Akamai API Security로 비정상 탐지

API는 고객에게 서비스를 제공하고 매출을 창출하며 효율적으로 운영할 수 있게 하는 기업의 핵심 구성요소입니다. 그러나 지속적인 성장, 민감한 데이터에 대한 근접성, 보안 제어의 부재로 인해 API는 오늘날 공격자들에게 매력적인 표적이 되고 있습니다. 사용자 행동에 대한 실시간 인사이트를 확보하는 것은 잠재적인 API 남용 또는 공격의 징후를 사전에 파악하는 데 핵심적인 요소입니다.

Akamai API Security 솔루션의 비정상 탐지 기능의 목표는 기업의 API를 악용하려는 잠재적인 악의적 시도를 나타내는 비정상적인 사용자 행동을 식별하는 것입니다. Akamai의 비정상 탐지 기능은 정상 트래픽의 기준을 설정해 들어오는 요청을 기준과 비교하고 공격자가 수행할 가능성이 있는지 판단할 수 있습니다.

Akamai의 비정상 탐지 알고리즘은 다음과 같은 비정상적인 행동을 식별합니다.

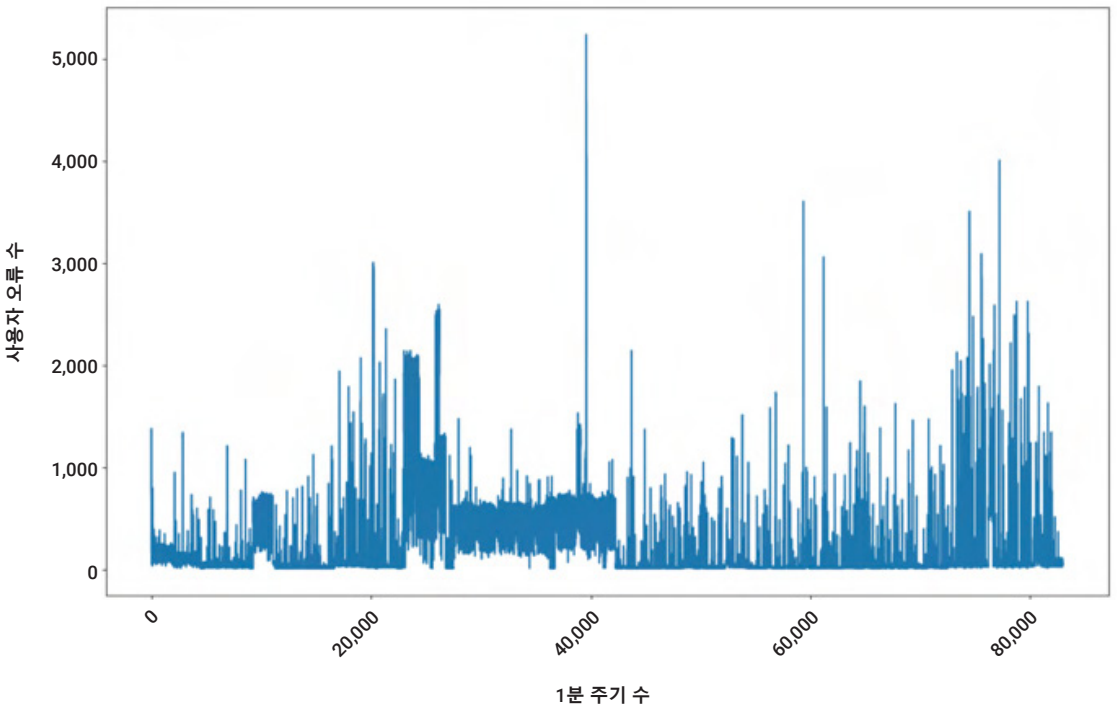
- API 요청에서 예상치 못한 필드 사용
- 일반 사용자보다 더 많은 데이터를 서버에서 가져옴
- 다른 사용자/관리자 리소스 사용 시도
- 예상치 못한 순서로 API 호출

이 알고리즘은 통계적 트래픽 행동의 여러 특징을 학습하고 고정된 학습 기간 후에 비정상적인 인시던트를 탐지하는 무감독 온라인 인공 지능 및 머신 러닝(AI/ML) 모델을 기반으로 합니다. Akamai의 모델은 시간이 지남에 따라 트래픽의 변화에 적응할 수 있으며, 사용자가 오탐이라고 표시한 비정상에 적응할 수 있습니다.

학습 단계에서 Akamai의 시스템은 고객의 데이터를 분석하고 다양한 API, 인증 방법, 사용자, 데이터 유형 등을 파악합니다. Akamai의 모델은 각 API에 대해 API 히트 수, 생성된 오류 수, 인증된 요청의 비율, 서버에서 검색된 데이터의 양 등을 포함해 일반 사용자 트래픽의 특징 목록을 개발합니다. Akamai의 알고리즘은 사용자 및 API의 특성을 자체 학습한 통계 모델이 예상하는 결과와 비교함으로써 사용자 비정상을 탐지합니다.

Akamai API Security의 비정상 탐지 작동 방식

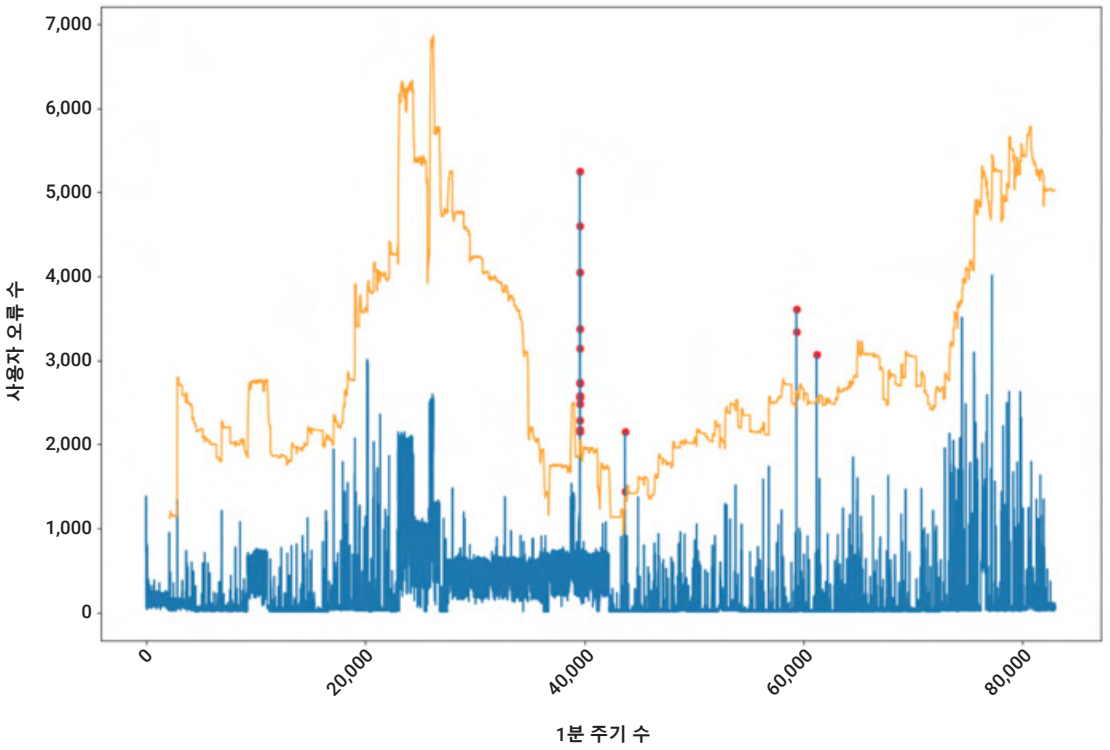
Akamai API Security의 비정상 탐지 기능은 다른 사용자보다 과도하게 많은 오류를 생성하는 사용자를 식별합니다. 이를 통해 무차별 대입, 경로 스캐닝, 스크레이핑과 같은 공격을 식별할 수 있습니다. 다음 그래프에서는 환경에서 사용자가 1분 주기로 생성하는 오류의 최대 양을 확인할 수 있습니다.



이 시나리오에서 비정상을 식별하는 데 여러 가지 어려움이 있습니다.

1. 모델은 임곗값을 계산할 때 데이터 드리프트를 고려해야 합니다.
2. 모델의 학습 기간 동안 비정상을 학습하지 않도록 해야 합니다.
3. 학습은 스트림으로 진행되므로 모델은 전체 데이터를 볼 수 없으며 매번 조정해야 합니다.
4. 알림은 실시간이어야 하므로 알고리즘은 미래의 데이터를 바탕으로 비정상을 예측할 수 없습니다.
5. Akamai의 모델은 사용자에게 스팸을 보내지 않기 위해 데이터에 대한 통계적으로 보장된 임곗값을 학습해야 합니다.

아래의 그래프에서 Akamai의 모델은 들어오는 데이터에 따라 임곗값을 조정함으로써 이러한 요구사항을 어떻게 충족하는지 확인할 수 있습니다.



주황색 선은 모델에 의해 계산된 임곗값 함수를 나타내고, 빨간색 점은 그 함수를 바탕으로 탐지된 비정상을 나타냅니다.

FAQ

Akamai의 비정상 탐지 알고리즘을 학습하는 데 필요한 기간은 얼마인가요?

대부분의 알고리즘은 2~7일의 학습 기간이 필요합니다. 또한, 학습 기간 동안 관찰된 사용자 행동의 수에 따라 알고리즘의 학습 기간이 달라집니다.

비정상적인 행동이 탐지되면 알림이 생성되기까지 얼마나 걸리나요?

Akamai의 알고리즘은 대부분의 경우 비정상적인 트래픽을 수신한 순간부터 30~60초 이내에 클라이언트에 대한 관련 알림을 생성합니다.

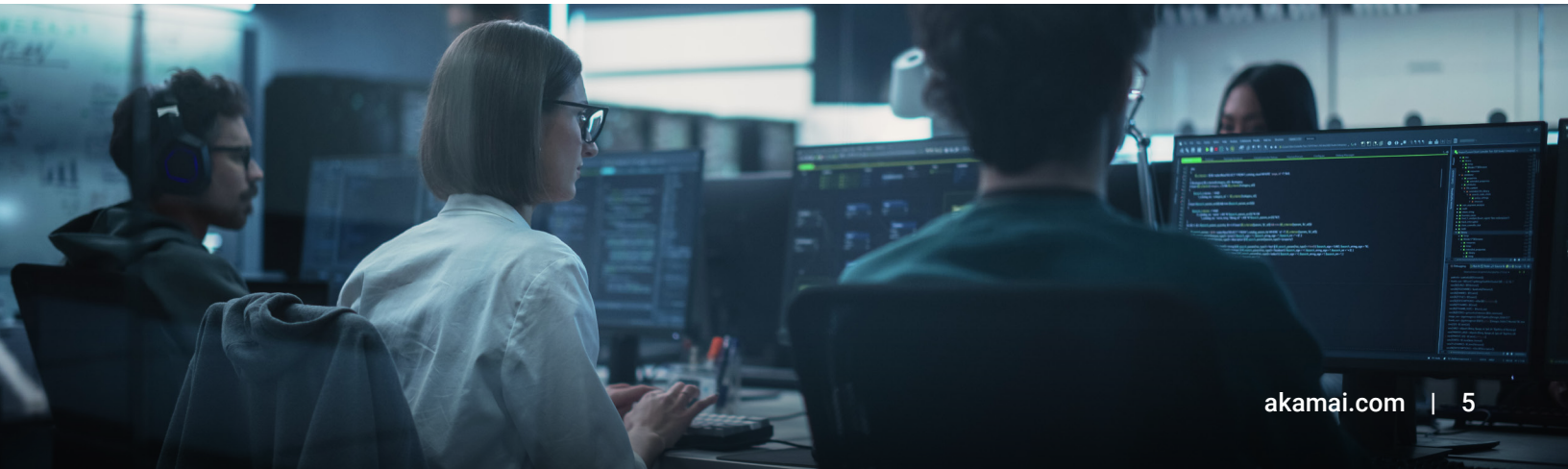
알고리즘이 감독 모델 또는 무감독 모델을 사용하나요?

Akamai의 알고리즘은 무감독 모델을 기반으로 하며, 각 고객의 환경에 대한 사전 지식 없이도 고객의 환경에 적응할 수 있습니다. 또한, Akamai의 알고리즘은 온라인 학습을 통해 시간이 지남에 따라 환경의 변화에 적응합니다.

Akamai API Security가 탐지하는 비정상에는 어떤 것들이 있나요?

Akamai API Security는 2가지의 비정상을 탐지합니다.

- 패턴 기반 - 웹 악용 기법, 명령어 인젝션, 경로 탐색, 의심스러운 사용자 에이전트 등 알려진 악성 사용자 에이전트와 같은 트래픽에서 악성 패턴을 식별하는 데 기반한 비정상.
- 행동 기반 - 사용자의 학습 행동에 기반을 두고, 과도한 API 사용, 범위 위반, 손상된 오브젝트 수준의 권한 확인 같은 비정상적인 사용자를 식별하는 비정상.



Akamai API Security는 비정상을 트리거할 때 어떤 변수를 고려하나요?

Akamai의 알고리즘은 다음과 같은 트래픽의 통계 분석을 통해 설계된 여러 가지 기능을 기반으로 합니다.

- API를 사용하는 다양한 사용자 수
- API의 인증 상태
- 서버의 응답 코드
- 사용자가 가져오는 데이터의 양
- 사용자의 IP 위치 정보
- 사용자의 사용자 에이전트, 기타

사용자가 알고리즘의 민감도를 제어할 수 있나요?

네, 사용자는 관련 정책 민감도를 수정해 각 비정상의 민감도를 제어할 수 있습니다. 정책 민감도는 1(낮음)에서 5(높음) 사이의 숫자로 설정되며 가장 높은 값을 선택하면 Akamai API Security는 각 비정상 정책에 대해 가장 민감하게 대응합니다. Akamai의 알고리즘은 해당 매개변수를 모델의 일부로 고려합니다.

사용자가 Akamai가 알림을 보낸 문제를 오탐으로 표시할 수 있나요? 그렇다면 알고리즘에 어떤 영향을 미치게 되나요?

Akamai는 비정상 탐지 기능을 개선하기 위해 사용자가 관련 문제를 '오탐'으로 표시할 수 있도록 하고 있습니다. 문제가 오탐으로 표시되면, Akamai의 알고리즘은 이 점을 고려해 사용자의 입력에 따라 모델을 조정합니다.

Akamai는 사용자가 동일한 공격 시나리오를 계속 보내는 클라이언트 '스팸'을 어떻게 방지하나요?

Akamai의 알고리즘은 동일한 사용자 및 API에서 계속 트리거되는 유사한 문제를 식별합니다. 이 경우, Akamai의 알고리즘은 일정 기간 동안 유사한 문제를 무시합니다.

Akamai는 데이터의 드리프트/계절성을 어떻게 처리하나요?

Akamai API Security는 데이터의 비정상을 탐지하기 위해 여러 가지 다른 알고리즘을 사용합니다. Akamai는 기본 데이터 전처리 및 알고리즘 복잡성에 따라 임곗값 조정을 방어하거나 비정상 탐지를 위해 통계적 임곗값 보장이 필요한 경우 주기마다 조정을 시행할 수 있습니다. 스팸 제어와 함께, 특정 알고리즘이 임곗값 조정을 위해 추가 주기를 필요로 하는 경우에도 번거로움 없는 인터페이스를 제공합니다.

Akamai는 데이터 오염을 어떻게 처리하나요?

온라인 학습 알고리즘인 Akamai API Security는 다음과 같은 다양한 문제를 해결해야 합니다.

- 새로운 API
- 기존 API의 새로운 필드
- 필드의 값 종류/범위의 변경
- 서버 가용성 문제
- 오류(404, 500 등)를 유발할 수 있는 API의 버그와 학습 대상과 비학습 대상을 결정하는 데 따르는 기타 문제(Akamai는 학습을 트리거하기 위해 최소 사용자 수, 기간, 지속성의 조합을 요구함으로써 이러한 비정상을 학습하지 않도록 예방 조치를 취합니다)

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

Akamai Security는 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/blog를 확인하거나 X(기존의 Twitter), LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 12월 발행.