Akamai

전자책

API 보안의 8가지 필수 사항과 금지 사항

강력한 API 보안 체계를 위한 핵심 요소

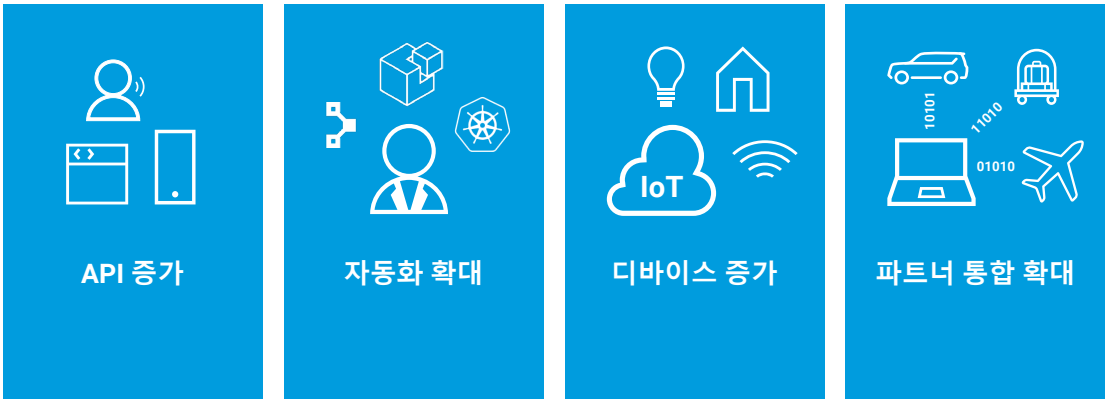
API를 보호하는 것이 어려운 이유

API 보안은 많은 IT 경영진의 우선순위 목록에서 1위를 차지할 만한 이유가 있습니다. 다음을 고려해보세요.

"API의 폭발적인 증가로 공격자들이 노리는 공격표면도 늘어났으며, API 보안은 보안 리더들을 계속 당황스럽게 만들고 있습니다."

— API 보안의 8대 구성요소, Forrester Research, Inc., 2023년 9월 28일

API 리스크를 증가시키는 요인



API 리스크에 대응하려는 기업은 효과적인 API 보안을 구축하기 전에 먼저 다음 사항을 이해해야 합니다.

API는 움직이는 표적	
내부 API 인식	**외부 API 노출**
빠르게 진행되는 DevOps 프로세스는 API를 지속적으로 생성하고 폐기해 불완전한 API 인벤토리 발생	미숙한 API 관행으로 인해 많은 섀도 API를 포함한 민감한 API가 의도치 않게 외부에 노출됨

API를 취약하게 만드는 두 가지 종류의 위협	
기술적 취약점	**오용 및 남용**
공격자가 OWASP API 보안 상위 10대 취약점을 비롯한 소프트웨어 취약점과 잘못된 설정을 악용할 수 있음	비즈니스 로직 남용과 공격적인 데이터 스크레이핑 같은 기타 행동은 기술적 취약점과 관계없이 발생

복잡한 API 보안 문제를 해결하려면 다음과 같은 신중한 접근 방식이 필요합니다.

최신 기술 발전의 통합

기업의 장벽 허물기

전체 API 위협 환경에 대응

다음은 기업을 위해 보다 정교한 API 보안 전략을 개발할 때 구축해야 할 몇 가지 필수 전략과 피해야 할 함정입니다.

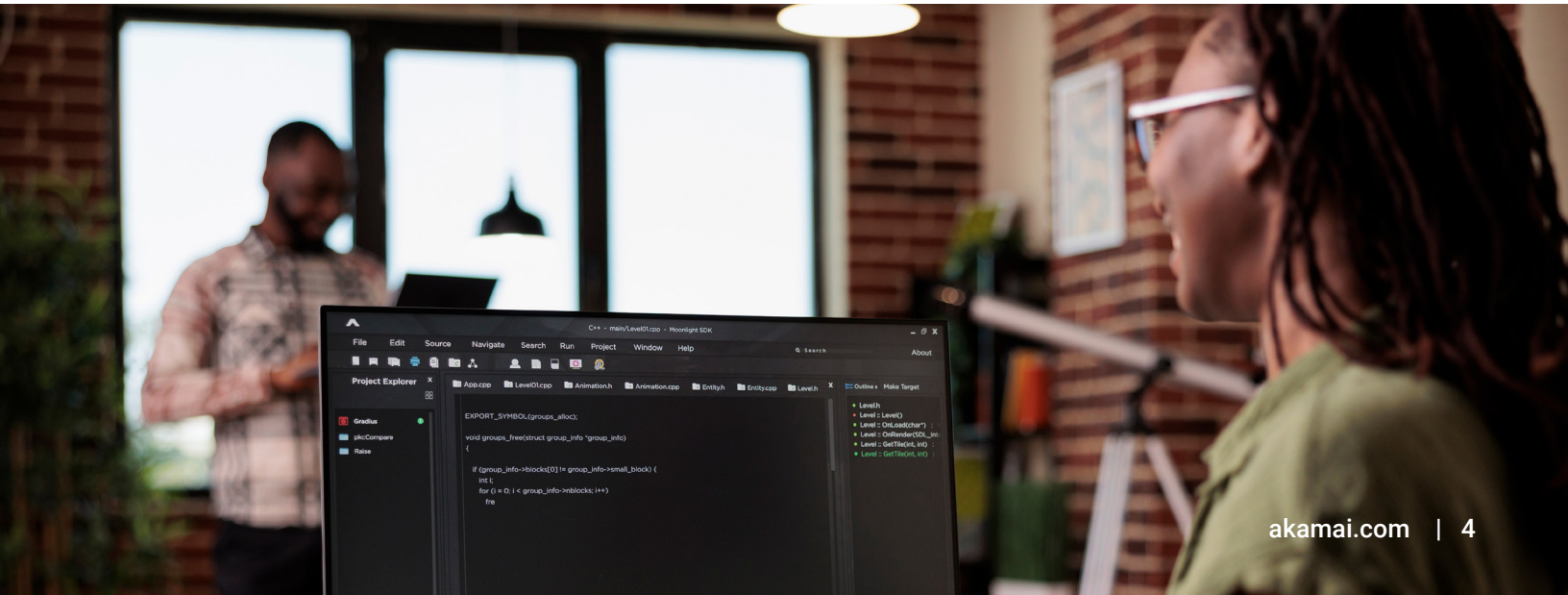
API 보안의 8가지 필수 사항과 금지 사항

1 완벽한 API 가시성을 확보할 것

다시 한번 강조하겠습니다. 존재 여부를 모르는 API는 보호할 수 없습니다. API가 식별되지 않고 모니터링되지 않는 기간이 길어질수록 공격자의 표적이 될 가능성이 높아집니다. 완벽한 가시성을 확보하는 가장 좋은 방법은 API 보안 플랫폼이 API 게이트웨이, 네트워크 디바이스, 마이크로서비스 오케스트레이션 솔루션, 클라우드 공급업체 등 최대한 광범위한 데이터 소스에서 정보를 수집하도록 하는 것입니다. 특히 다음과 같은 기능을 갖춘 API 보안 솔루션이 필요합니다.

시간	위치
• 지속적인 API 검색 • 개별 API 호출 모니터링 • 단기 세션 활동 기록 • 시간 경과에 따른 API 행동 분석	• 기업 전체의 API 검색 • 레거시 API 검색 • 섀도 API 발견

최신 데이터 유출 기법에서는 공격자가 저속 공격을 통해 API에서 데이터를 스크레이핑하기 때문에, 완벽한 API 가시성을 갖춰야 API 데이터 유출을 방지할 수 있습니다. 모든 API가 어디에 있는지 파악하는 것이 이 새로운 종류의 공격을 방지하는 첫 번째 단계입니다.



2 클라우드를 두려워하지 말 것

WAF(Web Application Firewall)는 시그니처 기반 기술을 사용해 권한이 없는 API가 기업에 침투하는 것을 방지합니다. API 공격이 진화함에 따라, 행동 애널리틱스를 사용해 가능한 모든 리스크로부터 API를 완벽하게 방어할 수 있는 추가 레이어가 필요해졌습니다. 이제 외부에 노출된 API뿐만 아니라 기업 내부에서 API의 행동을 모니터링해야 합니다.

행동 애널리틱스를 효과적으로 활용하려면 클라우드에서 API 트래픽을 분석해야 합니다. 기업의 활동에 대한 민감한 정보를 클라우드로 전송하는 것을 주저하는 보안팀도 있습니다. 그러나 대부분의 기업이 생성하는 방대한 양의 API 데이터에 확장된 탐지 및 대응 기술을 사용해 실질적인 행동 애널리틱스를 진행하는 것은 클라우드가 제공하는 규모와 탄력성이 없다면 실현 가능성이 매우 낮습니다.

보안팀의 한정된 리소스로 인해 발생하는 길고 복잡한 제품 배포 역시 발전을 가로막는 주요 장애물입니다. 광범위한 API 사용으로 인해 리스크가 증가하는 상황에서 보안팀은 더 이상 뒤처질 여유가 없습니다. 따라서 API 보안 전략의 일환으로 클라우드로 전환하는 것이 필수적입니다.

3 비즈니스 맥락을 전략의 중심에 둘 것

API를 발견하고 보안 리스크를 식별하는 것은 API 공격표면을 축소하기 위한 여정의 시작에 불과합니다. 다음 세 가지 질문을 고려하세요.

1. 특정 파트너의 API 인증정보가 감염되었는지 어떻게 확인하나요?

2. API에서 데이터 스크레이핑의 형태로 기업 스파이 행위가 발생하고 있는지 어떻게 확인하나요?

3. 사용자가 계정 데이터를 훔치기 위해 인보이스 번호를 열거하는 방식으로 인보이스 발행 API가 악용되고 있는지 어떻게 확인하나요?

첫 번째 시나리오의 경우 정상적인 사용자로부터 활동이 시작될 것입니다. 따라서 악성 의도를 탐지할 수 있는 유일한 방법은 해당 API에서 예상되는 행동과 다른 변화를 발견하는 것입니다. 두 번째와 세 번째 시나리오는 정상적인 API 접속 모델을 악용하는 승인되지 않은 행동 사례이기도 합니다. 이런 기술적인 문제 외에도 비즈니스 맥락을 이해하는 것이 중요한 경우가 있습니다.

4 데이터의 일방통행을 지양할 것

효과적인 API 보안 접근 방식의 기본 기능 중 하나는 선호하는 보안 모니터링 및 IT 워크플로우 툴로 알림과 이벤트를 전송하는 기능입니다. 보안 벤더사와 알림을 구축하는 팀이 흔히 저지르는 실수는 보안 알림과 자동화된 응답을 단방향 통신 흐름으로 간주하는 것입니다.

많은 정상적인 비즈니스 프로세스와 마찬가지로 공격은 오랜 시간에 걸쳐 발생할 수 있습니다. 제대로 된 결과를 얻으려면 API 사용에 대한 행동 애널리틱스를 최소 30일 이상 진행해야 합니다. 이를 통해 예상되는 기본 행동에 대한 보다 완전하고 정확한 그림을 얻을 수 있습니다. 며칠 또는 몇 주에 걸쳐 느리게 실행되는 공격과 수많은 API 세션도 탐지할 수 있습니다. 정의된 속도 제한에 미치지 못하는 저속 데이터 스크레이핑 공격을 생각해 보세요. 이러한 행동은 과거 행동과 변경 사항을 비교해 조사해야만 발견할 수 있습니다.

세부 정보가 뒷받침되지 않는 알림은 득보다 실이 많을 수 있습니다. 그러나 원인과 영향에 대한 풍부한 맥락이 포함된 알림은 훨씬 더 유용한 정보를 제공합니다. 맥락이 풍부하고 유용한 알림을 제공하며 수신자에게 보다 광범위한 데이터 집합을 쿼리해 인시던트를 분석할 수 있는 기능을 활용하면 진정한 승리를 거둘 수 있습니다. 그런 다음 WAF 방어 기능을 통해 비즈니스에 잠재적인 위협이 될 수 있는 트래픽을 즉시 차단할 수 있습니다.

5 부서 간 협업을 우선시할 것

설계, 개발, 배포 단계에서 취약점을 사전에 방지하면 API 보안을 크게 개선할 수 있습니다. 이를 효과적으로 달성하려면 팀 간 협업이 필요합니다.

협업 프로세스는 API 팀이 실제 환경에서 API가 어떻게 사용(및 악용)되고 있는지에 대한 가시성을 제공하는 것부터 시작해야 합니다. 이와 같은 가시성은 시간이 지남에 따라 API 개발 및 배포 프로세스의 초기에 보안을 중시하는 문화를 조성할 것입니다. 또한 다음과 같은 내용도 중요합니다.

- 접근 방식의 핵심 보안 기능 외에도 API 팀이 보다 효과적으로 작업하는 데 도움이 되는 비보안적 장점이 있습니다.
- 개발자와 같은 비보안 사용자가 API 인벤토리와 활동 정보를 쉽게 보고 쿼리할 수 있습니다.
- 개발자에게 필요한 보안 수정을 위해 사전에 티켓을 열어주는 Jira와 같은 개발 툴과의 통합 등으로 상황에 맞게 대응할 수 있습니다.

API 보안을 모두의 업무로 생각하고 보안팀 외부의 이해관계자가 쉽게 참여할 수 있도록 하면 개발, 운영, 보안팀이 서로를 탓하는 일이 없이 상호 유익한 방식으로 협력할 수 있습니다.

6 써드파티 API를 간과하지 말 것

피해야 할 또 다른 일반적인 API 보안 전략의 함정은 자체 API만 걱정하면 된다고 생각하는 것입니다. 구매한 WAF나 API 게이트웨이가 전체 API 보안 전략을 표준화한다고 믿을 수 있다면 더없이 좋겠지만, 항상 그런 것은 아닙니다.

예를 들어, 중앙 집중식 API 게이트웨이 전략이 구축되었다고 해서 섀도 API가 핵심 API 거버넌스 접근 방식을 우회하지 않을 것이라고 가정해서는 안 됩니다. 비즈니스가 써드파티 API에 의존하는 경우, 게이트웨이는 해당 API가 생태계와 연결되기 전에 감염되었더라도 인증된 것으로 간주합니다.

API 보안 전략은 API 게이트웨이와 같은 기본 API 기술과 연계되어야 하며, 네트워크 디바이스, 클라우드 플랫폼, 마이크로서비스 오케스트레이션 툴 같은 다른 소스에서 가능한 한 많은 정보를 수집해야 합니다. 그래야만 기술 및 인프라 전환이 불가피한 상황에서 API 공격표면에 대한 완전한 그림을 그리고 미래에 대비하는 보안 전략을 수립할 수 있습니다.

7 뒤늦게 대응하지 말고 선제적으로 움직일 것

알림에 신속하고 효과적으로 대응하는 것도 좋지만, 알림이 발생한 후 이를 방어하는 데에만 집중한다면 알림을 완전히 피할 기회를 놓치게 됩니다. 선제적으로 위협을 탐지하세요. 데이터 쿼리를 수행할 수 있도록 지원하는 API 보안 파트너가 있다면 자체적으로 가설을 테스트하고, 관계를 이해하고, 보안 인시던트로 확대되기 전에 잠재적인 위협을 식별할 수 있습니다. 예를 들어 특정 파트너가 API를 잘못 사용하고 있는 것을 알게 된 경우, 몇 번의 클릭만으로 다른 파트너나 공급업체의 유사한 행동을 찾을 수 있습니다.

모든 API 보안 파트너는 데이터 레이크에 기록 데이터를 저장하고 이 데이터에 대한 접속을 제공해 조사와 위협 탐지가 이뤄지도록 해야 합니다.

이러한 종류의 풍부한 쿼리 기능은 두 가지 방식으로 제공되는 것이 가장 좋습니다.

1. 간단하고 직관적인 사용자 웹 인터페이스

2. 보다 정교한 워크플로우 개발에 활용할 수 있도록 API 보안 공급업체의 자체적인 API 인터페이스 세트 제공

8 지속적인 라이프사이클 개념으로 API 보안에 접근할 것

API 보안을 비즈니스에 직접 구축하는 가장 좋은 방법은 API 테스트를 활용하는 것입니다. 이 툴을 API 라이프사이클에 추가하면 잘못 설정되거나 취약한 API가 프로덕션에 투입될 가능성을 제한할 수 있습니다. 개발 초기에 이러한 테스트와 수정 작업을 진행하면 골칫거리를 줄이고, 시간을 절약하고, 비용을 절감할 수 있습니다.

다음으로 보안팀은 기업에서 사용 중인 API의 인벤토리를 생성해 API 보안을 위한 노력을 시작해야 합니다. API는 지속적으로 추가되고 삭제되기 때문에, 보안팀은 민감한 애플리케이션과 데이터 리포지토리에 API 인터페이스의 인벤토리를 최신 상태로 유지해야 합니다. 지속적으로 API가 효과적으로 식별되면 섀도, 악성, 잊혀진, 좀비, 고아, 더 이상 사용되지 않는 API 문제에서 모두 벗어날 수 있습니다.

보안팀은 새로운 API 보안 위협을 광범위하게 탐지하고 방어하는 데 필요한 가시성을 확보해야 합니다. 위협 탐지는 런타임 중에도 이루어져야 합니다. 비즈니스 로직의 남용은 프로덕션 환경의 API에서만 발견됩니다. 런타임 행동과 기준이 되는 정상적인 사용 패턴을 비교하면 악성 행동을 발견할 수 있습니다.

마지막으로, 런타임 중 언제라도 API를 악용할 수 있는 위협을 실제로 차단해야 합니다. 단순히 모든 것에 대해 알림을 보내는 것만으로는 매크로 수준에서 비즈니스를 보호하기에 충분하지 않으므로 이 단계에서는 WAF를 통한 자동 차단이 중요합니다. API 게이트웨이의 속도 제한을 낮추거나, 개발자가 조사할 수 있도록 Jira 티켓을 열거나, 보안팀에 이메일을 보내는 등의 다양한 자동화된 응답을 사용자 지정할 수 있습니다. 맥락을 이해하고 대응 메커니즘을 맞춤형으로 지정할 수 있어야만 탐지된 모든 위협에 적절하게 대응할 수 있습니다.

요약

필수 사항	금지 사항
✔ 완벽한 API 가시성을 확보할 것	✘ 클라우드를 두려워하지 말 것
✔ 비즈니스 맥락을 전략의 중심에 둘 것	✘ 데이터의 일방통행을 지양할 것
✔ 부서 간 협업을 우선시할 것	✘ 써드파티 API를 간과하지 말 것
✔ 지속적인 라이프사이클 개념으로 API 보안에 접근할 것	✘ 뒤늦게 대응하지 말고 선제적으로 움직일 것

지금 시작하기

API 보안에 대한 현대적이고 체계적인 접근 방식을 위한 첫걸음을 내딛을 준비가 되셨나요?

Akamai API Security에 대해 자세히 알아보세요.

Akamai의 클라우드 기반 접근 방식을 사용하면 몇 분 안에 쉽게 시작할 수 있습니다. 비즈니스 로직과 API 간의 관계에 대한 상세한 이해를 포함해 기업 전반의 API 사용 현황을 몇 시간 내에 완벽하게 파악할 수 있습니다.

Akamai

Akamai는 어디에서 구축하고 제공하든지 생성하는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 인력, 시스템, 데이터를 보호합니다. Akamai 플랫폼은 글로벌 위협에 대한 가시성을 바탕으로 제로 트러스트 지원, 랜섬웨어 차단, 앱 및 API 보안 또는 DDoS 공격 차단을 목표로 보안 체계를 조정하고 발전시켜 지속적으로 안심하고 혁신하며 확장하고 가능성을 현실로 구현할 수 있습니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com와 akamai.com/blog를 확인하거나 X(기존의 Twitter)와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 12/23 발행.