Evaluation of Automated Security Scanning Tools in DevSecOps

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Introduction

DevSecOps integrates security into CI/CD
Enables “shift-left” approach
Widely adopted using security tools
Effectiveness in real-world pipelines unclear
Tools are often used without proper evaluation

Research Question

Effectiveness of automated security scanning tools within CI/CD pipelines?

- **Detection Effectiveness**
- **Performance Impact**
- **Practical Integration**

The Process

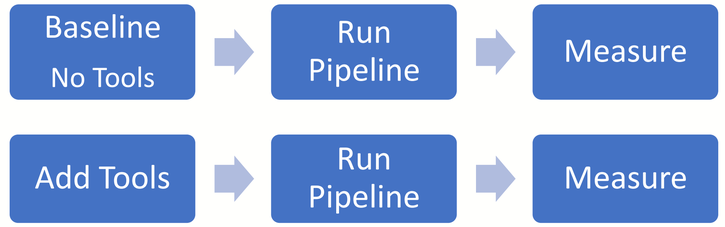

Figure 1: Evaluation Process

Methodology

CI/CD with Jenkins
Docker environment
Compare scan results

Literature Review

Shift-left improves security
Limited empirical comparisons
Trade-offs between tools unclear

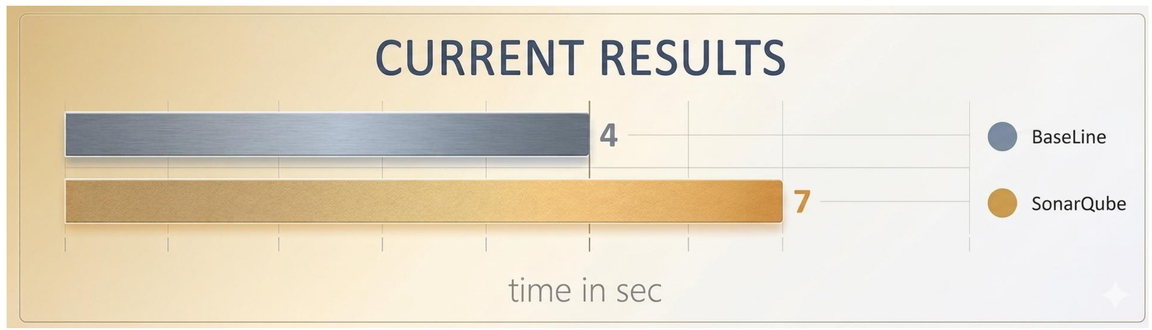

Figure 3: Scanning Tools Increase Pipeline Build Times

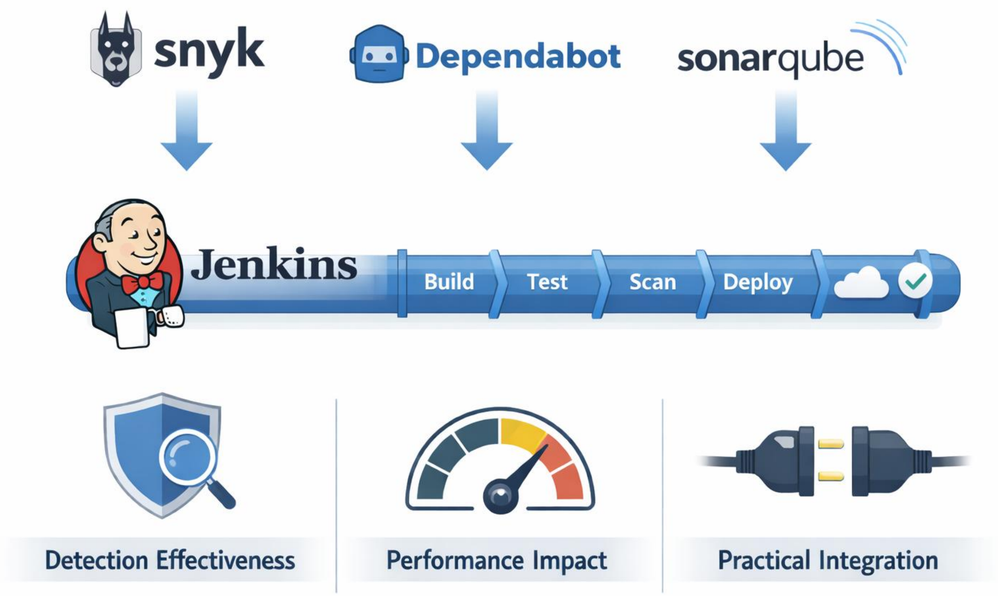

Figure 2: DevSecOps Integration Architecture

Next Steps

- Add more tools
- Analyse false positives
- Analyse Performance overhead
- Check Integration Issues

Angad Singh

setu.ie

C00315727@setu.ie