Continuous Integration & Delivery (CI/CD) in DevSecOps

Obaid ur Rehman
Software Architect / Engineering Manager @ **Folio3**

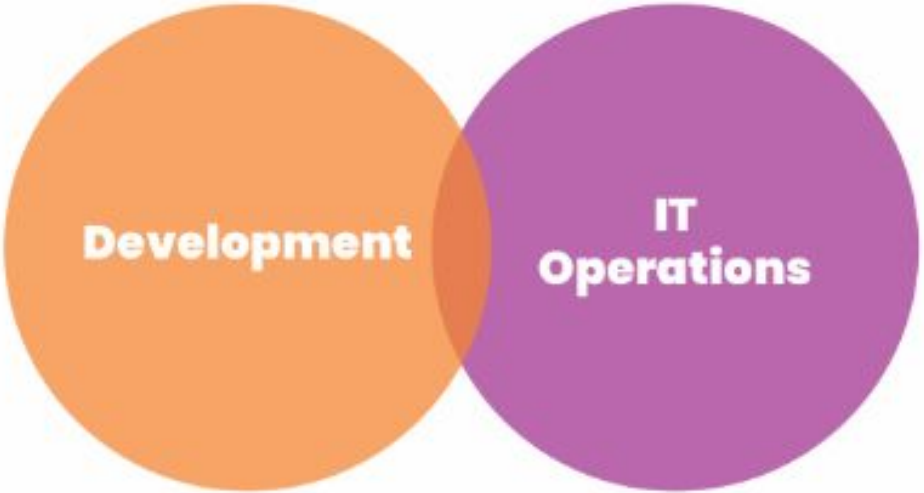
Introduction

- Software Architect / Engineering Manager at **Folio3**
- BS(CS) University of Karachi 2006, MS(SPM) FAST-NUECS 2010
- Over 17+ years of professional experience.
- Architected & Delivered numerous highly scalable, enterprise level applications in industries like Wall street trading systems, ecommerce, consumer applications.
- Part of Leadership team at the Folio3 Cloud Practice.

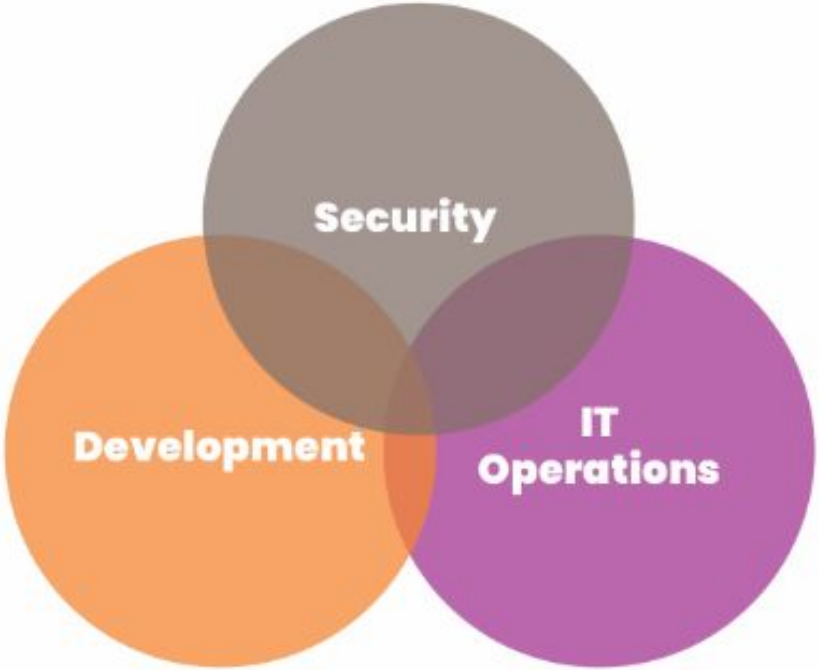
CI/CD: Agenda

- CI/CD in the DevOps cycle
- What is CI/CD
- Delivery v/s Deployment
- Benefits of CI/CD
- Pipelines
  - A typical CI/CD Pipeline
- CI/CD Tools / Provider
- Real world example
- Hands on CI/CD using Github Actions

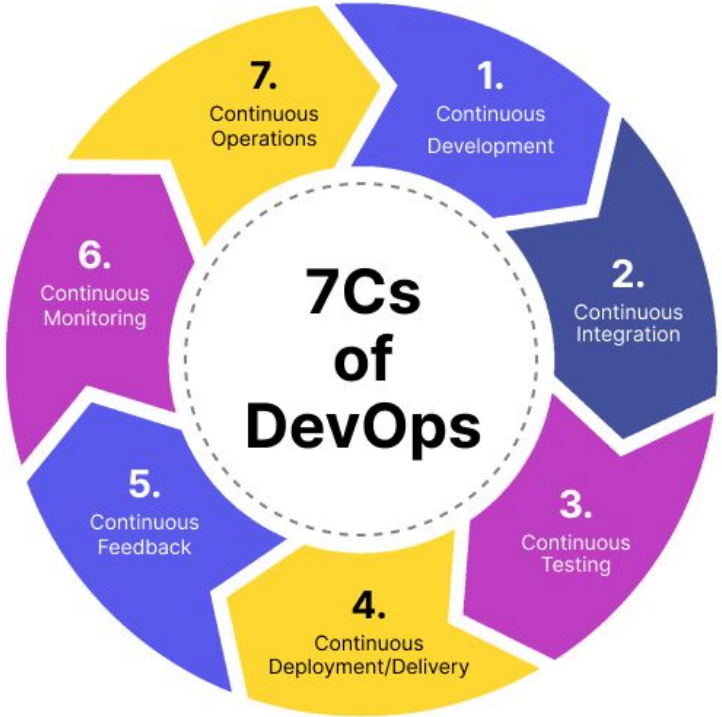
DevOps



DevOps



The DevOps Cycle - 7 Cs



What is CI/CD?

Continuous Integration

An approach to continuously **validate the state** of your codebase in the repository by building/compiling it.

Continuous Delivery / Deployment

An approach to continuously deploy artifacts that pass the CI Phase to some environment.

Delivery V/S Deployment

Continuous Delivery V/S Deployment

Continuous Delivery

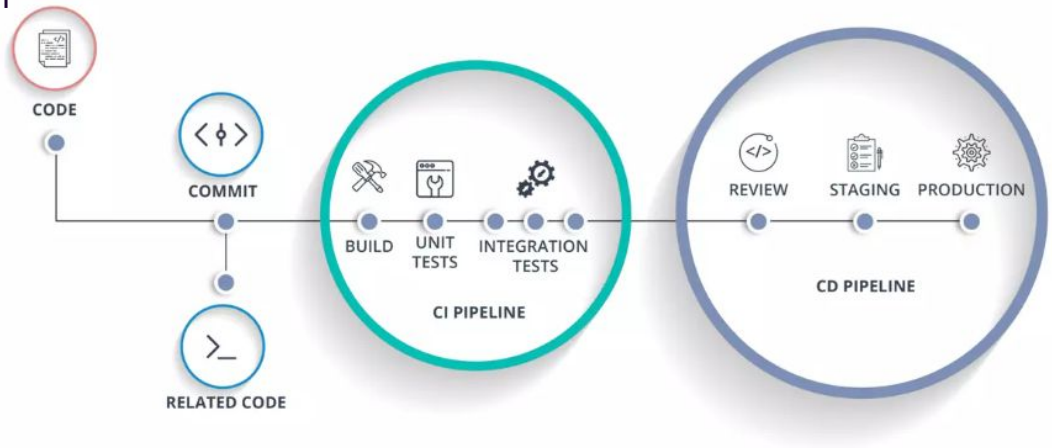
Automatically prepare and deploy to Production with a manual approval.

Continuous Deployment

Continuously deploy artifacts that pass the CI Phase to some Environment.

Why CI & CD?

- Smaller **changes in code - visibility**
- **Continuous Testing** in place
- Early **Fault detection**
- **Faster Release** to Production
- Rapid **Feedback**
- Customer **satisfaction**



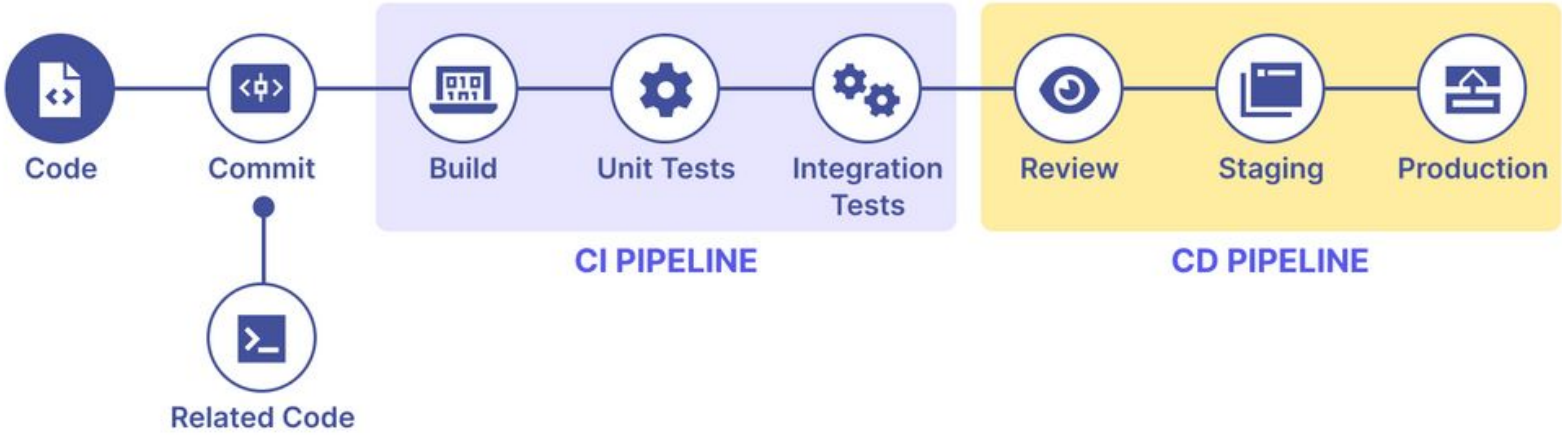
Benefits

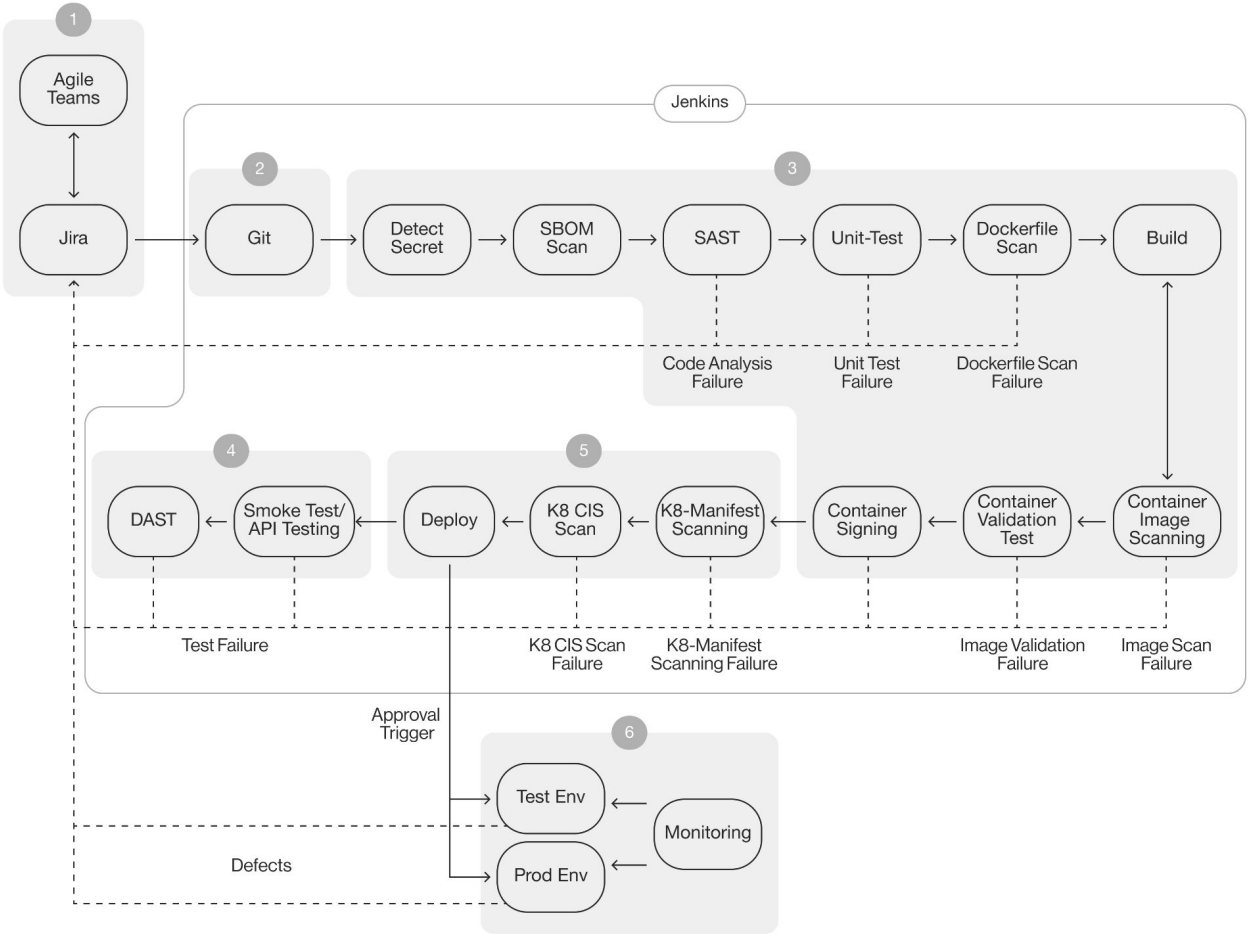
Faster Deployment
Improved Quality
Better Collaboration
Reliable Deployments
Rapid Feedback

What is a pipeline?

- A route from development to production.
- Within a CI/CD pipeline, a software release artifact moves and through various stage of the pipeline right from the code check-in stage through the builds → tests, deployment.

A Typical CI/CD Pipeline
Bringing CI/CD Together




1
Agile Teams
Jira
Jenkins
2
Git
3
Detect Secret
SBOM Scan
SAST
Unit-Test
Dockerfile Scan
Build
Code Analysis Failure
Unit Test Failure
Dockerfile Scan Failure
4
DAST
Smoke Test/ API Testing
5
Deploy
K8 CIS Scan
K8-Manifest Scanning
Container Signing
Container Validation Test
Container Image Scanning
Test Failure
K8 CIS Scan Failure
K8-Manifest Scanning Failure
Image Validation Failure
Image Scan Failure
Approval Trigger
6
Test Env
Monitoring
Prod Env
Defects

DevSecOps Tool chain

SAST: Bandit nodejsscan snyk

SBOM: aqua trivy

Container Scan: Docker Scout

K8 Manifest Scanners: aqua kube-bench

DAST: Pentest Tools

Popular CI/CD Providers

GitHub

GitLab

TeamCity

Jenkins

Travis CI

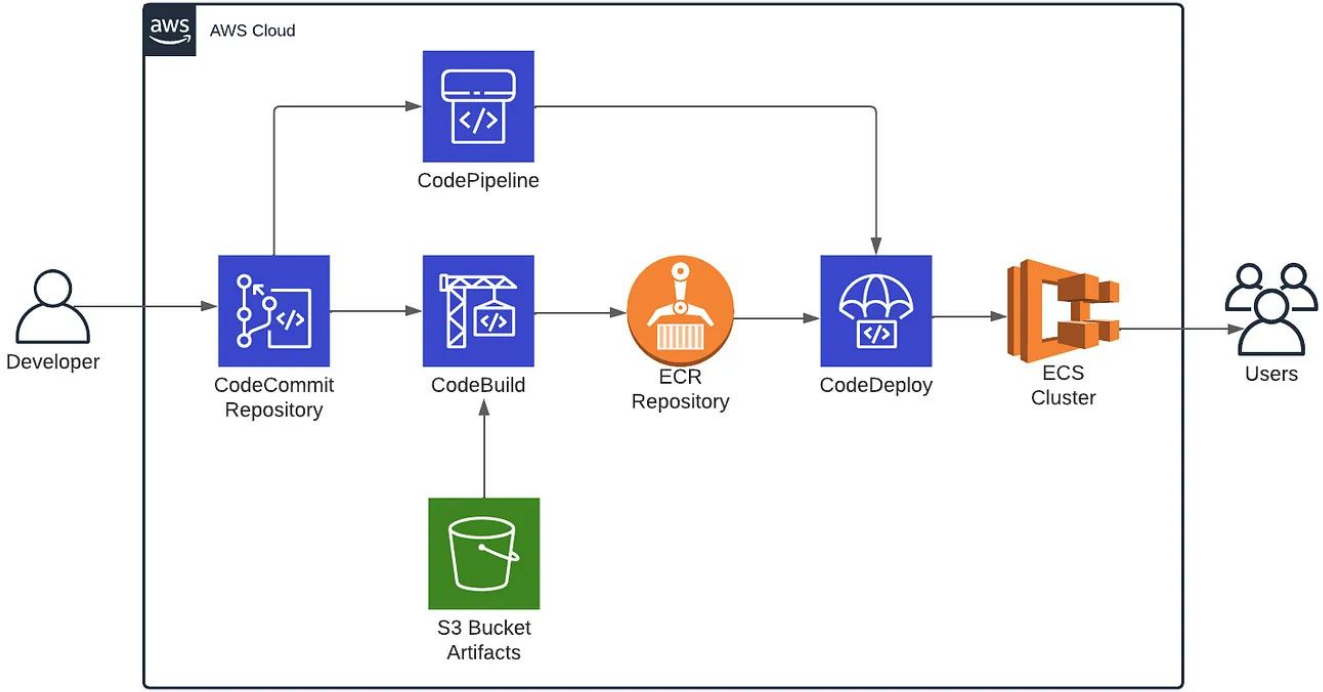
CircleCI

Codeship

Deploybot

CI/CD in the Realm of Cloud

Real world example - CI/CD on AWS



Lab: GitHub Actions Hands-on

Checkout code

Build → docker image→ **Test** → **Push** it to docker hub repository.

Requirements: Github Account, DockerHub account and some very basic Python

The End