DATENBLATT VON AKAMAI

API Security ShadowHunt

API Security ShadowHunt ist ein Managed Threat Hunting Service, der Ihr Sicherheitsteam mit Experten verbindet, die auf die Suche nach API-Bedrohungen spezialisiert sind. API Security ShadowHunt ist eine ausgelagerte Lösung, das bei der Risikoreduzierung hilft, und somit ideal für unterbesetzte Teams oder solche, denen es an API-Sicherheitsexpertise mangelt. Unsere Threat Hunter fungieren als Erweiterung Ihres Teams und erkennen und melden selbst die am besten getarnten und raffiniertesten Angriffe, die sich in Ihrem API-Traffic verstecken.

So funktioniert API Security ShadowHunt

ShadowHunt setzt bei den API-Aktivitätsdaten auf der API-Security-Plattform an. Diese automatisierten Analysen erkennen Verhaltensabweichungen und Sicherheitslücken, und Signale werden anhand von maschinellem Lernen zur Untersuchung an die ShadowHunt-Analysten gesendet. Dann kommt menschliche Expertise zum Einsatz:

Da die Analysten mit den API-Umgebungen der Kunden vertraut sind, können sie aktive Bedrohungen schnell identifizieren und eine ShadowHunt-Warnmeldung erstellen und übermitteln. Wenn die Ergebnisse nicht eindeutig sind, kontaktiert ein Analyst den ShadowHunt-Abonnenten zur weiteren Klärung. Die Analysten und das Forschungsteam von API Security nutzen Bedrohungsinformationen, um regelmäßig neue Bedrohungsberichte an alle Servicekunden zu senden.

API Security + menschliche Expertise

Die API-Security-Plattform bietet umfassende Funktionen, darunter:

- **API-Erkennung:** weitreichende und kontinuierliche API-Erkennung.
- **Risikopotenzial:** Einblicke in Ihre API-Risiken.
- **Bedrohungserkennung mit Verhaltensanalysen:** Unsere cloudbasierte Engine für Big-Data-Analysen untersucht alle API-Aktivitäten und erkennt kontinuierlich API-Missbrauch.
- **Prävention und Reaktion:** Nutzerdefinierte, bedingte Reaktionspläne verbessern die Sicherheit und API-DevSecOps-Prozesse.
- **Untersuchung und Threat Hunting:** Leistungsstarke Ermittlungsfunktionen ermöglichen die Suche nach Bedrohungen, die sich in Ihrem API-Traffic verstecken.

Threat Hunting ist eine der fortschrittlichsten Funktionen der API-Security-Plattform. API Security ShadowHunt ist für Kunden gedacht, die entweder nicht über die Tools, das Fachwissen oder die Zeit verfügen, um selbst nach API-Bedrohungen zu suchen.

VORTEILE FÜR IHR UNTERNEHMEN

- Die Gewissheit, dass Ihre API-Aktivitäten von Experten untersucht werden
- Die Erkennung von mehr Sicherheitsbedrohungen, die in Ihren API-Daten lauern
- Ihr Team hat mehr Zeit, während Akamai sich um die API-Sicherheit kümmert
- Verwertbare Erkenntnisse für Softwareentwicklung und IT-Betrieb
- Verbesserte Transparenz des API-Verhaltens durch zusätzliche Prüfung

Akamai

API Security ShadowHunt – Services, auf die Verlass ist

Warnmeldungen: *Benachrichtigung über eine Bedrohung in Ihrer API-Umgebung.* Der wichtigste Aspekt von API Security ShadowHunt ist die Warnmeldung, die sofort nach Bestätigung eines aktiven Vorfalls übermittelt wird. Warnmeldungen beinhalten:

- Vorfallsinformationen und -analyse
- Zusammenfassung der Bedrohungsinformationen zum Vorfall
- Empfehlungen zur Behebung

Bedrohungsberichte: *Erhalten Sie frühzeitig API-Sicherheitsinformationen*. Der API Security ShadowHunt Emerging Threat Report basiert auf dem Zugriff des Teams auf globale Bedrohungsinformationen, Erkenntnissen des Forschungsteam von API Security und laufenden Threat-Hunting-Aktivitäten. Der Emerging Threat Report beinhaltet:

- Informationen zu neuen API-Schwachstellen, Bedrohungen oder Angriffen, die vom Team identifiziert wurden
- Auswirkungen auf Ihre API-Umgebung
- Empfehlungen zur Behebung, falls erforderlich

Monatliche Überprüfungen: *Erhalten Sie einen vollständigen Einblick in Ihre API-Umgebung*. Der ShadowHunt Monthly Threat Report wird allen Kunden von API Security in der ersten Woche jedes Monats zur Verfügung gestellt. Es werden folgende Themen behandelt:

- Zusammenfassung der Warnmeldungen und Emerging Threat Reports von ShadowHunt, die im Vormonat versandt wurden
- Überblick über Ihre API-Umgebung
- Vergleich der API-Aktivitäten der letzten zwei Monate
- sicherheitsrelevante Schlagzeilen aus der API-Branche

Fragen Sie die Experten: Serviceabonnenten haben direkten Kontakt zum API Security ShadowHunt Team für Fragen und Diskussionen zu Warnmeldungen und Emerging Threat Reports.

Warum API Security?

API Security nutzt erweiterte Erkennungs- und Reaktionsprinzipien (Extended Detection and Response, XDR), um APIs vor Sicherheitslücken und Missbrauch zu schützen. Nur API Security sammelt API-Aktivitäten in seiner cloudbasierten Big-Data-Umgebung, gefolgt von einer komplexen Datenanreicherung und -organisation. Diese einzigartige Architektur ermöglicht eine kontinuierliche API-Erkennung, Risikobewertung, kontextbezogene Verhaltensanalysen zur Erkennung von API-Missbrauch und Bedrohungen sowie Threat Hunting. Die Architektur von API Security beinhaltet „Privacy by Design“, wobei jede API-Aktivität, die für den Datenpool bestimmt ist, mit Token versehen werden kann.

Professionelles Threat Hunting zum Schutz Ihrer APIs

Die Zunahme von API-Bereitstellungen kann die IT-Sicherheitsabteilungen von Unternehmen belasten. Der API Security ShadowHunt Service entlastet Ihr Sicherheitspersonal noch heute.

Sprechen Sie mit einem Experten, um mehr zu erfahren.

 | Support | Veröffentlicht: 08/23