Sense of Security™

DevOps – A How To for Agility with Security

Murray Goldschmidt, COO

ACSC
AUSTRALIAN CYBER SECURITY CENTRE
2016
CONFERENCE
12 – 14 April | Canberra

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney
Level 8, 66 King Street
Sydney NSW 2000
Australia

Melbourne
Level 15, 401 Docklands Drv
Docklands VIC 3008
Australia

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

What is DevOps?

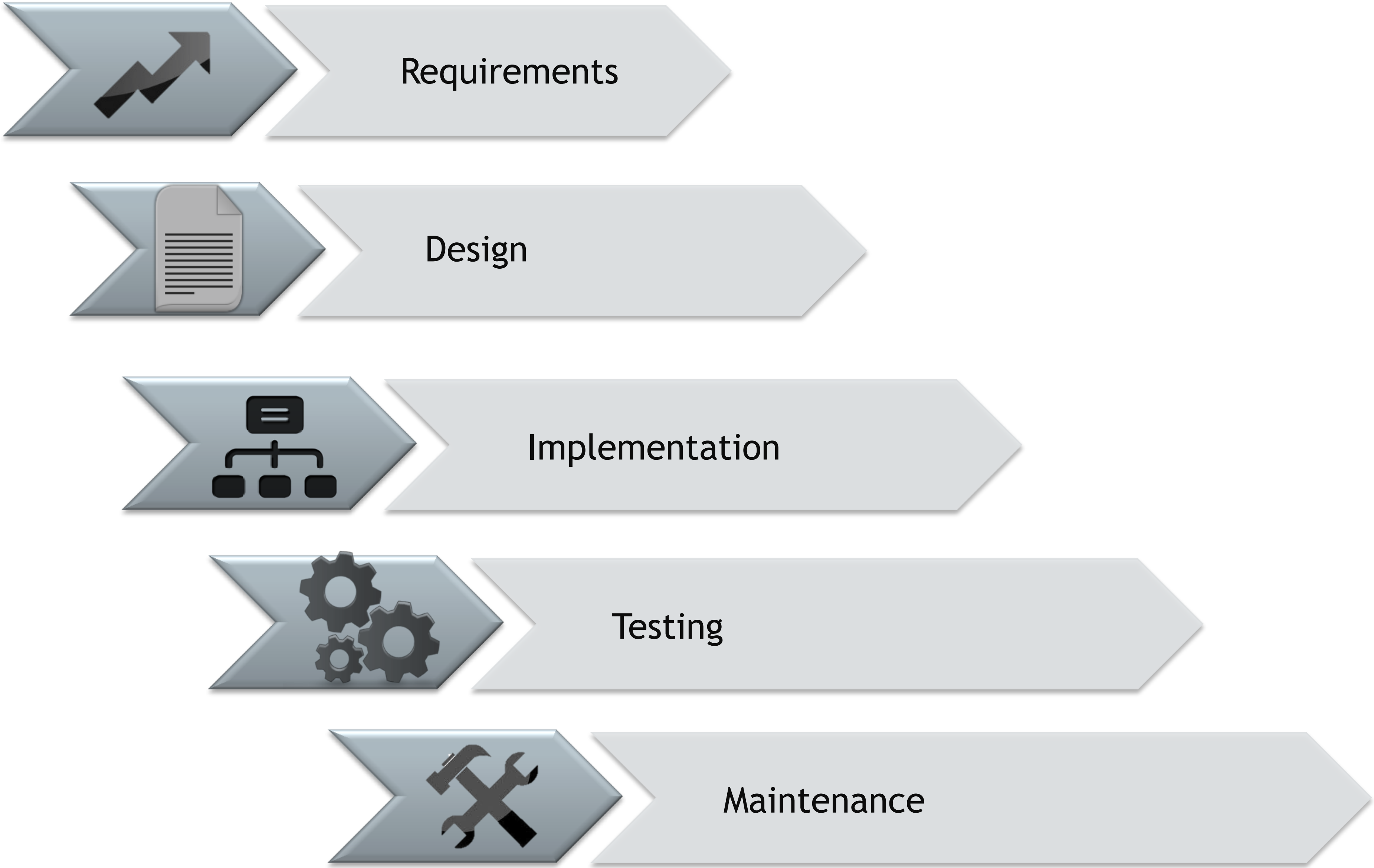
DevOps is the practice of ***operations*** *and* ***development*** *engineers participating together in the* ***entire service lifecycle****, from design through the development process to* ***production*** *support.*

Why DevOps?

*Lean practices, when applied to software delivery, **improve** both **throughput** and **stability**, leading to higher organisational **performance**.*

(Puppet Labs)

Waterfall



Requirements

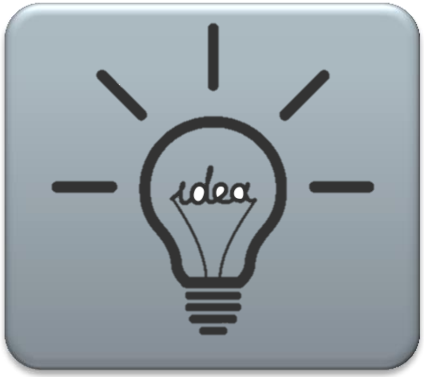
Design

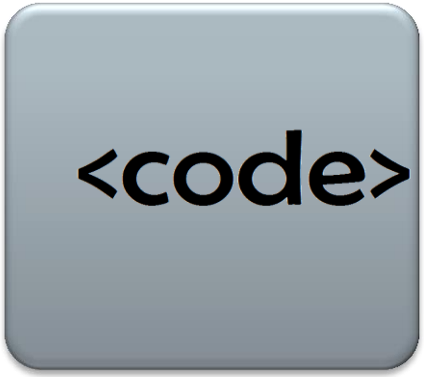
Implementation

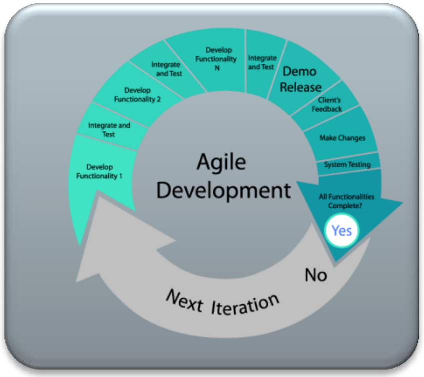
Testing

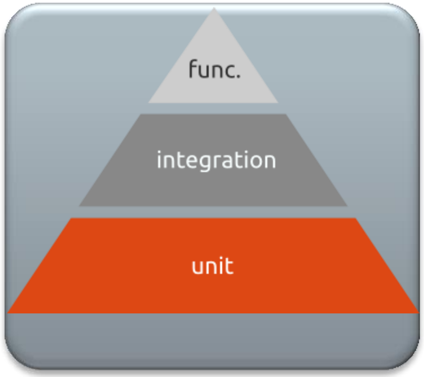
Maintenance

Agile Development

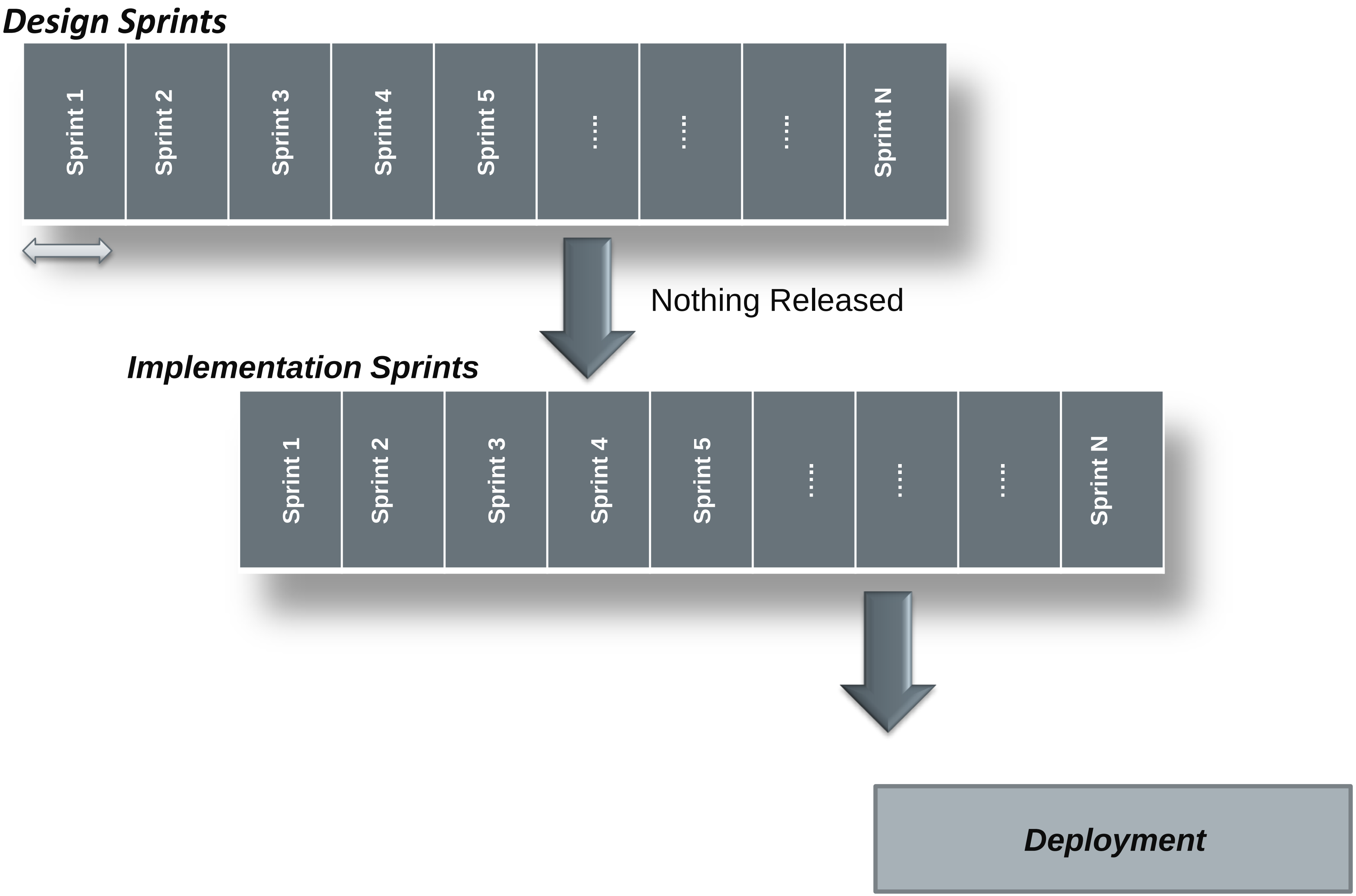








Agile Development?



Design Sprints

Sprint 1

Sprint 2

Sprint 3

Sprint 4

Sprint 5

…..

…..

…..

Sprint N

Nothing Released

Implementation Sprints

Sprint 1

Sprint 2

Sprint 3

Sprint 4

Sprint 5

…..

…..

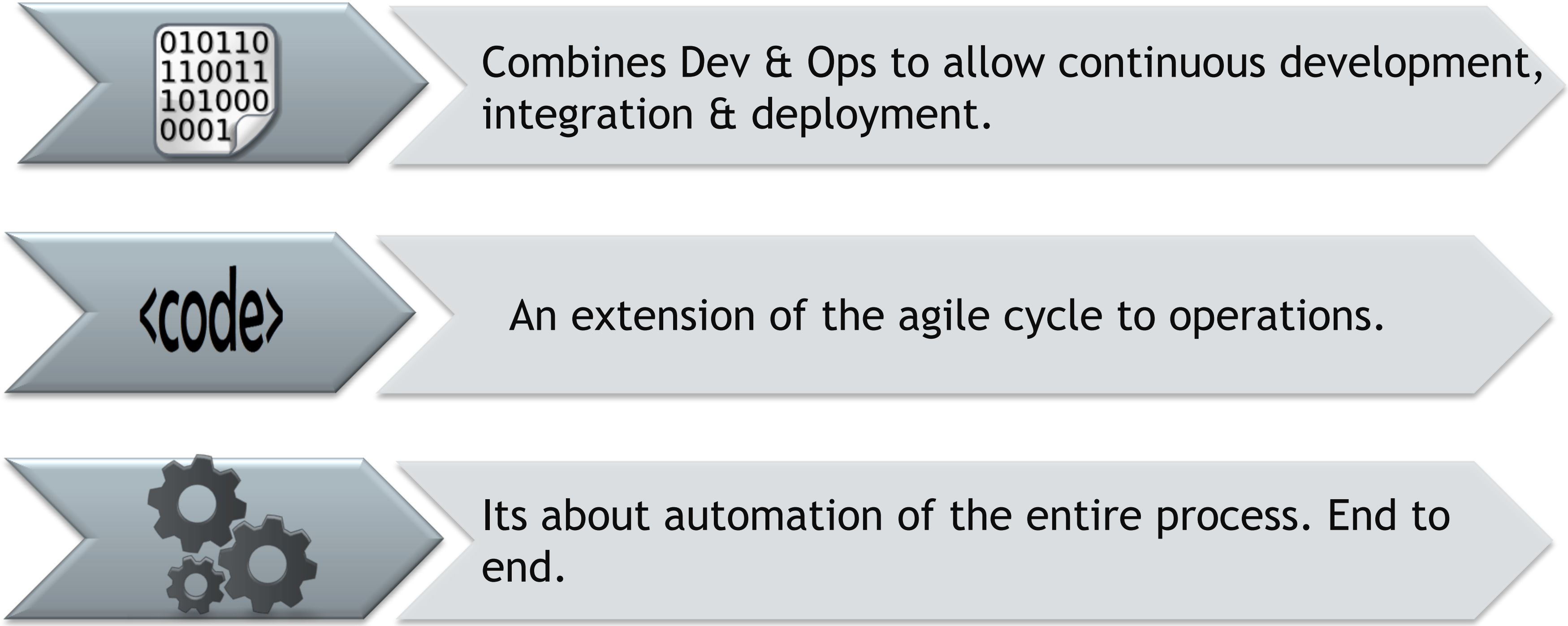
…..

Sprint N

Deployment

Sense of Security™

Enter DevOps. Designed to Fail?

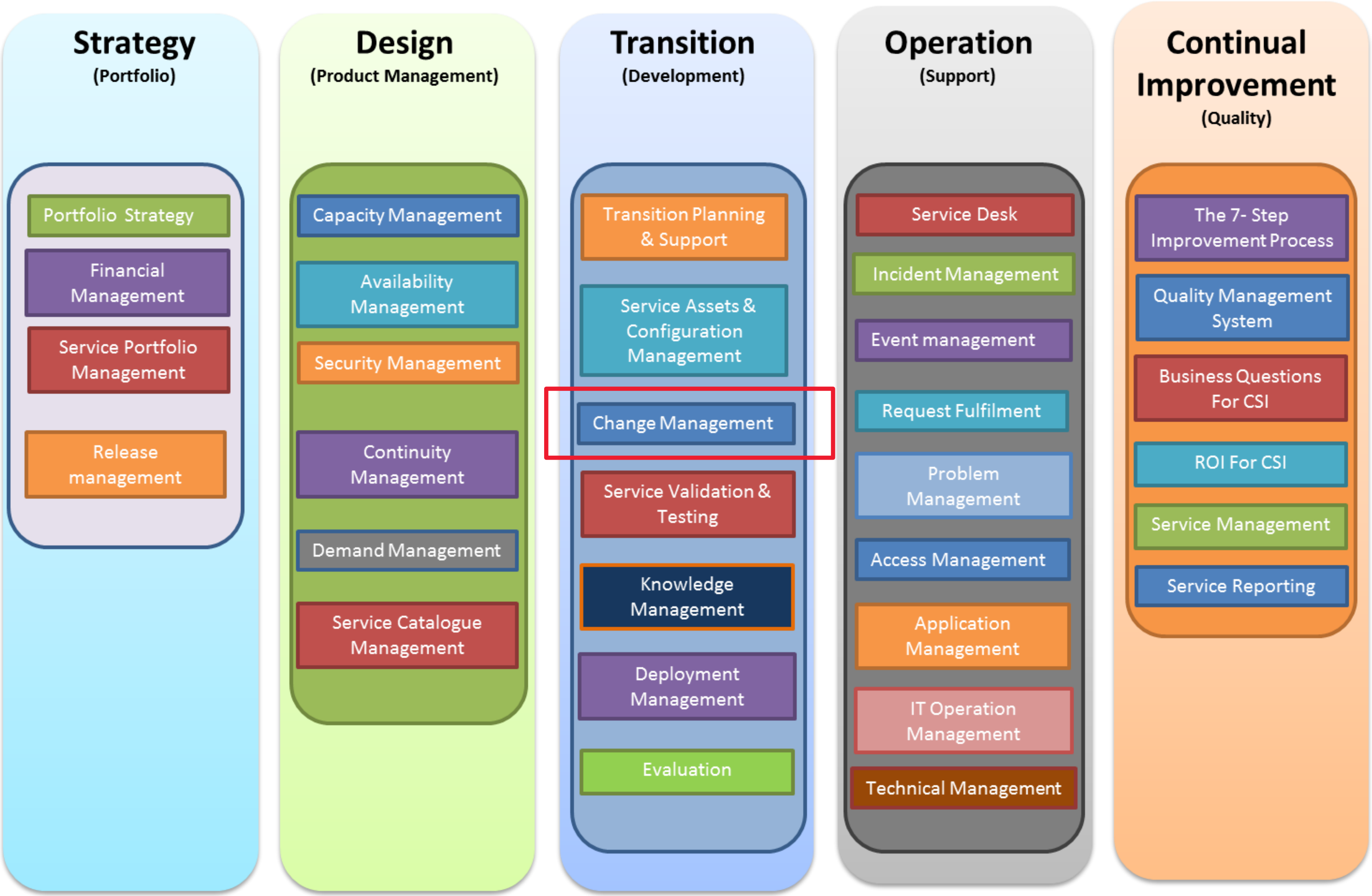


Combines Dev & Ops to allow continuous development, integration & deployment.

An extension of the agile cycle to operations.

Its about automation of the entire process. End to end.

Compatible with ITIL?



Strategy
(Portfolio)

- Portfolio Strategy
- Financial Management
- Service Portfolio Management
- Release management

Design
(Product Management)

- Capacity Management
- Availability Management
- Security Management
- Continuity Management
- Demand Management
- Service Catalogue Management

Transition
(Development)

- Transition Planning & Support
- Service Assets & Configuration Management
- Change Management
- Service Validation & Testing
- Knowledge Management
- Deployment Management
- Evaluation

Operation
(Support)

- Service Desk
- Incident Management
- Event management
- Request Fulfilment
- Problem Management
- Access Management
- Application Management
- IT Operation Management
- Technical Management

Continual Improvement
(Quality)

- The 7- Step Improvement Process
- Quality Management System
- Business Questions For CSI
- ROI For CSI
- Service Management
- Service Reporting

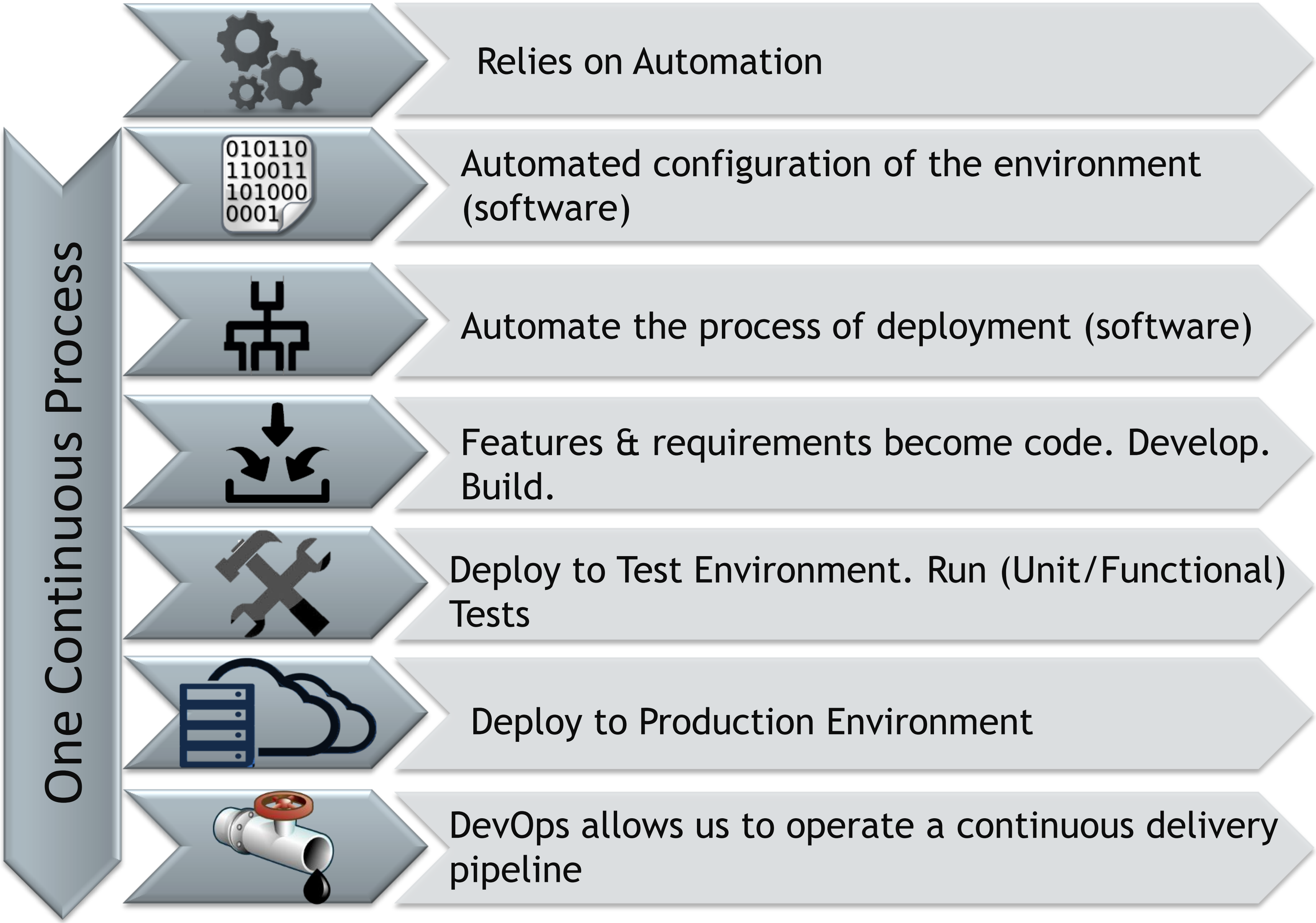
You Know What Happens

Too Many Barriers

Barriers Prevent Progress

Security – Productive Barriers

DevOps – Continuous Delivery



One Continuous Process

Relies on Automation

Automated configuration of the environment (software)

Automate the process of deployment (software)

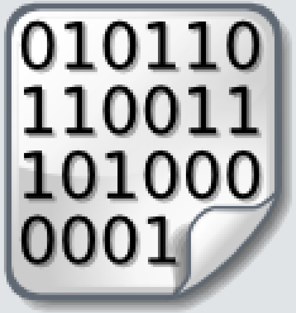
Features & requirements become code. Develop. Build.

Deploy to Test Environment. Run (Unit/Functional) Tests

Deploy to Production Environment

DevOps allows us to operate a continuous delivery pipeline

Silos Don't Work

Development	Operations	Security
		

Remove Gates – Provide Feedback

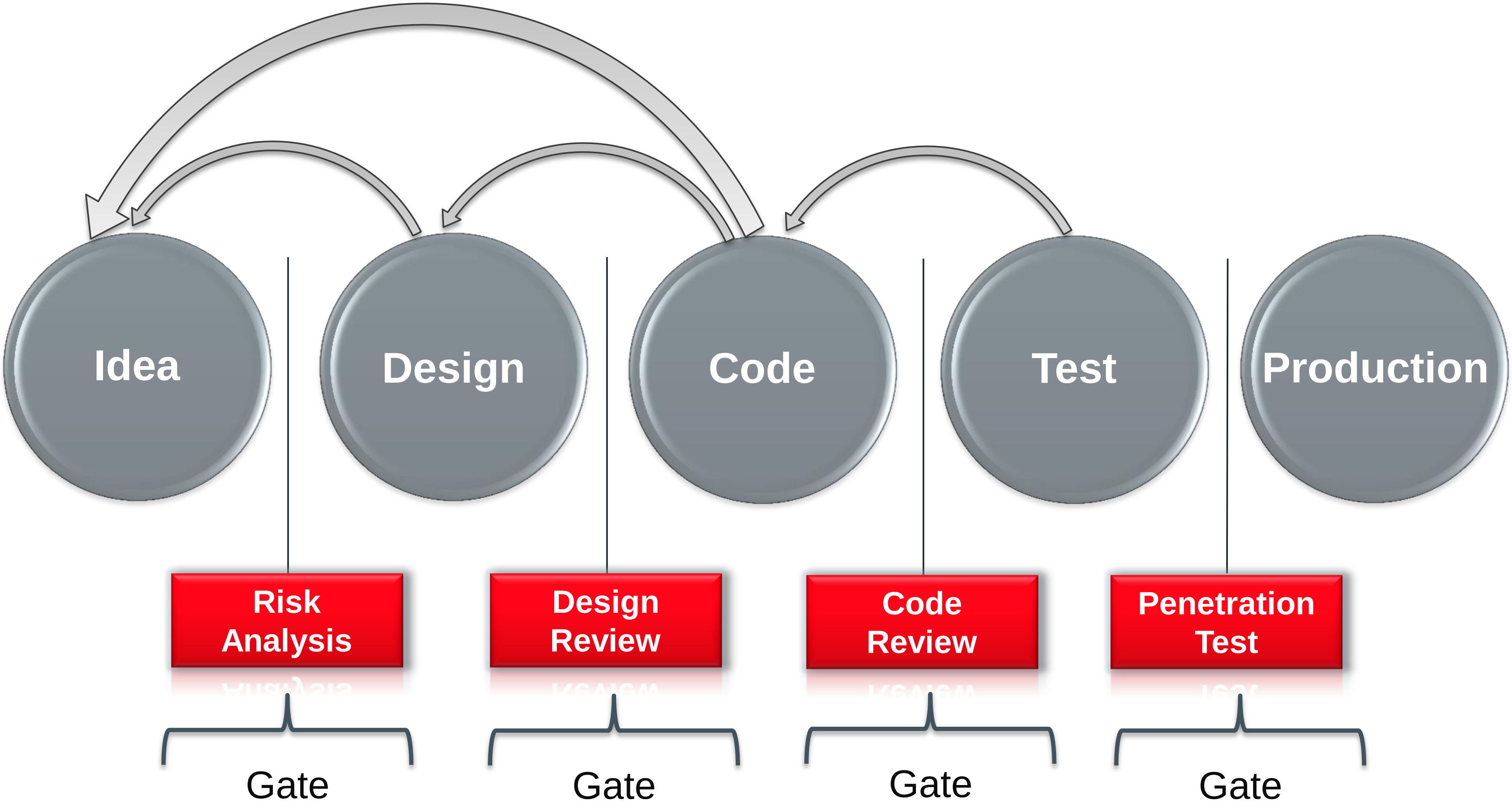


Image adapted from: Michael Brunton-Spall

DevOps Done Well

- Remove the barriers
- Shorten time to market. Transition from idea to product quickly (but securely)
- Identify issues quickly; Resolve issues quickly
- Quality at the source
- Improve feedback
- Remove silos
- Remove handovers

InfoSec Marginalised

*“The problem for the security person who is used to turning around **security reviews** in a **month** or two weeks is they're just being shoved out of the game. There's no way with how Infosec is currently configured that they can **keep up** with that. So, Infosec gets all the complaints about being **marginalized** and getting in the way of doing what needs getting done.”*

Gene Kim, author of *The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win*

The Problems

Lots of Developers

Fewer Ops People

Even Fewer
Security People

Viewpoint

Security & Compliance

can be a

drag on velocity

So we ….

need a change of view

DevOps Security is …..

A combination of

Security Culture

&

Security through

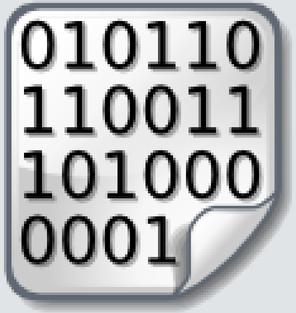
Technology Automation

Principles for Cyber Security

- $\Delta\chi\Delta\rho \geq \frac{\hbar}{2}$ Accept there will always be uncertainty
- Make everyone part of your delivery team
- Ensure the business understands the risks it is taking
- Trust competent people to make decisions
- Security is part of every technology decision
- User experience should be fantastic. Security should be good enough
- Demonstrate why you made the decisions - and no more
- Understand that decisions affect each other

Ref: https://www.gov.uk/government/publications/principles-of-effective-cyber-security-risk-management/principles-of-effective-cyber-security-risk-management

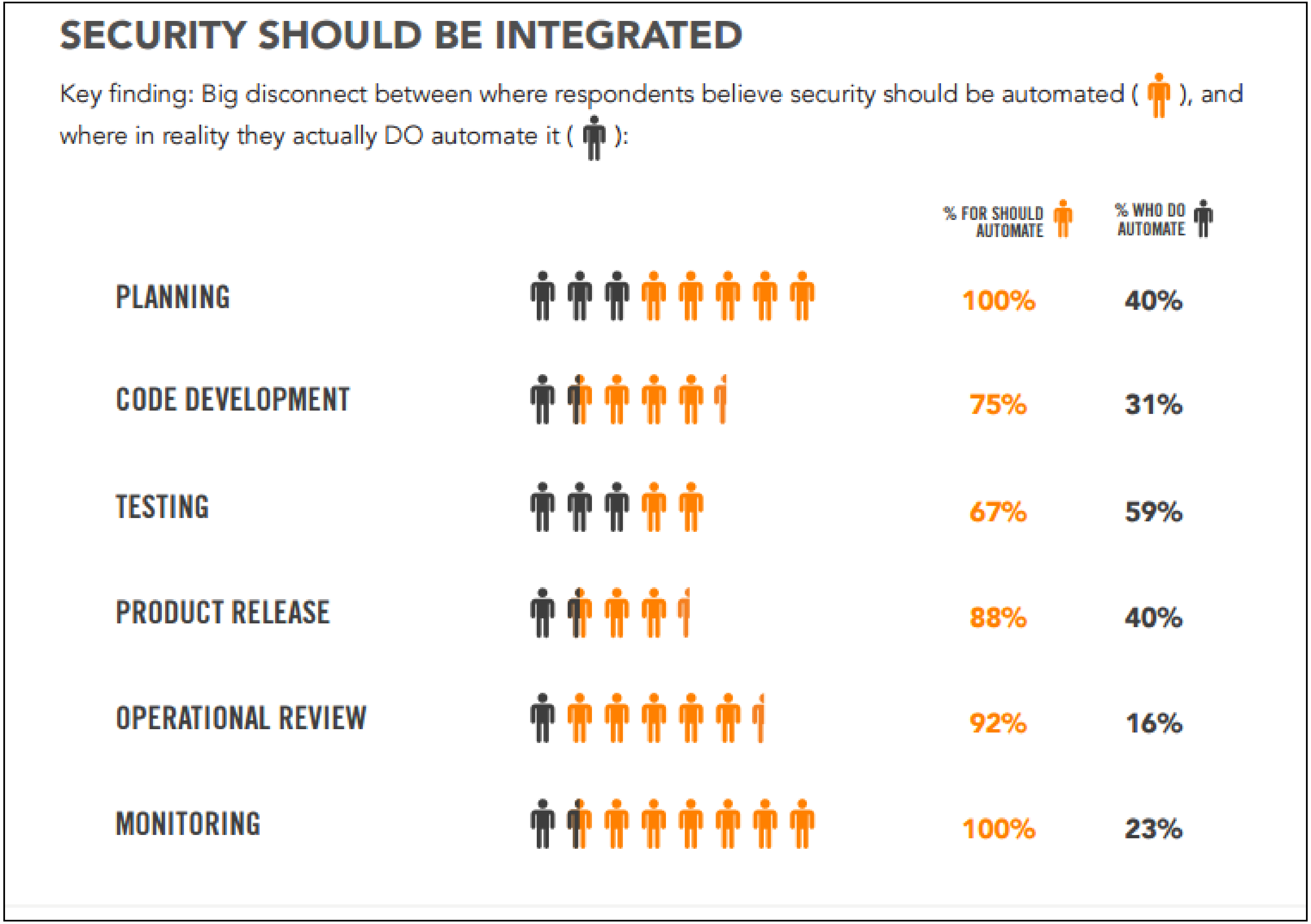
Cross Functional Teams

Business	Development	Operations	Security
			

Sharing: Ownership, Accountability, Objectives, Knowledge

Build Cross Functional Teams for a Service Delivery Lifecycle (SDLC)

Security Should be Integrated



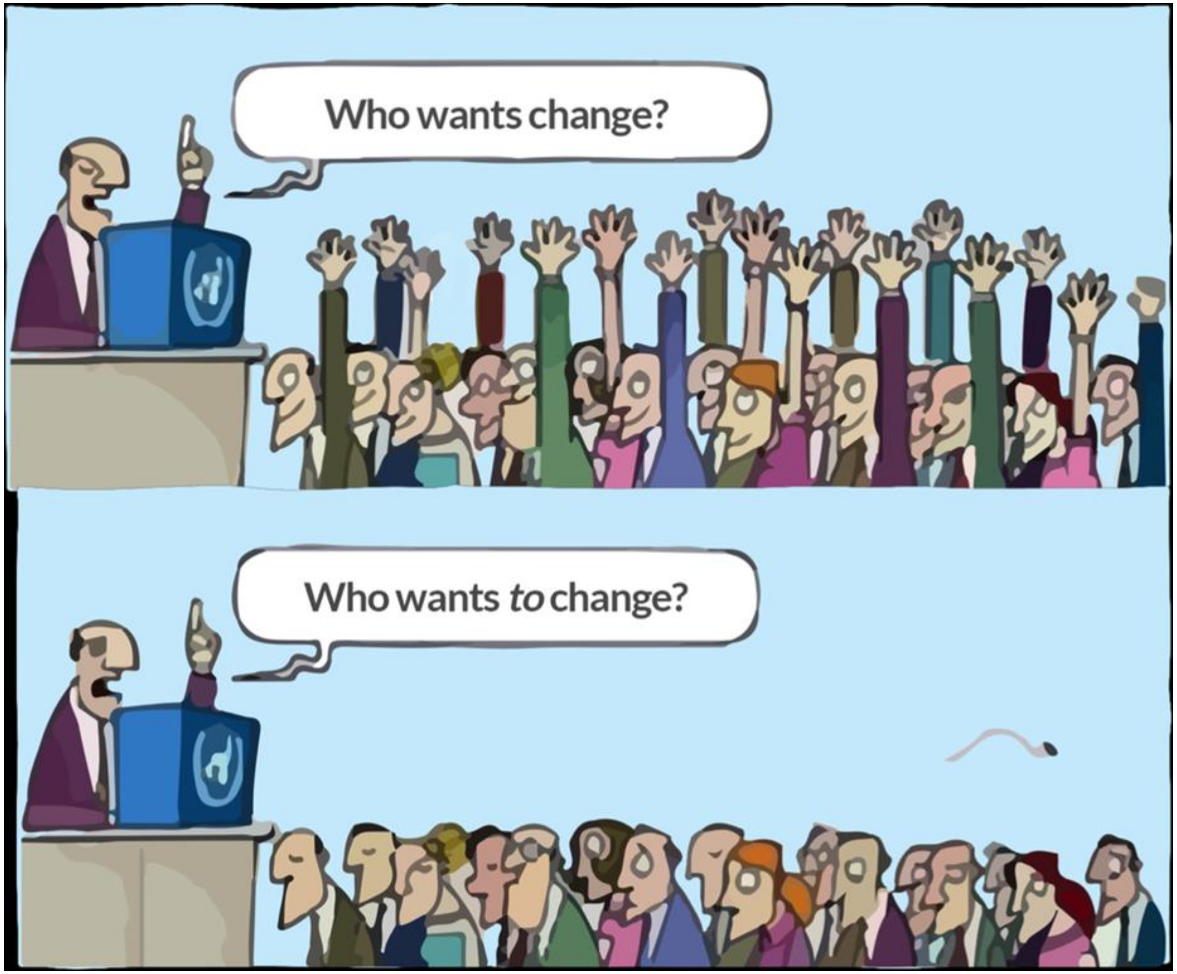
SECURITY SHOULD BE INTEGRATED

Key finding: Big disconnect between where respondents believe security should be automated (🧍), and where in reality they actually DO automate it (🧍):

	% FOR SHOULD AUTOMATE	% WHO DO AUTOMATE
PLANNING	100%	40%
CODE DEVELOPMENT	75%	31%
TESTING	67%	59%
PRODUCT RELEASE	88%	40%
OPERATIONAL REVIEW	92%	16%
MONITORING	100%	23%

Image sourced from AlertLogic: http://public.brighttalk.com/resource/core/63073/devops_the-security-gap-infographic_2015_92365.pdf

Who Wants Change?



Securing Continuous Delivery

Surround dynamic processes with protection

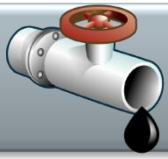
Security to keep up with speed of delivery

Discard detailed security roadmaps. Build in Security Testing Automation

Incremental but continuous improvement to security

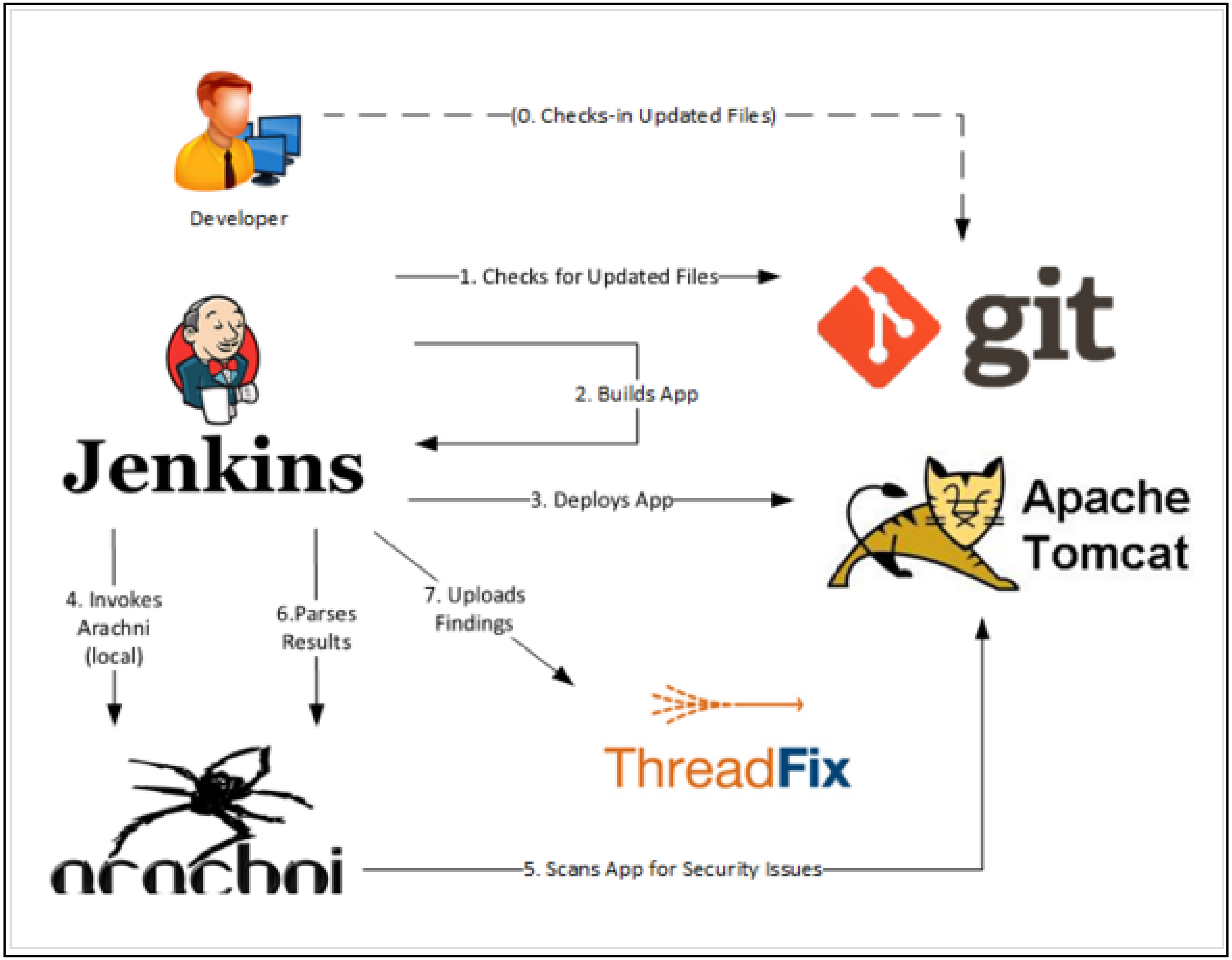
Software Defined Security. Put security in code. Tests are self verifying requirements. Automate

Embed security testing. Make security testable. Automate everything, incl continuous scanning



Test early. Test Often. Fail early. Rinse & Repeat.
AUTOMATED INTEGRATED REPEATABLE

Security in the Workflow


Developer
(0. Checks-in Updated Files)
1. Checks for Updated Files
git
2. Builds App
Jenkins
3. Deploys App
Apache Tomcat
4. Invokes Arachni (local)
6.Parses Results
7. Uploads Findings
ThreadFix
arachni
5. Scans App for Security Issues

Courtesy of: http://blog.secodis.com/2016/03/17/automated-security-tests-3-jenkins-arachni-threadfix/

Crawl, Walk, Run

Build incremental

security visibility

&

capability

Incremental Security

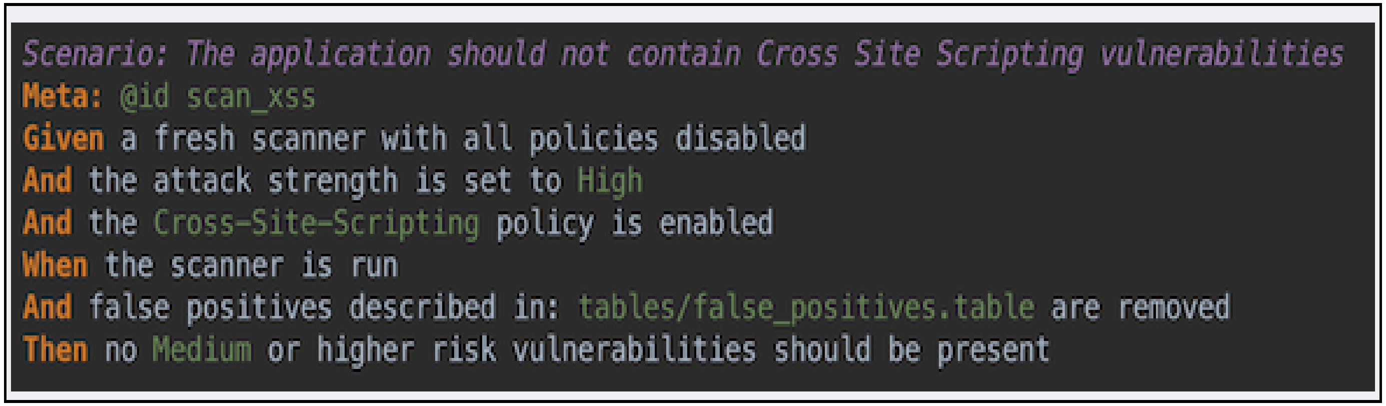
Coverage	Crawl	Walk	Run
Public Scan	●	●	●
Authenticated Scan		●	●
Web Service			●
DAST (Dynamic)	●	●	●
SAST (Static)		●	●
IAST (Interactive)			●
RASP (Realtime)			●
Fuzz			●

Incremental Security ...

Coverage	Crawl	Walk	Run
Network Scan – External	●	●	●
Network Scan – Internal		●	●
Network Scan – Continuous			●
Targeted Scans	●	●	●
Whitespot Scans			●
BDD (increasing coverage)	●	●	●
Multi-Tools, Correlate, De-Dupe			●
Phoenix			●

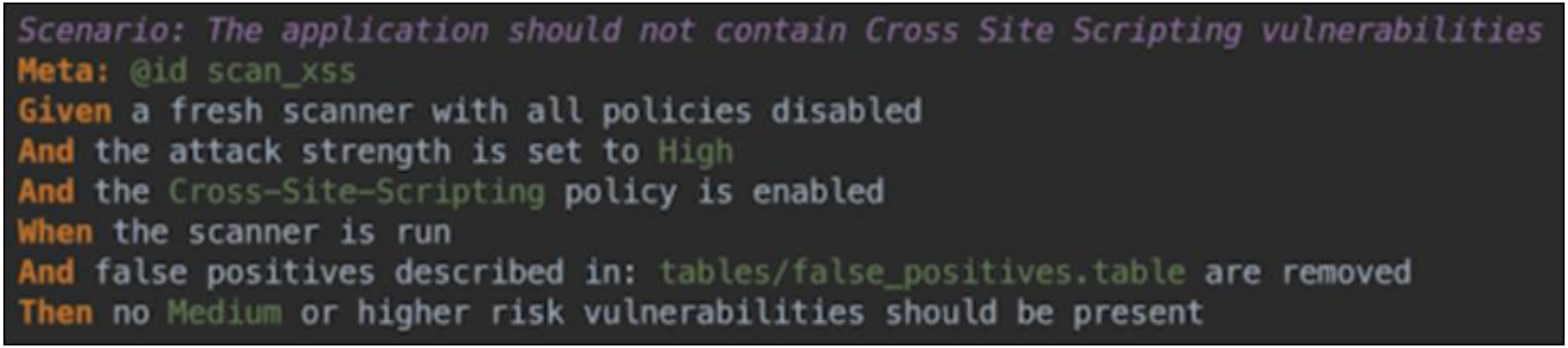
Example – BDD-Security

Launch automated scans



```
Scenario: The application should not contain Cross Site Scripting vulnerabilities
Meta: @id scan_xss
Given a fresh scanner with all policies disabled
And the attack strength is set to High
And the Cross-Site-Scripting policy is enabled
When the scanner is run
And false positives described in: tables/false_positives.table are removed
Then no Medium or higher risk vulnerabilities should be present
```

Test functional security requirements



Scenario: The application should not contain Cross Site Scripting vulnerabilities
Meta: @id scan_xss
Given a fresh scanner with all policies disabled
And the attack strength is set to High
And the Cross-Site-Scripting policy is enabled
When the scanner is run
And false positives described in: tables/false_positives.table are removed
Then no Medium or higher risk vulnerabilities should be present

https://github.com/continuumsecurity/bdd-security

End to End Cycle

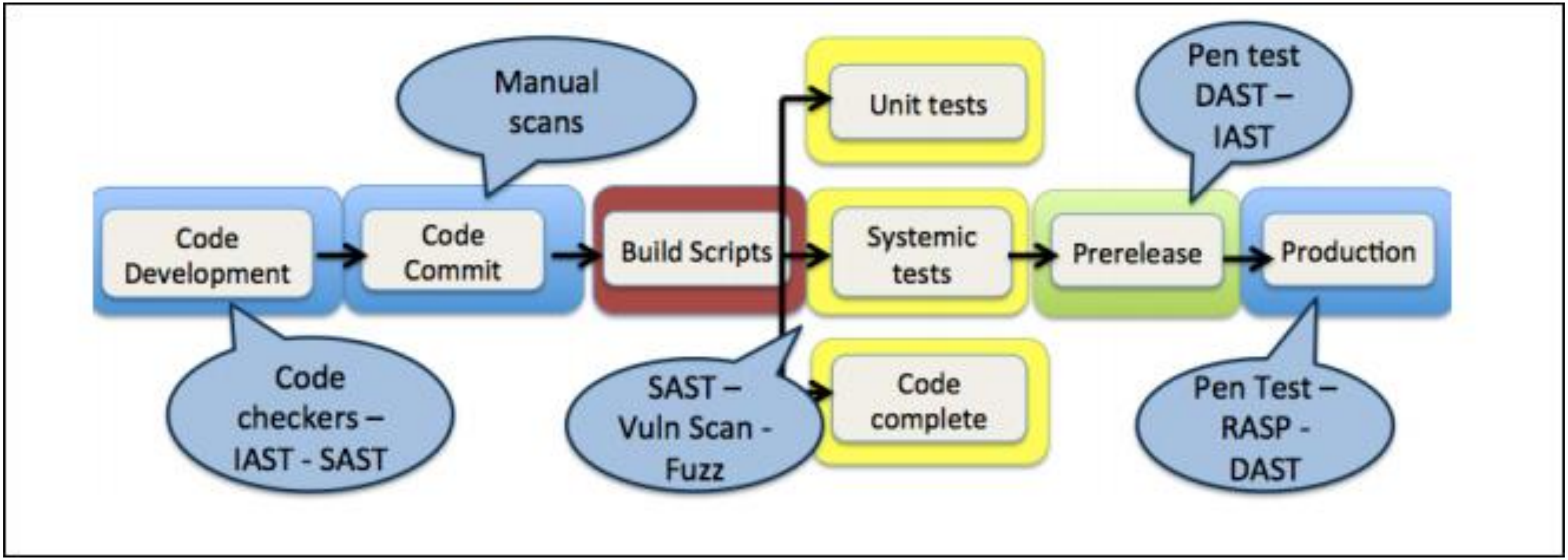


Image courtesy of: Putting Security Into DevOps, Version 1.0, Updated: October 30, 2015, Securosis, L.L.C

So – Where Do Consultants Fit In?

Conclusions

- You can get DevOps with security
- This is about system deployment lifecycle – more than software development lifecycle
- Through software almost everything can be automated across the whole stack: OS; app; environment
- You can “bake in security” into ongoing tests; but also the “fabric” of your deployment
- The earlier you provide feedback the less rework there is
- This means you need to test early and often
- Incorporate security into everything you do
- Reduce the handover points
- Use predefined libs so that quality of code is improved incrementally. Reduces wasted time for rework
- There are plenty of opps to insert security checks into the continuous dev and build cycle

Conclusions

- There are many open source and commercial products that can be used in this space for more predictable and secure outcomes
- Crawl, Walk, Run, Sprint
- Incrementally improve the process
- The threat landscape is constantly changing. Use continuous monitoring
- Use expert testers to check the logic through manual pen testing
- Standardise secure configuration settings for faster deployments, continually model potential security threats & vulnerabilities, test
- Feedback into the dev teams. Proactively mitigate security threats.
- Fail the build if the test fails. Test early. Test Often. Fail early.
- Move to 'security as code' – embedding security into scripts to automate processes. Execute in a repeatable and predictable way
- Use a Phoenix process to roll out new versions, increases your ability to rapidly respond to security issues and reduce the risk of deltas and drift

Questions?

Thank you

Murray Goldschmidt – Chief Operating Officer

Head office is level 8, 66 King Street, Sydney, NSW 2000, Australia. Owner of trademark and all copyright is Sense of Security Pty Ltd. Neither text or images can be reproduced without written permission.

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au