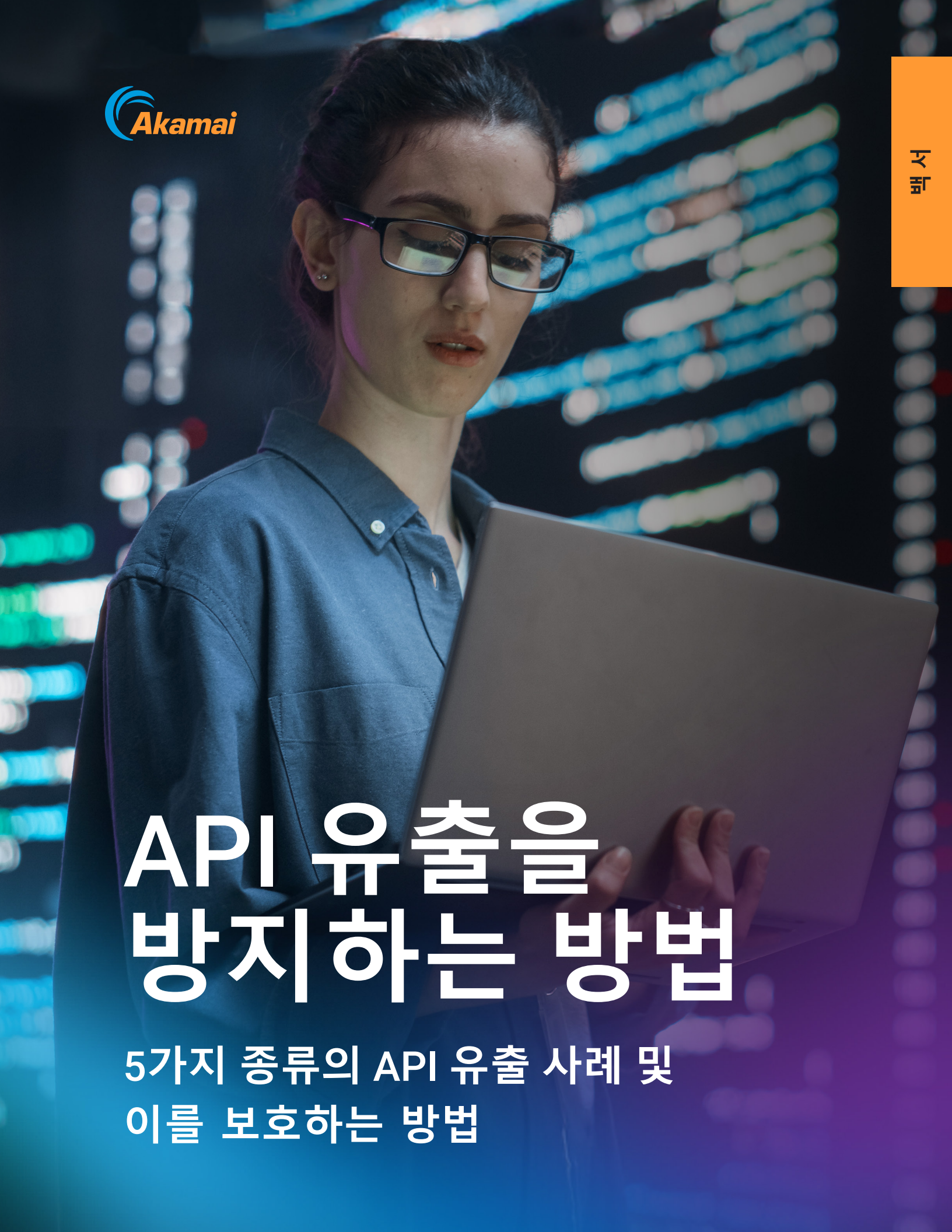


API 유출을 방지하는 방법

5가지 종류의 API 유출 사례 및 이를 보호하는 방법

보고서 내용

서론

API는 파트너, 공급업체, 고객과 데이터를 교환하는 방식으로 기업을 연결합니다. 그러나 대부분의 기업에서는 API 보안이 완전하지 않습니다. 실제로 취약한 API는 공격자들이 악용해 민감한 데이터에 접속하거나 다른 공격자에게 판매하거나 전 세계에 게시하는 등 최근 몇 년 동안 공격자들의 표적이 되어온 기업의 약점입니다. 2024년 소비자 통신, 기업 컴퓨팅, 가상 협업 분야의 글로벌 기업들은 API 유출로 인해 막대한 고객 데이터 및 기타 민감한 데이터의 유출을 겪으며 상당한 재정적 및 평판 비용을 부담해야 했습니다.

API 유출이란 무엇일까요?

간단하게 말하면, API 유출은 API를 의도적으로 악용 또는 남용하여 민감한 데이터에 대한 접속 권한을 얻는 행위입니다. API 유출의 종류는 다양한 기준에 따라 세분화할 수 있습니다. 프로덕션 운영 단계에서 리스크를 발견하고 유출을 방지하려면 리스크를 5가지 카테고리로 구분하는 다음 전략을 고려하는 것이 좋습니다.

1. **알려진 취약점**
   - 공격자는 패치되지 않은 알려진 취약점을 악용합니다.
2. **섀도, 악성, 좀비 및 사용되지 않는 API**
   - 관리되지 않고 잊혀진 API는 운영을 취약하게 만들 수 있습니다.
3. **외부 노출**
   - 인증정보, 키 및 기타 노출이 관리 범위를 벗어날 수 있습니다.
4. **설정 오류 및 운영자 오류**
   - 인프라 및 서비스의 보안 설정 오류는 공격자가 악용할 수 있는 엔트리 포인트를 생성할 수 있습니다.
5. **발견되지 않은 취약점 및 버그**
   - 기업이 최선의 노력을 기울였음에도 불구하고 공격자들은 프로덕션 환경에 생긴 버그와 취약점을 찾고자 합니다.

이 e-Book에서는 이러한 5가지 종류의 각 API 유출 사례에서 보안 실패가 발생하는 위치와 이를 방지하는 방법에 대해 설명합니다. 이 e-Book의 목표는 API 보안 프로그램의 특정 약점을 찾아내어 API 보안을 극대화하고 리스크를 최소화하는 데 도움을 주는 것입니다.

유출 종류: 알려진 취약점

패치되지 않은 알려진 취약점을 활용하는 API 유출은 아마 가장 보편적인 유형일 것입니다. 데이터를 원하는 사이버 범죄자는 일반적으로 제일 먼저 기업에 열려 있는 백도어가 있는지 확인합니다.

2024년 1월 공격자는 인증 관리가 없는 API 엔드포인트를 악용하여 널리 사용되는 프로젝트 관리 툴을 감염시켰습니다. 공격자는 API를 유출한 후 수백만 명의 사용자 정보에 무단으로 접속했고, 몇 달 후 이메일 주소와 이사회 멤버십을 포함한 21GB가 넘는 데이터를 인터넷에 유출했습니다.

인증 및 권한 확인 문제는 가장 일반적인 API 문제입니다. OWASP 10대 API 보안 리스크에서는 손상된 인증을 비롯해 기업이 보호해야 하는 10가지 주요 API 취약점에 대한 교육을 제공합니다.

OWASP 10대 API 보안 리스크에 포함된 리스크 종류로부터 API를 보호하는 것 외에도, 기업은 MITRE에서 운영하는 미국 국립 사이버 보안 FFRDC(Federally Funded Research and Development Center)에서 작성한 CVE(Common Vulnerabilities and Exposure) 목록의 전체 리스크로부터도 API 코드를 보호해야 합니다. 'Log4Shell'이라고도 하는 잘 알려진 Apache Log4j 2 취약점(CVE-2021-44228)이 기억나실 것입니다. Java 프로그래밍 언어 분야의 인기 있는 오픈 소스 로깅 라이브러리인 Log4j 라이브러리의 버그로 인해 공격자는 원격으로 임의 코드를 실행하여 시스템에 대한 접속 권한을 얻을 수 있었습니다. 공격자들은 일반적으로 기업 시스템에 이와 비슷하게 알려진 취약점이 있는지 조사합니다.

미국에서는 CISA(Cybersecurity and Infrastructure Security Agency)가 알려진 CVE(Common Vulnerabilities and Exposures) 카탈로그를 유지하고 있습니다. 다른 국가에도 유사한 카탈로그를 유지하고 있을 수 있습니다.

OWASP 10대 API 보안 리스크 목록은 2019년에 작성되어 2023년에 업데이트되었습니다. 이는 유용하기는 하지만 공격표면의 변화 속도를 따라갈 수는 없습니다. 2024년 한 해에만 2만 4000건이 넘는 새로운 CVE가 CISA 카탈로그에 추가되었으며, 그 중 500개가 넘는 사례가 API와 관련이 있습니다(2024년 8월 중순 기준).

알려진 취약점으로부터 기업을 완벽하게 보호하려면 2가지 방식을 동시에 사용해야 합니다.

1. 개발 및 테스트 프로세스가 알려진 취약점이 프로덕션 환경에 유입되지 못하게 할 만큼 충분히 견고한지 확인해야 합니다.

2. 새로운 취약점이 식별되었다면 가능한 빨리 패치해야 합니다.

많은 기업이 이 2가지 단계 모두에서 어려움을 겪고 있습니다. 게다가 별도의 다양한 취약점을 유입시킬 수 있는 타사 소스의 API 및 코드를 사용합니다. 2022년 한 연구진이 자동차 업계의 여러 제조업체에 영향을 미친 중요한 API 취약점을 발견했습니다. 이러한 취약점은 민감한 고객 정보뿐만 아니라 차량의 위치까지 노출시킬 수 있어 감염된 원격 관리 시스템을 통해 차량의 잠금을 풀거나 시동 또는 비활성화하는 일도 가능했을 것입니다.

예방하는 방법

알려진 취약점으로 인한 API 유출을 차단하는 잘 알려진 방법 중 하나는 보안 패치가 출시될 때 소프트웨어 및 시스템을 신속하게 업데이트하는 것입니다. 또한 개발 및 테스트 프로세스가 포괄적이고 API 보안 모범 사례에 기반을 두고 있는지 확인하는 것도 중요합니다. 여기에는 다음과 같은 내용이 포함됩니다.

- **소프트웨어 공급망 보호:** 사용하는 라이브러리, 오픈 소스 소프트웨어(OSS) 및 기타 타사 코드가 안전한지 확인합니다.
- **시프트 레프트 보안 테스트 구축:** API 보안 및 소프트웨어 테스트와 관련된 작업을 개발 프로세스 초기 단계로 이동시킵니다. 이는 소프트웨어 또는 업데이트를 신속하게 출시하라는 압박을 받고 있는 개발자 팀이 만들어낸 코딩 오류, 설정 오류 등 취약점을 찾아내는 데 도움이 될 수 있습니다.
- **API 보안 체계 관리 활용:** 이는 API 검색을 민감한 데이터 식별 및 취약점 탐지와 결합함으로써 문제를 해결할 때 가장 중요한 API에 우선적으로 초점을 맞추도록 합니다.

Akamai API Security의 이점

Akamai API Security를 사용하면 속도 저하 없이 새로운 것을 구축할 때 알려진 취약점을 줄일 수 있습니다. API Security는 API 관련 취약점을 포괄적으로 다루는 API 보안 테스트 솔루션입니다. 능동적인 테스트는 API 보안 테스트를 개발의 모든 단계로 통합하는 데 도움을 줍니다.

- **모든 API를 찾아서 테스트**하며 이는 애플리케이션의 비즈니스 로직에 대한 이해를 바탕으로 합니다.
- **시프트 레프트** 방식을 구현하기 위해 전체 소프트웨어 개발 수명 주기에 통합됩니다. CI/CD 프로세스 전반에 걸쳐 여러 상태와 환경에 대한 역동적인 API 가시성을 확보할 수 있습니다.
- **개발자 역량 강화**를 위해 간소한 설정 및 자동화, 인라인 테스트 결과, 탐지된 문제 해결을 위한 상황에 맞는 가이드 등 최고 수준의 사용성을 지원합니다.

또한 API Security의 체계 관리는 API 보안 체계를 평가할 수 있도록 트래픽, 코드, 설정에 대한 포괄적인 보기를 제공합니다. API Security는 로그 파일, 과거 트래픽 재생, 설정 파일 등 가능한 가장 광범위한 소스를 활용해 취약점을 탐지합니다. 또한 OWASP 10대 API 보안 리스크의 모든 취약점을 탐지하기도 합니다(체계 관리에 대한 자세한 내용은 '설정 오류 및 운영자 오류' 섹션 참조).

유출 종류: 섀도, 악성, 좀비 및 사용되지 않는 API

볼 수 없는 공격은 방어할 수도 없습니다. 많은 기업에서 대다수의 API가 관리되지 않기 때문에 섀도, 악성, 좀비 및 사용되지 않는 API(다음 페이지의 사이드바 참조)는 보이지 않거나 API 자산 내에 포함되지 않은 공격 표적이 됩니다. 또한 공격자는 기업의 노출된 API를 찾은 후 이전 버전을 찾기 위해 값을 퍼징하거나 조작하는 방식으로 악용할 수 있는 API 변형을 찾으려고 시도합니다.

호주의 한 거대 통신사에 정확히 이 문제가 발생했습니다. 이 기업은 이름, 주소, 생년월일 및 일부 정부 발행 신분증 번호 등 1120만 명 이상의 고객 기록을 실수로 노출시켰습니다. 이 공격은 알 수 없는 이유로 퍼블릭 인터넷에 접속 가능하게 된 테스트에 사용된 API를 악용했습니다. 이 악성 API는 인증 확인이 없었기 때문에 공격자는 수백만 개의 기록을 요청해 받을 수 있었습니다.

대부분의 기업은 다양한 레거시 API 및 새로운 API를 사용해 운영됩니다. 안타깝지만 악성, 좀비 및 섀도 API와 함께 이러한 모든 흔한 요소들이 비즈니스를 다양한 사이버 보안 리스크 및 운영 어려움에 노출시키곤 합니다.

이러한 보이지 않는 API의 출처는 다양합니다.

- **상용 API:** 일부 상용 소프트웨어 패키지에는 다른 애플리케이션 및 외부 데이터 소스와 연결할 수 있는 API가 포함되어 있습니다. 이 API는 누구에게도 발견되지 않고 활성화될 수 있습니다(이는 철저한 API 검색을 통해 해결할 수 있는 문제입니다).
- **이전 버전의 API:** 보안이 약하거나 알려진 취약점이 있는 이전 버전의 API가 제거되지 않고 남아 있는 경우가 많습니다. 소프트웨어가 업데이트되긴 하지만 잠시 동안 이전 버전이 새 버전과 공존해야 할 수 있으며, 프로세스 실패로 인해 이전 API가 차단되지 않으면 이러한 이전 버전은 좀비 API가 됩니다.
- **통지 및 프로세스 실패:** 적절한 사람에게 알리지 않았을 때 섀도 API가 발생합니다. 예를 들어, LOB(Line of Business) 팀이 IT 또는 보안 팀에 알리지 않고 특정 요구사항에 대응하는 API를 생성하거나, 개발자가 절차를 따르지 않을 수 있습니다.
- **상속된 API:** 합병 또는 인수로 인해 상속된 API 또한 자주 간과되어 섀도 API가 됩니다.
- **재활성화된 코드:** 이전 버전의 API를 실수로 다시 활성화하는 경우도 있습니다.

예방하는 방법

정확히 인벤토리화해야 하는 모든 인풋을 문서화하기 위한 수동 API 감사에는 특히 발견하는 모든 API를 평가 및 조치하는 데 소요되는 시간을 고려했을 때 몇 시간이 걸릴 수 있습니다. 이는 이미 업무량이 과도한 보안팀에게는 현실적으로 어려운 작업입니다. 기업은 악성, 좀비 및 섀도 API 악용을 막기 위해 종류에 상관없이 사용 중인 모든 API를 탐지할 수 있는 자동화된 API 검색이 필요합니다. 비즈니스 운영 전반에 걸친 모든 API를 찾아 인벤토리를 구축하고 API 게이트웨이로 관리되지 않는 API와 API 도메인을 검색하는 것은 중요합니다.

Akamai API Security의 이점

API Security는 광범위한 통합 소스를 활용해 원시 트래픽, 로깅 등 API 데이터를 수집할 수 있습니다. 또한 이러한 소스에서 파생된 데이터를 통해 API, 설정 오류, 취약점, API 남용을 탐지할 수 있습니다. 당사의 검색 툴은 OWASP 10대 API 보안 리스크의 모든 취약점을 탐지합니다.

추가 검색 기능을 통해 가능한 작업은 다음과 같습니다.

- 설정이나 종류에 관계없이 RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, gRPC 등 모든 API 탐색 및 인벤토리 구축
- 휴면, 레거시, 좀비 API 검색
- 잊혀졌거나, 방치됐거나, 알려지지 않은 섀도 도메인 탐지
- API 인벤토리를 유지하고 API 문서의 정확성 보장

공격자들이 찾는 높은 리스크의 관리되지 않는 API

섀도 API(일명 '문서화되지 않은 API')는 실제로 존재하며 기업의 공식 모니터링 채널 외부에서 운영됩니다. 이는 개발자가 좋은 의도로 작업을 빨리 하기 위해 만들었거나 이전 소프트웨어 버전의 잔재일 수도 있습니다.

악성 API는 시스템 또는 네트워크에 보안 리스크를 야기하는 인증되지 않았거나 악성 API입니다.

좀비 API에는 새 버전이나 다른 API로 완전히 대체된 후에도 계속 실행되는 API가 포함됩니다.

사용되지 않는 API는 API 변경으로 인해 더 이상 사용이 권장되지 않는 API입니다. 사용되지 않는 클래스, 방법, 항목은 현재는 구현되어 있지만 향후 구현에서는 제거될 수 있으니 새로운 코드에서는 사용하지 말아야 합니다.

유출 종류: 외부 노출

외부 API 취약점은 일반적으로 API 키 및 인증정보 유출, API 코드 및 스키마 노출, 부실한 문서화 및 리포지토리 취약점 등 잘못된 관행이나 절차상의 오류로 인한 것입니다. 운영 범위 밖에 있는 잠재적인 공격 기법을 검색하는 기능은 이제 필수가 되었습니다. 지난 1년 동안 여러 주요한 유출 사례가 API 키나 외부 소스의 기타 인증정보를 실수로 노출한 결과로 발생했습니다. 예를 들어, 해커들은 피싱 캠페인을 사용해 Dropbox의 소스 코드 리포지토리 130곳에 대한 무단 접속 권한을 확보했습니다. 이를 통해 해커들은 GitHub에 부적절하게 저장된 API 키에 접속할 수 있었습니다. 이러한 종류의 노출은 이제 너무 빈번하게 발생했고 GitHub는 API 키와 기타 비밀 유출을 방지하기 위한 조치를 취했지만, 다른 퍼블릭 리포지토리는 여전히 취약할 수 있습니다.

잘 알려진 또 다른 외부 노출 사례에서, 한 연구진이 트위터 API 키를 공개적으로 노출시키고 있는 3000개 이상의 모바일 앱을 발견했습니다. 이러한 실수는 개발자가 개발 중 편의를 위해 애플리케이션 코드에 API 키를 내장하는 경우가 많기 때문에 놀라울 정도로 흔하게 발생합니다. 개발자들이 공개 출시 전에 내장된 키를 제거하지 못하면 이는 키 노출의 잠재적 원인이 됩니다.

예방하는 방법

이러한 종류의 외부 노출을 줄이거나 없애려면 다음 2가지 방식을 동시에 사용해야 합니다.

- 절차를 강화해 키 및 인증정보 유출, 부적절한 리포지토리 사용 등과 같은 노출 소스를 식별하고 제거합니다.
- 외부 공격표면을 정기적으로 스캔하여 취약점을 탐지하고 해결합니다.

광범위한 API 위협으로부터 보호하려면 내부 검색('악성 API로 인한 유출' 참조)과 외부 검색이 모두 필요하며, 이를 통해 노출을 식별하고 외부 공격표면을 줄일 수 있습니다.

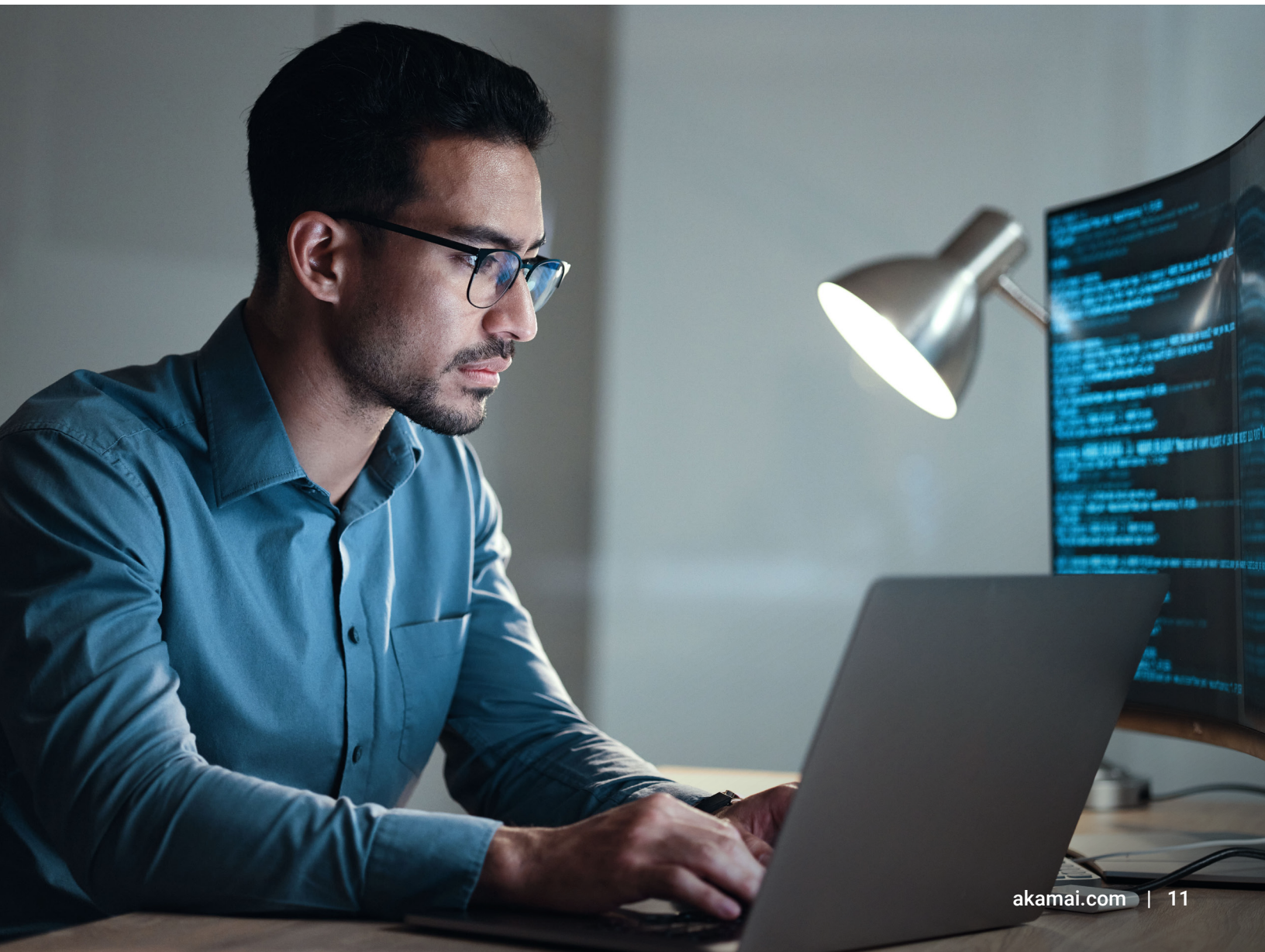
Akamai API Security의 이점

API Security는 해커가 사용하는 정찰 기술을 시뮬레이션하고 신속하게 문제를 찾아 해결할 수 있도록 함으로써 공격자보다 앞서 나갈 수 있도록 도와줍니다. 또한 아웃사이드 인 검색을 통해 외부 공격표면을 정기적으로 자동 스캔해 공격자가 발견하기 전에 취약점을 찾아내기 때문에 다음과 같은 이점을 제공합니다.

- **공개 취약점 찾기:** API 키 및 인증정보 누출, 코드 노출, 설정 오류, 리포지토리 취약점 등과 같은 중요한 문제를 신속하게 찾아 해결합니다.
- **기업과 관련된 도메인 및 하위 도메인 검색:** 인터넷 레지스트라, 인증서 레지스트라 및 오픈 소스 등 다양한 소스에서 수집한 데이터를 활용합니다.
- **실제 공격 방법 통합:** 기업의 도메인 또는 하위 도메인을 대상으로 제한된 쿼리를 실행해 정보를 수집하는 공격자의 외부 정찰 행위를 시뮬레이션합니다.

유출 종류: 설정 오류 및 운영자 오류

많은 사이버 공격자들이 서버, 네트워크, API 게이트웨이 및 API 트래픽을 중개하고 보호하는 방화벽의 설정 오류를 악용하여 침입합니다. IBM Security X-Force의 연구 결과에 따르면 클라우드 유출 사고의 3분의 2가 잘못 설정된 API와 관련이 있는 것으로 나타났습니다. 보안 설정 오류는 안전하지 않은 기본 설정, 접속 제어가 없는 클라우드 스토리지(매우 흔함), 불완전한 설정 또는임시 설정으로 인해 발생할 수 있습니다. 디지털 기반이 확대됨에 따라 여러 퍼블릭 클라우드의 가용성 영역 또는 AWS, Microsoft Azure, Google Cloud 등의 퍼블릭 클라우드를 포함한 더 많은 위치로 운영이 확장될 수 있습니다. 이러한 환경은 다양한 보안 제어를 받으며 운영되는 경우가 많기 때문에 보안이 모든 곳에서 올바르게 설정되도록 하는 것은 복잡하고 어렵습니다.



예방하는 방법

인프라 측면에서 보안 설정 오류를 방지하는 가장 좋은 방법 중 하나는 서버, 네트워크 디바이스, 게이트웨이 및 방화벽의 수동 설정을 최대한 방지하는 것입니다. 기업의 관리 팀이 인프라 및 애플리케이션 보안 제어를 수동으로 또는 정기적으로 '조정'할 경우 설정 취약점이 발생할 가능성이 높아집니다.

자동화는 보안에 있어 가장 좋은 방법입니다. 일부 기업은 수작업으로 인한 실수를 방지하기 위한 방법으로 변경 불가능한 인프라라는 개념을 도입하고 있습니다.

인프라, 서비스 및 API가 완벽히 보호되도록 모든 조치를 취했어도 여전히 API 체계 관리가 필요합니다. 체계 관리는 API 수명 주기 전반에 걸쳐 API 보안을 관리, 모니터링 및 유지하는 툴을 제공합니다.

API Security의 이점

API Security의 체계 관리 모듈은 API 호출과 인프라를 분석하여 설정 오류를 식별합니다. 일반적으로 Amazon S3 버킷 문제, 인증되지 않은 API의 민감한 데이터, 여러 쿠버네티스 접속 기반 설정 오류가 이러한 설정 오류에 속합니다.

체계 관리 모듈은 트래픽, 코드, 설정에 대한 포괄적인 보기를 제공하므로 API를 통해 이동하는 모든 형태의 민감한 데이터(예: 개인 식별 정보)를 포함해 API 및 웹 애플리케이션 전반에 걸쳐 전체 공격표면을 확인할 수 있습니다. 또한 민감한 데이터를 노출시킬 수 있는 취약한 암호화를 방지하기 위해 API 관리 툴이 강력한 프로토콜과 암호를 사용하고 있는지 확인하는 데 도움이 됩니다. 추가적으로, API는 만료된 JSON Web Tokens를 허용해서는 안 됩니다. 그러면 무단 접속이 허용되고 보안 리스크가 증가할 수 있기 때문입니다. 이 모듈은 리디렉션 없이 안전하지 않은 포트에서 수신 대기하는 애플리케이션 부하 분산과 같은 설정 오류를 방지하는 데도 도움이 됩니다. 이러한 모든 조치는 API 보안 체계를 강화하여 잠재적인 위협에 대한 보다 안정적인 방어를 보장합니다.

유출 종류: 발견되지 않은 취약점

대부분의 유출 종류와 마찬가지로, 인프라를 스캔하는 사이버 범죄자들은 주기적으로 CVE, OWASP 10대 API 보안 리스크, 기타 일반적인 설정 오류는 물론 악성, 좀비 및 섀도 API를 찾습니다. 또한 라이브러리, 오픈 소스 코드, 기타 종류의 퍼블릭 코드는 물론 코딩 오류, 버그, API 자산의 설정 오류의 악용 가능한 새로운 취약점을 찾기 위해 노출된 API를 조사하기도 합니다. 이러한 취약점을 통해 사이버 범죄자는 API 호출을 조작하고 퍼징 문자열을 요청에 삽입할 수 있습니다. 그 결과 사이버 범죄자들이 사용하는 기술은 끊임없이 발전하고 있습니다.

예방하는 방법

예방의 중요한 부분은 코드가 버그와 취약점으로부터 최대한 자유롭게 만드는 것입니다('알려진 취약점' 섹션 참조). 그러나 공격자들이 여전히 버그를 찾거나 API를 악용할 수 있는 키 또는 인증정보에 접속하려는 상황을 생각해야 합니다.

API 런타임 보안은 취약점이 알려져 있는지 여부에 상관없이 취약점을 악용하는 해커를 식별하도록 설계되었습니다. 이는 이전에 탐지되지 않은 버그 및 설정 오류가 프로덕션 환경에 들어가지 않도록 API 자산을 보호하는 유일한 방법인 동시에 감염된 인증정보와 키를 보호하는 최선의 방법입니다.

런타임 보안은 API 사용 및 데이터 접속에서 비정상적인 패턴과 비정상을 탐지하기 때문에 수천 또는 수백만 개의 데이터 레코드가 유출되기 전에 레이더에서 놓칠 수 있는 지속적인 공격을 탐지하고 문제를 해결할 수 있습니다.

API 런타임 보안은 다음과 같은 악성 API 요청을 식별하고 차단하는 데 도움이 됩니다.

- API에서 대량의 민감한 데이터를 빼내는 공격
- 손상된 오브젝트 수준의 권한 확인(BOLA) 공격

API 런타임 보안 솔루션은 다음을 탐지할 수 있습니다.

- 데이터 유출
- 데이터 정책 위반
- API 보안 공격
- 데이터 변조
- 의심스러운 행동

또한 런타임 보안 기능은 API 트래픽을 로깅하고, 민감한 데이터 접속을 모니터링하고, 위협을 탐지하며, 공격 기법을 차단하거나 해결합니다.

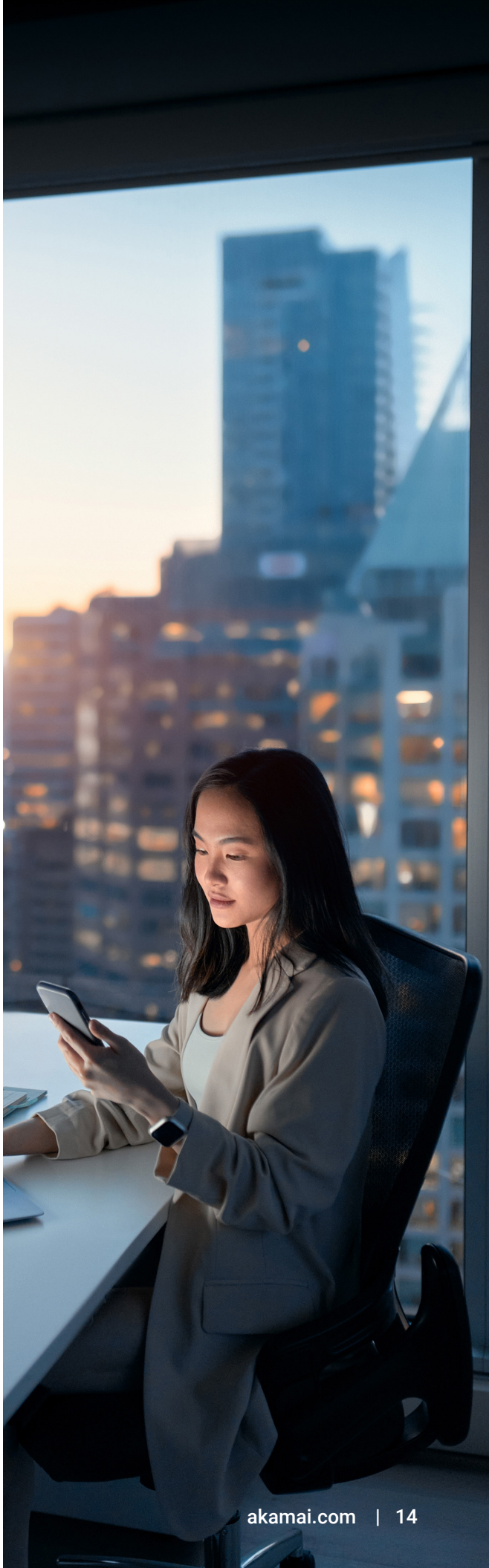
API Security의 이점

다른 예방 조치가 부족한 경우 런타임 보안은 최후의 방어선입니다. 런타임 보안의 가장 큰 기능은 실시간으로 API 공격을 탐지 및 차단하는 것입니다. API Security는 자율 머신 러닝(ML) 기반 모니터링 기능을 사용해 실시간으로 트래픽을 분석하고 데이터 유출, 데이터 변조, 데이터 정책 위반, 의심스러운 행동 및 API 보안 공격에 대한 상황별 인사이트를 제공합니다. 또한 API 트래픽에서 비정상 및 잠재적 위협을 탐지하고 사전에 선택한 인시던트 대응 정책을 기반으로 문제 해결을 용이하게 합니다.

API Security는 ML을 사용하여 각 API에 대해 행동 모델을 생성합니다. 그런 다음, 정상적인 행동에 관한 이 기준선을 사용해 API 비즈니스 로직 공격을 탐지합니다. 런타임 보안에서 발생하는 모든 문제에는 심각도, 상태, OWASP 10대 API 보안 리스크에 대한 매핑, 그리고 해당되는 경우 공격자 세부 정보가 포함됩니다. 또한 문제 분류 및 해결을 지원하기 위해 공격자의 세션 세부 정보, API 요청 및 응답 사본 등과 같은 증거들도 포함되어 있습니다.

API Security의 런타임 보안 기능은 실시간으로 API 공격을 탐지 및 예방하며 지속적으로 API 설정 오류를 탐지합니다. 또한 인기 있는 다양한 워크플로우의 통합을 통해 운영 및 해결을 간소화합니다.

아마 가장 반가운 소식은 API Security가 WAF, API 게이트웨이, ITSM, SIEM 및 기타 워크플로우 툴과 통합되어 공격에 대한 종합적인 방어 기능을 제공한다는 점입니다. 사용자는 위협 해결을 완전히 자동화하거나 더 나은 가시성 및 제어를 위해 다양한 수준의 수동 개입을 요구할 수 있습니다.



5가지 유출 종류, 5가지 예방 원칙

이제 사이버 범죄자들이 API를 어떻게 이용하는지 알기 때문에 이를 예방하는 데 집중할 수 있습니다. 다음에서 소개하는 내용은 함께 사용해야 하는 5가지 예방 툴과 전략적 관점입니다.

1. API 보안 시프트 레프트

- 시프트 레프트 API 보안 방식은 사이버 범죄자가 취약점을 찾을 수 있는 프로덕션 환경에 취약점을 노출시키지 않도록 개발 과정에서 API를 광범위하게 테스트하는 방식입니다.

2. 인사이드 아웃 검색

- 운영 전반에 걸쳐 모든 API를 식별합니다.

3. 아웃사이드 인 검색

- 유출된 키와 인증정보, 부적절한 리포지토리 사용과 같은 노출 소스를 탐지 및 제거하며, 정기적으로 외부 공격표면을 스캔해 취약점을 식별 후 해결합니다.

4. 포괄적인 체계 관리

- 설정 오류와 취약점을 방지함으로써 항상 API 보안을 위한 최선의 노력을 합니다.

5. 런타임 보안

- 비정상적인 API 활동을 탐지하고 이전에 식별되지 않은 취약점 및 버그 등 가능한 모든 위협으로부터 보호합니다.

데모 요청하기

Akamai API Security가 작동하는 방식을 확인하고 얼마나 쉽게 API의 설정 오류를 식별 및 해결하고 악성 API 공격을 방어할 수 있는지 경험해 보세요. 주요 기업들이 당사의 API 보안 솔루션을 선택하는 이유를 직접 알아보세요.

데모 다운로드