API 보안 영향 연구 2025

APAC 4개국의 API 공격 피해 비용

중국, 일본, 인도, 호주의 보안팀이 감염된 API의 영향을 어떻게 인식하고 있는지 알아보세요

Akamai

Akamai 인터넷 보안 현황(SOTI) 보고서 제휴사 출판물

목차

소개

API(Application Programming Interface)를 향한 공격 횟수가 늘어나고, 정교해질 뿐만 아니라 규모도 커지고 있습니다. 실제로 Akamai의 최근 SOTI(State of the Internet) 보고서에 따르면 **2023년 1월부터 2024년 6월까지 1080억 건의 API 공격이 집계되었습니다**.

그러나 기업 내 API가 빠른 속도로 급증하고 많은 API가 필요에 따라 민감한 데이터에 접근할 수 있다는 사실에도 불구하고, 리서치 결과 대부분의 보안팀은 API 보안을 최우선 과제로 삼고 있지 않습니다. 기업이 API 및 그 리스크에 대한 가시성 부족으로 어려움을 겪고 있는 가운데, 이번 조사 결과는 취약점 추적부터 유출 영향 측정까지 API 보안에 대한 책임이 중앙화되어 있지 않다는 업계의 우려와 일치합니다.

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.

요약 보고서

조사 결과는 APAC 지역 및 여러 업계 분야의 보안팀과 경영진에게 귀중한 인사이트를 제공하며 이 중 눈에 띄는 몇 가지 주요 트렌드가 있습니다.

1. **중국은 API 보안을 사이버 보안 전략의 핵심 요소로 삼고 있습니다.** API 보안에 충분한 관심을 기울이지 않고 있는 다른 지역과 대조된 모습이라 할 수 있습니다. 중국의 응답자는 "공격자로부터 API 보호"를 최우선 순위로 꼽았습니다. 2024년 API 보안 영향 연구에서 미국, 영국, 독일의 응답자는 "GenAI(Generative AI) 기반 공격 방어"와 "랜섬웨어 방어" 등 다른 우선순위에 이어 "공격자로부터 API 보안"을 9위로 뽑았습니다. 중국은 또한 지난 12개월 동안 API 보안 인시던트 대응 비용 추정액이 가장 높았으며, CN 568만 7373위안(US 77만 8271달러*)로 집계되었습니다.

> **"공격자로부터 API 보호"** | 중국 응답자가 답한 12개월 내 사이버 보안 우선순위 1위

2. **중요한 기업 역할 간 격차가 여전히 존재합니다.** 결과는 역할, 국가, 업계별로 달랐지만, 전반적으로 명확하게 드러나는 한 가지 메시지가 있습니다. API 보안 인시던트의 비용, 원인, 기업적 영향에 대해 최고 경영진, 수석 보안 전문가, AppSec 팀 간의 이해도가 일치하지 않으며 기업의 API 가시성에 대한 인식마저 차이가 있습니다.

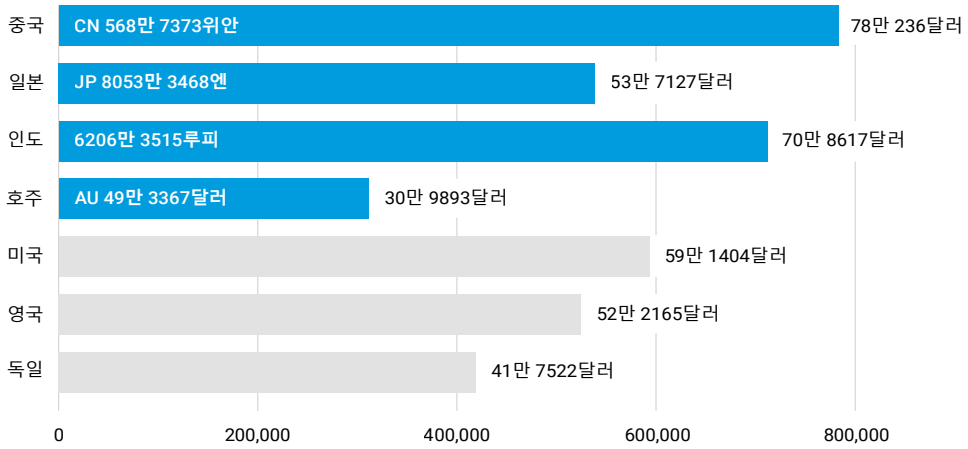
예를 들면 다음과 같습니다.

- 중국에서 최고 경영진 응답자의 API 보안 인시던트 비용 추정치는 다른 업무를 하는 사람들의 추정치보다 거의 두 배 높았습니다.
- 일본에서는 기업 내 여러 역할 간에 기업이 경험한 API 보안 인시던트의 주요 원인에 대한 합의가 없었습니다.
- 인도에서는 최고 경영진(77%)과 수석 보안 전문가(75%)가 전체 API 인벤토리를 보유하고 있다고 응답한 비율이 AppSec 팀(41%)보다 훨씬 높았습니다.
- 전체적으로 최고 경영진 응답자의 92%가 지난 12개월 동안 기업에서 API 보안 인시던트를 경험했다고 답했으며, 이는 AppSec 팀의 80%와 대비됩니다.

*모든 통화 환산은 2025년 3월 27일 기준입니다.

API 보안 인시던트를 경험한 경우, 해당 인시던트로 인해 발생한 총 재정적 영향은 얼마였나요?

지난 12개월 동안 API 인시던트의 평균 추정 비용

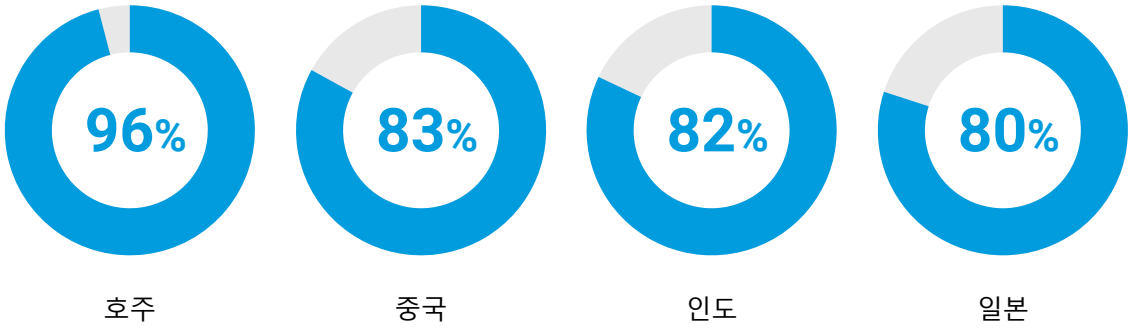


3. **API 보안 인시던트의 영향은 압도적인 한 가지 사건에 국한되지 않습니다.** 조사 결과는 API 공격 및 악용의 영향이 광범위하게 확산된다는 것을 보여줍니다. 응답자는 업무와 지역에 따라 가장 큰 영향을 다르게 평가했습니다. 일부 응답자는 보안팀이 예상하지 못한 API 공격의 대응 비용 등 재정적 영향을 가장 중요하게 여겼으며, 또 다른 응답자는 공격 이후 신뢰 하락(예: 이사회의 평판 하락)을 가장 큰 영향으로 꼽았습니다. 일본 응답자는 평판 하락을 가장 큰 영향으로 평가했습니다.

> **고위 경영진 및/또는 이사회에서 부서의 평판 하락**

일본 응답자가 답한 API 보안 인시던트의 가장 큰 영향 1위

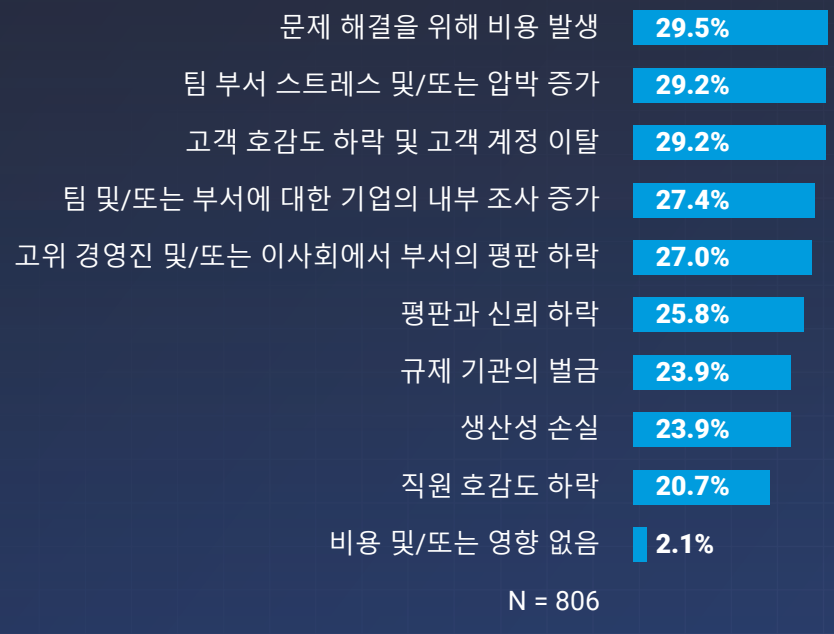
4. 현재 4개국 기업들은 정기적으로 API 보안 인시던트를 겪고 있습니다.



이 결과는 이전 보고서와도 크게 일치합니다. 이전 보고서에서 미국, 영국, 독일의 응답자 84%가 지난 12개월 동안 인시던트를 경험했다고 답했습니다.

중국, 일본, 인도, 호주에서 API 보안 인시던트의 영향 순위

API 보안 인시던트가 기업에 어떤 비용 및/또는 영향을 초래했나요? (최대 3개 선택)



지역별 트렌드 개요

4개국 간 규제, 정치, 경제적 차이가 크지만 이 결과는 전반적인 API 보안 이니셔티브의 성숙도를 이해하는 데 유용한 인사이트를 제공합니다. 연구 결과는 자체 API 보안 우선순위를 수립하는 전문가들에게 유용한 벤치마킹 데이터도 제공합니다. 공격자가 API를 표적으로 삼는 것은 분명합니다. Akamai의 **2024년 API 보안 인터넷 현황 보고서: API 위협에 대한 조명**은 APAC 지역에서 API 공격에 대한 우려가 커지고 있음을 보여주었습니다. Akamai의 리서치 결과, APAC 지역에서 발생한 모든 웹 공격의 15%가 API를 표적으로 삼았습니다. 전 세계적으로 APAC 지역은 유럽, 중동, 아프리카(EMEA) 지역(48%)과 북미 지역(27%)에 이어 API 공격 비율이 세 번째로 높았습니다.

기업이 증가하는 공격 기법에 대한 대응을 준비하는 가운데, 이번 조사 결과는 경영진과 현장 실무자가 API 보안 인시던트의 수, 근본 원인, 그리고 수익과 평판 하락 측면에서의 비용 등 중요한 기본 문제에 대한 공감대를 형성해야 함을 보여줍니다.

API 보안은 얼마나 중요한 우선순위인가요?

중국에서는 API 보안이 최우선 과제입니다. 모든 응답자에게 내년 사이버 보안 과제의 순위를 매겨달라고 요청했습니다. 세계 2위 경제대국인 중국은 유일하게 "공격자로부터 API 보호"를 최우선 순위로 꼽아 이 부분에서 다소 이례적인 모습을 보였습니다.

향후 12개월 동안 귀사의 주요 사이버 보안 우선순위는 무엇인가요? (최대 3개 선택)

중국

1. 공격자로부터 API 보호 — 27.6%
2. 특별 권한 IT 접속 보안 — **24.6%**
3. 애플리케이션 보안 — **24.1%**
4. SIEM — **24.1%**
5. 데이터 손실 차단 — **22.2%**

일본

1. 랜섬웨어 방어 — **25.5%**
2. SIEM — **25.5%**
3. 데이터 손실 차단 — **25.0%**
4. 공격자로부터 API 보호 — 22.0%
5. 애플리케이션 보안 — **22.0%**

인도

1. 클라우드 보안 솔루션 — **26.9%**
2. 개발자 비밀 관리 및 보안 — **24.9%**
3. 애플리케이션 보안 — **23.4%**
4. 공격자로부터 API 보호 — 22.9%
5. 특별 권한 IT 접속 보안 — **29.9%**

호주

1. 엔드포인트 보안 — **26.2%**
2. 개발자 비밀 관리 및 보안 — **24.3%**
3. SIEM — **23.8%**
4. 공격자로부터 API 보호 — 22.8%
5. 데이터 손실 차단 — **22.8%**

중국이 API에 집중하는 것은 중국 보안 전문가들이 API 보안 인시던트 비용을 추정하는 방식과 관련이 있을 수 있습니다.

- 수석 보안 전문가: CN 673만 3916위안(US 92만 4천 달러)
- AppSec 팀: CN 662만 2503위안(US 92만 달러)

다른 모든 국가에서는 "공격자로부터 API 보호"는 네 번째로 높은 우선순위로 나타났습니다. 전체적으로 "공격자로부터 API 보호"는 SIEM(Security Information and Event Management)에 이어 두 번째로 높은 우선순위로 나타났습니다.

비용에 대한 합의 부족

중국에서 수석 보안 전문가(CN 673만 3916위안, 또는 US 92만 5478달러)와 AppSec 팀(CN 662만 2503위안, 또는 US 91만 166달러)은 API 보안 인시던트의 비용을 높게 추정했지만, 경영진(최고 경영진)의 추정치는 훨씬 낮았습니다(평균 CN 375만 897위안, 약 US 51만 7293달러). 이 역할 간 차이는 일본과 인도에서도 관찰되었지만 호주에서는 나타나지 않았습니다. 그러나 이러한 차이는 최고 경영진과 현장 실무자 사이만의 문제가 아니었습니다. 예를 들어 일본에서는 수석 보안 전문가들이 가장 높은 비용 추정치를 제시한 반면, AppSec 팀은 가장 낮은 추정치를 보였습니다. 이러한 역할 간 차이는 기업이 API 보안 인시던트가 기업에 미치는 비용에 대한 공통된 인식이 부족함을 시사합니다. 또한 역할 간에 API 보안을 얼마나 우선순위로 삼아야 하는지에 대한 인식 차이를 설명합니다. 이러한 업무를 담당하는 사람들이 API 보안 인시던트가 비즈니스에 미치는 재정적 영향에 대해 합의하지 못한다면, API 보안은 우선순위 목록의 상위에 오르지 못할 것입니다.

API 보안 인시던트가 발생하고 있다는 것을 인식하지만 발생 빈도에 대한 이해 부족

API 보안 인시던트의 빈도에 대한 인식 차이도 존재합니다. 이전에 다른 지역에서 진행된 API 보안 영향 연구를 보면 해당 지역에서 시간 경과에 따라 인시던트 수가 지속적으로 증가했음을 알 수 있습니다. 그러나 중국, 일본, 인도, 호주에 대한 과거 데이터가 없어서, 이들 국가에서 API 보안 인시던트가 얼마나 증가했는지 측정할 수 없습니다. 그럼에도 불구하고 기업이 위협을 인식하고 있다는 것은 분명합니다. 전체적으로 조사 대상 기업의 85%가 지난 12개월 동안 API 보안 인시던트를 경험했다고 응답했으며, 호주에서 가장 높은 빈도인 95%를 기록했습니다.

API 보안 인시던트는 중국, 일본, 인도, 호주에서 널리 발생합니다

전체적으로 85%의 기업이 지난 12개월 동안 API 보안 인시던트를 경험했다고 응답했으며, 호주에서 가장 높은 발생률(95%)을 기록했습니다.

조사 결과는 경영진과 현장 실무자 간의 API 보안 인시던트 발생 빈도에 대한 이해 격차를 보여줍니다. 전체 최고 경영진 응답자의 92%는 지난 12개월 동안 API 보안 인시던트를 경험했다고 답하며, 보안 전문가의 83%와 AppSec 팀의 80%와 대비를 이루었습니다. 일부 국가에서 이러한 격차가 더 컸으며, 특히 중국에서는 최고 경영진 응답자의 97%가 인시던트를 보고한 반면, 보안 전문가의 78%와 AppSec 팀의 74%가 인시던트를 경험했다고 답했습니다.

API 보안 인시던트의 광범위한 영향

취약한 API에 대한 공격은 피해 복구 비용과 기업의 대외 이미지 실추를 넘어 기업 전반에 광범위한 영향을 미칠 수 있습니다. 공격의 영향에는 규제 벌금, 고객 손실(또는 이탈), 내부 이미지 손상, 보안팀의 직원 스트레스 증가(미국, 영국, 독일 응답자가 가장 많이 언급한 영향) 등이 포함될 수 있습니다.

조사 결과, APAC 4개국의 기업은 다양한 분야에서 영향을 받고 있는 것으로 나타났습니다. 4개국의 응답자 중 그 누구도 비즈니스 관련 API 보안 인시던트의 비용과 영향에 대해 압도적으로 하나의 요인을 지목하지 않았습니다. 4개국에 최대 3개의 비용 또는 영향 요인을 제시하도록 요청했을 때, "문제 해결을 위해 사용한 비용"이 가장 높은 요인(29.5%)으로 나타났으며, "팀 및 부서의 스트레스 및/또는 압박 증가"(29.2%)와 "고객 호감도 하락 및 고객 계정 이탈"(28.8%)이 뒤를 이었습니다. 기타 옵션 중에서는 "직원 신뢰도 하락"(20.7%)이 가장 낮은 점수를 기록했으며, "비용 및/또는 영향이 없었다"(2.1%)가 그 뒤를 이었습니다.

API 보안 인시던트의 원인에 대한 명확성 부족

응답자에 따르면, "API 설정 오류"가 API 보안 인시던트의 가장 흔한 원인으로 꼽혔으며, 호주와 인도에서 가장 많이 언급되었고 중국에서는 두 번째로 많이 언급되었습니다. 그러나 조사된 국가 중 어느 곳에서도 특정 API 취약점이 명확히 두드러지지 않았습니다. 종합 결과를 보면 응답자에게 최대 3개의 답변을 선택하도록 요청한 결과, "API 설정 오류"(22.3%)가 가장 높았고, "네트워크 방화벽의 탐지 실패"(20.8%), "API 게이트웨이의 탐지 실패"(20.7%), "권한 취약점"(20.6%)이 뒤를 이었습니다.

상위 6개 응답 간의 차이는 몇 퍼센트포인트에 불과했습니다. 이는 기업이 API 취약점이 다양한 경로를 통해 지속되고 있으며, API 보안 노력에 광범위한 약점이 존재한다는 것을 인식하고 있음을 시사합니다. 보안팀을 위한 주요 시사점은 다음과 같습니다.

- 모두가 주목하는 API 설정 오류 문제는 아마도 타당할 것입니다. 보안 설정 오류는 널리 참고되는 OWASP API 보안 상위 10대 취약점 목록에서 8위를 기록한 리스크 요소로, 손상된 오브젝트 수준의 권한(OWASP 1위), 손상된 인증(OWASP 2위), 과도한 데이터 노출(OWASP 3위)과 같은 취약점으로 이어질 수 있습니다.
- 네트워크 방화벽과 WAF(Web Application Firewall)와 같이 일반적으로 널리 사용되는 보안 툴은 증가하는 복잡한 공격을 탐지하도록 설계되지 않았다는 점도 우려의 원인이 될 수 있습니다. 이러한 툴은 기본적인 보호 기능을 제공하지만 빠르게 진화하는 API 공격 방법에는 더 포괄적인 API 보안이 필요합니다.

중국, 일본, 인도, 호주에서 API 보안 인시던트의 원인 순위

기업에서 경험한 API 보안 인시던트의 원인은 무엇인가요? (최대 3개 선택)

조사 대상 APAC 4개국의 종합 결과

API 설정 오류	22.3%
네트워크 방화벽의 탐지 실패	20.8%
API 게이트웨이의 탐지 실패	20.7%
권한 취약점	20.6%
API가 인터넷에 의도치 않게 노출됨	19.6%
LLM (Large Language Model)과 같은 GenAI 툴 내 API	19.2%
API 코딩 오류로 인한 취약점	18.7%
미드 티어 소프트웨어 솔루션(Slack)	18.7%
API 인증 제어 부족	18.1%
웹 애플리케이션 방화벽의 탐지 실패	17.5%
관리되지 않는 API(예: 휴면 또는 좀비 API)	16.6%
인터넷에서 다운로드한 소프트웨어 솔루션	16.3%
유명한 기술 툴 및 서비스(Microsoft 등)	15.8%
API 보안 인시던트를 경험한 적 없음	2.6%

N = 806

API 내 민감한 데이터에 대한 인식

전체 응답자의 70% 이상이 전체 API 인벤토리를 보유하고 있다고 답했습니다. 그러나 그 중 어떤 API가 민감한 데이터를 반환하는지 파악하는 것은 더 어려웠습니다. 응답자의 37%만이 API 인벤토리를 완전히 파악하고 있으며 그 중 어떤 API가 민감한 데이터를 반환하는지 알고 있다고 답했습니다. 이 결과는 역할에 따라 크게 달랐습니다. 최고 경영진 응답자의 44%는 어떤 API가 민감한 데이터를 반환하는지 알고 있다고 답했지만 (CISO만 보면 31%로 감소), AppSec 팀은 37%, 수석 보안 전문가는 28%에 그쳤습니다.

일본에서는 AppSec 응답자의 64%가 어떤 API가 민감한 데이터를 반환하는지 알고 있다고 답한 반면, 최고 경영진 응답자나 수석 보안 전문가는 24%에 불과했습니다. 공격자가 API에 허위 요청을 제출하고 민감한 데이터를 획득하는 것이 얼마나 쉬운지 고려하면, 보안팀의 입장에서 볼 때 이 분야에서 역할 간 불일치가 발생하면 안 됩니다.

AI로 확장되는 API 취약점

4개국에서 CIO가 CISO보다 3배 더 많이 기업의 GenAI 기술 취약점을 API 보안 인시던트의 원인으로 지목했습니다.

이러한 우려는 타당합니다.

기업이 배포하는 AI 기반 애플리케이션과 LLM은 누락 기능, 통합 작업, 데이터 교환을 위해 API에 의존합니다. 공격자는 다음과 같은 기법을 통해 AI 보안 취약점을 악용할 수 있습니다.

- 프롬프트 주입 공격: 공격자는 AI가 생성한 응답을 조작해 민감한 데이터를 유출하거나 보안 조치를 우회합니다.
- 데이터 유출 및 모델 도용: 공격자는 AI 모델에서 독점적인 지식을 추출하려고 시도합니다.

응답자의 37%만이 어떤 API가 민감한 데이터를 반환하는지 알고 있다고 답한 점을 고려하면 GenAI 애플리케이션과 LLM에 대한 위협은 IT 및 보안 리더들의 최우선 과제여야 합니다.

조사 대상 4개국 모두에서 API 보안 인시던트의 주요 원인으로 GenAI 취약점을 꼽은 상위 3개 업계는 다음과 같습니다.

1. 정부 및 공공 부문
2. 에너지 및 유틸리티
3. 보험

국가별 세부 분석

중국은 API 보안을 최우선으로 꼽았습니다

4개국 중 내년 사이버 보안 우선순위 측면에서 API 보안을 가장 중요하게 여기는 국가는 중국이었습니다. "공격자로부터 API 보호"는 중국 전체 응답자의 27%가 최우선 순위로 꼽으며 가장 높은 점수를 받았습니다. "특별 권한 IT 접속 보안"은 2위를 차지했으며, 에너지 및 유틸리티, 금융 서비스, 제조, 자동차, 헬스케어 분야에서 최우선 순위로 꼽혔습니다.

이러한 결과에 따라 당연히 중국은 API 테스트 분야에서도 선도적인 위치를 차지했습니다. 중국 응답자의 과반수(22%)는 실시간 테스트를, 28%는 매일 테스트를 실시한다고 답했습니다. 이 비율은 AppSec 팀에서 65%에 달했습니다. 이러한 테스트에 주목해야 합니다. 기업이 인시던트 원인으로 지목하는 많은 API 취약점은 개발팀이 API를 공개하기 전에 식별하고 수정할 수 있습니다.

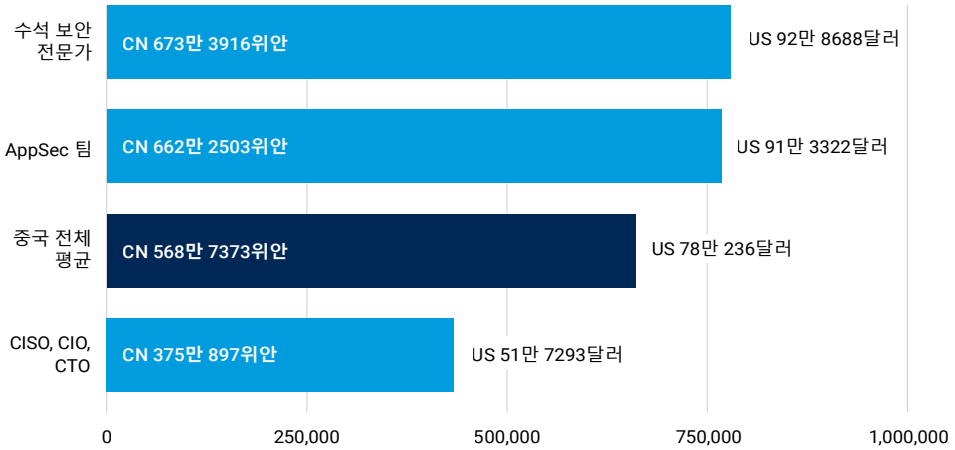
중국에서 고위 경영진은 지난 1년간 API 보안 인시던트를 명확한 문제로 인식했습니다. 최고 경영진 응답자의 거의 모두(97%)가 API 보안 인시던트를 보고하며 이는 현장 실무자와의 20포인트 차이를 반영했습니다. 지난 1년간 인시던트 발생률이 가장 높은 업계는 리테일로 100%가 인시던트를 보고했으며 보험업계는 72%로 가장 낮았습니다.

그러나 최고 경영진은 현장 실무자보다 인시던트 비용이 훨씬 적다고 생각합니다.

중국에서 CISO, CIO, CTO의 97%가 API 보안 인시던트를 경험했다고 보고했으며, 이는 최고 경영진과 현장 보안 실무자 사이의 20포인트 격차를 반영합니다.

API 보안 인시던트를 경험한 경우, 해당 인시던트로 인해 발생한 총 재정적 영향은 얼마였나요?

중국 보안 리더 및 실무자가 답한 API 보안 인시던트 비용



중국 응답자 사이에서는 API 보안 인시던트의 가장 큰 영향에 대해 일부 의견 차이가 있었습니다. AppSec 팀은 재정적 영향을 언급한 반면, 최고 경영진 응답자는 팀에 대한 스트레스 및 압박을 꼽았습니다. 이는 최고 경영진 응답자가 API 보안 인시던트와 관련된 비용을 가장 낮게 추산했기에 예상되는 당연한 결과일 수 있습니다. 흥미롭게도 자동차, 정부 및 공공 부문, 보험은 "문제 해결을 위해 사용한 비용"을 가장 큰 영향으로 평가한 유일한 업계였습니다.

이에 맞춰, 최고 경영진은 실무자보다 API가 민감한 데이터를 반환하는지 여부에 대한 지식에 훨씬 더 긍정적인 전망(53%)을 보였습니다(수석 보안 전문가: 25%, AppSec 팀: 40%). 이 역할들은 전체 API 인벤토리 보유 여부와 대체로 일치했습니다.

중국에서 보고된 API 보안 인시던트의 주요 원인은 다음과 같습니다.

- "네트워크 방화벽의 탐지 실패"
- "API 설정 오류"
- "API 게이트웨이의 탐지 실패"

많은 중국 응답자가 실시간 테스트를 실시했다고 보고했음에도 불구하고 "API 코딩 오류로 인한 취약점"이 근소한 차이로 4위를 차지했습니다. 리테일 및 이커머스 응답자의 50%가 "네트워크 방화벽의 탐지 실패"를 인시던트의 주요 원인으로 꼽으며 중국 업계별 응답에서 가장 높은 일치도를 보였습니다. 기타 업계에서는 주요 원인이 응답자의 약 40% 이하에서만 언급되었으며, 다른 업계는 API 자체의 내재적 요인(예: API 설정 오류)을 원인으로 지목했습니다. 중국 리테일 및 이커머스 응답자는 향후 12개월 동안의 최우선 사이버 보안 과제로 "데이터 손실 차단"을 50%가 언급하며 더 높은 일치도를 보였습니다.

API 중 어느 것이 민감한 데이터를 반환하는지 알고 있나요?

전체 API 인벤토리를 보유한 중국 응답자의 39.4%만이 어떤 API가 민감한 데이터를 반환하는지 알고 있습니다. 최고 경영진 응답자는 실무자에 비해 중요한 API 리스크 요소에 대한 지식에 훨씬 긍정적인 전망을 보였습니다.

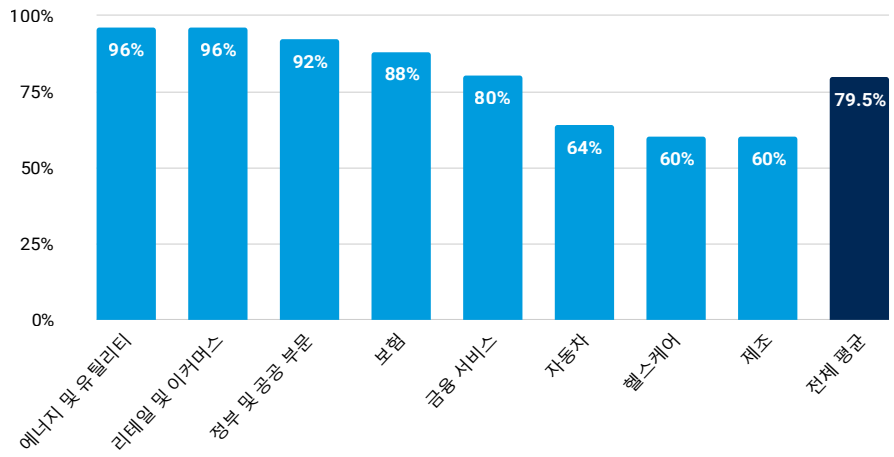
- CISO, CIO, CTO: 53%
- 수석 보안 전문가: 25%
- AppSec 팀: 40%

일본은 API에 더 낮은 우선순위를 부여했지만, API를 많이 사용하는 업계에서는 인시던트 발생률이 낮았습니다

일본에서 "공격자로부터 API 보호"는 "랜섬웨어 방어", "SIEM", "데이터 손실 차단"에 이어 네 번째로 높은 보안 우선순위였습니다. 그러나 수석 보안 전문가들은 "랜섬웨어 방어"와 함께 "공격자로부터 API 보호"를 최우선 순위로 꼽으며 그 중요성을 강조했습니다. "공격자로부터 API 보호"는 일본의 자동차 업계에서도 최우선 순위였으며, 이 업계의 응답자 중 8%만이 어떤 API가 민감한 데이터를 반환하는지 알고 있다는 점을 고려하면 중요한 데이터 포인트입니다.

일본 응답자의 약 80%가 지난 12개월 동안 API 보안 인시던트를 경험했다고 보고했지만(중국보다 훨씬 낮음), 자동차, 헬스케어, 제조 등 API를 많이 사용하는 업계의 일본 응답자 중 인시던트를 보고한 비율은 60%에 그쳤습니다. 역할별로는 최고 경영진과 AppSec 팀이 유사한 수준으로, 약 83%가 인시던트를 보고했습니다.

지난 12개월 동안 API 보안 인시던트를 경험했나요?
일본 업계의 현황과 국가 전체 평균 비교



일본에서는 다른 국가에 비해 보안 툴을 인시던트의 주요 원인으로 지목한 응답자가 적었으며 외부 툴을 지목한 응답자가 더 많았습니다. "인터넷에서 다운로드한 소프트웨어 솔루션"(22%)이 가장 많이 보고된 원인이며, "미드 티어 소프트웨어 솔루션(Slack)"이 4위(21%)를 차지했습니다. 흥미롭게도 "유명한 기술 툴 및 서비스(Microsoft 등)"는 최하위(15%)를 기록했습니다.

일본의 API 보안 인시던트 추정 비용:

- 전체: JP 8050만 엔(US 52만 8천 달러)
- 최고 경영진: JP 7400만 엔(US 48만 5천 달러)
- 헬스케어: JP 3321만 6389엔(US 21만 8천 달러)
- 수석 보안 전문가: JP 1억 1500만 엔(US 75만 4천 달러)
- AppSec 팀: JP 5600만 엔(US 36만 7천 달러)
- 자동차: JP 2억 2800만 엔(US 150만 달러)

일본에서 API 보안 인시던트의 내부적 영향은 AppSec 팀원들이 가장 강하게 느꼈습니다. "고위 경영진 또는 이사회에서 부서의 평판 하락"이 AppSec 그룹에서 가장 높은 응답률을 기록했으며, "팀 및 부서에 대한 기업의 내부 조사 증가"가 3위를 차지했습니다. "팀 및 부서에 대한 스트레스나 압박이 증가했다"는 답변이 4위를 기록했습니다.

일본 응답자 전체에서 두 번째로 큰 영향은 기업의 대외 평판 하락으로, 구체적으로 "고객 호감도 하락 및 고객 계정 이탈"이었습니다. 이것은 기업에만 해당되는 것이 아니었습니다. 일본 정부 기관들도 시민의 신뢰 상실과 계정 이탈을 가장 큰 영향으로 꼽았습니다.

일본 응답자의 약 80%가 전체 API 인벤토리를 보유하고 있다고 답했습니다. 한편, 37%가 민감한 데이터를 반환하는 API를 알고 있다고 답했지만 업계별로 차이가 컸습니다. 일본의 자동차 및 금융 서비스 업계 응답자 중 8%만이 민감한 데이터를 반환하는 API를 알고 있다고 답했으며, 이는 리테일 및 이커머스(80%)와 정부 및 공공 부문(64%)과 대비되며 현저한 차이를 보였습니다.

최고 경영진 및 수석 보안 전문가 중 23%만이 민감한 데이터를 반환하는 API를 알고 있다고 답한 반면, AppSec 팀은 64%가 알고 있다고 답해 업무별 차이도 분명하게 드러났습니다.

일본 응답자의 11%만이 실시간 API 테스트를 진행하며, 이는 중국의 22%에 비해 크게 뒤처집니다. 그러나 일본 수석 보안 전문가의 약 20%는 실시간 테스트를 진행한다고 답했으며, 12%는 리소스 부족으로 인해 API를 전혀 테스트하지 않는다고 밝혔습니다. 일본 헬스케어 업계에서도 응답자의 20%가 리소스 부족으로 인해 API를 전혀 테스트하지 않는다고 답했습니다. 그러나 대부분의 기업에서 일정 수준의 API 테스트를 진행하고 있습니다. 일본 전체 응답자 중 API 테스트를 전혀 진행하지 않는다고 답한 비율은 4%에 불과합니다.

일본 자동차 제조사는 API 리스크에 대한 가시성이 부족합니다

일본 자동차 기업의 8%만이 어떤 API가 민감한 데이터를 반환하는지 알고 있습니다. 일본 경제에서 자동차 업계가 차지하는 중요성과 기업이 커넥티드 차량과 같은 제품에 API 기반 기술을 자주 통합하는 점을 고려할 때, 이는 다소 놀라운 결과입니다. 보이지 않는 것을 보호하는 것은 어렵습니다.

일본의 API 보안 및 컴플라이언스

중국, 인도, 호주 응답자의 약 90%는 API 보안을 컴플라이언스 요건 충족에 반영한다고 답했습니다. 일본에서는 이 비율이 낮아, 응답자의 22%가 API 보안을 컴플라이언스 노력에 반영하지 않는다고 답했으며, 그 이유로 다음과 같은 요인을 꼽았습니다.

- 시간 또는 리소스 부족
- 규제 당국이 아직 요구하지 않는다고 생각

일본의 전반적인 답변은 최고 경영진의 의견에 크게 영향을 받았습니다. 일본의 CISO, CIO, CTO 중 28%는 API가 컴플라이언스 프로그램에 포함되지 않는다고 답했습니다.

인도의 결과는 직원과 경영진 간의 큰 격차를 보여줍니다

인도는 일본과 유사한 수준으로 API 보안 인시던트 발생률이 높았습니다. 전체 응답자의 82%가 지난 1년간 API 보안 인시던트를 경험했다고 답했으며, 에너지 및 유틸리티 업계의 모든 응답자(100%)가 인시던트를 보고했습니다. 보험 업계는 가장 낮은 발생률을 기록했으며, 응답자의 60%가 인시던트를 보고했습니다.

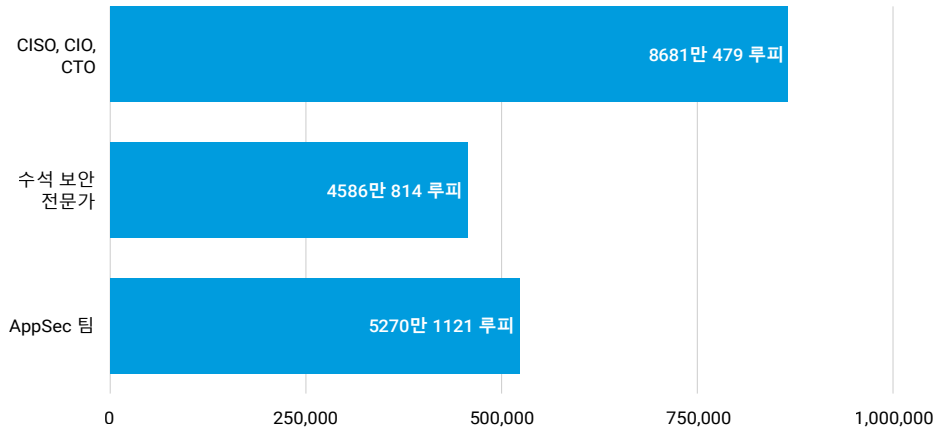
인도에서도 다른 국가의 전체 결과와 유사하게 "API 설정 오류"가 API 보안 인시던트의 가장 흔한 원인(23%)으로 꼽혔으며, 근소한 차이로 "잘 알려진 보안 툴 및 서비스(Microsoft 등)"(22%)과 "GenAI 툴 내 API"(22%)가 뒤를 이었습니다. 인도에서 API 보안 인시던트의 원인에 대한 추가적인 주요 포인트는 다음과 같습니다.

- 응답자는 "API 코딩 오류로 인한 취약점"을 가장 적게 지적했습니다.
- 에너지 및 유틸리티와 헬스케어 업계는 LLM 같은 GenAI 툴 내 API를 가장 많이 지적했습니다.
- 수석 보안 전문가들이 가장 많이 언급한 원인은 GenAI 툴 내 취약점으로, 인도 전체 평균보다 약 10% 포인트 높았습니다.
- 제조와 리테일 및 이커머스는 잘 알려진 외부 기술 툴 또는 서비스를 가장 많이 지적했습니다.

API 보안 인시던트는 인도 기업에 내부적, 직원 관련 요인으로 영향을 미쳤으며, 응답자의 대부분은 "팀 및 부서에 대한 기업의 내부 조사 증가"(32%)와 "팀 및 부서 스트레스나 압박 증가"(31%)를 가장 큰 영향으로 꼽았습니다. 보험과 리테일 및 이커머스 업계는 "고객 호감도 하락 및 고객 계정 이탈"을 가장 큰 영향으로 꼽았습니다.

인도에서 보고된 API 보안 인시던트의 평균 비용은 6206만 3515 루피였으며, 여기에서도 최고 경영진의 추산치는 현장 보안 담당자의 추산치보다 훨씬 높았습니다.

API 보안 인시던트가 기업에 어떤 비용 및/또는 영향을 초래했나요? (최대 3개 선택)
인도 보안 리더와 직원들의 API 인시던트 비용에 대한 관점

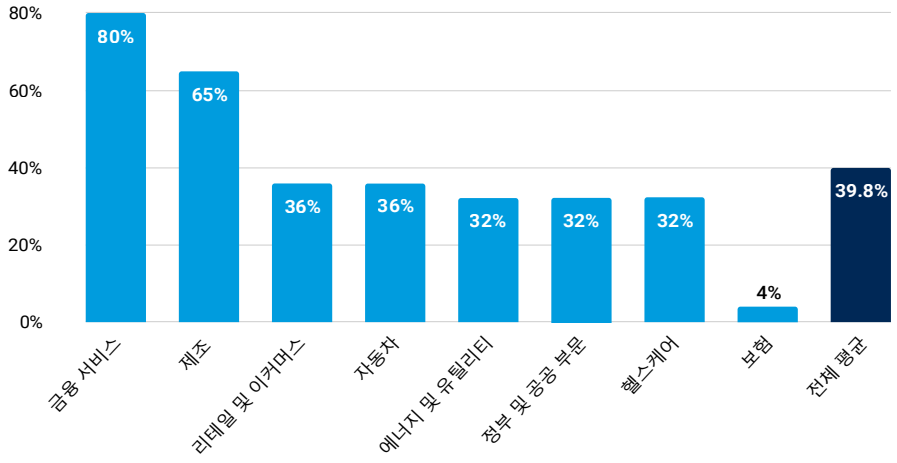


인도에서는 금융 서비스(1억 2828만 8777 루피, 또는 US 148만 552 달러)와 리테일 및 이커머스(1억 1797만 8722 루피, 또는 US 136만 1566 달러)의 두 업계가 전체 평균 비용을 크게 끌어올렸습니다.

인도에서 응답자의 64%가 전체 API 인벤토리를 보유하고 있다고 보고했지만, 이 중 39%만 민감한 데이터를 반환하는 API를 알고 있다고 답했습니다. 이 결과는 중국(39.4%)과 일본(37%)과 유사하지만 호주(27.9%)보다 높습니다. 금융 서비스(80%)와 제조(65%) 응답자의 대부분은 민감한 데이터를 반환하는 API를 알고 있다고 답했지만 보험업계 응답자 중에서는 4%만 이를 알고 있다고 답했습니다.

전체 API 인벤토리를 보유하고 있으며 어떤 API가 민감한 데이터를 반환하는지 알고 있나요?

인도 업계별 현황과 국가 전체 평균 비교



가시성 격차는 역할별로 더 두드러졌습니다.

- 최고 경영진(77%)과 수석 보안 전문가(75%)가 AppSec 팀(41%)보다 전체 API 인벤토리를 보유하고 있다고 응답한 비율이 훨씬 높았습니다.
- 최고 경영진(65%)과 수석 보안 전문가(43%)는 AppSec 팀(11%)보다 어떤 API가 민감한 데이터를 반환하는지 알고 있다고 응답한 비율이 훨씬 높았습니다.

이 때문에 AppSec 팀은 "공격자로부터 API 보호"를 최우선 과제(24%)로 꼽았지만, 최고 경영진은 "클라우드 보안 솔루션"(35%)을 더 우선시했습니다. 한편, 수석 보안 리더들은 평균적으로 "개발자 비밀 관리 및 보호"(36%)를 최우선 과제로 꼽았습니다.

전체적으로 "공격자로부터 API 보호"(21%)은 인도에서 사이버 보안 우선순위 4위를 차지했으며, "클라우드 보안 솔루션"(27%), "개발자 비밀 관리"(25%), "애플리케이션 보호"(23%)가 목록에 올랐습니다.

이제 중요한 주제인 API 테스트의 역할에 대해 알아보겠습니다. 조사 대상 4개국 중 인도에서 API 보안 인시던트의 원인으로 “코딩 오류로 인한 취약점”을 가장 적게 지목했으며 13개 원인 중 최하위를 기록했습니다. 코딩 오류는 개발 단계에서 발생하기 때문에 기업이 API를 얼마나 자주 테스트하는지 살펴보아야 합니다. 문제는 실시간 테스트가 없으면 API 공격이 코딩 오류로 인해 발생했는지조차 파악하기 어렵다는 점입니다. 기업이 취약점을 발견하지 못하면 이를 공격의 원인으로 지목하지 않을 가능성이 높습니다.

응답자에게 API 보안 테스트(프로덕션 단계 및 전체 API 수명 주기 전반)을 통해 악용 징후를 확인하는 빈도를 물었습니다. 인도에서 전체 API 테스트 빈도 분포는 다음과 같습니다.

- 매주: 31%
- 매일: 21%
- 실시간: 15%

실시간으로 API를 테스트하는 기업에 한정해 보면 인도 업계별 분포는 전체 평균 15%와 비교해 다음과 같습니다.

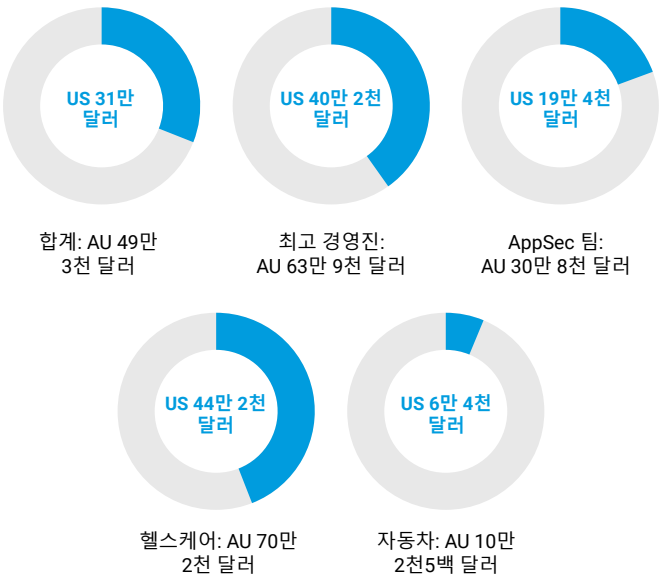
- 금융 서비스: 24%
- 헬스케어: 20%
- 제조: 19%
- 자동차: 4%
- 에너지 및 유틸리티: 4%

호주는 가장 많은 API 보안 인시던트를 경험했습니다

조사된 APAC 4개국 중 호주에서 응답자의 95%가 인시던트를 보고하며 지난 12개월 동안 API 보안 인시던트 발생률이 가장 높았습니다. 응답자의 대부분은 이러한 인시던트의 원인으로 "API 설정 오류"(23%) 또는 "API 게이트웨이의 탐지 실패"(23%)를 지목했지만, 많은 응답자는 내부 프로세스를 언급했으며 이는 "권한 취약점", "API 코딩 오류로 인한 취약점", "API가 인터넷에 의도치 않게 노출됨"(각각 약 21%) 등이 포함되었습니다.

API 보안 인시던트를 경험한 경우, 해당 인시던트로 인해 발생한 총 재정적 영향은 얼마였나요?

호주 응답자 5개 그룹의 API 인시던트 비용에 대한 관점



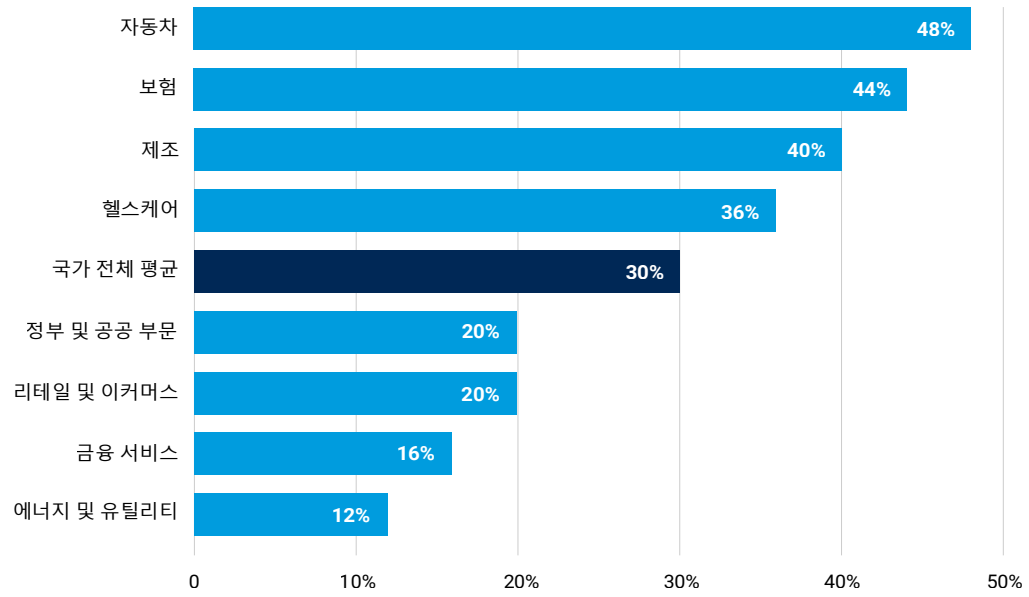
API 보안 인시던트의 비용은 호주에서 다른 APAC 국가보다 더 큰 영향으로 인식되었으며, "고위 경영진 또는 이사회에서 부서의 평판 하락"(33%)에 이어 두 번째로 높은 32%를 기록했습니다. "규제 기관의 벌금"은 전체적으로 볼 때 네 번째로 많이 언급된 영향이었지만, 수석 보안 전문가들 사이에서 가장 많이 언급되었으며 보험, 에너지 및 유틸리티, 제조 등 3곳의 업계에서도 마찬가지였습니다.

호주의 CISO, CIO, CTO는 API 보안 인시던트의 내부적 영향에 특히 집중했습니다. 이들이 가장 많이 언급한 영향은 "팀이나 부서 스트레스 및/또는 압박 증가"와 "고위 경영진 및/또는 이사회에서 부서의 평판 하락"이 32.8%로 동률을 이뤘습니다.

호주는 조사 대상 국가 중 전체 API 인벤토리를 보유하고 있다고 응답한 비율이 가장 높았지만(81%), 이 그룹에서 민감한 데이터를 반환하는 API를 알고 있다고 응답한 비율은 가장 낮았습니다(30%). 단 한 개의 기업만이 API 인벤토리를 전혀 보유하고 있지 않다고 응답했습니다.

전체 API 인벤토리를 보유하고 있으며 어떤 API가 민감한 데이터를 반환하는지 알고 있나요?

호주 업계별 현황과 국가 전체 평균 비교



호주에서 API 보안 인시던트가 자주 발생하지만, “공격자로부터 API 보호”는 호주 응답자의 사이버 보안 우선순위에서 최우선 순위가 아닌 4위(21%)를 차지했으며, “엔드포인트 보안”(26%), “개발자 비밀 관리 및 보안”(24%), “SIEM”(24%)이 목록에 올랐습니다. “공격자로부터 API 보호”는 호주 기업의 최우선 과제 중 “데이터 손실 차단”과 약 21%로 동일하게 나타났습니다.

호주 응답자는 API 취약점을 라이프사이클 초기 단계에서 조기 탐지하는 데 있어 필요한 실시간 API 테스트 비율이 4개국 중 가장 낮았으며(6%), 대부분의 테스트는 매일(34%) 또는 주간(35%)으로 진행되었습니다. 호주 금융 서비스, 헬스케어, 제조 업계 응답자 중 실시간 테스트를 실시한다고 답한 응답자는 없었습니다.

호주의 실시간 테스트 부족은 우려스러운 현상으로 추가 조사할 필요가 있습니다. API 보안 및 컴플라이언스를 다룬 다음 섹션에서 언급됐듯이 호주의 소비자 데이터 권리 규정은 기업 개발자가 표준화되고 안전한 방식으로 API를 구축하도록 보장하는 기준을 포함하고 있습니다.

코딩 오류나 기타 예방 가능한 리스크가 내장된 API야말로 공격자들이 노리는 대상입니다. 기업이 API를 조기에 자주 테스트하면 보안팀과 개발팀이 우위를 점할 수 있습니다.

기업이 API 리스크를 컴플라이언스 프로그램에 반영하고 있나요?

전 세계적으로 기업에 API를 문서화하고 설명하도록 요구하는 규제 기관이 증가하고 있으며 규제 기관의 메시지가 전달되고 있는 것 같습니다. 조사 대상 4개국의 응답자는 API와 API 보안이 규제 요구사항에 어떻게 반영되는지 잘 알고 있었습니다.

중국, 인도, 호주 응답자의 약 90%는 규제 요구사항을 충족하기 위해 API 보안을 고려한다고 답했습니다. 일본에서는 이 비율이 낮았으며, 응답자의 22%는 시간이나 리소스 부족, 또는 규제 기관이 아직 요구하지 않는다는 이유로 API를 고려하지 않는다고 답했습니다. 일본의 전체 응답은 최고 경영진의 영향이 컸습니다. 일본 CISO, CIO, CTO의 28%는 API가 컴플라이언스 프로그램에 포함되지 않는다고 밝혔습니다.

그러나 조사 대상 4개국에서 API를 컴플라이언스 프로그램에 통합하기 위해 필요한 조치를 취하는 기업이 아직 많지 않습니다. API를 고려한다고 답한 응답자 중에서도 대부분의 규제 당국이 요구하는 리스크 평가, 보고, 보안 계획 등의 세 가지 필수 영역에 API를 포함시킨 경우가 절반에 미치지 못했습니다. 실제로 리스크 평가에 API를 고려하는 응답자는 41%, 보고 요구사항으로 API를 고려하는 응답자는 40%에 불과했습니다.

이러한 차이가 왜 중요할까요? 공격자는 취약한 API를 직접 표적으로 삼아 데이터 유출 공격을 간소화할 수 있다는 점을 알고 있습니다.

개인정보 보호법 실행 (일본):

개인정보를 대량으로 처리하거나 리스크가 높은 데이터 처리 활동을 포함하는 API에 대한 데이터 보호 영향 평가를 실시해 리스크를 식별하고 방어해야 합니다.

중화인민공화국 데이터 보안법:

애플리케이션, 시스템, 클라우드 환경 간 정보를 교환하는 API와 같은 기술을 통한 고객 데이터 접속을 보호하기 위해 강력한 조치를 구축해야 합니다.

디지털 개인 데이터 보호법(인도):

API를 통해 발생할 수 있는 데이터 유출을 포함해 데이터 유출을 탐지하는 메커니즘을 갖추고, API와 API 보안 노력을 포함하는 정기적인 컴플라이언스 감사를 실시해야 합니다.

소비자 데이터 권리 (호주):

개발자가 API를 일관되고 안전한 방식으로 구축하도록 보장하는 기준을 포함하며, API를 포함한 방식을 통해 전송 및 접속 시 소비자 데이터를 보호하기 위한 프로토콜을 강조합니다.

보안팀을 위한 핵심 내용 및 다음 단계

우선순위에서 API 보안이 차지하는 비중을 확인하는 지침이 필요한 보안 리더 및 팀원에게 이번 조사 결과는 몇 가지 설득력 있는 출발점을 제공합니다.

- 공격, 악용, 데이터 유출 같은 API 보안 인시던트는 조사 대상 4개국에서 자주 발생하고 있습니다.
- 최고 경영진(CISO, CIO, CTO), 수석 보안 전문가, AppSec 팀 간에 이러한 인시던트의 비용 및 신뢰 상실과 같은 다양한 영향에 대한 인식 차이가 크게 존재합니다. 이들은 API에 대한 가시성과 해당 API의 민감한 데이터 반환 여부에 대한 지식 측면에서도 일관된 입장을 보이고 있지 않습니다.
- API의 취약점에 대한 기업의 이해가 부족하거나, 공격자가 악용할 수 있는 취약점이 널리 퍼져 있거나, 또는 둘 다일 수 있습니다. 이는 내부 프로세스의 부족과 기존 API 보안 솔루션의 취약점이 원인일 가능성이 높습니다.

기업이 중요한 데이터, 고객 관계, 내부 팀원을 보호하기 위한 효과적인 API 보안 접근 방식을 구축하려면 먼저 API 보안 인시던트의 원인, 영향, 우선순위 수준에 대한 합의를 도출해야 합니다. 그 다음, 개발 및 프로덕션 환경에서 API를 보호하기 위한 명확하고 포괄적인 프로세스를 수립하는 것이 도움이 됩니다. 마지막으로, 이러한 작업을 지원할 수 있는 보안 툴이 필요합니다.

다음은 지속 가능한 API 보안 전략을 구축하기 위한 단계별 접근 방식입니다.

1. **API 검색 및 가시성부터 시작하기**
   전체 API 자산의 완전한 인벤토리를 작성하려면 API와 이 API가 지원하는 마이크로서비스를 자동으로 검색할 수 있는 툴을 찾으세요. 관리되지 않는 API는 공격자의 주요 표적이 되므로 광범위한 보안 범위를 갖추는 것이 중요합니다.

2. **테스트에 투자하기**
   API가 의도된 기능을 수행하기 위해 코딩되었는지 쉽게 테스트할 수 있는 API 보안 솔루션을 선택하세요. 배포 전에 테스트를 진행하는 것이 이상적이지만, 트래픽 및 잠재적인 취약점에 대한 실시간 분석을 통해 이미 프로덕션 중인 모든 API를 테스트하는 것도 중요합니다.

3. **API를 완전히 문서화하기**
   전체 API 환경을 감사해 설정 오류가 있는 API나 기타 오류를 식별하는 것이 중요합니다. 또한 감사 기능을 통해 모든 API에 대한 적절한 문서화를 보장하고 민감한 데이터가 포함되어 있는지 또는 적절한 보안 제어가 부족한지 확인합니다. 이는 암시적 또는 명시적으로 API 보안을 포함하는 컴플라이언스 의무 사항을 준비하는 데도 도움이 됩니다.

4 **런타임 탐지 사용하기**
자동화된 런타임 탐지 기능을 갖춘 API 보안 솔루션을 사용하면 '정상'과 '비정상' API 활동을 구분할 수 있습니다. 이러한 방식으로 API 상호 작용을 모니터링하면 위협을 나타내는 행동을 실시간으로 탐지하고 조치를 취할 수 있습니다.

5 **의심스러운 행동에 대응하기**
API 보안 솔루션을 기존 보안 스택(예: WAF 또는 웹 애플리케이션 및 API 보안)과 통합하면 리스크 수준이 높은 행동을 찾아내고 의심스러운 트래픽이 중요한 리소스에 접속하기 전에 차단할 수 있습니다.

6 **위협 조사 및 탐색하기**
가장 성숙한 API 보안 단계에서는 과거 위협 데이터에 대한 포렌식 분석을 사용해 알림이 위협을 올바르게 식별했는지, 정교한 툴과 인간 지능의 조합을 사용해 선제적 위협 헌팅을 가능하게 하는 패턴이 나타났는지 파악합니다.

API 보안 모범 사례에 대한 추가 인사이트는 다음 두 논문을 참고하세요.

- **OWASP의 상위 10대 API 보안 리스크 방어**
- **API 위협 탐지 및 대응을 위한 11가지 핵심 기능**

추가 지원을 원하면 사용자 맞춤화 **Akamai API Security 데모를 예약하세요**

API 보안 영향 연구에 대한 정보

중국, 일본, 인도, 호주 기업을 대상으로 한 2025년 보안 영향 연구 리서치는 2024년 10월 14일부터 30일까지 Opinion Matters가 진행했습니다. Opinion Matters는 총 806명의 응답자를 대상으로 조사했으며, 각국에서 최소 200명의 응답자가 참여했습니다. 8개 주요 업계(자동차, 금융 서비스, 리테일 및 이커머스, 헬스케어, 보험, 정부 및 공공 부문, 제조, 에너지 및 유틸리티)에서 응답자 중 3분의 1은 CIO, CTO 또는 CISO, 3분의 1은 수석 보안 전문가, 나머지 3분의 1은 250~400명 미만에서 1000명이 넘는 규모까지 다양한 회사에서 근무하는 애플리케이션 보안팀에 속했습니다.

Opinion Matters는 Market Research Society의 규정에 따라 협회의 회원을 고용하며 MRS 행동 강령 및 ESOMAR 원칙을 준수합니다. Opinion Matters는 British Polling Council의 회원이기도 합니다.

크레딧

주저자
바니 빌(Barney Beal)

관리 편집자 겸 콘텐츠 전략가
존 나탈레(John Natale)

카피 에디터
쿨렌 피니(Cullen Pitney)

프로모션
엘렌 오브라이언(Ellen O'Brien)

마케팅 및 출판
조지나 모랄레스 햄프(Georgina Morales Hampe)

인터넷 보안 현황 보고서

Akamai의 지난 인터넷 보안 현황 보고서를 읽고 다음 보고서를 확인하세요. **akamai.com/soti**

Akamai 위협 연구팀

akamai.com/security-research에서 최신 위협 인텔리전스 분석, 보안 보고서, 사이버 보안 리서치 내용을 확인하세요.

Akamai API Security

Akamai가 API 검색, 체계 관리, 런타임 보호 및 API 보안 테스트 등 중요한 기능을 통해 개발부터 프로덕션까지 전체 수명 주기 동안 API를 보호하는 방법에 대해 알아보세요. **https://www.akamai.com/products/api-security**

이 보고서의 데이터 확인

이 보고서에 참조로 사용된 그래프와 차트의 고품질 버전을 확인하세요. Akamai가 제공한 소스라는 점이 정식으로 인정되고 Akamai 로고가 보존되는 경우 이러한 이미지를 무료로 사용 및 참조할 수 있습니다. **https://akamai.com/api-security-study-asia-data**

Akamai Security는 성능이나 고객 경험에 영향을 주지 않으면서 상호 작용이 일어나는 모든 지점에서 비즈니스의 원동력이 되는 애플리케이션을 보호합니다. 글로벌 플랫폼의 규모와 위협에 대한 가시성을 활용해 고객과 협력함으로써 위협을 예방, 탐지, 방어하고 브랜드 신뢰를 쌓고 비전을 실현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관한 자세한 정보를 보려면 akamai.com 및 akamai.com/blog를 방문하거나 X(기존의 Twitter) 및 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 05월 25일 발행.