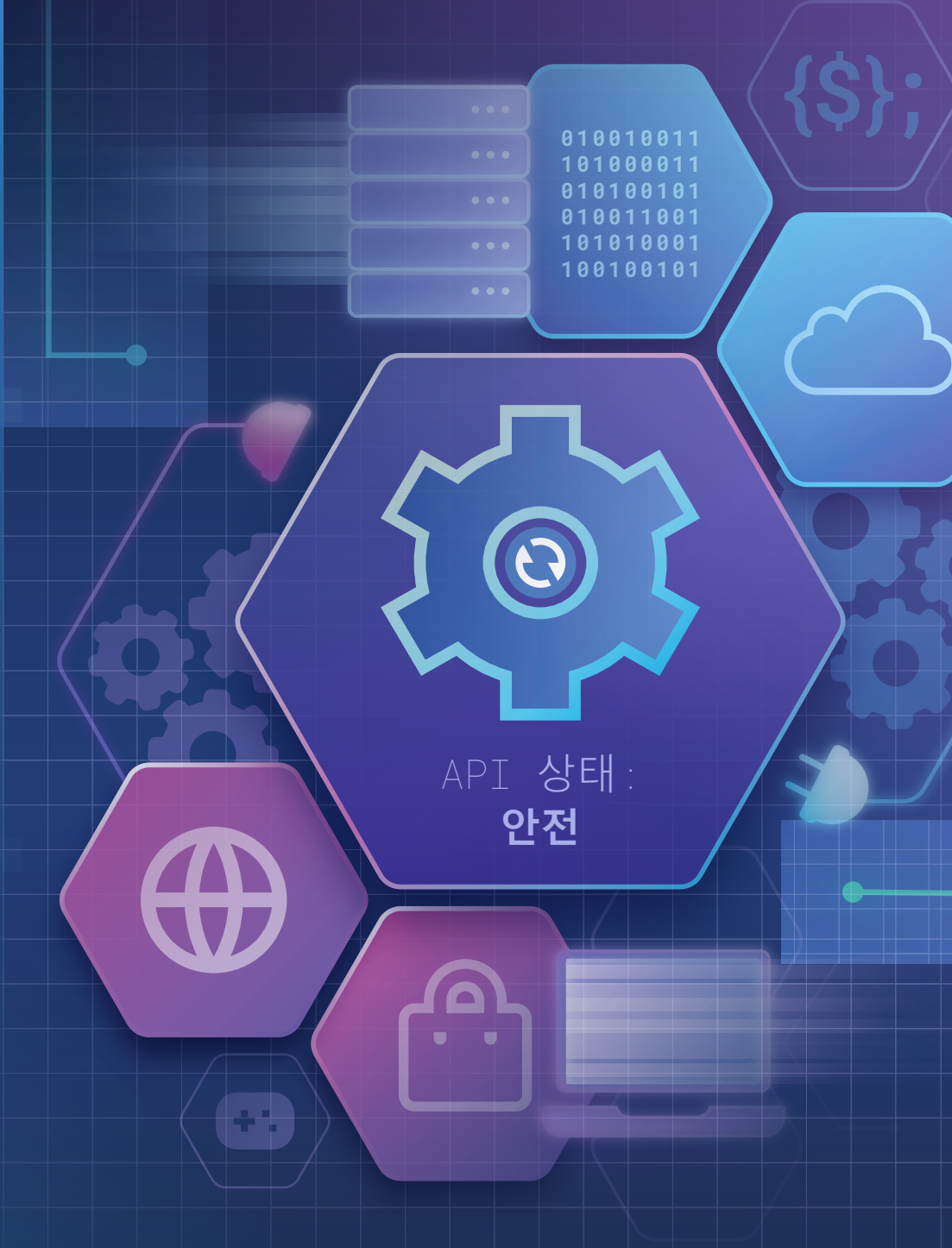
API 보안 영향 연구 2024



API 인시던트가 기업과 팀에 미치는 영향

Akamai

Akamai 인터넷 보안 현황(SOTI) 보고서 제휴사 간행물

목차

핵심 요약

이제 3년째에 접어드는 API 보안 영향 연구(기존의 API 보안 단절 보고서)에서는 미국, 영국 그리고 2024년에 새로 포함된 독일에서 1207명의 리더와 실무자를 대상으로 실시한 설문 조사를 바탕으로 API 보안 상태를 살펴봅니다. 이 연구에서는 기업이 API 보안 이벤트, 즉 이벤트의 빈도, 원인 및 영향을 어떻게 경험하는지 알아보고, 보안 부서가 어떻게 API를 공격 기법으로서 다루는지 살펴봅니다.

최대한 전체적으로 상황을 파악하기 위해 다음과 같이 조사 대상의 균형을 맞추었습니다.

CISO, CIO, CTO, 수석 보안 전문가, 직원 수 500명 미만~1000명이 이상 기업의 AppSec 팀원

8개 업계: 금융 서비스, 리테일 및 이커머스, 헬스케어, 정부 및 공공 부문, 제조, 에너지 및 유틸리티, 2024년에 새로 포함된 자동차와 보험

서론

API는 API가 널리 확산되어 있으며 피해를 주고 있다는 사실을 나타내는 데이터가 있음에도 새로운 공격 기법으로 간주되곤 합니다. 다음 통계를 확인해보세요.

- 최신 Akamai 인터넷 보안 현황(SOTI) 보고서에 따르면 2023년 1월부터 2024년 6월까지 1080억 건의 API 공격이 기록되었습니다.
- 2024년 5월, Gartner® API 보안 시장 가이드*에서는, "현재 데이터에 따르면, 평균적인 API 유출 사고에서 유출되는 데이터는 평균적인 보안 유출에서보다 10배 이상 더 많은 것으로 나타났습니다."라고 언급했습니다.
- 공격 또한 증가하고 있습니다. SOTI는 2023년 1분기와 2024년 1분기 사이에 웹 애플리케이션 및 API 공격이 합쳐서 49% 증가했다고 보고했습니다.

이러한 증가는 놀라운 일이 아닙니다. 보이지 않는 곳에서 API는 디지털 이니셔티브를 이끄는 거의 모든 기술 간의 통신 및 데이터 교환을 지원합니다. 여기에는 GenAI 툴, 고객 대면 앱, 클라우드 서비스 등이 포함됩니다. 그러나 인증 없이 구축되거나, 설정 오류를 포함하거나, 완전히 잊혀진 API에 대한 보호가 부족하기 때문에 사이버 범죄자들에겐 매력적이고 비용 효율적인 공격 기법으로 이용됩니다. 이들은 하나의 취약한 API를 찾기만 하면 해당 취약점을 통해 호출 시 반환되는 모든 데이터에 직접 접속할 수 있으며, 이는 수천 개의 레코드일 수 있습니다.

전체적으로 봤을 때, Akamai의 리서치에 따르면 API 보안은 아직 포괄적인 보안 전략의 핵심 요소가 되지 못한 것으로 나타났습니다. 대부분의 기업은 API 위협을 새로운 위협으로 간주하지만, 공격 데이터는 물론 Akamai의 연구에 나온 재정적 영향과 팀이 받는 스트레스까지 고려했을 때 API 위협은 늘어나고 있으며 종종 성공합니다. Akamai의 2024년 연구 결과에는 API 보안 인시던트가 업계 동료 및 기업에 어떤 영향을 미치는지 나와 있습니다. 이 데이터를 기반으로 API 보안을 보다 잘 평가하고 필요한 부분을 개선할 수 있기를 바랍니다.

많은 API들이 충분한 보호되고 있지 않기 때문에 사이버 범죄자들에게 매력적이고 저렴한 공격 기법으로 사용되고 있습니다.

주요 결과: 비즈니스에 영향을 미치고 스트레스를 유발하는 API 인시던트

2024년 연구 결과에 따르면, API는 점차 증가하고 있으며 팀에 상당한 보안 문제를 일으키는 공격 기법입니다. 응답자들은 다음과 같은 사항에 대해 동일한 의견을 보였습니다.

- 지난 3년간 API 보안 인시던트가 계속 증가하고 있음
- API 관련 인시던트의 처리 및 복구에 평균 50만 달러 이상 금액 지출(미국의 C레벨 응답자에 따르면 평균 재정적 영향은 미화 94만 3162달러 수준)
- API 인시던트에 대한 인적 부담, 팀이 받는 스트레스 및 평판 손상(특히 내부 조사로 이러한 압박이 가중됨), 인시던트를 해결하는 비용보다 훨씬 높은 수준

API 인벤토리의 완전성에 대한 응답자들의 견해는 매우 다양했으며, 직책별로 세분화했을 때 이런 의견 차이는 더욱 분명하게 나타났습니다(11페이지 참조). 특히 어떤 API가 민감한 데이터를 반환하는지 파악할 수 있는 완전한 API 인벤토리를 갖춘 기업이 2023년 40%로 이미 낮은 수준이었지만 2024년 27%로 더 하락했습니다.

응답자들은 또한 API를 보호하기 위해 사용한 기존 툴이 리스크를 완전히 해결하지 못한다고 지적했습니다. API 공격 성공의 일차적인 원인으로는 애플리케이션 방화벽(WAF), API 게이트웨이, 네트워크 방화벽 등의 툴이 언급되는 경우가 많았습니다(17페이지의 전체 원인 목록 및 12페이지의 WAF 및 WAAP에 대한 참고 사항 참조).

보안 전문가들은 API 인시던트에 대해 부담을 느끼고 있으며, 이러한 인시던트의 해결을 위한 비용보다 팀이 받는 스트레스와 평판 손상으로 인한 영향이 높은 순위를 차지했습니다.

또한 연구 결과에 따르면, API 보안 전략에 초점을 맞추어야 한다는 증거에도 불구하고, 아직 더 우선시되지 못하는 몇 가지 주요 이유를 추론해볼 수 있습니다. 한 가지 핵심 요소는 보호해야 하는 API의 수, 위치 및 리스크 속성에 대한 주요 보안 업무 담당자 간 조정이 부족하다는 점입니다. 그 원인으로는 API에 대한 가시성 부족 및 단일 데이터 소스 부재를 들 수 있습니다.

또한 API 공격의 원인에 대한 보안 리더와 실무자 간의 의견 불일치도 나타났습니다. 이들이 사용하는 툴, 개발 과정에서 코더가 저지른 실수 또는 GenAI 혁신의 허점 중 무엇이 공격의 원인일까요? 이는 응답자에 따라 다릅니다.

물론, API 보안이 전략적으로 주목받지 못하는 또 다른 이유는, 팀이 이미 다른 시급한 위협에 대처하기 위해 노력하고 있으며, 대부분의 예산, 팀의 주요 관심사 및 노력이 여기에 투입될 가능성이 크다는 점입니다. 이제 연구 결과에 대해 자세히 알아보겠습니다.

API 보안 영향 연구 — 2024
주요 연구결과 스냅샷

84% 지난 12개월 동안 API 보안 인시던트를 경험한 응답자의 비율

지난 12개월 동안 API 인시던트를 처리하는데 소요된 평균 비용:

미국	영국	독일
$591,404	£420,103	€403,453

낮은 가시성

전체 API 인벤토리를 보유한 기업 중 27%만이 어떤 API가 민감한 데이터를 반환하는지 알고 있습니다. 이는 2023년의 40%에서 줄어든 수치입니다.

높은 스트레스

API 인시던트의 영향 1위 CISO: 고위 경영진 또는 이사회에서 부서의 평판이 손상됩니다. CIO: 팀 또는 부서가 받는 스트레스나 압박이 증가합니다.

불충분한 테스트

API 개발부터 프로덕션까지 실시간으로 API를 테스트하는 응답자는 13%, 매일 테스트하는 응답자는 18%에 불과합니다.

API 보안 인시던트의 재정적 비용은 팀 및 리더에게 미치는 영향을 더욱 가중시킵니다. 비용이 많이 드는 유출이 발생하면 조사가 진행되고, 이사회와 같은 영향력 있는 관계자들에게 업무를 성공적으로 수행하고 있지 않은 것처럼 보일 수 있습니다. 그러면 스트레스가 더욱 가중됩니다. 실제로 여러 지역의 설문 조사 참가자들은 API 보안 인시던트의 가장 큰 영향이 팀이 받는 스트레스라고 말했습니다.

API 보안의 현황

지난 3년 동안 API 보안 인시던트를 보고하는 기업이 꾸준히 늘어났으며 2024년에 84%까지 증가했습니다(아래 참조). 이러한 API 공격이 기업에 어떤 영향을 미치고 있나요? 리스크를 낮추기 위해 무엇을 하고 있고, 무엇을 하고 있지 않나요? 이 보고서에서는 이러한 질문에 대한 답변의 형식으로 연구 결과를 제시했습니다.

API 공격이 기업과 보안 팀에 큰 영향을 미치고 있나요?

답은 '예'입니다. API 보안 인시던트의 재정적 영향에 대한 데이터를 수집하던 첫 해에, 지난 12개월 동안 API 보안 인시던트를 경험한 84%를 대상으로 조사한 결과, API 인시던트를 해결하는 평균 비용(시스템 수리, 다운타임, 법적 수수료, 벌금 및 기타 관련 비용 포함)이 상당한 수준인 것으로 나타났습니다.

- **59만 1404달러**(미국)
- **42만 103파운드**(영국)
- **40만 3453유로**(독일)

특정 지책에서 이 비용을 더 높게 평가했습니다. 특히 미국 C레벨 응답자는 94만 3162달러라고 보고했으며, 이는 전체 미국 응답자 평균보다 약 60% 더 높은 수준입니다.

지난 12개월 동안 API 보안 인시던트를 경험했나요?

년	합계	미국	영국	독일
2022	76%	75%	77%	—
2023	78%	85%	69%	—
2024	84%	83%	83%	84%

정확한 수치는 차치하더라도 API 보안 인시던트의 재정적 비용은 인적 영향을 더욱 가중시킵니다. 비용이 많이 드는 유출이 발생하면 조사가 진행되고, 이사회와 같은 영향력 있는 관계자들에게 업무를 성공적으로 수행하고 있지 않은 것처럼 보일 수 있습니다. 그러면 스트레스가 더욱 가중됩니다. 실제로 여러 지역의 설문 조사 참가자들은 API 보안 인시던트의 가장 큰 영향이 '스트레스', 특히 팀이 받는 스트레스라고 말했으며, 그 다음으로 '고위 경영진 또는 이사회에서 부서의 평판 손상', 3위로 '해결 비용'을 들었습니다. 특히 사기에 가장 큰 영향을 미치는 내부 영향이 다시 등장해 하위 3개 순위를 차지했으며, 거의 유사한 수치를 보였습니다(아래 참조).

업계별로 세분했을 때 결과는 유사했습니다. 'API 유출 후 팀이 받는 스트레스 또는 압박 증가'는 설문 조사에 포함된 8개 업계 중 4개 업계에서 1위를 차지했습니다(9페이지의 사이드바 참조). 여기에는 금융 서비스가 포함됩니다. 특히 이 분야는 전체 업계 중 가장 높은 재정적 영향(미화 83만 2801달러)을 보고했습니다.

가장 많이 인용된 API 보안 인시던트 영향

1. 팀 또는 부서 스트레스나 압박 증가 - **27.0%**
2. 고위 경영진 또는 이사회에서 부서의 평판 손상 - **26.6%**
3. 문제 해결을 위해 비용 발생 - **25.8%**
4. 규제 기관의 벌금 - **25.4%**
5. 고객 호감도 하락 및 고객 계정 이탈 - **25.0%**
6. 생산성 손실 - **24.1%**
7. 신뢰와 평판 손실 - **23.8%**
8. 직원 호감도 하락 - **23.8%**
9. 팀 또는 부서에 대한 기업의 내부 조사 증가 - **23.5%**

질문: API 보안 인시던트가 기업에 어떤 비용 및/또는 영향을 초래했나요? (최대 3개까지 선택) n=1207

API 공격으로 인한 재정적 비용과 인적 비용 간 관계또한 인시던트 영향에 대한 IT 및 보안 리더의 응답에서 확실하게 드러났습니다(본 설문 조사에서 각 응답자는 3개까지 응답 가능). 모든 지역의 모든 직책에서 공통된 한 가지는 API 보안 인시던트의 가장 큰 영향은 바로 직원에게 미치는 영향이라는 점입니다.

- CISO가 보고한 상위 2개의 영향('고위 경영진 또는 이사회에서 부서의 평판 손상' 및 '고객 호감도 하락 및 고객 계정 이탈')을 보면 인적 영향과 재정적 영향이 모두 31%로 거의 똑같은 수치를 나타냈습니다.
- 마찬가지로, CIO가 보고한 주요 영향('팀 또는 부서 스트레스나 압박 증가' 및 '해결 비용')은 34%로 비슷했습니다.

이 결과를 봤을 때 CISO와 CIO는 다음 질문을 고려해야 합니다. '근무 환경이 악화되고, 예산이 폭증하며, 고객 불만이 쏟아지게 만드는 보안 인시던트로 인해 내가 맡고 있는 팀이 계속해서 타격을 받는다면?' 이러한 리더들은 우수한 인재들이 떠나거나 해당 부서의 평판이 바닥으로 떨어지는 것을 원치 않습니다. 그리고 문제 해결 비용 및/또는 고객 이탈 등 재정적 압박이 추가되면 CISO와 CIO의 스트레스가 상당히 증가하게 됩니다. 실제로 '고객 평판 손상 및 고객 계정 이탈'은 보험 및 자동차 업계 응답자들의 응답에서 가장 높은 순위를 차지한 API 보안 인시던트 영향이었습니다 (업계별 결과에 대한 자세한 내용은 다음 페이지의 사이드바 참조).

나머지 업무에서 높은 순위를 차지한 응답은 다음과 같습니다.

- CTO, 30%, '직원 호감도 하락'
- 수석 보안 전문가, 27%, '고위 경영진 또는 이사회에서 부서의 평판 손상'
- AppSec 팀, 31%, '팀 또는 부서 스트레스나 압박 증가'

가장 많이 인용된 업계별 API 보안 인시던트 영향	
자동차	고객 호감도 하락 및 고객 계정 이탈 - **33%**
에너지 및 유틸리티	고위 경영진 또는 이사회에서 부서의 평판 손상 - **36%**
금융 서비스	'팀 또는 부서 스트레스나 압박 증가'와 '규제 기관의 벌금' 모두 동일 - **29%**
정부 및 공공 부문	팀 또는 부서 스트레스나 압박 증가 - **29%**
헬스케어	'신뢰와 평판 손실'과 '생산성 손실' 모두 동일 - **29%**
보험	고객 호감도 하락 및 고객 계정 이탈 - **28%**
제조	팀 또는 부서 스트레스나 압박 증가 - **34%**
리테일 및 이커머스	팀 또는 부서 스트레스나 압박 증가 - **29%**

질문: API 보안 인시던트가 기업에 어떤 비용 및/또는 영향을 초래했나요? (최대 3개까지 선택)
n=1207

API 및 잠재적 리스크에 대한 적절한 가시성이 있나요?

아니요, 정확히 말하자면 상황이 더 나빠졌습니다. 올해에는 전체 API 인벤토리를 갖추고 있으면서 어떤 API가 민감한 데이터를 반환하는지 알고 있는 응답자 비율이 2023년 40%로 이미 낮은 수준이었으나 2024년 27%로 더 하락했습니다. (더 많은 기업이 전체 인벤토리를 구축하려고 하지만, 모든 API를 찾고 각 API 내에서 벌어지는 활동을 식별하는 데 필요한 툴이 부족하다고 생각한다면 이 결과에 긍정적인 측면이 있을 수도 있습니다.)

전체 API 인벤토리를 갖추고 있으며, 어떤 API가 민감한 데이터를 반환하는지 알고 있는 응답자 비율은 **2023년 이미 낮은 수준인 40%**에서 **2024년 27%**로 더 하락했습니다.

API 인벤토리 및 인식 현황(전체 응답자)

	2024	2023
예, 어떤 API가 민감한 데이터를 반환하는지 **알고 있습니다**	27%	40%
예, 하지만 어떤 API가 민감한 데이터를 반환하는지 **모릅니다**	43%	32%
API에 대한 부분 인벤토리를 갖추고 있으며 어떤 API가 민감한 데이터를 반환하는지 **알고 있습니다**	23%	24%
부분 인벤토리를 갖추고 있지만 어떤 API가 민감한 데이터를 반환하는지 **모릅니다**	6%	4%
아니요, 인벤토리를 갖추고 있지 **않습니다**	1%	—

질문: API에 대한 전체 인벤토리를 갖추고 있으며 어떤 API가 민감한 데이터를 반환하는지 알고 있나요? (5가지 항목 중 선택) n=1207

조사에 응한 3개국 및 8개 업계의 리더들을 살펴보면, CISO보다 상당히 높은 비율의 CIO가 기업이 완전한 API 인벤토리를 갖추고 있다고 답변했습니다. 실무진 수준에서 보면 수석 보안 전문가와 AppSec 팀원 모두 CIO의 평균적인 관점과 대체로 일치하며 모든 API가 관리되고 있다고 믿었습니다.

그렇다면 이 5개의 직책은 API 호출 시 어떤 API가 민감한 데이터를 반환하는지 질문했을 때 어떤 차이를 보였을까요? 이러한 API 호출 대부분이 악성 소스에서 생성되고 일반적인 API 취약점을 악용하려고 하기 때문에 이에 대한 응답은 중요합니다.

공격자들이 데이터 접속을 위해 표적으로 삼는 관리되지 않는 API의 4가지 종류

1. **섀도 API**(일명 문서화되지 않은 API)는 실제로 존재하며 기업 내 공식 모니터링 채널 외부에서 운영됩니다.
2. **악성 API**는 시스템 또는 네트워크에 보안 리스크를 야기하는 인증되지 않았거나 악성 API입니다.
3. **좀비 API**에는 새 버전이나 다른 API로 완전히 대체된 후에도 계속 실행되는 API가 포함됩니다.
4. **사용되지 않는 API**는 API 변경으로 인해 더 이상 사용이 권장되지 않는 API입니다.

이러한 조사 결과는 API 리스크에 대한 가시성과 관련해 흥미로운 점을 시사합니다. 대부분의 CISO와 CTO는 전체 인벤토리를 갖추고 있지만 어떤 API가 민감한 정보를 반환하는지(앞으로 '민감한 데이터 인지'로 지칭) 모른다고 응답하거나, 부분 인벤토리를 갖췄으며 민감한 데이터를 인지하고 있다고 응답했습니다.

대부분의 CIO는 전체 API 인벤토리를 갖추고 있다고 보고했으며, 이들 중 42.9%는 민감한 데이터 인지가 충분하다고 답변한 반면, 36.3%는 이러한 인지가 없다고 답변했습니다. 수석 보안 전문가는 CIO와 의견을 같이했지만(75%가 전체 인벤토리 구축을 보고함) 민감한 데이터 인지에 대해서는 반대의 결과가 나타났습니다. 즉, 수석 보안 전문가의 32.5%는 민감한 데이터를 인지하고 있다고 말했으며 42.5%는 그렇지 않다고 응답했습니다.

마지막으로, 전체 응답자 중 가장 실무와 밀접한 AppSec 직원은 5개 직책 전체에서 가장 높은 수치를 나타냈습니다. 이들 중 거의 절반 정도가 민감한 데이터에 대한 인지 없이 전체 인벤토리를 갖추었다고 보고했으며, 나머지 절반은 다음 두 영역으로 분류되었습니다.

- 민감한 데이터를 인지하고 인벤토리를 모두 완전히 갖추고 있음
- API에 대해 민감한 데이터는 완전히 인지하고 있지만 인벤토리는 부분적으로 갖춤

인벤토리 측정이 아직 표준화되지 않아 단일 소스의 API 수를 산출하기에는 부족하다는 것을 알 수 있습니다. 이러한 차이를 감안할 때, 많은 기업이 전체 인벤토리를 갖추었어도 민감한 데이터를 완전히 인지하지 못할 가능성이 큽니다. 어떤 API가 민감한 데이터를 반환하는지 아는 것은 항상 중요합니다. 그러나 섀도, 악성, 좀비 및 사용되지 않는 API는 표적이 되기 쉽고, 보호되지 않으며, 일반적으로 기존의 보안 툴에서 간과되기 쉽기 때문에 부분 인벤토리도 중대한 리스크 요소입니다.

직책별로 살펴본 API 인벤토리 및 인식에 대한 현황

	CISO	CIO	CTO	Sr Sec Pro	AppSec
전체 인벤토리를 갖추고 있으며 어떤 API가 민감한 데이터를 반환하는지 **알고 있습니다**	17.2%	42.9%	16.5%	32.5%	26.4%
전체 인벤토리를 갖추고 있지만 어떤 API가 민감한 데이터를 반환하는지 **모릅니다**	41.4%	36.3%	34.8%	42.5%	47.4%
API에 대한 부분 인벤토리를 갖추고 있으며 어떤 API가 민감한 데이터를 반환하는지 **알고 있습니다**	32.5%	15.4%	39.9%	18.3%	20.4%
부분 인벤토리를 갖추고 있지만 어떤 API가 민감한 데이터를 반환하는지 **모릅니다**	8.3%	5.5%	8.2%	5.8%	5.2%

질문: API에 대한 전체 인벤토리를 갖추고 있으며 어떤 API가 민감한 데이터를 반환하는지 알고 있나요? (5가지 항목 중 선택)
n=1207

관리되지 않는 API가 만연해 있고 기존의 보안 툴로 탐지하기 어려운 현재와 같은 상황에서, 이 설문 결과에 따르면 API 공격 기법을 공격자에게 보다 매력적인 기법으로 만드는 공통의 보안 격차가 있음을 알 수 있습니다.

물론 관리되지 않는 API는 보안팀이 확인하고 평가해야 하는 최소 5가지 이상의 API 속성 중 하나일 뿐이며 다음과 같은 API가 포함됩니다.

- **알려진 취약점이 있는 API**로 패치가 적용되지 않은 API
- **관리되지 않거나 잊혀진 API**(섀도, 악성, 좀비, 사용되지 않는 API)
- **외부에 노출된 API**(예: 기업의 관리 범위를 벗어난 인증정보, 키 및 변수)
- **운영자 오류가 있는 API**(인프라 및 서비스의 보안 설정 오류)
- **발견되지 않은 취약점이 있는 API**로 공격자들이 취약점과 버그를 포착 및 악용하는 API

API 인벤토리 및 API 취약점에 대한 가시성과 관련해 여러 직책의 응답을 종합했을 때 최소 다음과 같은 결론이 도출되었습니다.

- 여전히 기업들은 API, 특히 리스크가 크고 관리되지 않은 API 발견 및 보안을 목적으로 설계되지 않은 보안 제품에 의존하고 있습니다.
- 보안 부서들은 식별 및 평가가 필요한 API의 리스크 속성을 아직 정의하지 못하고 있으며, API 검색 및 인벤토리화 전략에 대해 다양한 사업부, 개발자 팀, 벤더사 간 합의를 조율하지 못하고 있습니다.

모든 API를 보호하기 위한 보다 강력한 역량 구축에 투자하고 이를 효과적인 사례로 남기려면, 첫 번째 단계는 바로 이러한 단절을 극복하는 것입니다(18페이지의 'API 보안을 위한 보다 성숙한 보안 체계 구축 방법' 참조). 하지만 현재로서는 API 보안 예산을 받기 위해 필요한 관심과 지지가 부족합니다. 따라서 API와 웹 애플리케이션 방어 체계뿐만 아니라 기업의 전반적인 보안 체계를 강화하는 이니셔티브의 우선 순위를 높이고 예산을 편성하기 어렵습니다.

함께 하면 더 좋은 조치: WAAP + API 전용 보안

다중 공격 기법에서 위협을 신속하게 탐지하고 방어하기 위해 설계된 웹 애플리케이션 및 API 보안(WAAP)은 기존 WAF의 보호 기능을 확장합니다. **여기에 API 보안 솔루션을 함께 사용하면 방화벽 너머로 보안을 확장하기 때문에 훨씬 더 강력한 방어가 가능합니다**.

남용 또는 유출 리스크를 줄이기 위해 API를 자주 테스트하나요?

아니요, 그렇지 않습니다. 설정 오류가 있거나, 인증 제어 기능이 없거나, 코딩 오류가 있거나, 기타 예방 가능한 리스크를 은폐하는 퍼블릭 API가 바로 공격자들이 노리는 표적이며, 이들은 점점 더 효과적으로 이러한 표적을 찾고 있습니다.

따라서 개발 팀에서 이러한 API를 먼저 포괄적으로 테스트하지 않고 프로덕션에 보낼 때마다 의도치 않게 향후 보안팀에 과중한 업무를 안길 수 있습니다. 이러한 업무는 긴급한 조치가 필요하며, 조사 결과에서도 드러났듯이 팀이 받는 스트레스에도 크게 기여합니다.

하지만 이것은 예방 가능한 리스크입니다.

프로덕션에 릴리스하기 전에 개발 과정에서 자동화 방식으로 자주, 그리고 효율적으로 API를 테스트하면 기업, 개발자 및 보안 팀에게 도움이 됩니다. 그리고 알려지지 않은 취약점으로 인한 스트레스를 줄이고, 프로덕션에서는 오류를 근절할 수 있다는 점(프로덕션에서 오류가 발생할 경우 찾기 어렵고 비용이 기하급수적으로 증가할 수 있음)에서 즉각적으로 이점을 얻을 수 있습니다.

그러나 응답자들은 지금까지 테스트에는 큰 노력을 기울이지 않았습니다. 실시간 또는 매일 자주 이루어지는 API 테스트는 작년에 비해 프로덕션에서는 물론 API 수명 주기 전반에 걸쳐 감소했습니다.

- 2023년 미국 및 영국 응답자 중 18%가 실시간 테스트를 진행한다고 답했습니다. 동일한 집단에서 **2024년 해당 수치는 13%로 감소**했습니다.
- 2023년 미국 및 영국 응답자 중 37%가 최소 하루에 한 번 테스트를 진행했다고 답했습니다. 독일 응답자의 26%는 하루에 한 번 테스트했지만, **2024년 이 빈도로 테스트한 비율은 13%에 불과**했습니다.

프로덕션에 릴리스하기 전에 개발 과정에서 자동화 방식으로 자주, 그리고 효율적으로 API를 테스트하면 기업, 개발자 및 보안 팀에게 도움이 됩니다.

여러 지역 내 응답자에게서 주 단위 API 테스트가 가장 일반적이었지만 어떤 지역에서도 비율이 50%에 미치지 못했습니다. 또한 여러 지역에 걸쳐 API 테스트 빈도는 실시간 테스트에서 전혀 테스트를 진행하지 않는 경우까지 다양하게 나타났습니다. 특히 응답자의 6%만이 "API를 프로덕션에 공개하기 전에만 API 보안 테스트를 수행합니다."라고 답했습니다. API 수명 주기 전반에 걸쳐 지속적으로 테스트하는 것이 가장 이상적입니다.

API를 지속적으로 테스트하는 것은 무슨 의미인가요?

개발 과정에서 발생한 코딩 오류부터 사용자가 API와 상호 작용하기 시작한 후 발생하는 보안 격차에 이르기까지, API의 수명 주기 모든 단계에서 취약점이 발생할 수 있습니다. 따라서 개발 단계에서 API 테스트를 수행하고(시프트 레프트) 프로덕션에서도 지속적으로 API 테스트를 수행하는 것(시프트 라이트)이 이상적입니다.

개발 단계에서 API 테스트의 예:

- 악성 트래픽을 시뮬레이션하는 자동화된 테스트를 실행합니다.
- 확립된 거버넌스 정책에 대해 API 스펙을 검사합니다.
- 요청 시 API를 테스트하거나 CI/CD 파이프라인의 일부로 테스트합니다.

프로덕션 단계에서 API 테스트의 예:

- API 트래픽을 지속적으로 모니터링하고 트래픽 메타데이터를 평가합니다.
- 자동 분석을 통해 기존 API의 변경 사항을 포착합니다.
- 실시간으로 문제를 찾고 공격자가 눈치채기 전에 해결합니다.

API 보안 프로토콜이 컴플라이언스 요구사항을 충족하나요?

많은 데이터 보안 규제에서 API가 언급되지는 않지만, 요구사항은 API가 작동하는 애플리케이션과 인프라를 보호하는 데 중점을 두고 있습니다. 컴플라이언스 요구사항은 항상 변화하고 있습니다. 향후에는 미국 개인정보 보호법(초안 입법 단계에 있음) 및 EU 사이버 안정성 법 등 API에 영향을 미치는 새로운 규제가 추가로 제정될 것입니다.

API 보안에 대한 직접적인 영향을 미치는 규제 및 프레임워크는 다음과 같습니다.

- PCI DSS(최신 버전: v4.0.1)
- GDPR(General Data Protection Regulation)
- DORA(Digital Operational Resiliency Act)
- HIPAA(Health Insurance Portability and Accountability Act)
- NIS2(Network and Information Security) Directive

중요성이 부각되긴 했지만 여전히 뒷전으로 밀려나 있는 API 보안

API 공격으로 인해 사후 비용이 많이 들고 벌금이 부과됩니다. 또한 고객 신뢰를 잃고, 직원이 스트레스를 받으며, 기업 이사회의 신뢰를 잃는데도 보다 확실한 대응 조치를 취하지 않는 이유는 무엇일까요? 이를 이해하기 위해 다음 질문에 대한 답변을 살펴봅시다.

기업 내 여러 직책에 따라 API 보안의 우선순위를 어떻게 평가하나요?

응답자에게 향후 12개월의 주요 사이버 보안 우선 순위를 확인하고 방대한 목록에서 최대 3개의 우선순위를 선택하도록 요청했습니다(사이드바 참조). 상위 6개 우선순위의 차이는 2%, 하위 6개 우선순위 차이는 1%에 불과합니다. 이는 우선순위가 지역 및 업계 전반에 걸쳐 비슷하며 팀에서 종종 이 모든 우선순위를 동시에 처리해야 함을 뜻합니다.

그러나 일부 업계에서는 API의 핵심과 관련된 순위가 다릅니다. 예를 들어, 에너지 및 유틸리티는 다른 모든 업계와 비교했을 때 API 보안의 우선순위를 13.2%로 가장 낮게 평가합니다(조사 참가자 평균인 18%보다 낮음). 이와 동시에 에너지 및 유틸리티는 참여한 8개 업계 중에서 API 보안 인시던트를 91%로 가장 많이 경험했으며 이는 8개 업계 평균인 84%보다 높은 것으로 나타났습니다. 그 이유는 무엇일까요? 바로 API 보안의 낮은 우선순위가 높은 공격 비율로 이어지기 때문입니다.

향후 12개월 내 가장 많이 언급된 보안 우선순위

1. GenAI 기반 공격 방어 - **21.2%**
2. 랜섬웨어 방어 - **20.5%**
3. 직원 사용자를 위한 인증 보안 - **19.7%**
4. 개발자 비밀 관리 및 보안 - **19.6%**
5. 엔드포인트 보안 - **19.2%**
6. 클라우드 보안 솔루션 - **19.1%**
7. 특별 권한 IT 접속 보안 - **18.6%**
8. 데이터 손실 차단 - **18.6%**
9. 공격자로부터 API 보안 - **17.9%**
10. 애플리케이션 보안 - **17.7%**
11. 보안 정보 및 이벤트 관리 - **17.6%**
12. 인시던트 대응 및 관리 - **17.6%**

질문: 향후 12개월 동안 귀사의 주요 사이버 보안 우선순위는 무엇인가요? (최대 3개까지 선택) n=1207

직책별로 응답 데이터를 분류해 수집된 더 의미 있는 데이터:

- CISO는 GenAI 기반 공격과 API 보안을 각각 **25.5%** 및 **24.8%**로 가장 많이 언급했습니다.
- AppSec 직원은 CISO와 마찬가지로 GenAI 기반 공격을 가장 높은 우선순위로 지목한 비율이 **22.5%**였습니다.
- CIO와 CTO는 모두 특별 권한 접속에 초점을 맞추었고, CTO는 인시던트 대응을 비슷한 비율로 응답했습니다.
- 수석 보안 전문가들만이 랜섬웨어를 가장 높은 우선순위로 평가했습니다.

이러한 차이는 또 다시 다음과 같은 질문으로 이어집니다. 'IT 보안 기업의 여러 계층이 서로 다른 플레이북에 기반해 활동하는 것처럼 보이는 이유는 무엇일까요?' '주요 보안 리더와 일선 직원 모두 GenAI 기반 공격에서 중요한 부분을 차지하는 API와 관련 리스크에 뜻을 같이하는 반면, 다른 직책은 이와 다른 의견을 보이는 이유는 무엇일까요?'

아마 CISO는 사업부에서 수요를 충족하기 위해 GenAI에 기반한 혁신적인 앱을 서둘러 출시하는 것을 목격하는 반면, AppSec 팀원은 동일한 상황에서 민감한 데이터를 다루는 AI 구성요소(LLM 등)의 취약점에 대해 알려지지 않은 부분은 어디까지인지 알고 있기 때문일 것입니다. 또한 이 팀은 공격자들이 GenAI를 공격 방법에 포함하고 있다는 여러 가지 경고 신호를 가까이서 보고 있습니다.

하지만 주된 이유는 아주 단순합니다. 하향식 및 상향식 의사소통은 특히 대기업에서 충분히 자주 이루어지지 않습니다. 그래서 팀이 일상적으로 처리해야 하는 업무와 핵심 우선순위에서 차이가 발생합니다.

마지막으로, 응답자의 주요 사이버 보안 우선순위와 이들이 생각하는 API 보안 인시던트의 원인을 비교해보겠습니다. 17페이지에 나와 있는 것처럼, 가장 많이 인용된 원인 중 3가지는 API 문제를 탐지할 수 없었던 기존의 애플리케이션 보안 툴과 관련이 있습니다. 이러한 비교 결과는 API 검색 및 테스트 솔루션이 API 보안뿐만 아니라 어떻게 대부분의 주요 보안 우선순위를 개선할 수 있는지에 대해 논의할 좋은 기회입니다.

즉, 적절한 API 보안 툴이 API를 보호할 뿐만 아니라 데이터, 클라우드 및 애플리케이션과 같은 영역의 보안을 강화하면 API 보안이 더 이상 이해관계자들에게 고립된 틈새 영역으로 간주되지 않을 것입니다. 큰 그림을 제시하면 쉽게 승인을 받아 API의 우선순위를 높일 수 있습니다.

올바른 API 보안 툴이 API를 보호할 뿐만 아니라 데이터, 클라우드 및 애플리케이션과 같은 영역의 보안을 강화하면 API 보안이 더 이상 이해관계자들에게 고립된 틈새 영역으로 간주되지 않을 것입니다.

API 보안 인시던트에 대한 의견 차이는 단일 데이터 소스가 없다는 의미인가요?

전체 보안 우선순위에서 C레벨과 일선 직원 사이에 차이가 나며, 이러한 차이는 특히 API 위협과 관련한 문제에서도 여전히 존재합니다. 예를 들어 CIO는 API 공격에 대한 인식 측면에서 AppSec 팀과 의견을 같이합니다(각 직책의 약 88%에서 인시던트 경험을 보고함). 한편 CISO, CTO, 수석 보안 전문가는 모두 인시던트 경험에 대해 약 8%포인트 더 낮은 80%로 보고했습니다.

API 보안 인시던트에 대해 가장 많이 인용된 원인 또한 직책별로 다르게 나타났습니다. 대부분의 CISO와 수석 보안 전문가는 API 게이트웨이에서 탐지하지 못했다고 말했으며, 나머지 세 직책은 각각 다른 원인을 들었습니다.

- CISO: API 게이트웨이의 탐지 실패 - **26.8%**
- CIO: 의도하지 않은 인터넷 노출 - **28.6%**
- CTO: WAF의 탐지 실패 - **25.9%**
- 수석 보안 전문가: API 게이트웨이의 탐지 실패 - **23.3%**
- AppSec 팀: API 설정 오류 - **23.2%**

API 보안 인시던트의 가장 많이 언급된 원인, 모든 응답자

1. API가 인터넷에 의도치 않게 노출됨 - **21.8%**
2. 웹 애플리케이션의 탐지 실패 - **21.8%**
3. API 게이트웨이의 탐지 실패 - **20.2%**
4. GenAI 툴/기술의 API(예: LLM) - **20.0%**
5. API 설정 오류 - **19.9%**
6. 네트워크 방화벽의 탐지 실패 - **19.6%**
7. 유명한 기술 툴 및 서비스(예: Microsoft) - **19.2%**
8. API 코딩 오류로 인한 취약점 - **19.1%**
9. 관리되지 않는 API(예: 휴면 또는 좀비 API) - **18.9%**
10. API 인증 제어 부족 - **18.8%**
11. 권한 확인 취약점 - **18.7%**
12. 인터넷에서 다운로드한 소프트웨어 솔루션 - **17.6%**
13. 미드 티어 소프트웨어 솔루션(예: Slack) - **16.3%**

질문: 기업에서 경험한 API 보안 인시던트의 원인은 무엇인가요? (최대 3개까지 선택) n=1207

API 보안 인시던트에 대해 보고된 비용에서도 상위 직책과 하위 직책 간 의견이 달랐습니다. 그러나 직책 및 지역별로 데이터를 분류하면 자연스럽게 표본 크기가 작아진다는 점에 유의해야 합니다. 그럼에도 불구하고 특히 미국 내에서 이러한 하위 집합의 차이는 주목할 만합니다. 미국의 CIO와 CTO는 인시던트 비용을 미화 약 1백만 달러, CISO는 약 73만 7000달러에 달하는 것으로 보고한 반면, 수석 보안 전문가 및 AppSec 직원은 각각 미화 37만 5000달러 및 44만 4000달러로 보고했습니다.

영국의 경우 AppSec 팀원은 74만 9000파운드(가장 높은 수치), CISO는 19만 파운드(가장 낮은 수치)를 보고했지만, 일반적으로 직책별 하위 집합에서 비용에 대한 의견은 더 많이 일치했습니다. (중간 직책이 보고한 비용은 높은 순으로 37만 4000파운드에서 22만 2000파운드까지 다양했습니다.) 비용에 있어 독일의 차이는 영국의 경우와 비슷했으며, 직책은 가장 낮지만 실무에 가장 가까운 직원이 가장 높은 추정치인 34만 5000유로, 가장 직책이 높은 CISO는 가장 낮은 비용인 19만 7000파운드로 답변했습니다. 이는 미국과 반대되는 결과입니다. 모든 지역의 모든 직책에서 공통된 한 가지는 API 보안 인시던트의 가장 큰 영향은 바로 직원에게 미치는 영향이라는 점입니다 (7페이지의 영향 참조).

API 보안을 위한 보다 성숙한 보안 체계 구축 방법

앞서 언급한 바와 같이 기업의 여러 계층에 있는 보안 팀 직원들이 동일한 관점으로 API 보안을 바라보지 않는다는 것이 분명합니다. 그러나 다른 측면도 있습니다. 한 가지 분명한 또 다른 사실은 이들이 공통의 토대를 가지고 있다는 점입니다. 이들은 비용(재정 및 인적)을 파악하고 있으며, 사용하는 툴이 부족하다는 점을 인정합니다.

API 보안이 기업에 큰 영향을 미치는 이런 상황에서 다음 단계는 무엇을 구축할지, 무엇을 변경할지 결정하고 API 보안이 수익에 미치는 긍정적 영향을 리더에게 제시하는 것입니다. CISO에서 AppSec 팀에 이르기까지 보안 부서 내에서 API 보안의 순위를 높이는 방법에 대한 합의를 도출하는 작업부터 시작하는 것이 좋습니다. 그 다음으로, 리더십과 일선 AppSec 팀원 사이, 그리고 그 사이의 관리 계층 간에 열린 의사소통을 적극적으로 추진해야 합니다.

앞으로 진행해야 하는 단계

이번 연구를 마치며, 보안 팀이 API 보안 전략을 시작하거나 전략을 확장하고, 성숙한 API 보안을 향해 나아가기 위해 사용할 수 있는 일련의 점진적 단계를 준비했습니다.

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 API(10페이지의 사이드바 참조)는 공격자의 주요 표적이 되므로 광범위한 보안 범위를 갖추는 것이 중요합니다.

2 테스트에 투자하기

API가 의도된 기능을 수행하기 위해 올바르게 코딩되었는지 쉽게 테스트할 수 있는 API 보안 솔루션을 선택하세요. 배포 전에 테스트를 수행하는 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 요구사항을 준비하는 데 도움이 됩니다(14페이지 참조).

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 WAAP)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 경보가 위협을 올바르게 식별했는지, 정교한 툴과 인간 지능의 조합을 사용해 선제적 위협 탐색을 가능하게 하는 패턴이 나타났는지 파악합니다.

결론

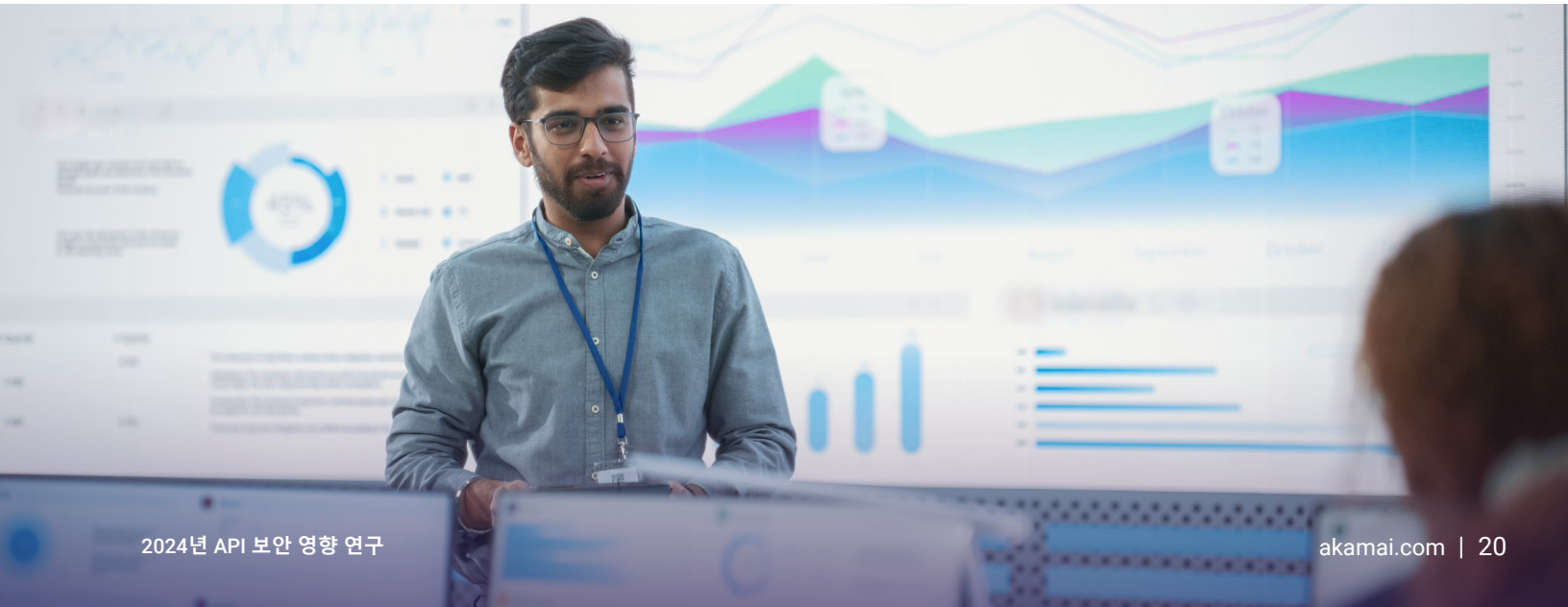
올해 보고서에서는API 보안이 단순히 위협 목록이나 툴에 관한 것이 아니라 사람에 관한 것임이 명확하게 드러났습니다.

이 연구를 통해 보안팀이 과도한 압박을 받고 있으며 완전히 새로운 공격 기법을 팀의 워크로드에 추가할 경우 큰 부담이 될 수도 있다는 점을 확인했습니다. 그러나 API는 계속 더 확산되는 추세이며, API 보안을 위한 조치를 취하면 GenAI 취약점(LLM과 데이터를 교환하는 API 보호) 및 클라우드 보안(전환하는 워크로드에 포함된 모든 API의 리스크 경감) 등 여러 가지 높은 우선순위에도 강력한 파급 효과를 가져올 수 있습니다.

API 보안에 대한 선제적 대응은 기업을 보호할 뿐만 아니라 업계 동료, 리더, 이사회가 이 중요한 공격 기법을 바라볼 때, 팀의 신뢰도를 높여줄 것입니다. 또한 팀의 스트레스를 낮추는 데도 큰 도움이 됩니다. 연구 결과에 따르면, 팀은 API 보안 인시던트 및 내부 조사, 고객 및 동료 직원 사이에서 호감도 감소에 큰 영향을 받는 것으로 나타났습니다.

이제 단계를 밟아나가면 컴플라이언스 계획 및 보고를 미리 간편하게 수행할 수 있으며, 규제기관의 벌금을 적절한 타이밍에 예방할 수 있습니다. 시작하지 않을 이유가 없습니다.

- 성숙한 API 보안 체계를 향한 여정의 다음 단계로 나아갈 준비가 되었다면 API 보안의 기본 원칙 백서부터 살펴보세요.
- 귀사의 도전 과제를 Akamai가 어떻게 도울 수 있는지에 대해 대화하고 싶으시다면 맞춤형 Akamai API Security 데모를 요청하시기 바랍니다.



API 보안 영향 연구에 대한 정보

2024년 API 보안 영향 연구를 위한 리서치는 Opinion Matters가 2023년 6월 12일부터 2024년 7월 7일까지 수행했습니다. 총 1207명의 응답자를 대상으로 설문 조사를 실시했으며 회사 소재지별로 영국 404명, 미국 402명, 독일 401명입니다. 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 또는 CISO, 3분의 1은 수석 보안 전문가, 나머지 3분의 1은 500명 미만에서 1000명이 넘는 규모까지 다양한 회사에서 근무하는 애플리케이션 보안팀에 속했습니다.

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

저자 소개

주저자
애니 브런홀츨(Annie Brunholzl)

관리 편집자
존 나탈레(John Natale)

리서치 책임자
미치 메인(Mitch Mayne)

카피 에디터
랜디 크라비츠(Randi Kravitz)

프로모션
바니 빌(Barney Beal)

마케팅 및 출판
조지나 모랄레스 햄프(Georgina Morales Hampe)

검토 및 주제별 기여
팜 코브(Pam Cobb)
킴벌리 고메즈(Kimberly Gomez)
짐 루빈스카스(Jim Lubinskas)
스타스 네이만(Stas Neyman)

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**