Akamai

전자책

API 탐지 및 대응을 위한 10가지 핵심 기능

API 보안 전략 강화

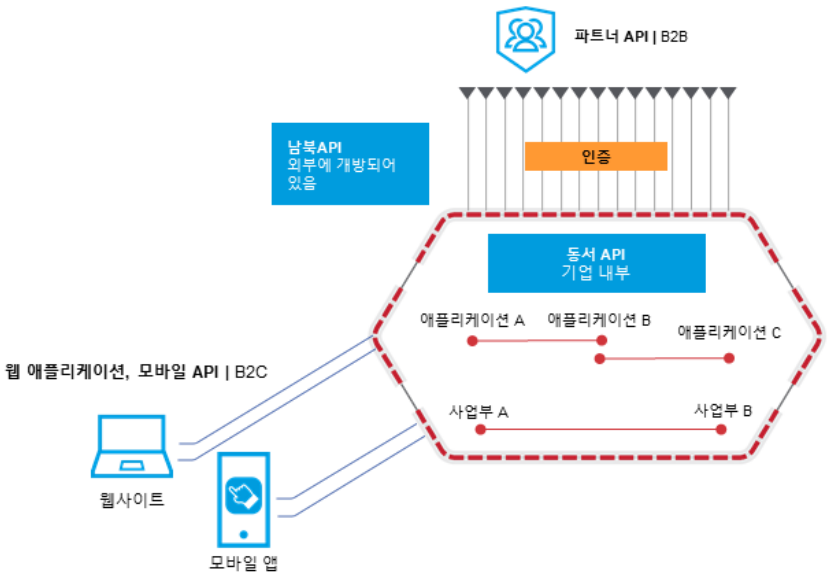
서론

API는 혁신을 주도하는 핵심 구성요소이며, 이러한 변화의 중심에는 B2B(business-to-business) 및 B2C(business-to-consumer) 애플리케이션이 있습니다. 따라서 내부적으로는 마이크로서비스 간, 외부적으로는 고객과 파트너 간의 중요하고 민감한 통신을 보호하는 것이 중요합니다. 현재 대부분의 기업은 장기적인 비즈니스 성공을 위해 올바른 애플리케이션 보안 전략이 필요하다는 점을 인식하고, 애플리케이션 보안 리스크를 줄이기 위해 WAAP(Web Application and API Protection) 플랫폼, 클라우드 보안 기능 및 제품, 보안 테스트 툴 같은 보안 기술을 활용하고 있습니다. 이제 WAAP를 우회하고 기업 내 API를 표적으로 삼는 공격이 어떻게 진화해 왔는지 이해하고, 이러한 위협에 대비해 API 보안 전략을 어떻게 조정할지 논의해야 할 때입니다.

API 탐지 및 대응은 API 보안 전략의 어떤 부분에 대응할까요?

지난 몇 년 동안 기업은 웹 애플리케이션 인터페이스보다 훨씬 더 많은 API 채널을 만들었으며, 이러한 API에는 점점 더 많은 양의 핵심 비즈니스 데이터와 비즈니스 로직이 포함되고 있습니다. API는 더 많은 사용 사례를 지원하고, 변화를 가속하고, 더 민감한 데이터를 전달하고, 더 많은 사용자에게 열려 있다는 특성으로 인해 비즈니스 운영 방식에 변화를 가져왔습니다.

여러분의 API 환경은 어떤가요?



API의 보급이 증가하고 있기 때문에 대부분의 보안 제품 카테고리가 어떤 식으로든 API를 지원하지만, API는 기존과 다른 자산 클래스이며 일부 컴플라이언스 프레임워크에서는 독특한 자산으로 간주되기도 합니다. WAAP 플랫폼 같은 레거시 보안 제품에 API 위협 방어 기능을 추가한다고 해서 API 자산으로 인해 발생하는 새로운 문제를 해결할 수 있는 것은 아닙니다. 보안 기업은 API를 별도의 자산 클래스로 취급하고 API를 대규모로 완벽하게 보호하는 데 필요한 핵심 기능을 인식해야 합니다.

새로운 위협에 대응하기 위해 API 보호가 어떻게 변화했는지에 대한 기초부터 살펴보겠습니다. 과거에는 기업이 API에 대한 전체 인벤토리와 강력한 WAAP를 보유하고 있다면 API 위협을 대체적으로 피할 수 있었습니다. 이제 공격은 WAAP를 우회하도록 설계된 방식으로 기업과 파트너 기업 내의 API를 표적으로 삼고 있습니다.

예를 들어, 일부 형태의 API 남용은 부여받은 API 인증정보를 허가되지 않은 방식으로 사용하는 고객과 파트너로부터 발생합니다. 정상적으로 보이는 API 인증정보나 보안 토큰을 탈취하는 방법도 있습니다. API 클라이언트 구축에 숨겨진 취약점은 공격자가 기존 보안 툴로는 탐지할 수 없는 방식으로 API를 남용하기 위해 악용할 수 있는 또 다른 공격 기법입니다.

다행히 기업은 이렇게 새로운 트렌드로부터 API를 보호하는 데 필요한 중요한 기능, 특히 탐지 및 대응 기능을 대규모로 이용할 수 있습니다. 다음 페이지에서는 이와 같은 플랫폼이 끊임없이 변화하는 API 위협 환경에 효과적으로 대응할 수 있도록 지원하는 핵심 기능을 자세히 살펴봅니다.

핵심 기능 #1
플랫폼 중립적 보호

API 서비스는 일반적으로 기업 내 여러 그룹에서 다양한 플랫폼과 기술을 사용해 구축하는 경우가 많습니다. 예를 들어 일부 API는 온프레미스에서 구축되는 반면, 퍼블릭 클라우드에서 실행되는 API도 있습니다. 리버스 프록시, API 게이트웨이, WAF(Web Application Firewall), CDN(Content Delivery Network) 같은 중개 기술이 사용되기도 하는데, 이는 API 가시성을 복잡하게 만들 수 있습니다.

이렇게 다양한 각 기술로부터 API 활동 데이터에 접속할 수 있는 기능이 반드시 필요합니다. 플랫폼 중립적인 API 위협 방어 접근 방식은 구축 세부 정보나 사용 중인 인프라에 관계없이 기업이 항상 모든 API 활동을 완벽하게 파악하도록 지원합니다. 이를 통해 다음과 같은 보호 범위를 제공합니다.

- 모든 부서, 인수한 회사, 환경
- 승인된 API 및 섀도 API(API 게이트웨이 사용 여부와 무관)
- 퍼블릭, 파트너, 내부 동서 API를 포함해 남북 API를 넘어 확장된 가시성

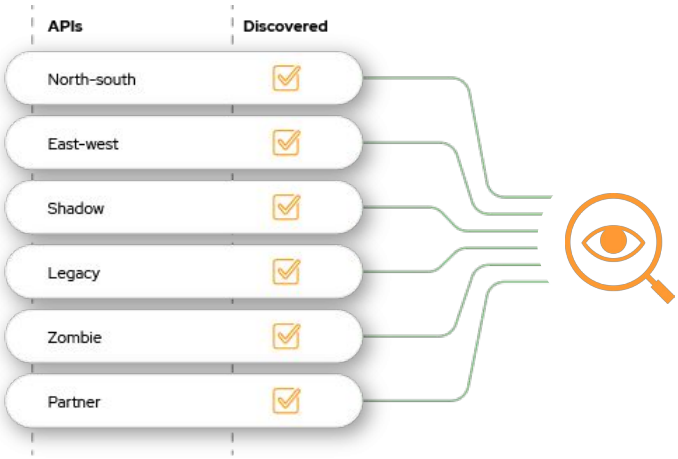
API 위협 방어 플랫폼으로 최대한 넓은 가시성을 확보하면 외부 공격자의 리스크뿐만 아니라 내부자 위협과 파트너 기업의 API 남용으로부터 기업을 보호할 수 있습니다.

핵심 기능 #2
지속적인 API 검색 및 체계 관리

기업 전체에서 사용 중인 모든 API에 대한 포괄적이고 지속적으로 업데이트되는 인벤토리는 모든 API 보안 전략의 중요한 토대입니다. 이는 기업이 자사 환경에 존재하는지 모르는 대상을 보호할 수 없기 때문입니다. 많은 API 보안 제품이 일정 수준의 API 검색을 수행한다고 주장하지만 온디맨드 또는 일상적인 작업으로 제한됩니다. 따라서 플랫폼의 API 검색 기능에 다음과 같은 기능이 포함되어 있는지 확인해야 합니다.

- 한 번만 사용되는 API의 검색을 포함해 24시간 내내 API를 자동으로 지속적으로 검색 (온디맨드 또는 일일 검색만으로는 불충분)
- 다양한 기술 및 인프라 전반의 모든 API 검색
- 새로 배포된 API를 검색하고 잘 문서화된 API와 비교해 섀도 API 탐지
- 각 API 서비스 및 엔드포인트의 리스크 점수 산정
- OWASP API ▯▯ 10▯ ▯▯ ▯▯▯에 설명된 것과 같이 알려진 API 취약점의 인스턴스 탐지

가시성 개선
API 인벤토리에 대한 가시성 유지



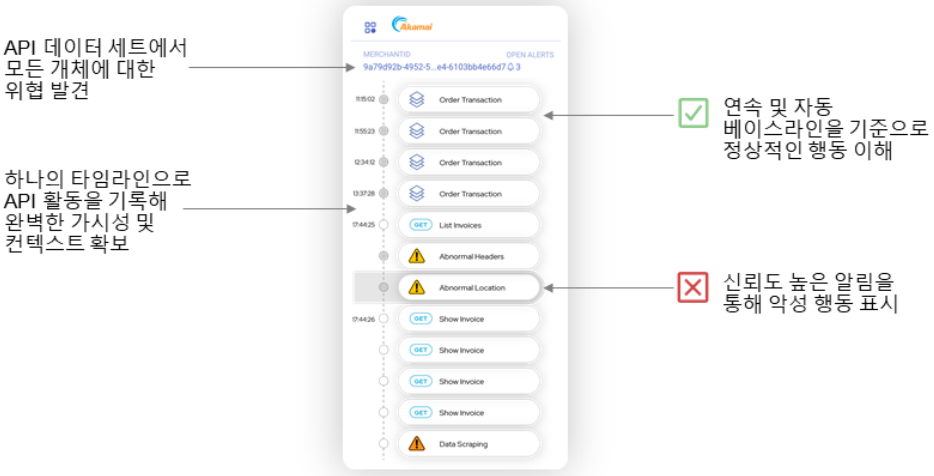
핵심 기능 #3

API 동작 시각화

실제 API 동작(API 호출)을 표시하고 시각화하는 기능은 API 보안 플랫폼의 기본 기능입니다. 이 기능은 보안, 개발, 운영 부서의 주요 이해관계자가 API가 어떻게 사용되거나 남용되는지 확인하고 파악해 팀 간에 소통하고 사례를 조사할 수 있도록 하는 데 필요합니다. 구체적으로 살펴봐야 할 시각화 기능은 다음과 같습니다.

- **조사:** 알림의 특정 트리거를 탐지할 수 있도록 모든 알림에는 호출별로 원래의 API 활동을 조사할 수 있는 기능이 포함되어야 합니다.
- **위협 탐색:** 기록 데이터는 모든 API 활동을 확인하고 특정 알림 이외의 기간 및 호출을 쿼리하는 기능을 포함해 최소한 30일의 기간으로 확장되어야 합니다. 이 기능은 컴플라이언스에도 도움이 됩니다.
- **데이터 충실도 및 보강:** 모든 API 호출에 대해 사용자가 누구인지, 어떤 작업을 사용했는지, 어떤 레코드에 접속하거나 조작했는지, 어떤 헤더와 매개 변수를 사용했는지 등을 파악할 수 있어야 합니다.
- **데이터 프라이버시:** 데이터 충실도는 중요하지만, 민감한 데이터를 유휴 상태로 저장할 수는 없습니다. 민감한 데이터를 저장하지 않으면서도 풍부한 데이터를 보존하려면 토큰화가 필요합니다.
- **타임라인 시각화:** 사용자가 활동 시퀀스를 앞뒤로 쉽게 이동할 수 있는 보기를 제공해야 합니다.

행동 애널리틱스를 활용해 위협 탐지



핵심 기능 #4

여러 사용자 엔티티 추적

엔티티를 이해하고 관련 API 활동을 볼 수 있으면 모든 사용 또는 남용에 대한 맥락이 확보되기 때문에, API 보안 플랫폼은 이러한 각 엔티티를 개별적으로 추적할 수 있는 정교한 기능을 갖춰야 합니다. 이것이 필수적인 맥락을 제공하는 이유는 한 범주의 사용자에 대한 정상적인 활동이 다른 사용자에게는 남용의 경고 신호일 수 있기 때문입니다. 타임라인에서 각 엔티티의 활동을 볼 수 있는 기능은 중요한 가시성과 맥락적 이해를 제공합니다. 예를 들면 다음과 같습니다.

API 활동	참가자	엔티티	비즈니스 프로세스 엔티티
예	내부 사용자, B2B 파트너, 외부 사용자	IP 주소, API 토큰, 판매자 ID, 세션 ID, 테넌트 ID	결제 ID, 인보이스 ID

핵심 기능 #5
B2B 및 동서 API 범위

API 사용의 가장 큰 성장 영역은 내부와 외부를 대상으로 하는 B2B 사용 사례입니다. API 보안은 남북(외부 대상) 및 동서(내부 대상) 인스턴스를 모두 포함한 B2B, 머신 대 머신 API를 지원해야 합니다.

B2C 웹 애플리케이션은 WAAP 및 WAF 플랫폼의 보호를 받지만, 내부 동서 API 또는 B2B API를 통해 파트너에게 노출되는 독점 애플리케이션 기능과 같이 가장 민감한 종류의 API 활동은 WAAP를 통과하는 경우에도 여전히 감염될 수 있습니다.

B2B 파트너 API에서 사용자가 인증을 받으면 안전한 것으로 간주해 추가 모니터링을 수행하지 않는 경우가 많습니다. 이로 인해 많은 기업의 API 보안 체계에 심각한 공백이 발생합니다. API 활동과 광범위한 위협 환경을 전체적으로 파악하려면 모든 사용 사례에 대해 효과적인 가시성, 관찰 가능성, 모니터링을 제공하는 접근 방식을 취해야 합니다.

핵심 기능 #6
행동 애널리틱스 및 탐지

개별 API 호출 또는 개별 세션을 분석하는 것만으로는 정교한 API 위협을 탐지할 수 없습니다. API 탐지 및 대응을 위해서는 행동 맥락에 대한 심층적인 이해와 학습이 필요합니다. API의 행동이 비정상적인지, 즉 감염당했을 가능성이 있는지 알기 위해서는 장기간에 걸친 API 사용량을 분석해야 합니다. 행동 애널리틱스 기술은 기준이 되는 정상적인 사용자 행동을 결정하고 해당 행동을 지속적으로 모니터링해 비정상을 탐지합니다.

일반적인 기업의 API 활동에 대해 이러한 수준의 분석을 수행하려면 상당한 스토리지 및 컴퓨팅 리소스가 필요하기 때문에, 규모에 제약이 있는 온프레미스 API 보안 툴을 사용하는 것은 비현실적입니다. EDR 및 XDR 솔루션은 의미 있는 행동 애널리틱스를 수행하려면 SaaS(Software as a Service) 기반 아키텍처가 필요하다는 것을 보여줌으로써 시장을 선도했습니다. 클라우드의 강력한 성능과 규모를 활용하면 데이터를 장기간 저장할 수 있으며, 시간이 지남에 따라 정상적인 사용자 행동을 파악하는 분석을 통해 발견하기 어려운 악용 사례를 탐지할 수 있습니다. SaaS 접근 방식은 더 빠르고 간편한 구축, API 사용량 증가에 따른 확장성 및 탄력성 향상과 같은 추가적인 이점도 있습니다.

핵심 기능 #7
맥락이 포함된 의미 있는 알림

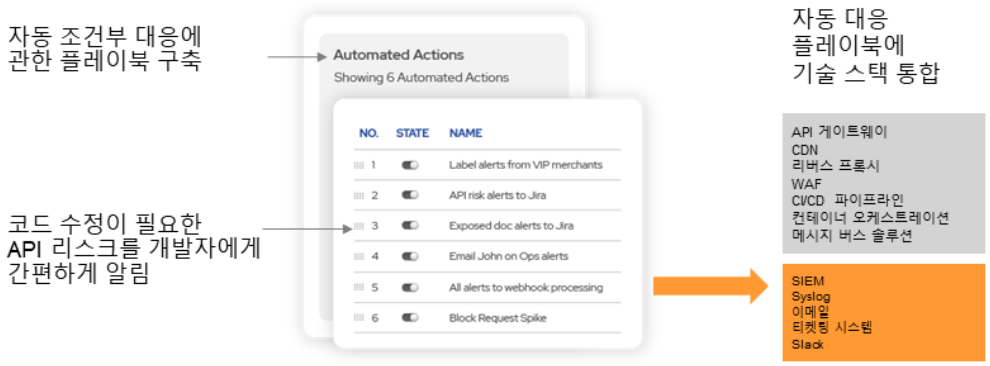
기업이 모든 API 활동과 행동 애널리틱스에 대해 대규모로 가시성을 확보하면 API 활동에 대한 알림이 훨씬 더 많은 의미를 가지게 됩니다. 이후 보안 모니터링 접근 방식을 더욱 추상화함으로써 가능한 모든 공격 방법을 예측할 필요성을 없앨 수 있습니다. 정상 동작을 기준으로 삼고 비정상을 탐지하면 어떤 패턴이나 시그니처로도 탐지할 수 없는 API 남용을 탐지할 수 있습니다. 또한 공격을 되돌리고 알림이 발생하기 전에 무슨 일이 일어났는지 확인할 수 있으면 API 자산의 사용과 남용에 대한 귀중한 인사이트를 얻을 수 있습니다.

핵심 기능 #8
맞춤형 자동 대응

기존의 인라인 API 접근 방식은 자동화된 조치를 취해 의심스러운 API 공격을 차단할 수 있지만, 기업이 공격을 탐지할 수 있어야 한다는 단점이 있습니다. API에 대한 행동 애널리틱스와 비정상 탐지는 시간이 지남에 따라 훨씬 더 많은 비즈니스 맥락에서 수행되기 때문에 심층적인 탐지를 통해 비정상이 드러날 수 있습니다. 이를 통해 광범위한 자동화된 맞춤형 대응의 정확도를 높일 수 있습니다. 예를 들면 다음과 같습니다.

- 지원되는 API 게이트웨이 및 CDN 엣지 필터에서 트래픽 차단 또는 스로틀링
- 보안 및 비즈니스 이해관계자를 위한 이메일 알림
- 개발자를 위한 티켓 생성
- 웹훅 트리거

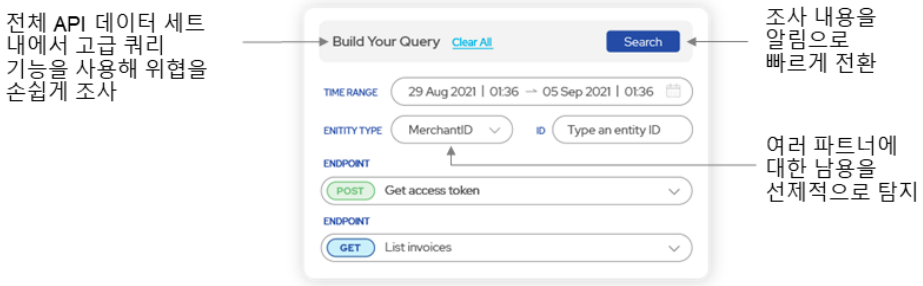
비즈니스 프로세스에 맞춰 대응 설정 가능



핵심 기능 #9
선제적 조사 및 위협 탐색

대부분의 기업은 보안 인시던트가 발생할 때까지 기다렸다가 조치를 취할 여유가 없습니다. 보다 효과적인 접근 방식은 원치 않는 상황을 탐지하고 이를 적극적으로 탐색하는 것입니다. 예를 들어, 한 API에서 악용을 탐지한 알림이 선제적 위협 탐색을 통해 다른 API에서 동일한 동작을 수행하는 것을 탐지할 수 있습니다. 따라서 API 위협 방어 플랫폼에는 활성 인시던트에 대응해 생성된 알림 외에 특정 종류의 행동을 검색할 수 있는 기능이 포함되어야 합니다. 위협 탐색 기능을 사용하려면 API 활동 데이터에 숨어 있는 악용 사례를 찾기 위해 과거 데이터에 접속할 수 있어야 합니다. 데이터를 보강해 맥락을 제공하지 않는 단일 요청 솔루션은 일관된 스토리를 구성할 수 없습니다. 위협 탐색과 조사는 기존의 기록 데이터를 토대로 구축됩니다.

간편한 위협 탐지 및 조사 역량



핵심 기능 #10
관찰 가능한 데이터 레이크

강력한 API 보안 전략을 위한 모든 기능 중에서도 '맥락'은 장기간에 걸쳐 모든 API를 보호하는 데 핵심적인 역할을 합니다. 위협을 관찰하고, 잠재적 취약점을 탐지하고, 공격 발생 시 문제를 해결하기 위해 충분한 맥락을 유지하는 가장 좋은 방법은 모든 API 동작을 기록하고 이 활동의 백로그를 보관하는 것입니다. 이는 API 보안 솔루션과 연결된 데이터 레이크를 통해 달성할 수 있습니다. 전략 수립에 도움이 되는 가장 많은 양의 과거 세부 정보를 제공하는 데이터 레이크를 찾아야 합니다. 기본적인 요청 데이터를 머신 러닝 모델에 제공하는 것도 도움이 될 수 있지만, 요청 매개 변수 같은 세부 정보가 있으면 기업이 기록 데이터를 바탕으로 향후 위협과 공격을 방어하기 위한 실질적인 조치를 취할 수 있습니다.

#1 플랫폼 중립적 보호	API 위협 방어 플랫폼의 가시성을 최대한 넓게 확보하면 위협과 악용으로부터 기업을 보호할 수 있습니다.
#2 지속적인 API 검색 및 체계 관리	기업 전체에서 사용 중인 모든 API에 대해 포괄적이고 지속적으로 업데이트되는 인벤토리를 유지하는 것이 매우 중요합니다. 환경에 존재하는지 모르는 경우 이를 보호할 수 없기 때문입니다.
#3 API 행동 시각화	보안, 개발, 운영의 주요 이해관계자가 API가 어떻게 사용되거나 남용되는지 확인하고 이해하며 팀 간에 소통하고 사례를 조사할 수 있도록 하려면 가시성이 필요합니다.
#4 여러 사용자 엔티티 추적	엔티티를 이해하고 관련 API 활동을 볼 수 있으면 모든 사용 또는 남용에 대한 맥락이 확보되기 때문에, API 보안 플랫폼은 각 엔티티를 개별적으로 추적할 수 있는 정교한 기능을 갖춰야 합니다.
#5 B2B 및 동서 API 범위	API 활동과 광범위한 위협 환경을 전체적으로 파악하려면 모든 사용 사례에 대해 효과적인 가시성, 관찰 가능성, 모니터링을 제공하는 접근 방식을 취해야 합니다.
#6 행동 애널리틱스 및 탐지	API의 행동이 비정상적인지, 즉 감염당했을 가능성이 있는지 알기 위해서는 장기간에 걸친 API 사용량을 분석해야 합니다. 행동 애널리틱스 기술은 기준이 되는 정상적인 사용자 행동을 결정하고 해당 행동을 지속적으로 모니터링해 비정상을 탐지합니다.
# 7 맥락이 포함된 의미 있는 알림	기업이 모든 API 활동과 행동 애널리틱스에 대해 대규모로 가시성을 확보하면 API 활동에 대한 알림이 훨씬 더 많은 의미를 가지게 됩니다. 이후 보안 모니터링 접근 방식을 더욱 추상화함으로써 가능한 모든 공격 방법을 예측할 필요성을 없앨 수 있습니다.

#8 맞춤형 자동 대응	API에 대한 행동 애널리틱스와 비정상 탐지는 시간이 지남에 따라 훨씬 더 많은 비즈니스 맥락에서 수행되기 때문에 심층적인 탐지를 통해 비정상이 드러날 수 있습니다. 이를 통해 광범위한 자동화된 맞춤형 대응의 정확도를 높일 수 있습니다.
#9 선제적인 조사 및 위협 탐색	대부분의 기업은 보안 인시던트가 발생할 때까지 기다렸다가 조치를 취할 여유가 없습니다. 보다 효과적인 접근 방식은 원치 않는 상황을 탐지하고 이를 적극적으로 탐색하는 것입니다.
#10 관찰 가능한 데이터 레이크	위협을 관찰하고, 잠재적 취약점을 탐지하고, 공격 발생 시 문제를 해결하기 위해 충분한 맥락을 유지하는 가장 좋은 방법은 모든 API 동작을 기록하고 이 활동의 백로그를 보관하는 것입니다. 이는 API 보안 플랫폼과 연결된 데이터 레이크를 통해 달성할 수 있습니다.

이 내용이 도움이 되었다면 가장 강력한 API 보안 전략을 수립할 수 있도록 지원하는 Akamai의 API Security 솔루션을 확인해보세요.