Approaching Automated Security Testing in DevSecOps

UNDERSTANDING WHAT AND WHERE TO TEST DURING AUTOMATED SECURITY TESTING

Peter Mosmans
LEAD PENETRATION TESTER

@onwebsecurity https://www.onwebsecurity.com

Scenario

Maeve

"I can't wait to see..."

"Let's take a look at what can be tested...

...where in the life cycle...

...and how to approach the implementation."

Jennifer

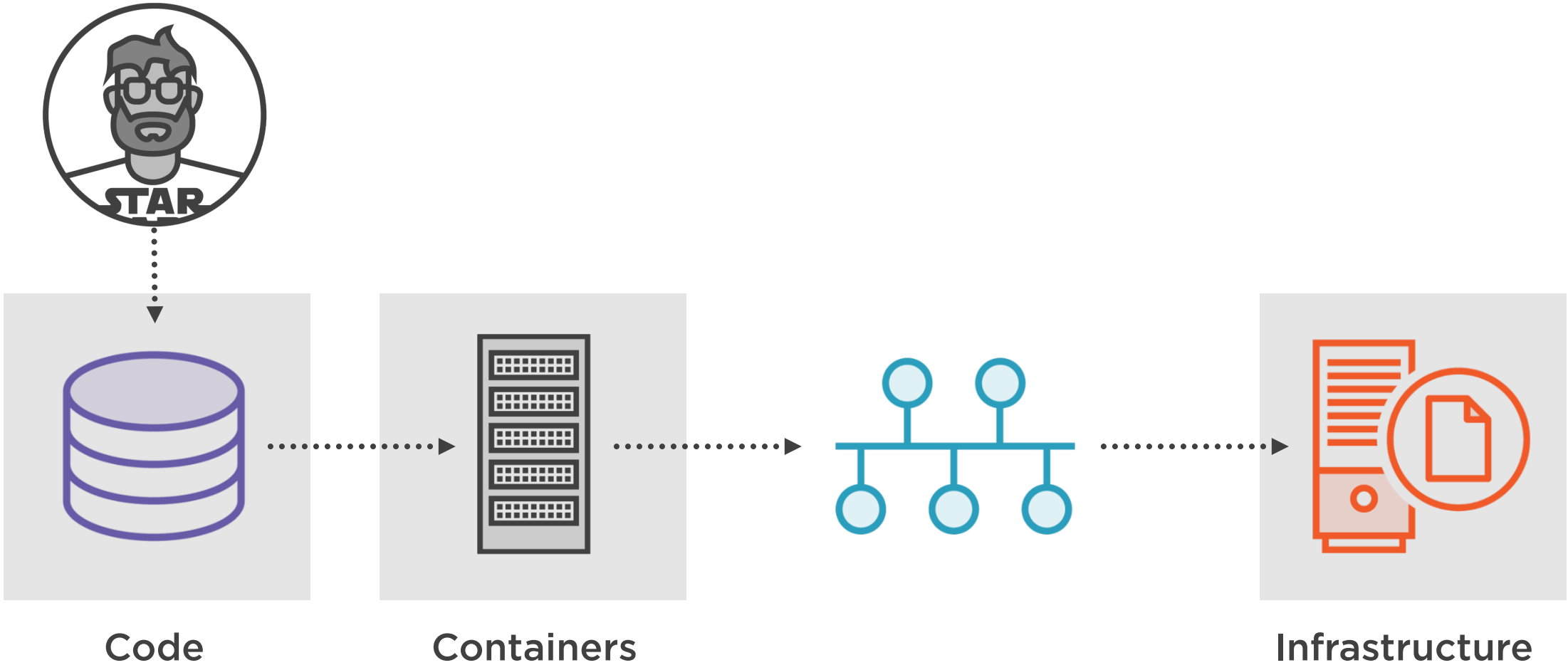
Module Overview

What can be tested

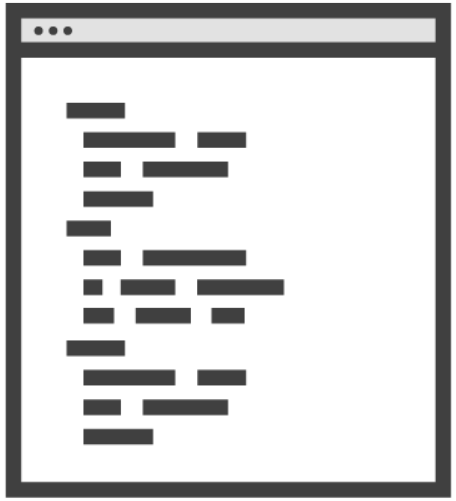
Where it can be tested in the software development life cycle

How to approach implementing automated security testing

Web Application

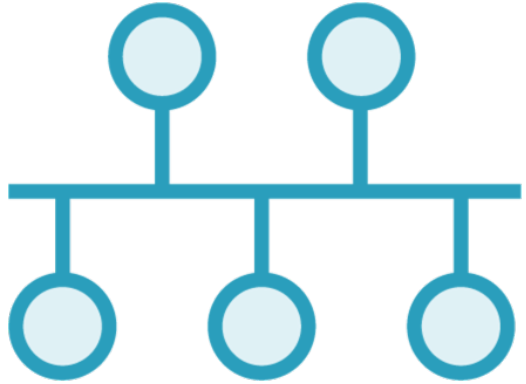


What to Test



Code

Containers



Infrastructure

Code

Readability

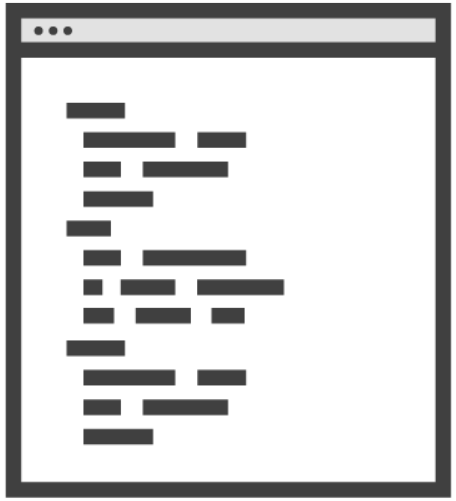
Maintainability and clarity

Insecure patterns

(Hardcoded) secrets

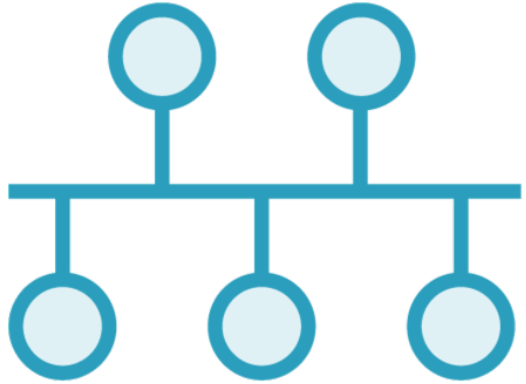
Insecure third-party libraries

What to Test



Code

Containers



Infrastructure

Containers

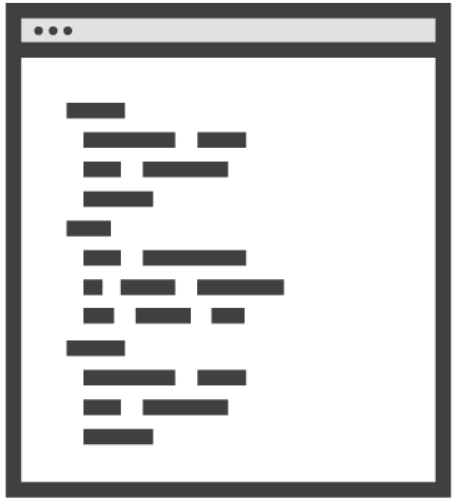
Poisoned images

Insecure third-party software

Hardening

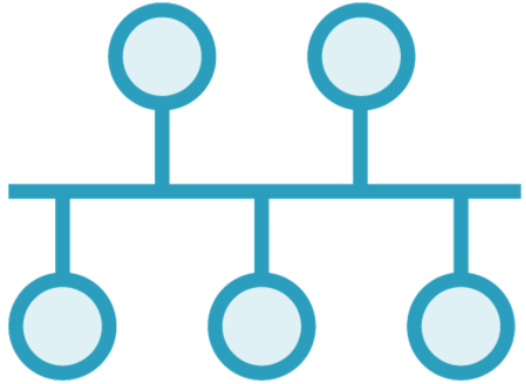
Integrity and verification

What to Test



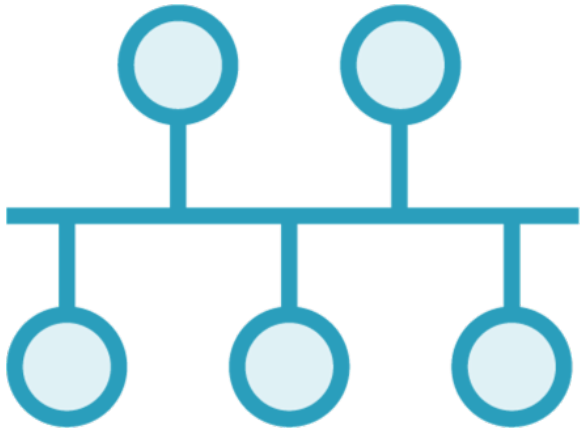
Code

Containers



Infrastructure

Infrastructure



Hardening

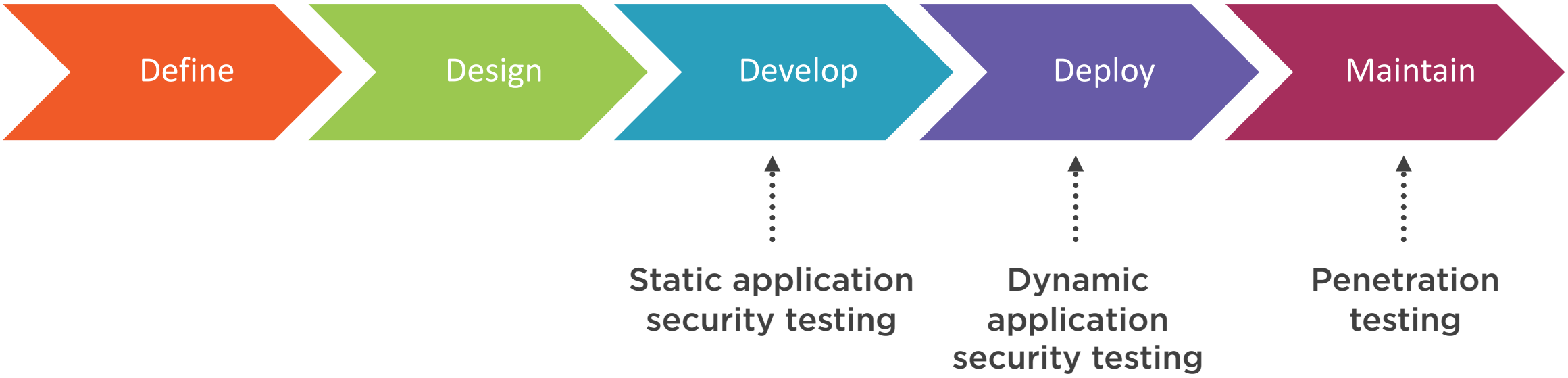
Configuration errors

Server and network vulnerabilities

See the course “Performing DevSecOps Automated Security Testing” for more information about tooling.

Where to Perform Automated Security Testing

Shift Left


Define
Design
Develop
Deploy
Maintain
Static application security testing
Dynamic application security testing
Penetration testing

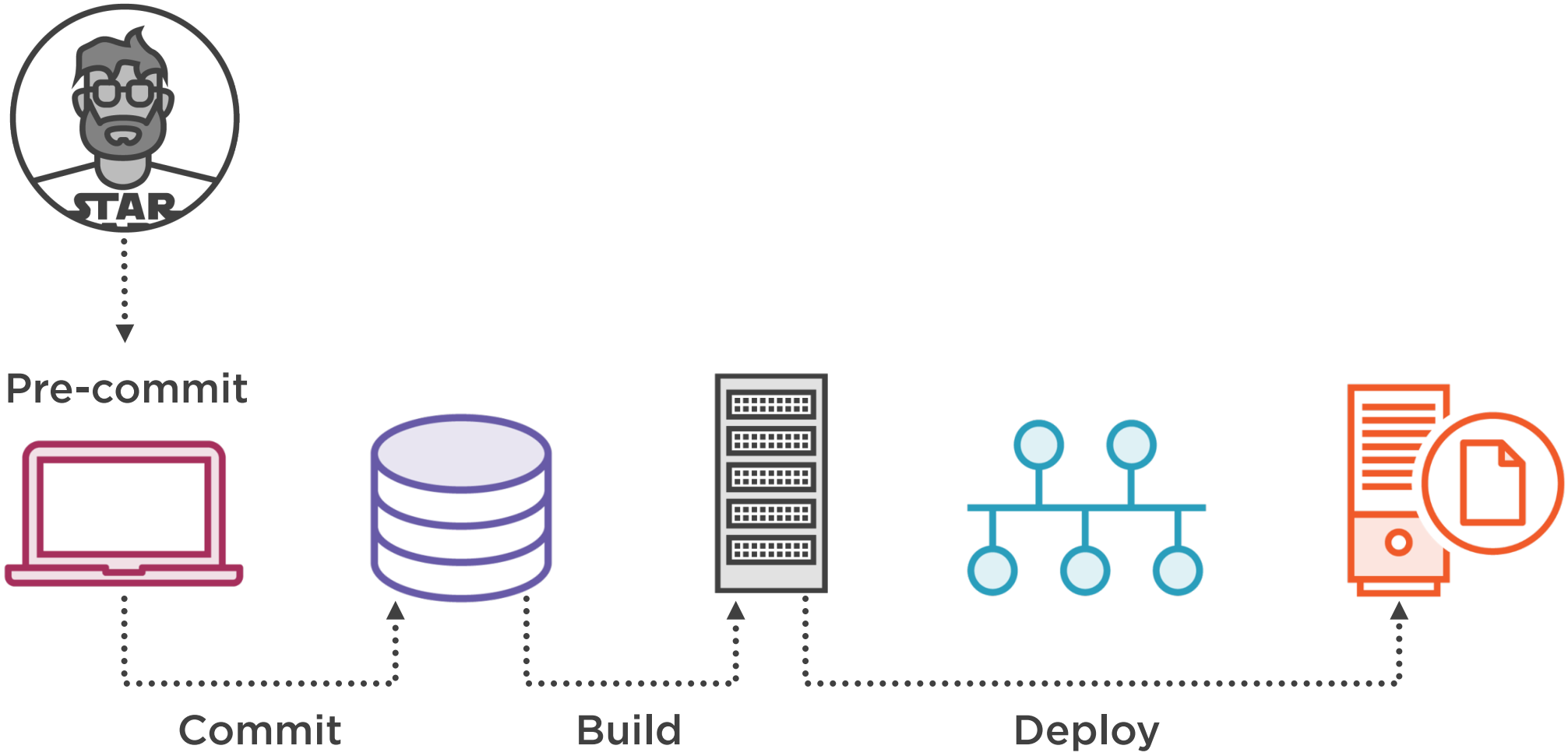
Advantages of Shifting Security Testing Left

Better accountability

Sooner means easier and cheaper to fix

It codifies security requirements earlier on

Where to Perform Tests



Pre-commit

Linters

- Formatting (readability and clarity)

Hardcoded secrets

Commit

Linters

- Formatting

Maintainability

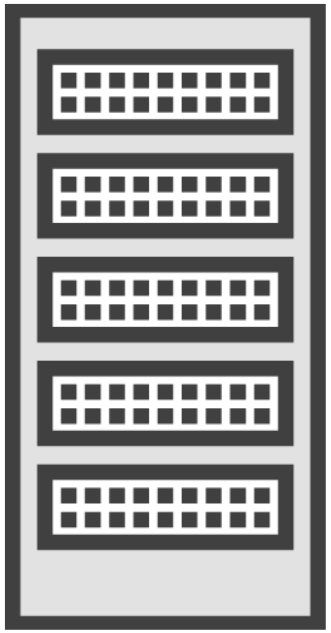
Clarity

Insecure patterns

(Hardcoded) secrets

Insecure third-party libraries

Build



Dynamic scanning

- Attack proxies

Fuzzing

Configuration errors

Deploy

Compliance checks

Runtime defense

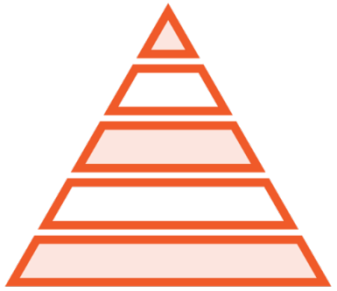
Hardening

How to Approach Implementing Automated Security Testing

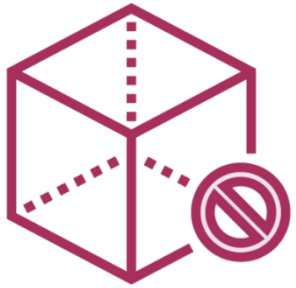
How to Approach Automated Security Testing

Let the team pick its own tools

Start with quick wins first



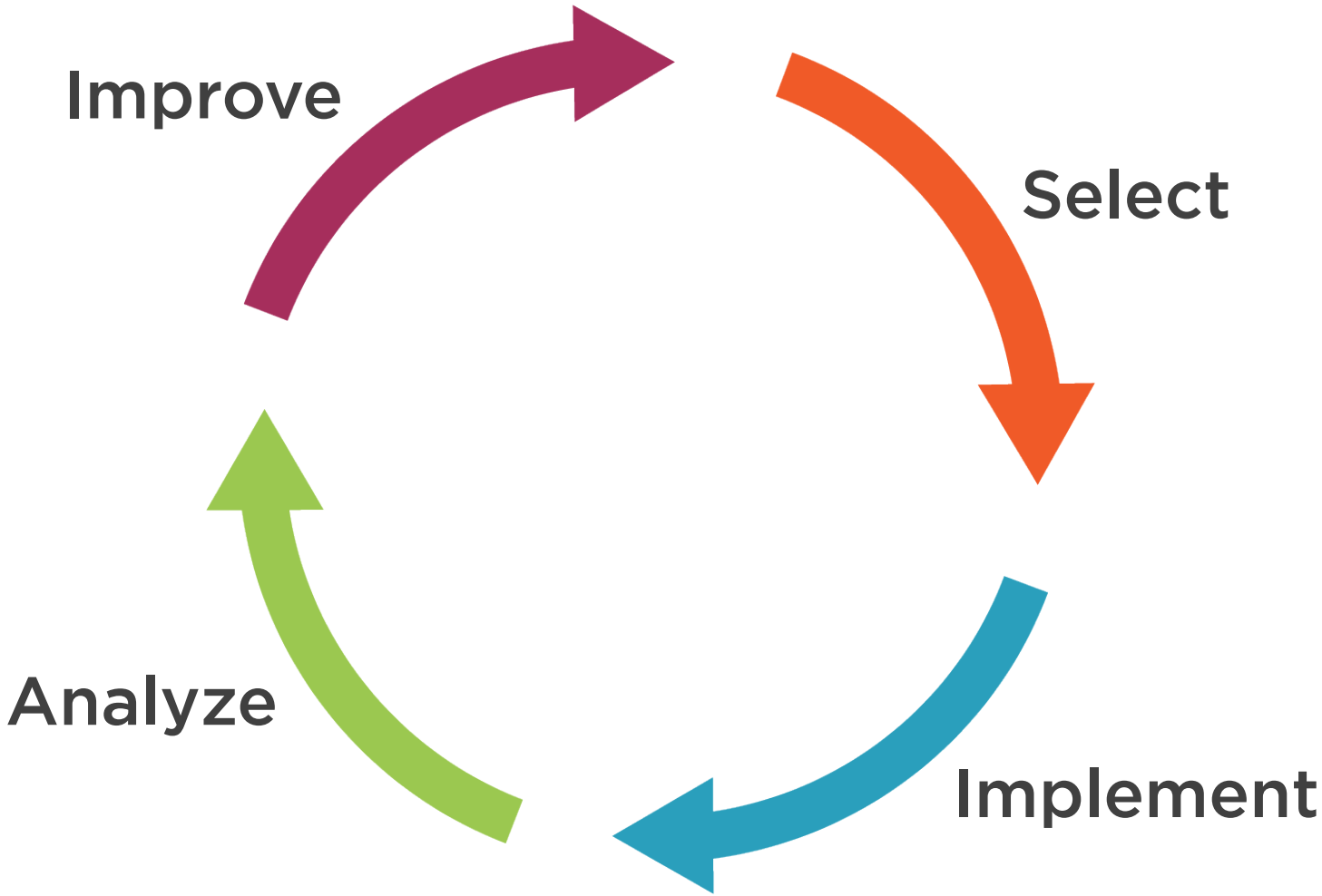
Invest time in setting a baseline



Don’t use hard quality gating

Plan time to configure and weed out false positives

Iterative Process



Automated Security Testing
is a process,
and not a product

Summary

Focus on quick wins first

Facilitate, not mandate

Start with a case-by-case approach

Security is always a trade-off

- Costs vs. benefits

Automated security testing is a process

Scenario

Maeve

"Thanks for explaining the concepts"

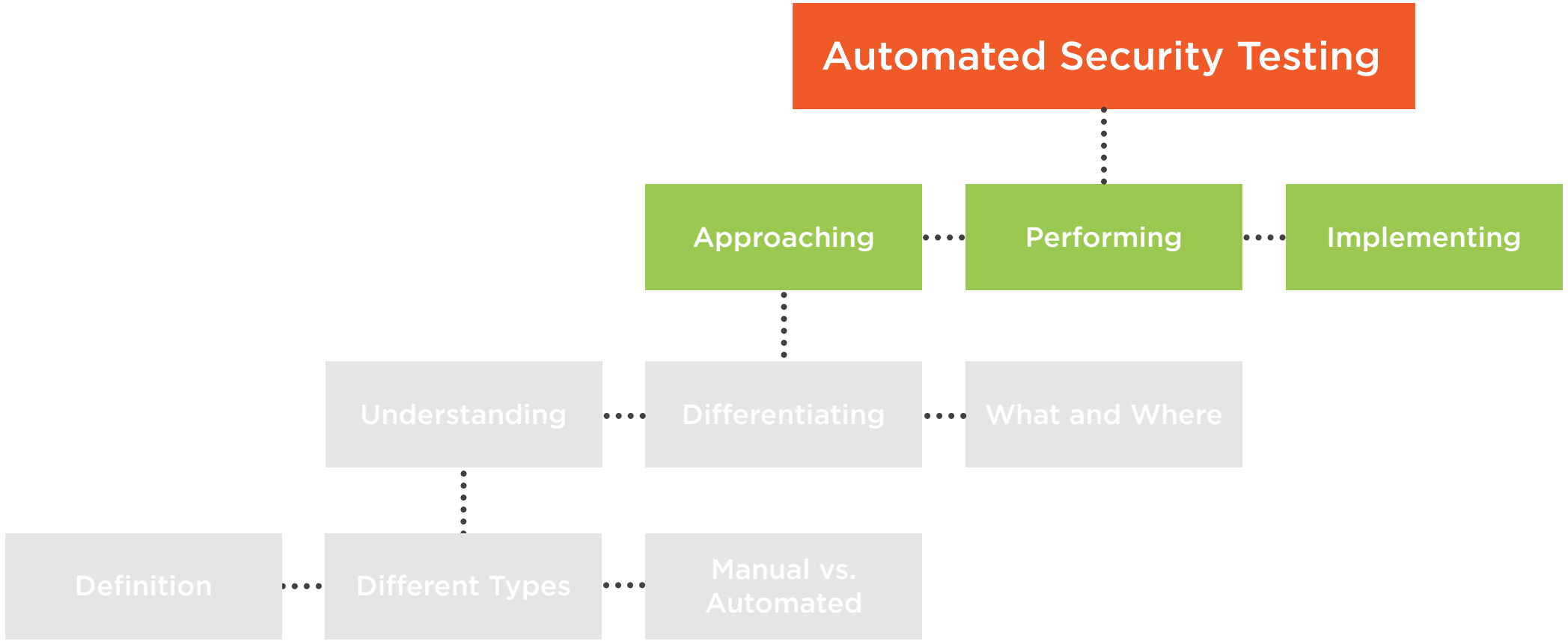
"What are my next steps?"

"You

"

Jennifer

Automated Security Testing Overview



Thanks for Watching!

Peter Mosmans
LEAD PENETRATION TESTER

@onwebsecurity https://www.onwebsecurity.com