42crunch

21 March 2023

Build secure APIs in VS Code with instant API security testing

Colin Domoney

Chief Technology Evangelist

About the speaker

Colin Domoney

Chief Technology Evangelist

DevSecOps specialist and evangelist, lifelong learner/hacker and latent developer

- **VP of AppSec at Deutsche Bank**
  - 20k developers, 6k app
  - Fixed over 3 million high-severity flaws
  - Built global AppSec program
- **Innovation manager/DevRel/Solution Architect at Veracode Inc.**
  - Frequent speaker and blogger
  - Advised Fortune 100 on DevSecOps implementations
- **Independent DevSecOps consultant**
- **Industry analyst and advisor**
- **Advocates for API Security**
- **Curator of APISecurity.io**

Agenda

- Security testing in the IDE
- 42Crunch VS Code extension
- Live demonstration
  - Incorrectly responding to undefined verbs
  - Malformed responses to operations
  - Incorrect handling of edge-case input
- Getting started on your own
- Questions and Answers

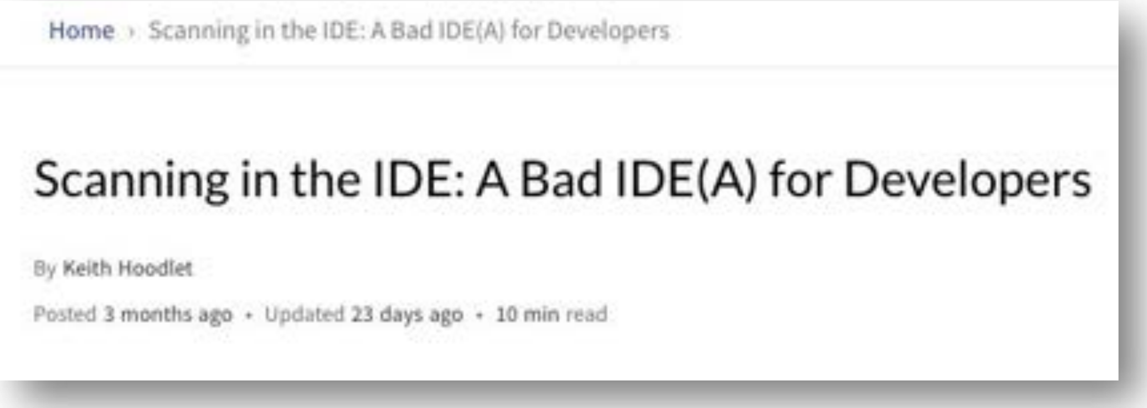
Perspectives on IDE testing

Security testing in the IDE

IDE security in the IDE :- a bad idea?

- IDE Scanners make for distracted developers
- Even if IDE Scanners weren’t a distraction - they will be challenging to implement at scale
- You still need to scan outside of the IDE for audits and ongoing security validation.

- What developers really want: **Results in the IDE**



Home › Scanning in the IDE: A Bad IDE(A) for Developers

Scanning in the IDE: A Bad IDE(A) for Developers

By Keith Hoodlet

Posted 3 months ago • Updated 23 days ago • 10 min read

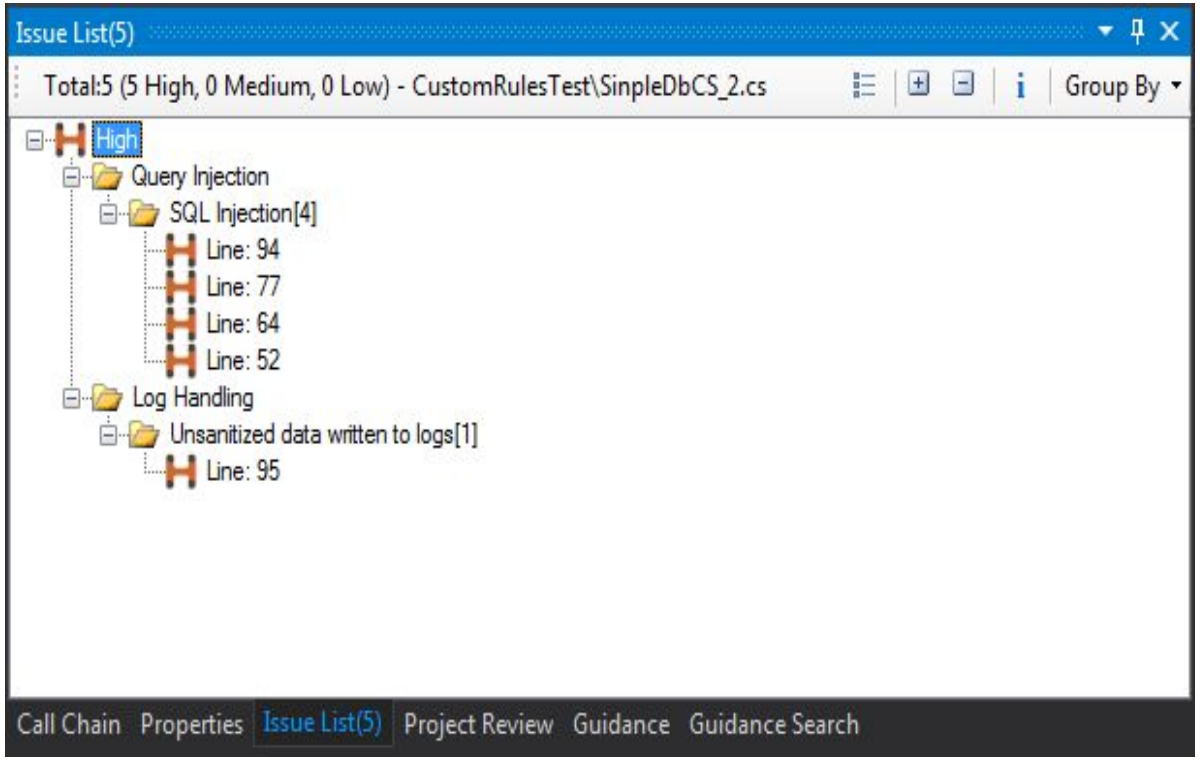
securing.dev

Pseudo-random musings on Security, Software Development, and Life

https://securing.dev/posts/ide-scanners-are-a-bad-idea/

Security extensions often underwhelm

- Distract developers
- Create too much noise
- Slow down the code-run-debug cycle
- Lack configurability
- **Fail to deliver any real value**

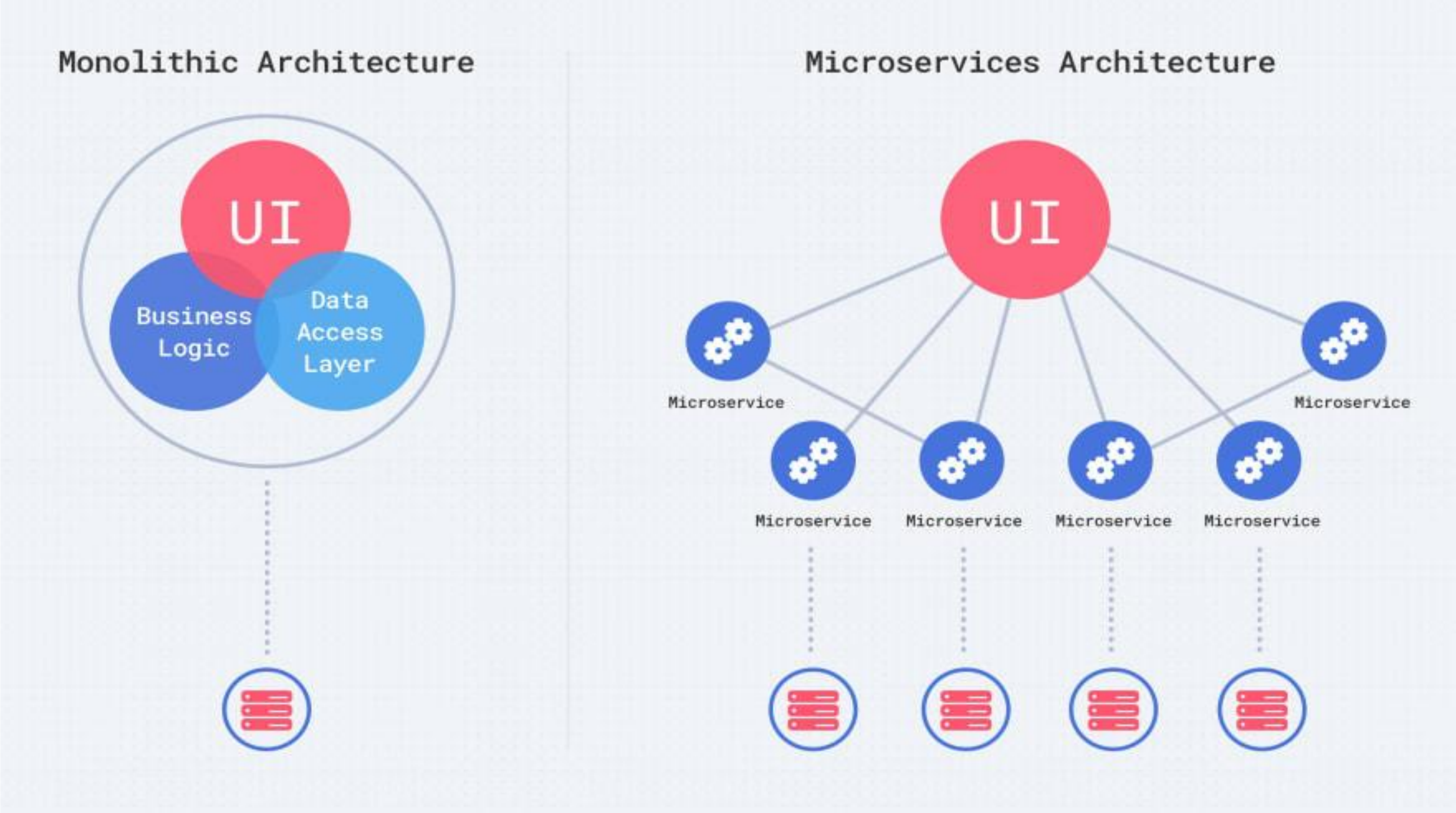


Issue List(5)

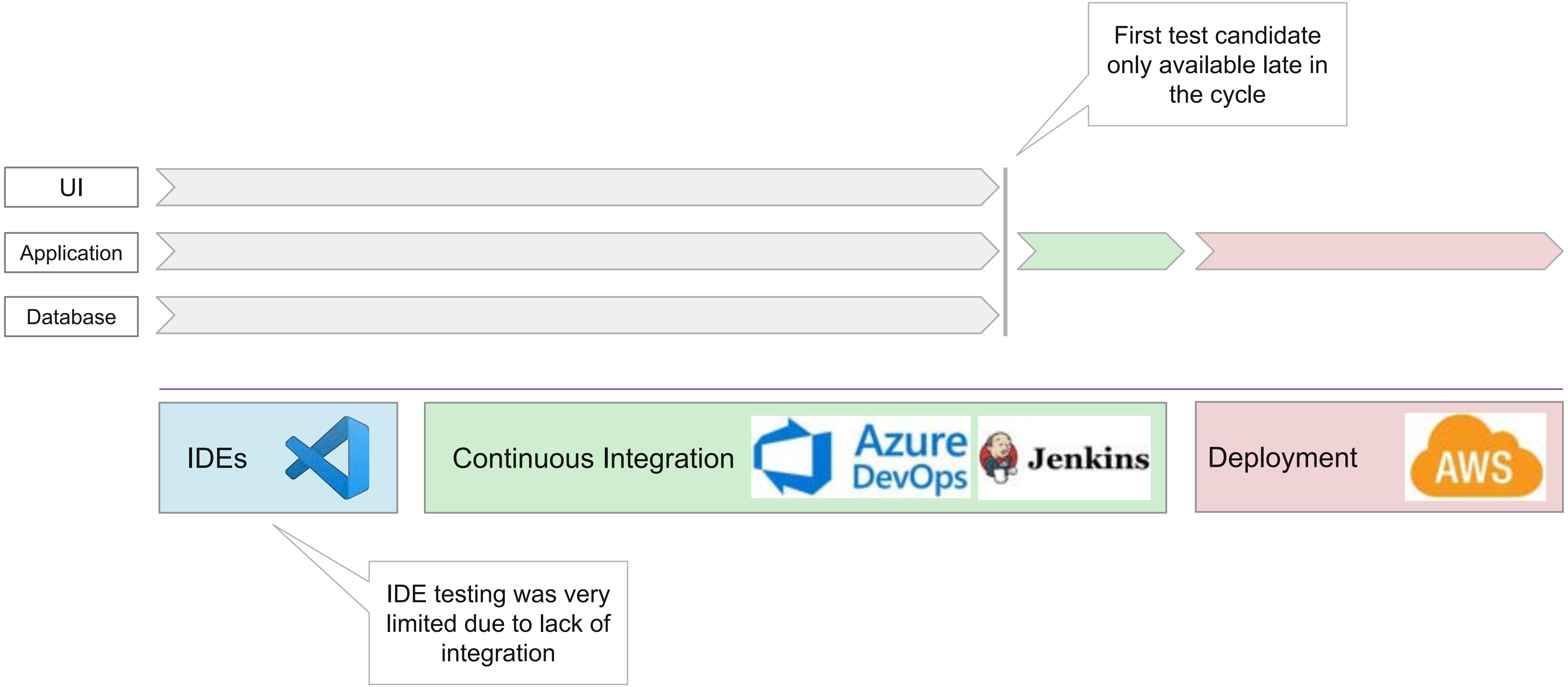
Total:5 (5 High, 0 Medium, 0 Low) - CustomRulesTest\SinpleDbCS_2.cs

```
High
  Query Injection
    SQL Injection[4]
      Line: 94
      Line: 77
      Line: 64
      Line: 52
  Log Handling
    Unsanitized data written to logs[1]
      Line: 95
```

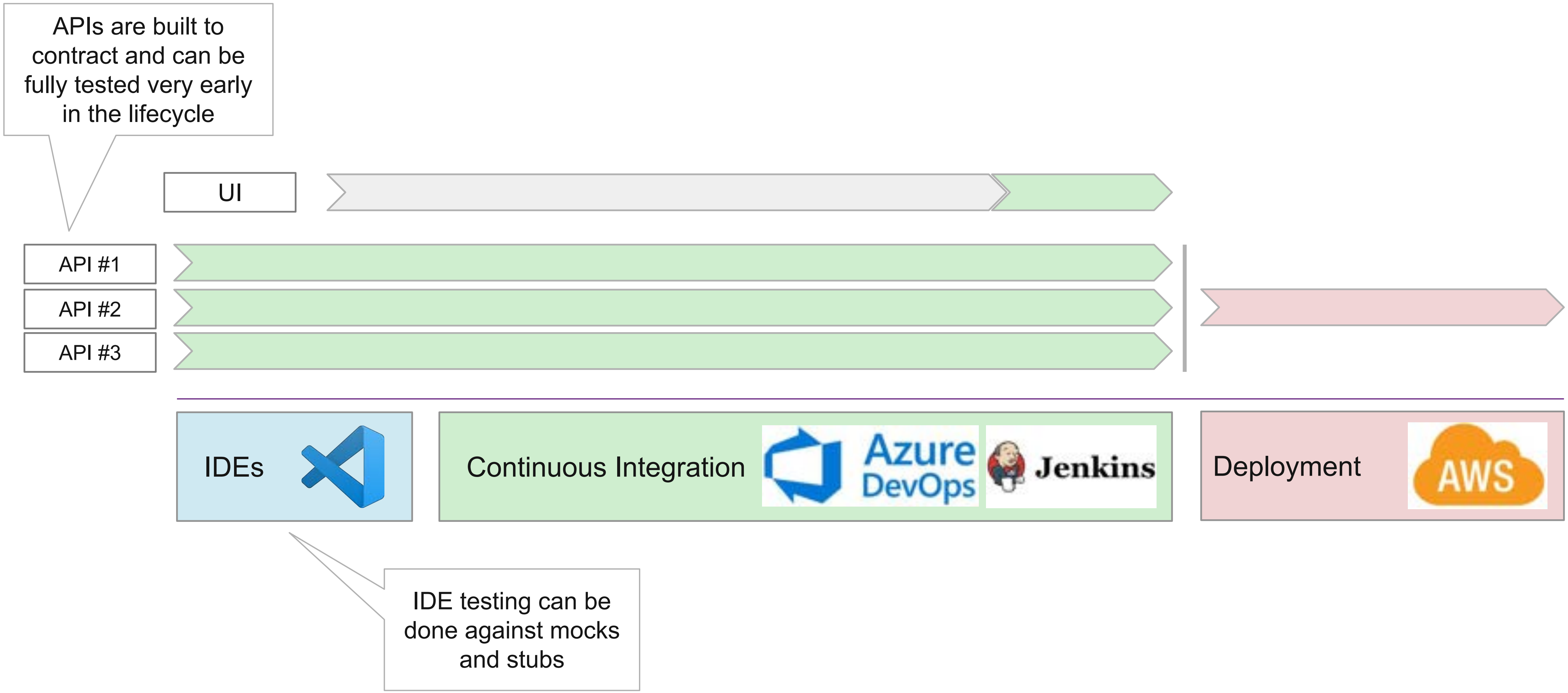
From the monolith to microservices



The testing cycle is changing


First test candidate only available late in the cycle
UI
Application
Database
IDEs
Continuous Integration
Azure DevOps
Jenkins
Deployment
AWS
IDE testing was very limited due to lack of integration

APIs and microservices change everything

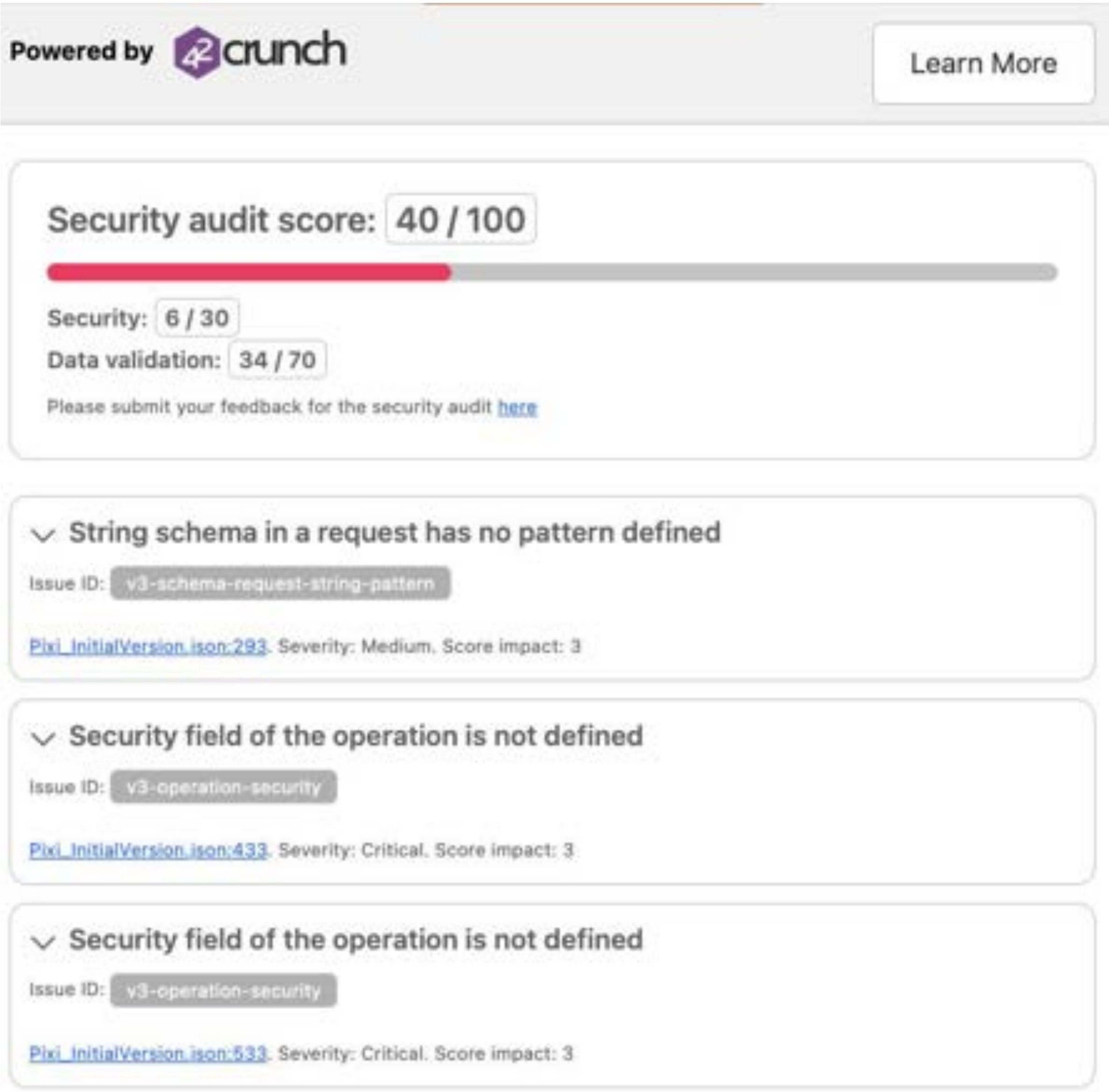


APIs are built to contract and can be fully tested very early in the lifecycle

IDE testing can be done against mocks and stubs

Perspectives on IDE testing

Security testing in the IDE with 42Crunch



Security audit score: 40 / 100

Security: 6 / 30

Data validation: 34 / 70

Please submit your feedback for the security audit here

String schema in a request has no pattern defined

Issue ID: v3-schema-request-string-pattern

Pixi_InitialVersion.json:293. Severity: Medium. Score impact: 3

Security field of the operation is not defined

Issue ID: v3-operation-security

Pixi_InitialVersion.json:433. Severity: Critical. Score impact: 3

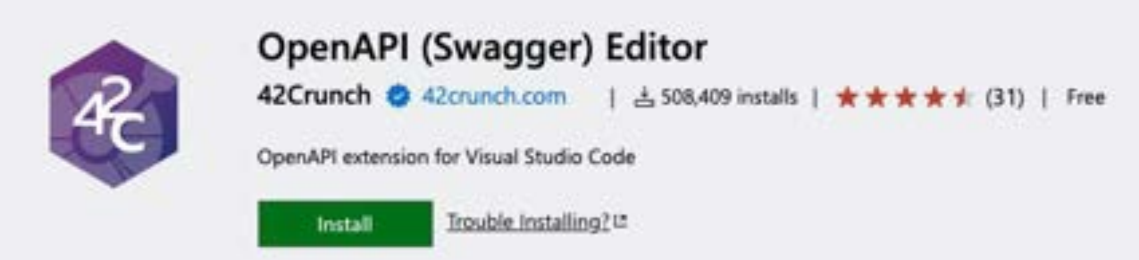
Security field of the operation is not defined

Issue ID: v3-operation-security

Pixi_InitialVersion.json:533. Severity: Critical. Score impact: 3

Introducing the 42Crunch OpenAPI editor extension

- OAS generation in YAML or JSON
- IntelliSense for OAS
- Linting
- Schema enforcement
- Code navigation
- Snippets
- OAS v2 and v3 supported



OpenAPI (Swagger) Editor

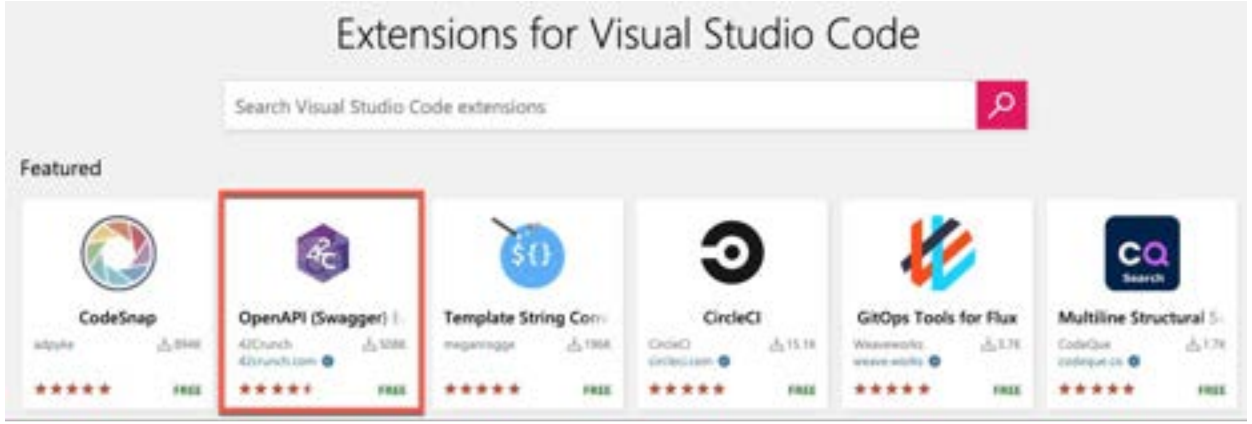
42Crunch 42crunch.com | 508,409 installs | ★★★★☆ (31) | Free

OpenAPI extension for Visual Studio Code

ulrik ★★★★★
09/03/2023
Indispensable when working with OpenAPI files.

Felix Wu ★★★★★
14/06/2019
Great extension

Haykel Ben Jemia ★★★★★
08/12/2020
Awesome extension, very helpful and a huge time saver. Thanks a lot!

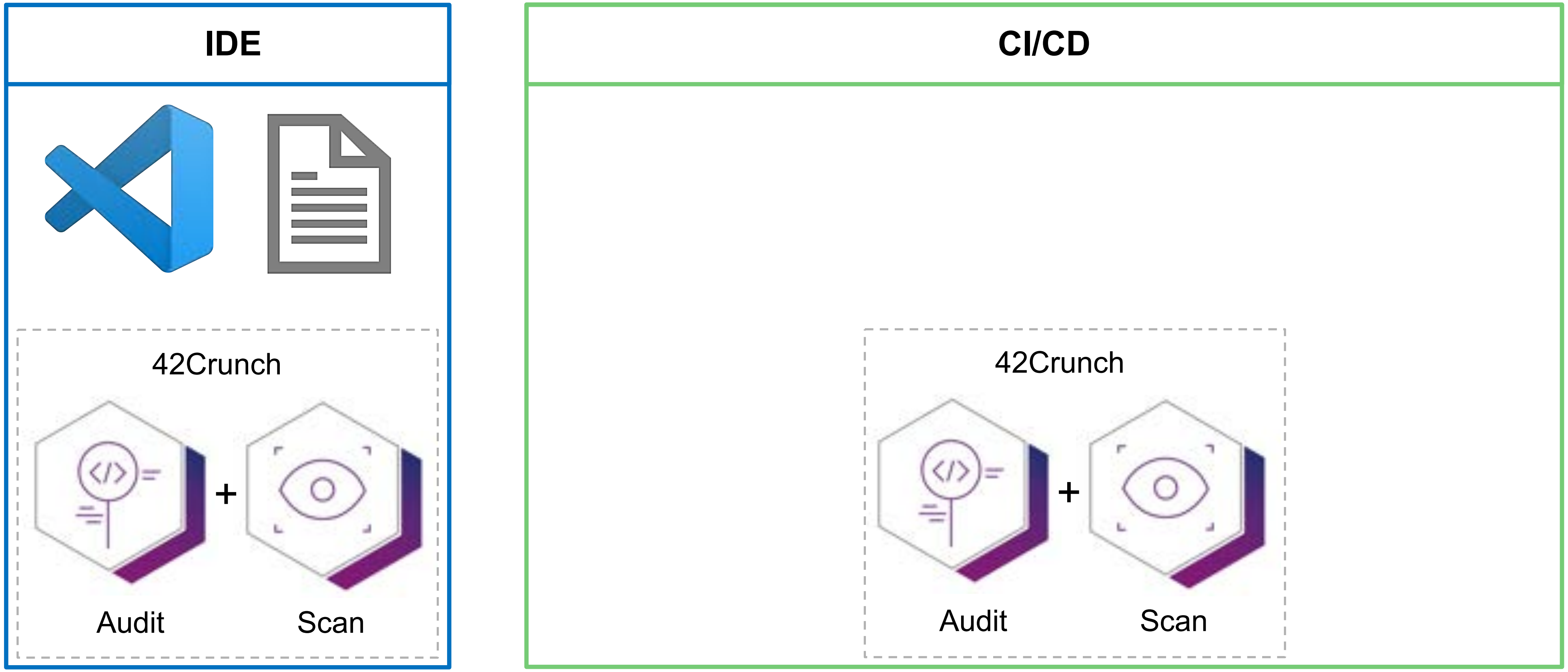


Extensions for Visual Studio Code

Same audit, same scan – IDE or CI/CD

Scan APIs **per method** as they are implemented

Scan **entire** API as they are integrated



Getting started on your own

https://marketplace.visualstudio.com/items?itemName=42Crunch.vscode-openapi

https://42crunch.com/free-tools/

Additional Resources

Learning more

APISecurity.io

https://apisecurity.io/

“Microservice APIs” – José Haro Peralta

Copyrighted Material

Using Python, Flask, FastAPI, OpenAPI and more

Microservice APIs

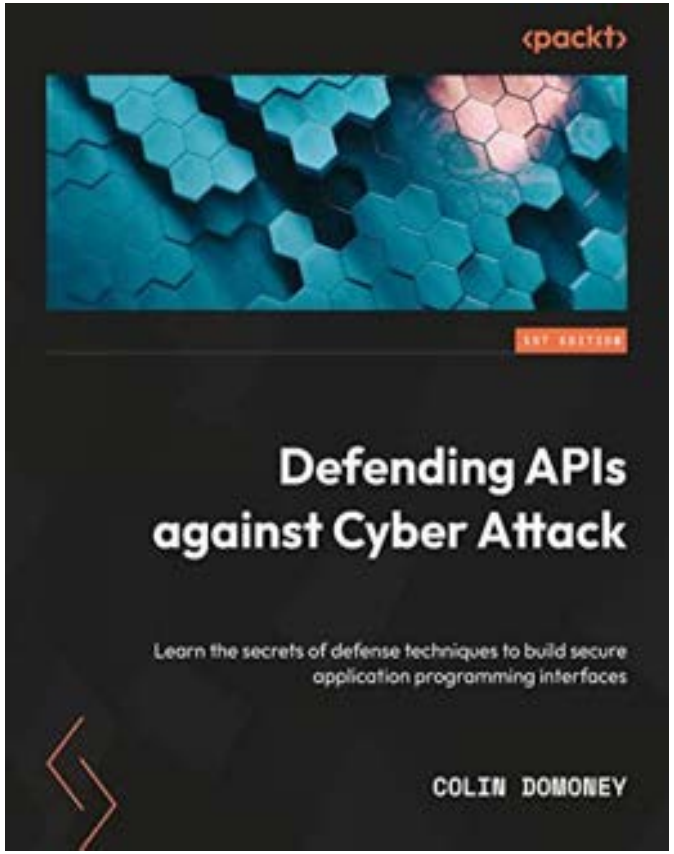
José Haro Peralta

MANNING

Copyrighted Material

https://www.manning.com/books/microservice-apis

“Defending APIs against Cyber Attack” – Colin Domoney



‹packt›

1ST EDITION

Defending APIs against Cyber Attack

Learn the secrets of defense techniques to build secure application programming interfaces

COLIN DOMONEY

https://amzn.to/3fHp8Mz

Guide

API Security: A Blueprint for Success

- *Practical Guide on an API Security program.*
- *Map your enterprise's API security posture against 6 key domains.*
- *Champion the case for API Security.*

Using the assessment, the organization can map (and track) a roadmap for continuous API security capability improvement.

API INVENTORY
Do you understand what APIs you own? Do you track shadow and zombie APIs?

API DESIGN
Are you doing API design first? Do you incorporate security into the design phase?

API DEVELOPMENT
Are your developers trained to code securely? Do they understand API security threats and risks?

API TESTING
Are you doing automated API testing? Are you considering security in your test strategy?

API PROTECTION
Are you using API protection technology (WAFs, WAAPs, API gateways) in your deployments?

API GOVERNANCE
Do you control and actively monitor your API estate and environments?

Download Guide here: https://42crunch.com/ebook-api-security-blueprint/

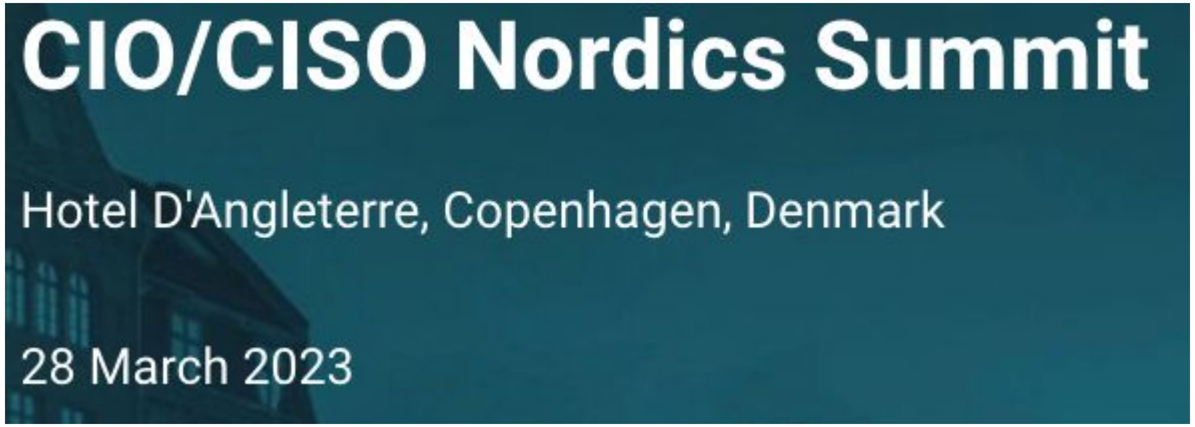
Events

Upcoming Events

RSAConference™

Apr. 24 - 27, 2023
San Francisco

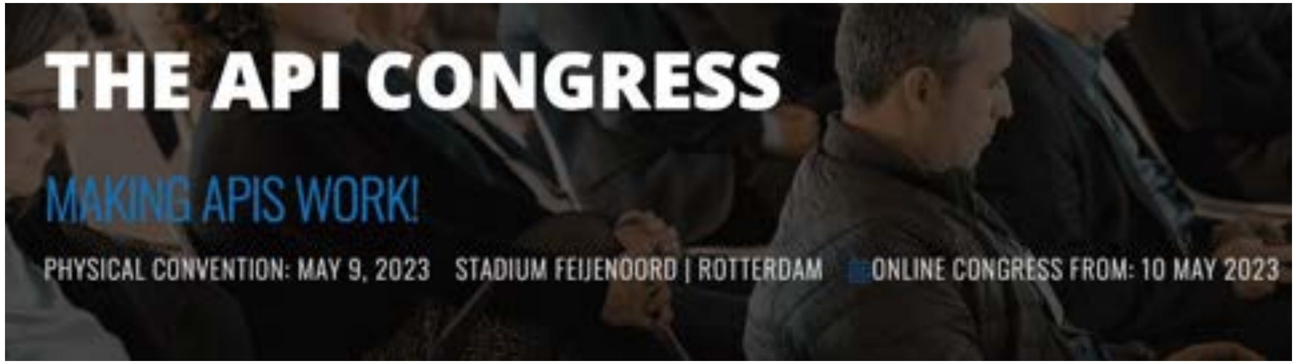
Stronger
Together



CIO/CISO Nordics Summit

Hotel D'Angleterre, Copenhagen, Denmark

28 March 2023



THE API CONGRESS

MAKING APIS WORK!

PHYSICAL CONVENTION: MAY 9, 2023 STADIUM FEIJENOORD | ROTTERDAM ONLINE CONGRESS FROM: 10 MAY 2023