DevSecOps Project Report

1. Introduction

Name: Idah Makena Ncooro

Institution: Strathmore University

Project: Final DevSecOps Project

This project represents a practical assessment applying industry best practices in CI/CD, testing, and monitoring. It showcases an automated DevSecOps pipeline deploying a containerized web application using tools like Docker, Jenkins, SonarQube, Selenium, Kubernetes, Netdata, and AWS CloudWatch.

2. Project Objectives

- Automate builds and deployments using Jenkins
- Scan code quality using SonarQube
- Package and serve the application using Docker and Nginx
- Deploy via Helm on Kubernetes (local and AWS)
- Monitor with Netdata and AWS CloudWatch
- UI testing with Selenium and Pytest
- Track progress with Jira
- Secure app with SSL and security headers

3. Environment and Tools Setup

Development Tools: VS Code, PowerShell, Git Bash, GitHub, Jira

Infrastructure: Docker, AWS EKS, AWS ECR

CI/CD: Jenkins, BlueOcean plugin

Code Analysis: SonarQube

Monitoring: Netdata, AWS CloudWatch

Testing: Selenium, Pytest

4. Appendix Summary

Appendix A: Tools setup and GitHub repository

Appendix B: React + Vite application with Docker containerization

Appendix C: Jenkins pipeline setup for CI/CD

Appendix D: Static code analysis via SonarQube, Selenium + Pytest tests

Appendix E: Kubernetes deployment (local + AWS)

Appendix F: Monitoring using Netdata and CloudWatch

Appendix G: Security with SSL and headers

Appendix H: Jira for sprint and issue tracking

Appendix I: EKS, ECR, Grafana, Prometheus, AWS deployments