FICHE TECHNIQUE AKAMAI

API Security ShadowHunt

API Security ShadowHunt est un service géré de détection des menaces permettant d'agrandir votre équipe de sécurité grâce aux analystes experts spécialisés dans la recherche des menaces liées aux API. Idéal pour les équipes en sous-effectif ou celles qui manquent d'expertise en matière de sécurité des API, API Security ShadowHunt est une solution externalisée qui vous aide à la réduction des risques. Les détecteurs de menaces travaillent comme une extension de votre équipe pour détecter et signaler les attaques les plus souterraines et les mieux dissimulées qui se cachent dans le trafic de vos API.

Comment fonctionne API Security ShadowHunt

Les opérations de ShadowHunt commencent avec les données d'activité des API dans la plateforme API Security. Ces analyses automatisées détectent les écarts comportementaux et les exploitations de vulnérabilités. Les signaux d'apprentissage automatique sont transmis aux analystes de ShadowHunt pour investigation. C'est là que l'expertise humaine rentre en jeu.

Comme les analystes connaissent bien les domaines API des clients, ils identifieront rapidement les menaces actives et créeront et transmettront une alerte ShadowHunt. En cas d'ambiguïté au niveau des résultats, un analyste contactera un abonné ShadowHunt pour fournir des explications. Les analystes et l'équipe de recherche API Security utilisent des informations sur les menaces pour fournir des rapports périodiques sur les menaces émergentes à tous les clients du service.

Une expertise humaine en plus d'API Security

La plateforme API Security offre des fonctionnalités de sécurité des API complètes, notamment :

- **Détection des API :** découverte étendue et continue d'API
- **Profil de risque :** comprenez les risques liés à vos API
- **Détection des menaces à l'aide de l'analyse comportementale :** notre moteur d'analyse de Big Data basé sur le cloud examine toute l'activité des API au fil du temps et détecte en permanence les exploitations d'API
- **Prévention et intervention :** les playbooks de réponse conditionnelle personnalisés améliorent la sécurité et les processus DevSecOps des API
- **Enquête et détection des menaces :** de puissantes capacités d'investigation permettent de détecter les menaces qui se cachent dans votre trafic des API

La détection des menaces est l'une des capacités les plus avancées de la plateforme API Security. Le service API Security ShadowHunt est destiné aux clients qui ne disposent pas des outils, de l'expertise ou du temps nécessaires pour rechercher les menaces.

AVANTAGES POUR VOTRE ENTREPRISE

- La tranquillité d'esprit de savoir que des experts examinent l'activité de vos API
- La détection d'un plus grand nombre de menaces de sécurité se cachant dans vos données API
- Plus de temps pour votre équipe pendant qu'Akamai se concentre sur la sécurité des API
- Des informations exploitables pour le développement de logiciels et les opérations informatiques
- Une visibilité améliorée du comportement des API grâce à un examen plus approfondi

Akamai

Des services API Security ShadowHunt sur lesquels vous pouvez compter

Alertes : *notification d'une menace dans votre domaine API.* Transmises immédiatement après la confirmation d'un incident actif, les alertes constituent l'élément le plus important du service API Security ShadowHunt. Elles incluent :

- Les résultats et analyses des incidents
- Une synthèse des informations sur les menaces relatives à l'incident
- Des recommandations sur les mesures correctives

Rapports sur les menaces : *obtenez des informations sur la sécurité des API rapidement*. Le rapport sur les menaces émergentes d'API Security ShadowHunt est basé sur l'accès de l'équipe aux informations sur les menaces mondiales, les contributions de l'équipe de recherche d'API Security et les activités de détection des menaces en cours. Le rapport sur les menaces émergentes comprend :

- Des informations sur les nouvelles vulnérabilités, menaces ou attaques des API identifiées par l'équipe
- Les effets sur votre domaine API
- Des recommandations sur les mesures correctives, en fonction des besoins

Rapports mensuels : *visibilité totale sur votre domaine API*. Le rapport mensuel sur les menaces ShadowHunt est envoyé à tous les clients d'API Security la première semaine de chaque mois. Il comprend :

- Une synthèse des alertes ShadowHunt et les rapports sur les menaces émergentes envoyés le mois précédent
- Un aperçu de votre domaine API
- Une comparaison de l'activité des API au cours des deux derniers mois
- Les actualités en matière de sécurité du secteur des API

Contact avec les experts : les abonnés au service peuvent contacter l'équipe API Security ShadowHunt pour poser des questions et échanger sur les alertes et les rapports sur les menaces émergentes.

Pourquoi API Security ?

API Security applique les principes de découverte et de réponse étendues (XDR) afin de sécuriser les API contre les vulnérabilités et les exploitations. Seul API Security regroupe l'activité des API dans son environnement de Big Data basé sur le cloud. S'ajoute à cela un enrichissement et une organisation complexes des données. Cette architecture unique permet la découverte continue d'API, l'évaluation des risques, l'analyse comportementale contextuelle pour détecter les menaces et les exploitations d'API, ainsi que la détection des menaces. L'architecture d'API Security inclut la confidentialité dès la conception, toute activité des API destinée au lac de données pouvant être tokenisée.

Expertise en matière de détection des menaces pour protéger vos API

La croissance des déploiements d'API peut mettre à rude épreuve les services de sécurité informatique des entreprises. Le service API Security ShadowHunt permet de renforcer votre personnel de sécurité dès aujourd'hui.

Échangez avec un expert pour en savoir plus.

 | Assistance | Publication : 08/23