University of the West of Scotland

School of Computing, Engineering and Physical Sciences

**MSc Information Technology**

**MSc Final Project**

**Design and Implementation of Automated CI/CD Pipeline using DevSecOps Practices**

Student name: **Shahid Rasool**

Banner ID: **B01801311**

Email: **shahidchaudhary1119@gmail.com**

Project being undertaken on part-time or full-time basis: **Full Time**

MSc Programme (specify the specialist pathway, if any): **MSc Information Technology (DevOps)**

MSc Programme Leader:

**Contents**

**Abstract**

**1. Introduction to DevSecOps**

**2. Literature Review**

**2.1 CI/CD Automation and Pipelines**

**2.2 Security Integration in DevOps**

**2.3 Infrastructure as Code and Policy as Code**

**2.4 Monitoring and Feedback Loops**

**3. Gaps in Literature and Research Question**

**4. Tool Comparison and Selection**

**5. Short Methodology Outline**

**6. References**

**Abstract**

Security is often treated as an afterthought in the software development life cycle, despite the fact that a single breach can compromise the stability and reliability of an entire system. To achieve secure and continuous software delivery, security practices must be embedded throughout all stages of development rather than appended as a final step. In modern development environments, where developers frequently push code to central repositories multiple times a day, manual build and deployment processes are time-consuming, error-prone, and reliant on human oversight. These challenges underscore the necessity for automated systems that can manage builds, testing, and deployments efficiently while incorporating security controls at every stage of the pipeline.

This project proposes the design and implementation of an automated Continuous Integration and Continuous Deployment (CI/CD) pipeline integrated with DevSecOps practices. The proposed solution aims to streamline the software delivery process, reduce human error, and ensure that essential security checks are conducted automatically. The research is motivated by the growing demand for secure automation in software engineering and the limited availability of practical academic models demonstrating the integration of DevSecOps within CI/CD workflows.

The primary aim of this project is to design, implement, and evaluate an automated CI/CD pipeline with integrated DevSecOps mechanisms that enhance both the efficiency and security of software development and deployment processes.

1. **Introduction to DevSecOps**

DevSecOps, which merges Development, Security and Operations, is a methodology that incorporates security practices into the DevOps Workflow. It highlights the need of cooperation among development, operations, and security teams to guarantee that software applications are created securely, vulnerabilities are addressed, and risks are reduced during the software development lifecycle. DevSecOps advocates for the “shift left” principle, signifying that security measures should be integrated during the initial phases development instead of being considered later in development. By automating security procedures and establishing a culture of collective responsibility, DevSecOps improves a company’s security stance, accelerates application time to market, and encourages a proactive approach to security threats. (Tigera, 2025)

1. **Background: From DevOps to DevSecOps:**

**6. References**

Tigera. (2025, October 28). *What Is DevSecOps and What Do You Need to Succeed?* Retrieved from Tigera.io: https://www.tigera.io/learn/guides/devsecops/