

Automated DevSecOps infrastructure deployment recipes to secure your DevOps tool chain

ABDESSAMAD TEMMAR



BOSTON 10-11 SEPT 2018

About me

- Abdessamad TEMMAR
- Head of Offensive and R&D Activities
- OWASP Contributor
- CEH, CEI & OSCP



Marrakech. Morocco

About me



Marrakech. Morocco

About me



Atlas Mountains and Three Valleys. Morocco

***“I AM A NICE SECURITY PROFESSIONAL, NOT MINDELESS
VULNERABILITY SPEWING MACHINE. IF I AM TO CHANGE
THIS IMAGE, I MUST FIRST CHANGE MYSELF.***

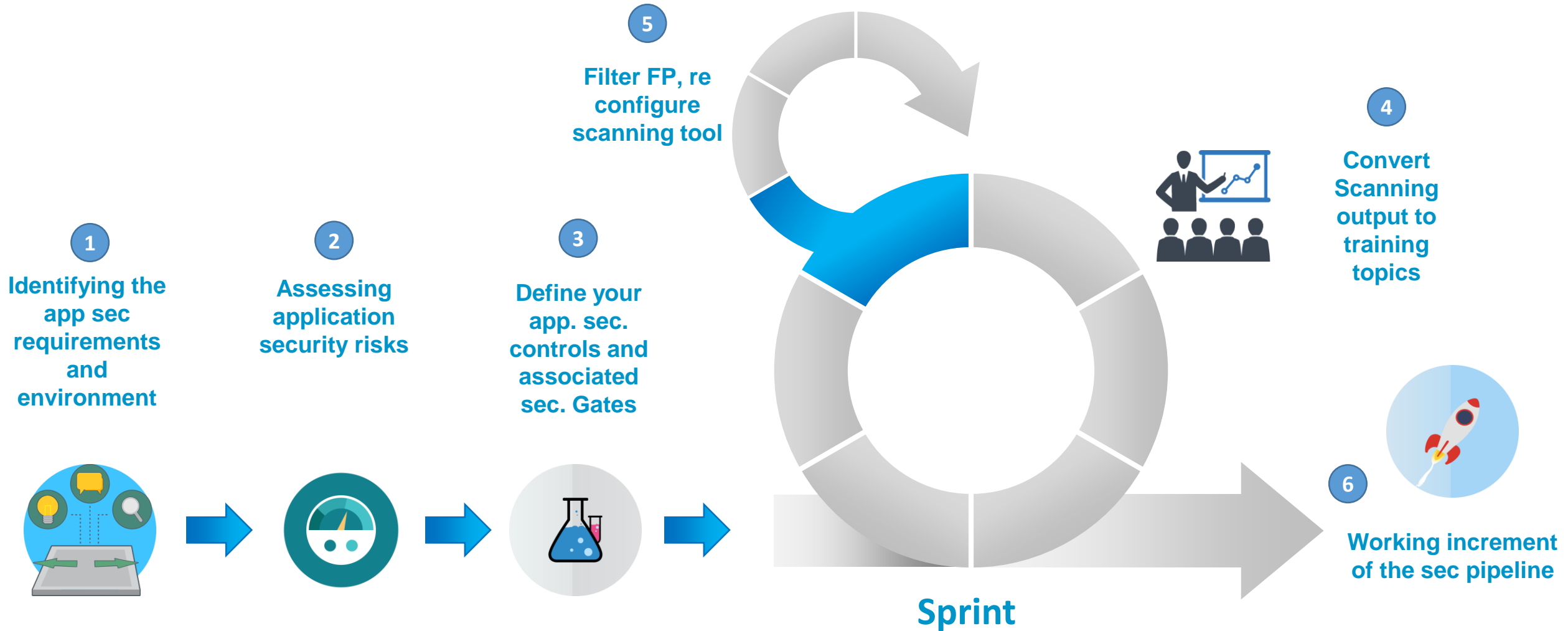
DEVELOPERS ARE FRIENDS, NOT FOOLS.”

- Bruce, Aaron and Matt

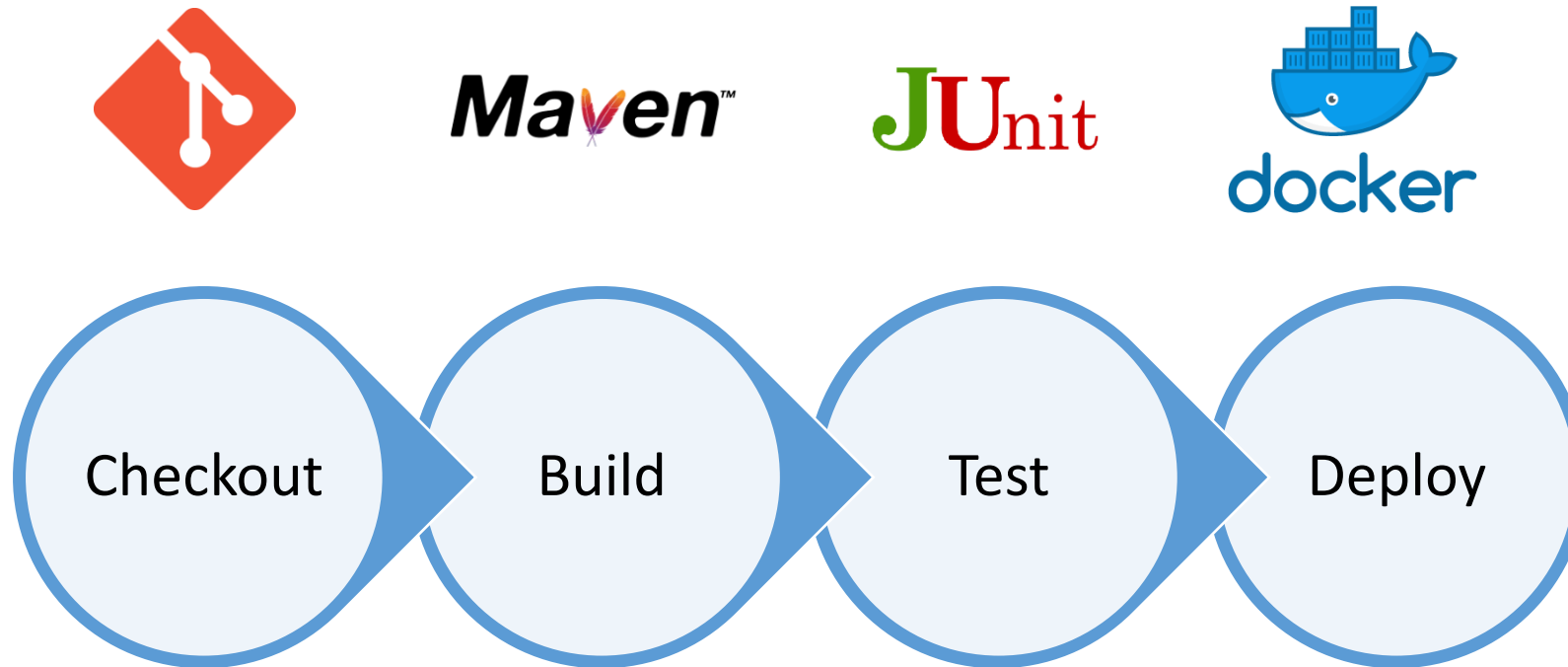
AST challenges

- 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 FURIOUS) !

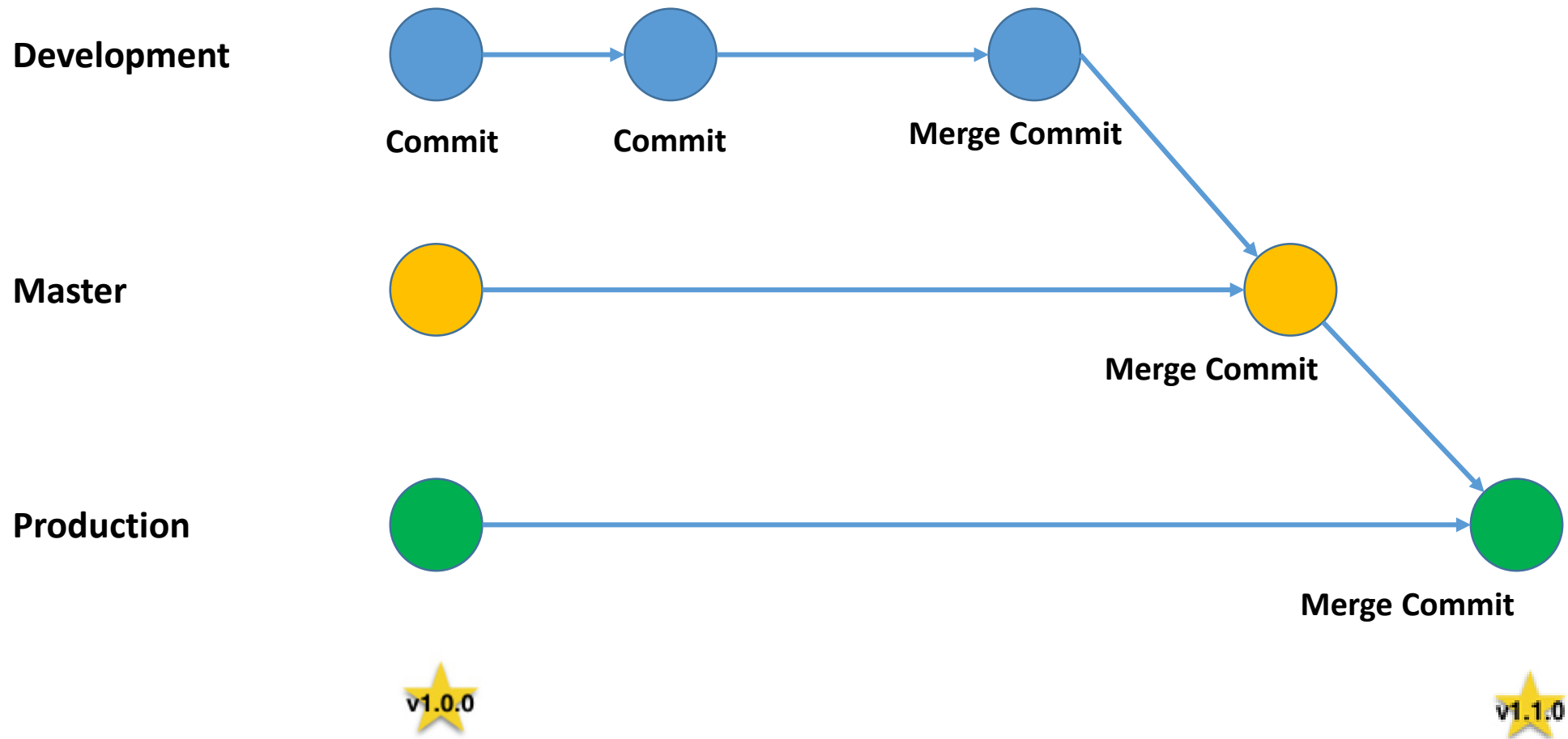
Securing your pipeline : agile approach



Our initial pipeline (1/2)



Our initial pipeline (2/2)



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 exercises
- Secret management

TOOLS NEEDED



Existing DevOps Tools

SAST DAST MAST IAST

TIME TO PREPARE



It depends !

DIRECTIONS

See the following slides

Task 1 : Static code analysis tool

Scanning once is good. Scanning daily is better !



{} Find Security Bugs

The FindBugs plugin for security audits of Java web applications.



Task 2 : Web application scanner tool



OWASP ZAP



Task 3 : Inspect Your Infrastructure



Task 4 : Vulnerability management system



Task 4 : Vulnerability management system

ThreadFix
Powered by Denim Group

Dashboard Teams Scans Analytics user

Applications Index / Team: Test Team / Application: Test Application

Test Application

Successfully edited application Test Application

Vulnerability Trending

View More

Severity	Sep-2014	Oct-2014	Nov-2014	Dec-2014	Jan-2015	Feb-2015	Mar-2015
Medium	50	45	40	35	30	25	20
Low	35	30	25	20	15	10	5
Info	20	15	10	5	0	0	0

Top 10 Vulnerabilities

View More

CWE-ID	Count
CWE-16	35
CWE-200	18

53 Vulnerabilities 1 Scan 0 Files 0 Scan Agent Tasks 0 Scheduled Scans

Action

Results

Collapse All

16 Medium
16 Information Exposure

10 25 First 1 2 Last Check All

Path	Parameter	Issue
/jsessionid=[removed]	jsessionid	OWASP Zed Attack Proxy
		Issue THREAD-327 (Open)

Filters

Filters Load Filters

Expand All Clear

+ Scanner and # Merged

+ Field Controls

+ Admin

JIRA Dashboards Projects Issues Agile Create

ThreadFix / THREAD-327

This is test.

Edit Comment Assign More Start Progress Resolve Issue Close Issue Admin

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](http://localhost:9966/petclinic/jsessionid=[removed]?null)
Parameter: jsessionid

Activity

All Comments History Activity

There are no comments yet on this issue.

Comment

THANKS!

Any questions?

You can find me at :

MAIL : ATEMMAR@ABCIT.FR

TWITTER : [@T333333R](https://twitter.com/T333333R)



BOSTON 10-11 SEPT 2018