DevSecCon

Automated DevSecOps infrastructure deployment
recipes to secure your DevOps tool chain

ABDESSAMAD TEMMAR

BOSTON 10-11 SEPT 2018

About me

AB Conseils
Information Technology

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

Marrakech. Morocco

About me

AB Conseils
Information Technology

Marrakech. Morocco

About me

AB Conseils
Information Technology

Atlas Mountains and Three Valleys. Morocco

About me

AB Conseils
Information Technology

"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 FURIOUIS) !

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

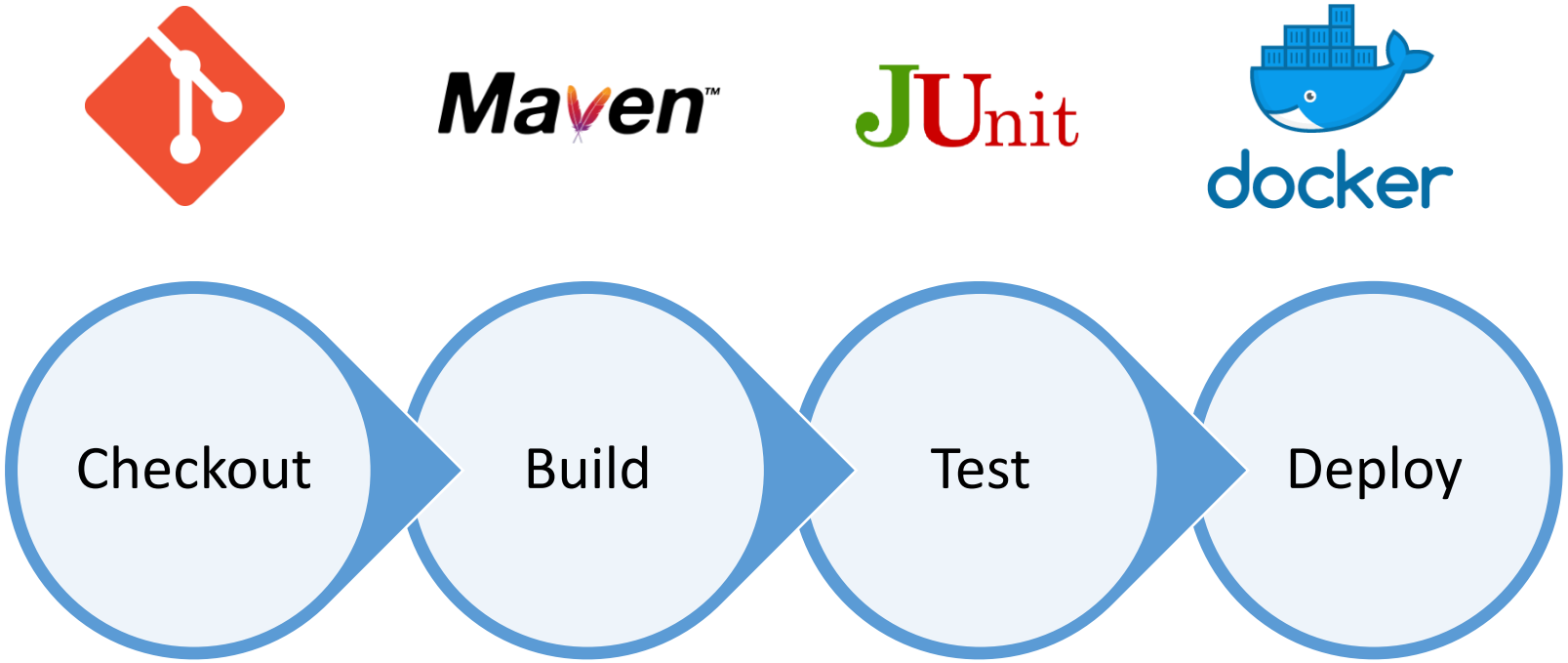
5 Filter FP, re configure scanning tool

4 Convert Scanning output to training topics

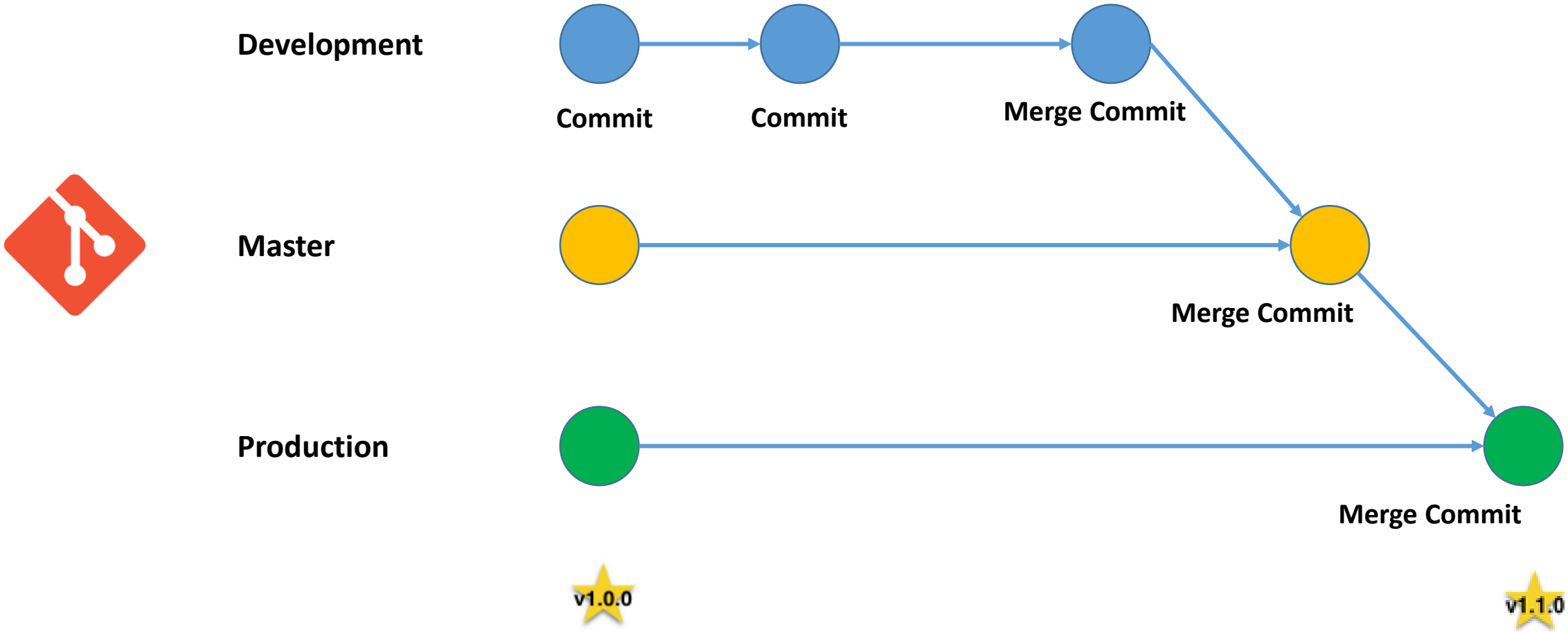
6 Working increment of the sec pipeline

Sprint

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 exercices
- Secret management

TOOLS NEEDED

Exsiting DevOps Tools

SAST DAST MAST IAST

TIME TO PREPARE

It depends !

DIRECTIONS

See the following slides

Task 1 : Static code analysis tool

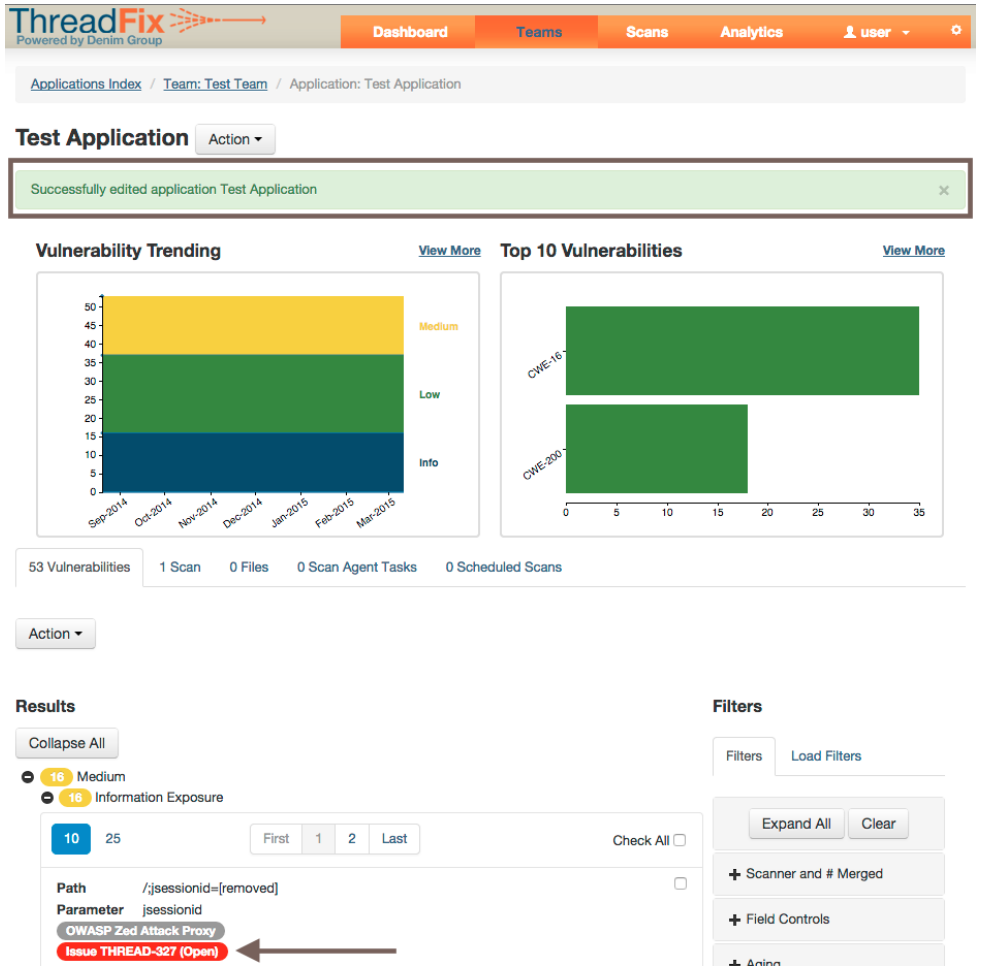
Scanning once is good. Scanning daily is better !

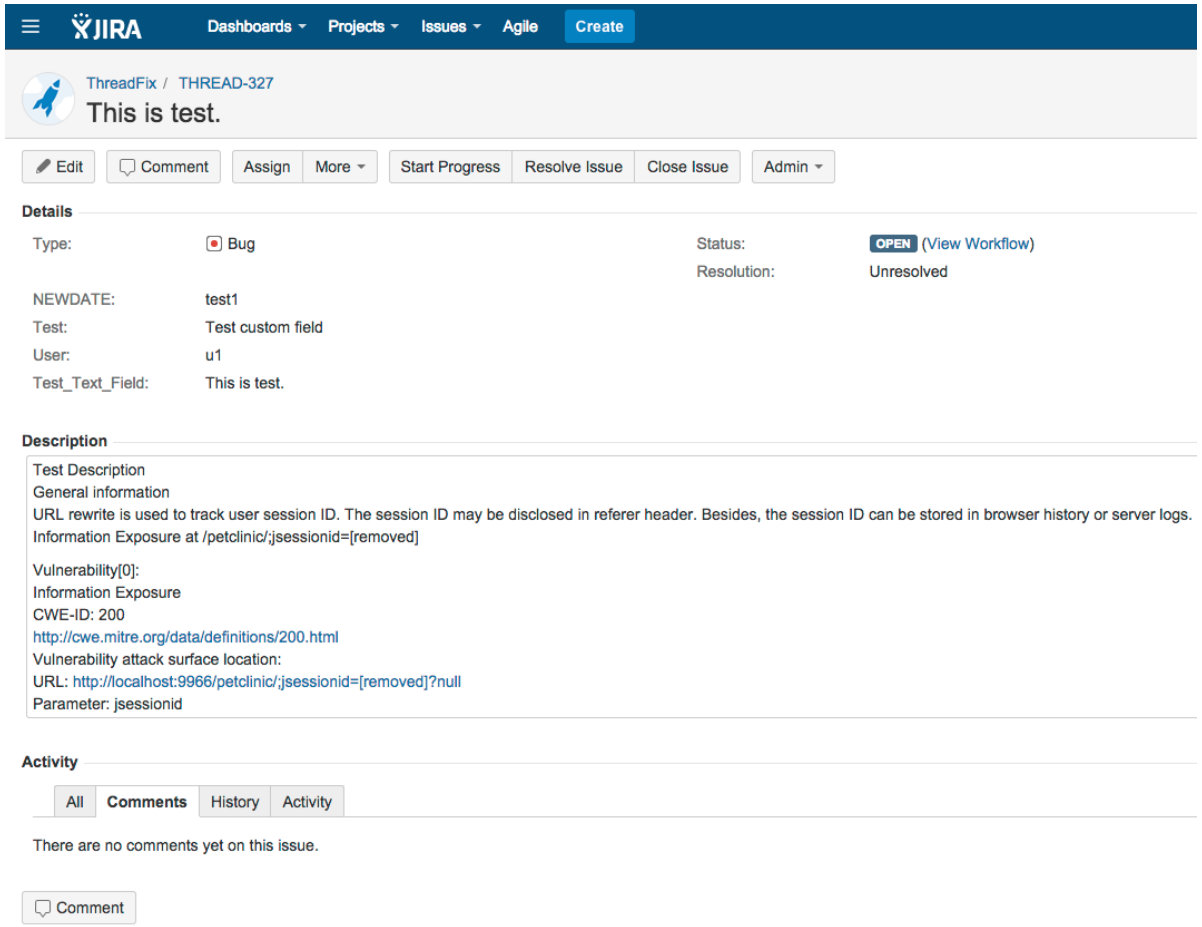
Task 2 : Web application scanner tool

Task 3 : Inspect Your Infrastructure

Task 4 : Vunerability management system

Task 4 : Vunerability management system





DevSecCon

AB Conseils
Information Technology

THANKS!

Any questions?

You can find me at :

MAIL : ATEMMAR@ABCIT.FR

TWITTER : @T333333R