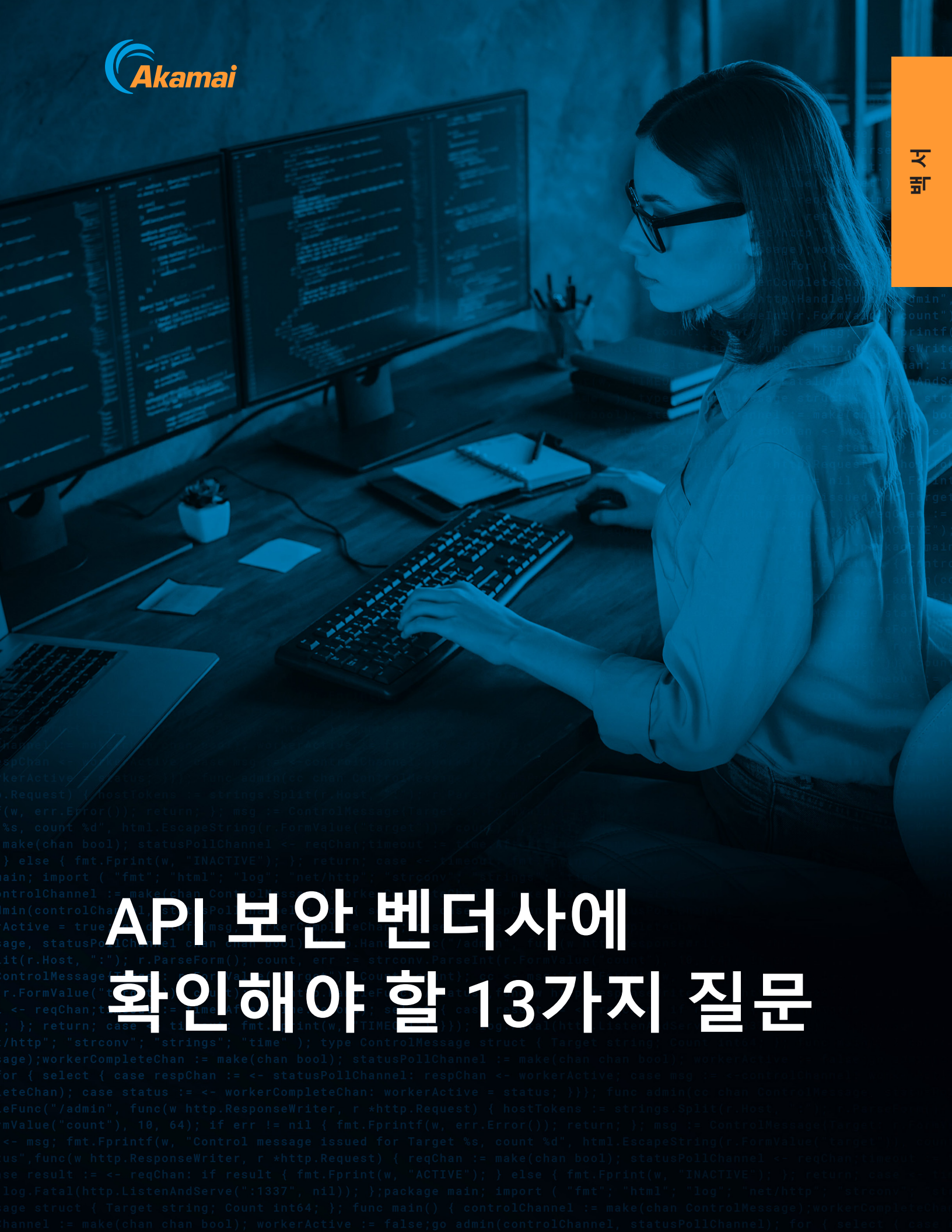
Akamai

eBook



API 보안 벤더사에 확인해야 할 13가지 질문

서론

B2B API 네트워크는 기하급수적으로 성장하고 있습니다. 또한 사물 인터넷 디바이스의 세계가 확장되면서 개발자가 API를 통해 실제 데이터를 애플리케이션으로 가져올 수 있는 새로운 기회가 열리고 있습니다.

API는 혁신과 성장을 위한 여러 새로운 기회를 제공하지만 다음과 같은 새로운 보안 문제도 발생합니다.

- API 인증정보 도난
- 탐지되지 않는 API 정찰
- 인증 및 권한 부여 설정 오류
- 보호에 취약한 섀도 및 좀비 API
- 원격 코드 실행, 인젝션, 로컬 파일 인클루전, 기타 공격 기법
- 데이터 유출
- API 스크레이핑
- 비즈니스 로직 남용

보안 벤더사는 이러한 위협과 기타 API 위협을 탐지하고 방어할 수 있도록 다양한 옵션을 제공하지만, 이러한 옵션이 모두 동일한 효과를 제공하거나 사용하기 쉬운 것은 아닙니다.

다음은 API 보안 벤더사와 논의를 진행할 때 벤더사의 제품이 기업의 API 보안 요구사항을 얼마나 효과적으로 해결할 수 있는지 평가하는 데 도움이 될13가지 질문입니다.

1 API 보안 제품이 전사적으로 API 검색을 할 수 있나요?

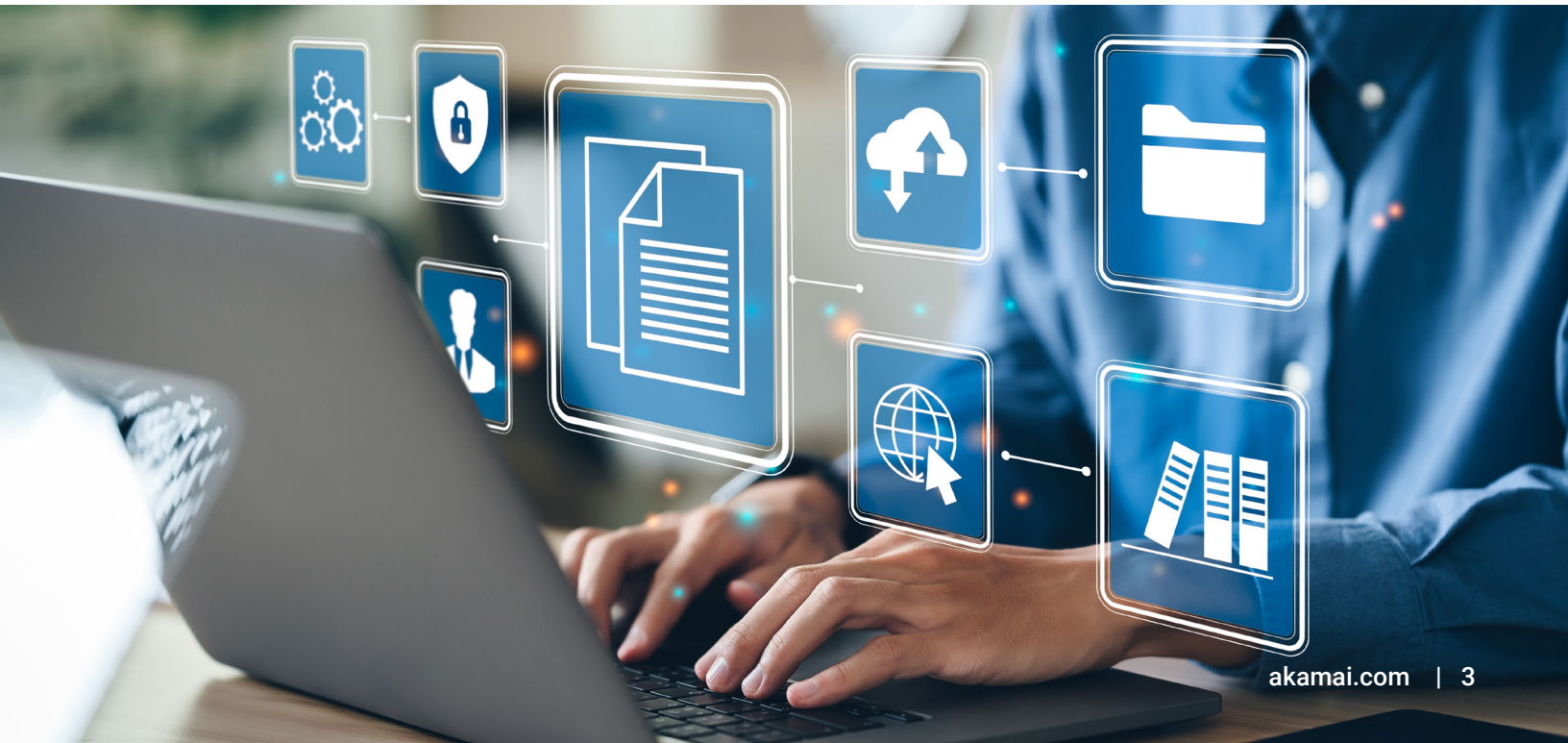
보안팀이 직면하는 가장 큰 문제 중 하나는 기업이 노출하는 모든 API에 대한 완전하고 정확한 인벤토리를 가지고 있지 않다는 것입니다. 보안팀이 놓치는 문서화되지 않은 섀도 API 중 상당수는 공식적인 API 관리 및 보안 프레임워크에 포함되지 않습니다. 기업에서 폐기했다고 생각한 좀비 API가 여전히 접속할 수 있는 경우도 흔합니다. 승인되고 문서화된 API 중에도 악용될 수 있고 문서화되지 않은 API 매개변수가 있을 수 있습니다. 따라서 남북, 동서, 아웃바운드 API를 반드시 모두 검색해야 합니다. 전사적으로 완벽한 API 가시성을 확보하는 유일한 방법은 다양한 기술 및 클라우드 플랫폼에서 기존의 API 활동 데이터를 조사하는 것입니다.

2 제품이 지속적으로 API를 발견하나요, 만약 그렇다면 프로세스가 얼마나 수동으로 이루어지나요?

API는 빠르게 진행되는 DevOps 프로세스로 인해 정기적으로 나타나고 사라집니다. 따라서 특정 시점의 API 인벤토리만으로는 충분하지 않습니다. API 보안 제품은 지속적인 검색을 통해 문서화된 새로운 API를 인벤토리화하고 분석 및 보호해야 합니다. 또한 섀도 또는 좀비 API의 향후 인스턴스도 탐지해야 합니다. 결과를 해석하고 조치를 취해야 하는 부담을 지속적으로 주는 제품은 장기적으로 지속 가능하지 않습니다. 반면, 자동화 및 머신 러닝을 API의 검색과 평가에 모두 적용하는 제품은 매일 해야 하는 업무 목록에 수작업을 추가하지 않고 비즈니스를 원활하게 운영할 수 있도록 지원합니다.

3 제품이 API 문서화 툴과 프로세스에 어떤 도움이 되나요?

문서화 접근 방식을 API 보안 플랫폼과 통합하면 많은 장점이 있기 때문에 벤더사가 이런 기능을 제공하는지 확인해야 합니다. 예를 들어, CI(Continuous Integration) 및 CD(Continuous Delivery) 프로세스의 일부로 기존 Swagger 문서를 API 보안 플랫폼에 자동으로 업로드하면 섀도 API 탐지 및 섀도 매개변수 식별의 정확도가 높아집니다(벤더사가 발견된 API 매개변수와 이미 문서화된 매개변수를 비교할 수 있는 경우). 보안 플랫폼은 문서화가 부족한 API에 대해 버튼 클릭 한 번으로 사용자 지정 Swagger 파일을 생성할 수 있어야 하며, 이는 개발자가 문서화 프로세스를 시작하고 개선하는 데 도움이 됩니다.



4 환경에 제품을 배포하는 데 얼마나 많은 시간과 노력이 필요한가요?

가장 빠르고 효과적으로 시작할 수 있는 방법은 기존 시스템에서 API 활동 데이터를 비침입적으로 수집하고 분석할 수 있는 SaaS(Security as a Service) 기반의 API 보안 제품을 사용하는 것입니다. 잘 설계된 API 보안용 SaaS 아키텍처는 몇 분 안에 환경에 통합할 수 있기 때문에 가치 실현 시간을 크게 단축하고 시스템 업데이트와 관련된 지속적인 비용과 리스크를 제거할 수 있습니다. 더욱 민첩하게 대응하려면 WAAP(Web Application and API Protection)와 API 탐지 및 응답을 모두 제공하는 벤더사를 찾아 수신 트래픽을 보호하는 솔루션과 기업 내 모든 API 트래픽을 보호하는 솔루션 간에 API 트래픽 데이터가 원활하게 흐를 수 있도록 해야 합니다.

5 리스크가 발견된 API를 식별하고 우선순위를 지정하는 데 제품이 어떤 도움이 되나요?

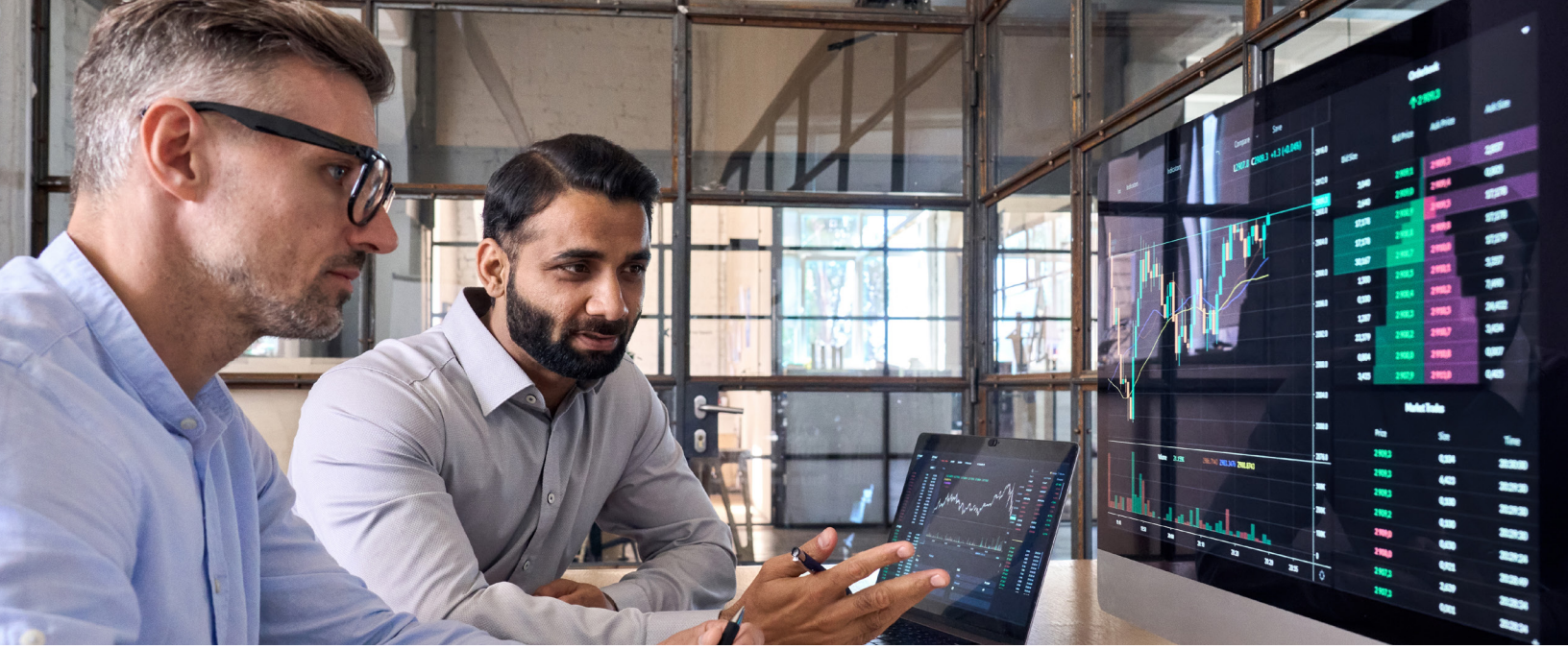
포괄적인 API 인벤토리를 처음 접하면 역량이 강화되는 동시에 부담을 느낄 수 있습니다. 많은 보안팀이 정보 과부하로 인해 어려움을 겪고 있으며, API 보안 노력을 집중해야 할 영역을 식별하는 데 어려움을 겪고 있습니다. 이를 방지하는 가장 좋은 방법은 다음과 같이 이런 작업의 대부분을 대신 수행하는 API 보안 제품을 선택하는 것입니다.

- 민감한 데이터에 접속할 수 있는 API의 존재를 강조
- 민감한 데이터를 종류별로 자동 레이블링(개인 식별 정보, 이메일 주소, 신용카드 데이터 등)

API 팀과 보안팀이 비즈니스 목표 및 보안 우려 사항에 부합하는 내용을 공유하려면 API 보안 플랫폼에서 사용자 지정 레이블링 카테고리를 생성할 수 있어야 합니다.

6 제품이 행동 애널리틱스를 사용해 예상되는 행동의 기준선을 결정하고 비정상을 찾아내나요?

공격 시그니처를 사용해 WAAP 수준에서 차단하면 많은 종류의 공격을 탐지할 수 있습니다. 그러나 손상된 오브젝트 수준 권한(BOLA)처럼 OWASP(Open Web Application Security Project) 2023 API 보안 상위 10개 목록에서 발견된 많은 종류의 공격은 이런 방식으로 발견할 수 없습니다. 이런 공격은 보다 수동적이고 비즈니스 악용에 초점을 맞추기 때문에 탐지하기가 더 어렵습니다. 모든 API 위협 기법을 효과적으로 방어하는 유일한 방법은 행동 애널리틱스와 머신 러닝을 활용하는 것입니다. 효과적인 행동 애널리틱스는 대규모 데이터 세트, 사용자 환경의 특성을 학습하는 머신 러닝 알고리즘, 글로벌 정보를 기반으로 자동으로 업데이트하고 적응할 수 있는 유연성과 민첩성을 요구합니다. SaaS 모델은 이런 활동을 대규모로 수행할 수 있는 유일하고 실용적인 방법입니다.



7 정상 행동의 기준을 효과적으로 결정하고 비정상을 탐지할 수 있을 만큼 의미 있는 데이터 세트를 캡처하고 분석할 수 있나요?

많은 API 보안 제품은 개별 API 호출 또는 기껏해야 단기 세션 활동 모니터링에 집중합니다. 그러나 수많은 정상적인 비즈니스 프로세스와 공격이 훨씬 더 긴 기간에 걸쳐 발생하기 때문에 이러한 방식으로는 충분하지 않습니다. API 사용은 일정 기간(최소 30일) 동안 분석해야 합니다. 이렇게 하면 한 달에 한 번만 발생하는 비즈니스 프로세스(인보이스 발행 등)를 포함해 예상되는 행동에 대한 보다 완전하고 정확한 기준선을 확보할 수 있습니다. 며칠 또는 몇 주에 걸쳐 느리게 실행되는 공격과 수많은 API 세션도 탐지할 수 있습니다.

8 제품이 원시 API 데이터 내의 모든 엔티티, 관계, 활동을 식별해 비즈니스 맥락을 제공할 수 있나요?

API 활동 데이터를 유용한 데이터로 만드는 가장 좋은 방법은 API 사용이 비즈니스에 미치는 영향을 고려해 이를 보강하는 것입니다. API 보안 플랫폼이 다양한 엔티티 간의 관계를 평가하고 프로파일링하려면 다음과 같은 식별 및 레이블링 기능이 필수적입니다.

- IP 주소, API 키, 접속 토큰, userID, partnerID, merchantID, supplierID 등과 같은 API 사용자(사용자 엔티티)에 대한 표현.
- 예약, 결제, 인보이스, 계정 잔액 등과 같은 비즈니스 프로세스(비즈니스 프로세스 엔티티)의 표현.

이 수준의 정밀한 분석이 API에서 생성되는 방대한 양의 데이터를 예상되는 행동에 대한 의미 있고 이해할 수 있는 기준으로 전환할 수 있는 유일한 방법입니다.

9 API의 모든 엔티티에 의한 모든 활동을 타임라인에 표시해 시간 경과에 따른 행동 변화를 보여줄 수 있나요?

거시적인 수준에서 API 활동과 위협을 이해하고 모니터링하는 것도 중요하지만, 분석의 초점을 특정 엔티티로 좁힐 수 있는 능력도 그에 못지않게 중요합니다. 예를 들어 특정 비즈니스 파트너의 비정상적인 행동이 확인된 경우, 해당 엔티티의 모든 활동을 타임라인에서 볼 수 있는 기능이 매우 중요합니다. 비즈니스 프로세스 엔티티도 마찬가지입니다. API 내의 모든 엔티티에 대한 타임라인에서 언제, 어떤 일이 발생했는지에 대한 전체 스토리를 보는 것은 정상적인 사용과 비즈니스 악용을 명확하게 구분할 수 있게 하는 강력한 시각화 기능입니다. 활동을 되감아 알림 발생 전후에 무슨 일이 일어났는지 확인할 수 있는 기능은 비즈니스 로직 남용을 이해하는 데 도움이 되는 강력한 툴입니다.

10 제품을 기존 툴, 프로세스, 워크플로우와 통합하려면 어떻게 해야 하나요?

SIEM(Security Information and Event Management) 제품에 알림을 보내는 것도 도움이 되지만, 이는 시작에 불과합니다. 보안 위협과 인시던트가 탐지되면 미리 정의된 워크플로우를 시작하기 위해 보다 정교한 SOAR(Security Orchestration, Automation, Response) 툴을 사용하는 보안팀이 증가하고 있습니다. 많은 API 보안 문제는 보안팀 외부의 개발자가 해결해야 하기 때문에 API 보안 플랫폼은 개발팀의 이슈 추적 및 워크플로우 관리 툴과 통합되어야 합니다. 보안 툴이 API 트래픽을 분석하는 경우, API를 사용해 CDN, 웹 애플리케이션 방화벽 또는 API 게이트웨이에서 응답을 조율하고 자체 플레이북을 만들 수 있도록 지원하는 것이 합리적입니다.

11 선제적인 위협 탐지와 리스크 방어를 위해 제품의 API 및 활동 데이터를 쿼리할 수 있나요?

보안 및 개발 툴의 통합은 단순히 툴에 단방향 알림을 보내는 블랙박스가 되어서는 안 됩니다. 보안 및 API 팀은 알림이나 이슈의 소스 데이터를 활용할 수 있는 기능이 필요합니다. 사용자가 빌트인 웹 인터페이스를 통해 직접 API 세부 정보를 쿼리하거나 API 보안 플랫폼을 선호하는 다른 툴 및 인터페이스와 통합할 수 있는 API를 통해 API 세부 정보를 쿼리할 수 있는 API 보안 플랫폼을 찾아야 합니다. 이를 통해 보안팀은 선제적 위협 탐지를 효율적이고 효과적으로 수행할 수 있습니다. 개발자와 기타 비보안 이해관계자는 API가 어떻게 정상적으로 사용되고, 어떻게 공격자의 표적이 되는지 이해할 수 있습니다.

12 비즈니스와 관련하여 수집하는 민감한 데이터를 보호하기 위해 어떤 조치를 취하나요?

오늘날의 위협 환경으로부터 API를 보호하는 데 필요한 고급 행동 애널리틱스는 클라우드의 규모를 통해서만 가능합니다. API 데이터 세트의 규모와 민감도를 고려하면 보안 벤더사가 데이터를 확실히 보호하도록 하는 것이 중요합니다. 벤더사가 클라우드 인프라 보안에 적용하는 관행을 확인하는 것도 중요하지만, 이는 시작에 불과합니다. API 보안 벤더사에 토큰화, 즉 민감한 데이터를 클라우드로 전송하기 전에 익명화된 토큰으로 대체하는 등의 기술을 사용하도록 요구해야 합니다. 이렇게 하면 벤더사 또는 벤더사의 업스트림 클라우드 공급업체에서 보안 인시던트가 발생하더라도 데이터 프라이버시를 유지할 수 있습니다.

13 API 활동 데이터에 대한 세분화된 접속을 제공하나요?

데이터는 컴플라이언스부터 공격 방지를 위한 맥락에 이르는 모든 부분에 있어 중요한 전략적 요소입니다. 많은 벤더사가 시간이 지남에 따라 API 데이터를 위한 자체 버전의 스토리지를 제공하지만, 실제로 무엇이 제공되는지 자세히 살펴봐야 합니다. 감염된 API 활동은 알림이 한 번만 발생했을 때뿐만 아니라 시간이 지남에 따라 서서히 발생할 수 있기 때문에, 알림만 제공하는 솔루션은 전체 스토리를 놓칠 수 있습니다. 종합적인 벤더사는 모든 API 활동을 기록해 사각지대를 제거하고, 모호한 머신 러닝 모델에서 해당 활동을 놓치지 않고 자세히 검토할 수 있는 툴을 제공합니다. 이렇게 세분화된 데이터 접속 권한을 확보하는 것이 중요한 이유는 공격 알림이 발생한 후 사후 대응하는 대신, 위협을 사전에 모니터링할 수 있기 때문입니다.

API 보안 벤더사에 확인해야 할 13가지 질문

1. API 보안 제품이 전사적으로 API 검색을 할 수 있나요?
2. 제품이 지속적으로 API를 발견하나요, 만약 그렇다면 프로세스가 얼마나 수동으로 이루어지나요?
3. 제품이 API 문서화 툴과 프로세스에 어떤 도움이 되나요?
4. 환경에 제품을 배포하는 데 얼마나 많은 시간과 노력이 필요한가요?
5. 리스크가 발견된 API를 식별하고 우선순위를 지정하는 데 제품이 어떤 도움이 되나요?
6. 제품이 행동 애널리틱스를 사용해 예상되는 행동의 기준선을 결정하고 비정상을 찾아내나요?
7. 정상 행동의 기준을 효과적으로 결정하고 비정상을 탐지할 수 있을 만큼 의미 있는 데이터 세트를 캡처하고 분석할 수 있나요?
8. 제품이 원시 API 데이터 내의 모든 엔티티, 관계, 활동을 식별해 비즈니스 맥락을 제공할 수 있나요?
9. API의 모든 엔티티에 의한 모든 활동을 타임라인에 표시해 시간 경과에 따른 행동 변화를 보여줄 수 있나요?
10. 제품을 기존 툴, 프로세스, 워크플로우와 통합하려면 어떻게 해야 하나요?
11. 선제적인 위협 탐지와 리스크 방어를 위해 제품의 API 및 활동 데이터를 쿼리할 수 있나요?
12. 비즈니스와 관련하여 수집하는 민감한 데이터를 보호하기 위해 어떤 조치를 취하나요?
13. API 활동 데이터에 대한 세분화된 접속을 제공하나요?

Akamai API Security는 이 목록에서 권장하는 보안 기능을 효과적으로 제공합니다. Akamai 솔루션 살펴보기.