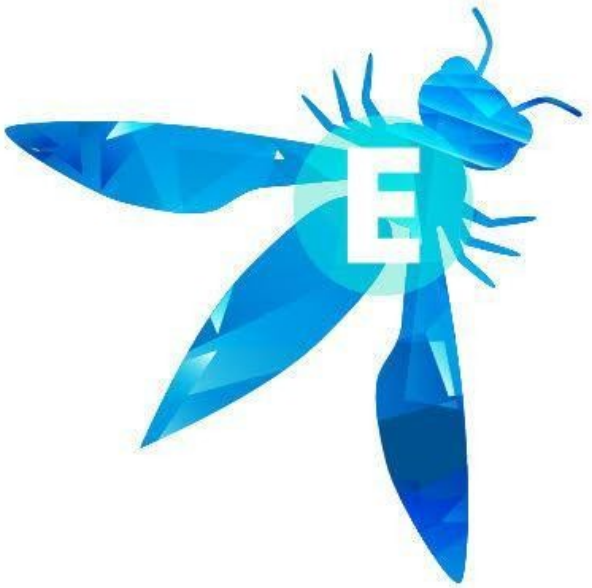


SecOps live cooking with OWASP appsec tools

Maciej Lasyk

OWASP EEE – Kraków

2015-10-06

Join Fedora Infrastructure!

→ learn Ansible

→ join the security team!

→ use Fedora Security Lab (spin)

http://fedoraproject.org/en/join-fedora

Agenda?

- → about delivery pipeline
- → demos
  - → manual testing
  - → automation
  - → delivery pipeline

Agenda?

- → about delivery pipeline
- → demos
  - → manual testing
  - → automation
  - → delivery pipeline

Agenda?

- → about delivery pipeline
- → demos
  - → manual testing
  - → automation
  - → delivery pipeline

Agenda?

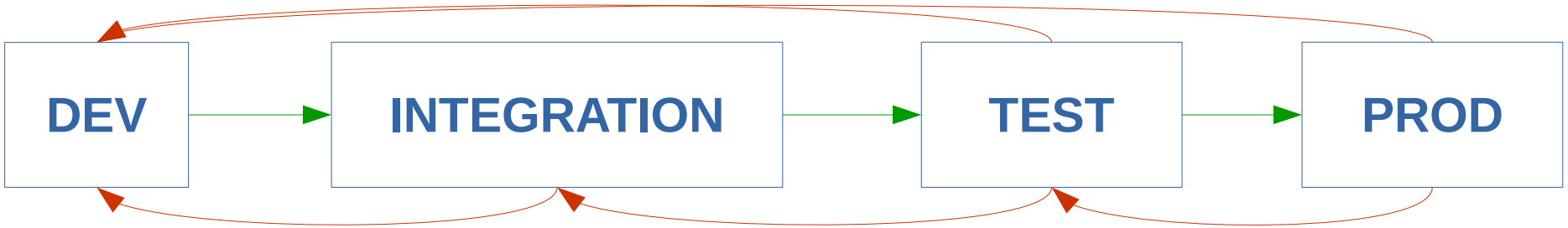
- → about delivery pipeline
- → demos
  - → manual testing
  - → automation
  - → delivery pipeline

Agenda?

- → about delivery pipeline
- → demos
  - → manual testing
  - → automation
  - → delivery pipeline

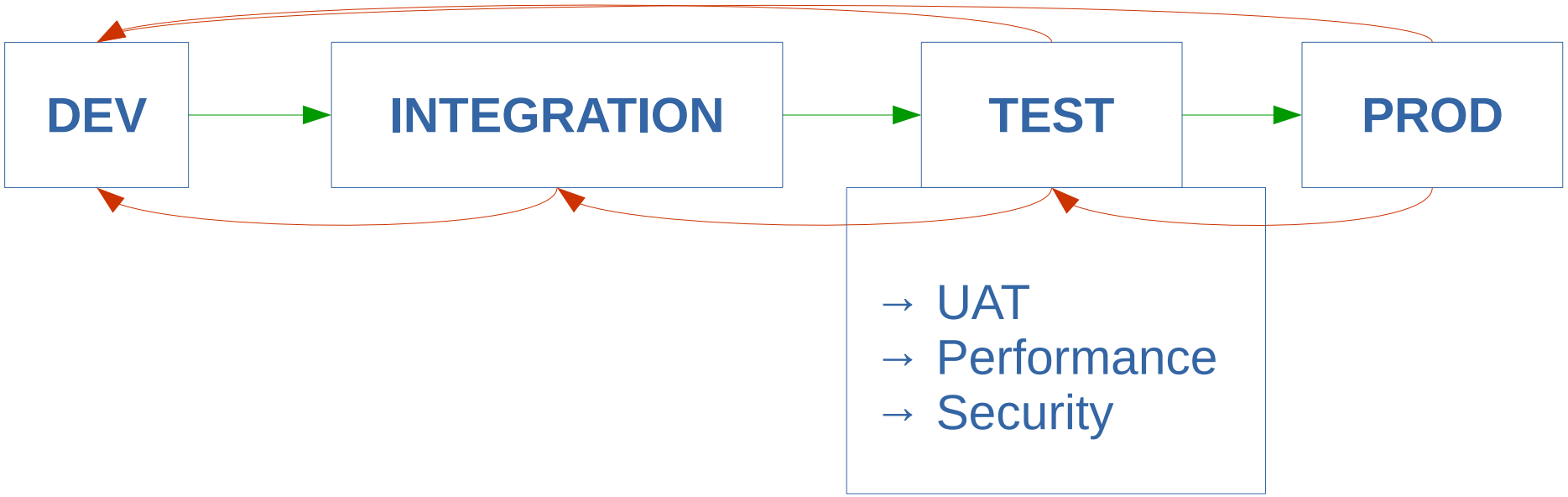
Delivery Pipeline & security testing

Delivery Pipeline!



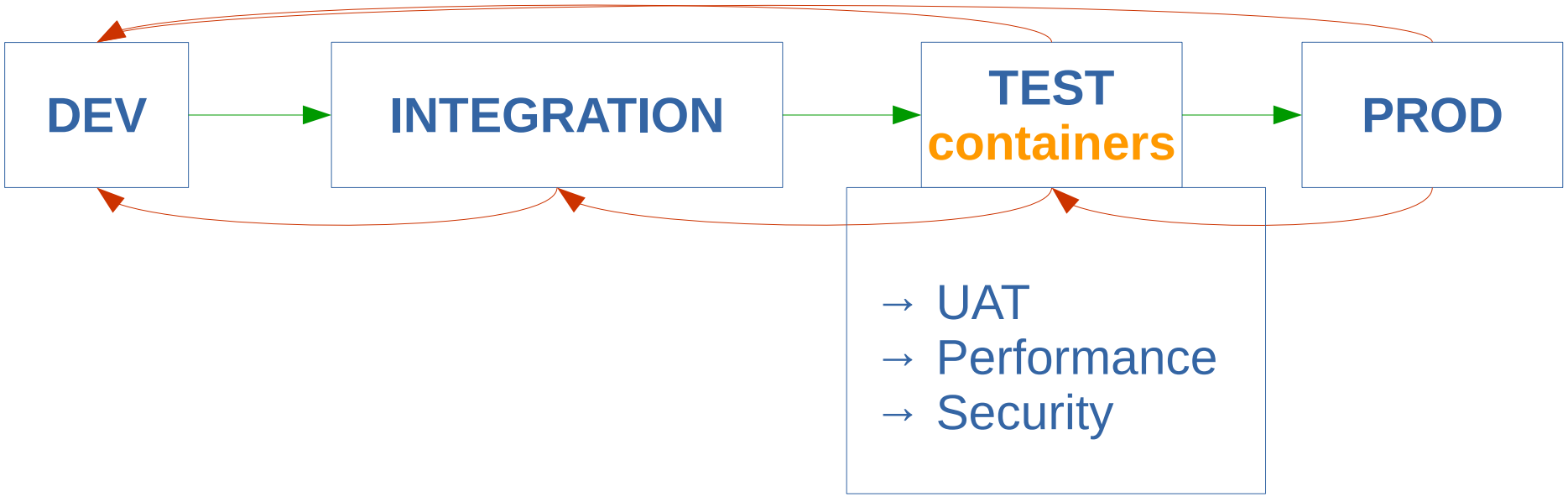
Feedback loop!

Delivery Pipeline!



Feedback loop!

Delivery Pipeline!



Feedback loop!

Experimentation gives you improvements!

Continuous security scanning

Delivery Pipeline!

→ shortening the cycle time

→ viability of scanning windows

→ burndown charts - security testing slice is usually tiny

→ security testing has to be faster

→ providing instant feedback

→ CD is a goal

Delivery Pipeline!

→ shortening the cycle time

→ viability of scanning windows

→ burndown charts - security testing slice is usually tiny

→ security testing has to be faster

→ providing instant feedback

→ CD is a goal

Delivery Pipeline!

→ shortening the cycle time

→ viability of scanning windows

→ burndown charts - security testing slice is usually tiny

→ security testing has to be faster

→ providing instant feedback

→ CD is a goal

Delivery Pipeline!

→ shortening the cycle time

→ viability of scanning windows

→ burndown charts - security testing slice is usually tiny

→ security testing has to be faster

→ providing instant feedback

→ CD is a goal

Delivery Pipeline!

→ shortening the cycle time

→ viability of scanning windows

→ burndown charts - security testing slice is usually tiny

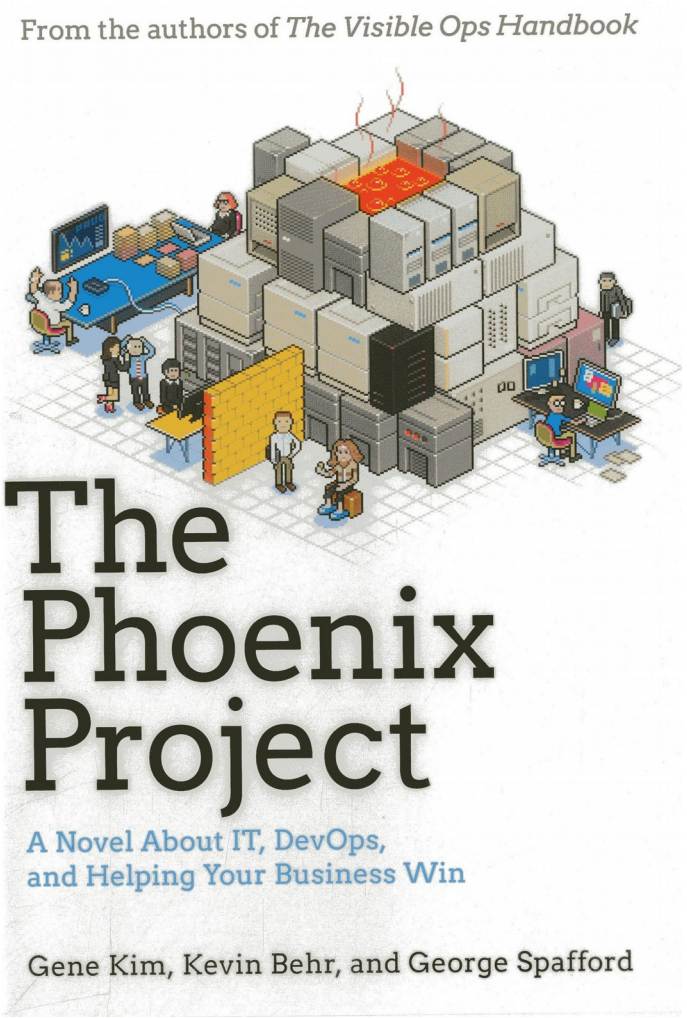
→ security testing has to be faster

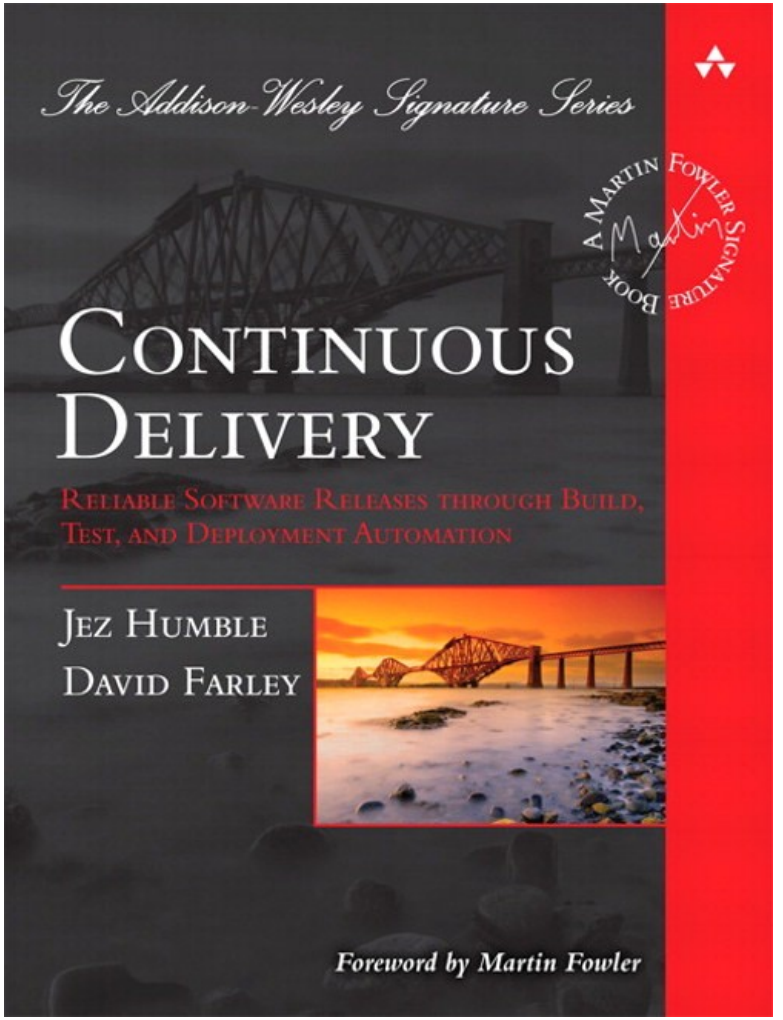
→ providing instant feedback

→ CD is a goal

Delivery Pipeline!

- → shortening the cycle time
- → viability of scanning windows
- → burndown charts - security testing slice is usually tiny
- → security testing has to be faster
- → providing instant feedback
- → CD is a goal


From the authors of *The Visible Ops Handbook*
The Phoenix Project
A Novel About IT, DevOps, and Helping Your Business Win
Gene Kim, Kevin Behr, and George Spafford


The Addison-Wesley Signature Series
A Martin Fowler Signature Book
CONTINUOUS DELIVERY
Reliable Software Releases through Build, Test, and Deployment Automation
Jez Humble
David Farley
Foreword by Martin Fowler

Manual testing demo #1

OWASP webgoat, OWASP hackademic story

test-app

vs

OWASP ZAP

Manual testing demo #1

OWASP webgoat, OWASP hackademic story

test-app

vs

OWASP ZAP

Manual testing demo #2

Fedora Pagure

vs

OWASP Dependency Check

Automation tools

→ Ansible (www.ansible.com)

→ Jenkins (jenkins-ci.org)

→ GoCD (www.go.cd)

Automation tools

→ Ansible (www.ansible.com)

→ Jenkins (jenkins-ci.org)

→ GoCD (www.go.cd)

Automation tools

→ Ansible (www.ansible.com)

→ Jenkins (jenkins-ci.org)

→ GoCD (www.go.cd)

Automation demo #1

Installing Jenkins w/Ansible

Linux Containers - Docker

→ Docker?

→ Docker Registry

Linux Containers - Docker

→ Docker?

→ Docker Registry

Automation demo #2

OWASP ZAP && Dependency Check + Docker

Automation demo #3

OWASP ZAP && Dependency Check + Docker

+

Jenkins

Automation demo #4

Containerization of security tools

Docker inside Docker?

Pros and cons

Automation demo #5

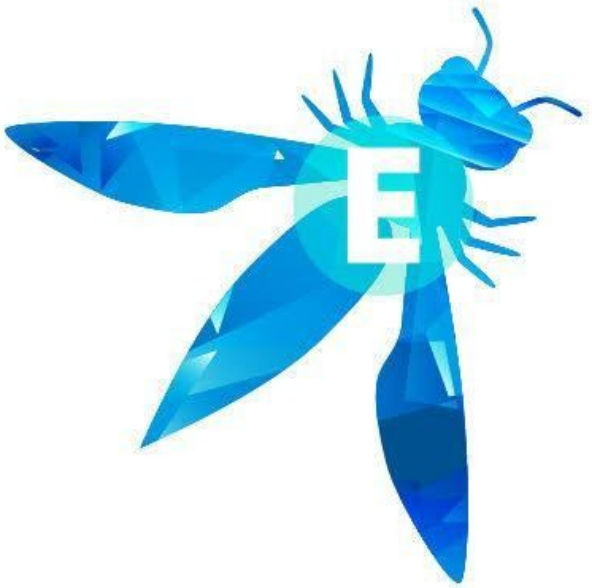
What about false positives / negatives?

Automation demo #6

Full delivery pipeline

Summary

Should we replace classical pentests with automation?



SecOps live cooking with OWASP appsec tools

Maciej Lasyk

OWASP EEE – Kraków

2015-10-06