FICHA TÉCNICA DE AKAMAI

API Security ShadowHunt

API Security ShadowHunt es un servicio gestionado de búsqueda de amenazas que puede ayudar a su equipo de seguridad con nuestros analistas especializados en amenazas de API. Ideal para equipos con poco personal o aquellos que carecen de los conocimientos en seguridad de API, API Security ShadowHunt es una solución externalizada que le ayuda a reducir el riesgo. El equipo de seguridad actúa como una extensión de su equipo para detectar e informar sobre los ataques más clandestinos que se ocultan en su tráfico de API.

Cómo funciona API Security ShadowHunt

Las operaciones de ShadowHunt comienzan con los datos de actividad de las API en la plataforma API Security. Estos análisis automatizados detectan desviaciones en el comportamiento e intentos de explotación de las vulnerabilidades. Las señales de aprendizaje automático se envían a los analistas de ShadowHunt para su investigación. Aquí es donde entran en juego las competencias de los expertos.

Dado que los analistas están familiarizados con los entornos de API de los clientes, identificarán rápidamente las amenazas activas y crearán y transmitirán una alerta ShadowHunt. Si hay ambigüedad en los resultados, un analista se pondrá en contacto con un suscriptor de ShadowHunt para obtener aclaraciones. Los analistas y el equipo de investigación de API Security utilizan la información de inteligencia contra amenazas para enviar informes periódicos sobre amenazas emergentes a todos los clientes del servicio.

API Security y las competencias de los expertos

La plataforma API Security ofrece completas funciones de seguridad de API, entre las que se incluyen:

- **Detección de API:** detección amplia y continua de API
- **Estrategia de riesgo:** comprensión de los riesgos de las API
- **Detección de amenazas mediante análisis del comportamiento:** nuestro motor de análisis de Big Data basado en la nube examina toda la actividad de las API a lo largo del tiempo, detectando continuamente los posibles abusos
- **Prevención y respuesta:** las guías personalizadas de respuesta condicional mejoran la seguridad y los procesos de DevSecOps de las API
- **Investigación y búsqueda de amenazas:** las potentes funciones de investigación permiten detectar amenazas ocultas en el tráfico de API

La búsqueda de amenazas es una de las funciones más avanzadas de la plataforma API Security. El servicio API Security ShadowHunt está diseñado para clientes que carecen de las herramientas, los conocimientos o el tiempo necesarios para dar caza a las amenazas.

VENTAJAS PARA SU EMPRESA

La tranquilidad de que los expertos examinan la actividad de sus API

La detección de un mayor número de amenazas de seguridad que acechan en los datos de sus API

Más tiempo para su equipo mientras Akamai se centra en la seguridad de las API

Información procesable para el desarrollo de software y las operaciones de TI

Visibilidad mejorada del comportamiento de las API con un escrutinio adicional

Akamai

API Security ShadowHunt: servicios en los que puede confiar

Alertas: *notificación de una amenaza en su entorno de API.* El elemento más importante del servicio API Security ShadowHunt es la alerta, que se transmite inmediatamente después de la confirmación de un incidente activo. Las alertas incluyen:

- Resultados de incidentes y análisis
- Resumen de inteligencia contra amenazas relativo al incidente
- Recomendaciones de corrección

Informes de amenazas: *inteligencia sobre seguridad de API en las primeras fases*. El informe sobre amenazas emergentes de API Security ShadowHunt se basa en el acceso del equipo a la inteligencia global contra amenazas, la información del equipo de investigación de API Security y las actividades de búsqueda de amenazas en curso. El informe sobre amenazas emergentes incluye:

- Información sobre nuevas vulnerabilidades, amenazas o ataques de API identificados por el equipo
- Efectos en su entorno de API
- Recomendaciones para la corrección, según sea necesario

Revisiones mensuales: *plena visibilidad de su entorno de API*. El informe mensual sobre amenazas de ShadowHunt se envía a todos los clientes de API Security la primera semana de cada mes, e incluye lo siguiente:

- Un resumen de las alertas de ShadowHunt y los informes sobre amenazas emergentes enviados el mes anterior
- Una descripción general de su entorno de API
- Una comparación de la actividad de las API de los últimos dos meses
- Titulares sobre seguridad del sector de las API

Preguntas a expertos: los suscriptores del servicio tienen acceso al equipo de API Security ShadowHunt para hacerles preguntas y hablar con ellos de las alertas y los informes sobre amenazas emergentes.

¿Por qué elegir API Security?

API Security aplica los principios de detección y respuesta extendidas (XDR) al desafío de proteger las API frente a vulnerabilidades y abusos. Solo API Security agrega la actividad de las API a su entorno de Big Data basado en la nube, seguido de un enriquecimiento de datos y una organización complejos. Esta arquitectura única ofrece funciones de detección continua de API, valoración del riesgo, análisis del comportamiento teniendo en cuenta el contexto para detectar abusos y amenazas a las API, y búsqueda de amenazas. La arquitectura de API Security incluye la privacidad desde el diseño, en la que cualquier actividad de las API destinada al lago de datos se puede convertir en token.

Competencias en la búsqueda de amenazas para proteger sus API

El mayor número de implementaciones de API puede ejercer presión sobre los departamentos de seguridad de TI de las organizaciones. El servicio API Security ShadowHunt amplía su personal de seguridad hoy mismo.

Hable con un experto para obtener más información.

 | Asistencia | | Publicado en 08/23