API 보안 구매자 가이드

API 보안 관련 도전 과제 해결

기업이 점점 클라우드 중심적이고 디지털화됨에 따라 API의 범위와 규모가 증가하여 기업의 가치도 함께 증가합니다. API는 현재 다음과 같이 사용되고 있습니다.

- 최신 AI 혁신을 비롯해 고객과 파트너에게 서비스를 제공하는 애플리케이션과 서비스의 핵심에서 운영됨
- 개발자가 사용하는 서비스부터 엔지니어가 리프트 앤 시프트(lift and shift)하는 워크로드에 이르기까지 클라우드 환경 전반에 걸쳐 내장됨
- 매출 흐름을 대변하고 비즈니스를 성장시키며 개발자 생태계를 구축

그러나 API 보안 인시던트를 경험한 IT 및 보안 전문가의 78%에 해당하는 분이라면[1] API가 점점 리스크로 다가오고 있다는 사실을 직접 확인하셨을 것입니다. 노출되었거나 설정 오류를 내재한 API를 쉽게 발견할 수 있고, 보안이 취약하며 쉽게 감염될 수 있습니다. 많은 기업이 자사의 API에 대해 모든 것을 알고 있지는 않기 때문에 이를 관리하지 못하는 경우가 많습니다. 이러한 휴면 또는 좀비 API는 주요 공격 기법입니다.

이는 매우 위험합니다. API에 대한 공격은 기업의 매출, 안정성 및 규제 컴플라이언스에 심각한 영향을 미칠 수 있습니다. 대부분의 기업은 아직 API 공격을 방어할 수 있는 적절한 관리 능력 및 기능을 갖추고 있지 않습니다. 게다가 많은 기업들이 API 게이트웨이 및 웹 애플리케이션 방화벽 등 기존 스택에 API 툴을 보유하고 있습니다. 그러나 이러한 툴은 일부 보호 기능을 제공할 수 있지만, 최신 API 공격을 방어하기 위한 가시성, 실시간 보안, 지속적인 테스트를 제공하도록 설계되지는 않았습니다.

1. Akamai Technologies, “API Security Disconnect Report,” 2023

그렇다면 API 자산을 완전히 보호하기 위해 무엇이 필요할까요? 지난 몇 년 동안 수많은 API 보안 제품이 등장했지만, 점점 늘어나는 벤더사의 범위와 기능을 파악하는 것은 어려운 일입니다.

오늘날의 위협은 API 검색, 체계 관리, 위협 탐지 및 해결, 보안 테스트라는 4개의 주요 영역을 포괄하는 완전한 API 보안 솔루션을 필요로 합니다. 이 구매자 가이드에서는 생태계의 모든 API를 찾아서 보호하는 동시에 보안 API를 개발 및 유지 관리하는 데 필요한 기능 및 보안 제어를 정의하고 포괄적인 API 보안 솔루션의 핵심 기능에 대해 설명합니다.

포괄적인 API 보안을 위한 핵심 기능

필요한 API 보안 기능을 결정하려면 직면한 도전 과제의 특성을 이해하는 것이 중요합니다.

API는 온프레미스에서 하이브리드 클라우드에 이르기까지 여러 환경에 분산되어 있는 경우가 많습니다. 여기에 API 생태계가 자체 네트워크와 클라우드를 훨씬 넘어 확장되어 있을 가능성이 높다는 점이 이를 더 복잡하게 만듭니다. API 보안을 우선시할 수도 있고 그렇지 않을 수도 있는 써드파티의 앱, 서비스 및 시스템과 API가 무수히 많은 연결을 맺어온 것을 생각해보세요.

게다가 다음과 같은 내용에 대한 실시간 인사이트를 얻는 것은 어렵습니다.

- API가 라우팅되는 위치
- 설정 방식
- 이동하는 민감한 데이터
- 발생하는 리스크

기업이 새로운 애플리케이션과 API를 빠르게 개발 및 출시함에 따라 공격표면이 기하급수적으로 증가합니다. 오래된 API의 경우, API 보안이 중요한 요구 사항으로 떠오르기 몇 년 전에 구축 및 생산된 API 클러스터가 기업에 있을 수 있습니다.

가시성이 부족하면 문제가 발생할 수 있습니다. 전체 API 인벤토리를 보유한 보안 전문가 10명 중 4명만이 어떤 API가 호출될 때 민감한 데이터를 반환하는지 알고 있습니다. 이러한 API 호출의 대부분은 취약점을 테스트하는 악의적인 공격자로부터 발생하며, 일단 취약점을 발견하면 가차 없이 공격하는 경우가 많습니다.

API를 완벽하게 보호할 수 있다고 주장하는 보안 벤더사를 검토할 때는 4가지 주요 영역에 걸쳐 인프로덕션 제어 및 기능을 확립하는 것이 중요합니다.

벤더사의 기능을 검토하는 데 사용할 수 있는 구매자 체크리스트에 대해 알아보려면 계속 읽어보세요.

01

API 검색

아무도 모르는 API가 생각보다 많습니다. 그러나 정확한 인벤토리가 없으면 기업은 다양한 리스크에 노출될 수 있습니다. API를 효과적으로 인벤토리화하려면 다음이 가능해야 합니다.

- ☑ 설정이나 종류에 관계없이 API를 찾아 인벤토리화
- ☑ 휴면, 레거시, 좀비 API 탐지
- ☑ 잊히거나, 방치되거나, 알려지지 않은 섀도 도메인 탐지
- ☑ 사각지대를 제거하고 잠재적인 공격 경로 발견

02

API 체계 관리

단순한 API 설정 오류로 인해 공격자에게 공격의 문이 열릴 수 있습니다. 일단 내부에 침투하면 민감한 데이터에 빠르게 접속해 유출할 수 있습니다. 모든 API가 어떻게 설정되었는지 이해하려면 다음이 가능해야 합니다.

- ☑ 인프라를 자동으로 스캔해 설정 오류와 숨겨진 리스크 발견
- ☑ 주요 이해관계자에게 취약점을 알리는 맞춤형 워크플로우 생성
- ☑ 민감한 데이터에 접속할 수 있는 API 및 내부 사용자 식별
- ☑ 탐지된 문제에 심각도 순위를 할당해 해결 우선순위 지정

03

API 위협 탐지 및 해결

API 공격은 이제는 피할 수 없는 상황으로 접어들고 있습니다. 위협을 효과적으로 탐지하고 개선하려면 다음이 가능해야 합니다.

- ☑ 데이터 변조 및 유출, 정책 위반, 의심스러운 행동, API 남용 모니터링
- ☑ 보안관제센터에 알릴 수 있도록 모든 소스의 API 트래픽을 분석하고 기존 워크플로우(티켓팅, 보안 정보 및 이벤트 관리 등)와 통합
- ☑ 부분적으로 또는 완전히 자동화된 해결을 통해 실시간으로 공격 및 오용 방지

04

API 보안 테스트

개발자가 구축하는 모든 애플리케이션에는 속도가 필수적이지만, 이는 취약점이나 설계 결함을 발견하기 어렵게 만듭니다. API를 제대로 테스트하려면 다음이 가능해야 합니다.

- ☑ 악성 트래픽을 시뮬레이션하고 기본 API 비즈니스 로직을 따르는 광범위한 자동화된 테스트 수행
- ☑ API가 프로덕션 환경에 들어가기 전에 취약점을 발견해 공격 성공 리스크 줄이기
- ☑ 확립된 거버넌스 정책 및 룰에 따라 API 사양 검사
- ☑ 온디맨드 또는 CI/CD 파이프라인의 일부로 실행되는 API 중심 보안 테스트 실행

API 검색: 핵심 기능에 대해 자세히 알아보기

많은 기업이 레거시 및 신규 API를 모두 운영하고 있습니다. 운영팀이나 보안팀의 누구도 알지 못하는 관리되지 않는 API가 프로덕션에 존재하는 경우가 종종 있으며, 이로 인해 기업은 다양한 사이버 보안 리스크와 운영상의 어려움에 노출될 수 있습니다. 로그 API는 통지 및 프로세스 실패, 폐기 시 종료되지 않는 등의 요인으로 인해 발생할 수 있습니다. 다음 페이지에는 주의해야 할 주요 예시가 나와 있습니다.

상용 API

일부 상용 소프트웨어 패키지에는 다른 애플리케이션 및 외부 데이터 소스와 연결할 수 있는 API가 포함되어 있습니다. 이러한 API는 아무도 눈치채지 못하게 활성화될 수 있습니다.

비활성화 실패

API는 공식적으로 폐기되었지만 운영상의 실수로 계속 가동될 수 있습니다. 이러한 API를 좀비 API라고 하기도 합니다.

이전 버전의 API

이전 버전의 API가 폐기되지 않는 경우도 있습니다. 소프트웨어가 업데이트되는 동안 이전 버전이 일정 기간 동안 새 버전과 공존해야 할 수 있습니다. 하지만 API를 비활성화할 책임이 있는 담당자가 퇴사하거나, 인사이동이 있거나, 단순히 이전 버전을 중단하는 것을 잊어버리면 어떻게 될까요?

통지 및 프로세스 실패

적절한 사람에게 알리지 않았을 때 악성 API가 발생하기도 합니다. 예를 들어, LOB(Line of Business)팀은 IT 팀에 알리지 않고 특정 요구사항에 대응하는 API를 생성할 수 있고, 개발자는 절차보다 실행에 더 관심을 가질 수도 있습니다. 합병으로 인해 '물려받은' API들도 자주 간과됩니다. 이러한 종류의 악성 API는 종종 섀도 API라고 합니다.

벤더사와 상담할 때는 악성, 레거시, 좀비, 섀도 API가 악용되기 전에 이를 식별하고 처리하는 방법을 설명해 달라고 요청하세요. 레거시 및 좀비 API는 API 보안의 가장 취약한 고리인 경우가 많습니다. 따라서 API 게이트웨이의 관리 밖에 있는 API를 발견하고 찾아내어 이를 인벤토리화하고, 해결이나 폐기가 필요한지 결정하는 것이 중요합니다.

핵심 API 검색 기능

API 보안 솔루션에는 다음과 같은 검색 기능이 포함되어야 합니다

API 자산 검색 및 정밀한 인벤토리

API 검색 툴은 설정이나 종류에 관계없이 RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, gRPC 등 보유하고 있는 API를 찾아 식별할 수 있어야 합니다. 또한 인벤토리가 오래되지 않도록 자동으로 업데이트되는 인벤토리를 생성해야 하며, 모든 속성을 기반으로 API를 검색, 태그 지정, 필터링, 할당 및 내보낼 수 있는 기능을 제공해야 합니다.

휴면, 레거시 및 좀비 API 탐지

레거시 및 좀비 API는 기업의 API 보안 이니셔티브보다 앞서 있을 수 있습니다. 이러한 API들은 일반적으로 소유권이 없으며 보이지 않거나 보안 제어가 없는 상태에서 작동합니다. API 검색 툴에게 이러한 API를 찾아낼 수 있는 능력은 중요합니다.

섀도 도메인 검색

섀도 API 외에도 사용자가 전혀 모르는 API 도메인 이름, 즉 전체 섀도 도메인이 있을 수 있습니다. API 검색 툴은 보안 리스크를 초래할 수 있는 잊혀지거나, 방치되거나, 알려지지 않은 섀도 도메인을 식별할 수 있어야 합니다.

자동 스캔

스캐닝은 사각 지대를 제거하고 다음과 같은 중요한 문제를 식별하는 데 필수적입니다.

- 유출된 API 키 및 인증정보
- API 코드 및 스키마 노출
- 인프라 설정 오류
- 문서, GitHub 리포지토리, Postman Workspaces 등의 취약점

이러한 문제점 및 기타 악용 가능한 인텔리전스 소스를 파악하면 팀이 사이버 범죄자들에게 악용될 수 있는 잠재적인 공격 경로를 이해하는 데 도움이 될 수 있습니다.

제한된 맞춤형 개발

마지막으로, 적절한 API 검색 툴을 사용하면 트래픽 소스에 대한 맞춤형 개발이 필요하지 않습니다. 이러한 툴은 주요 인프라 구성요소를 위해 사전 구축된 통합 작업과 함께 제공되어야 합니다. 맞춤형 개발은 일반적으로 시간이 많이 걸리며, 소스 오리진이 변경되면 통합 작업을 다시 해야 할 가능성이 높기 때문에 이미 과부화된 IT 보안팀이 확장시키기란 불가능합니다.

API 체계 관리: 핵심 기능에 대해 자세히 알아보기

API 자산에 대한 위협은 중앙 집중식 IT에서 분산된 LOB 운영으로의 전환, 클라우드 리소스 사용 증가, 마이크로서비스 기반 아키텍처로 전환 등의 트렌드로 인해 빠르게 증가하고 있습니다.

API 자산을 보호하기 위한 첫 번째 단계는 (이전 섹션에서 설명한) 강력한 검색입니다. 현재 사용 중인 모든 종류의 API를 검색하고 인벤토리화해야 합니다.

API 전반에 걸쳐 보안 체계를 관리하는 데 필수적인 몇 가지 추가 기능이 있습니다. 고객 정보와 같은 데이터에 접근하는 API는 반드시 인증되어야 합니다. 따라서 어떤 API가 민감한 데이터에 접속하고 이를 전송하는지 식별해야 하며, 그에 따라 이러한 API를 분류할 수 있어야 합니다. 또한 API를 더욱 취약하게 만들 인프라 취약점을 파악하는 것도 중요합니다.

설정 평가

많은 사이버 공격은 네트워크, API 게이트웨이 또는 API 트래픽을 중개하고 보호하는 방화벽의 단순한 설정 오류로 인해 성공합니다.

API 보안 솔루션은 로그 파일, 과거 트래픽의 재생, 설정 파일 등 인프라 및 소프트웨어 설정을 정기적으로 검사해야 합니다. 이를 통해 설정 오류 및 취약점을 발견하고 설정 드리프트로 인한 리스크를 제거할 수 있습니다.

맞춤화 가능한 심각도

사용자 환경에서 새로운 취약점을 식별하는 솔루션은 발견된 문제에 심각도 수준을 지정하여 문제 해결에 우선 순위가 지정될 수 있도록 해야 합니다. 심각도 수준은 기업의 리스크 허용 한도, 규제 요구 사항 및 내부 정책에 맞게 맞춤화할 수 있어야 합니다.

맞춤형 워크플로우

맞춤화 가능한 심각도와 함께 이상적인 체계 관리 툴은 취약점을 발견하면 즉시 조치를 취할 수 있는 맞춤형 워크플로우를 만들 수 있어야 합니다. 이러한 워크플로우는 티켓 생성부터 주요 이해 관계자에게 알리는 것, 네트워크 설정 업데이트까지 다양합니다.

자동 생성된 문서

API 문서는 API의 기능과 사용 방법을 소비자에게 알려줍니다. 기업은 사양 및 정확한 문서화에 대한 컴플라이언스를 위해 API를 평가해야 합니다. 문서가 부실하거나 존재하지 않으면 보안 테스트가 더 어려워지고, 탐지되지 않은 취약점이 있는 API가 프로덕션 환경에 도달할 리스크가 높아집니다. 이 문제는 종종 API 개발을 아웃소싱함으로써 악화됩니다. API 보안 프로그램의 성공을 원한다면 문제의 원인과 상관없이 오래된 문서, 미완료 문서 및 문서 누락을 허용하지 말아야 합니다.

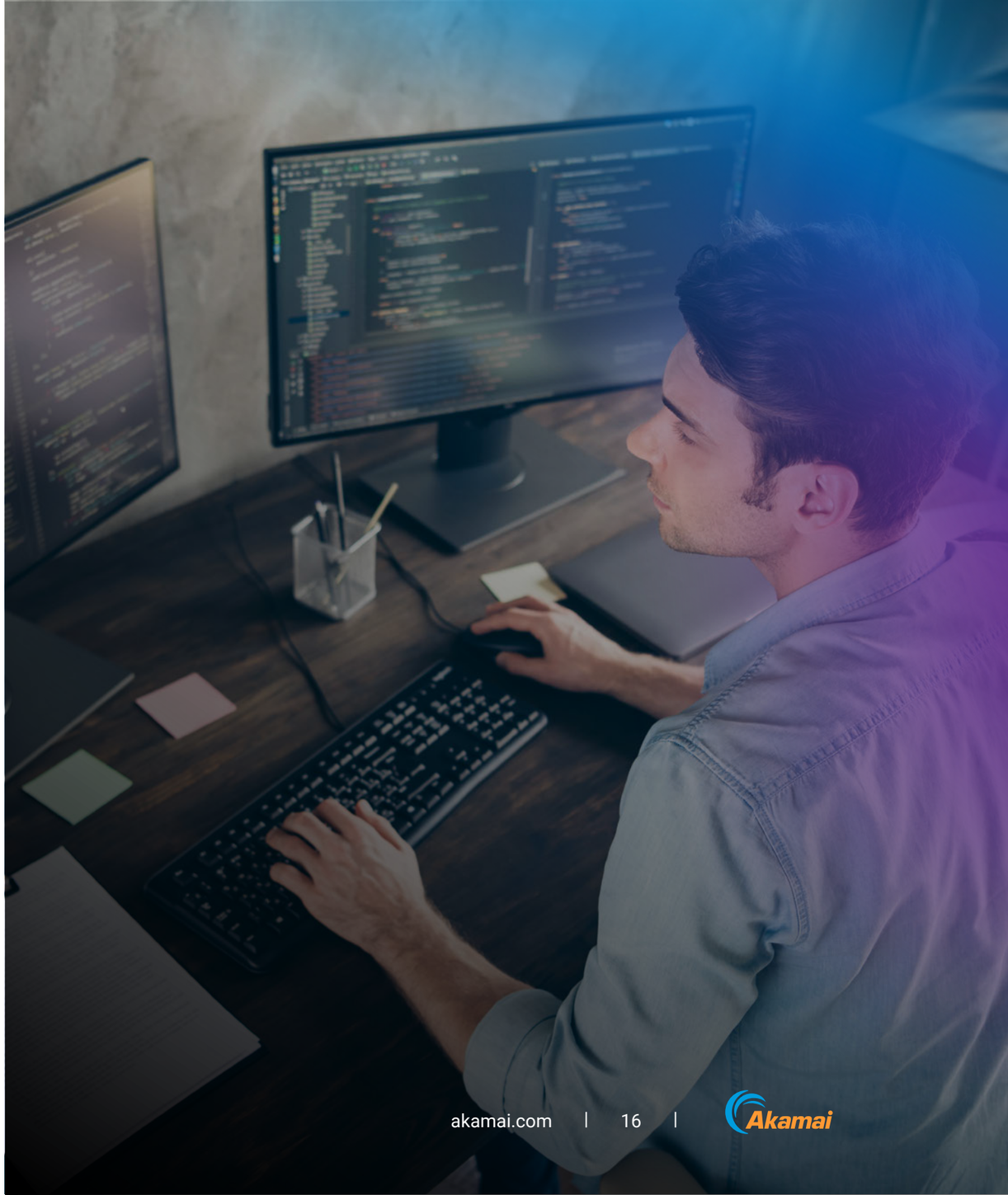
OpenAPI 사양은 표준 인터페이스 설명을 정의합니다. API 보안 솔루션은 다음이 가능해야 합니다.

- 기업이 배포된 API 중 어떤 API가 사양을 벗어났으며 잠재적인 리스크가 될 수 있는지 확인할 수 있도록 API 사양과 실제 관찰 가능한 트래픽을 비교하고 차이점 식별
- 모든 API가 제대로 문서화되고 문서가 최신 상태를 유지할 수 있도록 API의 현재 및 미래 상태를 기반으로 전체 OpenAPI 문서를 자동으로 생성 이러한 문제점 및 기타 악용 가능한 인텔리전스 소스를 파악하면 팀이 사이버 범죄자들에게 악용될 수 있는 잠재적인 공격 경로를 이해하는 데 도움이 될 수 있습니다.

API 위협 탐지 및 해결: 핵심 기능에 대해 자세히 알아보기

API 취약점을 악용하려는 공격은 이제 현실이 되었습니다. 이제 기업이 공격을 받을지 여부가 중요한게 아니라 언제, 어떻게 공격받을지가 관건입니다. 개인 고객 데이터 유출 등 심각한 피해를 입힐 수 있는 공격은 사전에 신속하게 탐지하여 차단해야 합니다. API를 최대한 안전하게 만들더라도 데이터 유출, 데이터 변조, 데이터 정책 위반, 의심스러운 행동 및 API 보안 공격을 탐지하려면 능동적인 런타임 보호 기능이 필요합니다. 여기에는 API 트래픽 로깅, 민감한 데이터 접속 모니터링, 위협 탐지, 공격 기법 차단 또는 해결 등이 포함되어야 합니다.

다음 두 페이지에서는 API 보안 솔루션에 포함되어야 하는 핵심 기능에 대해 설명합니다.



실시간 아웃오브밴드 모니터링

API 보안 모니터링은 API 트래픽에 영향을 미치거나 느리게 만들어서는 안 됩니다. 기업이 더 빠르게 배포하고 더 많은 트래픽을 확인할 수 있도록 에이전트리스 접근 방식을 제공할 수 있는 벤더사를 찾아보세요. 하지만 복잡한 온프레미스 환경과 같이 적절한 상황에서는 에이전트도 지원할 수 있는 충분한 유연성을 갖춘 솔루션이어야 합니다.

API 보안 솔루션은 식별된 데이터 소스의 트래픽을 미러링하고 백그라운드에서 해당 트래픽 데이터를 분석해 발견된 모든 문제를 실시간으로 알려야 합니다.

API 비정상 및 악용 탐지

API 수와 API 트래픽의 전체 규모가 계속해서 확장되기 때문에 수동적인 데이터 수집만으로는 충분하지 않습니다. API 활동을 지속적으로 분석해 비정상적인 이벤트를 탐지하고 보안 및 운영팀에 통보해야 합니다.

최신 툴에는 실시간으로 트래픽을 분석하고 상황에 맞는 인사이트를 활용하는 AI 및 머신 러닝 기능이 통합되어 있습니다. 이를 통해 데이터 유출, 데이터 변조, 데이터 정책 위반 및 기타 API 보안 공격을 나타낼 수 있는 비정상적인 활동을 식별할 수 있습니다.

API 공격 방어

비정상이나 기타 다른 문제가 식별되고 알림이 만들어지면 이제는 시간이 가장 중요합니다. API를 통한 민감한 데이터의 무단 이동 또는 그밖에 다른 API의 오용으로 의심되는 경우 이를 탐지하고 차단해야 합니다. API 보안 솔루션은 기존 방화벽 및 API 게이트웨이와의 통합을 통해 오용을 차단할 뿐만 아니라, 문제 해결을 부분적으로 또는 완전히 자동화해야 합니다. 또한 특정 종류의 알림을 다루려면 반자동적인 문제 해결이 가능해야 합니다. 이전에 식별된 반복적인 문제의 경우 완전 자동화된 대응을 제공하는 옵션이 있어야 합니다.

공격 신뢰도 점수 산정

시장에 출시된 일부 솔루션은 API 행동, 네트워크 트래픽 패턴, 지리적 위치 데이터 및 위협 인텔리전스 피드를 비롯한 외부 및 내부 신호를 평가할 목적으로 학습된 머신 러닝 알고리즘을 사용합니다. 이러한 맥락적 요소를 사용하는 솔루션은 탐지된 런타임 인시던트가 악성 활동의 결과라는 것에 대해 신뢰도 수준을 결정할 수 있습니다.

인시던트 대응 통합

인시던트가 발생할 경우 API 보안 솔루션에는 적절한 팀에 해결 작업이 배정되도록 하는 데 필요한 통합 작업 기능이 포함되어 있어야 합니다. 설정 오류, 데이터 정책 위반 또는 의심스러운 행동이 탐지되면 올바른 수준의 상황 인식을 보장할 수 있도록 API 게이트웨이, SIEM 시스템 및 기타 정보 보안 엔진에 보고되어야 합니다.

일반적으로 API 보안 솔루션은 기업에서 사용하는 다른 보안, 모니터링 및 관리 툴과 쉽게 통합되어야 합니다.

API 보안 테스트: 핵심 기능에 대해 자세히 알아보기

많은 개발팀이 저지르는 실수 중 하나는 API 테스트를 너무 오래 기다렸다가 시작해 테스트가 병목 현상을 일으키는 것입니다. 개발팀은 개발 프로세스 초기에 테스트를 시작해 포괄적인 테스트가 이루어지도록 하기 위해 시프트-레프트 접근 방식을 취해야 합니다. 효과적인 API 보안 테스트의 이점은 다음과 같습니다.

- **공격 방지**
  - API가 프로덕션 환경에 들어가기 전에 취약점을 발견함으로써 공격 성공의 리스크를 줄일 수 있습니다.
- **컴플라이언스 개선**
  - 포괄적인 테스트를 통해 컴플라이언스를 보장하고 벌금 및 평판 훼손을 방지할 수 있습니다.
- **신뢰도 향상**
  - 철저하고 효과적인 테스트를 통해 기업의 API에 대한 신뢰도를 높이고, 개발자가 정해진 일정에 제품을 출시할 수 있도록 지원합니다.

시중의 일부 벤더사는 기업의 환경 문제를 해결하는 방법과 포괄적인 API 테스트 설정을 활성화하는 방법에 대한 권장 사항을 기업에 제공할 수 있습니다. 권장 사항에는 적절한 인증을 설정하거나 API 의존성을 수정하는 작업 단계가 포함될 수 있습니다. 장점: 환경 내에서 비즈니스 로직 문제를 해결할 수 있는 경우 테스트에 최적화된 API의 수를 늘려 테스트 범위를 늘릴 수 있습니다.

그러나 API 보안 테스트의 개념 자체는 아직도 모호한 상태입니다. 개발팀은 여기에 필요한 모든 사항을 완전하게 이해하고 있지 않을 수도 있습니다. 시프트-레프트 API 검사는 다음 세 단계 프로세스로 구성됩니다.

1. **API 이해:** API의 사용 사례를 잘 이해하면 특히 까다로운 비즈니스 로직 문제에 대한 테스트를 더 효과적으로 수행할 수 있습니다.
2. **사용자가 API와 올바르게 상호 작용할 수 있는지 확인:** API를 의도한 대로 사용할 수 있는지 확인합니다. 사용자가 API 작동 방식을 정확히 이해하는지 반드시 확인해야 합니다.
3. **API로 공격 트래픽 전송:** 여기에는 API에 대한 요청을 수동으로 조작하거나, 요청에 퍼징 문자열을 삽입하거나, 자동화된 툴을 사용해 API 보안 테스트를 수행하는 것이 포함될 수 있습니다. 오늘날 IT에서 자동화는 속도 저하 없이 대규모 작업을 수행하는 가장 효과적인 방법입니다.

주요 API 보안 테스트 기능

API 보안 테스트에는 정적, 동적 테스트 및 모의 해킹이 포함되어야 합니다. API 보안 솔루션에는 테스트 프로세스를 최대한 자동화하여 철저한 테스트를 가능하게 하는 툴이 포함되어야 합니다. API 보안 솔루션에서 다음과 같은 API 테스트 기능을 찾아보세요.

사전 예방적 자동 API 보안 테스트

자동화된 보안 테스트는 API가 프로덕션에 들어가기 전에 설정 오류, 취약점 및 규정 미준수를 파악하여 리스크와 비용을 크게 줄여줍니다.

API 거버넌스

업무, 책임, 정책과 같은 거버넌스 문제를 반드시 고려해야 합니다. 여기에는 개발자, 보안 엔지니어 및 플랫폼 엔지니어에 대한 실무 수준의 책임, 리스크에 대한 정책 감독 및 결정이 포함됩니다. API 보안 솔루션을 사용하면 확립된 거버넌스 정책 및 룰에 따라 API 사양을 검사할 수 있습니다.

CI/CD 파이프라인 및 코드 리포지토리 통합

DevSecOps는 소프트웨어 개발 워크플로우에 보안을 추가하는 DevOps의 변형입니다. API 보안은 DevSecOps 이니셔티브의 일부가 되어야 합니다. 또한 API 보안 솔루션은 온디맨드 또는 CI/CD 파이프라인의 일부로 실행되는 API 중심 보안 테스트 제품군을 제공해야 합니다. CI/CD 통합은 애플리케이션 개발 속도를 따라잡는 데 필요한 지속적이고 신속한 API 보안 테스트를 가능하게 하므로 필수적입니다.

모든 것을 한 번에,
API 보안 공백을 파악하고 해결

API는 점점 더 디지털화되고 클라우드 중심적인 경제에서 고객에게 서비스를 제공하고 매출을 창출하며 효율적으로 운영할 수 있게 하는 기업의 필수 구성요소입니다. 그러나 지속적인 성장, 민감한 데이터에 대한 근접성, 보안 제어의 부재로 인해 API는 오늘날 공격자들에게 매력적인 표적이 되고 있습니다.

많은 기업이 API를 관리하고 기본적인 보안을 확보하기 위해 사용하는 기존 툴들은 어느정도 리스크를 줄이는 효과가 있습니다. 그러나 오늘날 API 위협을 방어하기에는 충분하지 않습니다. 이 툴을 유일한 보안 수단으로 생각해 의존해서는 안 됩니다.

대신, 기업은 이 구매자 가이드에 나오는 4가지 구성요소, 즉 검색, 체계 관리, 위협 탐지 및 해결, 보안 테스트 등을 모두 제공할 수 있는 포괄적인 API 보안 솔루션을 찾아야 합니다. 특정 분야에서 효과가 입증된 기존 툴들을 버리지 않아도 됩니다. 기존 툴과 원활하게 통합될 수 있는 솔루션을 찾아 보세요.

API 보안을 시작한다고 해서 중요한 리소스를 할당해야 하는 것은 아닙니다. 보안 스택의 특정 취약점을 해결하는 소규모의 측정 가능한 파일럿으로 시작할 수 있습니다. 또는 포괄적인 업데이트를 통해 API 보안 여정을 시작할 수도 있습니다. 모든 기업은 다릅니다.

API에 초점을 맞춘 공격이 증가하고 있는 가운데 가장 중요한 단계는 조치를 취하기로 결정하는 것입니다. 이 구매자 가이드가 도움이 되셨기를 바랍니다.

API 공격 방법, 일반적인 API 취약점 및 기업을 보호하는 방법에 대해 **자세히 알아보세요**.

맞춤 Akamai API Security 데모 일정을 예약하고 어떤 도움을 받을 수 있는지 알아보세요.

Akamai 보안은는 성능이나 고객 경험에 영향을 주지 않으면서 모든 상호 작용 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 관해 자세히 알아보려면 **akamai.com** 및 **akamai.com/blog**를 확인하거나 **X**(기존의 Twitter), **LinkedIn**에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 9월 발행.

Akamai