Secure git workshop

Workshop | 2022

by **André Rainho**
DevSecOps @ **Mindera**

(In)secure git workshop ?

Workshop | 2022

by **André Rainho**
DevSecOps @ **Mindera**

Hello !

Who am I ?

- BSc and MSc at University of Aveiro
- Currently a DevSecOps at Mindera Software Craft.
- I enjoy OpenSource, Linux, Security and APIs
- You can find more on about.me/arainho

Contents

- Experiments around Secure SDLC
- Sharing ideas and what worked
- In case it helps others
- *However, It may not work for you !*

Timeline

...

- Rising of DevOps movement
- Software Development Life Cycle paradigm is changing
- Adoption of Cloud Services and OpenSource Software
- Monolithic applications replaced by micro-services

DevOps

“ DevOps is the combination of cultural philosophies, practices, and tools that increases an organization’s ability to deliver applications and services at high velocity.”

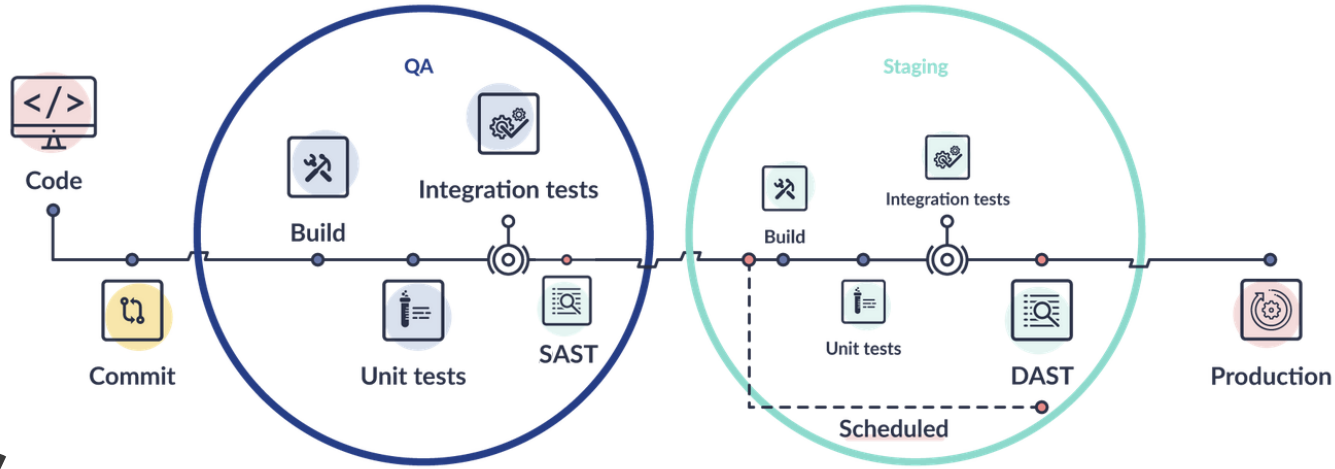
devops model defined by AWS

DevSecOps

“DevSecOps or SecDevOps is the practice of including application security principles in a typical DevOps cycle, delivering security best practices earlier in SDLC..”

what is devsecops by NewRelic

new challenges



- Usually, all security tests are executed after services are up and running in production
- DevSecOps delivers application security earlier in the Software development life cycle (Shift-left)
- Securing DevOps' workflows is vital

https://blog.probely.com/integrating-web-vulnerability-scanners-in-continuous-integration-dast-for-ci-cd-7637eaff26bd

Git on SDLC ?

Git is distributed version control system

SDLC is Software Development Life Cycle

WaterFall methodology uses SVN

Agile methodologies use Git

Environments in SDLC

Dev / Staging / **Prod**

Use distinct #git_branches for each environment !!!

Workshop

Enough talking !

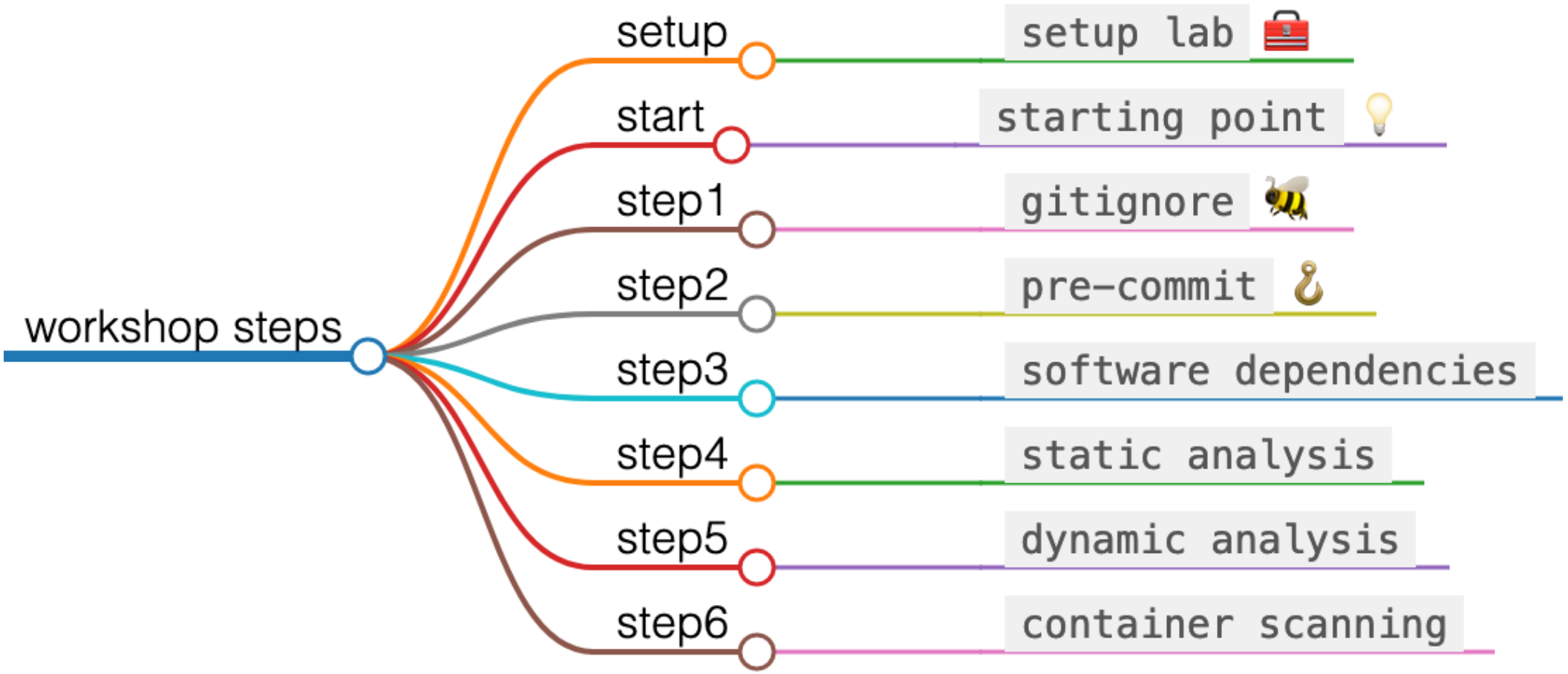
- We have a Workshop waiting ...
- With challenges in branches ;-)
- Challenges tackle diverse topics
- Related to software development

Workshop

Let’s go !

https://github.com/arainho/secure-git-workshop

Workshop steps



Workshop

Security tests ^)~

Initiatives to add security tests in CI/CD pipelines

1 - secret detection
2 - dependency scanning
3 - static analysis
4 - container scanning
5 - dynamic analysis

Workshop

Other Security tests

Interactive Application Security Testing (IAST)
Software Composition Analysis (SCA)
Infrastructure as Code (IaC) scanning
License compliance
API scanning, fuzzing

Workshop | 2022

(In)secure Git workshop

by **André Rainho**
DevSecOps @ **Mindera**

END

Questions ?