#10 Secure Development

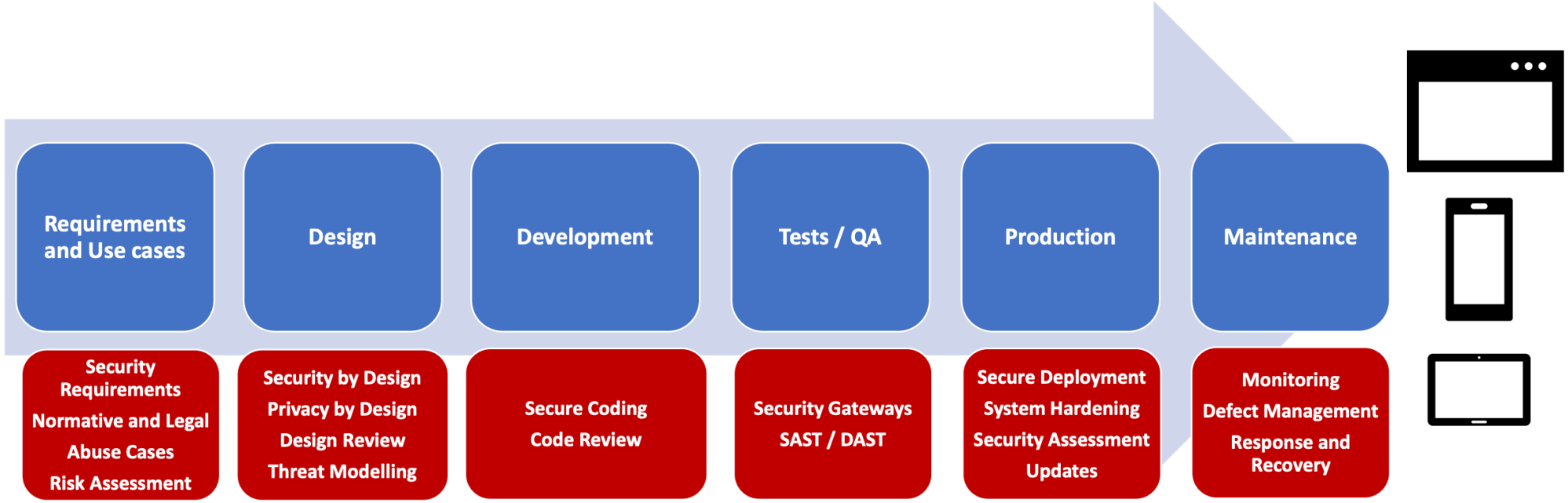
SEGURANÇA NAS ORGANIZAÇÕES E INFORMÁTICA

deti universidade de aveiro
departamento de eletrónica,
telecomunicações e informática

2024/2025

Secure Development

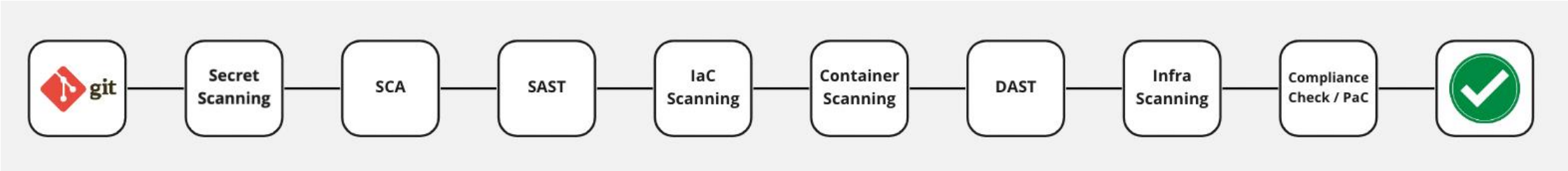
Recap (from theory)



Secure Development

A Secure Pipeline

A pipeline is a set of steps. We can build a software development pipeline that incorporates security considerations.



Example: OWASP DevSecOps Guideline to implement a secure pipeline (on github)

Reference

- Scan git repositories for finding potential credentials leakage.
- SAST (Static Application Security Test)
- SCA (Software Composition Analysis)
- IAST (Interactive Application Security Testing)
- DAST (Dynamic Application Security Test)
- IaC Scanning (Infrastructure as Code Scanning / scan configs)
- Infrastructure scanning
- Compliance check

Secure Development

Our pipeline focus for today

Source Code Management	How you handle git and some of the usual problems that arise, such as credential management, secrets, and passwords.
Dependency management	How you manage the libraries that are used for development and shipped with our applications.
Code Analysis	How to analyze existing source code for vulnerabilities and potential security problems.

Workshop Time

Step by step with GIT for a secure piple

Quick Changes

Bugfixes

STEP 4: SonarCloud
rename branch from master to main on sonar cloud

Step 5: ZAP

Update API Scanning:
https://github.com/oEscal/secure-git-workshop/blob/step5/.github/workflows/api-scanning.yml

Optional
Update rest-api-goat/docker-compose.yaml