Akamai-Partnerbericht

Apiiro stellt vollständige API-Sicherheit von Code bis Laufzeit bereit

Das Unternehmen nutzte API Security, um sicherzustellen, dass Kundenantworten auf API-Warnungen so nahtlos wie möglich verliefen.

Strategisch reduziertes Risiko

Schnellere Behebung

Zeitersparnis für Entwickler

Kontextbezogene Verbesserung der Anwendungssicherheit

Apiiro ist eine ASPM-Plattform (Application Security Posture Management) und stellt Teams für Anwendungssicherheit und -entwicklung die nötigen Einblicke bereit, um Anwendungen sicher in der Cloud bereitzustellen. Um das Ökosystem des API-Schutzes zu vervollständigen – von Bedrohungserkennung und Warnungen mithilfe von Verhaltensanalysen bis hin zu API-Management und Bedrohungsabwehr – hat sich Apiiro mit Akamai zusammengetan. API Security verbindet die Leistungsfähigkeit der Apiiro-Plattform mit der Laufzeit von Akamai und ermöglicht es Unternehmen, APIs nahtlos vom Code bis zur Produktion zu schützen.

Erweiterung des API-Schutzes

Anwendungs- und Entwicklungsteams müssen API-Sicherheitskontrollen validieren, bevor sie in der Cloud bereitgestellt werden. Apiiro verwendet tiefgreifende Codeanalysen und Laufzeitkontext, um die Codebasis eines Unternehmens zu scannen, sie mit Kontext anzureichern und alle APIs im Code zu erkennen. So können Entwickler Risiken priorisieren und beheben, bevor sie Code in der Cloud bereitstellen.

apiiro

Boston, Massachusetts, USA

apiiro.com

Branche

Hightech

Lösung

Akamai API Security

Akamai

Idan Plotnik, Mitgründer und CEO von Apiiro, erklärt: „Da APIs exponentiell schneller entwickelt und veröffentlicht werden, erweitert sich die Angriffsfläche kontinuierlich. Es reicht nicht aus, dass Unternehmen ihre APIs im Code schützen. Für den Fall, dass es zu einem Vorfall kommt, sollten sie auch die Behebung beschleunigen."

Verbesserung der Selektierung

Apiiro nutzte die offene API in Verbindung mit Akamai API Security, um Unternehmen einen Echtzeitbestand der APIs in Code und Laufzeit bereitzustellen und gleichzeitig zu verhindern, dass Bedrohungen eskalieren.

Die Kombination aus API Security und der Apiiro-Plattform ermöglichte es Unternehmen, von Akamai erkannte Laufzeit-API-Risiken mit API-Code zu verknüpfen. Apiiro bot Sicherheitsteams umfassende Einblicke in den Codekontext: die Ursache, das Code-Repository, die spezifische Codezeile und den Codeeigentümer. So konnten Sicherheitsteams genau das Problem identifizieren, das eine Sicherheitswarnung ausgelöst hat, und mussten nicht unzählige Risikowarnungen bewerten. Außerdem musste der verantwortliche Entwickler nicht identifiziert oder kontaktiert werden.

„Durch die Kombination von Laufzeit-Risikoerkennung mit detaillierter Transparenz auf Code-Ebene ermöglichen Apiiro und Akamai es Unternehmen, API-Sicherheitsbedrohungen schnell zu identifizieren, zu priorisieren und zu bekämpfen", so Plotnik.

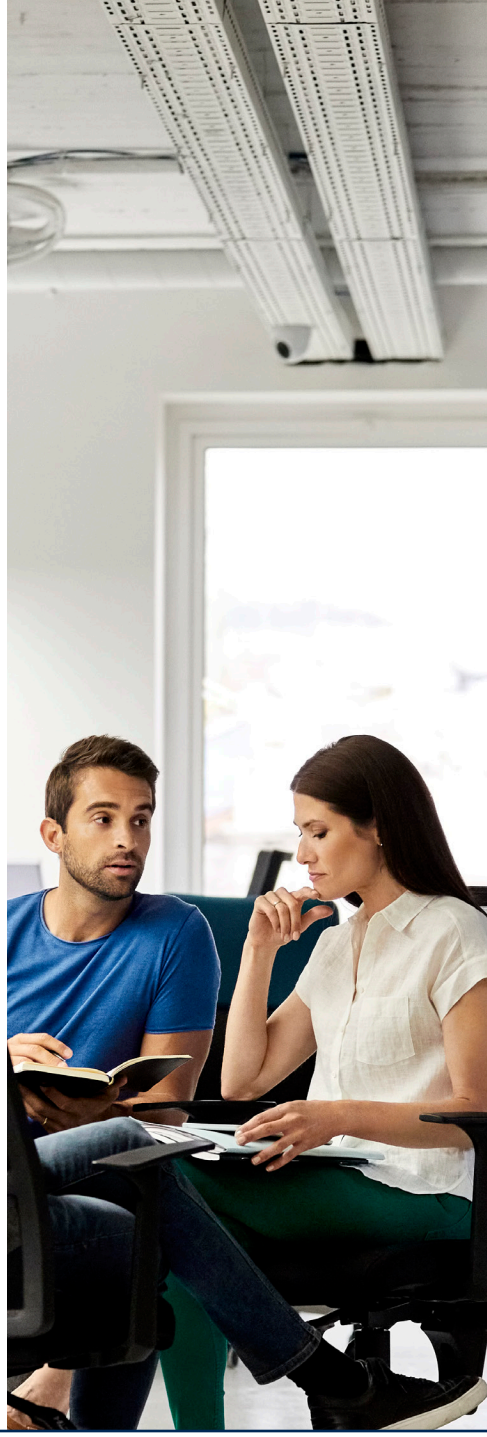
> Jedes Unternehmen, das Software entwickelt oder Software von Drittanbietern verwendet, benötigt API-Sicherheit – sowohl im Code als auch in der Laufzeit. Und unsere Partnerschaft mit Akamai gibt ihnen genau das.
>
> – Idan Plotnik
> Mitgründer und CEO, Apiiro

Schnelle Behebung

Apiiro leitete Warnungen und risikobasierten Kontext an den jeweiligen Codeeigentümer weiter – zusammen mit praktischen Behebungsempfehlungen, die von API Security vorgeschlagen wurden. Dank der Verbindung zwischen Apiiros tiefgreifendem Wissen über Code und den Einblicken in API-Verhalten und -Bedrohungen in der Laufzeit von API Security konnten Entwickler die Wahrscheinlichkeit und die Auswirkungen eines Risikos genauer bestimmen. Und so konnten sie geschäftskritische API-Risiken priorisieren.

Hierzu Plotnik: „Mit der Kombination von Akamai und Apiiro können Unternehmen Risiken strategisch reduzieren und gleichzeitig wertvolle Zeit sparen und ihre SLAs erfüllen.“ Sicherheitsteams haben weniger Zeit damit verbracht, die richtigen Entwickler zu finden und dringende Korrekturen anzufordern. Darüber hinaus konnten Entwickler Probleme schneller beheben, indem sie klare Einblicke in API-Bedrohungen erhielten.

„Indem wir die Erkenntnisse aus der tiefgreifenden Codeanalyse von Apiiro mit den Erkenntnissen zur Laufzeit-API-Sicherheit von Akamai API Security kombinieren, bieten wir Kunden den nötigen Kontext, um wichtige API-Risiken zu priorisieren, zu beheben und zu verhindern“, so Plotnik.



apiiro

Apiiro unterstützt Teams für Anwendungssicherheit und -entwicklung von Unternehmen wie Morgan Stanley, Rakuten, SoFi und Colgate dabei, die Transparenz, Priorisierung, Bewertung und Behebung von Anwendungsrisiken zu vereinheitlichen. So können sie Zeit bei der Selektierung von Sicherheitsergebnissen und der Behebung realer Risiken sparen und sichere Anwendungen in der Cloud bereitstellen. Das Unternehmen wird von Greylock, Kleiner Perkins und General Catalyst unterstützt.

| Veröffentlicht: August 2024

Akamai