Akamai

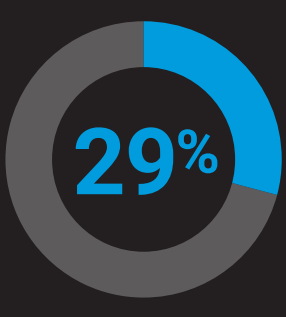
10 YEARS OF SECURITY INSIGHT

공격 트렌드 분석

숨어 있는 API 위협에 대한 공격 트렌드 분석

API의 광범위한 도입은 오늘날 기업의 혁신과 효율성 제고로 이어졌습니다. 하지만 보안팀은 이러한 API로 인해 발생한 리스크의 규모와 복잡성을 이해하는 데 어려움을 겪고 있습니다. 대부분의 기업은 문서화되지 않은 API 또는 섀도 API를 모두 파악하지 못해 네트워크 경계에 진입 지점이 생겨나고 있습니다. 최신 리서치 보고서에서 API 공격의 최신 트렌드를 확인하세요.

API 도전 과제



2023년 전체 웹 공격에서 API가 표적이 된 비율

상위 3대 API 공격 기법

44%
HTTP 공격

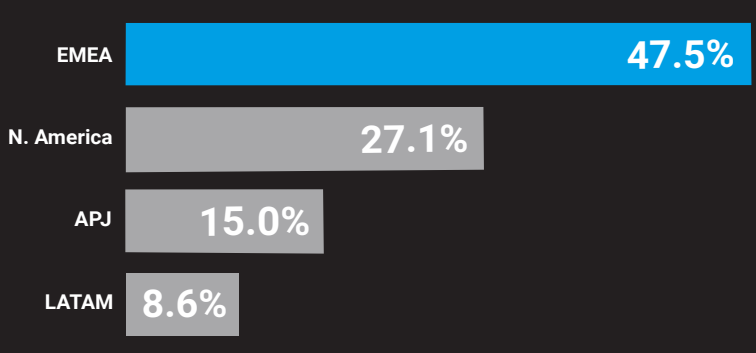
25%
활성 세션

14%
구조화된 쿼리 언어 인젝션

숫자로 보는 API 환경

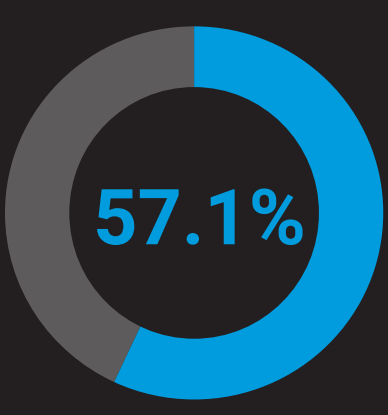
지역별 API 공격

2023년 01월 1일~2023년 12월 31일



API 공격 비율

EMEA(Europe, Middle East, Africa) 지역은 전 세계적으로 API 공격 발생 비율이 47.5%로 가장 높습니다.



API 인벤토리의 정확도를 25%에서 75% 사이로 추정한 응답자의 비율

2023년 SANS API 보안 설문조사 기준

API 공격 상위 3대 업계

- 커머스
- 비즈니스 서비스
- 기타 디지털 미디어

기업에 대한 3가지 질문

API 남용 및 악용은 OWASP API 보안 상위 10대 취약점을 넘어 광범위하게 발생할 수 있습니다. 다음 중 해당하는 항목을 체크해 포괄적인 보안 전략이 갖춰져 있는지 확인해 보세요.

- ☐ **취약점**: API 개발의 모범 사례를 따르고 있나요?
- ☐ **가시성**: 프로그램이 모든 API를 확실히 보호하도록 하기 위한 프로세스 및 기술적 제어 수단을 갖추고 있나요?
- ☐ **비즈니스 로직 악용**: 의심스러운 활동을 식별하기 위해 정상적인 API 트래픽에 대한 기준이 있나요?

가시성이 중요한 이유

API 취약점은 기업 환경으로 진입하는 지점이기 때문에 공격자보다 먼저 취약점을 발견해야 합니다.

API 환경 방어하기

API를 방어하는 방법

- ✔ 모든 API를 문서화하고 API 보안 제어에 통합해 가시성을 강화하세요
- ✔ API의 잘못된 설정 문제를 해결하고 향후 취약점 발생을 방지하기 위한 프로세스를 구축하세요
- ✔ API 모니터링 및 위협 탐색 원칙을 확립해 공격자가 악용하기 전에 보안 격차를 제거하세요
- ✔ OWASP API 보안 상위 10대 리스크부터 기존의 웹 공격까지 모든 범위의 위협을 방어할 수 있는 솔루션을 선택하세요
- ✔ 가장 일반적인 공격을 방지할 수 있도록 코딩 관행에 OWASP 가이드를 활용하세요
- ✔ 행동 애널리틱스를 제공하는 보안 솔루션을 사용해 비즈니스 로직 남용 및 기타 비정상을 탐지하세요

기업의 API까지 적용되는 컴플라이언스

PCI DSS v4.0에는 데이터 감염 리스크를 줄이기 위해 시스템과 소프트웨어의 개발 및 유지 관리 과정에서 API를 사용하는 방법에 대한 새로운 표준이 포함되었습니다.

시프트 레프트(Shift Left)로 공격 방지

코딩 모범 사례에는 API를 프로덕션에 적용하기 전에 테스트하고 API 수명 주기 전반에 걸쳐 보안을 강화하는 방안이 포함되었습니다.

보고서 전문에서 API 공격 트렌드와 해결책을 자세히 살펴보세요. 지금 읽어보세요.

보고서 다운로드

| 2024년 03월 발행