OWASP
Open Web Application
Security Project

# Automated DevSecOps infrastructure deployment

Recipes to secure your DevOps tool chain

# About me

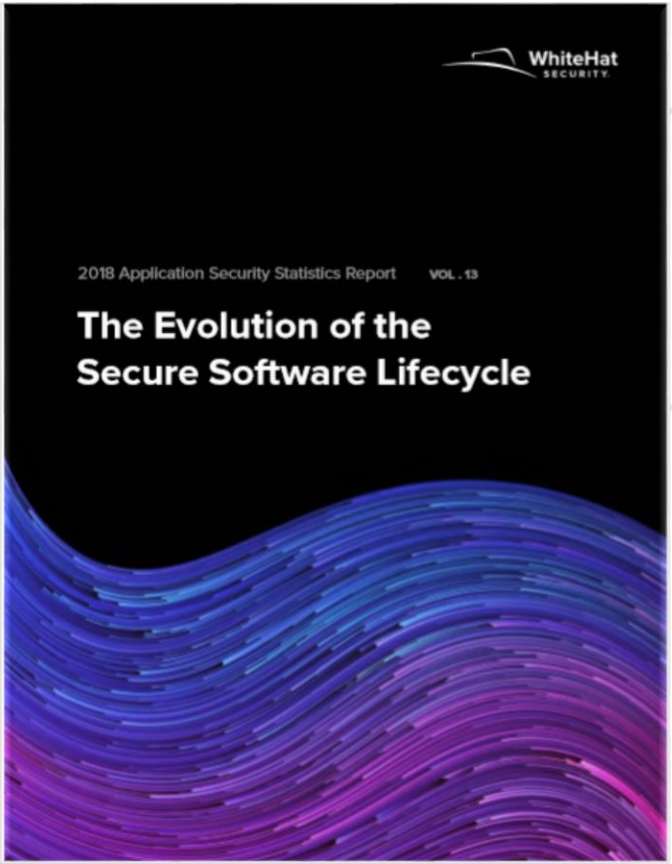
- Abdessamad TEMMAR
- Head of Offensive and R&D Activities
- OWASP Contributor (OPC, MSTG & MASVS)
- CEH, CEI & OSCP

# What is DevOps ?

- Culture + Automation + Measurement + Sharing
- Agile : Shorter release cycles
  Fast (and Furious) Dev. Life Cycle
  - Amazon : deploy every 11.6 seconds
  - Etsy : deploy 25+ times/day
  - Gov.uk : deploys 30 times/day
- Continuous deployment
- Agile/continuous dev process can be interrupted during a sprint by trad. Security testing

# Statistics speak for themselves …

- Product teams are pushing insecure software out into the wild at a faster rate than previous years.
- Nearly 70% of every application is comprised of reusable software components (e.g. third-party libraries, Open Source Software (OSS), etc.).
- 85% of mobile apps violated one or more of the OWASP Mobile Top 10.



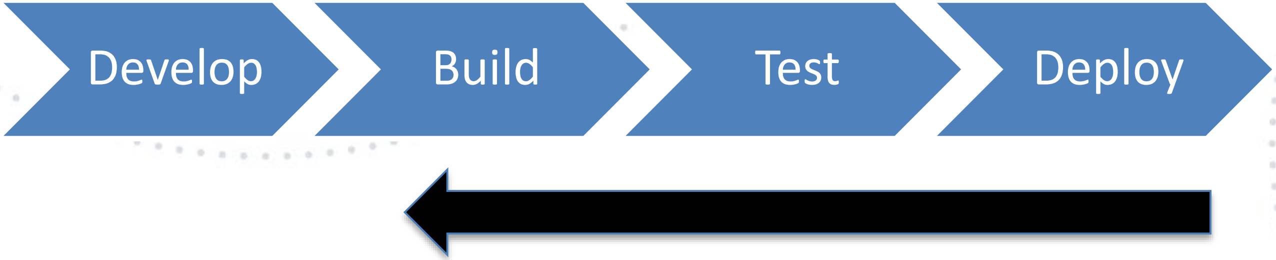
WhiteHat SECURITY

2018 Application Security Statistics Report VOL. 13

The Evolution of the Secure Software Lifecycle

# What is DevSecOps ?

- Safer Sooner : Shifting security to the left
- Security As Code: classical/essential security tests can be automated and executed as standard unit/integration tests.
- Continuous security monitoring
- Using DevOps to Secure DevOps



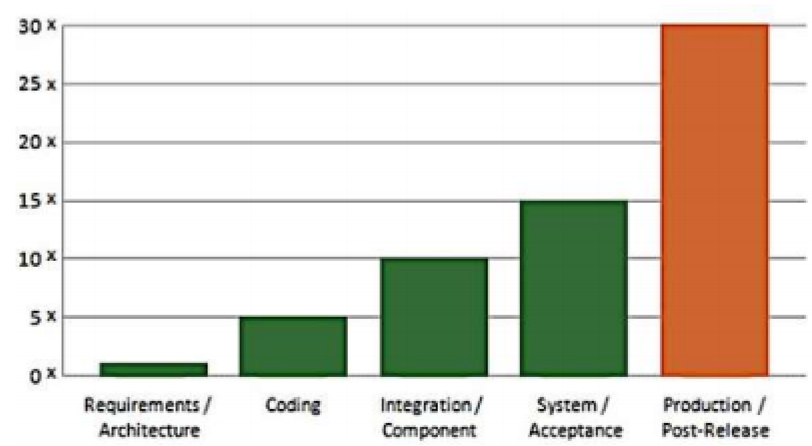
Develop

Build

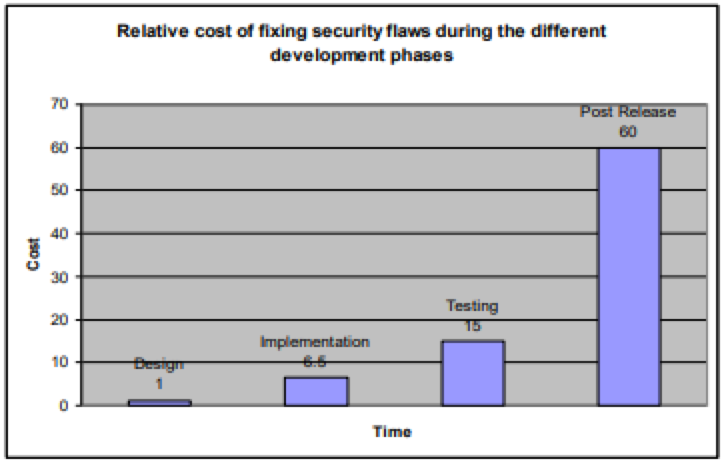
Test

Deploy

# Why DevSecOps ?

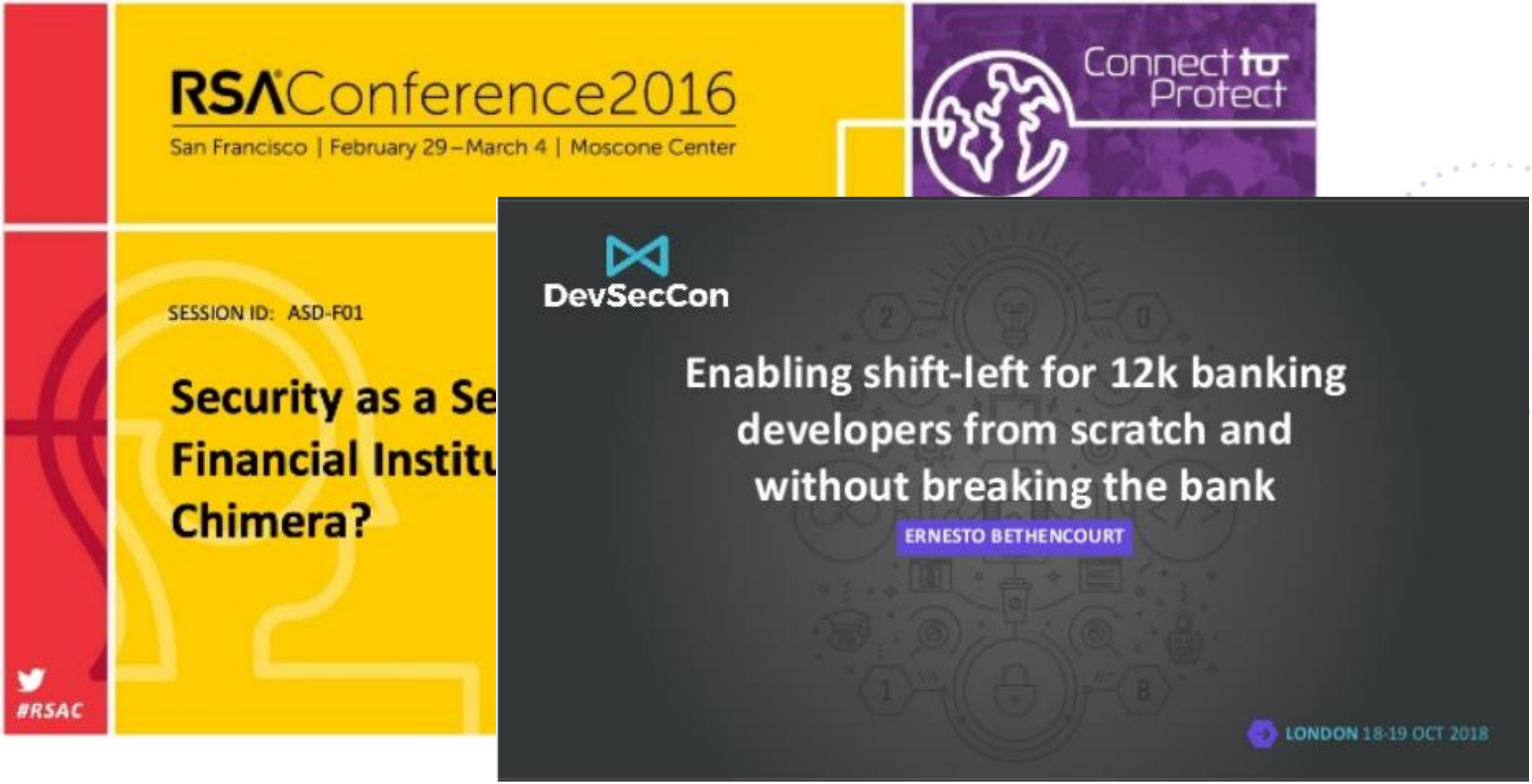


Source: National Institute of Standards & Technology (NIST)



Source: IBM Systems Sciences Institute

# DevSecOps : Reality ?



RSAConference2016

San Francisco | February 29–March 4 | Moscone Center

Connect to Protect

SESSION ID: ASD-F01

Security as a Se
Financial Institu
Chimera?

#RSAC

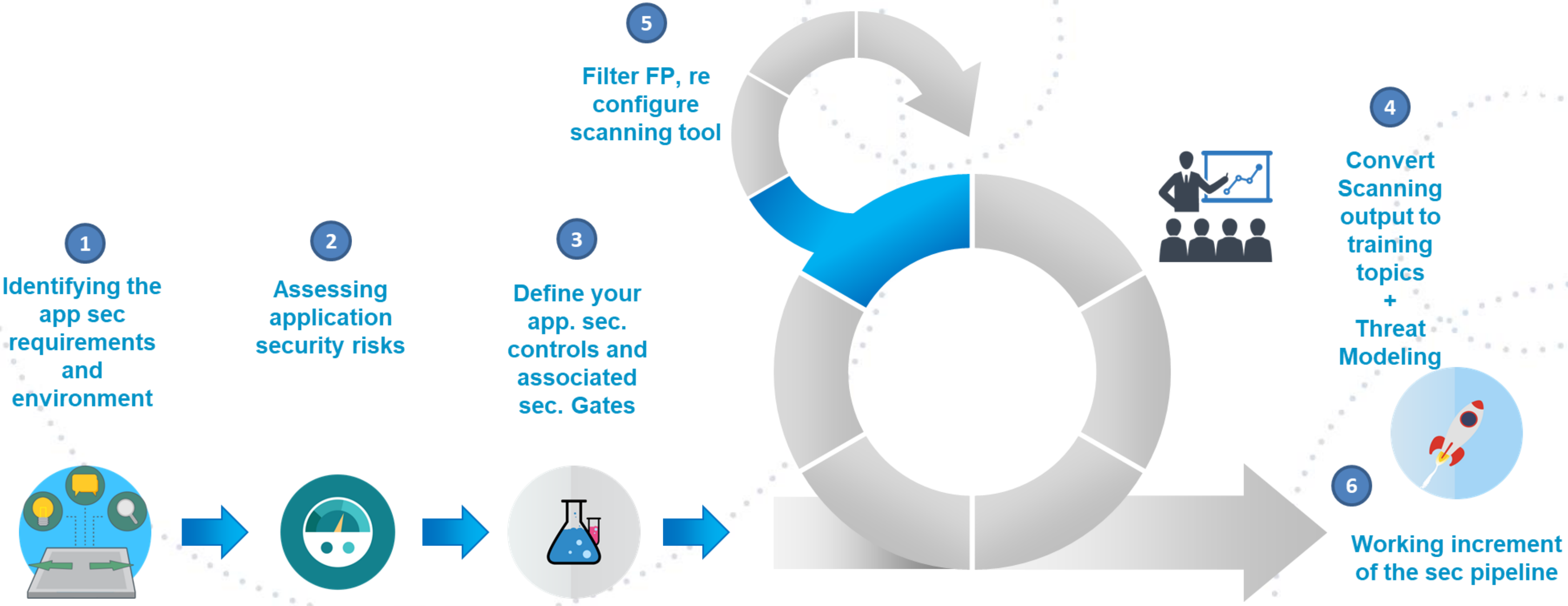
DevSecCon

Enabling shift-left for 12k banking developers from scratch and without breaking the bank

ERNESTO BETHENCOURT

LONDON 18-19 OCT 2018

# Securing your pipeline : agile approach



1 Identifying the app sec requirements and environment

2 Assessing application security risks

3 Define your app. sec. controls and associated sec. Gates

4 Convert Scanning output to training topics + Threat Modeling

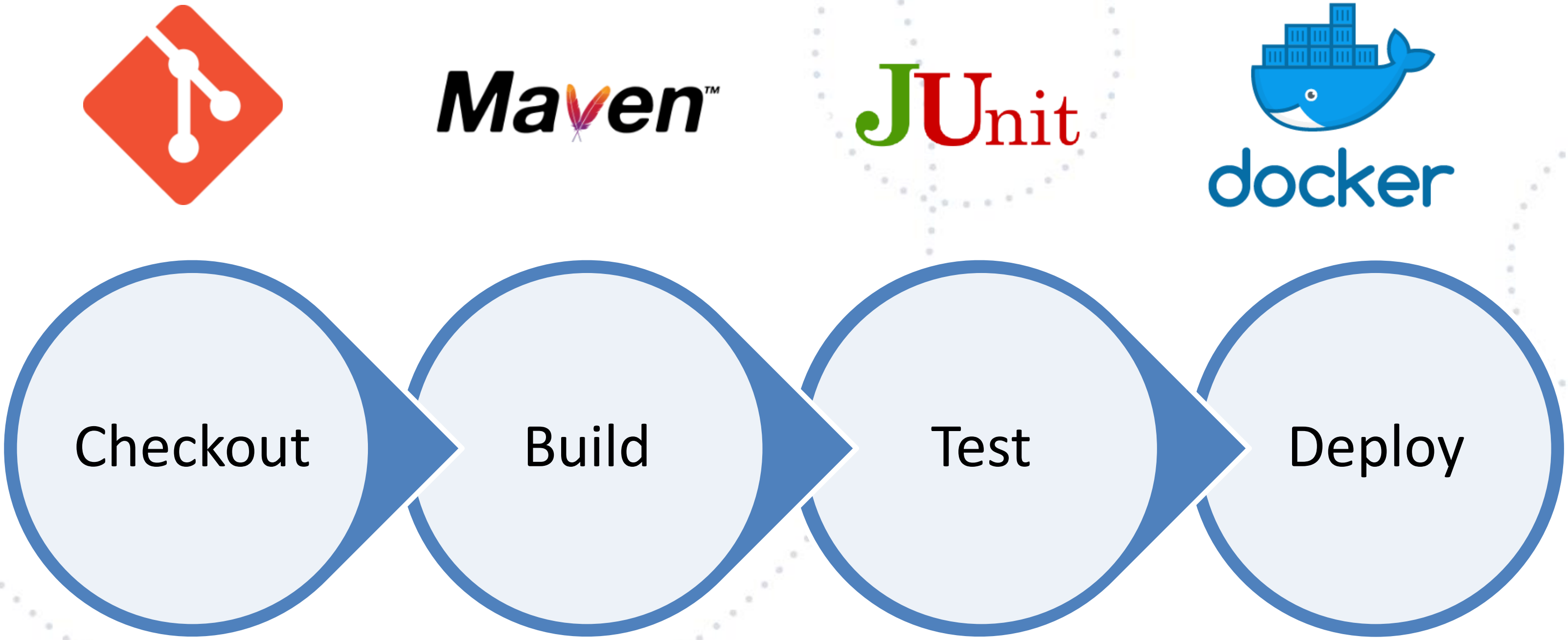
5 Filter FP, re configure scanning tool

6 Working increment of the sec pipeline

# AST challenges

- Communication : provide metrics (and evidence) about the security level of each/every stage/sprint of the application’s life cycle.
- Integration : appropriate (and Efficient) investment for application security (Improvise, adapt, overcome !)
- Ease of use : the ability to transform the current pipeline without forcing the developers to change the way they work (or the tools they used).
- Accuracy : continuously work on filtering FP and writing custom scanning rules
- Speed : automate everything ! be FAST (and FURIOUIS) !

# Our initial pipeline



# Our recipe to build a secure pipeline :p

## INGREDIENTS

- Static code analysis tool (SAST)
- Web application scanner tool (DAST)
- Environment compliance check
- Vulnerability management system

OPTIONAL :

- Continuous security monitoring
- Redteaming exercices
- Secret management

## TOOLS NEEDED

Exsiting DevOps Tools

SAST DAST MAST IAST

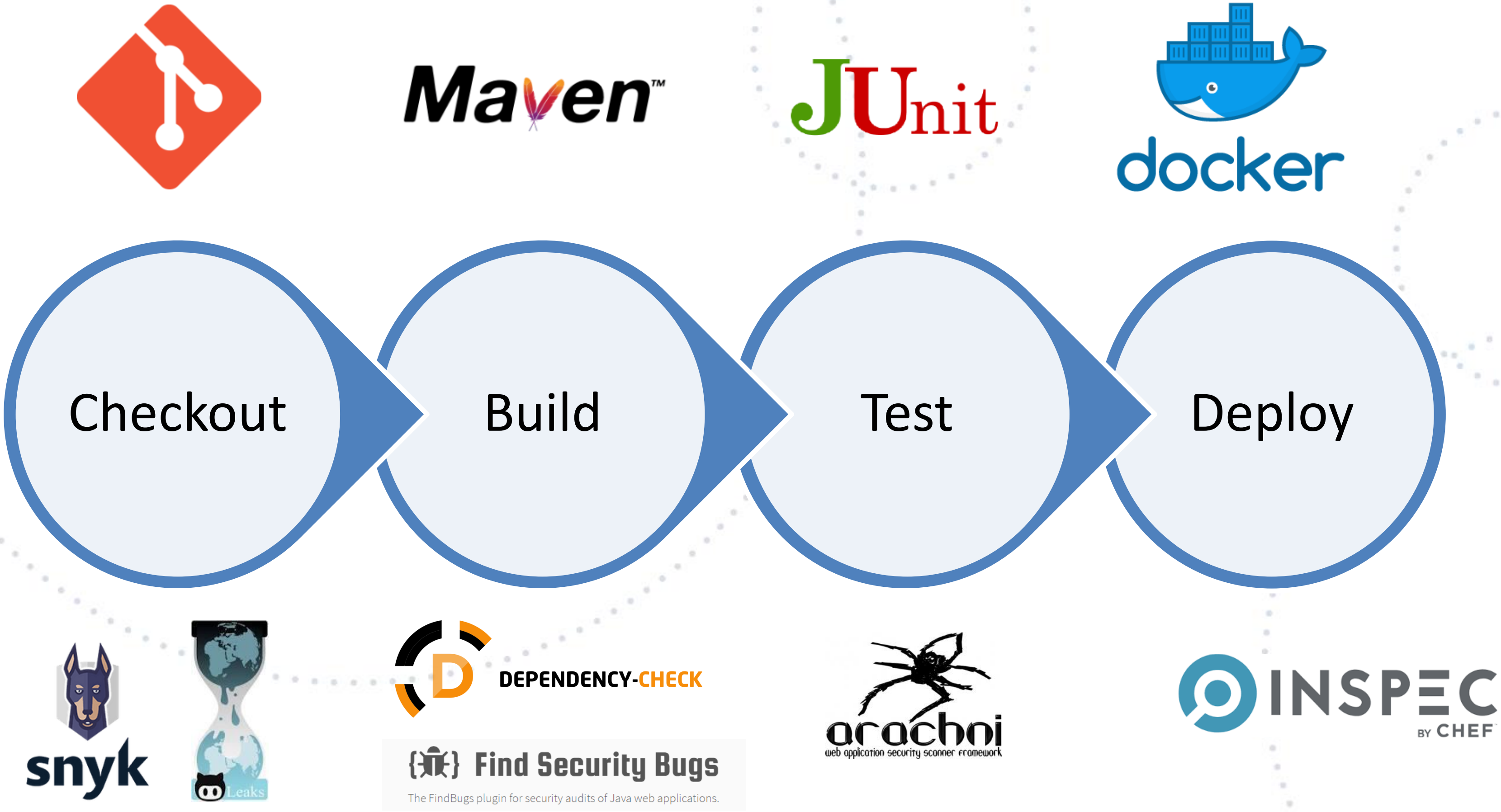
## TIME TO PREPARE

It depends !

## DIRECTIONS

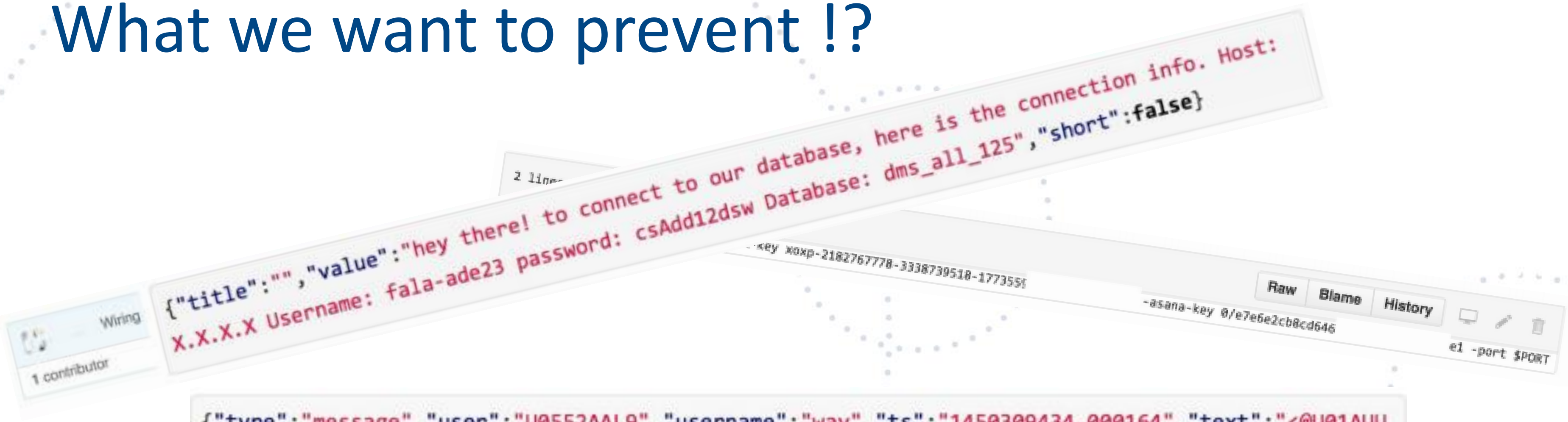
See the following slides

# Secure pipeline version


Maven™
JUnit
docker
Checkout
Build
Test
Deploy
snyk
Leaks
DEPENDENCY-CHECK
Find Security Bugs
The FindBugs plugin for security audits of Java web applications.
arachni
web application security scanner framework
INSPEC
BY CHEF

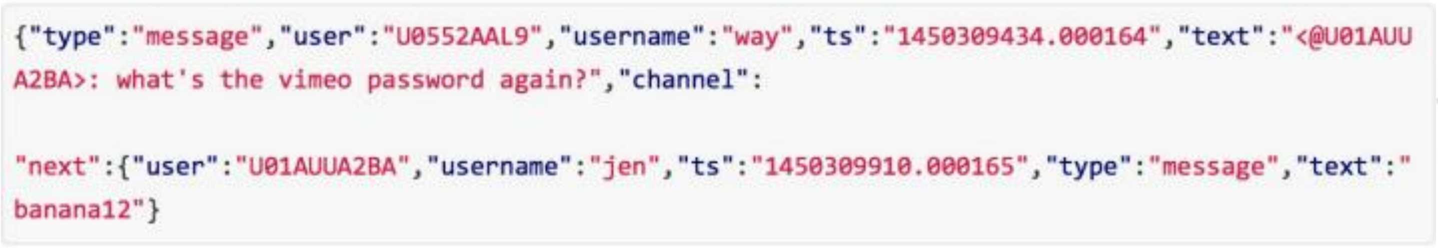
# Task 1 : Gittyleaks

# What we want to prevent !?



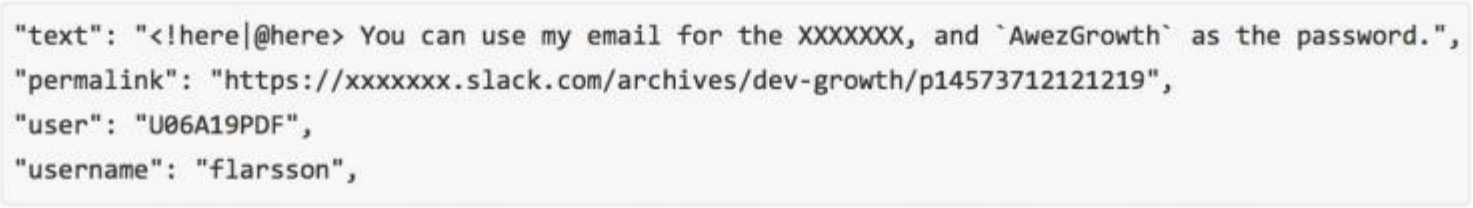
```
{"title":"","value":"hey there! to connect to our database, here is the connection info. Host:
X.X.X.X Username: fala-ade23 password: csAdd12dsw Database: dms_all_125","short":false}
```

```
2 line
-key xoxp-2182767778-3338739518-177355
-asana-key 0/e7e6e2cb8cd646
e1 -port $PORT
```



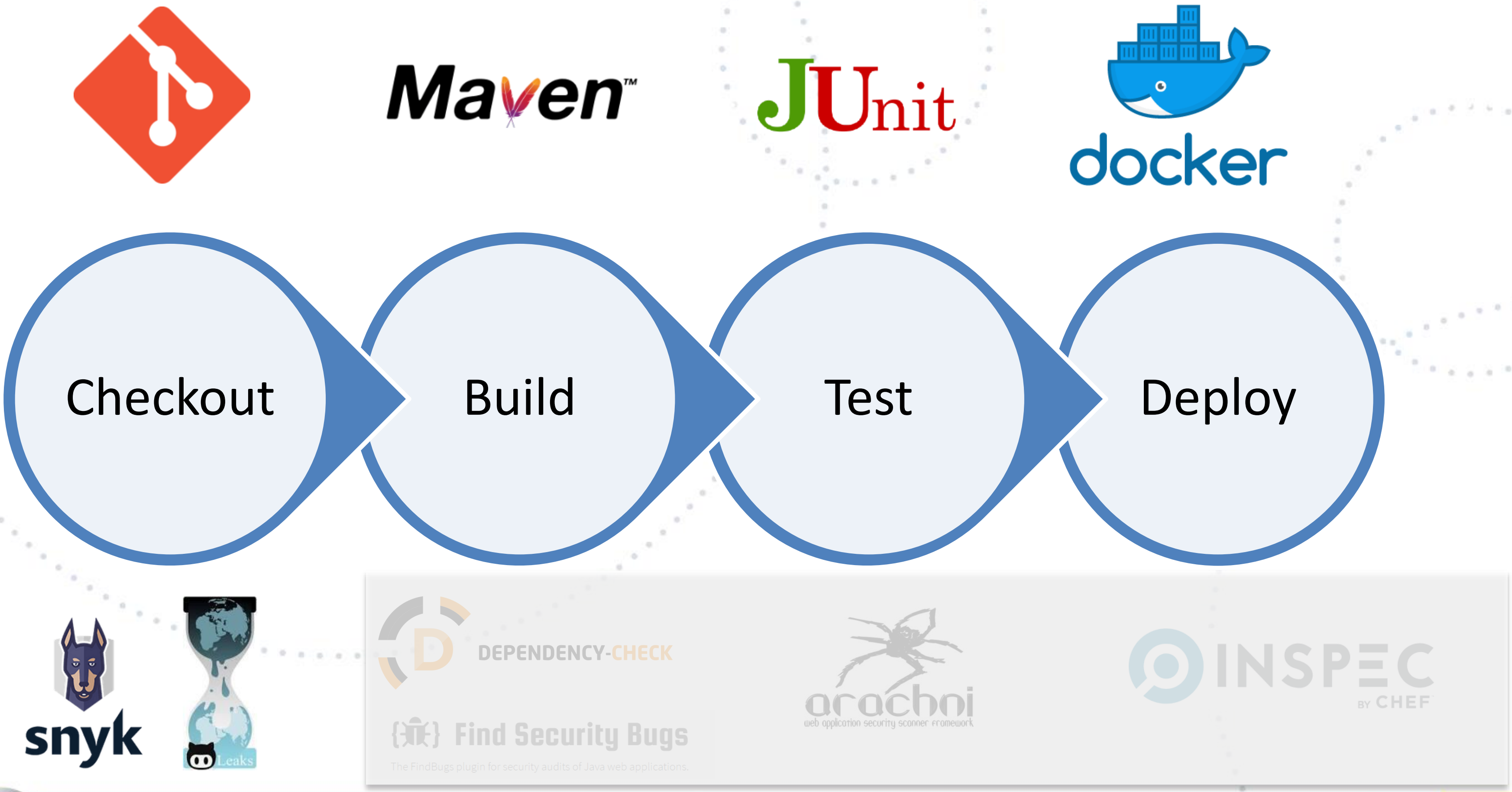
```
{"type":"message","user":"U0552AAL9","username":"way","ts":"1450309434.000164","text":"<@U01AUU
A2BA>: what's the vimeo password again?","channel":

"next":{"user":"U01AUUA2BA","username":"jen","ts":"1450309910.000165","type":"message","text":"
banana12"}
```



```
"text": "<!here|@here> You can use my email for the XXXXXXX, and `AwezGrowth` as the password.",
"permalink": "https://xxxxxxx.slack.com/archives/dev-growth/p14573712121219",
"user": "U06A19PDF",
"username": "flarsson",
```

# Current pipeline version



Checkout

Build

Test

Deploy

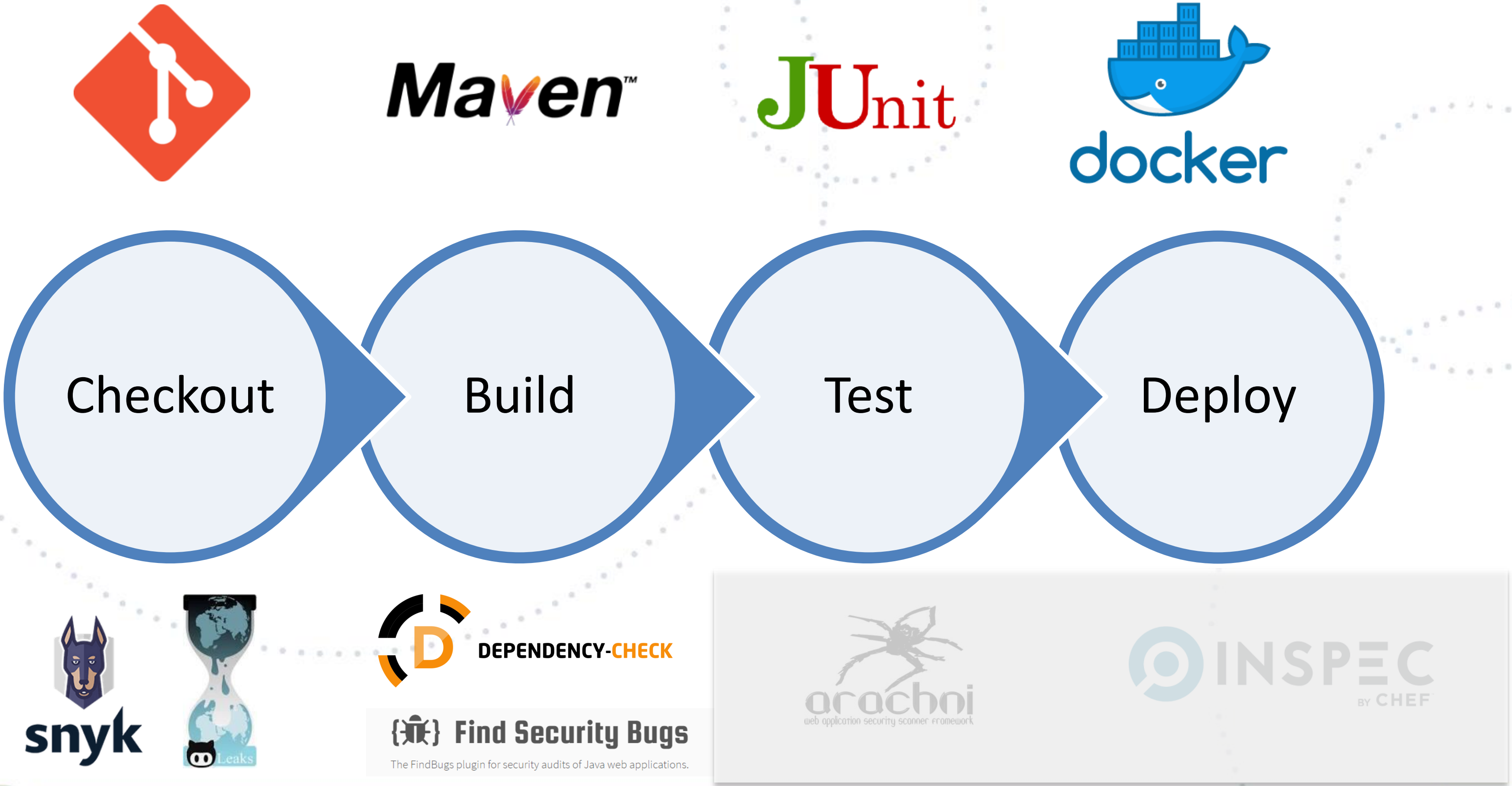
Maven™
JUnit
docker
snyk
Leaks
DEPENDENCY-CHECK
Find Security Bugs
The FindBugs plugin for security audits of Java web applications.
arachni
web application security scanner framework
INSPEC
BY CHEF

# Task 2 : OWASP Dependency Check

# What we want to prevent !?

Pittsburgh, Pennsylvania
DEVELOPING STORY
EQUIFAX CEO OUT AFTER MASSIVE DATA BREACH
Josh Shapiro | Attorney General of Pennsylvania
@qu

# Current pipeline version



Checkout

Build

Test

Deploy

Maven™
JUnit
docker
snyk
Leaks
DEPENDENCY-CHECK
Find Security Bugs
The FindBugs plugin for security audits of Java web applications.
arachni
web application security scanner framework
INSPEC
BY CHEF

# Task 3 : Static code analysis tool

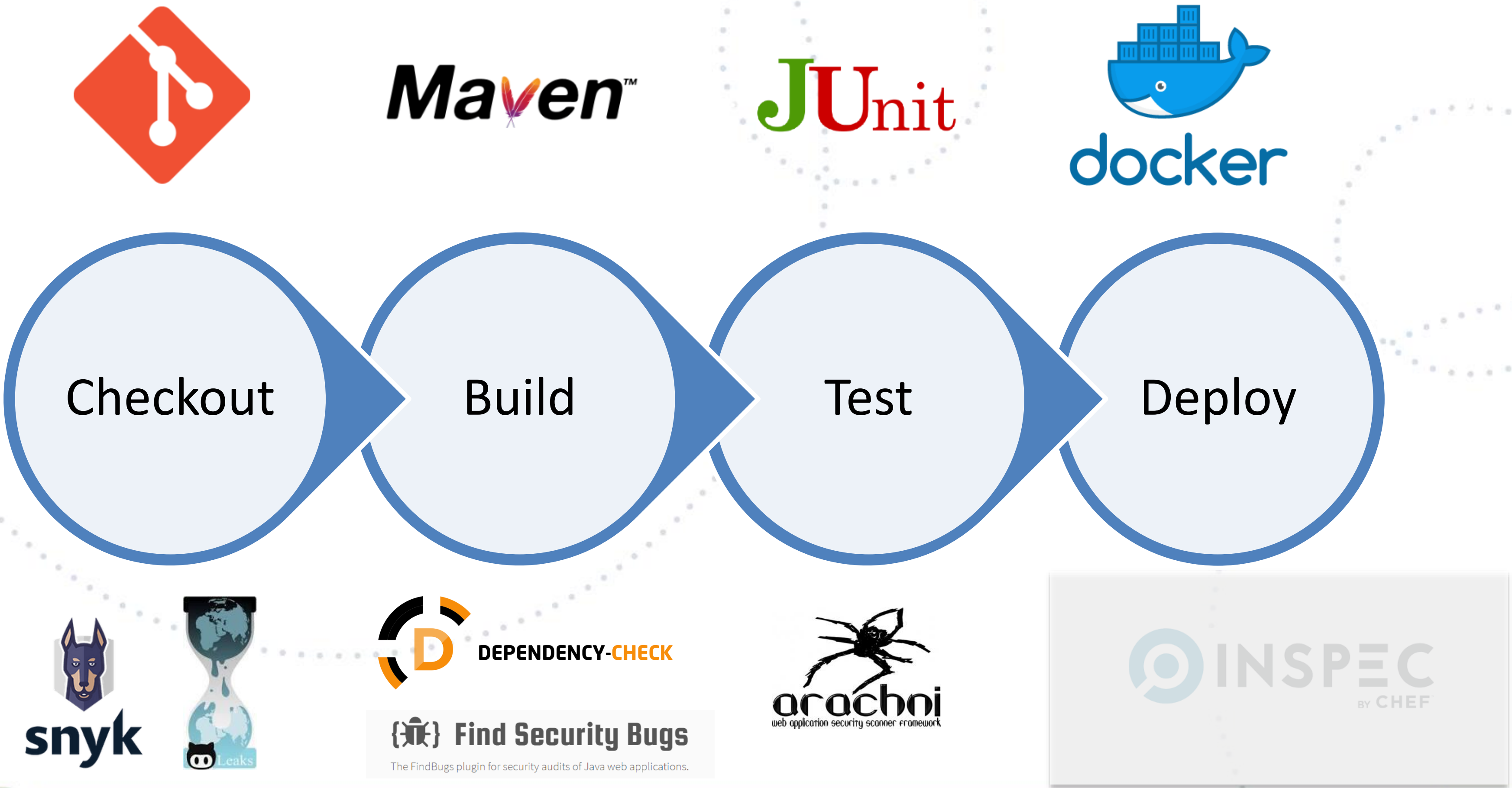
Scanning once is good. Scanning daily is better !

sonarqube
Find Security Bugs
Leaks

The FindBugs plugin for security audits of Java web applications.

# Task 4 : Web application scanner tool

# Current pipeline


Maven
JUnit
docker
snyk
Leaks
DEPENDENCY-CHECK
Find Security Bugs
The FindBugs plugin for security audits of Java web applications.
arachni
web application security scanner framework
INSPEC
BY CHEF

Checkout

Build

Test

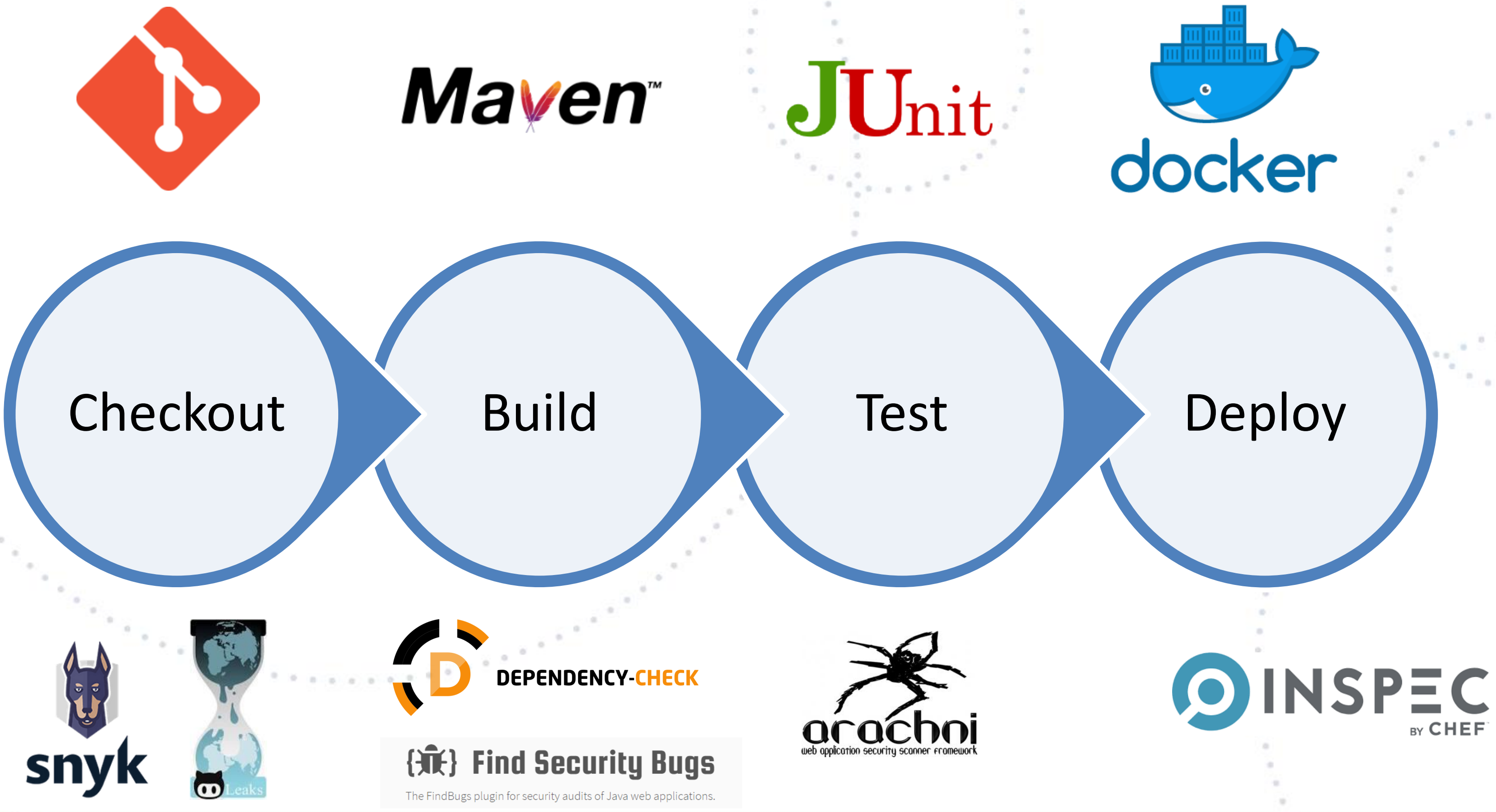
Deploy

# Task 5 : Inspect Your Infrastructure

# What we want to prevent !?

**https://www.shodan.io/search?query=ssl+v2**

# Current pipeline


Checkout

Build

Test

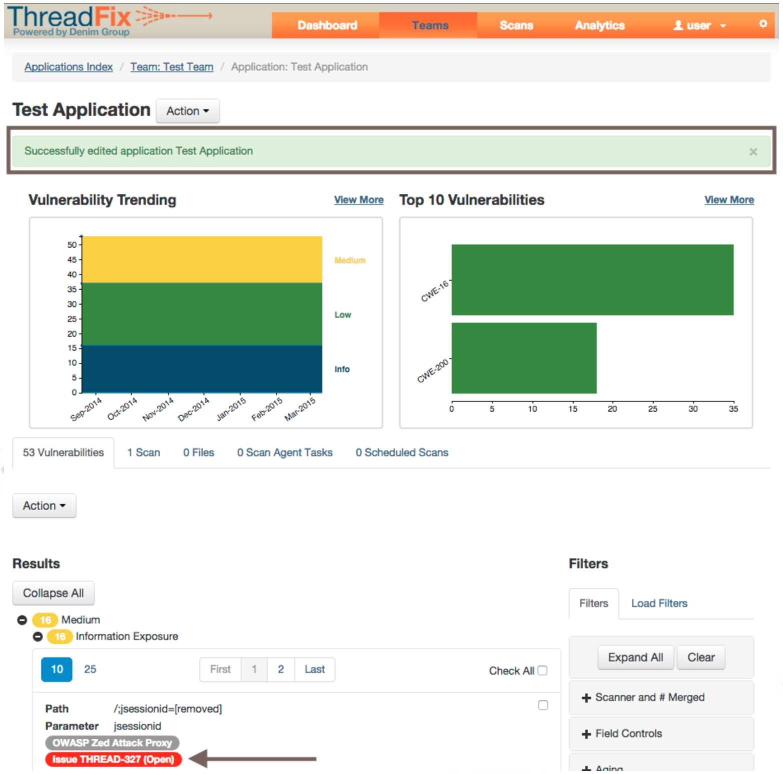
Deploy

Maven™
JUnit
docker
snyk
Leaks
DEPENDENCY-CHECK
Find Security Bugs
The FindBugs plugin for security audits of Java web applications.
arachni
web application security scanner framework
INSPEC
BY CHEF

# Task 6 : Vunerability management system

SO YOU THOUGHT ALL IS AUTOMATED
GOOD LUCK FILTERING MY FRIEND
imgflip.com

# Task 5 : Vulnerability management system



Test Application

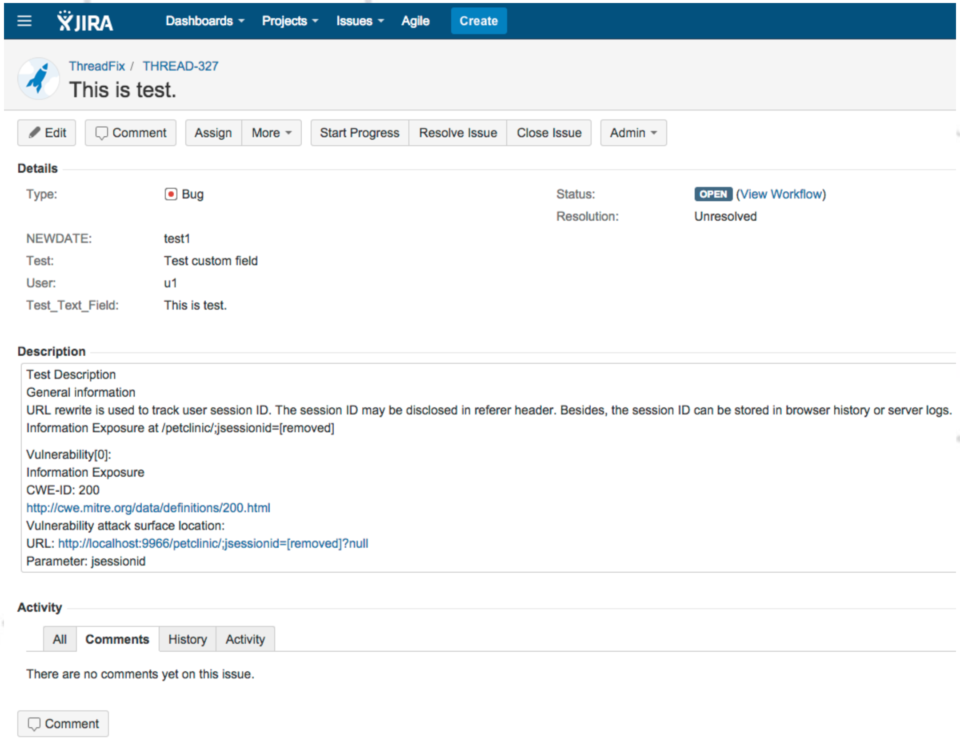
Successfully edited application Test Application ×

- 16 Medium
  - 16 Information Exposure

| | |
|---|---|
| Path | /;jsessionid=[removed] |
| Parameter | jsessionid |

OWASP Zed Attack Proxy

Issue THREAD-327 (Open)



ThreadFix / THREAD-327

This is test.

**Details**

| | | | |
|---|---|---|---|
| Type: | Bug | Status: | OPEN (View Workflow) |
| | | Resolution: | Unresolved |
| NEWDATE: | test1 | | |
| Test: | Test custom field | | |
| User: | u1 | | |
| Test_Text_Field: | This is test. | | |

**Description**

Test Description
General information
URL rewrite is used to track user session ID. The session ID may be disclosed in referer header. Besides, the session ID can be stored in browser history or server logs.
Information Exposure at /petclinic/;jsessionid=[removed]

Vulnerability[0]:
Information Exposure
CWE-ID: 200
http://cwe.mitre.org/data/definitions/200.html
Vulnerability attack surface location:
URL: http://localhost:9966/petclinic/;jsessionid=[removed]?null
Parameter: jsessionid

**Activity**

There are no comments yet on this issue.

OWASP
Open Web Application
Security Project

# THANKS!

## Any questions?

## You can find me at :

MAIL : ATEMMAR@ABCIT.FR
TWITTER : @T333333R

LINKEDIN : QR CODE

in