**SWE 599 – Modern DevSecOps Architecture**

**Cankut ER**ID: 2022719219

Date: 10.11.2024

**The Plan for the Term Project**

This report aims to provide an outline of the tasks to be accomplished to complete the term project for “Modern DevSecOps Architecture”. Purpose of this report is mainly to inform the instructor regarding the steps to be taken and provide an estimated timeline to complete those.

This project will be composed of components and processes that will make up for a modern DevOps architecture where security elements is incorporated in the workflow. Infrastructure for the whole project will be a local Kubernetes cluster, most probably Minikube with docker as the driver for ease of reproduction. To further improve reproducibility, all infrastructure will be managed by Terraform to leverage IaC (Infrastructure as Code) concept. At the core of the CI/CD processes , Jenkins will be utilized build and deploy images. For security purposes, steps for static code analysis, dynamic application security testing, container image scanning and dependency vulnerability checks will be included. Below are the tentative list of tools to be used for security concerns.

* Trivy: Container Image Scanning (Possibly also for IaC script scanning)
* SonarQube: Static Code Analysis
* OWASP: Dynamic Application Testing and Dependency Checks

A repository will be chosen to be processed by the DevSecOps pipeline, preferably an API written in Java as it is supported by many of the tools mentioned above.

All the tools in the pipeline will be deployed to Kubernetes cluster as standalone services, configurations of which will also be covered in Terraform script. Jenkins will communicate to these services in the same Kubernetes cluster to conduct the analyses and scans. In the case of certain parameters are met, application will be deployed within the cluster.

As for the timeline of the project, implementation will be completed before any work done on the report. By the progress report deadline, I aim to have a very clear design and pipeline flow and a reasonably configured infrastructure. Until the final deadline, pipeline implementation will be completed and the project report will be written.

Tentative list of subjects in the project report are provided below.

1. Introduction

Definition of the project will be given. Additionally, personal motivation behind choosing this topic is going to be mentioned.

2. Project Overview

Definition of the problem the project aims to solve, introduction of the tools used in the project.

3. Architectural Design

Design of the infrastructure and pipeline will be discussed. Reasoning behind the design will be justified.

4. Implementation

Certain details, concepts or tunings will be discussed. Example snippets from the scripts will be shared and explained in order to give a more concrete feeling about how everything comes together.

5. Example Cases

Example cases and results of the pipeline for those will be demonstrated.

5. Conclusion and Future Growth

Key points obtained during the development of the project will be summarized. Possible improvements in the future will also be discussed.