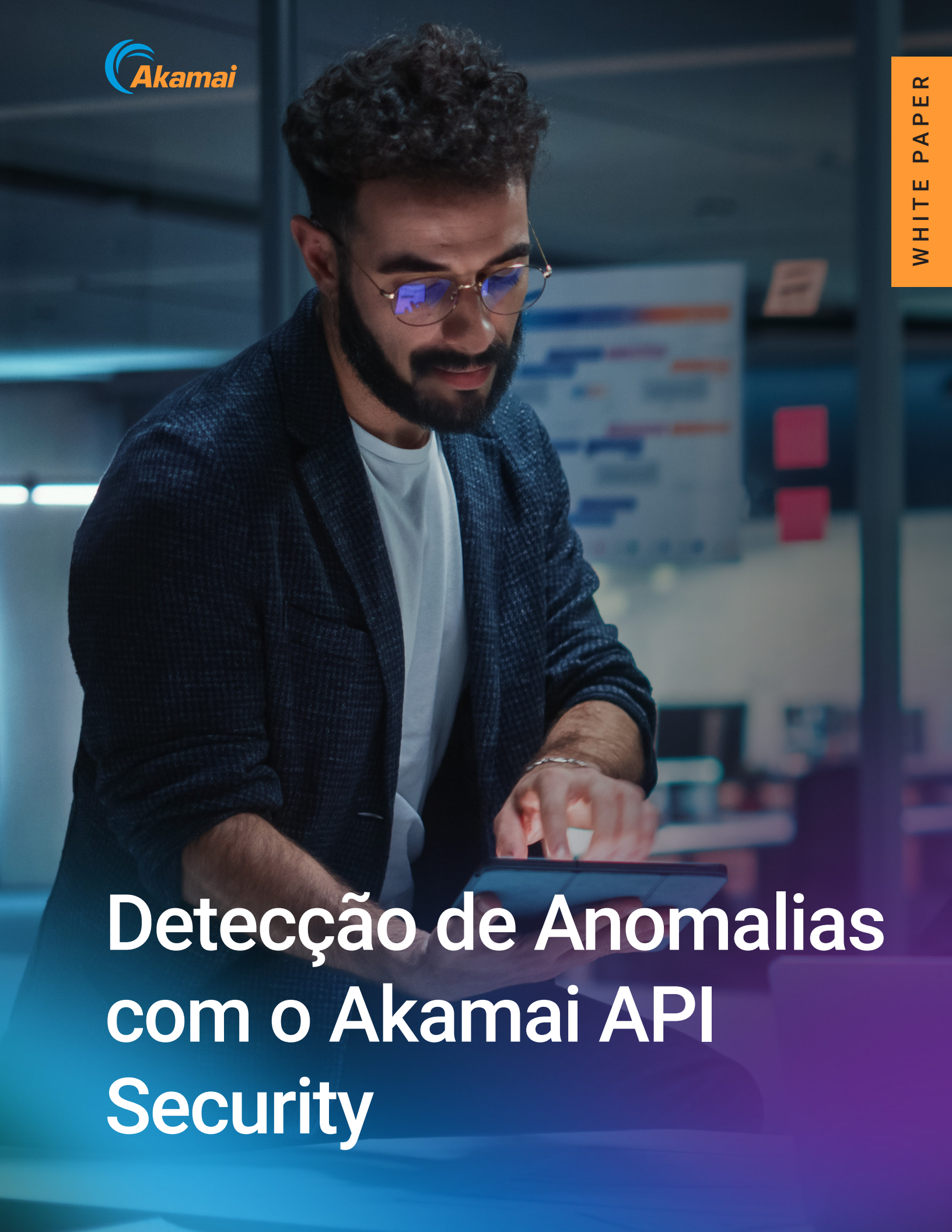


WHITE PAPER

Detecção de Anomalias com o Akamai API Security

As APIs são um componente fundamental para que sua organização possa atender clientes, gerar receita e operar de forma eficiente. No entanto, seu crescimento contínuo, a proximidade com dados confidenciais e a falta de controles de segurança tornam as APIs um alvo atraente para os invasores modernos. Obter insights em tempo real sobre o comportamento dos usuários é fundamental para identificar de forma proativa sinais de possíveis violações ou ataques contra APIs.

O objetivo dos recursos de detecção de anomalias da solução Akamai API Security é identificar comportamentos incomuns de usuários que possam indicar tentativas maliciosas de explorar as APIs da organização. Ao estabelecer um padrão de tráfego normal, os recursos de detecção de anomalias da Akamai comparam solicitações recebidas com essa base de referência para determinar se é provável que a ação seja conduzida por um agente malicioso.

Nosso algoritmo de detecção de anomalias identifica comportamentos incomuns, como:

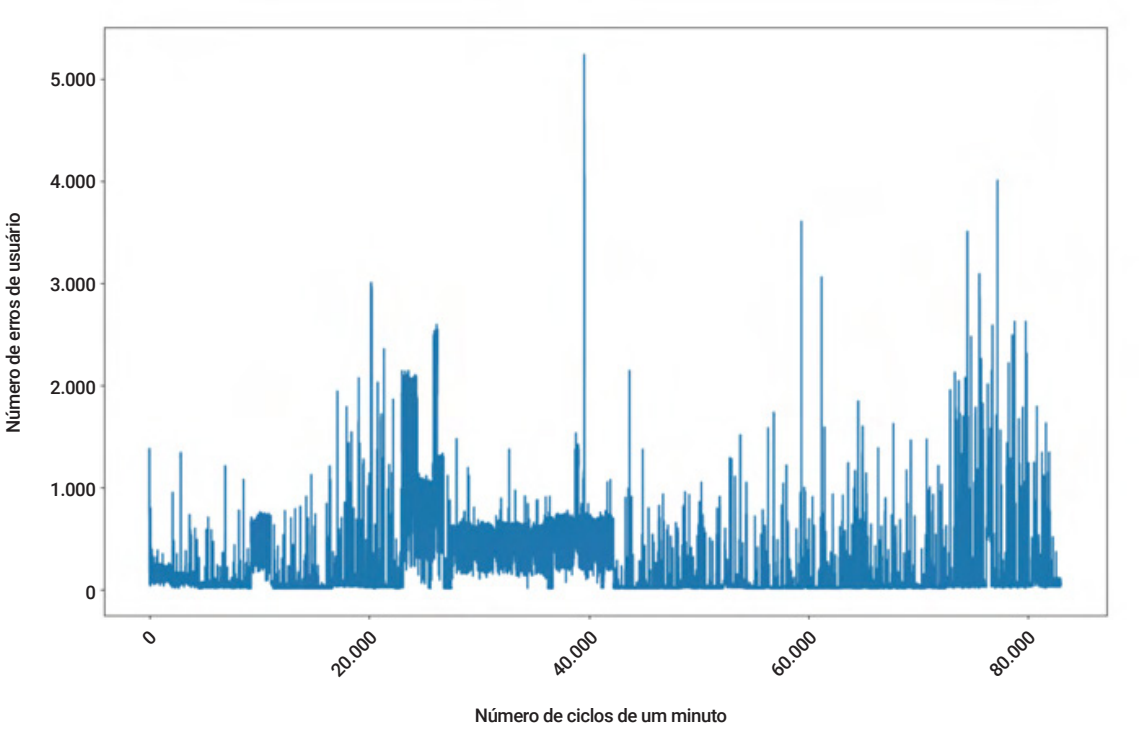
- Uso de um campo inesperado na solicitação à API
- Extração de mais dados do servidor do que um usuário típico
- Tentativa de acessar outros recursos de usuário/admin
- Chamada às APIs em uma sequência inesperada

Baseado em um modelo de inteligência artificial e aprendizado de máquina (IA/ML) com aprendizado online não supervisionado, o algoritmo aprende as diversas caraterísticas do comportamento estatístico do tráfego e detecta incidentes anômalos após um período de aprendizado fixo. Nosso modelo se adapta às mudanças no tráfego ao longo do tempo e às anomalias identificadas como falsos positivos pelos usuários.

Durante a fase de aprendizado, o sistema analisa os dados do cliente e identifica diferentes APIs, métodos de autenticação, usuários, tipos de dados, entre outros. Para cada API, o modelo desenvolve uma lista de características do tráfego regular de usuários, incluindo o número de acessos à API, o número de erros gerados, a porcentagem de solicitações autenticadas, a quantidade de dados recuperados do servidor e outros aspectos. Nosso algoritmo detecta anomalias no comportamento do usuário comparando as características do usuário e da API aos resultados esperados pelo modelo estatístico aprendido.

Como funciona a detecção de anomalias do Akamai API Security

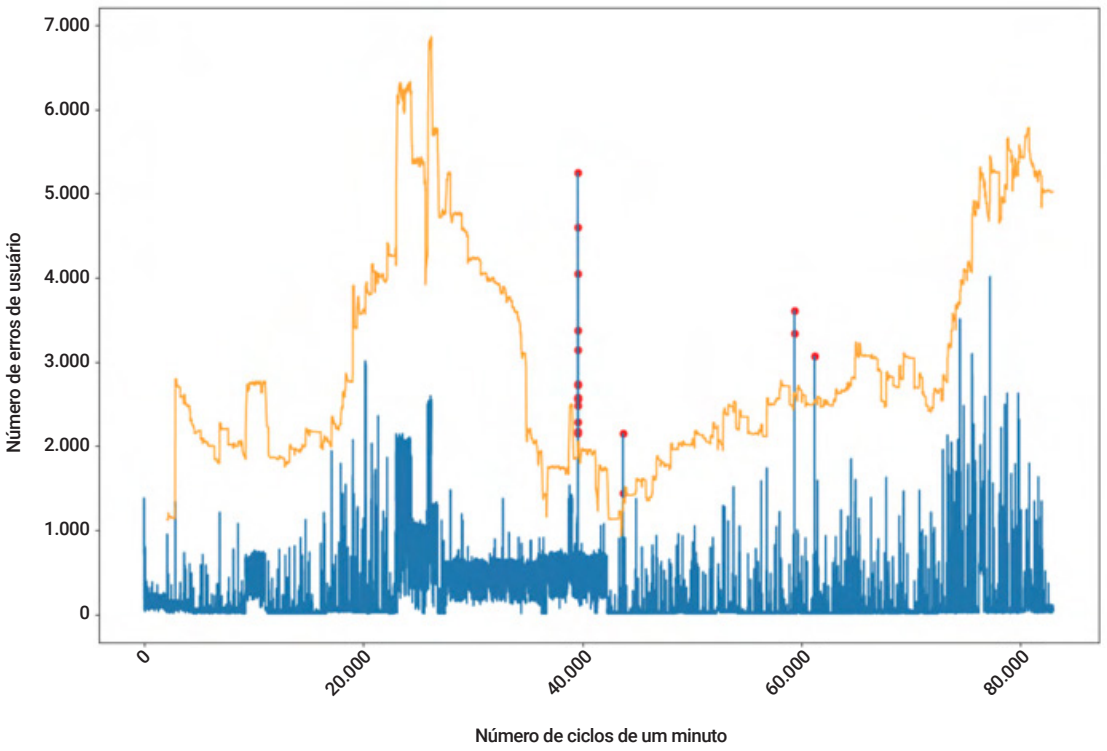
Os recursos de detecção de anomalias do Akamai API Security identificam usuários que geram um número de erros excessivamente maior do que outros usuários. Isso permite a identificação de ataques dos tipos força bruta, varredura de caminho e scraping. O gráfico a seguir mostra a quantidade máxima de erros gerados por um usuário a cada ciclo de um minuto em um ambiente.



Existem diversos desafios para identificar anomalias nesse cenário:

1. O modelo precisa levar em consideração a variação de dados ao calcular o limite.
2. Evitar que anomalias sejam aprendidas durante o período de aprendizado do modelo.
3. O aprendizado é realizado em fluxo/em sequência, o que significa que o modelo nunca vê todos os dados de uma vez e precisa se ajustar a cada etapa.
4. Os alertas precisam ser em tempo real, ou seja, nosso algoritmo não pode se basear em dados futuros para prever uma anomalia.
5. Para evitar o envio excessivo de alertas ao usuário, o modelo precisa aprender um limite estatisticamente garantido para os dados.

No gráfico abaixo, podemos ver como nosso modelo atende a esses requisitos ajustando os limites de acordo com os dados recebidos.



A linha laranja mostra a função de limite calculada pelo modelo, e os pontos vermelhos indicam as anomalias detectadas com base nessa função.

Perguntas frequentes

Qual é o período de aprendizado necessário para o algoritmo de detecção de anomalias da Akamai?

A maioria dos nossos algoritmos exige um período de aprendizado de dois a sete dias. Além disso, o período de aprendizado do algoritmo também é afetado pela quantidade de diferentes comportamentos de usuários observados durante esse período.

Quando um comportamento anômalo é detectado, quanto tempo leva para o alerta ser gerado?

Nosso algoritmo cria um alerta relevante para o cliente em 30 a 60 segundos, na maioria dos casos, a partir do momento em que recebe o tráfego anômalo.

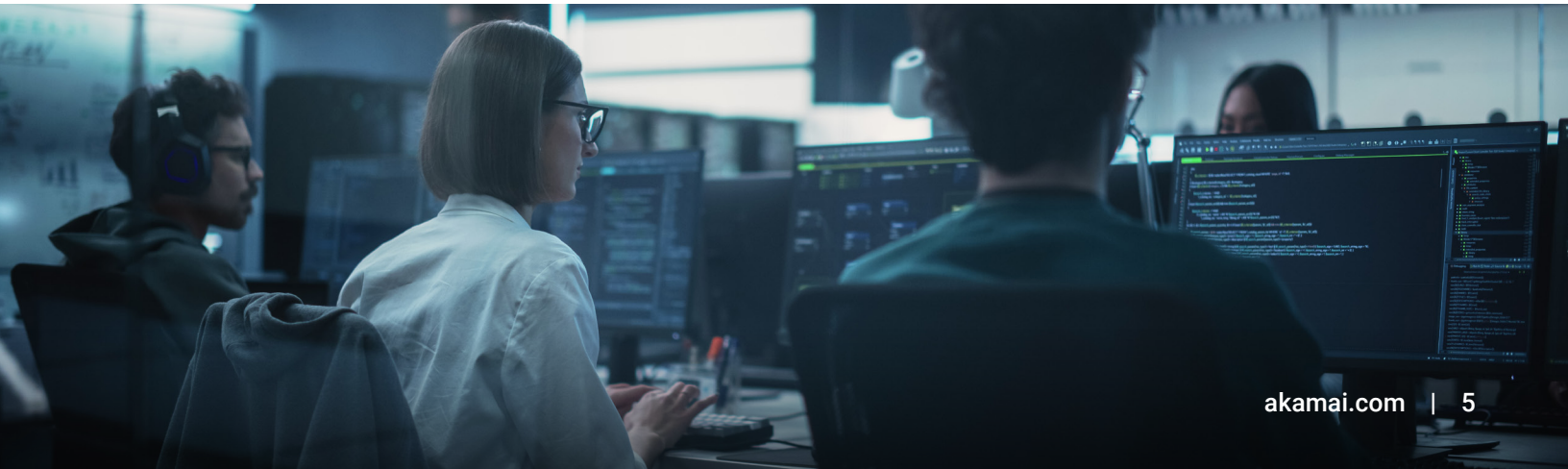
O algoritmo usa um modelo supervisionado ou não supervisionado?

Nosso algoritmo é baseado em um modelo não supervisionado, o que permite que ele se adapte ao ambiente de cada cliente sem ter conhecimento prévio sobre suas características. Além disso, nosso algoritmo usa aprendizado online para se ajustar às mudanças do ambiente ao longo do tempo.

Quais são os diferentes tipos de anomalias detectadas pelo Akamai API Security?

O Akamai API Security detecta dois tipos de anomalias:

- Baseadas em padrão — anomalias que identificam padrões maliciosos no tráfego, como técnicas de exploração na Web e agentes de usuário maliciosos conhecidos, como injeção de comandos, travessia de caminho e agentes de usuário suspeitos.
- Baseadas em comportamento — anomalias baseadas no aprendizado do comportamento dos usuários e na identificação de usuários anômalos, como nos casos de uso excessivo de APIs, violação de intervalo e autorização em nível de objeto corrompida (BOLA).



Quais parâmetros o Akamai API Security considera ao indicar uma anomalia?

Nossos algoritmos são baseados em várias características a partir da análise estatística do tráfego, como:

- Número de usuários diferentes que utilizam uma API
- Status de autenticação da API
- Código de resposta do servidor
- Quantidade de dados extraídos pelo usuário
- Geolocalização do IP do usuário
- Agente de usuário do usuário etc.

O usuário pode controlar a sensibilidade do algoritmo?

Sim, o usuário pode controlar a sensibilidade de cada anomalia modificando a sensibilidade da política relevante. A sensibilidade da política é um número entre 1 (baixa) e 5 (alta); o valor mais alto torna o sistema o mais sensível possível para cada política de anomalia no Akamai API Security. Nosso algoritmo leva esse parâmetro em consideração como parte do modelo.

O usuário pode marcar um alerta gerado pela Akamai como falso positivo? Como isso afeta o algoritmo?

Sim, para melhorar nossa detecção de anomalias, os usuários podem marcar problemas relevantes como "falsos positivos". Quando um problema é marcado como falso positivo, nosso algoritmo leva isso em consideração e ajusta o modelo de acordo com a informação fornecida pela usuário.

Como a Akamai evita criar spam para o cliente com excesso de alertas quando um usuário que continua gerando o mesmo cenário de ataque?

Nosso algoritmo identificará problemas semelhantes que continuam sendo acionados pelo mesmo usuário e API. Nesse caso, nosso algoritmo ignorará problemas semelhantes por um período constante.

Como a Akamai lida com a variação/sazonalidade dos dados?

O Akamai API Security utiliza diversos algoritmos para detectar anomalias nos dados. Dependendo do pré-processamento dos dados e da complexidade do algoritmo, podemos flexibilizar o ajuste do limite ou aplicar ajustes a cada ciclo onde sejam necessários limites estatísticos garantidos para a detecção de anomalias. Junto com o controle de spam, proporcionamos uma interface simplificada, mesmo quando um algoritmo específico exige ciclos adicionais para ajustar os limites.

Como a Akamai lida com "envenenamento de dados"?

Já que é baseado em um algoritmo de aprendizado online, o Akamai API Security enfrenta diversos desafios, como:

- Novas APIs
- Novos campos em APIs existentes
- Alteração do tipo/intervalo de valores em um campo
- Problemas de disponibilidade do servidor
- Bugs em APIs que possam causar falhas (404, 500 etc.) e outros desafios para decidir quais dados devem ser aprendidos e quais não devem (a Akamai adota medidas preventivas para evitar o aprendizado dessas anomalias exigindo uma combinação de número mínimo de usuários, período de tempo e persistência para que o aprendizado seja acionado)

Descubra como podemos ajudar você agendando uma **demonstração personalizada do Akamai API Security**.