로케이션 데이터	지오로케이션 기반 트래픽 필터링에 사용

VDB	취약성 정보 및 호스트 핑거프린트	취약성 평가 및 위험 분석에 사용

Cisco Secure Firewall 콘텐츠 업데이트는 각기 다른 릴리스 빈도 및 권장 예약 방식을 갖는 세 가지 서로 다른 유형으로 분류됩니다. 이 표에서는 각 업데이트 유형에 대한 모범 사례 예약 권장 사항을 간략하게 설명합니다.

업데이트 유형	릴리스 빈도	제안된 일정	기본 FMC 일정	탐색 경로(수정)
SRU/LSP	자주	매일	매일	System > Content Updates > Rule Updates
지역 DB	~매주	매주	매주	System(시스템) > Content Updates(콘텐츠 업데이트) > Geolocation Updates(위치 정보 업데이트)
VDB	~월	매주	매주	System(시스템) > Tools(툴): 예약 > 매주 소프트웨어 다운로드

최적의 보안 컨피그레이션 및 상태를 위해 모범 사례는 Cisco에서 이러한 업데이트를 릴리스하는 즉시 적용하는 것입니다. 이러한 업데이트 파일 중 일부는 상당히 클 수 있으며 대역폭 할당을 고려해야 합니다. 동일한 네트워크를 사용하는 경우 최대 트래픽 시간 외에 더 큰 업데이트를 설치하는 것이 좋습니다.

SRU/LSP(침입 규칙) 업데이트

SRU(Snort Rule Updates) 및 LSP(Lightweight Security Packages)에는 침입 탐지 및 방지 규칙이 포함되어 있습니다. 이러한 업데이트는 새로운 위협에 대한 보호를 유지하기 위해 운영의 실행 가능한 한 자주 적용되어야 합니다.

SRU/LSP 일정을 수정하려면 FMC 인터페이스에서 System > Content Updates > Rule Updates로 이동하여 시간, 날짜 및 빈도 설정을 조정합니다.

SRU/LSP 업데이트는 자동화된 배포를 지원하며 다운로드 및 설치 후 자동으로 배포되도록 예약할 수 있습니다.

GeoDB(Geolocation Database) 업데이트

지오로케이션 데이터베이스 업데이트는 IP 주소에 대한 현재 지리적 위치 데이터를 제공하며 일반적으로 매주 릴리스됩니다.

GeoDB 일정을 수정하려면 FMC 인터페이스에서 System > Content Updates > Geolocation Updates로 이동하여 스케줄링 매개변수를 조정합니다.

GeoDB 업데이트는 다운로드 및 설치를 위해 예약할 수 있지만 관리되는 디바이스에 구축하려면 수동 푸시가 필요하며 SRU/LSP 업데이트처럼 완전히 자동화할 수 없습니다.

VDB(취약성 데이터베이스) 업데이트

취약점 데이터베이스 업데이트는 약 매월 릴리스되며 콘텐츠 업데이트가 아닌 소프트웨어 업데이트로 관리됩니다.

VDB 일정을 수정하려면 System > Tools로 이동합니다. 다운로드 빈도와 시간을 조정하려면 매주 소프트웨어 다운로드 작업을 예약하고 수정합니다.

VDB 업데이트는 소프트웨어 업데이트에 해당되며 독립적으로 구축할 수 없습니다. 보류 중인 모든 변경 내용을 컴파일하는 수동 배포를 수행할 때 포함됩니다.

구축 고려 사항

업데이트를 구축할 때 FMC는 보류 중인 모든 컨피그레이션 변경 사항을 컴파일하며, 단일 구축 작업에 여러 유형의 콘텐츠 업데이트를 포함할 수 있습니다. 일부 업데이트의 경우 구축 중에 짧은 Snort 서비스가 재시작될 수 있습니다. 이는 프로덕션 시간 중에 업데이트를 예약할 때 고려해야 합니다.

조직은 변경 관리 정책에 따라 업데이트 일정을 조율해야 하며, 운영 환경에 대한 간략한 서비스 중단이 문제가 될 경우 유지 보수 기간 중에 업데이트를 예약하는 것을 고려해야 합니다.

원인

이는 기술적 오작동이라기보다는 구성 및 운영 안내 요청이었다. Cisco Secure Firewall 환경에서 업데이트 스케줄링 방식, 자동화 기능 및 다양한 콘텐츠 업데이트 유형이 운영에 미치는 영향에 대한 불확실성으로 인해 명확성이 요구되었습니다.

관련 콘텐츠

- Cisco Secure Firewall Management Center 관리 가이드, 7.6: 업데이트
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.