AKAMAI-PRODUKTBESCHREIBUNG

Akamai Hunt findet auch die am besten getarnten Bedrohungen

Ein Sicherheitsservice zur Erkennung und Beseitigung von Bedrohungen und Risiken

Nutzen Sie die Infrastruktur von Akamai Guardicore Segmentation sowie globale Bedrohungsinformationen von Akamai, um auch die am besten getarnten Bedrohungen in Ihrem Netzwerk zu stoppen.

Moderne Angriffe umgehen regelmäßig Sicherheitskontrollen

Das Hunt-Team ist sich bewusst, dass Sicherheitsverletzungen in jeder Umgebung und zu jeder Zeit vorkommen können. Daher sucht das Team ständig nach anomalem Angriffsverhalten und fortschrittlichen Bedrohungen, die selbst die modernsten Sicherheitslösungen immer wieder überwinden. Das Erkennen von Techniken wie laterale Netzwerkbewegungen, die Ausführung von Malware und die Kommunikation mit Command-and-Control-Servern zu einem frühen Zeitpunkt in der Angriffskette kann eine Katastrophe verhindern, selbst wenn die Sicherheitskontrollen versagen. Mit Hunt werden Sie sofort über alle kritischen Vorfälle in Ihrem Netzwerk informiert und unsere Experten arbeiten eng mit Ihrem Team zusammen, um gefährdete Assets zu beseitigen und schnell zu reagieren.

Der Hunt-Prozess

Sammeln	Analysieren	Untersuchen	Benachrichtigen	Abwehren
Hunt **sammelt einzigartige Signale** von verschiedenen Quellen	Die Plattform **analysiert diese Daten** mit einer Vielzahl von Erkennungs-algorithmen	Experten **untersuchen jedes verdächtige Ereignis**, um False Positives zu minimieren	Die Plattform sendet **detaillierte Warn-meldungen** über die Bedrohung und die zu ergreifenden Maßnahmen	Das Hunt-Team hilft bei der **Eindämmung der Bedrohung**

Wichtige Funktionen

Fachkundige menschliche Analyse rund um die Uhr

Unsere Cybersicherheitsprofis stammen aus verschiedenen Bereichen wie Sicherheitsforschung, offensive Sicherheit, militärische Aufklärung, Red Teams, Incident Response und Data Science.

Benachrichtigung bei echten Bedrohungen

Um Ermüdungserscheinungen bei häufigen Warnmeldungen zu vermeiden, warnt das Hunt-Team seine Kunden nur vor echten Bedrohungen und vermeidet so False Positives. Unsere Experten verfügen über Daten aus einem globalen Kundenstamm und erhalten so die Grundlage für eine „gesunde“ Rechenzentrums- und Cloudanwendungskommunikation aufrecht, was uns dabei hilft, die schwerwiegendsten Bedrohungen zu erkennen.

Proprietäre Tools für die Bedrohungssuche

Die Hunt-Experten entwickeln routinemäßig fortschrittliche Algorithmen zur Bedrohungsbekämpfung wie Anomalien bei der Nutzer- und Netzwerkaktivität, ausführbare Analysen, Log-Analysen und mehr, um ein leistungsstarkes Toolset für eine schnelle Detektion und Reaktion aufzubauen. Akamai Guardicore Insight, ein leistungsstarkes und osquery-basiertes Tool zur Abfrage von Endpunkten und Servern in Echtzeit, ist ohne zusätzliche Kosten im Service inbegriffen.

VORTEILE FÜR IHR UNTERNEHMEN

Laufende Angriffe aufdecken
Das Team von Guardicore Hunt sucht proaktiv nach laufenden und sich ankündigenden Angriffen. Dadurch wird die Verweildauer minimiert und die Zeit bis zur Schadensbegrenzung verkürzt.

Neue Möglichkeiten für Ihr Team
Die Experten von Guardicore Hunt arbeiten im Namen Ihres Teams an der Überwachung Ihrer Umgebung. Sie spüren potenzielle Angreifer auf und sparen Ihnen dadurch Zeit, Mühe und Kosten.

Schnelle Reaktion
Sie werden bei jedem kritischen Vorfall sofort benachrichtigt. So können Sie sich voller Vertrauen auf Ihre eigentliche geschäftliche Tätigkeit konzentrieren.

Maßgeschneiderte Bedrohungssuche
Indem das Team Ihre Umgebung kontinuierlich überwacht, entwickelt es ein grundlegendes Verständnis Ihrer Sicherheitskonfigurationen und kann seine Überwachungs-methoden an Ihre spezifische Topologie anpassen.

Akamai

Kontextbezogene Bedrohungsinformationen

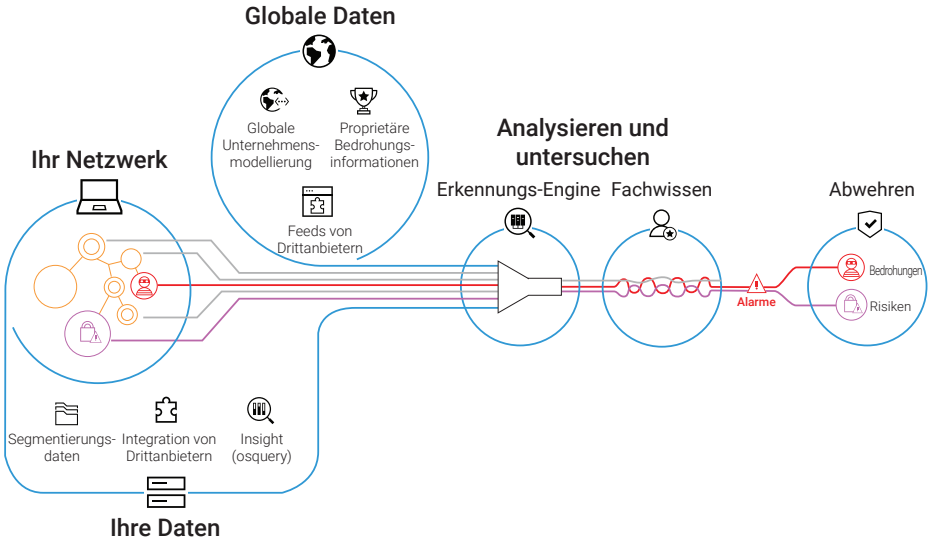
Unsere Threat Hunter sammeln Indicators of Compromise, die von IPs und Domains bis hin zu Prozessen, Nutzern und Services reichen, indem sie Akamai Guardicore Segmentation und die umfassenden globalen Bedrohungsinformationen von Akamai nutzen.

Transparenz von Netzwerken, Cloud und Endpunkten

Die Kombination aus durch Akamai Guardicore Segmentation und globale Sensoren von Akamai generierten Daten – darunter über sieben Billionen DNS-Anfragen pro Tag an die Akamai DNS-Cloud – bietet unserem Team einen umfassenden Überblick über Ihre Umgebung.

Sofortige Benachrichtigung und proaktive Einblicke

- E-Mail-Benachrichtigungen zu Bedrohungen werden sofort gesendet, nachdem eine Bedrohung erkannt wurde.
- Regelmäßige Berichte über Bedrohungen auf Führungsebene mit Analysen, Statistiken und Metriken, damit Ihre Führungskräfte oder Vorstandsmitglieder in Bezug auf maßgebliche Angriffe immer auf dem neuesten Stand sind.
- Das Vorfallmanagement ist dank der Integration in die Akamai Guardicore Segmentation-Konsole denkbar einfach.



> Ich möchte mich ganz herzlich beim Team von Akamai Hunt dafür bedanken, dass sie uns bei der Bekämpfung des Datendiebstahls und der schnellen Wiederherstellung der Daten unterstützt haben. Das hat uns dabei geholfen, alle Angriffe auf unsere geschäftskritischen Systeme zu verhindern.
>
> **CIO**
> Führendes Gesundheitszentrum

Wenn Sie mehr über Akamai Hunt und unsere anderen Sicherheitslösungen erfahren möchten, wenden Sie sich an einen unserer Experten.