noname

PCI DSS 4.0 Requirements for APIs

The PCI Security Standards Council (PCI SSC)

The PCI Security Standards Council (PCI SSC) is a global forum that brings together the stakeholders of the payments industry to develop and drive adoption of data security standards and resources for safe payments worldwide.

The PCI SSC mission is to enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders. PCI SSC achieves this with a strategic framework to guide the decision-making process and ensure that every initiative is aligned with the PCI SSC mission and supports the needs of the global payments industry.

The four pillars of the PCI SSC strategic framework are:

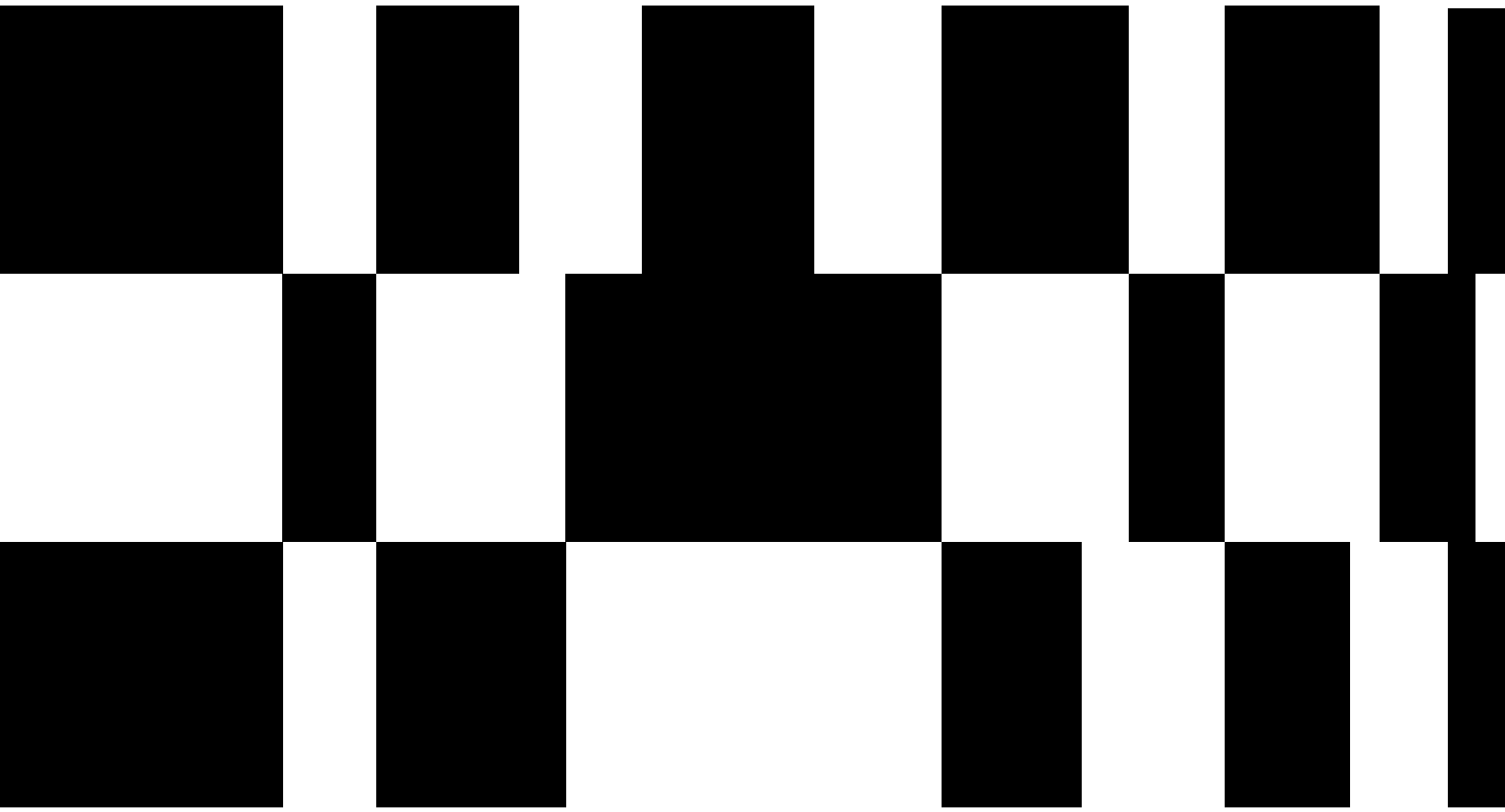
1. Increase industry participation and knowledge in the PCI Standards development process and stakeholder support for standards implementation. This ensures that standards and resources reflect and address industry needs and challenges.
2. Evolve security standards and validation programs to support a range of environments, technologies and methodologies for achieving security. This ensures standards and resources that support and enable safe commerce and the flexibility to use different approaches to meet those standards.
3. Secure emerging payment channels via development of PCI Standards and resources to support broader payment acceptance. This enables safe commerce in new and emerging card and card-based payment channels such as mobile and internet-of-things.

4 Increase standards alignment and consistency of PCI Standards to minimize redundancy and support effective implementation.

The PCI SSC covers 15 different PCI security standards and specifies where they apply to the payment process. For the topic of PCI DSS 4.0 pillar 2 and 4 stand out specifically as a driving factor for this new standard and its requirements. All organizations that are covered by PCI DSS 4.0 must comply with the new standards by March 31, 2024. A new addition to the standard as compared to the 3.x one is the inclusion of APIs. (The changes between v3.2.1 and 4.0 are outlined here:

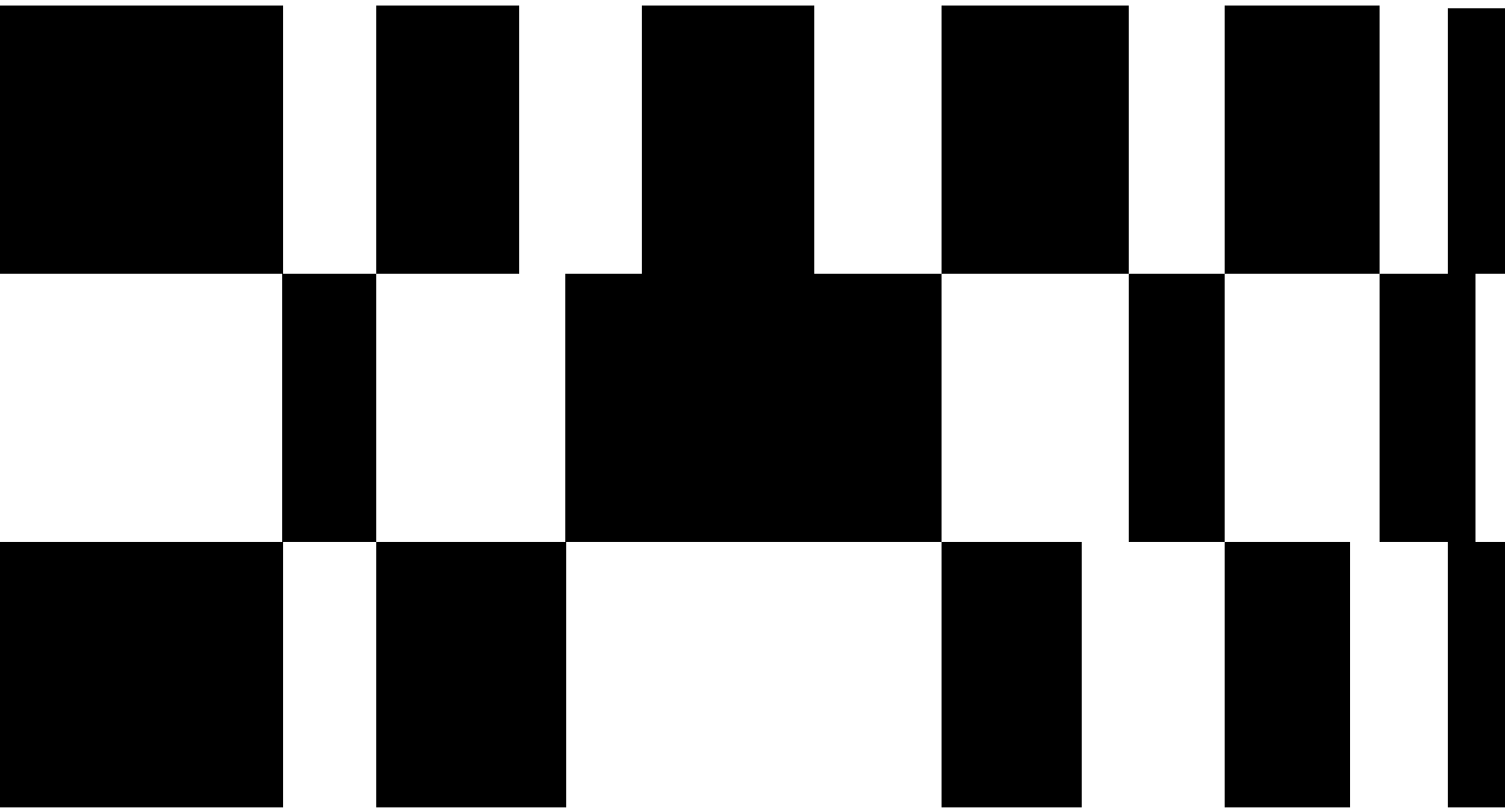
Learn more

The rest of this whitepaper covers the implications of the PCI DSS 4.0 standard on the usage of APIs and how Noname Security addresses these specifically.



The PCI Data Security Standard (PCI DSS)

The PCI Data Security Standard (PCI DSS) is a global standard that provides a baseline of technical and operational requirements designated to protect payment data. PCI DSS v4.0 is the next evolution of the standard. The goals of this new standard are to continue to meet the security needs of the payment industry, promote security as a continuous process, add flexibility for different methodologies, and enhance the validation methods. Development of PCI DSS v4.0 was driven by industry feedback. This version furthers the protection of payment data with new controls to address sophisticated cyber attacks like API abuse.

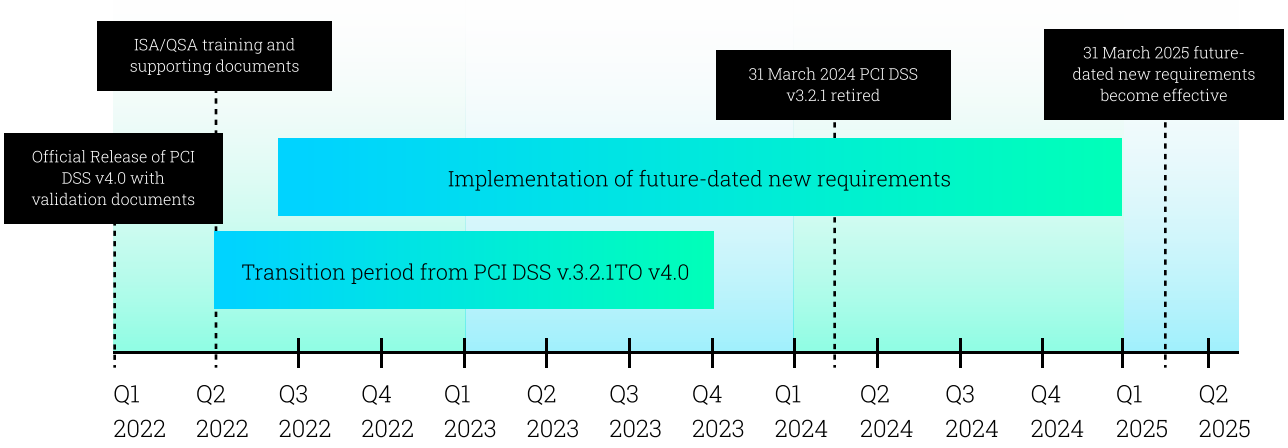


PCI Data Security Standard - High Level Overview

Build and Maintain a Secure Network and Systems	Install and Maintain Network Security Controls
	Apply Secure Configurations to All System Components
Protect Account Data	Protect Stored Account Data
	Protect Cardholder Data with Strong Cryptography During Transmission over Open, Public Networks.
Maintain a Vulnerability Management Program	Protect all Systems and Networks from Malicious Software
	Develop and Maintain Secure Systems and Software
Implement Strong Access Control Measures	Restrict Access to System Components and Cardholder Data Business Need to Know
	Identify Users and Authenticate Access to System Components
	Restrict Physical Access to Cardholder Data
Regularly Monitor and Test Networks	Log and Monitor All Access to System Components and Cardholder Data
	Test Security of Systems and Networks Regularly
Maintain an Information Security Policy	Support Information Security with Organizational Policies and Programs

Implementation Timeline

PCI DSS v3.2.1 will remain active for two years after v4.0 is published. This provides organisations time to become familiar with the new version, and plan for and implement the changes needed.



PCI DSS Requirements for APIs

Requirement 6: Develop and Maintain Secure Systems and Software

PCI-DSS 4.0 requirement 6 specifically calls out APIs and in the sub sections below we'll address these one by one. However this does not mean Noname Security's platform does not fully or partially address some of the other PCI-DSS requirements, in fact Noname Security is relevant in many cases of the overall standard.

In general, requirement 6 addresses the following sections;

- Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.
- Bespoke and custom software are developed securely
- Security vulnerabilities are identified and addressed
- Public-facing web applications are protected against attacks
- Changes to all system components are managed securely

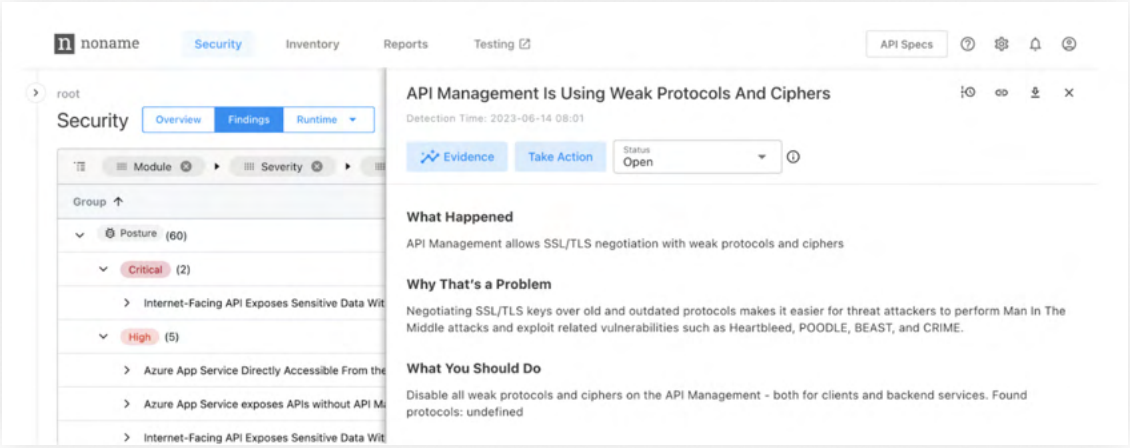
Requirement 6.2.3

This requirement touches on the practice of reviewing your bespoke (i.e. developed by a third party vendor - but not standard COTS applications) custom application code to ensure no vulnerabilities are released into production. Specifically on APIs it states as guidance to confirm that software securely uses external components' functions (libraries, frameworks, APIs, etc).

Noname Security addresses this in a number of ways:

Noname Security Core Platform:

- Using the Core Platform we can confirm the usage of API based components and their security posture (e.g. find any misconfigurations leading to vulnerabilities, including the usage of weak encryption ciphers as called out in the standard).
- Using the Core Platform we can validate normal and expected behavior of API usage and implement controls to block suspicious actors from abusing your systems. (e.g. checking the application's behavior to detect logical vulnerabilities).



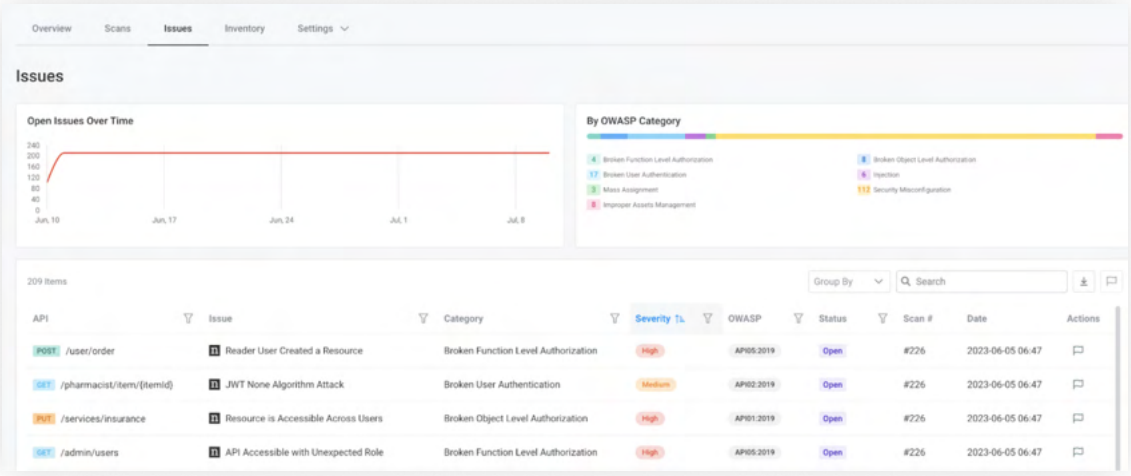
(example of weak cipher usage detection)

Additionally, Noname Security has the capability to detect third party frameworks used to power your APIs which you can then match to outdated and vulnerable.

Noname Security also provides a full inventory of all your APIs, including the different versions of APIs you are running thus giving you insight into potential undocumented features and backdoors you need to manage.

Noname Active Testing

- Using Noname Active Testing we can validate the security of your API code and help you avoid putting any API related vulnerabilities into production.
- Using Noname Active Testing we can implement secure coding best practices for APIs allowing you to adopt a programmatic approach to securely deliver code on a continuous basis.



(example of security vulnerabilities detected during API development)

The added benefit of using Noname Active Testing for this requirement is that it addresses the automated code review method but can also be used manually for addressing any manual code review requirements you have.

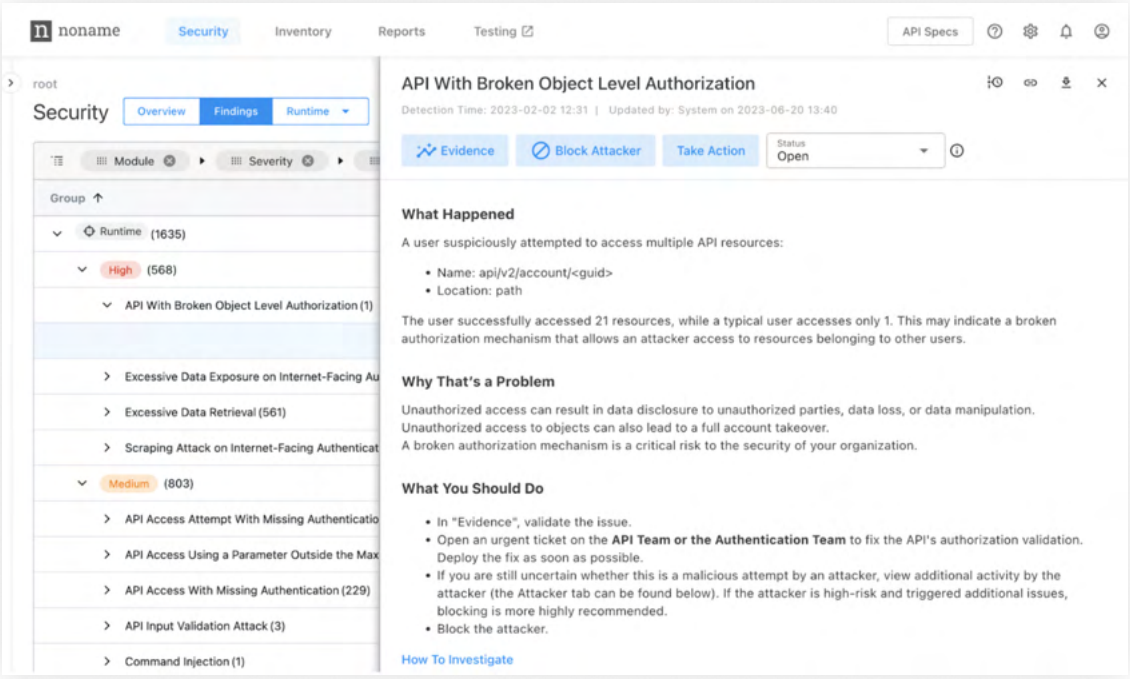
Requirement 6.2.4

This requirement touches on using software engineering techniques or other methods, to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software. The attacks called in this requirement range from relatively straightforward injected based attacks to more sophisticated API business logic based attacks.

Noname Security addresses this in a number of ways;

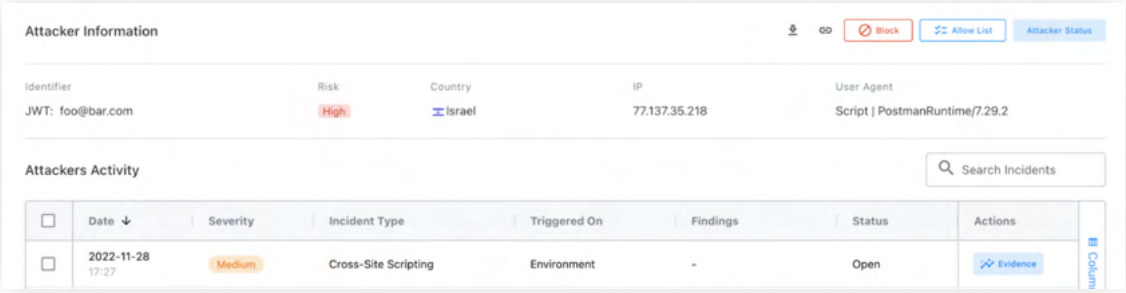
Noname Security Core Platform:

- Using the Core Platform we can leverage our Runtime Security module, which relies on unsupervised online machine learning to identify potential malicious behaviour targeting misuse of the API business logic.
- Using the Core Platform we can also detect injection attacks and guide you on any mitigation techniques needed to address the root cause of these vulnerabilities.

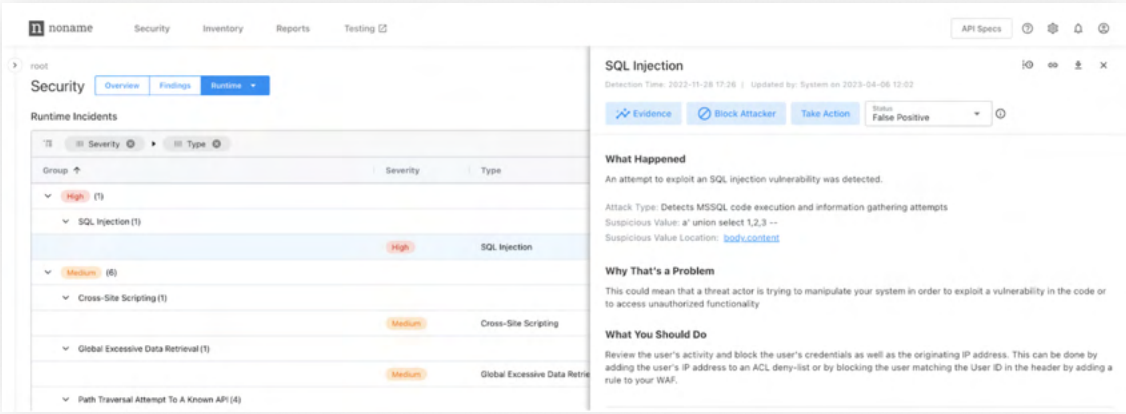


(detection of sophisticated BOLA attack using our ML model)

Noname will automatically identify the attacker responsible for this attack by correlating all relevant transactions, this will allow you to block the attack and implement necessary remediation to address the root cause.

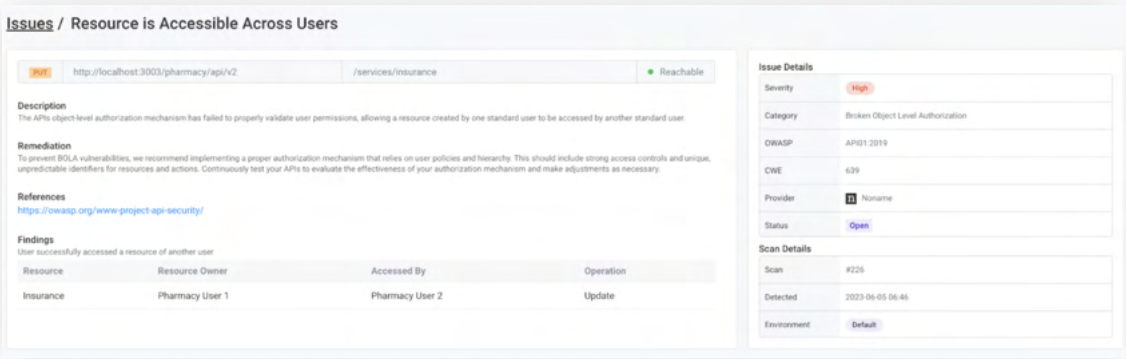


Injection based attacks are similarly detected and the Noname Platform will provide guidance to remediate the issues.



Noname Active Testing

- Using Noname Active Testing we can validate the security of your API code and help you avoid putting any API related vulnerabilities into production, these uniquely include business logic vulnerabilities.



These logic based flaws are next to impossible to detect using inline, transactional focused security tools like Web Application Firewalls and API Gateways as the historical transactions need to be understood in context and linked to individual attackers over an extended period of time.

Noname Security Active Testing also allows for the secure re-use of API components to speed up development whilst maintaining the highest security standards.

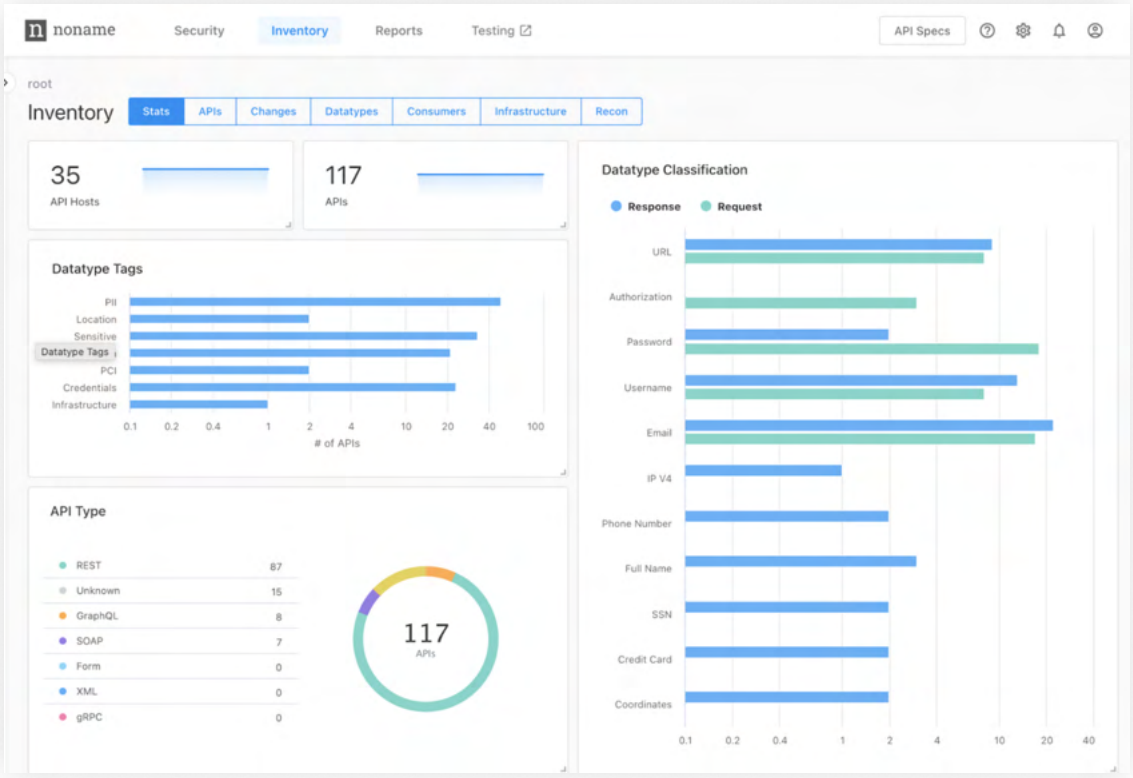
Requirement 6.3.2

This requirement applies to maintaining an inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software, to facilitate vulnerability and patch management.

Noname Security addresses this in a number of ways;

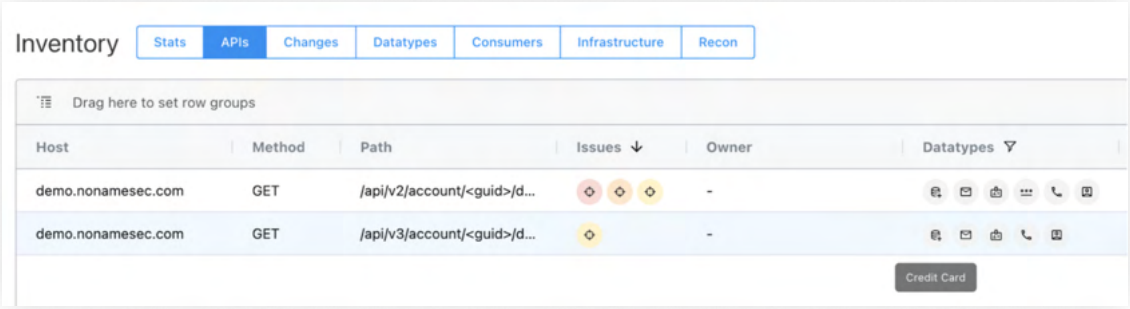
Noname Security Core Platform:

- Using the Core Platform we can create a full and extensive inventory of all your APIs, including the third party frameworks and infrastructure components influencing the security posture of your APIs.
- Using the Core Platform we can monitor and list any changes to functionality of your APIs, the system can also validate your documented functionality with the usage reality detected on the network.
- Using the Core Platform we monitor the type of data being exchanged across these APIs and create policies to address any data exchange concerns specifically for PCI-DS.



(high level inventory of all APIs including datatype classification)

Noname Security allows you to look for specific patterns, like the PCI-DSS relevant data types (e.g. the 16 digit credit card number) and apply data policies to respond to these detections.



Noname Security also allows you to implement complex validation and alerting, for example certain data might be allowed on APIs with specific properties (e.g. internal facing, authenticated using specific policies) but disallowed on others.

Requirement 6.2.2

This requirement addresses training for software development personnel working on bespoke and custom software. It states these developers need to be trained at least once every 12 months on security relevant to their job function, including secure software design and secure coding techniques. This includes security testing tools, and how to use those tools for detecting vulnerabilities in software.

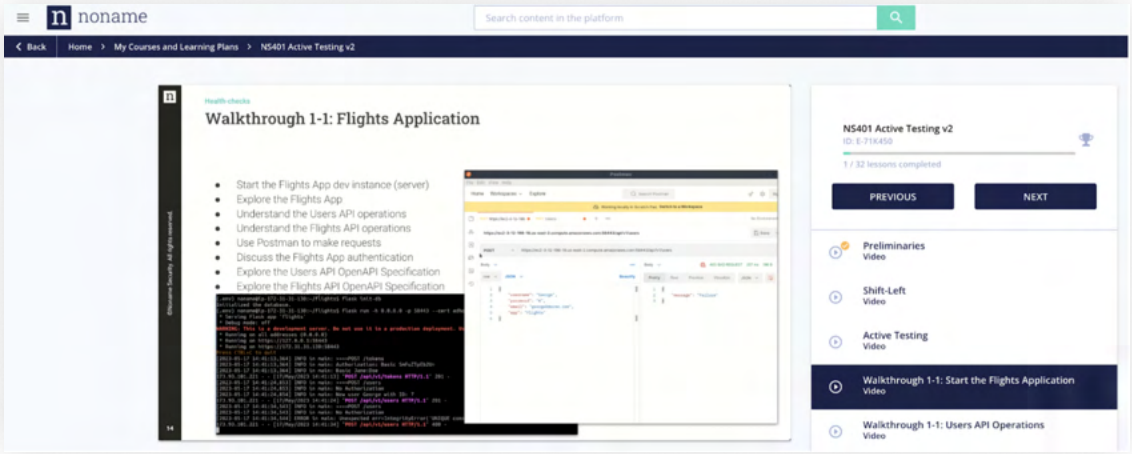
Noname Security can alleviate this in a number of ways;

Noname Security LMS

- The Active Testing platform is very intuitive and highly automated, remote.However, in-person training on the platform is available through Noname's Learning Management System (LMS) and accessible to all Noname Security customers.

Noname Security Workshops

- Noname Security runs online and in-person workshops going over the capabilities of the core platform and the active testing module. (https://events.nonamesecurity.com/workshop)



Conclusion

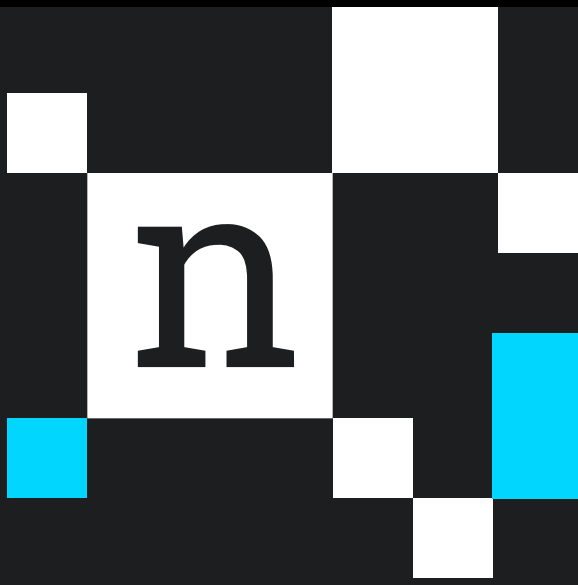
APIs have become the default connectivity and data exchange method of modern application environments. With that in mind securing APIs from both a pre-production (shift-left) and post-production (shield-right) is paramount to securely operating in our digital first world. Noname Security's comprehensive platform addresses the new PCI-DSS 4.0 requirements and beyond using an intuitive and straightforward to implement solution.

Noname Security's Platform covers the critical capabilities you need to implement an API security strategy across API Discovery, API Posture Management, API Runtime Protection, and API security testing.

To learn more about how Noname Security simplifies various compliance requirements please visit: https://nonamesecurity.com/solutions/simplify-compliance/

About Noname Security

Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope across four pillars — Discovery, Posture Management, Runtime Security, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, California, and offices in London.



nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371