2023

# DevSecOps

## LEERDOEL DOCUEMENT

SEM PLASMEIJER

# Contents

1. DevSecOps 2
1.1 Deployment 2
1.2 Kubernetes and container orchestration 2

# 1. DevSecOps

Due to the rise of AGILE working at the start of the century many companies have development teams that work more efficient, deliver faster and produce more features of higher quality than before. As a result, the more traditional way of delivering and operating the production of that code can't keep up. To counteract this change in development speed DevOps was created and the development team became responsible for maintaining quality of production, testing and release.

The idea of integrating different parts of development into single development team where multiple developers are responsible for the whole product on its own, also fused with the security aspects of development. DevSecOps was created to make it so the whole team knew about security features and how to create security by design.

## 1.1 Deployment

CI CD has become common place in most development teams where in the GIT environment automatic tests are run after a new merge request, after they have passed a new build is created which can be deployed to a server.

The deployment can happen in different steps DTAP is a common order where the first step is merging to development where most other developers can pull their features from and merge to. After they passed review, they can be deployed on a testing or test acceptance server where they can be tested by a dedicated team or customers. Lastly after all features have passed testing it can be deployed to production.

## 1.2 Kubernetes and container orchestration

Due to how servers work when expanding or even creating a new deployment server it will have different configurations than another server. Containers exist to standardize these configurations and create an environment where deployment can be automized. To help with the management of different containers and their scalability you need a tool to manage them the two market leaders in this field are Kubernetes and Docker swarm.

## 2. Observability

To make sure a system is built, deployed, and secured correctly a DevSecOps team needs to be able to observe the state of its application. For this they require to log, trace, and collect metrics of the production environment and come these with the function and non-function requirements.

The three main ways to track and observe your system are:

1. Logs
2. Metrics
3. Traces

Logs or logging is the act of collecting information your system or device puts out and storing them. Due to how data protection works you need to be able to achieve a complete deletion of logs which contain user information. Time stamping and identifying features of logs make them more useful for observation.

Metrics are the number your system puts out. How many requests does your system receive, how long per request, size of your data volume. Labelling different metrics, what they are and where they come from will help the team with finding core problems within the system.

Traces are event trackers. When did an event happen, what changed with the event, was the operation successful. A trace register what happens when an event is called and should be reproduceable if all circumstances are the same.

Different logs, traces and metrics can be linked to KPIs here a few important ones:

- Application Response Time
- Peak Response Time
- Error Rate
- Concurrent Users
- Requests per Second
- Application Availability Ratio