API 보안 사고 사례 및 대응 방안

Defending Against the Top API Security Threat of 2023

엔시큐어(주) 손장군 이사
sohn.jg@ensecure.co.kr

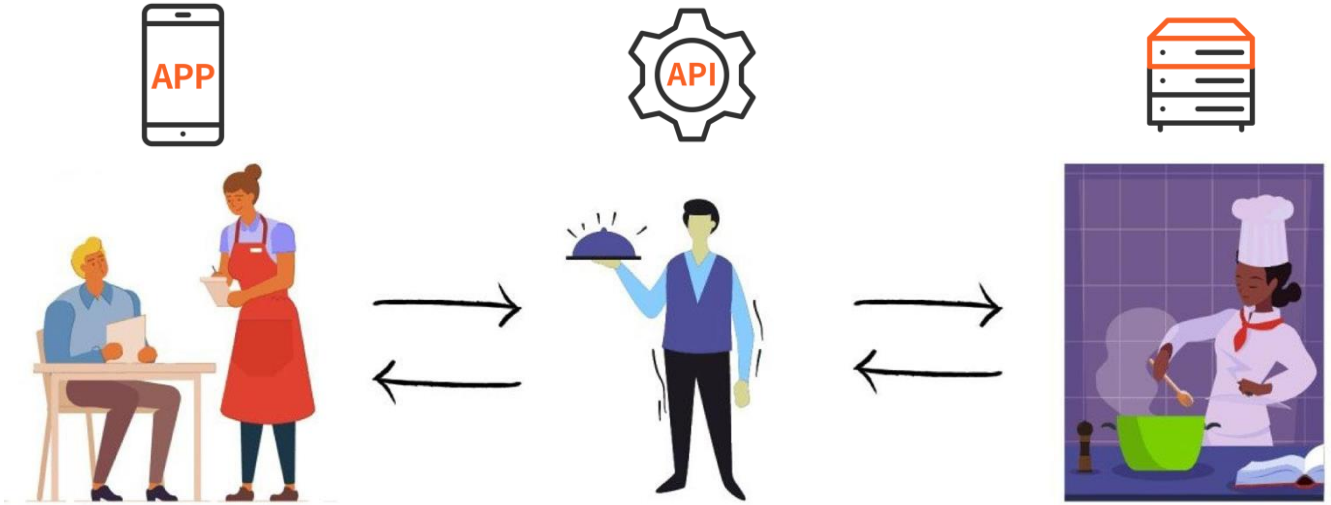
Application Programming Interface

API - Connecting Software Services

API (Application Program Interface)

WIKIPEDIA

: API(응용 프로그램 인터페이스)는 컴퓨터 간 또는 컴퓨터 프로그램 간의 연결



Customer → Application

Waiter → API

Kitchen → Server

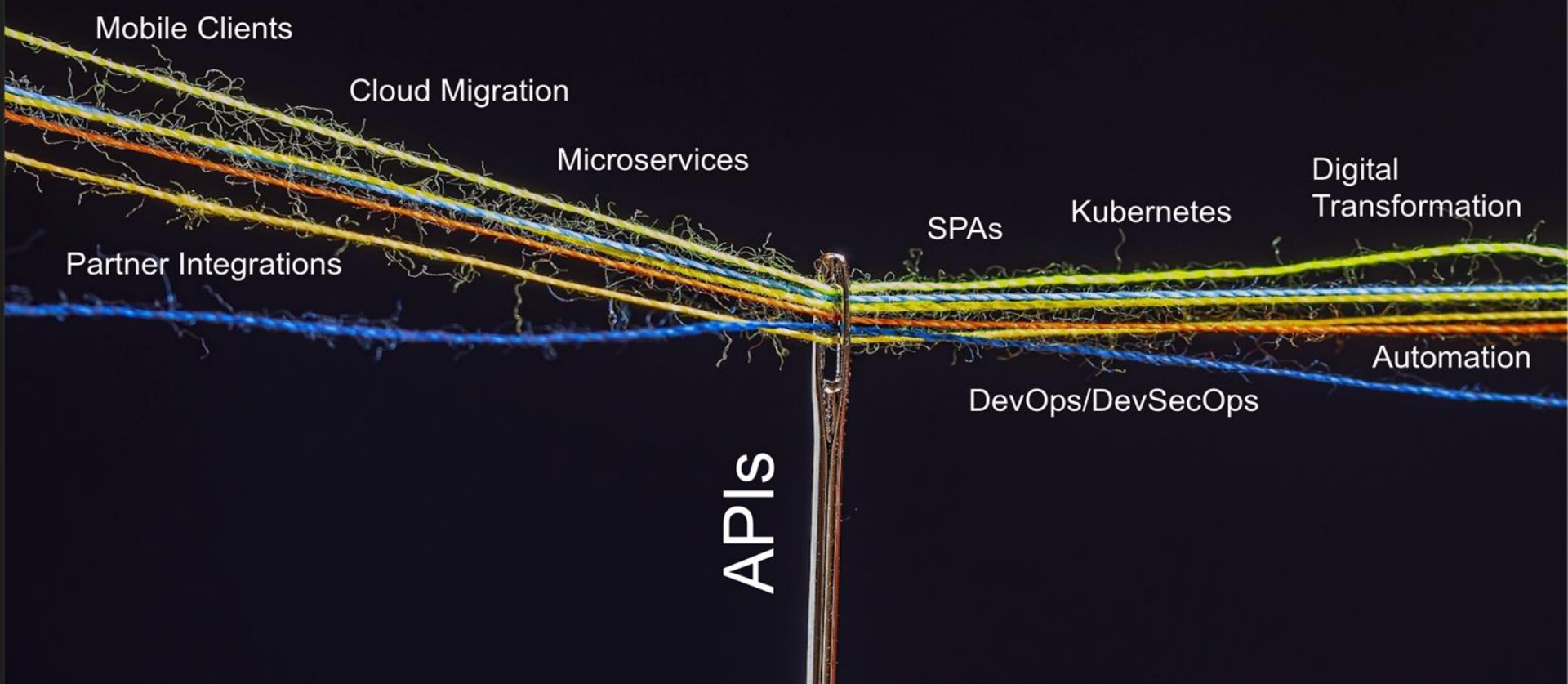
APIs are an **efficient** and **developer-friendly** means to unlock value, enabling interoperability of software and data

API의 비즈니스의 이점

https://expediapartnersolutions.com/products/api

"API는 대부분의 조직에서 한번에 달성할 수 없는
비즈니스 기술에 대한 액세스를 제공"

APIs Are Everywhere



API 위협 상황 및 동향

API abuses - 가장 빈번한 공격 벡터

언제 어디서나 존재하는 API 위협

기업은 데이터 유출로 큰 타격을 입을 수 있음
문제는 점점 커지고 있으며 산업 전반에 걸쳐 존재

BRITISH AIRWAYS

500,000 사용자의 개인정보 데이터 도난

GDPR 위반으로

ICO로부터 $229.5M 벌금 (1.5% ATO)

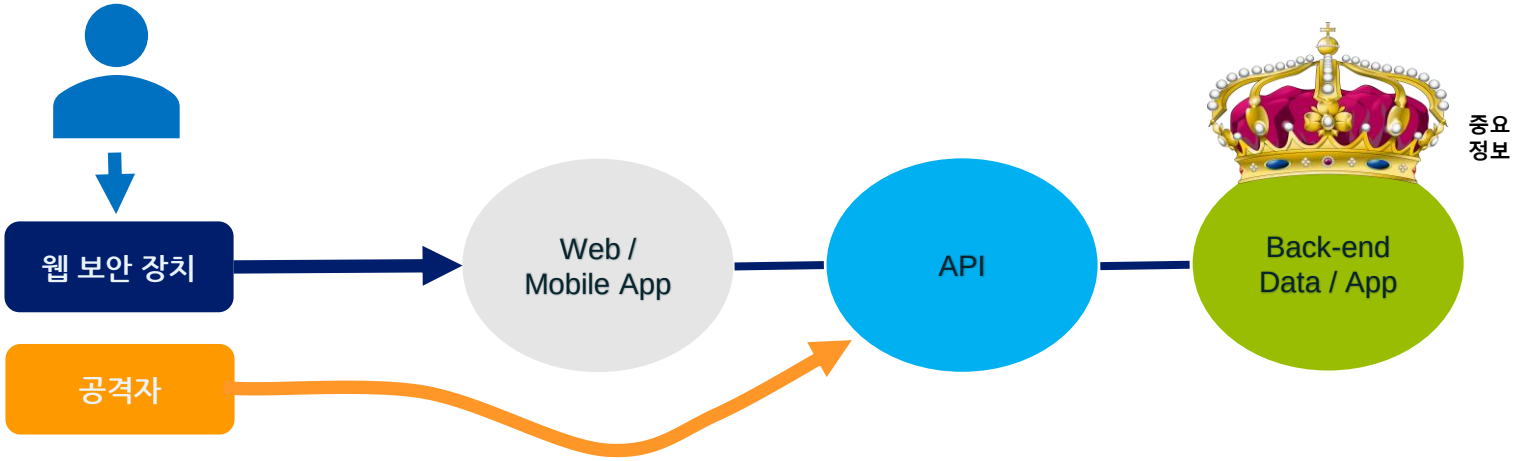
ICO에 따르면 데이터 침해는

브리티시 에어웨이가 고객 정보를 보호하기 위한

"보안 준비가 미흡" 했기 때문에 발생

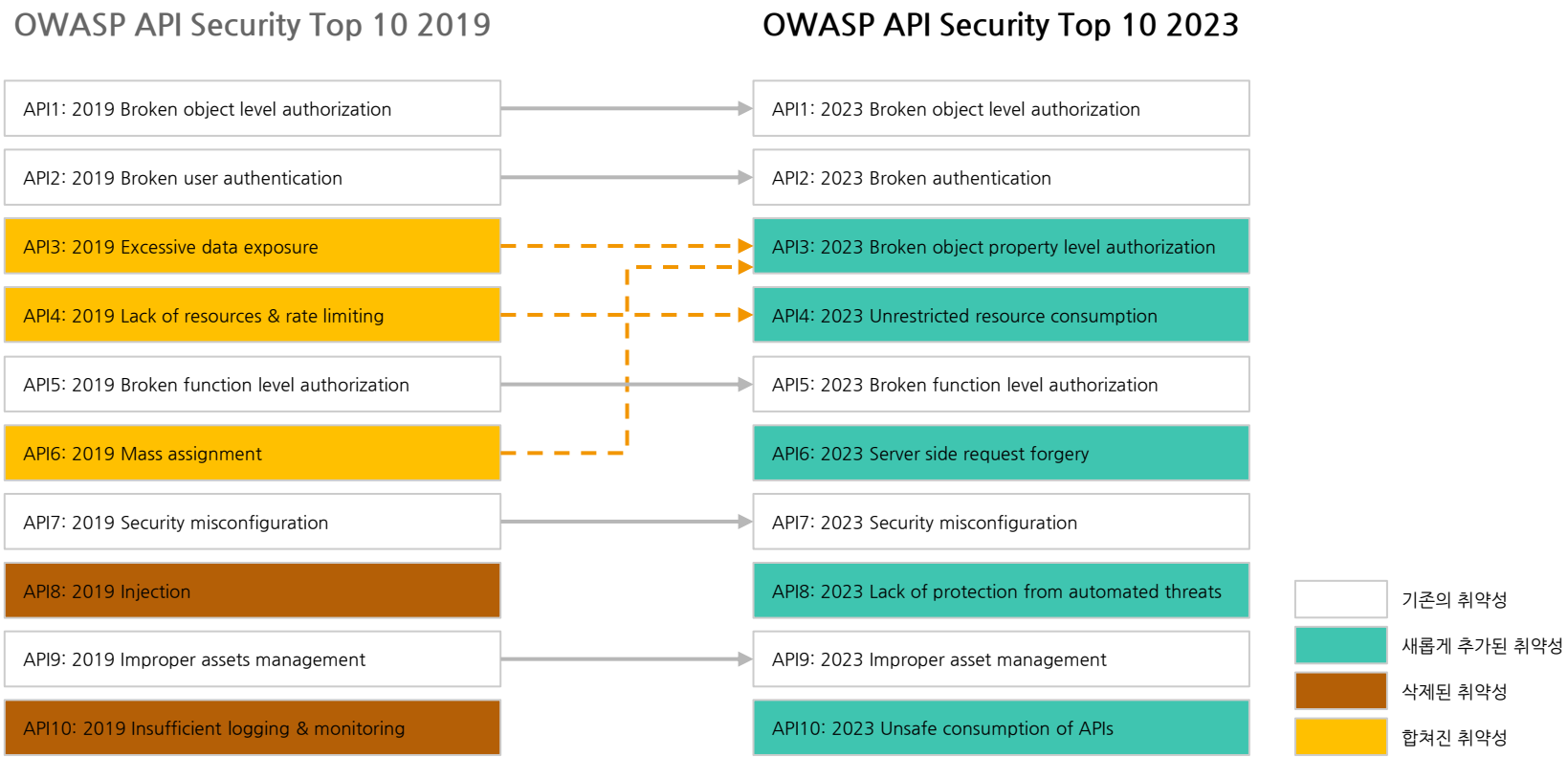
"API의 폭발적 성장이 API 관리 도구의 기능을 능가 하므로 2025년에는
엔터프라이즈 API의 50% 미만만 관리가 될 것이다" (Gartner 2022)

API 공격은 기존의 방식과 다름



- 공격자는 웹 및 모바일 앱을 직접 공격하여 API로 이동한 다음 중요 데이터가 저장되어 있는 백엔드로 바로 이동!
- 공격자는 기존의 웹 및 모바일 앱 보안 보호를 우회하고 있음
- **API 위반은 비즈니스 로직 결함이나 권한 부여 격차, 약한 인증 등을 이용**

OWASP Top10 API 위협 2023



OWASP Top10 API 위협 2023

OWASP API 보안 위협 2019	API 공격 요소
A1 - 손상된 객체 수준 권한	변조/데이터탈취
A2 - 손상된 인증	변조/데이터탈취
A3 - 깨진 개체 속성 수준 권한 부여	변조/데이터탈취
A4 - 무제한 리소스 소비	DoS
A5 - 손상된 기능 수준 인증	변조/데이터탈취
A6 - 민감한 비즈니스 흐름에 대한 무제한 액세스	데이터 탈취/서비스오용
A7 - 서버 측 요청 위조	보안우회/DoS
A8 - 잘못된 보안 구성	서비스손상/데이터탈취
A9 - 부적절한 자산 관리	엔드포인트 스캐닝
A10 - 안전하지 않은 API 사용	서비스거부/데이터 탈취

⚠ 공격 이유

- 데이터 탈취
- 계정 탈취
- 사기
- 서비스 거부(DoS)

API 사고 사례

통신사 T-Mobile (2023)

"T-MOBILE API를 통해 고객정보 유출"

T-Mobile이 API 데이터 유출로 3700만 계정의 데이터를 훔치기 위해 해킹당했습니다.

에 의해세르지우 가틀란 2023년 1월 19일 오후 05:19 삼

T-Mobile은 위협 행위자가 API(애플리케이션 프로그래밍 인터페이스) 중 하나를 통해 3,700만 개의 현재 후불 및 선불 고객 계정의 개인 정보를 훔친 후 새로운 데이터 유출을 공개했습니다.

API는 응용 프로그램이나 컴퓨터가 서로 통신하기 위해 일반적으로 사용하는 소프트웨어 인터페이스 또는 메커니즘입니다.

새로운 데이터 유출로 3,700만 계정에 영향을 미침

T-Mobile은 공격자가 2022년 11월 25일경 영향을 받은 API를 사용하여 데이터를 훔치기 시작했다고 목요일 밝혔습니다. T-Mobile은 2023년 1월 5일 악성 활동을 감지하고 하루 후 API에 대한 공격자의 액세스를 차단했습니다.

https://www.bleepingcomputer.com/news/security/t-mobile-hacked-to-steal-data-of-37-million-accounts-in-api-data-breach/

인터넷 강의 업체 (2023)

API 보안 취약점 주의...인강 영상과 개인정보 무차별 유출

씨디네트웍스 '2022 웹 애플리케이션 및 API 보안 보고서' 최근 발표
OTT 콘텐츠에 이어 인터넷 강의 유출 급증… 인강 유출에 교육업계 '비상''

OTT 콘텐츠에 이어 인터넷 강의(이하 인강) 영상이 온라인에 무차별 유출되며 교육업계에 비상이 걸린 가운데 씨디네트웍스가 이에 대한 원인과 인사이트를 제시했다.

8월 1일 유명 인강 플랫폼 2곳이 해킹을 당해 온라인 교육 비즈니스의 핵심 자산인 인강 영상이 불법 유출되는 일이 벌어졌다. 유출 영상은 텔레그램 채널 '누누스터디'를 통해 공개됐으며 인기 강사의 이름과 아이디, 비밀번호, 휴대전화 번호 등 500여명의 개인정보도 함께 공개됐다. 누누스터디 채널 운영자는 "해당 플랫폼 가입자 전부 다 털었다"며 "보안이 허술해서 인증번호가 API로 넘어온다"고 주장했다.

이번 유출이 기존과 다른 점은 불법 유출·녹화의 타깃이 OTT 업체 등의 영화, 드라마에서 인터넷 강의로 바뀌었다는 것이다. 콘텐츠 제작이나 배포 비즈니스에서 콘텐츠는 주요 자산이자 핵심 비즈니스다. 따라서 이번 인터넷 강의와 개인 정보 유출 수사와 별개로 해당 비즈니스에는 적절한 보안 조치와 개선안이 촉구될 것으로 보인다.

씨디네트웍스가 최근 발표한 '2022 웹 애플리케이션 및 API 보안 보고서'에 따르면, 지난 한 해 동안 API 비즈니스를 대상으로 한 공격은 빠르게 확대돼 전체 공격의 약 58.4%를 차지했다. 특히 영화, TV 등 미디어 산업은 조사 분야에서 4번째로 많이 API 공격을 당했다.

"인강 플렛폼을 통해 개인정보 및 강의 동영상 유출"

https://www.bleepingcomputer.com/news/security/t-mobile-hacked-to-steal-data-of-37-million-accounts-in-api-data-breach/

호주 최대 통신사 Optus (2022)

“Optus, 데이터 유출로 인한 100만 달러 강탈 위협”

Optus Under $1 Million Extortion Threat in Data Breach

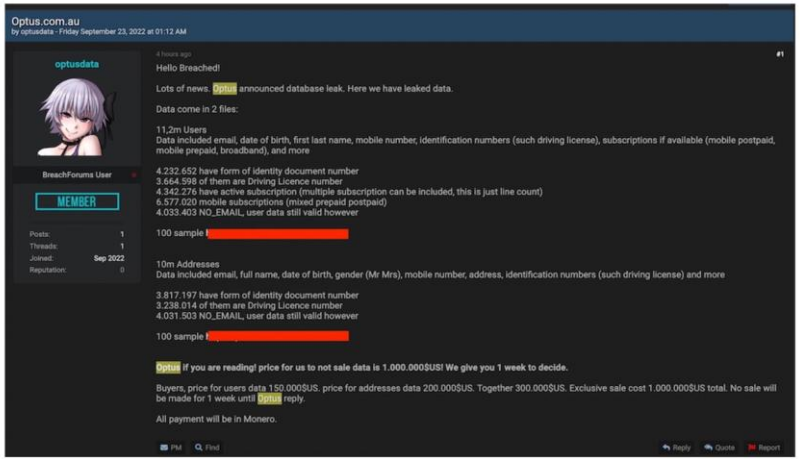
Exclusive: Optus Attacker Says Unauthenticated API Endpoint Led to Breach

Jeremy Kirk (jeremy_kirk) · September 25, 2022

An Optus store in greater Sydney.

Australia’s second-largest telecommunications company is facing a US$1 million extortion demand to prevent the sale of what an attacker says are up to 11.2 million sensitive customer records.

Early Saturday, a person going by the nickname "Optusdata" published two samples of the purported stolen data on a well-known data leak forum. The attacker writes that Optus can prevent the sale of the data to other cybercriminals if it pays $1 million in the Monero cryptocurrency.



The person claiming to have hacked Optus published data samples as well as an extortion demand against the company on a data breach forum early Saturday.

Optusdata writes that Optus has one week to pay, otherwise the data will be available for sale in parcels.

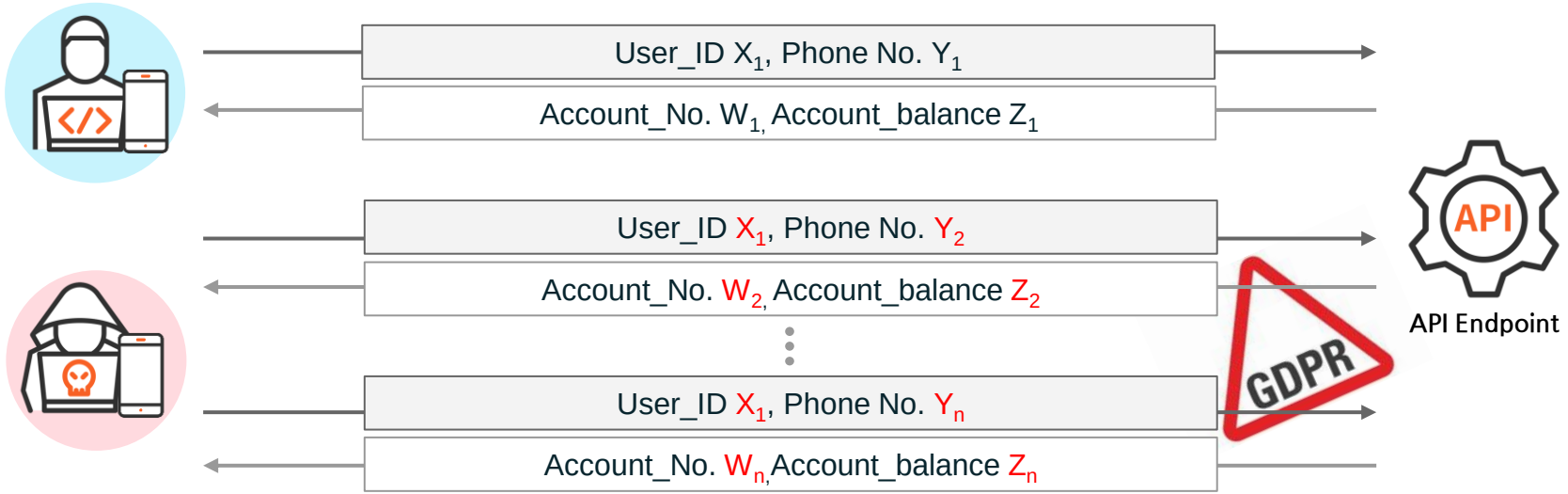
API 공격 예시

페퍼저축은행

PEPPER Saving Bank

[A1- 손상된 객체 수준 권한]

- 100% API 중심으로 운영되는 소규모 신생 은행
- 공격 유형: 데이터 도난
- “Pepper Invest” API를 이용하여 민감한 데이터를 탈취하는 화이트 해킹 공격

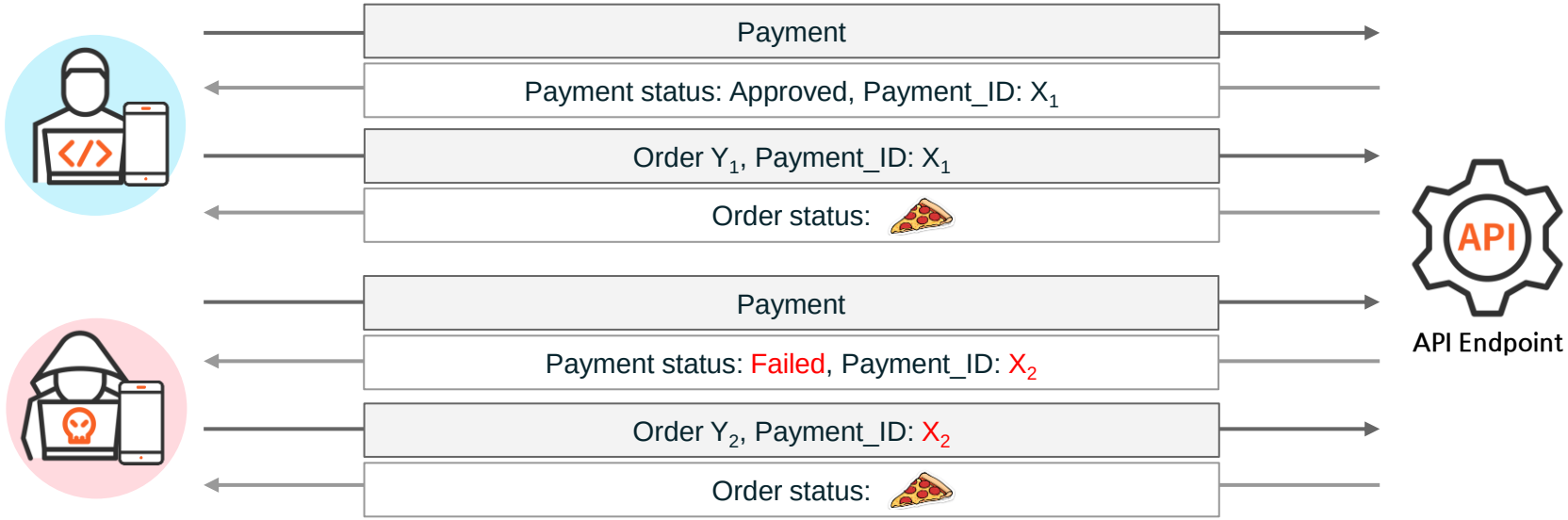


도미노피자

Domino's Pizza

[A7 - 보안 구성의 오류]

- 세계 70개국, 1만 개 이상 점포를 둔 미국 피자 배달 전문 브랜드
- 공격 유형: API 다중 조작
- API 호출을 연속적으로 조작하여 부정한 트랜잭션을 발생시킴



API 위협 완화 전략

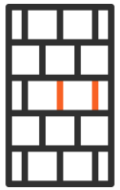
코드에서 프로덕션까지 API 보호

Gartner®

"범용 애플리케이션 보안 솔루션만으로
웹 API를 보호하는 것은 효과가 없다" - Gartner 2019

API 게이트웨이

- 암호화
- 접근 제어
- API 트래픽 조절



웹 방화벽

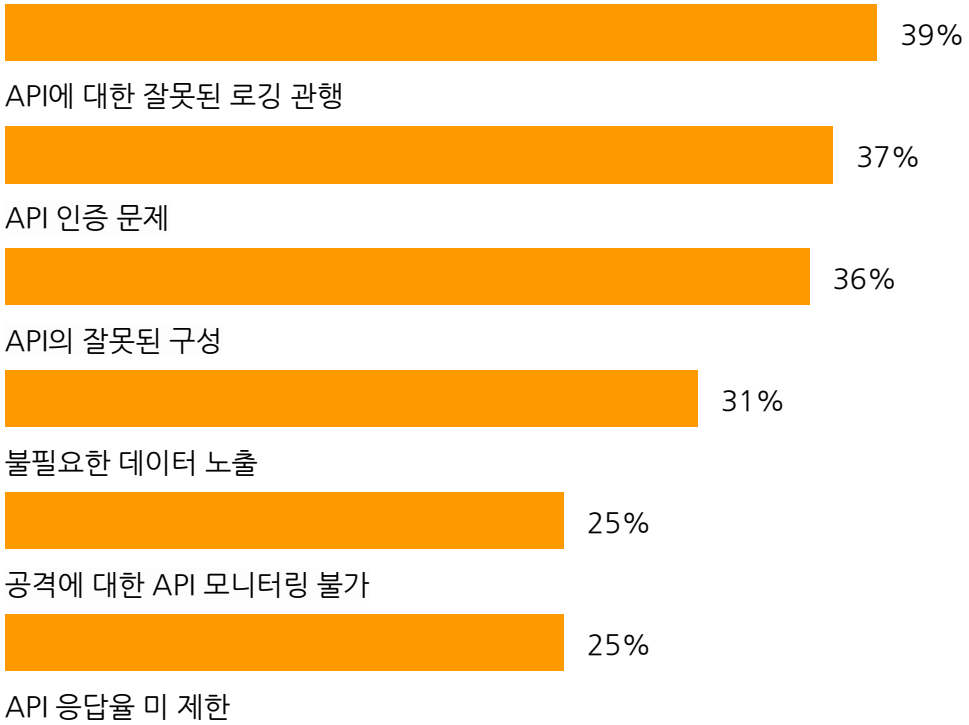
- 서명/경험 기반 보호
- 웹 인프라의 알려진 취약점 탐지

소스코드 분석 툴

- 소스코드 알려진 취약점 탐지

API 위협은 애플리케이션 로직의 취약성을 활용
기존 솔루션 중 애플리케이션 동작을 분석하는 솔루션은 존재하지 않음

API 보안은 인간의 한계를 뛰어넘는 문제이기 때문에 '머신러닝'이 필요



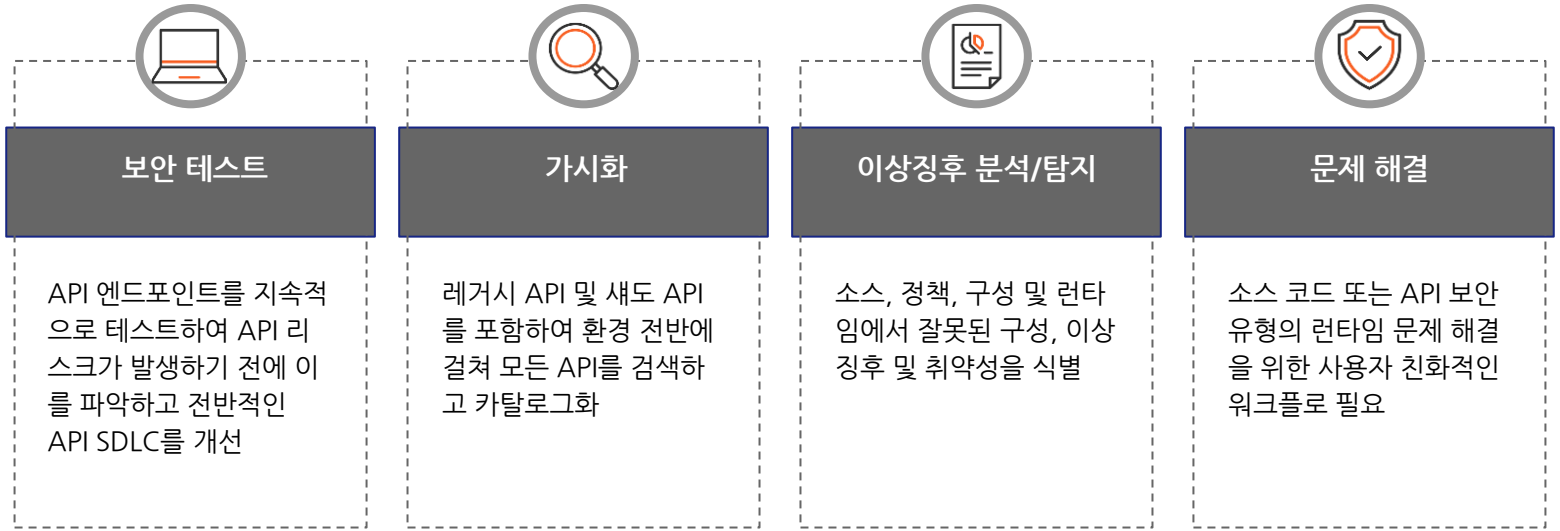
15,564
엔터프라이즈 API의 평균 규모(수)

76%
지난 1년간 보안 위배를 경험한 조직 비율

37 days
27 days for discovery
10 days for remediation
per incident

Whitepaper
The 2022 API Security Trends Report

API 위협 완화 전략 - 머신러닝을 통한 API 위협 테스트/탐지/분석 자동화



자동화

이러한 전략은 코드에서 프로덕션까지 API 에코시스템 전반에 걸쳐 360도 보안 기능을 제공

API 위협 완화 전략 - 자동화로 보안이 확보된 빠른 API 서비스 배포 및 운영 보안성 확보

배포 전

보안이 확보된 API를 빠르게 적용

Code

Deploy

- 긴 문제 해결 시간
- **보안을 위해 수익 흐름이 느려짐**
- 타사 테스트로 인한 높은 비용
- API에 대한 낮은 개발자 신뢰도

배포 후

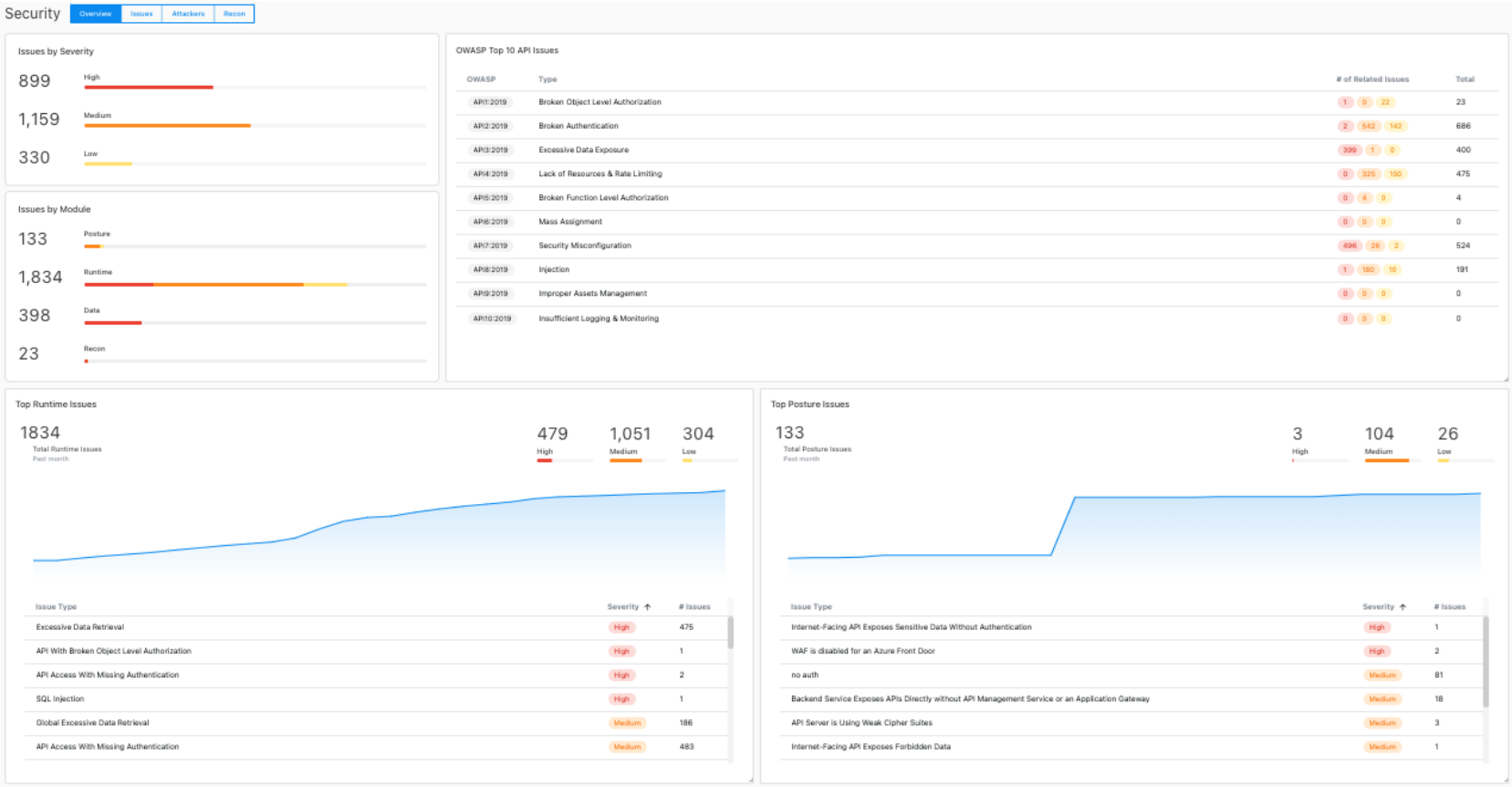
API 및 중요 자산 보호

Operate

Defend

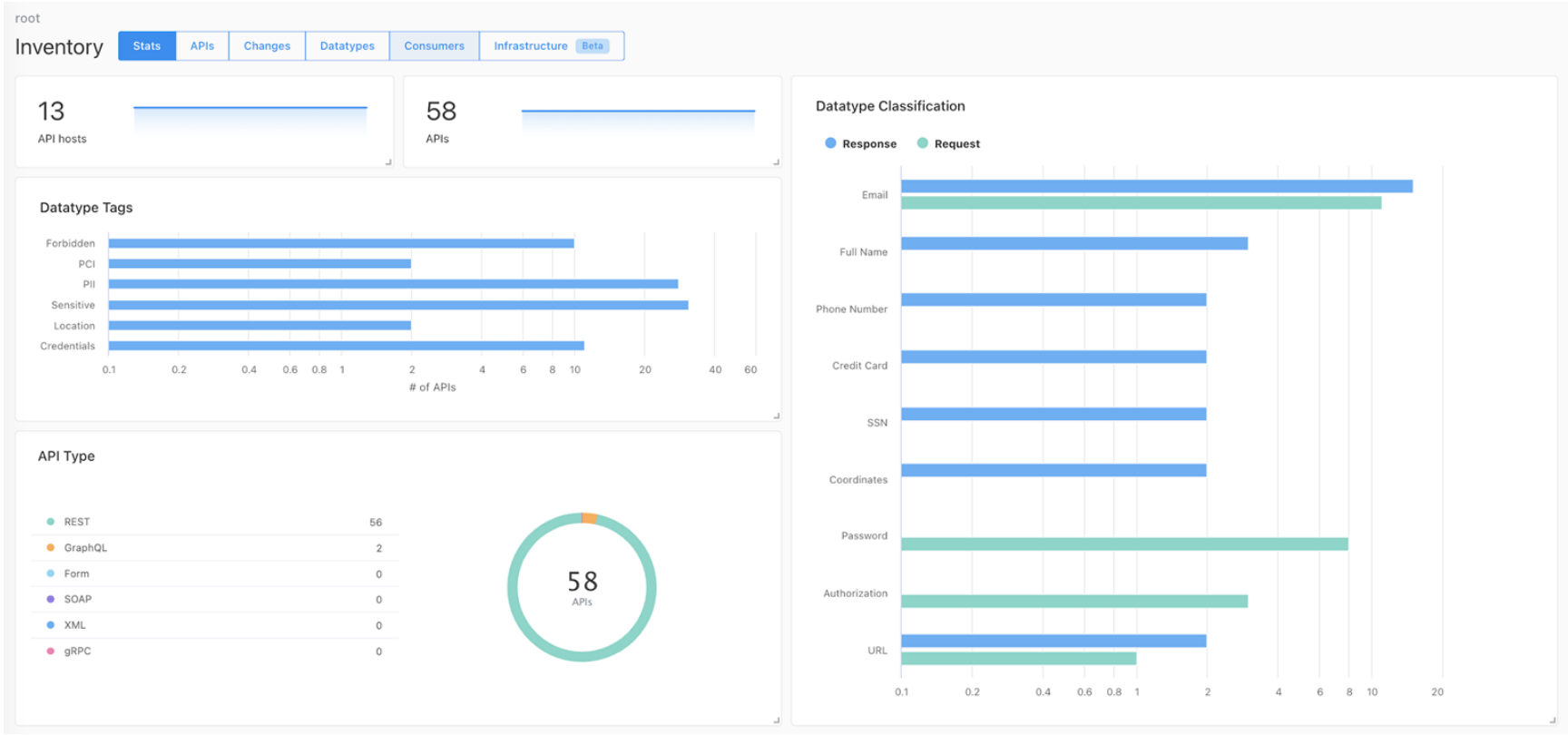
- 거대한 공격 표면
- 고가치 공격 대상
- 공격의 용이함
- **공격 시간 < 업데이트 적용 시간**
- 브랜드, 매출, 고객 만족도 등에 부정적인 영향

API 위협관리 자동화 관리 예시(1)



eNsecure

API 위협관리 자동화 관리 예시(2)



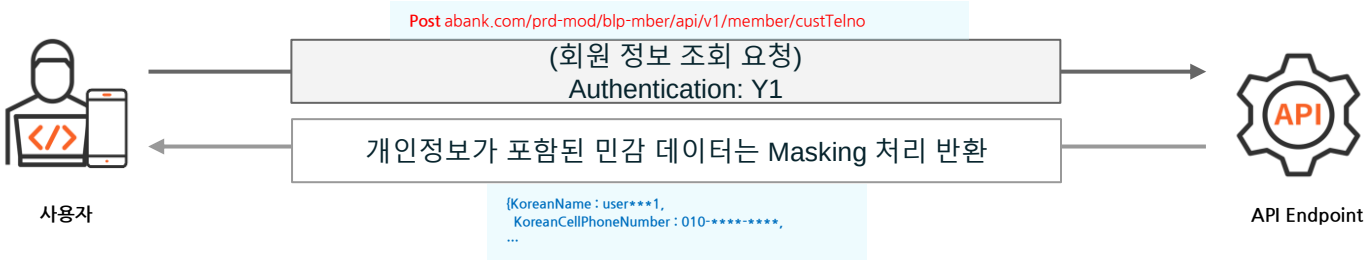
eNsecure

실제 탐지 사례 (국내 금융사)

API 정의

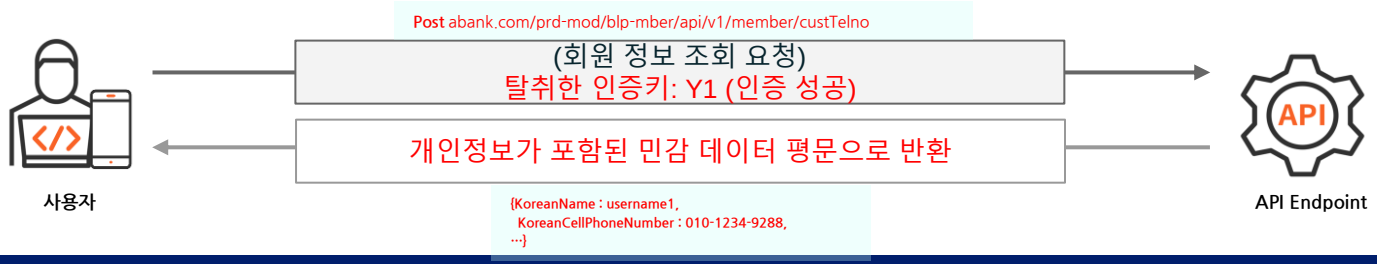
abank.com/aaaa/mber/api/v1/member/custTelno

- **용도** : 회원정보 조회
- **Method** : POST (조회 용도)
- Endpoint 특징 : *API 인증 Hash 검사 후 민감 데이터의 경우 Masking 처리되어 반환하도록 설계*
- **데이터 유형** : *개인정보가 포함된 민감 데이터 (사용자 이름 및 휴대 전화번호)*



발견된 취약점(크리티컬 2종)

1. API Endpoint에서 인증키에 대한 Hash 검사 루틴이 없음
2. 민감 데이터로 분류된 매개변수의 경우 마스킹 처리되어 조회가 되어야 하지만, 응답에서 대량의 민감 데이터가 평문으로 반환 됨



실제 탐지 사례 (국내 금융사)

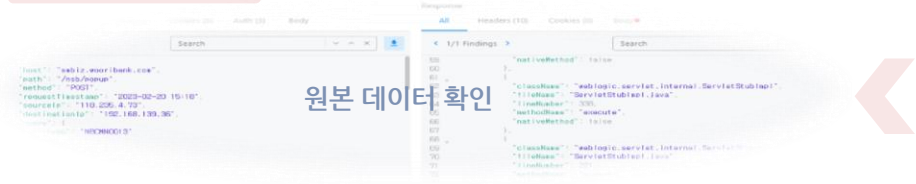
OWASP API3(2023) : 손상된 개체 속성 수준 권한 부여

탐지 모듈 : Excessive Data Exposure with Authenticated API

- 사용자가 인증한 API에서 *필요 또는 의도한 것보다 더 많은 데이터를 반환*하고 클라이언트가 *접근권한이 없는 데이터 노출이 있을 경우* 탐지

〈이슈 확인 및 조치 절차〉

1. 증거 수집

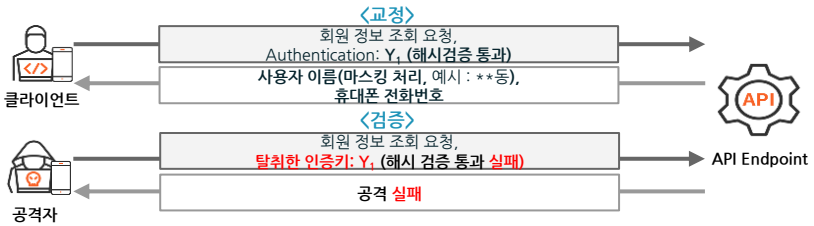


2. 문제 확인

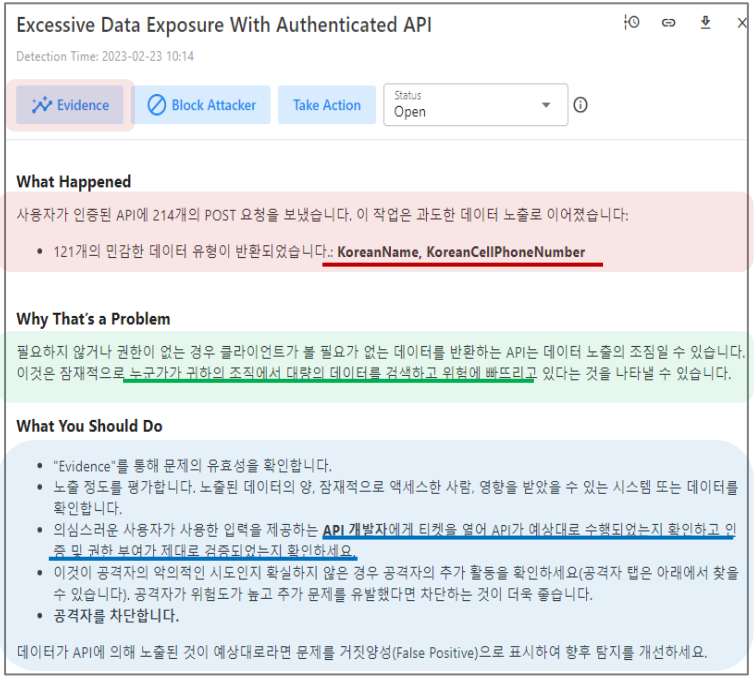
- 대량의 민감 데이터 노출로 인한 2차 피해 발생 예상
  예) 개인 정보 유통으로 인한 (스팸 확산, 명의도용, 금융사기)

3. 조치 및 사전예방

- Key hash 적용 및 민감데이터 Masking 처리하여 교정 후 검증(개발팀 수정)



〈Noname 이슈 화면〉



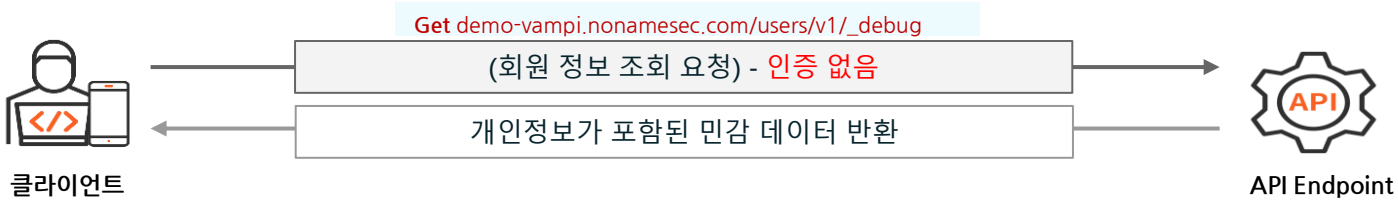
eNsecure

실제 탐지 사례 (해외 리테일)

API 정의

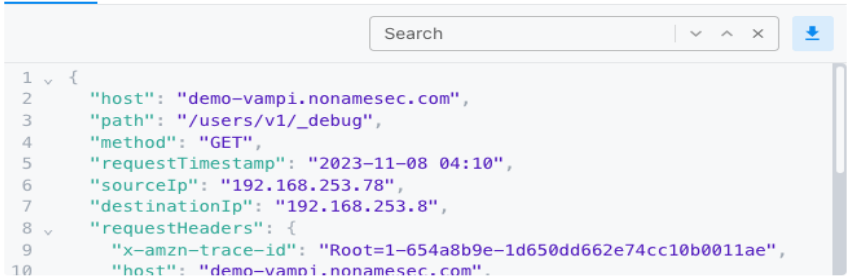
demo-vampi.nonamesec.com/users/v1/_debug

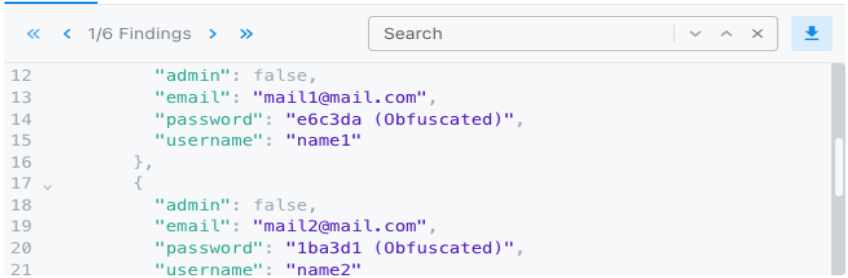
- **용도** : 회원정보 조회(디버깅)
- **Method** : GET (테스트 조회 용도)
- Endpoint 특징 : *요청에 따른 사용자 정보 반환*
- **데이터 유형** : *개인정보가 포함 된 민감 데이터 (사용자 이름 , 이메일, 관리자 여부, 휴대 전화번호, 비밀번호)*



발견된 취약점

1. API Endpoint에서 인증이 없음.
2. 인증 없이 응답에서 대량의 민감 데이터가 평문으로 반환 됨.



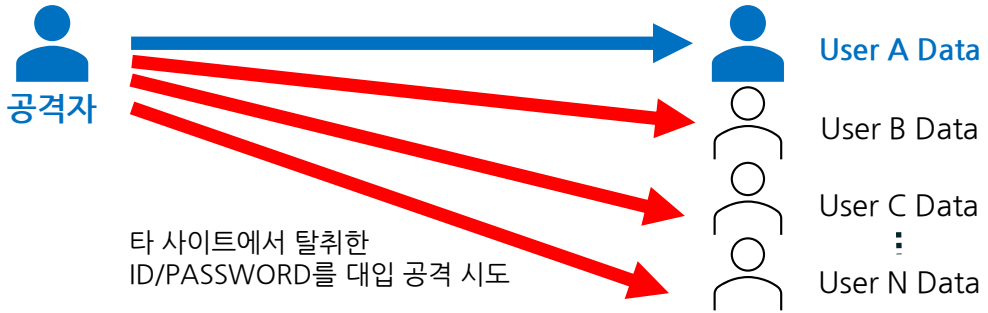


실제 탐지 사례 (해외 리테일)

발견된 취약점 (Password spraying attack)

1. 타 사이트에서 탈취한 PASSWORD를 대입 공격 하는 행위 탐지
2. 대량 요청에 따라 초기에는 401 error 반환 하였지만 대입 공격으로 조기 탐지 하여 시도 차단

n/api/v1/auth/login	[redacted]	Fri Feb 23 2024 13:15:57.000	401
n/api/v1/auth/login		Fri Feb 23 2024 13:15:57.000	401
n/api/v1/auth/login		Fri Feb 23 2024 13:15:57.000	401
n/api/v1/auth/login		Fri Feb 23 2024 13:15:57.000	401
n/api/v1/auth/login		Fri Feb 23 2024 13:15:57.000	401
n/api/v1/auth/login		Fri Feb 23 2024 13:15:57.000	401



감사합니다.

eNsecure

https://ensecure.biz

02-2191-5010

070-7826-6807

mktg@ensecure.co.kr

서울시 용산구 한강대로 71길 4, 7층 엔시큐어