Automating Container Security Testing

Peter Mosmans
LEAD PENETRATION TESTER

@onwebsecurity https://www.onwebsecurity.com

Scenario

Maeve

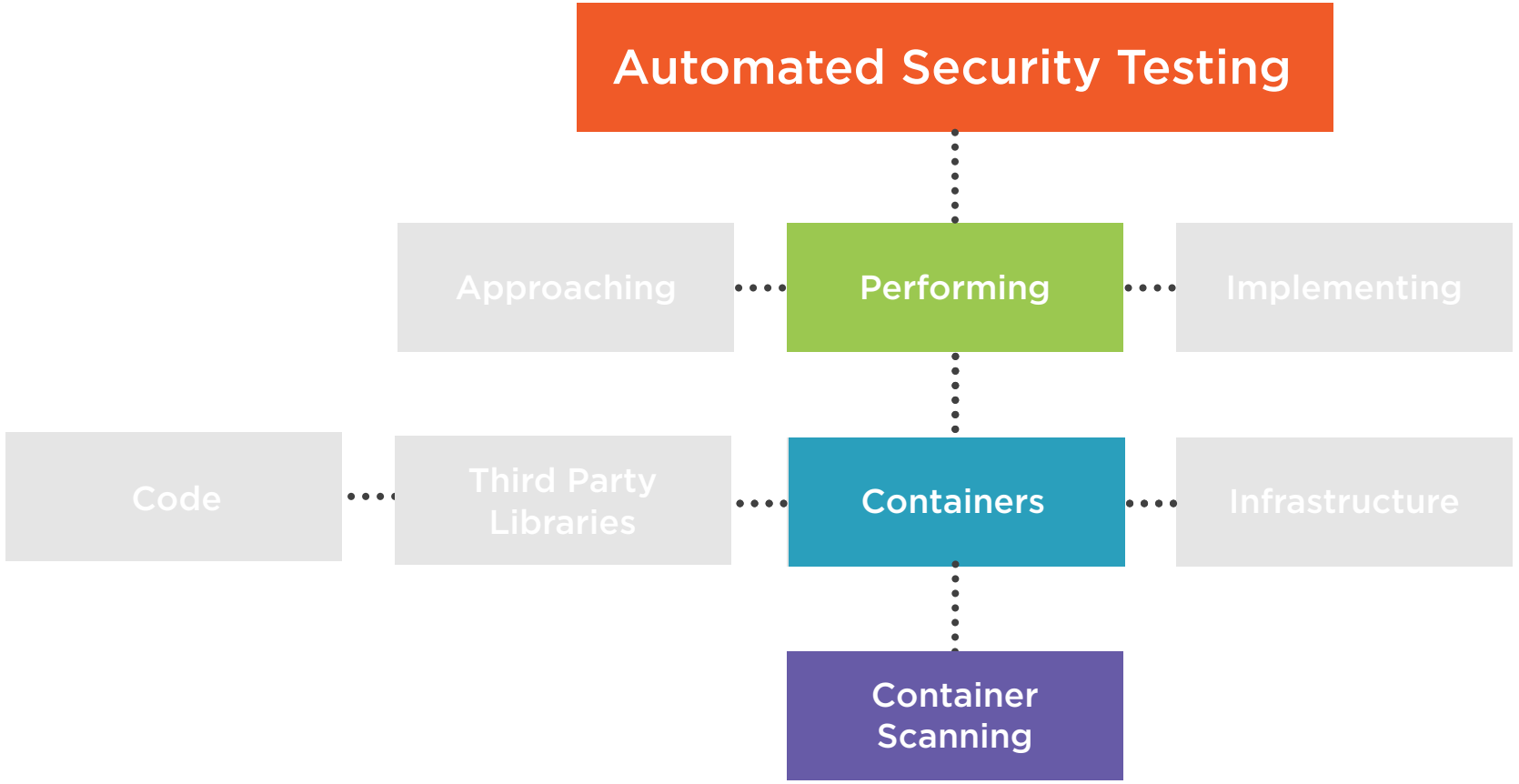
"Are all of the containers we're using secure enough?"

"Let's take a look at all those containers we're using"

Jennifer

"I'll demonstrate a container security scanner for you"

Automated Security Testing Overview



Module Overview

Container security scanning

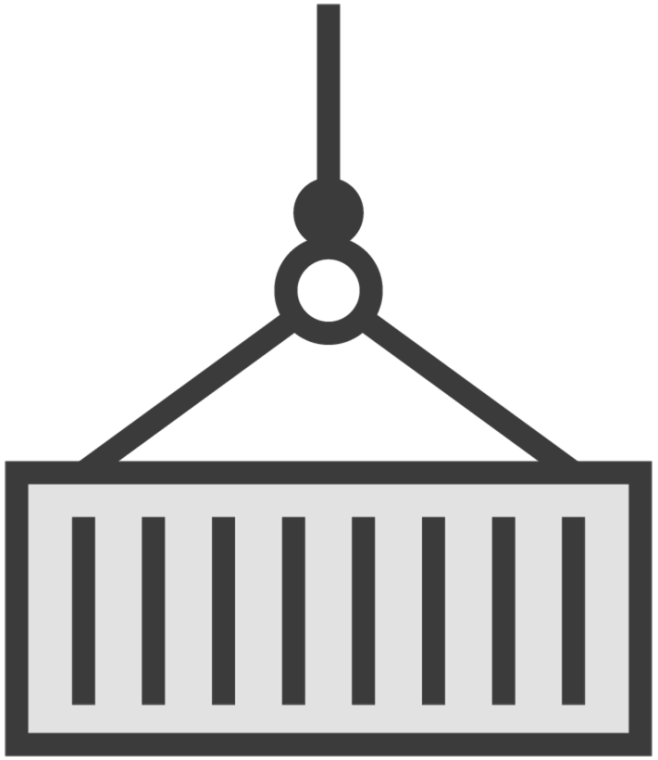
Demos:

- Scanning and validating a container
- Scanning and validating a container in a build pipeline

Summary

Container Security Scanning

Wat Can Container Security Scanning Do?



Detect insecure containers

- Detect outdated libraries
- Detect incorrectly configured containers
- Detect outdated operating system

Detect compliance validations

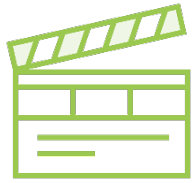
Suggest best practices

How Container Security Scanning Works

Issues With Container Security Scanners

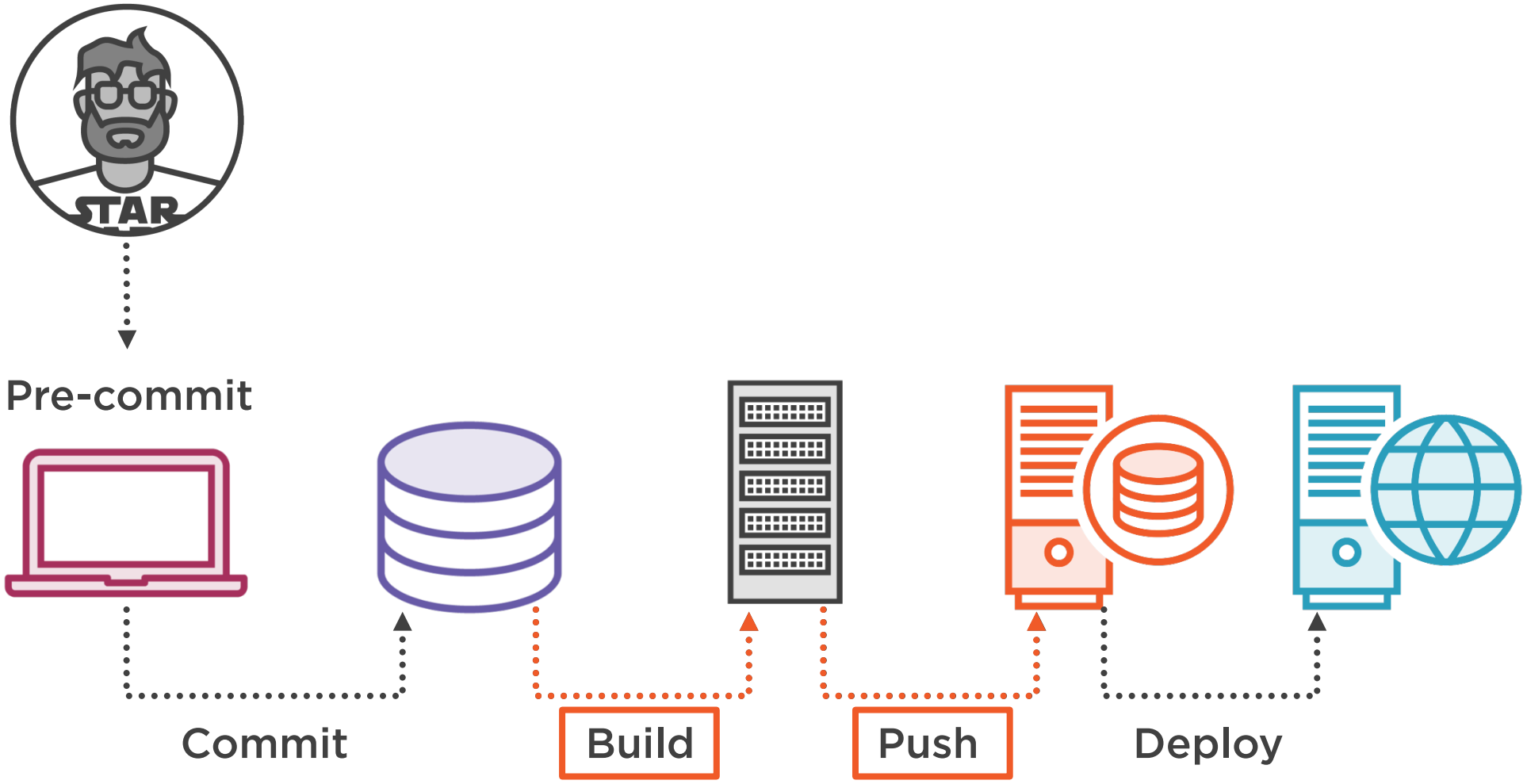
Level of depth depends on tool being used

Easy to go “too far” with configuration

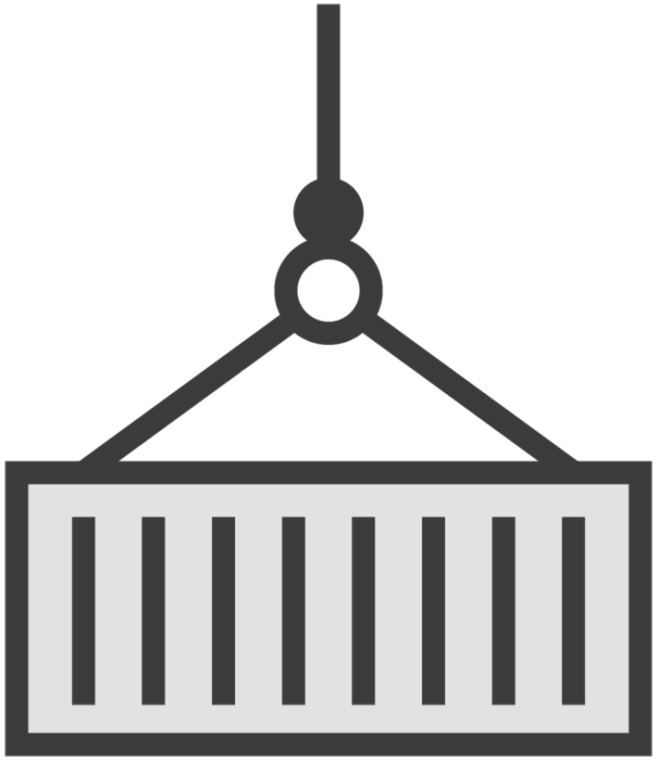


Will it lead to actionable events?

Where and When to Use Container Scanners



Tool That Will Be Demo-ed



Anchore Engine

- A docker container analysis and compliance tool

Demo

Scanning and validating a container

- Configure and use Anchore Engine on command-line

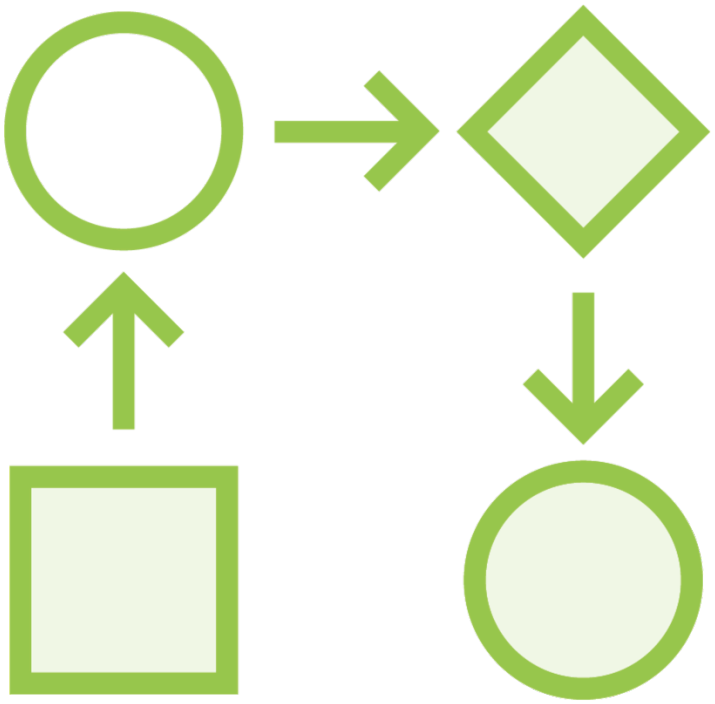
Demo

Scanning and validating an image

- Add build image stage to pipeline
- Add push to registry stage
- Add scan container stage
- Fail test when policy check fails

Workflow and Summary of Container Scanning

Workflow for Container Scanners



Agree upon 'what to test'

- Can you do something with the output?
- Will you do something with the output?

Use policies sparingly

Modify, update or upgrade container when necessary

Container Scanners

Detect compliance validations

Detect out of date libraries

Suggest best practices

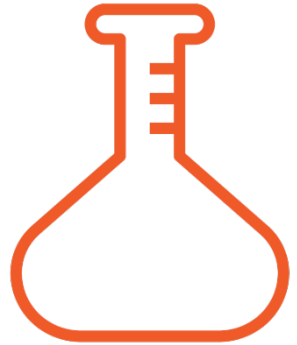
Advantage

Hardens containers

Ensures out of date operating system is being noticed

Compatibility

Open Container Initiative (OCI) image format widely supported



Trialability

Substantial infrastructure requirements

Choice for a ‘framework’

Container security scanning is fairly young, and the landscape changes rapidly

More Information

https://anchore.com/opensource

Summary

Be notified when containers are outdated or insecure

Container security scanning becomes more important

Relatively more difficult to implement

Next Up

Maeve

"We will take a look at this in due time"

"So far we focused mainly on static scanning"

"Are you interested in dynamic infrastructure security testing?"

"Absolutely, let's go!"

Jennifer