Approaching Automated Security Testing in DevSecOps

UNDERSTANDING AUTOMATED SECURITY TESTING

Peter Mosmans
LEAD PENETRATION TESTER

@onwebsecurity https://www.onwebsecurity.com

Scenario

Maeve

"What is automated security testing?"

"Is it something for us?"

"How should I approach it?"

Jennifer

What it is.

What can be tested.

Whether it's the right fit.

How to approach it.

Course Overview

Understanding Automated Security Testing

Differentiating the Pros and Cons of Automated Security Testing

Understanding What and Where to Test during Automated Security Testing

What's in It for Maeve?

Maeve

Jennifer

Who's This Course For?

- DevOps engineers
- Security professionals
- Developers
- Product owners
- Scrum masters
- Anyone interested in automated security testing

This course teaches concepts.

Part of the DevSecOps Path

Approaching
Automated
Security Testing

Performing
DevSecOps
Security Testing

Integrating
DevSecOps
Security Testing

Module Overview

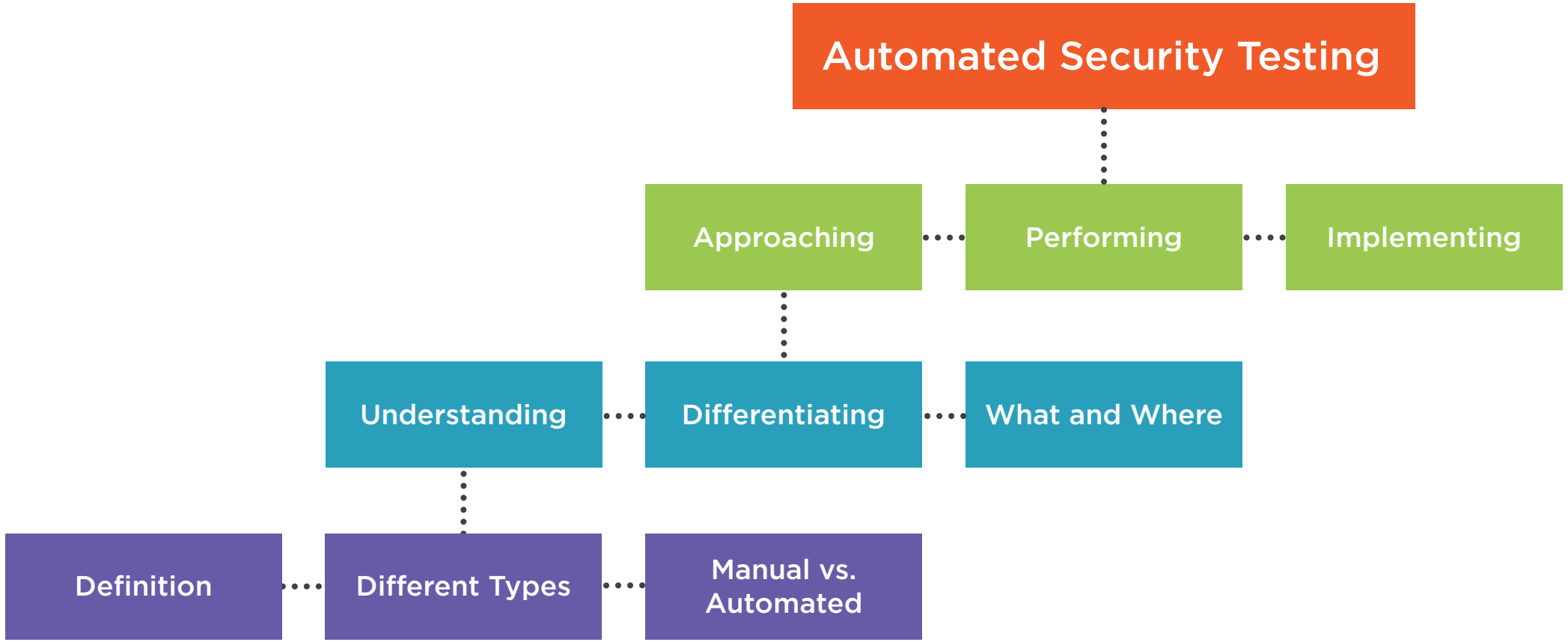
What is automated security testing?

Different types of security testing

- Static application security testing
- Dynamic application security testing
- Vulnerability scanning

Manual vs. automated testing

Automated Security Testing Overview

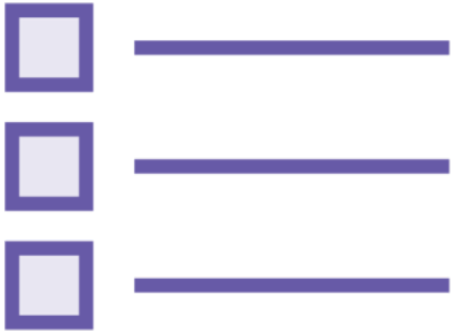


What Is Automated Security Testing?

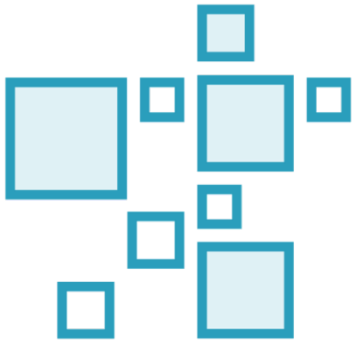
Automated Security Testing

Testing

Test Paths

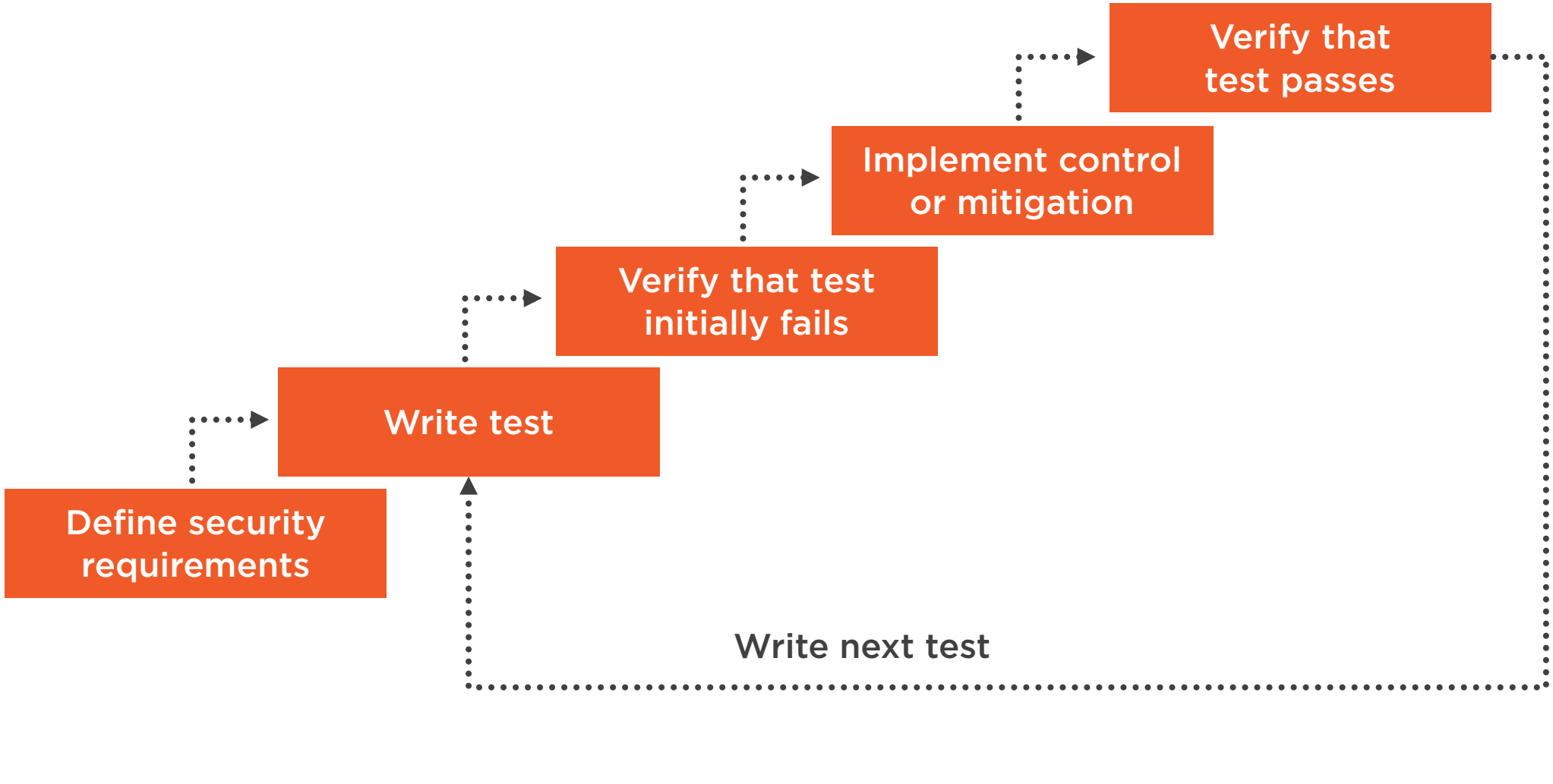


Testing Methods



Security Testing Types

Test-driven Security



Test-driven Security

Similar to test-driven development

Forces team to think of security beforehand...

...therefore security has to be defined

Happy path testing

Different Test Paths

Positive testing

Happy path

Negative testing

Sad path

Bad path

Negative Testing is Difficult

How do you know what it's not supposed to do?

Instead of a set of inputs there are unlimited different inputs

Output doesn't always show the error (sad path)

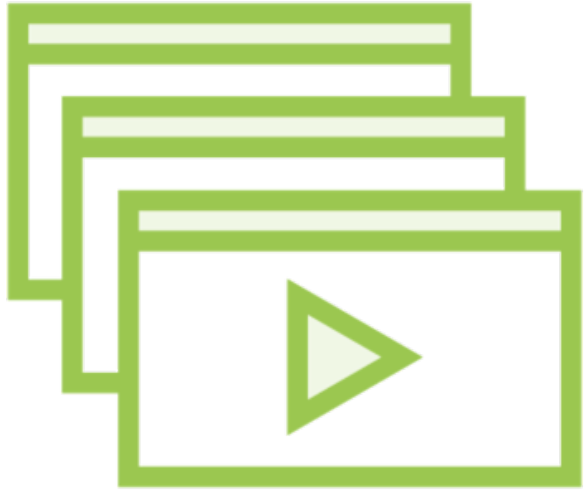
Two Methods of Testing

Static testing

Nothing is executed

Static source code review

Configuration review



Dynamic testing

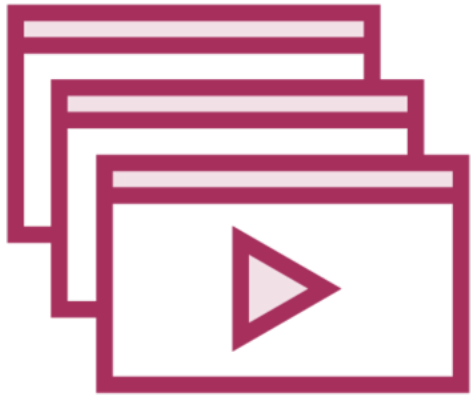
Running code or application

Dynamic application security testing

Network vulnerability scanning

Types of Security Testing

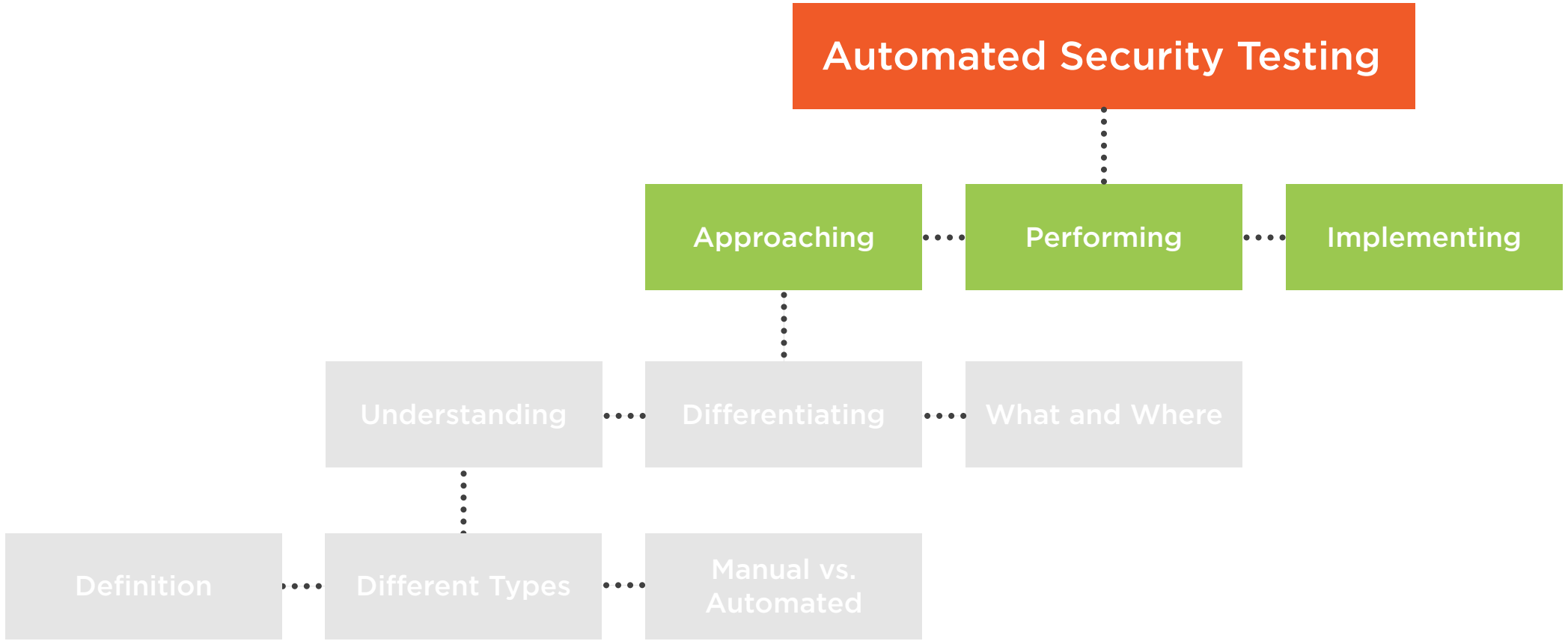
Static application security testing



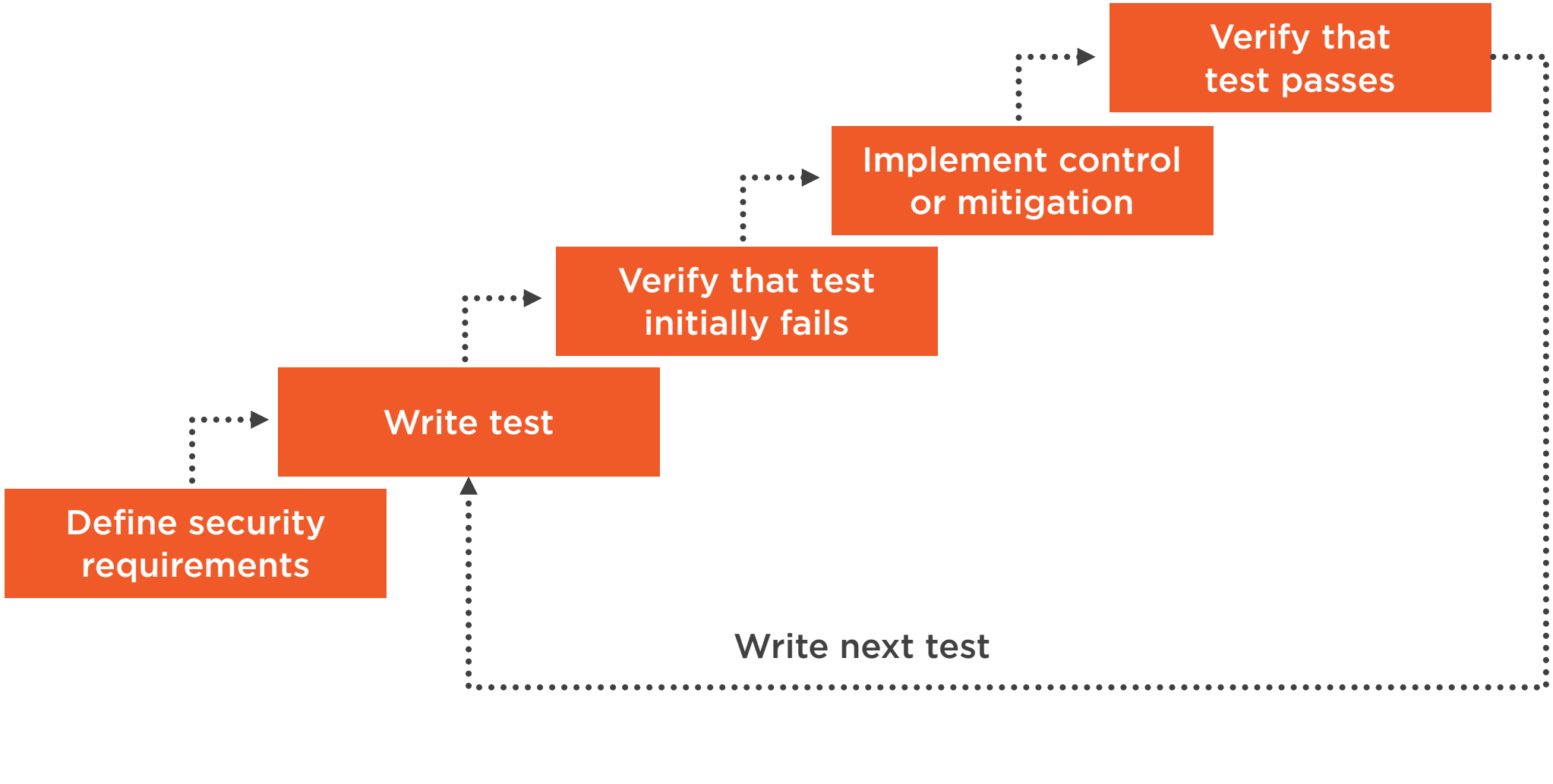
Dynamic application security testing

Vulnerability scanning

Automated Security Testing Overview



Test-driven Security



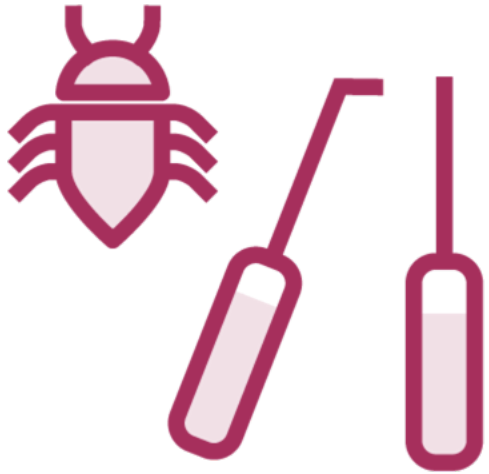
Static Application Security Testing

Static source code analysis

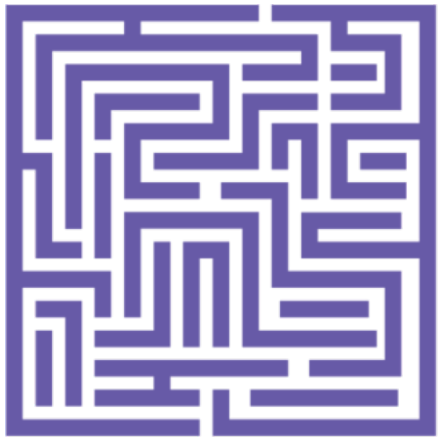
Linters

Checks on secrets in code

Dynamic Application Security Testing



Dynamic source code analysis



Fuzzers

Attack proxies

Vulnerability

A weakness that can be exploited

Which Vulnerabilities?

Known (and published) vulnerabilities

See the Pluralsight course

Secure Coding: Using Components with Known Vulnerabilities

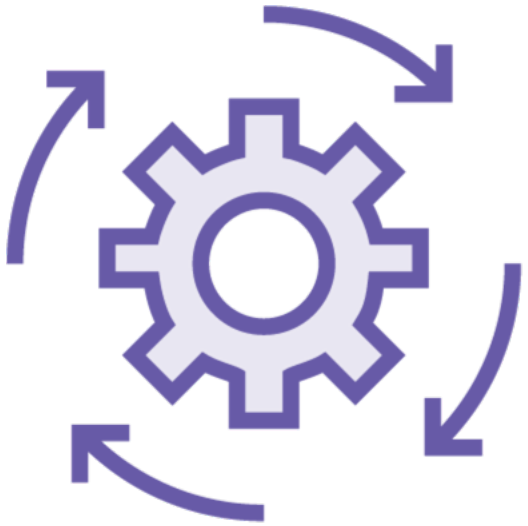
Automated Vulnerability Scanner

Fingerprint assets

Ingest lists of known vulnerabilities

Compare assets with lists

Automated Vulnerability Scanners



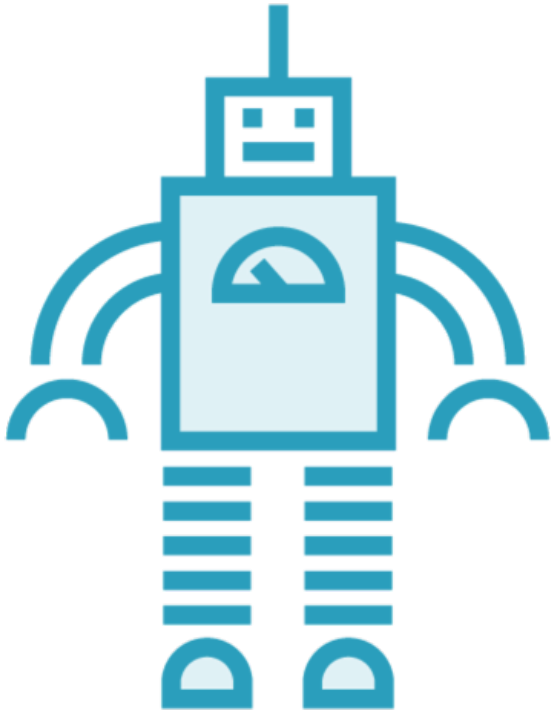
Network vulnerability scanner

Container vulnerability scanner

Third-party libraries scanner

Manual vs. Automated Testing

Automated Security Testing



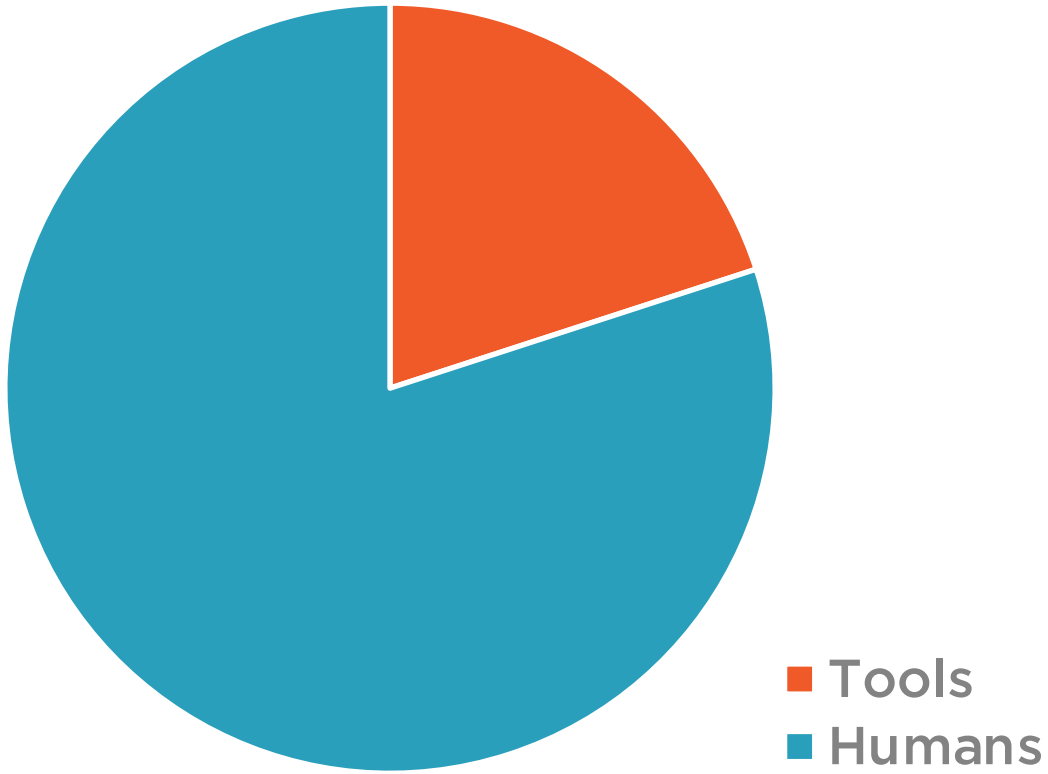
- Automated tests that run without manual intervention
- Static as well as dynamic testing
- Can be remote (centralized) as well as local
- Usually integrated into build pipelines
- Mainly negative testing

Manual vs. Automated Testing

Manual	Automated
Code review	Source code scanning
Check on credentials	Pre-commit git hook tools
Penetration test	Vulnerability scanning
Establish trustworthiness of third-party source code	Third-party trust verification

Automated testing
is not a
drop-in replacement
for manual testing

Effort to Use Tooling Effectively



Summary

Automated security testing

- Negative testing

Static application security testing

Dynamic application security testing

Vulnerability scanning

- Match assets against lists of known vulnerabilities

Manual vs. automated testing

- One not a replacement for the other

Next Up

Maeve

"Thanks"

"You're very welcome."

"Do you want to know about the pros and cons?"

"That would be great."

Jennifer