WHITE PAPER

Detección de anomalías con Akamai API Security

Las API son un componente clave para las organizaciones a la hora de atender a los clientes, generar ingresos y operar de forma eficiente. Sin embargo, su crecimiento continuo, su proximidad a los datos confidenciales y la falta de controles de seguridad las convierte en un objetivo atractivo para los atacantes de hoy en día. Para identificar de forma proactiva los signos de un posible abuso o un ataque relacionados con las API, es imprescindible tener información en tiempo real sobre el comportamiento de los usuarios.

Por eso, las funciones de detección de anomalías de Akamai API Security identifican comportamientos extraños en los usuarios que reflejen posibles usos maliciosos o abusos en las API de una organización. Estas funcionalidades de Akamai comparan las solicitudes entrantes con una línea de base de lo que sería un tráfico normal y determinan si es probable que se trate de ataques.

Nuestro algoritmo de detección de anomalías identifica comportamientos anómalos, como:

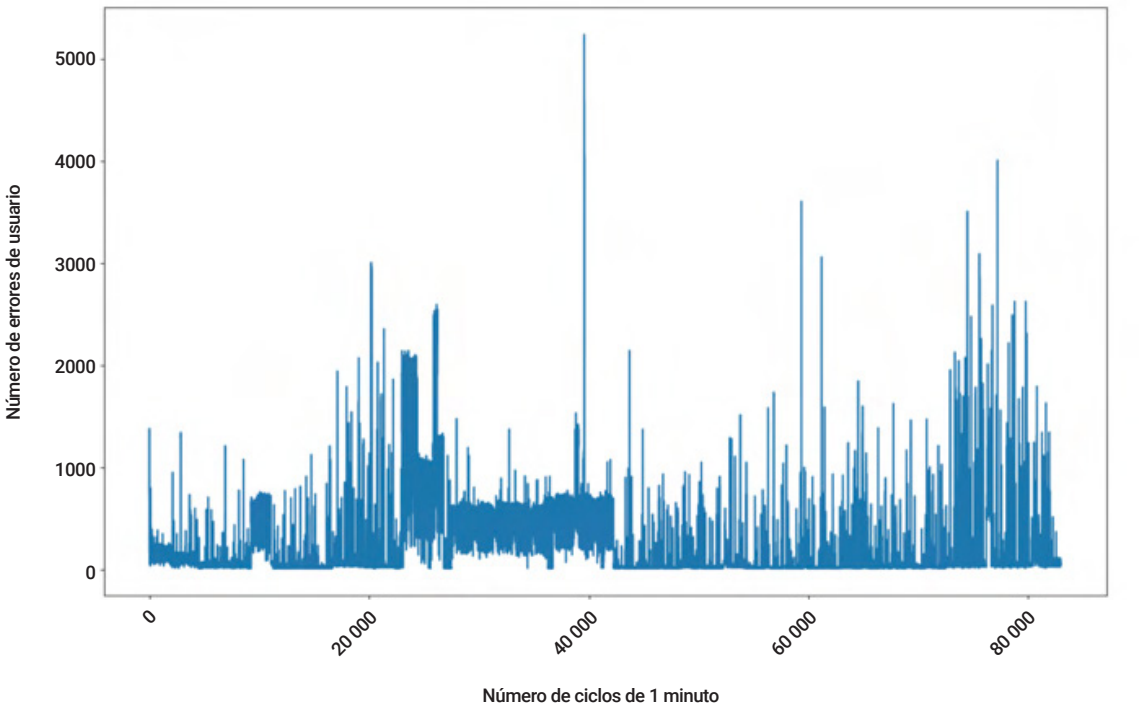
- Uso de un campo inesperado en la solicitud de API
- Extracción de más datos del servidor que el usuario normal
- Intentos de utilizar otros recursos de usuario/administrador
- Llamadas a las API en un orden inesperado

El algoritmo se basa en un modelo de inteligencia artificial y aprendizaje automático (IA/ML) en línea y no supervisado que aprende de las distintas características del comportamiento estadístico del tráfico y detecta incidentes anómalos después de un periodo de aprendizaje determinado. Nuestro modelo se adapta a los cambios que se van produciendo en el tráfico y a las anomalías que los usuarios marcan como falsos positivos.

Durante la fase de aprendizaje, el sistema analiza los datos del cliente e identifica cualquier API, método de autenticación, usuario, tipo de datos, etc. Para cada API el modelo desarrolla una lista de características del tráfico de usuario normal, incluido el número de visitas a la API, el número de errores generados, el porcentaje de solicitudes autenticadas y la cantidad de datos recuperados del servidor, entre otros. Nuestro algoritmo detecta las anomalías en un usuario comparando sus características y las de la API con los resultados esperados según el modelo estadístico que el algoritmo ha aprendido.

Funcionamiento de la detección de anomalías de Akamai API Security

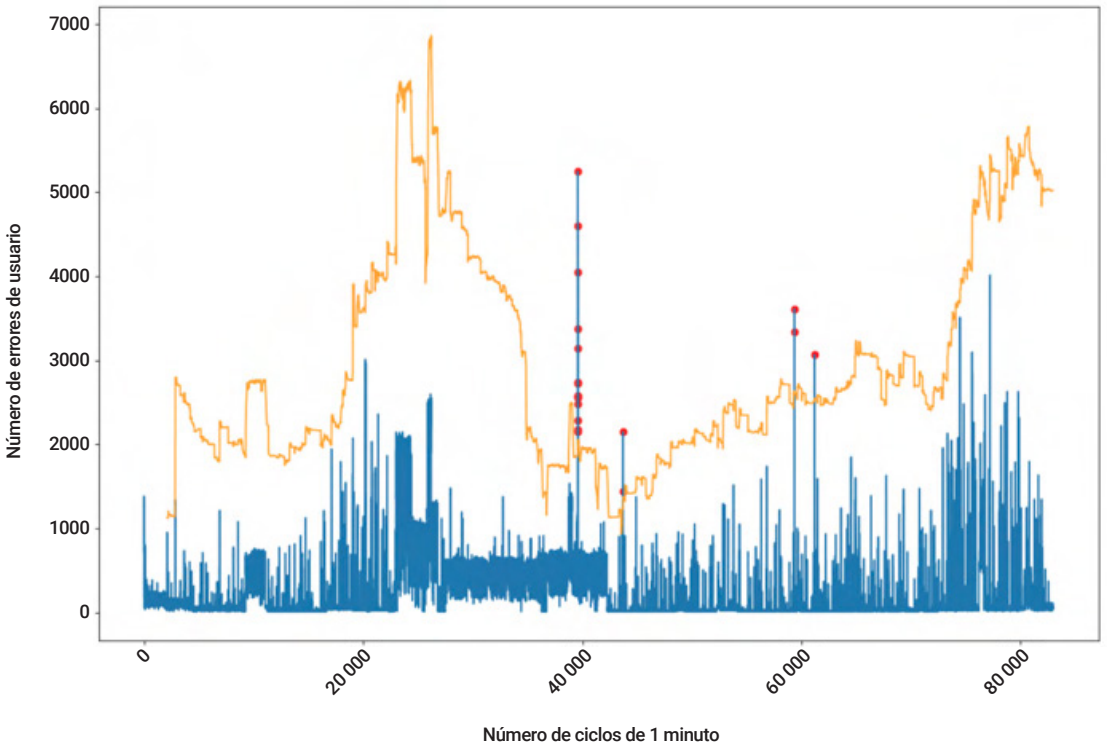
La detección de anomalías de Akamai API Security identifica qué usuarios generan muchos más errores que los demás. De este modo, se pueden identificar ataques como aquellos de fuerza bruta, exploración de rutas y scraping. El siguiente gráfico muestra la cantidad máxima de errores de usuario generados por un usuario cada ciclo de un minuto en un entorno determinado.



En este caso, la identificación de anomalías plantea varios retos:

1. El modelo debe tener en cuenta la desviación de datos al calcular el umbral.
2. Hay que evitar que, durante el periodo de aprendizaje del modelo, este se entrene con datos anómalos.
3. El aprendizaje se lleva a cabo en flujo, lo que significa que el modelo nunca ve todos los datos y necesita ajustarse en cada etapa.
4. Las alertas deben emitirse en tiempo real, por lo que nuestro algoritmo no puede confiar en datos futuros para predecir una anomalía.
5. Para evitar que el usuario reciba spam, nuestro modelo necesita aprender un umbral estadísticamente garantizado según los datos.

En el siguiente gráfico, podemos ver cómo nuestro modelo satisface esos requisitos ajustando los umbrales en función de los datos entrantes.



La línea naranja muestra la función de umbral calculada por el modelo, y los puntos rojos representan las anomalías detectadas según esa función.

Preguntas frecuentes

¿Cuál es el periodo de aprendizaje necesario para el algoritmo de detección de anomalías de Akamai?

La mayoría de nuestros algoritmos requieren un periodo de aprendizaje de dos a siete días. Además, el periodo de aprendizaje del algoritmo también se ve afectado por el número de comportamientos diferentes de los usuarios.

Cuando se detecta un comportamiento anómalo, ¿cuánto tiempo tarda en generarse la alerta?

A partir de la recepción del tráfico anómalo, nuestro algoritmo creará una alerta relevante para el cliente en un periodo de entre 30 a 60 segundos en la mayoría de los casos.

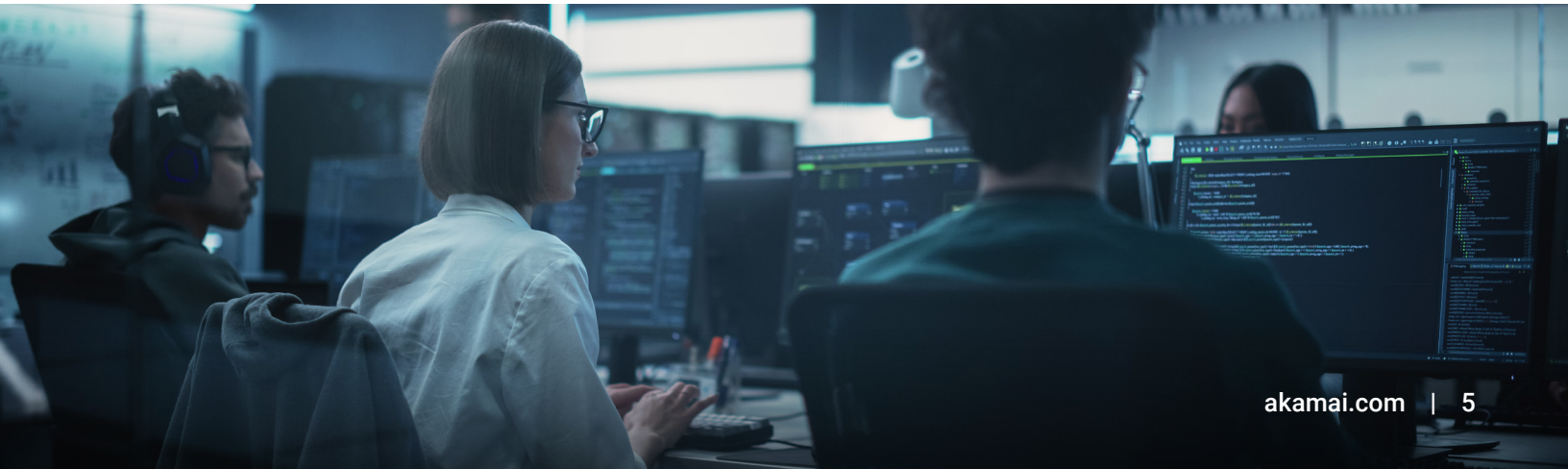
¿Utiliza el algoritmo un modelo supervisado o no supervisado?

Nuestro algoritmo se basa en un modelo no supervisado, que le permite adaptarse al entorno de cada cliente sin tener conocimientos previos de sus características. Además, usa el aprendizaje en línea para ajustarse a los cambios que se van produciendo en el entorno paulatinamente.

¿Qué tipos de anomalías detecta Akamai API Security?

Akamai API Security detecta dos tipos de anomalías:

- Según los patrones: anomalías que se basan en la identificación de patrones maliciosos en el tráfico, como técnicas de explotación web y agentes de usuario maliciosos conocidos, lo que incluye la inyección de comandos, el cruce de directorios y agentes de usuario sospechosos.
- Según el comportamiento: anomalías que se basan en el aprendizaje de comportamientos de los usuarios, y la identificación de comportamientos anómalos, como un uso excesivo de API, una infracción de rango o una autorización a nivel de objeto rota (BOLA).



¿Qué parámetros tiene en cuenta Akamai API Security para registrar una anomalía?

Nuestros algoritmos se basan en varias características tras analizar de forma estadística el tráfico, como:

- El número de usuarios diferentes que utilizan una API
- El estado de autenticación de una API
- El código de respuesta del servidor
- La cantidad de datos que extrae el usuario
- La geolocalización de la IP del usuario
- El agente de usuario en cada caso

¿Puede el usuario controlar la sensibilidad del algoritmo?

Sí, el usuario puede controlar la sensibilidad de cada anomalía modificando sus niveles en la política correspondiente. La sensibilidad de la política se mide entre el 1 (baja) y el 5 (alta); el valor más alto representa el nivel de sensibilidad máximo configurable para cada política de anomalías en Akamai API Security. Nuestro algoritmo tiene en cuenta este parámetro como parte del modelo.

¿Puede el usuario señalar como falso positivo un problema notificado por Akamai? ¿Cómo afectaría esto al algoritmo?

Sí, para mejorar la detección de anomalías, los usuarios pueden marcar los problemas pertinentes como "falsos positivos". Nuestro algoritmo tiene en cuenta si un problema se marca como falso positivo y ajusta el modelo según la información indicada por el usuario.

¿Cómo evita Akamai el "spam" al cliente si un usuario envía sin cesar el mismo escenario de ataque?

Nuestro algoritmo identificará problemas similares que se sigan dando en el mismo usuario y API. En este caso, el algoritmo ignorará problemas similares durante un periodo constante.

¿Cómo gestiona Akamai la desviación/estacionalidad de los datos?

Akamai API Security utiliza algoritmos diferentes para detectar anomalías en los datos. En función del preprocesamiento de los datos subyacentes y de la complejidad del algoritmo, podemos relajar el ajuste del umbral o aplicar ajustes en cada ciclo cuando necesitamos umbrales estadísticos garantizados para la detección de anomalías. Además de controlar el spam, ofrecemos una interfaz sencilla incluso cuando un algoritmo específico requiere ciclos adicionales para ajustar los umbrales.

¿Cómo gestiona Akamai el envenenamiento de datos?

Al tratarse de un algoritmo de aprendizaje online, Akamai API Security debe abordar una serie de retos, como:

- Nuevas API
- Nuevos campos en API existentes
- Cambios del tipo/rango de valor en un campo
- Problemas de disponibilidad del servidor
- Fallos en las API que pueden provocar errores (404, 500, etc.) y otros desafíos que implican decidir de qué datos aprender y de cuáles no (Akamai toma precauciones para no aprender estas anomalías: se requiere una combinación de un número de usuarios, un periodo de tiempo y una persistencia mínimos para activar el aprendizaje)

Descubra cómo podemos ayudarle con esta **demostración de Akamai API Security personalizada**.