SCHEDA TECNICA AKAMAI

API Security ShadowHunt

API Security ShadowHunt è un servizio gestito di ricerca delle minacce a disposizione del vostro team di sicurezza che si avvale degli analisti Akamai esperti in tema di minacce alle API. Ideale per team a corto di personale o con scarse competenze a livello di sicurezza delle API, API Security ShadowHunt è una soluzione esternalizzata in grado di ridurre i rischi. Gli addetti all'identificazione delle minacce lavorano come un'estensione del vostro team, al fine di rilevare e segnalare gli attacchi più clandestini e camuffati che si nascondono nel traffico delle API.

Come funziona API Security ShadowHunt

ShadowHunt inizia a inviare i dati relativi alle attività delle API alla piattaforma API Security. Queste analisi automatizzate rilevano eventuali deviazioni nel comportamento e tentativi di sfruttamento delle vulnerabilità, quindi i segnali di apprendimento automatico vengono inviati agli analisti di ShadowHunt per condurre al meglio le indagini. A questo punto, entrano in azione le competenze degli esperti.

Poiché gli analisti hanno dimestichezza con il patrimonio delle API dei clienti, identificano rapidamente le minacce attive, creando e trasmettendo un avviso ShadowHunt. In caso di ambiguità nei risultati, un analista contatta un abbonato ShadowHunt per eventuali chiarimenti. Gli analisti insieme al team addetto alle ricerche di API Security utilizzano l'intelligence sulle minacce per fornire rapporti periodici sulle minacce emergenti a tutti i clienti dei servizi.

API Security e le competenze degli esperti

La piattaforma API offre funzioni complete per la sicurezza delle API, tra cui:

- **Rilevamento delle API:** rilevamento esaustivo e continuo delle API
- **Strategia relativa ai rischi:** scoprite i rischi delle vostre API
- **Rilevamento delle minacce grazie all'analisi comportamentale:** il nostro sistema di analisi dei big data basato su cloud esamina l'attività di tutte le API nel tempo per rilevare eventuali abusi in modo continuativo
- **Prevenzione e risposta:** la disponibilità di playbook su risposte condizionali e personalizzabili migliora la sicurezza e i processi DevSecOps delle API
- **Ricerca delle minacce e indagini:** le potenti funzionalità investigative offrono la possibilità di cercare le minacce nascoste nel traffico delle API

La ricerca delle minacce è una delle funzionalità più avanzate della piattaforma API Security. Il servizio API Security ShadowHunt è concepito per i clienti che non dispongono del tempo, delle competenze o degli strumenti necessari per cercare le minacce.

VANTAGGI PER LE AZIENDE

- La tranquillità di sapere che le attività delle API vengono esaminate da esperti
- La capacità di rilevare un maggior numero di minacce alla sicurezza che proliferano nei dati delle API
- Una maggior quantità di tempo per il team mentre Akamai si focalizza sulla sicurezza delle API
- Preziose informazioni per lo sviluppo di software e le operazioni IT
- Una migliore visibilità sul comportamento delle API con un maggior livello di controllo

Akamai

I servizi API Security ShadowHunt su cui poter contare

Avvisi: *notifiche delle minacce rilevate nel patrimonio delle API.* L'elemento più importante del servizio API Security ShadowHunt è rappresentato dalla funzione degli avvisi, che vengono inviati immediatamente dopo la conferma di un incidente attivo. Gli avvisi includono:

- Individuazione e analisi degli incidenti
- Riepilogo sull'intelligence sulle minacce relativo agli incidenti
- Consigli per la risoluzione dei problemi

Rapporti sulle minacce: *un'intelligence tempestiva sulla sicurezza delle API*. Il rapporto sulle minacce emergenti di API Security ShadowHunt si basa sull'accesso del team all'intelligence globale sulle minacce, alle indicazioni del team di ricerca di API Security e alle continue attività di ricerca delle minacce. Il rapporto sulle minacce emergenti include:

- Dettagli sulle nuove vulnerabilità delle API, sulle minacce o sugli attacchi identificati dal team
- Gli effetti sul patrimonio delle API
- Consigli per la risoluzione dei problemi in base alle specifiche esigenze

Revisioni mensili: *Completa visibilità sul patrimonio delle API*, il rapporto mensile sulle minacce di ShadowHunt, viene fornito a tutti i clienti di API Security la prima settimana di ogni mese e include:

- Un riepilogo dei rapporti sulle minacce emergenti e sugli avvisi di ShadowHunt inviati il mese precedente
- Una panoramica sul patrimonio delle API
- Un confronto delle attività delle API negli ultimi due mesi
- Le novità sulla sicurezza nel settore delle API

Consulenza di esperti: gli abbonati al servizio possono accedere al team di API Security ShadowHunt per porre domande e per discutere sui rapporti sulle minacce emergenti e sugli avvisi.

Le competenze sulla ricerca delle minacce per la protezione delle API

Il maggior numero di implementazioni delle API può mettere sotto pressione i reparti addetti alla sicurezza IT delle organizzazioni. Il servizio API Security ShadowHunt adesso espande il personale addetto alla sicurezza.

Perché API Security?

API Security applica i principi XDR (Extended Detection and Response) per la protezione delle API da vulnerabilità e abusi. Solo API Security aggrega le attività delle API nel suo ambiente dei big data basato su cloud seguito da un livello complesso di organizzazione e arricchimento dei dati. Questa architettura esclusiva offre funzioni di rilevamento continuo delle API, valutazione del rischio, abuso e minacce delle API e ricerca delle minacce. L'architettura di API Security include la privacy per impostazione predefinita, grazie alla quale è possibile tokenizzare tutte le attività delle API destinate al data lake.

Parlate con un esperto per ulteriori informazioni.