DSOFM

DevSec Operations Field Manual

The DevSecOps FieldManual

Tom Herfort und Dominik Sigmund

15 April 2021

1. Introduction

Here is my intro

2. 4-types-of-work

There are 4 types of work in IT:

1 Business projects. Projects around delivering direct customer value.

2 Internal IT projects. Infrastructure and operations projects, internal improvements.

3 Changes. Fixed, changes, improvements generated by the two above.

4 Unplanned work. Incidents

We should focus to use our time on business value only. For that we need to have internal IT projects to improve our components.

To minimize the unplanned work we need to have:

1 Stable Systems.

2 Trained Users.

3 Automation

4 Best Practises

3. docker

Docker is a set of platform as a service (PaaS) products that use OS-level virtualization to deliver software in packages called containers. Containers are isolated from one another and bundle their own software, libraries and configuration files; they can communicate with each other through well-defined channels. Because all of the containers share the services of a single operating system kernel, they use fewer resources than virtual machines.

Container: These are are what docker is built on. They encapsulate an application and all of its libraries and dependencies, so it can be run anywhere Docker is installed. There are other containerization platforms, so check out how Docker stacks up against Kubernetes.

Image: A Docker Image is a file that is essentially a snapshot of a container. You can create a container by running a Docker Image

A typical Dockerfile (node.js)

Base Image FROM node:alpine

Create app directory WORKDIR /opt/app

Copy Package.json into container COPY package*.json ./

RUN npm install

Copy more files COPY . .

Expose inner port EXPOSE 7500

Run node.js Service CMD ["node", "index.js"]

Build an image

docker build --tag <IMAGENAME> .

Run an image in a container

docker run <IMAGENAME> [-p <OUTERPORT>:<INNER-PORT>] [--name <NAME>]

Check running containers

docker ps

Check Logs from a container

docker logs <NAME> [-f]

Stop the Containers

docker stop <NAME>

4. npm-audit

Checks for vulns in packages

npm audit

It may also fix some issues

npm audit --fix

5. npm-outdated

Checks outdated packages.

Table of Contents