2025년 보안팀 가이드

미래 방어를 강화하세요

새로운 공격 기법과 공격자들이 오래된 표적을 악용하는 새로운 방법을 미리 파악하세요. 아래 소개된 Akamai 보안팀 가이드의 하이라이트를 먼저 살펴보세요.

심층 보안을 통한 방어 체계화

3가지 핵심 고려사항

특정 위협의 가능성과 해당 대응의 잠재력을 기반으로 대응의 우선순위를 정해 기업의 취약점을 줄이는 **리스크 관리**

방화벽, 세그멘테이션, 접속 제어를 통해 계층형 보안을 구축해 유출을 방어 및 차단하는 **네트워크 아키텍처**

시스템 업데이트, 안티바이러스 소프트웨어, 방화벽, 접속 제어를 통해 멀웨어와 무단 접속으로부터 개별 디바이스를 보호하는 **호스트 보안**

멀웨어가 숨어 있을 수 있는 장소

2024년 오픈 포트 인시던트의 상위 프로토콜

58.0%
서버 메시지 블록 (SMB)

14.5%
원격 데스크톱 프로토콜(RDP)

12.9%
SSH(Secure Shell)

공격자가 VPN 침입 시 할 수 있는 행동

- 원격 인증 서버를 사용해 사용자 인증
- 정상 인증 악용
- 악성 인증 서버 사용
- 설정 파일 비밀 추출 및 해독

XSS 취약점 예방

- 모든 사용자 제어 매개변수에 아웃풋 인코딩 추가
- 코드 검토 및 웹 애플리케이션 방화벽으로 방어
- 쿠키 도용, 웹사이트 변조, 세션 라이딩 및 크로스 사이트 요청 위조와 같은 공격자의 실전 기법 차단

공격자가 컨테이너를 표적으로 삼는 이유

Akamai 연구원들은 쿠버네티스 내 여러 취약점과 기법을 발견했으며, 이 취약점은 악용 시 다음과 같은 결과로 이어질 수 있습니다.

- 데이터 탈취
- 권한 확대
- 원격 코드 실행

사전 조치와 사후 준비 결합

적용해야 할 4가지 기본 원칙:

- 어디서나 사이버 위생 확립
- 보안 플랫폼 뒷단의 환경을 지속적으로 계층화
- 비즈니스 크리티컬 서비스에 집중할 수 있도록 신뢰할 수 있는 인시던트
- 대응팀 또는 파트너 확보

2025년 보안팀 가이드 다운로드