Automating Infrastructure Security Testing

Peter Mosmans
LEAD PENETRATION TESTER

@onwebsecurity https://www.onwebsecurity.com

Scenario

Maeve

“Finally the application is ready for production”

“Have we tested everything?”

Jennifer

“Almost, because we still need to test the infrastructure”

“Fortunately, we can also automate that”

Module Overview

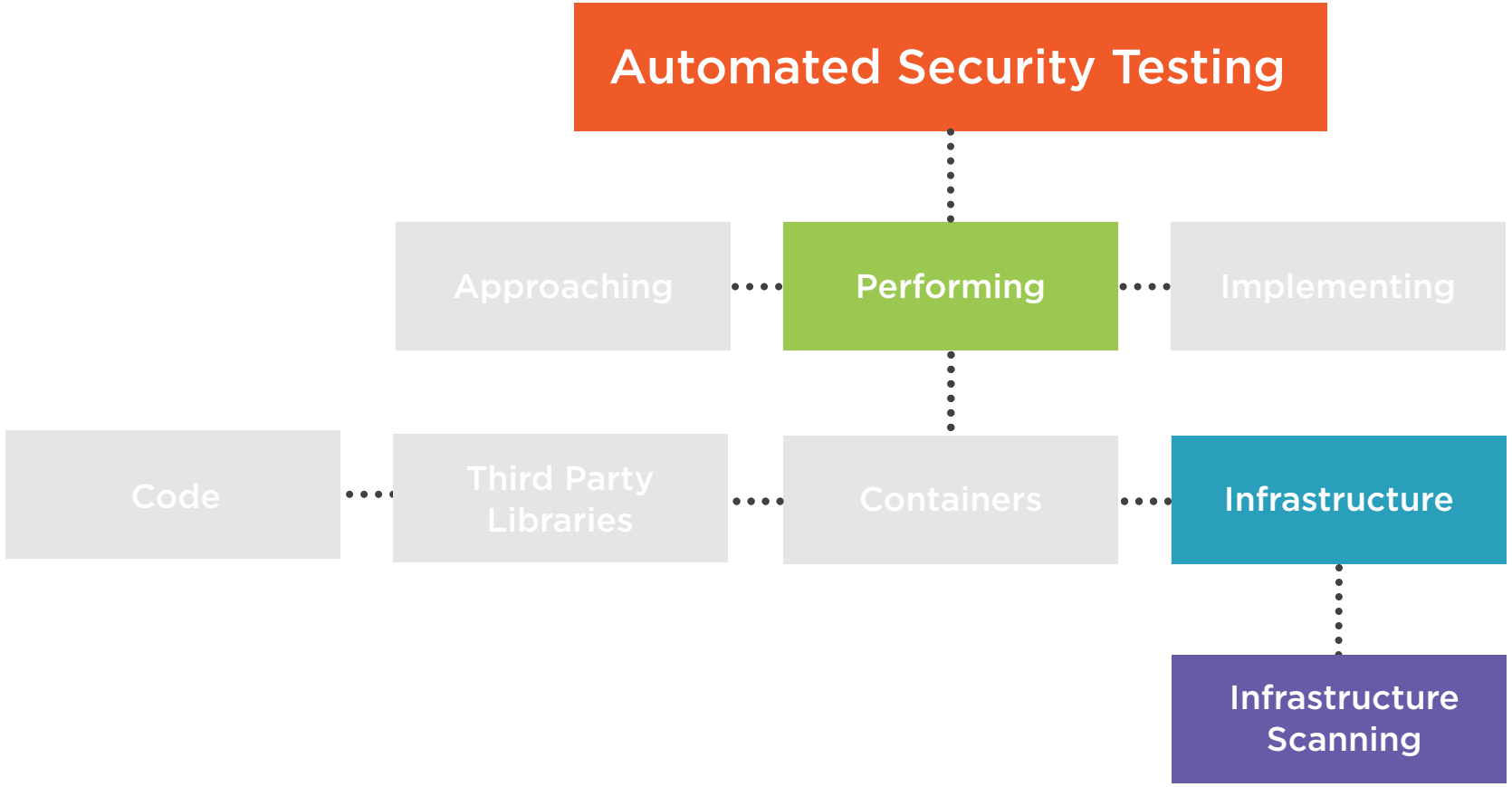
Infrastructure scanning

Demos:

- Scanning for web server misconfigurations
- Dynamic application security testing
- Implementing all automated security tests

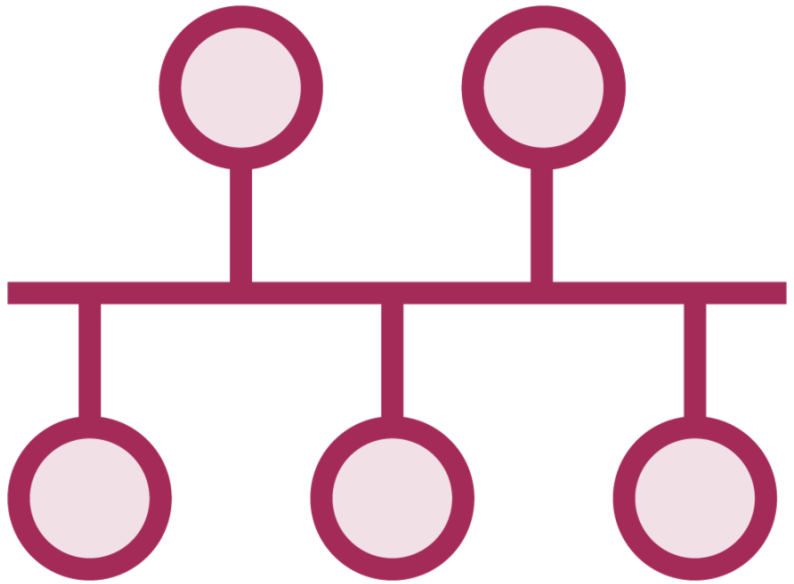
Module and course summary

Automated Security Testing Overview



Infrastructure Scanning

What Can an Infrastructure Scanner Do?



Find known misconfigurations

Find issues with missing hardening

Detect vulnerabilities

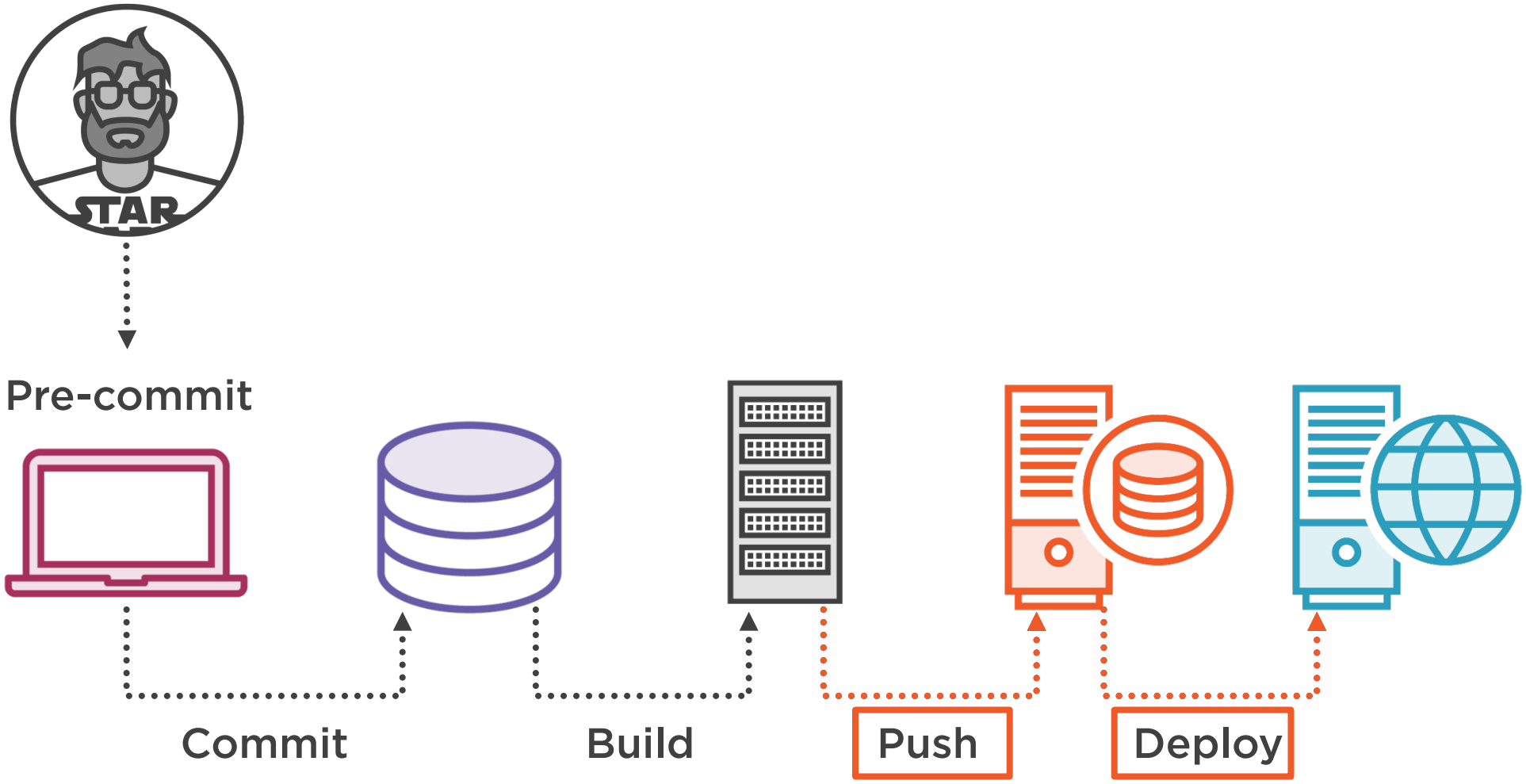
Characteristics of Good Scanners

Use extensive testing methods

Make it easy to suppress false positives

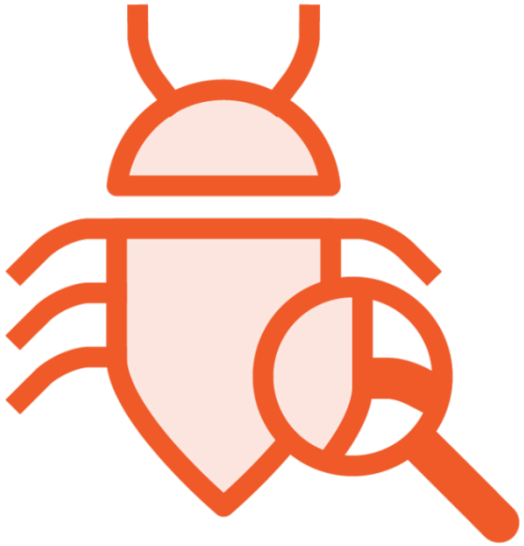
Focus on quality over speed

Where and When to Use Scanners



Which Infrastructure To Test

Development

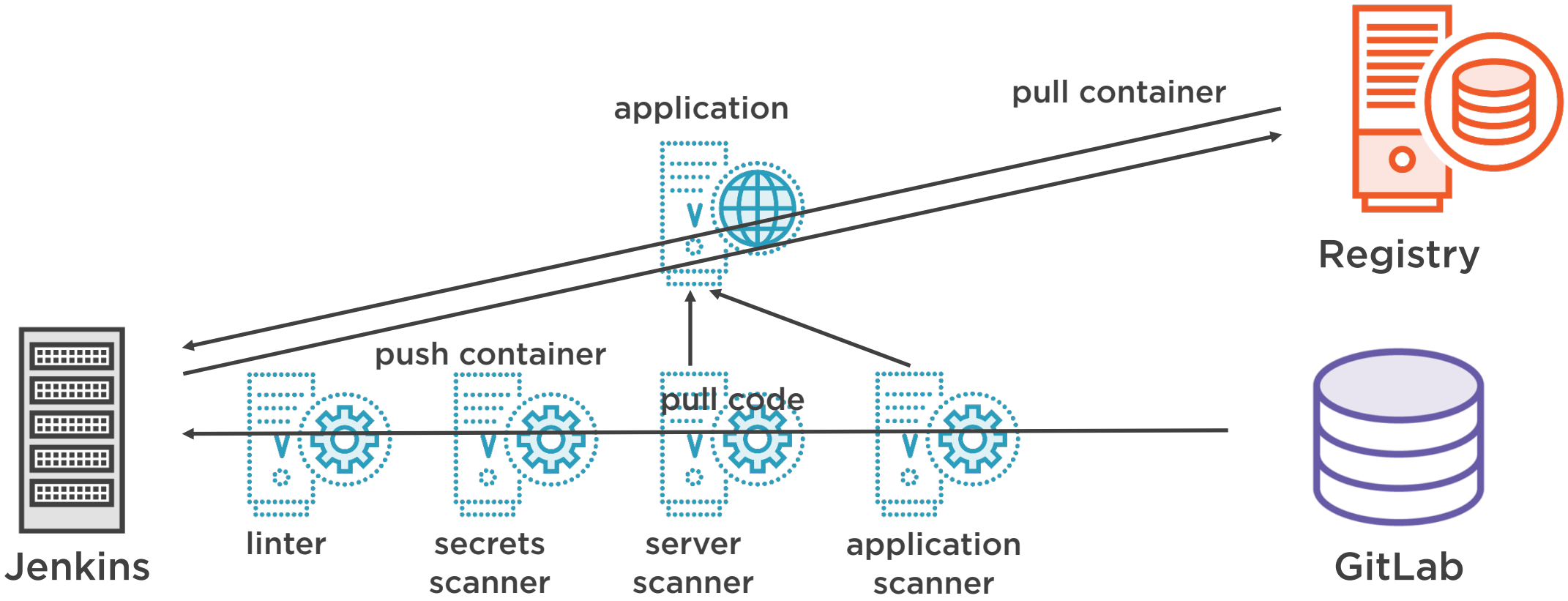


Test

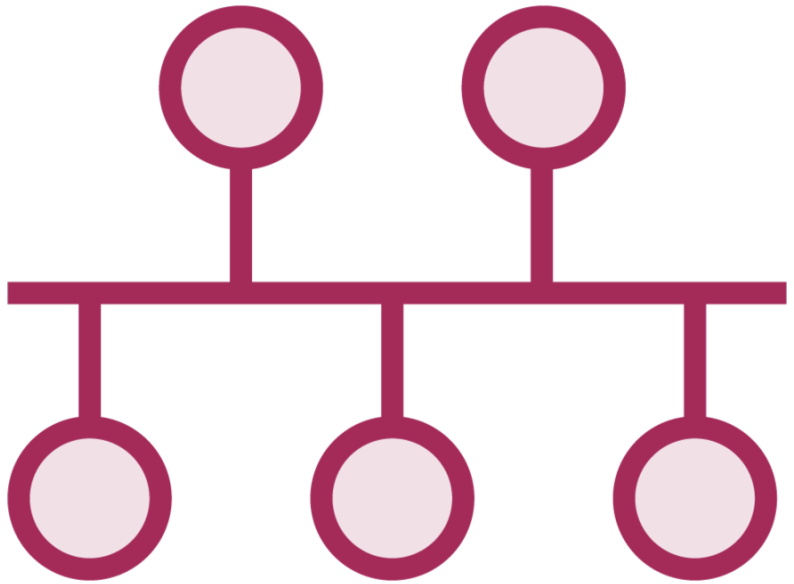
Acceptance

Production

Static Application Security Testing Workflow



Tools That Will Be Demo-ed



Nikto

- Comprehensive web server scanner

OWASP ZAP

- Dynamic web application scanner

Demo

Using Nikto

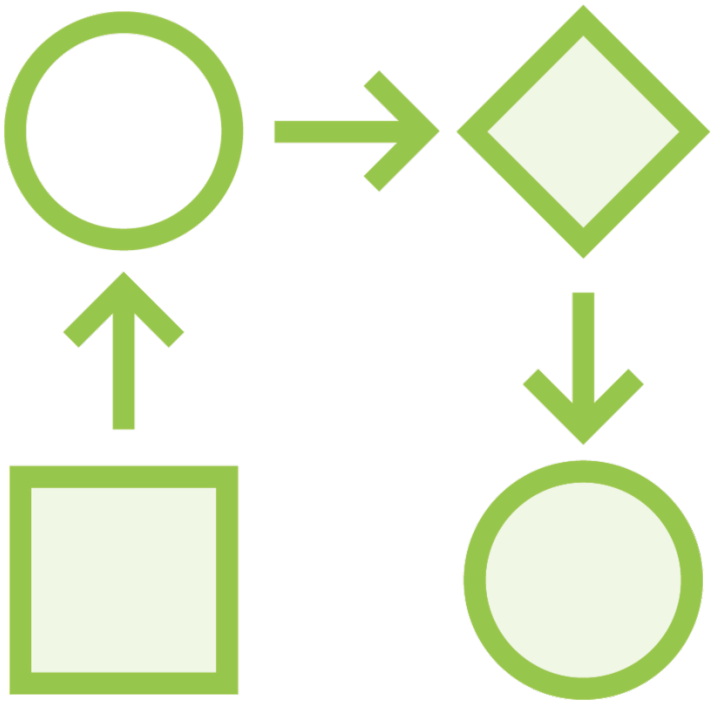
- Use Nikto on command-line
- Add sidecar to pipeline
- Scan running container in pipeline

Demo

Implementing whole testing pipeline

- Use OWASP ZAP in build pipeline
- Add all automated security tests

Workflow for Infrastructure Scanners



Start application as sidecar

- As closely resembling production as possible

Scan application

Filter out false positives

- Thoroughly configure scanners

Infrastructure Scanning

Alerts about security misconfigurations

Scans the running application / infrastructure

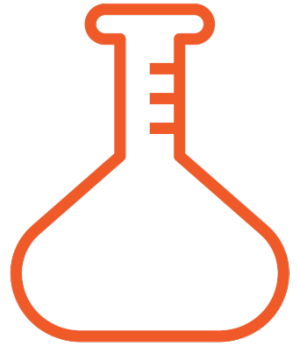
Advantage

Find security misconfigurations before production

Compatibility

Most web interfaces can be scanned

User sessions are more difficult



Trialability

Moderately easy to add to pipeline

Useful scans take a long time

More Information

https://cirt.net/Nikto2

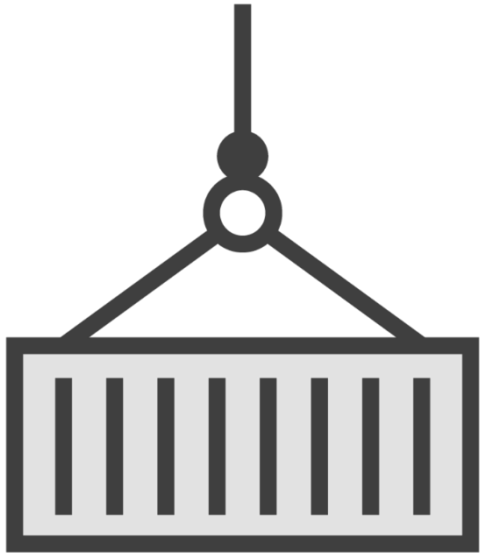
https://www.zaproxy.org/

Module and Course Summary

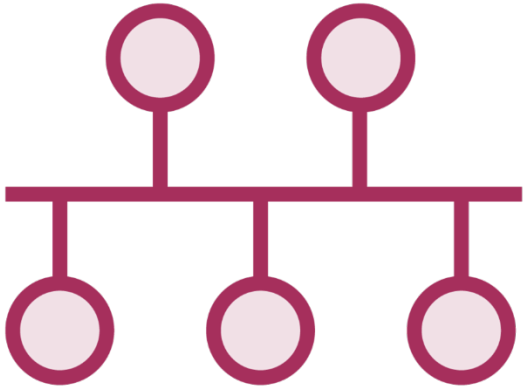
Change Frequency

Code

Third Party Libraries



Containers



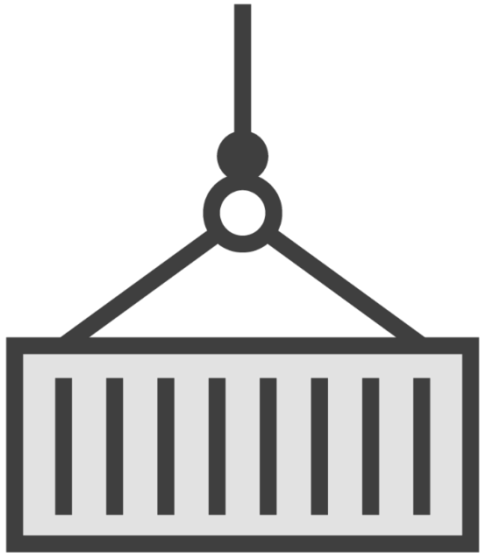
Infrastructure

Changes often ⟶ Changes less often

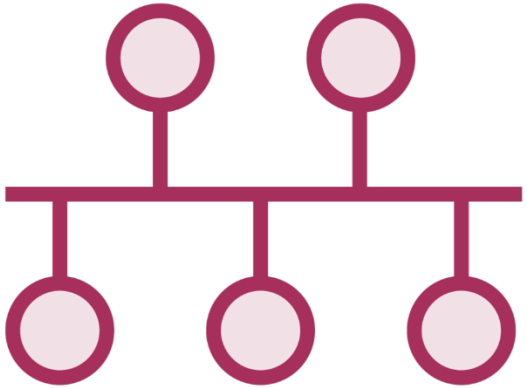
Scanning Frequency

Code

Third Party Libraries



Containers



Infrastructure

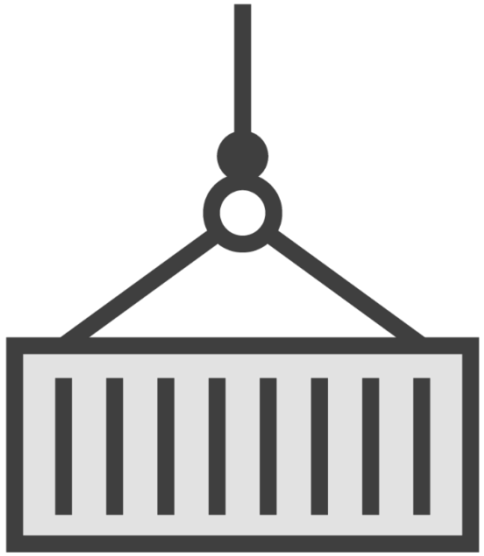
Often

Less often

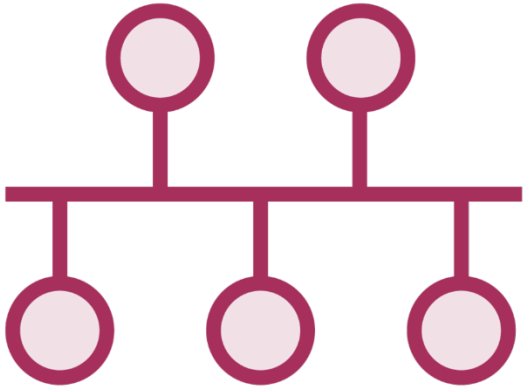
Trialability

Code

Third Party Libraries



Containers



Infrastructure

Easy

Difficult

Summary

- Start with quick wins
- Think beforehand what to expect from a tool
- Don’t underestimate the time for configuring
- Well-configured automated security testing pipeline is very valuable

Automated Security Testing
is a process,
and not a product

Thanks for Watching!

Peter Mosmans
LEAD PENETRATION TESTER

@onwebsecurity https://www.onwebsecurity.com

Next Up

Maeve

"This is immediately applicable"

"How to implement those tools in my pipeline.."

"Guess what the next course in this series is about..."

Jennifer

Automated Security Testing Overview