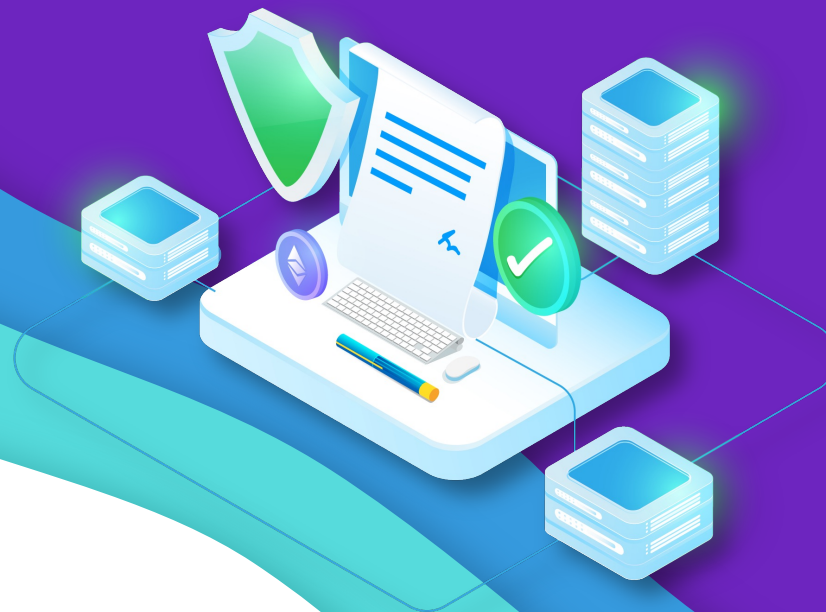


# 没有未经测试的API:API安全左移

By: 伏学民



# CONTENTS

## 目录



API安全现状

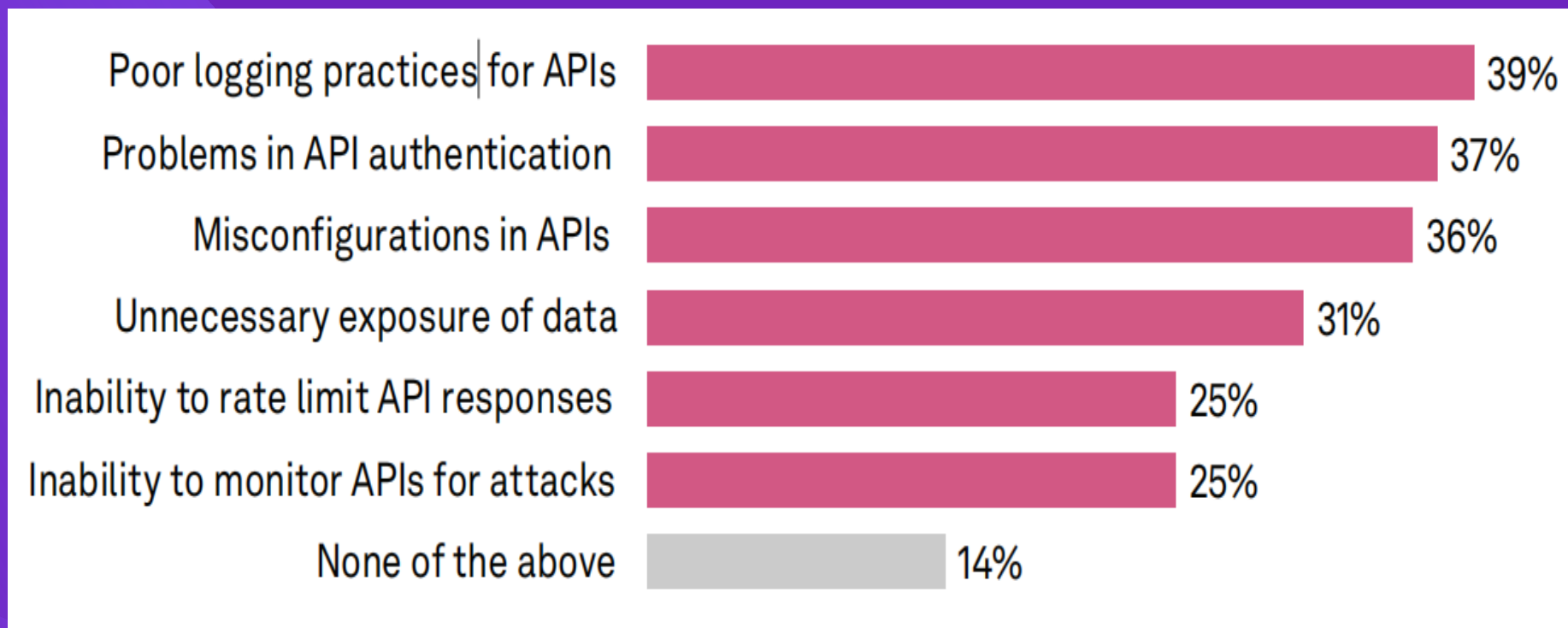
OWASP Top 10 API Security Risks

The Noname API Security Platform



01

# API安全现状



- Average number of Production Enterprise APIs 15564
- 63% of organizations experienced a security breach in the past year
- 37 days-per incident
  - 27 days for discovery
  - 10 days for remediation



02

## OWASP Top 10 API Security Risks





1. Broken Object level Authorization
2. Broken User Authentication
3. Excessive Data Exposure
4. Lack of Resources & Rate Limiting
5. Broken Function Level Authorization



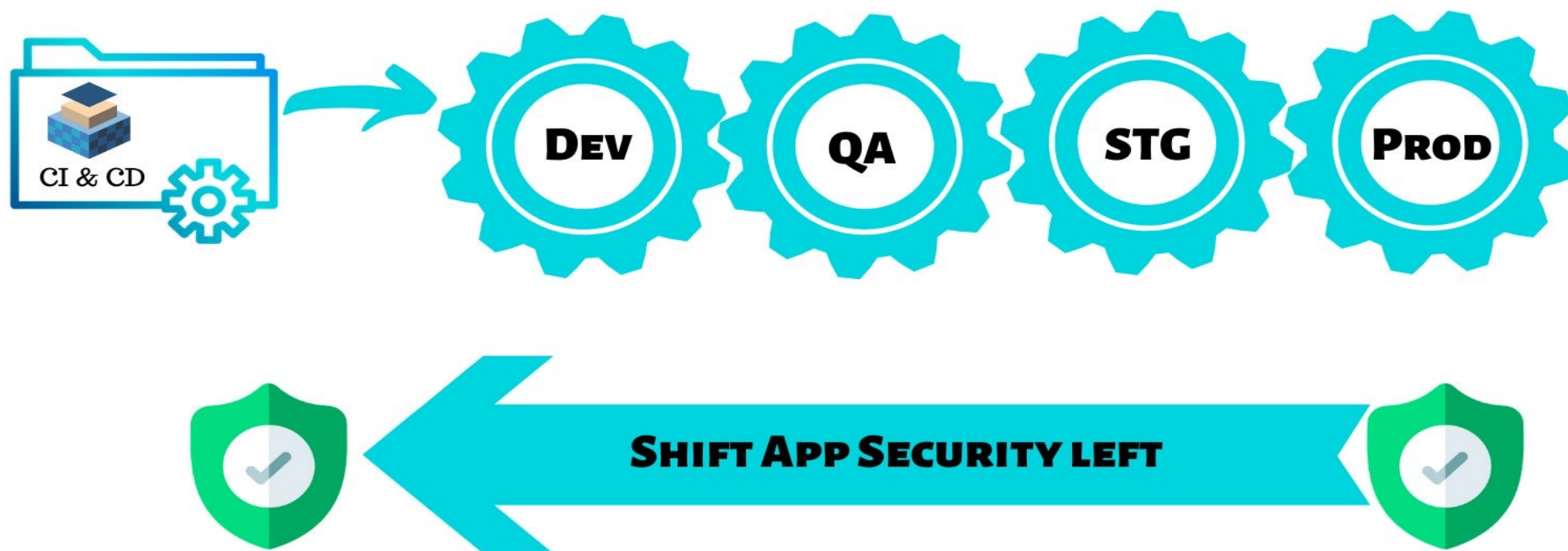
6. Mass Assignment
7. Security Misconfiguration
8. Malicious Code Injections
9. Improper Assets Management
10. Insufficient Logging & Monitoring



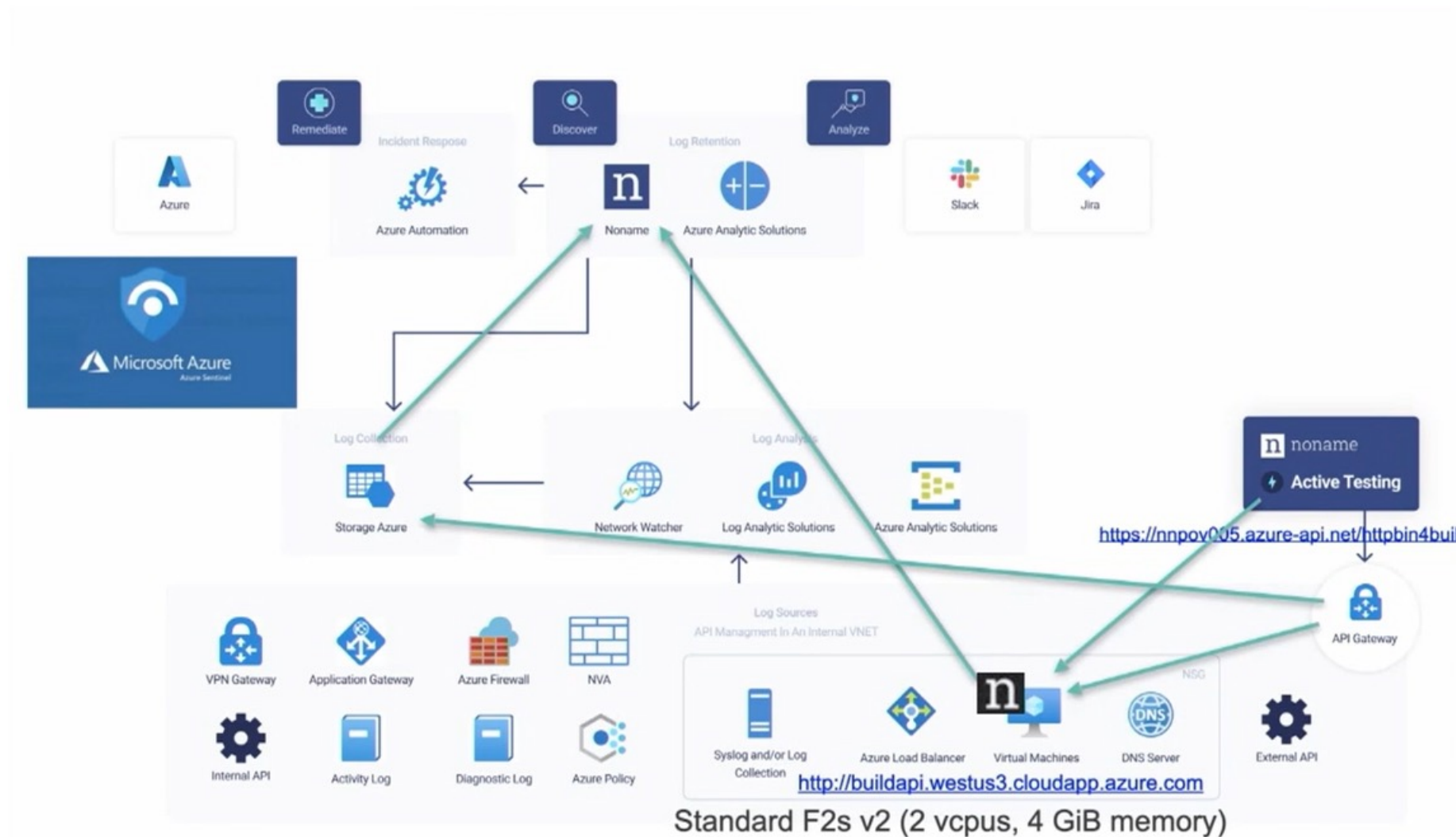


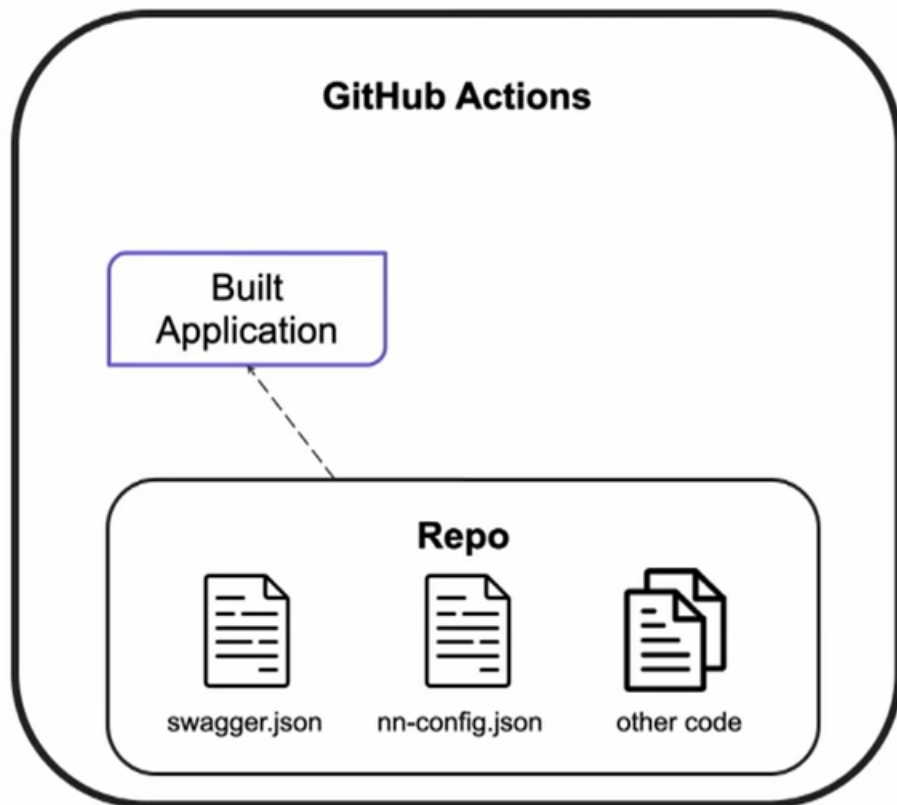
03

## The Noname API Security Platform



# API安全左移 Azure DevOps CI/CD pipelines



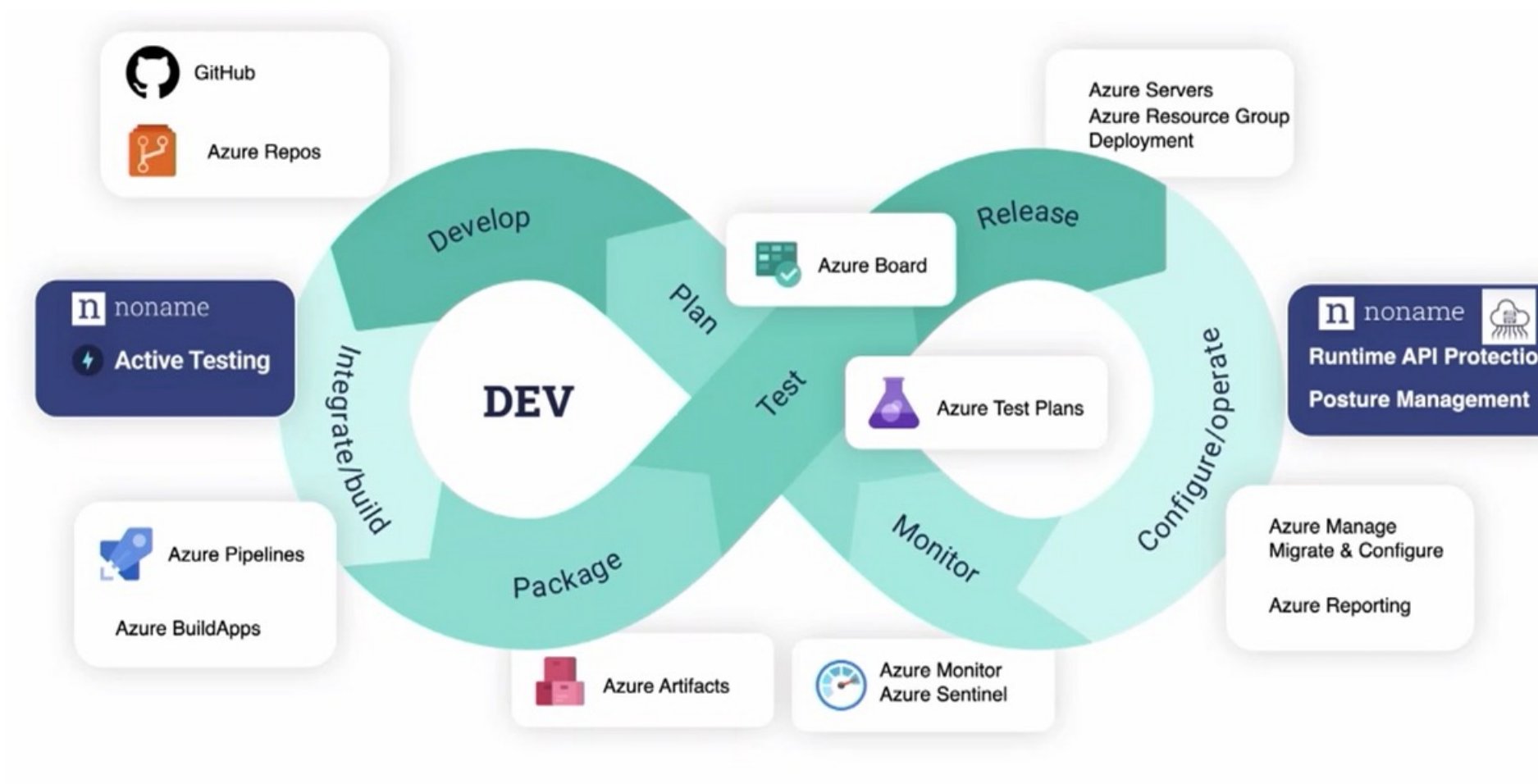


JFROG Repo

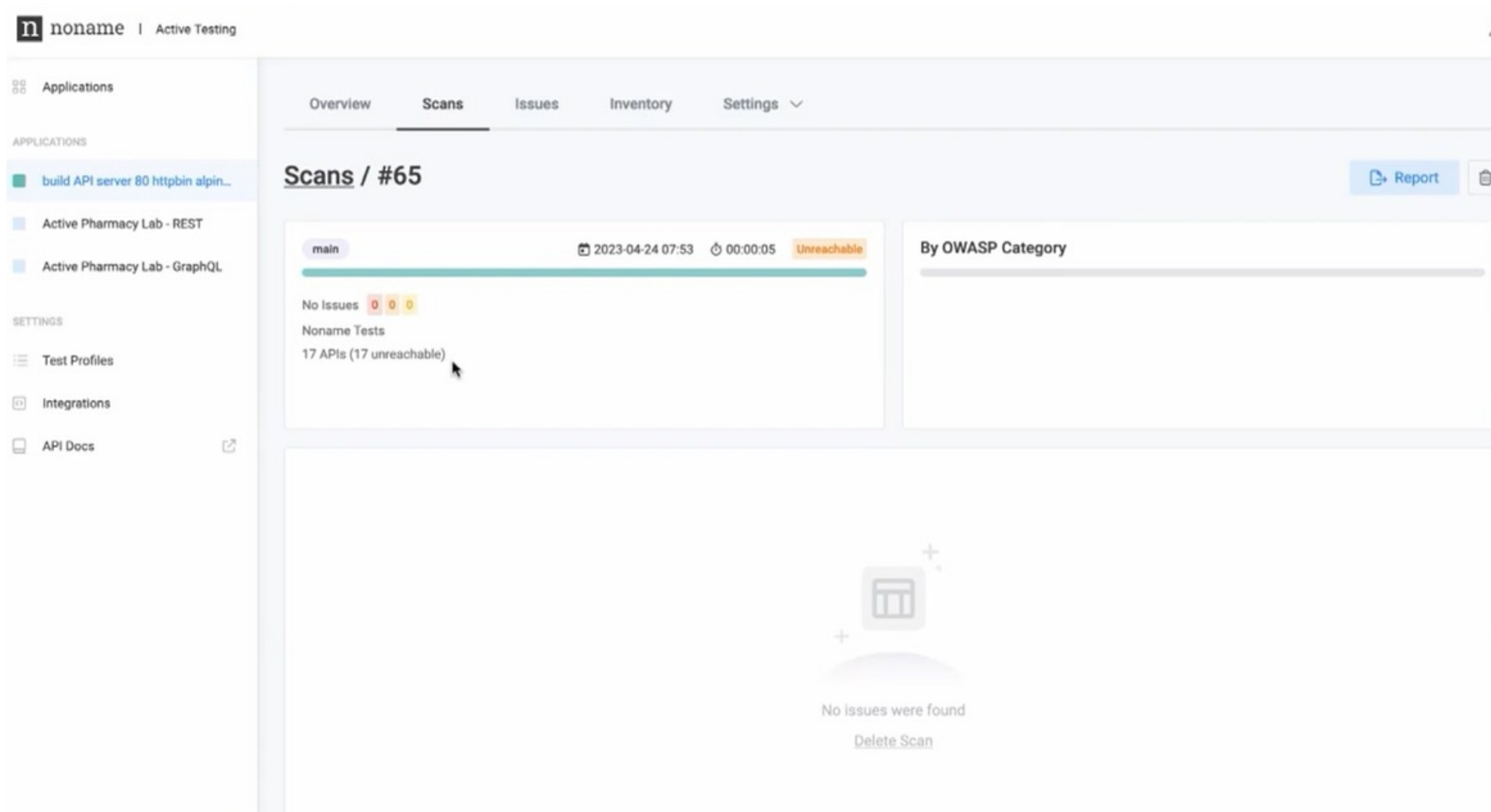
Active-Testing

<https://build.nonamesec.com/active>

# API安全左移 Azure DevOps CI/CD pipelines



# No Api management



The screenshot displays the 'noname' Active Testing web interface. The left sidebar contains navigation links for 'Applications', 'Test Profiles', 'Integrations', and 'API Docs'. The main content area is titled 'Scans / #65' and shows a scan for 'main' dated '2023-04-24 07:53' with a duration of '00:00:05' and a status of 'Unreachable'. A progress bar is shown with the text 'No issues' and three colored circles (red, yellow, green). Below this, it says 'Noname Tests' and '17 APIs (17 unreachable)'. A 'Report' button is visible in the top right. At the bottom, a large message states 'No issues were found' with a 'Delete Scan' link.

noname | Active Testing

Applications

APPLICATIONS

- build API server 80 httpbin alpin...
- Active Pharmacy Lab - REST
- Active Pharmacy Lab - GraphQL

SETTINGS

- Test Profiles
- Integrations
- API Docs

Overview Scans Issues Inventory Settings

Scans / #65

main 2023-04-24 07:53 00:00:05 Unreachable

No issues 0 0 0

Noname Tests

17 APIs (17 unreachable)

By OWASP Category


Report

No issues were found

Delete Scan



# Api management

 noname | Active Testing

Applications

APPLICATIONS

build API server 80 httpbin alpin...

Active Pharmacy Lab - REST

Active Pharmacy Lab - GraphQL

SETTINGS

Test Profiles

Integrations

API Docs

OverviewScansIssuesInventorySettings

Scans / #68

main2023-04-24 09:2600:00:09Scanning 97%

34 Issues15163

Noname Tests

17 APIs

By OWASP Category

2 Broken Function Level Authorization13 Broken User Authentication

15 Security Misconfiguration3 Improper Assets Management

34 Items

Group BySearchDownload0

API	Severity	Issue	Category	OWASP	Actions
DELETE /delete	high	Reader role successfully deleted a resource	Broken Function Level Authorization	API05:2019	
GET /html	high	Lack of Secret Content Validation	Broken User Authentication	API02:2019	
GET /xml	high	Lack of Secret Content Validation	Broken User Authentication	API02:2019	
GET /	high	Lack of Secret Content Validation	Broken User Authentication	API02:2019	

1-10 of 3410

# The Noname API Security Platform

**Shift Left with  
API Security  
Testing**



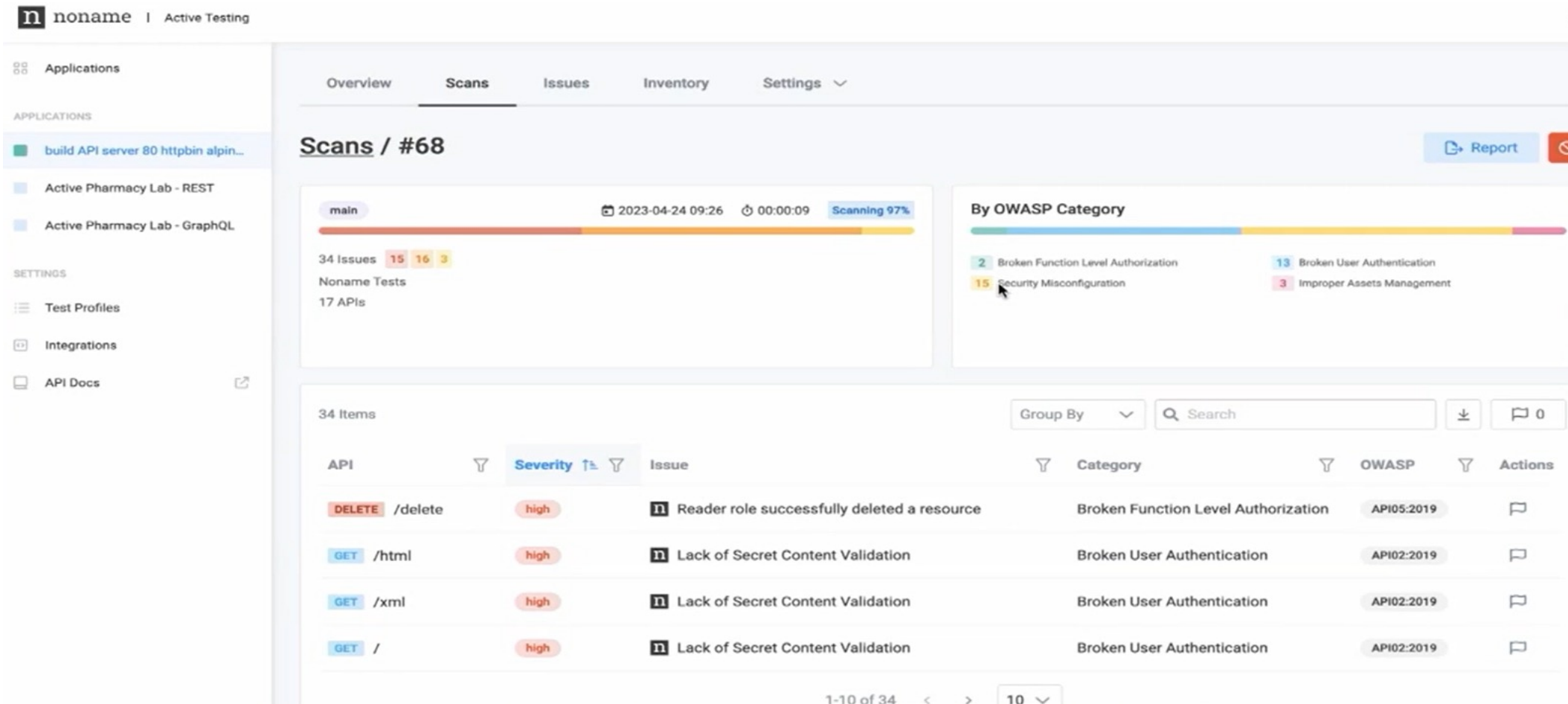
**API Posture  
Management**



**Runtime API  
Protection**



API Security Testing goes a long way in avoiding API breaches by preventing security vulnerabilities from ever reaching production environments. Noname Active Testing focuses on finding and remediating API security vulnerabilities during the development phase of the SDLC, before they can be exploited.

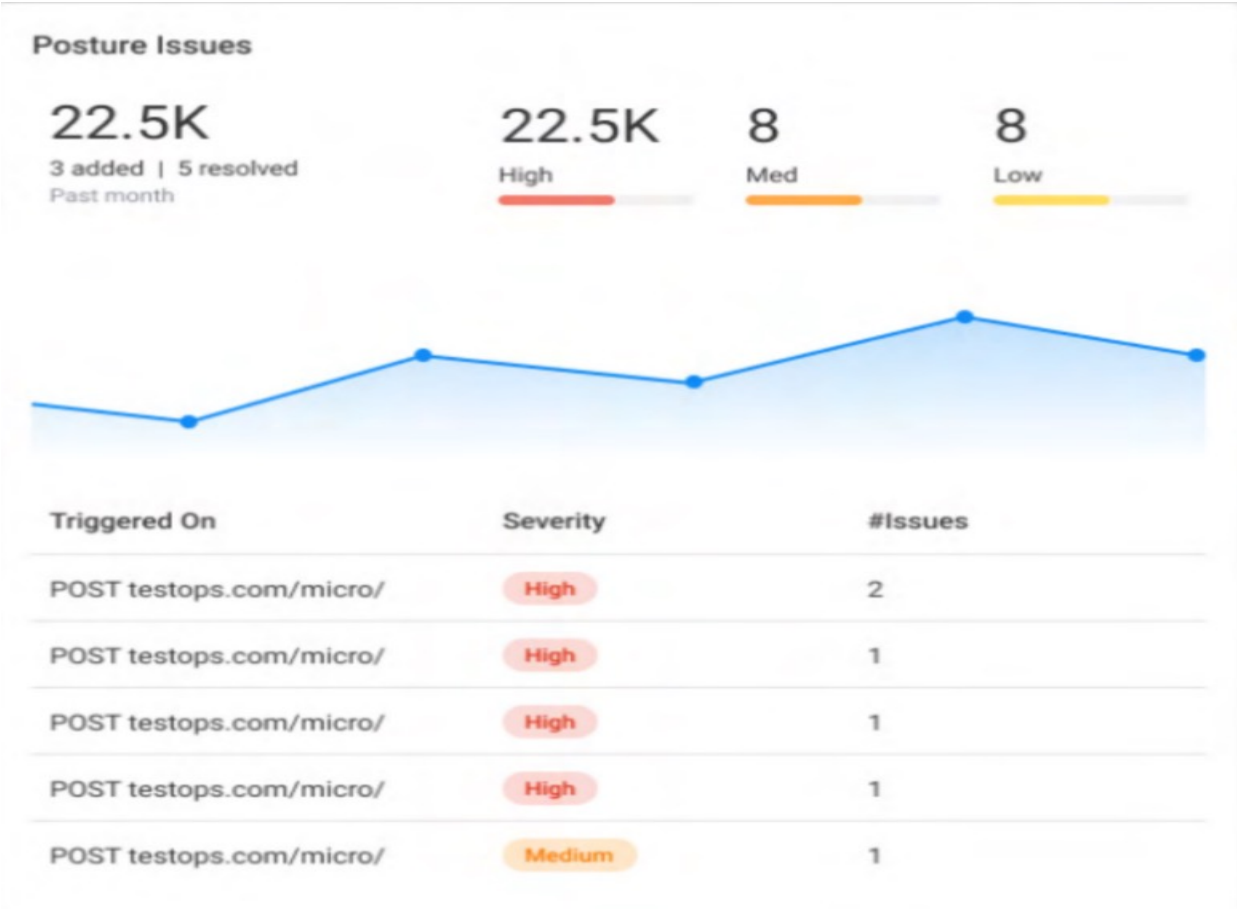


The screenshot displays the Noname Active Testing interface. The left sidebar contains navigation options: Applications, Applications (with a list of 'build API server 80 httpbin alpin...', 'Active Pharmacy Lab - REST', and 'Active Pharmacy Lab - GraphQL'), and Settings (with 'Test Profiles', 'Integrations', and 'API Docs'). The main content area is titled 'Scans / #68' and shows a progress bar for a scan on '2023-04-24 09:26' with 'Scanning 97%'. Below this, it indicates '34 Issues' (15 high, 16 medium, 3 low) and 'Noname Tests 17 APIs'. A 'By OWASP Category' chart shows: 2 Broken Function Level Authorization, 13 Broken User Authentication, 15 Security Misconfiguration, and 3 Improper Assets Management. A table lists 34 items, showing the first four: a high severity issue for 'DELETE /delete' (Reader role successfully deleted a resource), and three high severity issues for 'GET /html', 'GET /xml', and 'GET /' (all Lack of Secret Content Validation). The table includes columns for API, Severity, Issue, Category, OWASP, and Actions. A pagination bar at the bottom shows '1-10 of 34' and a dropdown for '10'.

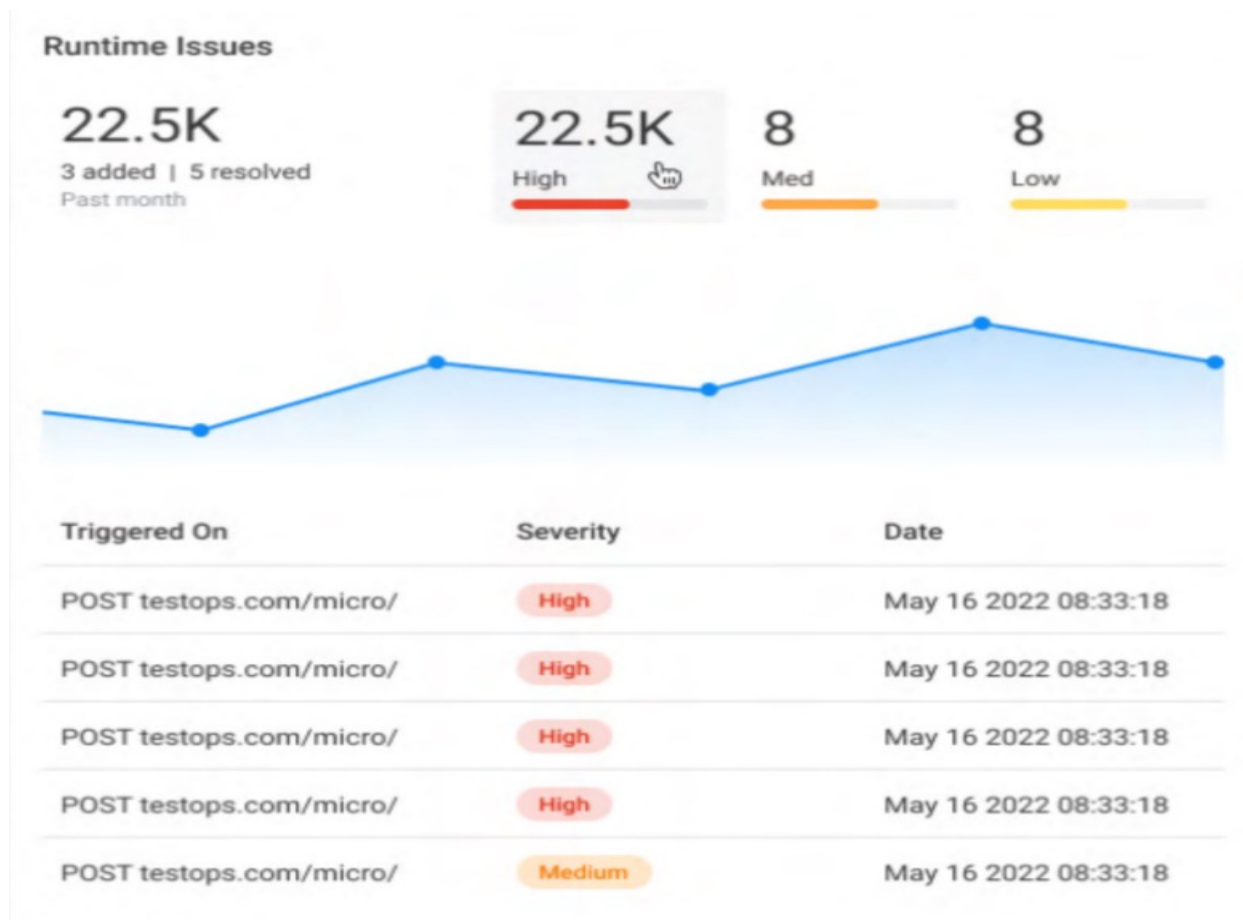
API	Severity	Issue	Category	OWASP	Actions
DELETE /delete	high	Reader role successfully deleted a resource	Broken Function Level Authorization	API05:2019	🚩
GET /html	high	Lack of Secret Content Validation	Broken User Authentication	API02:2019	🚩
GET /xml	high	Lack of Secret Content Validation	Broken User Authentication	API02:2019	🚩
GET /	high	Lack of Secret Content Validation	Broken User Authentication	API02:2019	🚩

# API Posture Management

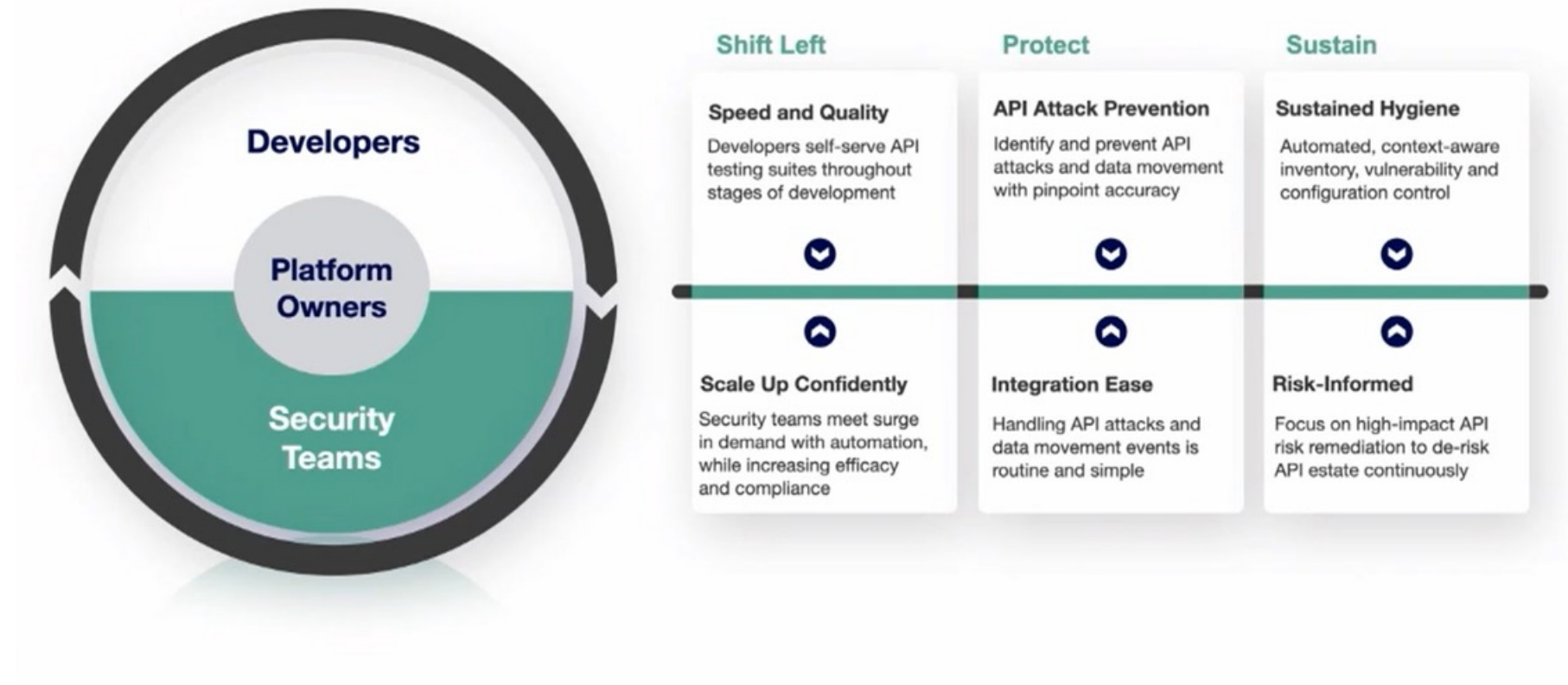
Next to providing a complete inventory of APIs using Discovery, Noname Security Posture Management will assess your APIs and broader infrastructure for misconfigurations and vulnerabilities to identify potential risks and understand their true attack surface.



One of the unique and complicated properties of APIs is that usage patterns differ greatly depending on the functionality of the API. To adequately detect malicious traffic during runtime, you need to successfully differentiate between normal and abnormal behavior.



# A New Model for API Security





### Noname Security:

<https://nonamesecurity.com/>

<https://azuremarketplace.microsoft.com/zh-tw/marketplace/apps/nonamegateinc1627221832172.noname-security>

[https://azuremarketplace.microsoft.com/zh-tw/marketplace/apps/nonamegate.nonamesecurity\\_sentinelsolution](https://azuremarketplace.microsoft.com/zh-tw/marketplace/apps/nonamegate.nonamesecurity_sentinelsolution)

### 清源SCA:

<https://www.sectrend.com.cn/>

**Beyond Security, more than**

**open**

**source.**

**Thank you!**