Akamai

WHITEPAPER

Kritische Überlegungen zu API-Sicherheit und PCI DSS v4.0-Konformität

Einführung

Die Notwendigkeit, immer neue Vorschriften erfüllen zu müssen, kennen IT-Sicherheitsteams zur Genüge. Da hat man endlich die EU-Richtlinie zur Netz- und Informationssicherheit (NIS1) erfüllt und schon kommt NIS2. Angesichts der Tatsache, dass mehr als 130 Länder weltweit Datenschutzgesetze mit regelmäßigen Aktualisierungen erlassen haben[1], ist es nicht verwunderlich, dass nur 9 % der Führungskräfte[2] sehr zuversichtlich sind, alle Offenlegungsanforderungen erfüllen zu können.

Wenn Ihr Unternehmen die Version 4.0 des Payment Card Industry Data Security Standard (PCI DSS) einhalten muss, geht es Ihnen möglicherweise genauso. Seit 2018 muss jedes Unternehmen, das Kreditkarten wichtiger Anbieter akzeptiert und Karteninhaberdaten elektronisch verarbeitet, speichert oder überträgt, die Anforderungen gemäß PCI DSS-Version 3.2.1 erfüllen. Doch im März 2022 veröffentlichte der Payment Card Industry Data Security Council die Version 4.0 und gab Unternehmen zwei Jahre Zeit, die Einhaltung der neuen Regeln sicherzustellen. Bald darauf wurden auch schon Pläne für eine Reihe weiterer Aktualisierungen verkündet, die im März 2025 kommen sollen.

Diese Updates können eine Belastung für viel beschäftigte Sicherheitsteams darstellen, aber es steht einiges auf dem Spiel. Unter den zahlreichen Updates, die Unternehmen in PCI DSS v4.0 erfüllen müssen, gibt es auch welche, die mit API-Risiken und -Schwachstellen zusammenhängen. In diesem Whitepaper geben wir Einblicke in die Anforderungen von PCI DSS v4.0 in Bezug auf APIs, und wir zeigen, welchen Nutzen Akamai API Security in diesem Zusammenhang bietet.

1. Morrison Foerster, Catch Up on Privacy Around the World on Data Privacy Day 2021! 29. Januar 2021.
2. PwC, CEE findings from the 2023 Global Digital Trust Insights Survey

Was bleibt unverändert?

Die Anforderungen der ursprünglichen Version decken Sicherheitsgrundlagen ab, die heute genauso wichtig sind wie bei der Veröffentlichung des PCI DSS im Jahr 2006. Zum Beispiel:

- Überwachung und Kontrolle des Zugriffs auf alle Verwaltungskonten in allen IT-Systemen, die Karteninhaberdaten verarbeiten oder speichern
- Zuweisung des Zugriffs auf System- und Karteninhaberdaten auf Need-to-know-Basis und Definieren der Zugriffsanforderungen nach Rolle

Was hat sich geändert?

Die Komplexität der Bedrohungslandschaft hat gegenüber 2006, als PCI DSS erstmals in Kraft trat, exponentiell zugenommen. Unternehmen müssen zwar immer noch berücksichtigen, dass Cyberkriminelle Bereiche wie privilegierte Konten und Nutzer mit übermäßigen Berechtigungen angreifen. Sie müssen aber auch ihre Compliance-Programme anpassen, um auf Angreifer reagieren zu können, die häufig Tausende von APIs in Zahlungstechnologien ins Visier nehmen. Diese Angreifer wissen, dass APIs leicht ausgenutzt werden können und eine effiziente Möglichkeit bieten, Karteninhaberdaten zu stehlen und die digitale Infrastruktur zu attackieren.

Die Ziele von PCI DSS v4.0 bestehen darin, den Sicherheitsanforderungen der Zahlungsbranche weiterhin gerecht zu werden, die Sicherheit als kontinuierlichen Prozess zu fördern, die Flexibilität für verschiedene Methoden zu erhöhen und die Validierungsmethoden zu verbessern. Diese Version verbessert den Schutz von Zahlungsdaten durch neue Kontrollen, um die Bedrohung durch komplexe Cyberangriffe wie API-Missbrauch abzuwehren.

PCI DSS v4.0 – Allgemeiner Überblick

Aufbau und Wartung sicherer Netzwerke und Systeme	Installation und Verwaltung von Netzwerksicherheitskontrollen
	Anwendung sicherer Konfigurationen auf alle Systemkomponenten
Schutz von Kontodaten	Schutz gespeicherter Kontodaten
	Schutz von Karteninhaberdaten mit starker Kryptographie während der Übertragung über offene, öffentliche Netzwerke
Einsatz eines Programms für Sicherheitsmanagement	Schutz aller Systeme und Netzwerke vor schädlicher Software
	Entwicklung und Pflege sicherer Systeme und Software
Implementierung wirkungsvoller Maßnahmen zur Zugriffskontrolle	Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten je nach Geschäftsinformationsbedarf
	Nutzeridentifizierung und Authentifizierung des Zugriffs auf Systemkomponenten
	Beschränkung des physischen Zugriffs auf Karteninhaberdaten
Regelmäßiges Überwachen und Testen der Netzwerke	Protokollierung und Prüfung aller Zugriffe auf Karteninhaberdaten
	Regelmäßige Sicherheitstests für Systeme und Netzwerke
Durchsetzen von Informationssicherheitsrichtlinien	Unterstützung der Informationssicherheit mit Unternehmensrichtlinien und -programmen

PCI-DSS-Anforderungen für APIs

Anforderung 6: Entwicklung und Pflege sicherer Systeme und Software

PCI DSS v4.0-Anforderung 6 bezieht sich speziell auf APIs. Dieses Whitepaper behandelt zwar die einzelnen Unterabschnitte von Anforderung 6, Akamai API Security ist jedoch für viele Fälle relevant, die sich aus den PCI-DSS-Anforderungen insgesamt ergeben.

Anforderung 6 bezieht sich auf die folgenden Aspekte:

- Maßgeschneiderte und kundenspezifische Software muss sicher entwickelt werden
- Sicherheitslücken müssen identifiziert und behoben werden
- Öffentlich zugängliche Webanwendungen müssen vor Angriffen geschützt werden
- Änderungen an allen Systemkomponenten müssen sicher verwaltet werden

Anforderung 6.2.2

Diese Anforderung behandelt Schulungen für Softwareentwickler, die an maßgeschneiderter und nutzerdefinierter Software arbeiten. Diese Entwickler müssen mindestens einmal alle zwölf Monate in Bezug auf Sicherheitsaspekte, die für ihre Tätigkeit relevant sind, geschult werden. Das schließt sicheres Softwaredesign und sichere Codierungstechniken mit ein. Diese Schulung vermittelt, wie Sicherheitstesttools zur Erkennung von Software-Schwachstellen verwendet werden.

API Security kann mit Schulungen der Akamai University und Workshops zum Thema API-Sicherheit zur Erfüllung dieser Anforderung beitragen.

Akamai University

Präsenzschulungen zur Plattform sind über die Akamai University verfügbar und stehen allen Kunden von API Security zur Verfügung.

Workshops zu API Security

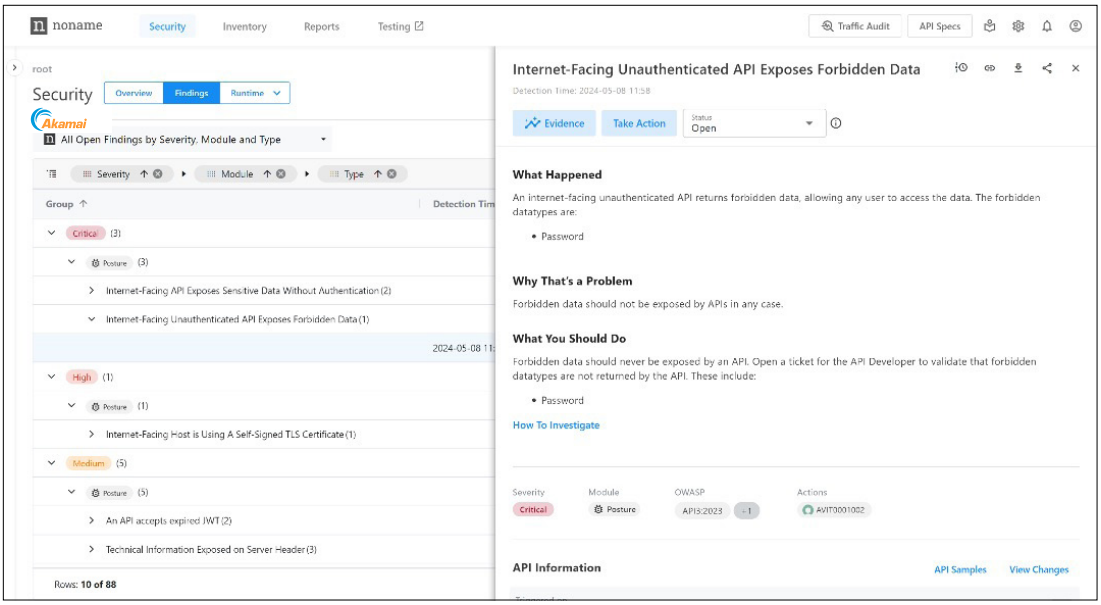
API Security führt Online- und Präsenz-Workshops zu den Funktionen der Plattform und des Active-Testing-Moduls durch und trägt gleichzeitig dazu bei, dass Kunden APIs entwickeln, die die Sicherheit vom Code bis zur Produktion gewährleisten.

Anforderung 6.2.3

Die Anforderung umfasst Überprüfungsroutinen für maßgeschneiderten Anwendungscode (das heißt für den Code, der von einem Drittanbieter entwickelt wurden und bei dem es sich nicht um gängige Standardanwendungen handelt). So ist sichergestellt, dass keine Schwachstellen in die Produktion gelangen. Konkret auf APIs bezogen, werden Unternehmen aufgefordert zu bestätigen, dass die betreffende Software die Funktionen externer Komponenten wie Bibliotheken, Frameworks und APIs sicher verwendet.

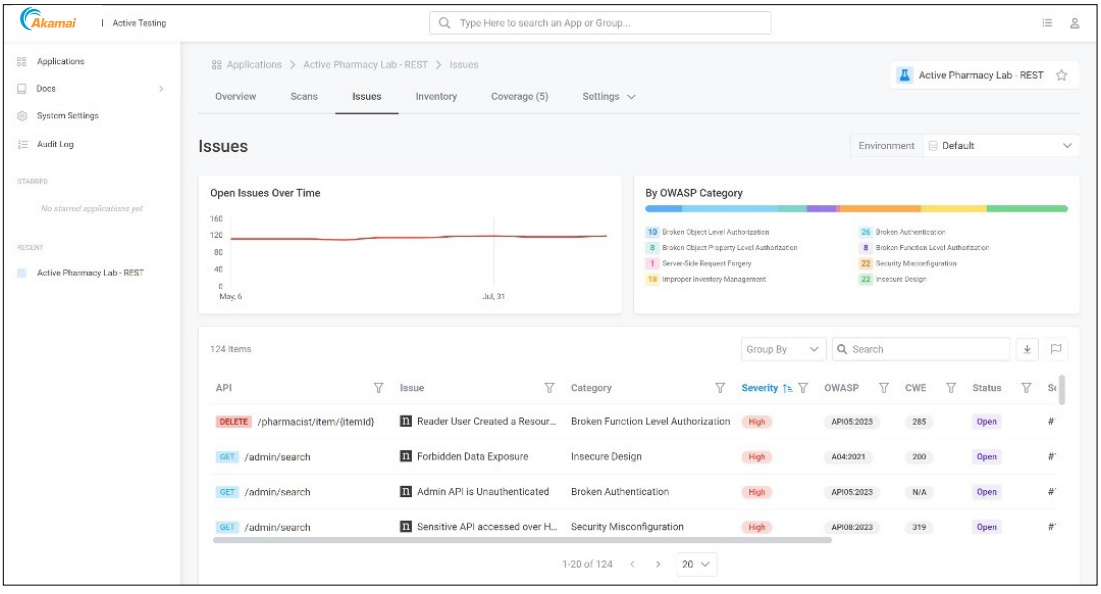
API Security erfüllt diese Anforderung auf unterschiedliche Weise:

- API Security kann bestätigen, welche API-basierten Komponenten verwendet werden und wie ihr Sicherheitsstatus ist. Unternehmen haben so die Möglichkeit, Fehlkonfigurationen zu erkennen, die Sicherheitslücken zur Folge haben könnten. Ein Beispiel wäre hier die Verwendung schwacher Verschlüsselungscodes.
- API Security kann auch überprüfen, ob APIs normal verwendet werden und sich wie erwartet verhalten. Anschließend kann die IT-Abteilung Kontrollen implementieren, um Cyberkriminelle daran zu hindern, Ihre Systeme zu missbrauchen – zum Beispiel wenn ein Angreifer das Verhalten der Anwendung testet, um Logikschwachstellen zu erkennen.
- Darüber hinaus kann API Security erkennen, welche Frameworks von Drittanbietern Funktionen für Ihre APIs bereitstellen, sodass Sicherheitsteams diese dann mit Listen veralteter und anfälliger Frameworks abgleichen können.
- API Security bietet außerdem eine vollständige Bestandsaufnahme all Ihrer APIs, einschließlich der verschiedenen Versionen, sodass Sie Einblicke in potenzielle nicht dokumentierte Funktionen und Backdoors erhalten, um die Sie sich kümmern müssen.



Auch Active Testing ist in mehrfacher Hinsicht für Anforderung 6.2.3 relevant:

- Active Testing kann die Sicherheit Ihres API-Codes prüfen und mit dazu beitragen, dass keine API-bezogenen Schwachstellen in die Produktion gelangen.
- Active Testing unterstützt auch die Implementierung von Best Practices für die sichere Codierung von APIs, mit denen Sie einen programmatischen Ansatz zur kontinuierlichen sicheren Bereitstellung von Code verfolgen können.
- Active Testing umfasst die automatisierte Codeprüfung, kann aber auch manuell verwendet werden, um gegebenenfalls erforderliche manuelle Codeprüfungen zu berücksichtigen.

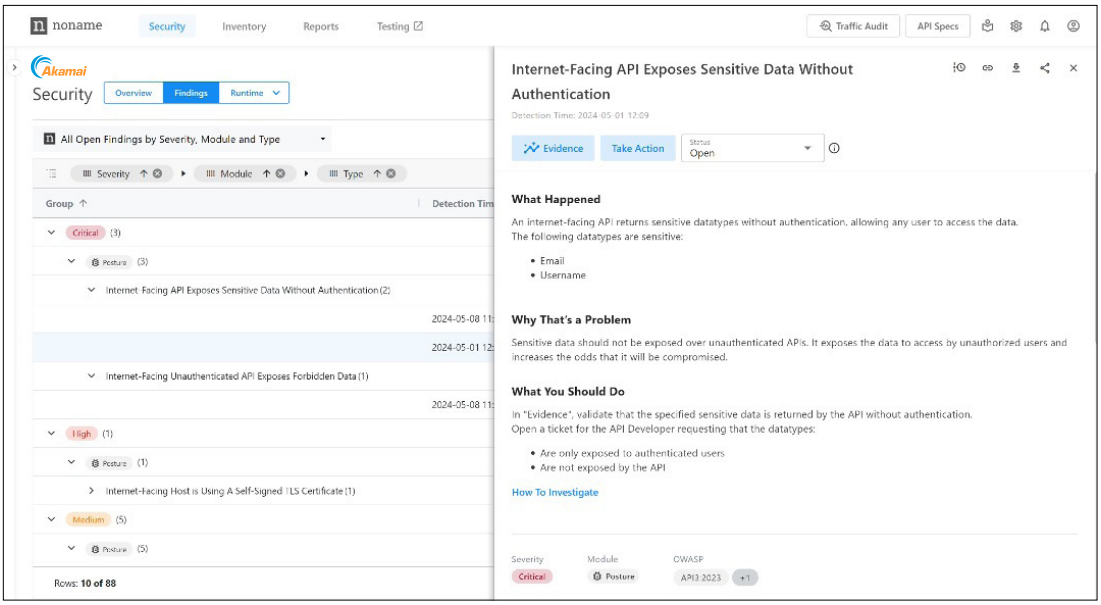


Anforderung 6.2.4

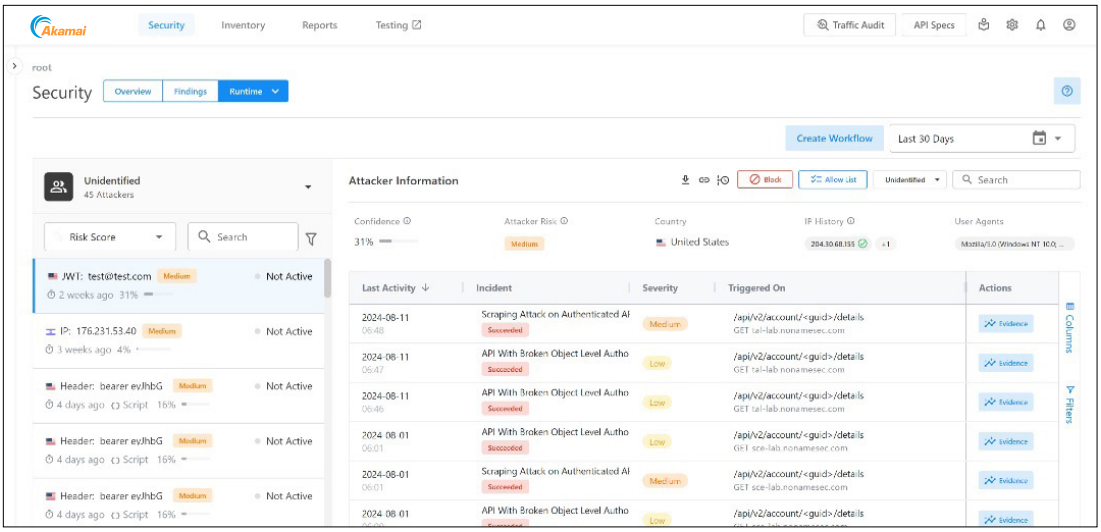
Diese Anforderung umfasst die Verwendung von Software-Engineering-Techniken oder anderen Methoden, mit denen sich verbreitete Softwareangriffe und verwandte Sicherheitsrisiken verhindern oder abwehren lassen. Die in dieser Anforderung genannten Bedrohungen reichen von relativ einfachen Injection-Attacken bis hin zu ausgefeilteren, bei der API-Geschäftslogik ansetzenden Angriffen.

API Security erfüllt diese Anforderung auf unterschiedliche Weise:

- Das Laufzeitsicherheitsmodul in der API-Security-Lösung von Akamai kann potenziell schädliche Aktivitäten erkennen, die auf die Ausnutzung der Geschäftslogik der API und ihrer unbeaufsichtigten ML-Komponente abzielen. Das Laufzeitsicherheitsmodul erkennt autonom Abweichungen vom typischen API-Verhalten und gibt bei potenziellen Angriffen Warnungen aus.
- API Security kann auch Abwehrstrategien für Injection-Angriffe ermitteln und vorschlagen, um die zugrunde liegenden Schwachstellen zu beheben.



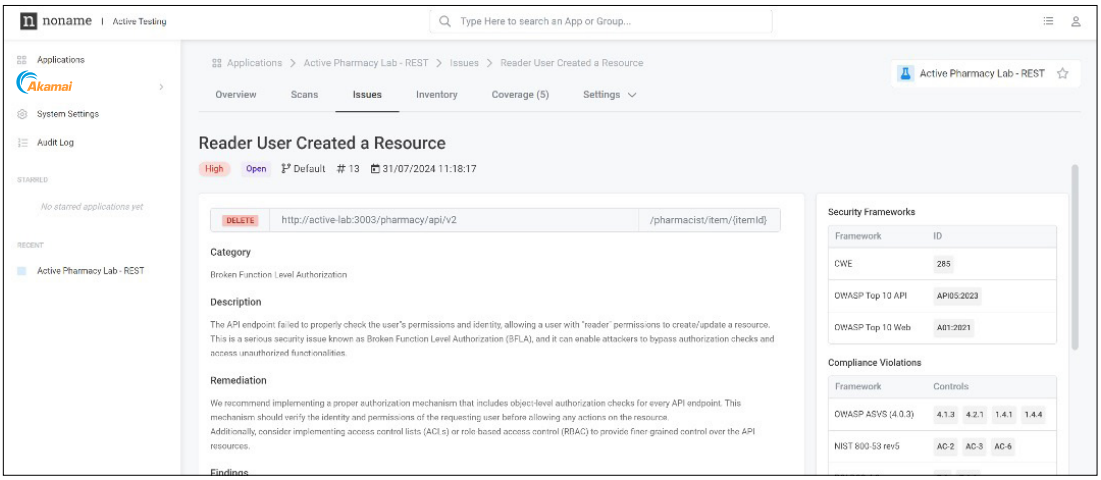
- API Security korreliert alle relevanten Aktivitäten und Aktionen und kann so die für den Angriff verantwortlichen Akteure identifizieren. Auf diese Weise können Sie den Angriff blockieren und die erforderlichen Kontrollen und Abhilfemaßnahmen implementieren, um die Ursache des Angriffs zu beheben.



- In ähnlicher Weise werden auch Injection-Angriffe erkannt. API Security bietet auch hier Anleitungen zur Problembehebung.

Auch Active Testing berücksichtigt Anforderung 6.2.4 in mehrfacher Hinsicht:

- Active Testing kann die Sicherheit Ihres API-Codes prüfen und mit dazu beitragen, dass keine API-bezogenen Schwachstellen und Fehlkonfigurationen in der Geschäftslogik in die Produktion gelangen. Fehler in der Geschäftslogik lassen sich durch Nutzung von Inline-APIs und Komponenten für die Anwendungssicherheit wie Web Application Firewalls und API-Gateways nur sehr schwer erkennen. Diese Tools arbeiten ohne Berücksichtigung des Kontexts von API-Transaktionen und sind nicht in der Lage, schädliche oder ungewöhnliche Aktivitäten einzelnen Angreifern zuzuordnen.



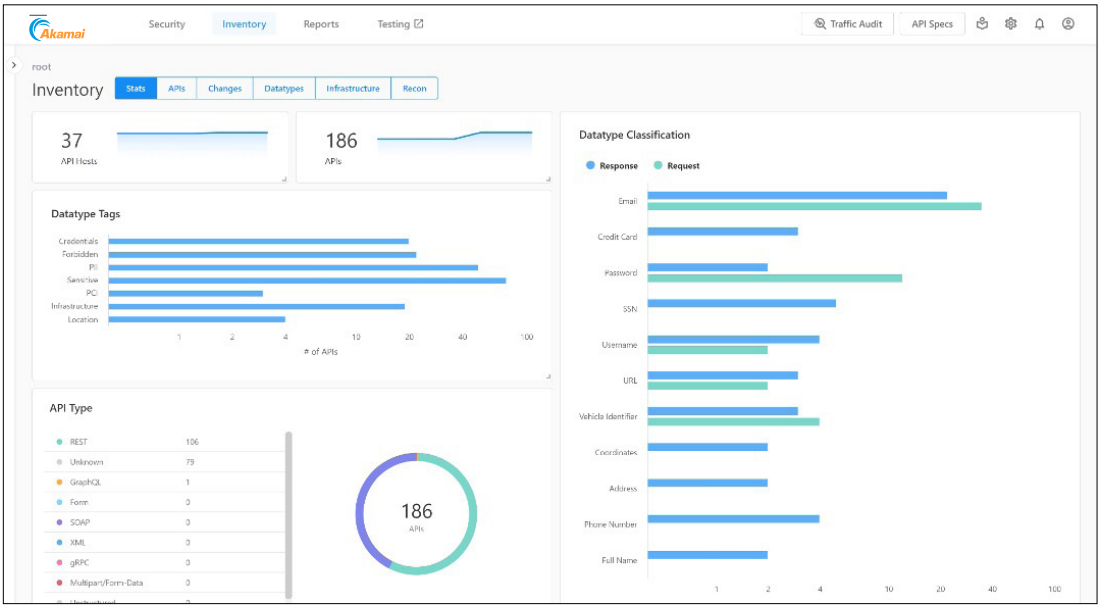
- Active Testing kann auch API-Komponenten sicher wiederverwenden, um die Entwicklung unter Einhaltung der höchsten Sicherheitsstandards zu beschleunigen.

Anforderung 6.3.2

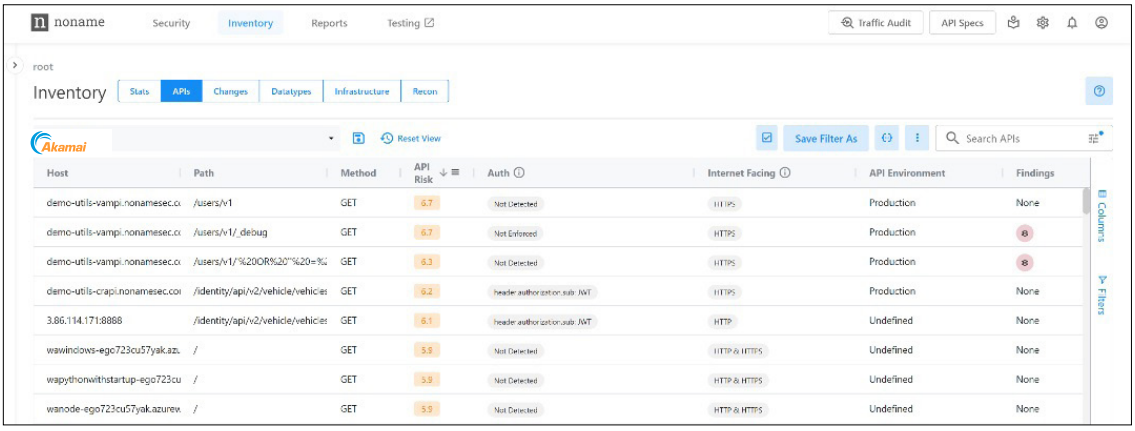
Um Schwachstellen- und Patch-Management ordnungsgemäß durchzuführen, müssen Unternehmen jetzt alle ihre maßgeschneiderten Software-Lösungen identifizieren und auflisten, einschließlich der von ihnen integrierten Software von Drittanbietern.

API Security erfüllt diese Anforderung auf verschiedene Weisen:

- API Security kann eine vollständige und umfassende Bestandsaufnahme aller APIs erstellen, einschließlich der Frameworks von Drittanbietern, die die Sicherheitslage Ihrer APIs beeinflussen können.
- API Security kann auch Veränderungen an der Funktionalität Ihrer APIs überwachen und identifizieren. Darüber hinaus kann die Lösung Ihren tatsächlichen API-Traffic mit API-Spezifikationen vergleichen und Abweichungen identifizieren, die sich auf die API-Funktionalität auswirken können.
- API Security kann die Art der Daten überwachen, die über Ihre APIs ausgetauscht werden, und Richtlinien erstellen, um speziell mit Blick auf die PCI DSS-Compliance Probleme beim Datenaustausch zu beheben.



- Mit API Security können Sie nach bestimmten Mustern suchen, etwa nach den für PCI DSS relevanten Datentypen (z. B. der 16-stelligen Kreditkartennummer), und Datenrichtlinien anwenden, um entsprechend zu reagieren.



- API Security ermöglicht Ihnen auch die Implementierung komplexer Prüfungen und Warnungen. So können beispielsweise bestimmte Daten in APIs mit bestimmten Eigenschaften zugelassen sein (z. B. intern ausgerichtet oder über bestimmte Methoden authentifiziert), in anderen dagegen unzulässig sein.

Fazit

APIs sind in modernen Anwendungsumgebungen zur Standardmethode für Konnektivität und Datenaustausch geworden. Vor diesem Hintergrund ist der Schutz von APIs sowohl aufseiten der Vorproduktion (Shift-Left) als auch der Postproduktion entscheidend, damit der Betrieb gesichert bleibt. API Security erfüllt die neuen Anforderungen von PCI DSS v4.0 und darüber hinaus durch Anwendung einer intuitiven und einfach zu implementierenden Lösung.

API Security deckt die wesentlichen Funktionen ab, die Sie benötigen, um eine API-Sicherheitsstrategie für API-Erkennung, API-Posture-Management, API-Laufzeitschutz und API-Sicherheitstests zu implementieren.

Erfahren Sie, wie Sie sich vor den OWASP API Security Top 10 schützen können**.**

Erfahren Sie, wie wir Sie unterstützen können, und vereinbaren Sie eine individuelle Demo zu Akamai API Security**.**