Historia de cliente de Akamai

Una empresa de moda de la lista Fortune 500 protege sus API y operaciones de retail

Protección de las API que ofrecen una experiencia de compra fácil y personalizada, a la vez que se evita la filtración de datos de clientes

Detección de todas las API

Identificación de vulnerabilidades

Refuerzo del nivel de seguridad

Las API han desempeñado un papel fundamental en la transición del retail de las tiendas tradicionales a las plataformas de comercio electrónico. Detrás de cada interacción digital, hay una API en segundo plano que permite a los retailers:

- Conectar varios sistemas, aplicaciones y servicios de manera fluida
- Integrar sus tiendas online con sistemas back-end de gestión de inventario, pasarelas de pago, servicios de envío y herramientas de gestión de las relaciones con los clientes
- Facilitar un intercambio rápido de datos para que la experiencia de compra online sea personalizada y fácil

Con la protección de esos datos como prioridad, la seguridad de API desempeña un papel fundamental a la hora de garantizar la confianza, la integridad y la confidencialidad de las operaciones empresariales online.

La proximidad de las API a los datos confidenciales las convierte en objetivos atractivos para los ciberdelincuentes que buscan explotar las vulnerabilidades. Una vulneración de API puede dar lugar a la exposición de información del cliente, como datos personales, de tarjetas de pago o historiales de compra. Por estas razones, este retailer de moda de la lista Fortune 500 recurrió a Noname Security (ahora una empresa de Akamai) en busca de ayuda, ya que no estaba satisfecho con su relación con Salt Security.

Fashion Retailer

Ubicación

Estados Unidos

Sector

Retail

Solución

Akamai API Security

Akamai

Creación de un enfoque programático para la seguridad de API

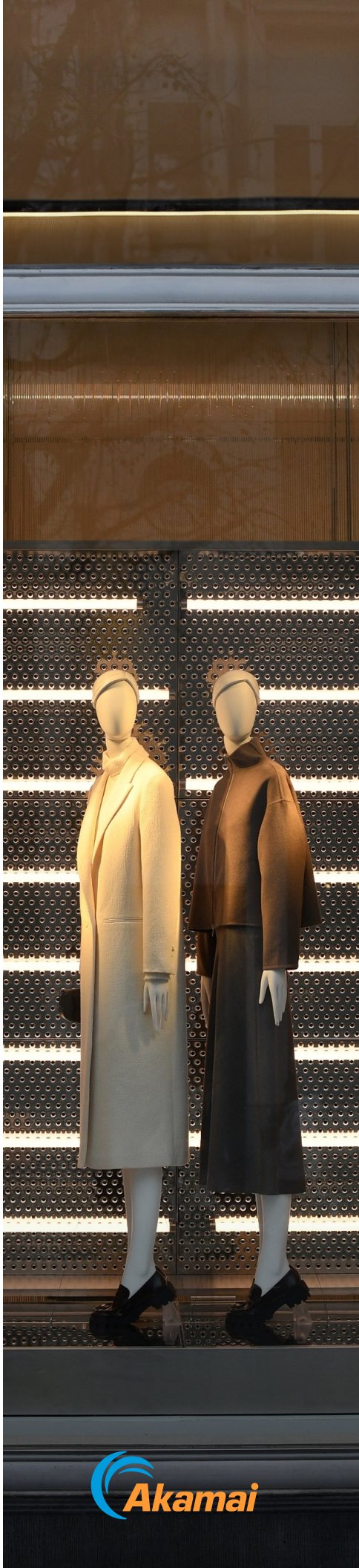
El retailer de la lista Fortune 500 buscaba crear un flujo de trabajo integral que mitigara los riesgos de seguridad de API y fuese más allá de los firewalls de aplicaciones web y las puertas de enlace de API. Para lograrlo, necesitaba una estrategia de seguridad sólida y controles fiables para las API. La empresa también se centró en la mitigación de bots, distinguiendo en última instancia entre usuarios legítimos y bots maliciosos, lo que le permitió proteger sus sistemas, los datos y la experiencia de usuario.

Dado el tamaño del proyecto, el retailer y Akamai acordaron un enfoque por fases. La primera fase implicaría la localización de todas sus API, la clasificación de los datos confidenciales, la implementación de mecanismos de detección y respuesta, y la integración con Splunk. La segunda fase conllevaría la adopción del modelo "shift-left" para las pruebas de seguridad de API con el fin de promover la creación de código seguro.

Implementación acelerada para reducir el tiempo de amortización

A pesar de que la primera fase era todo un reto, el equipo de Akamai pudo implementar los módulos de detección de API y protección del tiempo de ejecución de Noname en tan solo 120 días, a la vez que ejecutaba la integración de Splunk. La detección de API desempeña un papel fundamental a la hora de controlar su proliferación e implica la identificación y la catalogación sistemáticas de todas las API de una organización. Al mantener un repositorio centralizado de API, los desarrolladores pueden buscar y descubrir fácilmente las API existentes antes de emprender nuevas iniciativas de desarrollo. De esta forma, se evita la creación de API duplicadas y se fomenta su reutilización, lo que ahorra tiempo y esfuerzo.

Akamai utiliza funciones de detección automatizada basadas en el aprendizaje automático para identificar las vulnerabilidades de las API, incluidas la filtración y la manipulación de datos, las infracciones de las políticas de datos, los comportamientos sospechosos y los ataques a la seguridad de las API. Así, el retailer de la lista Fortune 500 puede mejorar significativamente la seguridad y la integridad de sus API, proteger los datos confidenciales y mantener la confianza de los usuarios y partners.



 | Publicado en agosto de 2024