

10th  
**UCAAT**

User Conference on  
Advanced Automated Testing

# Shifting Left: Integrating Automated Security Testing into Development Operations of a Research Project

**Dimitris Bougioukos**

*Application Security Team Lead*

**netcompany**

intrasoft

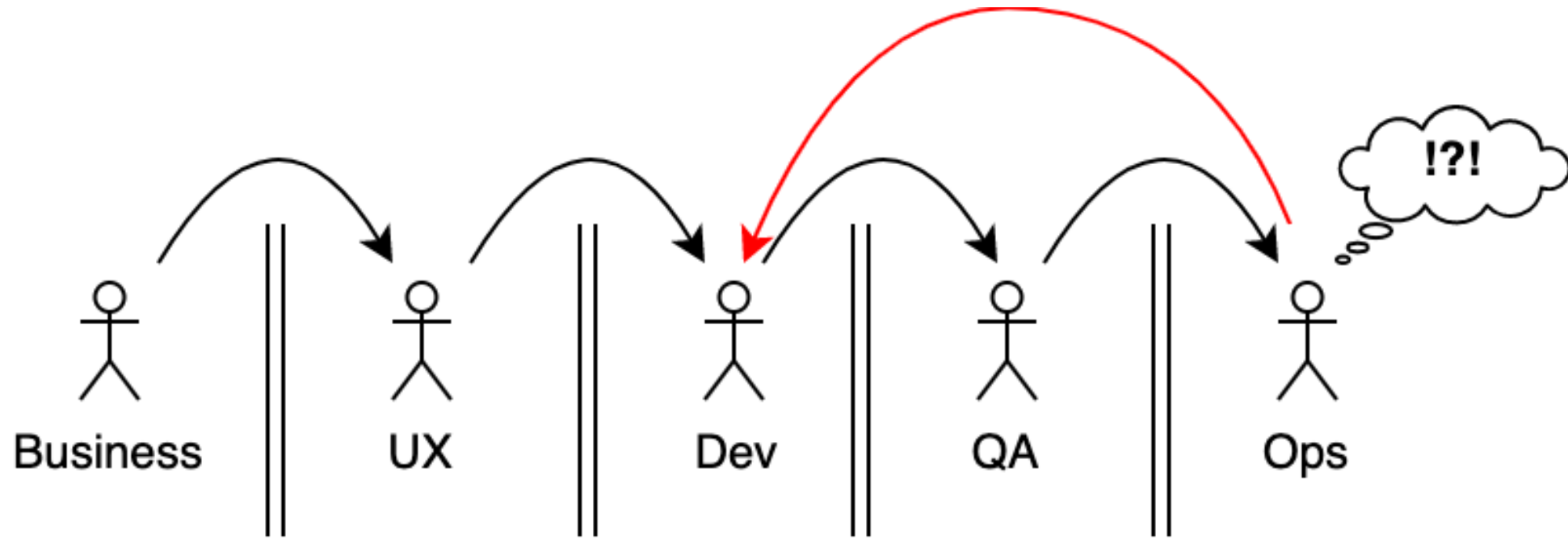
15/11/2023



INTRODUCTION

# WHAT IS DEVOPS?

# Traditional Software Engineering



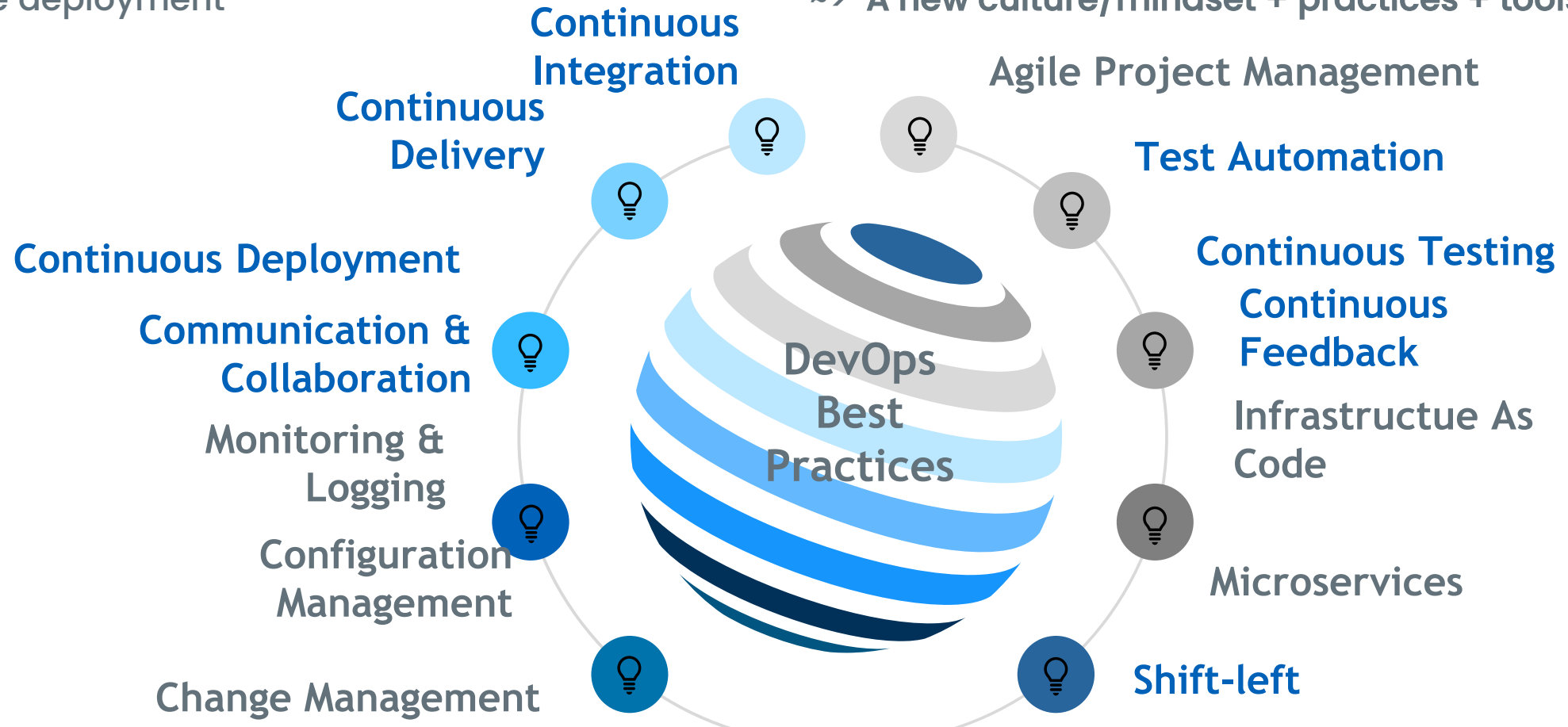
# The Wall of Confusion in Project Teams



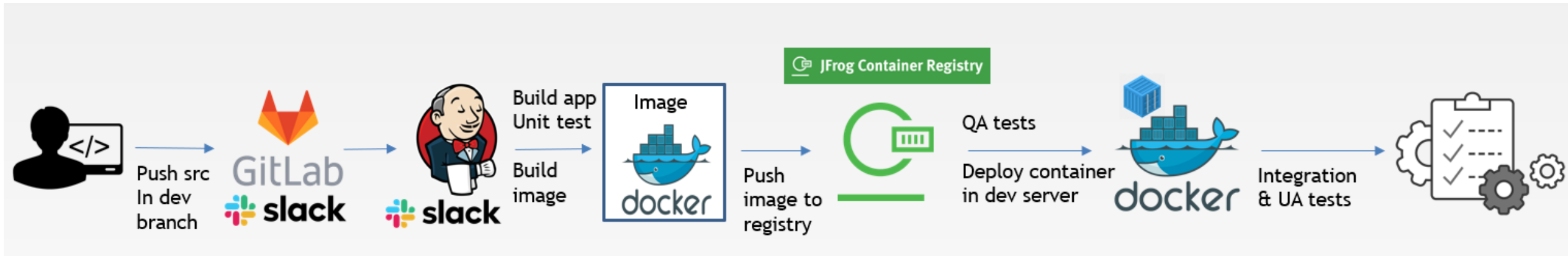
Graphic: <https://www.rightbrainnetworks.com/2016/01/08/5-promising-developer-tips-success-devops-world/>

# DevOps & CI/CD

DevOps stands for Development & Operations - A business drive to improve communication and collaboration among development and operations teams, in order to increase the speed and quality of software deployment  
~> A new culture/mindset + practices + tools



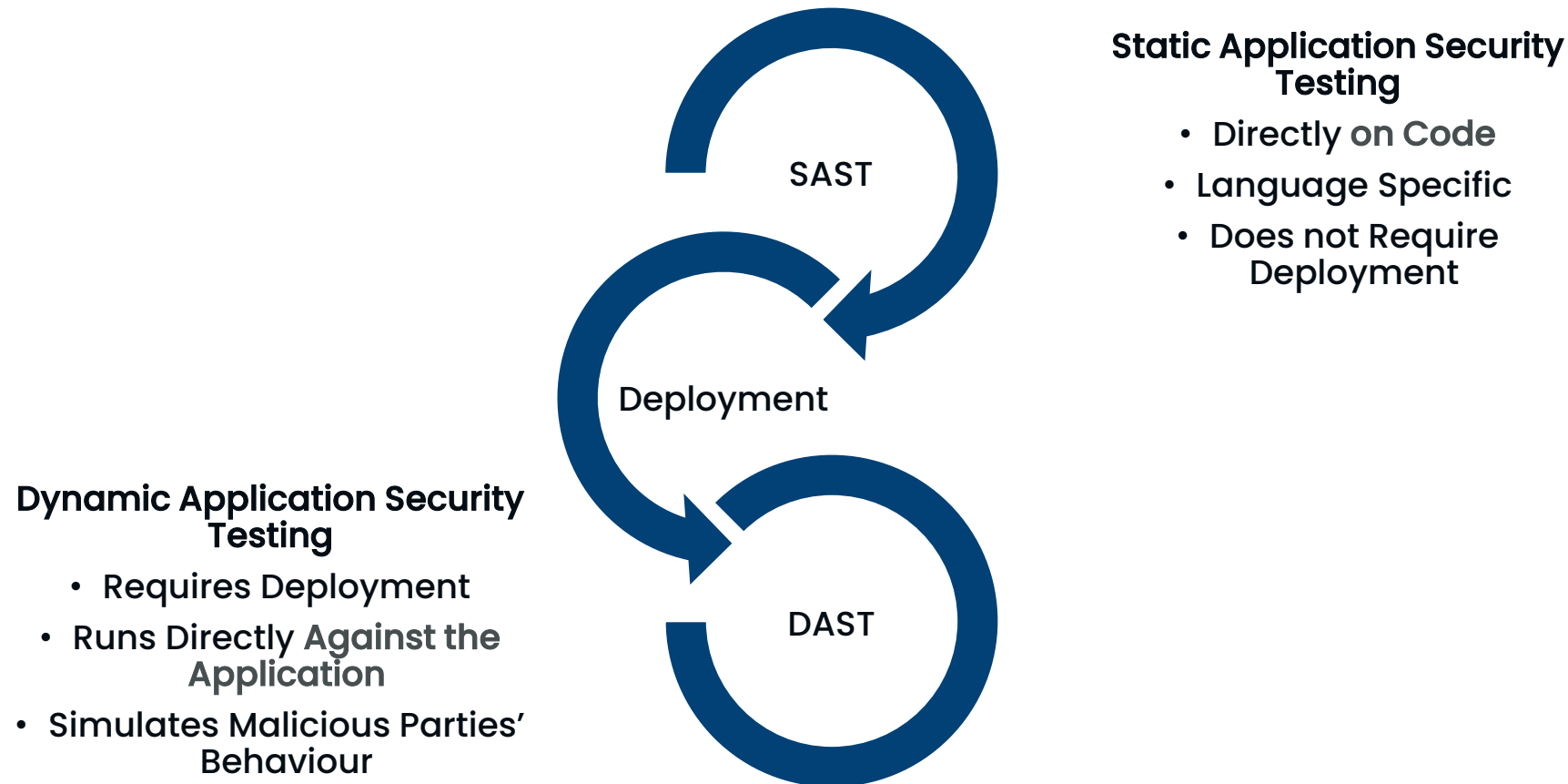
# Benefits of Automation Pipelines



- ✓ Teams focus on business requirements and high-quality code
- ✓ Multiple deployments per day if needed: faster-to-market/pilot sites
  - ✓ Significantly lower change failure rate

# From DevOps to DevSecOps

**DevSecOps** automates the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery!



Embracing DevOps principles  
is above all a change in  
**Organizational Culture.**



CHALLENGES OF

# MULTI-ORGANIZATION TEAMS

# Observation Sources



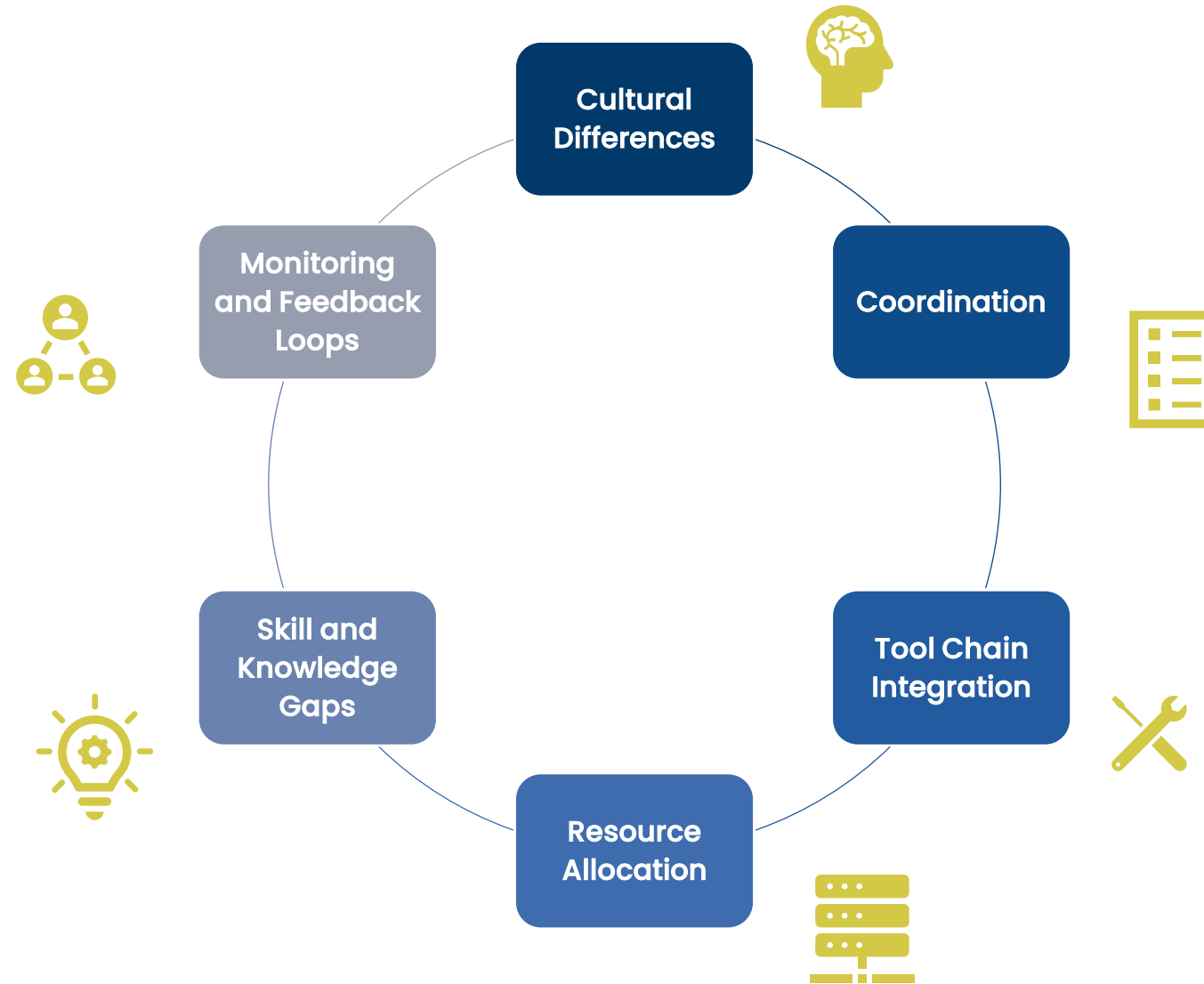
Funded under European Union's Horizon 2020 research and innovation programme under grant agreement No 952684.



Funded under European Union's Horizon 2020 Research and Innovation programme under grant agreement No 101017168.



# Challenges impeding DevSecOps in Multi-Organization Teams




# Hot Tips to Tackle Problems (1/2)

1. Establish and promote common DevSecOps **Culture**.
2. Identify a **common** set of DevSecOps tools.
3. Use **Infrastructure-as-Code** principles to define and manage infrastructure and environment configurations consistently.
4. Provide **training** and knowledge-sharing opportunities to bridge skill gaps.
5. Communicate **the benefits** of DevSecOps and the project changes effectively to reduce resistance.



# Hot Tips to Tackle Problems (2/2)

6. Develop a clear synchronization and coordination plan, including **release calendars** and dependencies.
7. Define a **common testing strategy** that includes unit tests, integration tests, security tests, performance tests, user acceptance tests. 
8. Set common **Acceptance Gates** for both security and general quality levels.
9. Continuously **monitor and optimize** the performance and scalability of the DevSecOps pipeline.

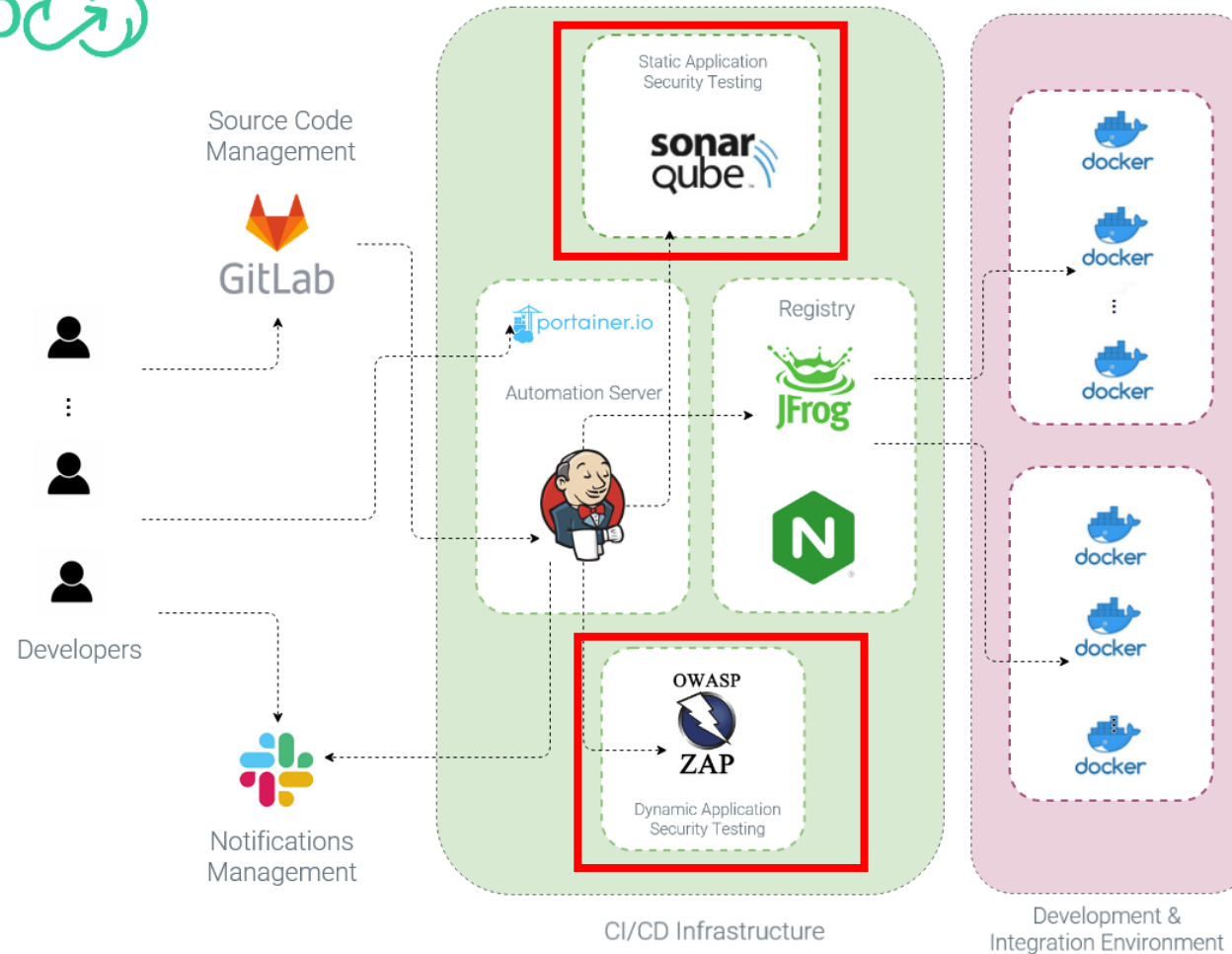
A TOUCH OF

SAST & DAST

# Sample CI/CD and Integration Testing Environment with SAST&DAST



**Disclaimer:** All depicted tools are open-source, possess "community editions" and may be replaced with equivalents, proprietary or not.





# Declarative Pipeline Definition

```

31 stages {
32   stage('Checkout') {
33     steps {
34       echo 'Checkout SCM'
35       checkout scm
36       checkout([[$class: 'GitSCM',
37                 branches: [[name: env.BRANCH_NAME]],
38                 extensions: [[[$class: 'CleanBeforeCheckout']],
39                 userRemoteConfigs: scm.userRemoteConfigs
40               ])
41     }
42   }
43
44   stage('Execute Unit Tests with Maven') {
45     steps {
46       echo 'Execute Unit Tests with Maven'
47       sh 'mvn -f pom.xml clean test'
48     }
49   }
50
51   stage('Assemble .jar with Maven') {
52     steps {
53       echo 'Assemble .jar with Maven'
54       sh 'mvn -f pom.xml package -DskipTests'
55     }
56   }
57
58   stage('Perform SAST with SonarQube') {
59     environment {
60       scannerHome = tool 'SonarQube'
61     }
62     steps{
63       withSonarQubeEnv(installationName: 'SonarIOTAC'){
64         echo 'Starting Static Application Security Testing analysis using SonarQube'
65         sh "mvn -X sonar:sonar"
66       }
67     }
68   }
69
70   stage('Perform System-Wide Vulnerability Assessment') {
71     steps {
72       script {
73         try {
74           echo 'Starting System-Wide Vulnerability Assessment analysis'
75           sh " curl --max-time 1 -X GET 'http://${SWVA_ADDRESS}/MultiModuleVulnerabilityPredictor"
76         }
77         catch (err) {

```



GITHUB + GIT

1. Developer Pushes Code using Git as SCM



GITHUB + GIT

2. GitHub Webhook Detects the Push Event



JENKINS + GIT

3. Code is Pulled From Git on CI/CD Server



JENKINS

4. **Unit / Functionality Tests** Are Being Executed



JENKINS

5. Code Is Packaged via a Build Automation Tool (Depending on Language)



SONARQUBE

6. **SAST** is Performed Directly on Code



SWVA Module

7. System-Wide Vulnerability Assessment (**SAST**) Performed



JENKINS + DOCKER

8. Docker Image Built following Dockerfile instructions



JFROG ARTIFACTORY

9. Docker Image Pushed to Registry



JENKINS + DOCKER

10. Earlier Version of App Undeployed



JENKINS + DOCKER

11. New Docker Image Deployed



OWASP ZAP

12. **DAST** is Performed



# Quality Gate Example



The screenshot displays the SonarQube interface for a project named 'master'. The 'Overview' tab is selected. The 'QUALITY GATE STATUS' section shows a green 'Passed' status with the message 'All conditions passed.'. The 'MEASURES' section shows two metrics: 'New Vulnerabilities' with a value of 0 and 'New Security Hotspots' with a value of 0. The 'Security' metric is shown as 'A' and 'Security Review' is also shown as 'A'. The 'Overall Code' section is partially visible.

- ✓ Quality Gates in SonarQube enforce a quality policy that sets conditions against which the master branch of the code repository is measured. Definition of Quality Gates in SonarQube is a combination of a measure, a comparison operator and an error value. Example: number of critical vulnerabilities must not exceed 0 and medium vulnerabilities 3.
- ✓ By using these KPIs a Quality Gate answers the practical question of whether a development project meets certain criteria and is ready for release.
- ✓ These KPIs will ensure the production of high-quality solutions and will drive the different components developments.

# Testing



# Thank you! Questions?

Feel free to contact me at:

[Dimitris.  
Bougioukos@netcompany.com](mailto:Bougioukos@netcompany.com)

**netcompany**

intrasoft