API 보안 영향 연구의 최신 보고서는 아시아-태평양(APAC) 지역 에서 가장 큰 규모의 4대 경제권(중국, 인도, 일본, 호주)에서 사이버 보안 분야에 종사하는 800여 명 이상의 응답자를 대상으로 API 보안 현황을 조사했습니다. 이는 Noname Security(현재 Akamai Technologies의 일부)가 보안 전문가들에게 지난 3년간 API가 보안 이니셔티브에 어떻게 통합되었는지 묻는 연간 설문 조사를 기반으로 합니다. 리서치는 API 취약점에 대한 인식이 증가했음에도 불구하고 상충하는 우선순위의 범위 확대에 따라 CISO 및 CIO가 이를 해결하는 데 어려움을 겪으면서 API 보안에 대한 고위 경영진의 의지가 흐름을 따라가지 못하고 있음을 일관되게 보여주었습니다.

2024년 **API 보안 영향 연구**는 기존 조사 대상 국가인 미국과 영국을 넘어 독일로 범위를 확장했습니다. 연구 결과 다음과 같은 점이 확인되었습니다.

- API 보안 인시던트가 3년 연속 증가했습니다.
- 이러한 인시던트에 대응하는 비용은 평균 50만 달러를 초과하는 것으로 추산되며, IT 및 보안 리더들에 따르면 거의 100만 달러에 달했습니다.
- 대부분의 응답자는 이러한 인시던트가 보안팀에 미치는 스트레스와 평판 하락을 인식하고 있었습니다.

이번 설문 조사 응답자는 8개 업계 분야의 기업에서 근무하는 최고 경영진(CISO, CIO, 최고 기술 책임자), 수석 보안 담당자, AppSec 팀 구성원으로 구성되었습니다.

- 자동차
- 보험
- 금융 서비스
- 정부 및 공공 부문
- 리테일 및 이커머스
- 제조
- 헬스케어
- 에너지 및 유틸리티

조사 결과는 API 보안 관행과 우선순위에 대한 귀중한 인사이트를 제공하며 다음과 같은 내용을 포함합니다.

- API 보안 인시던트의 원인
- 전체 사이버 보안 우선순위
- API 보안 인시던트와 관련된 비용(벌금 및 복구 비용 등)
- API 보안 인시던트가 보안팀에 미치는 영향
- API 인벤토리 구축 및 테스트 실행 현황
- 민감한 정보를 반환하는 API에 대한 인식
- 컴플라이언스 측면에서의 API 보안 현황

API 보안 인시던트란 무엇일까요?

인시던트에는 API 악용, API 공격, API를 대상으로 한 데이터 유출, 악성 공격자의 전반적인 API 감염 시도 등이 포함됩니다.