PLANILHA DE DADOS DA AKAMAI

API Security ShadowHunt

O API Security ShadowHunt é um serviço de busca de ameaças gerenciado que expande a equipe de segurança com analistas especializados em busca de ameaças a APIs. Ideal para equipes com falta de pessoal ou para quem não tem experiência em segurança de API, o API Security ShadowHunt é uma solução terceirizada que ajuda a reduzir os riscos. Os caçadores de ameaças trabalham como uma extensão de sua equipe para detectar e relatar os ataques mais clandestinos e ofuscados que se escondem no tráfego de API.

Como funciona o API Security ShadowHunt

As operações do ShadowHunt começam com dados de atividade da API na plataforma API Security. Essas análises automatizadas detectam desvios comportamentais e explorações de vulnerabilidade. Os sinais de machine learning são entregues aos analistas do ShadowHunt para investigação. É aí que o conhecimento humano entra em ação.

Como os analistas estão familiarizados com propriedades de API do cliente, eles identificarão rapidamente ameaças ativas e criarão e transmitirão um Alerta do ShadowHunt. Se houver ambiguidade nas descobertas, um analista entrará em contato com o assinante do ShadowHunt para esclarecimento. Os analistas e a equipe de pesquisa do API Security consomem informações de inteligência de ameaças para fornecer relatórios periódicos de ameaças emergentes a todos os clientes de serviços.

API Security associada ao conhecimento humano

A plataforma API Security oferece recursos abrangentes de segurança de API, como:

- **Detecção de APIs:** Detecção de APIs ampla e contínua
- **Postura de risco:** Entenda seus riscos de API
- **Detecção de ameaças usando a análise comportamental:** Nosso mecanismo de análise de big data baseado em nuvem examina todas as atividades da API ao longo do tempo, detectando continuamente o abuso de API
- **Prevenção e resposta:** Os guias estratégicos de resposta condicionais e personalizados melhoram a segurança e os processos de API do DevSecOps
- **Investigação e busca de ameaças:** Os recursos investigativos poderosos fornecem a capacidade de procurar ameaças ocultas no tráfego de API

A busca por ameaças é um dos recursos mais avançados da plataforma API Security. O serviço API Security ShadowHunt é destinado a clientes que não possuem ferramentas, competências ou tempo para procurar ameaças.

BENEFÍCIOS PARA SUA EMPRESA

- A tranquilidade de que os especialistas estão examinando sua atividade de API
- A detecção de mais ameaças à segurança espreitando os dados de API
- Mais tempo para sua equipe enquanto a Akamai se concentra na segurança das APIs
- Insights acionáveis para desenvolvimento de software e operações de TI
- Visibilidade aprimorada do comportamento da API com análise adicional

Akamai

Serviços do API Security ShadowHunt nos quais você pode confiar

Alertas: *Notificação de uma ameaça em sua propriedade de API.* O elemento mais importante do serviço API Security ShadowHunt é o alerta, transmitido imediatamente após a confirmação de um incidente ativo. Os alertas incluem:

- Descobertas e análises de incidentes
- Resumo da inteligência de ameaças referente ao incidente
- Recomendações de correção

Relatórios de ameaças: *Obtenha inteligência de segurança de API desde cedo*. O Relatório de ameaças emergentes do API Security ShadowHunt é baseado no acesso da equipe à inteligência global de ameaças, nas informações fornecidas pela equipe de pesquisa do API Security e nas atividades contínuas de busca de ameaças. O Relatório de ameaças emergentes inclui:

- Informações sobre novas vulnerabilidades, ameaças ou ataques a APIs identificados pela equipe
- Efeitos na sua propriedade de API
- Recomendações para correção, conforme necessário

Revisões mensais: *Visibilidade total da sua propriedade de API*. O Relatório mensal de ameaças do ShadowHunt é entregue a todos os clientes do API Security na primeira semana de cada mês. Ele inclui:

- Um resumo dos alertas do ShadowHunt e dos relatórios de ameaças emergentes enviados no mês anterior
- Uma visão geral da sua propriedade de API
- Uma comparação da atividade de API dos últimos dois meses
- Notícias sobre segurança do setor de API

Pergunte aos especialistas: Os assinantes do serviço têm acesso à equipe do API Security ShadowHunt para perguntas e discussões sobre alertas e relatórios de ameaças emergentes.

Por que o API Security?

O API Security aplica os princípios de detecção e resposta estendidas (XDR) ao desafio de proteger APIs contra vulnerabilidades e abuso. Apenas o API Security agrega a atividade da API em seu ambiente de big data baseado em nuvem, seguido por um complexo enriquecimento e organização de dados. Essa arquitetura exclusiva permite detecções contínuas de API, pontuação de risco, análise comportamental sensível ao contexto para detectar abuso e ameaças a APIs e busca de ameaças. A arquitetura do API Security inclui privacidade por design, em que qualquer atividade de API destinada ao data lake pode ser tokenizada.

Experiência em busca de ameaças para proteger suas APIs

O crescimento das implantações de API pode sobrecarregar os departamentos de segurança de TI das organizações. O serviço API Security ShadowHunt expande sua equipe de segurança hoje mesmo.

Fale com um especialista para saber mais.