DevSecOps 101

Rashid Shaikh

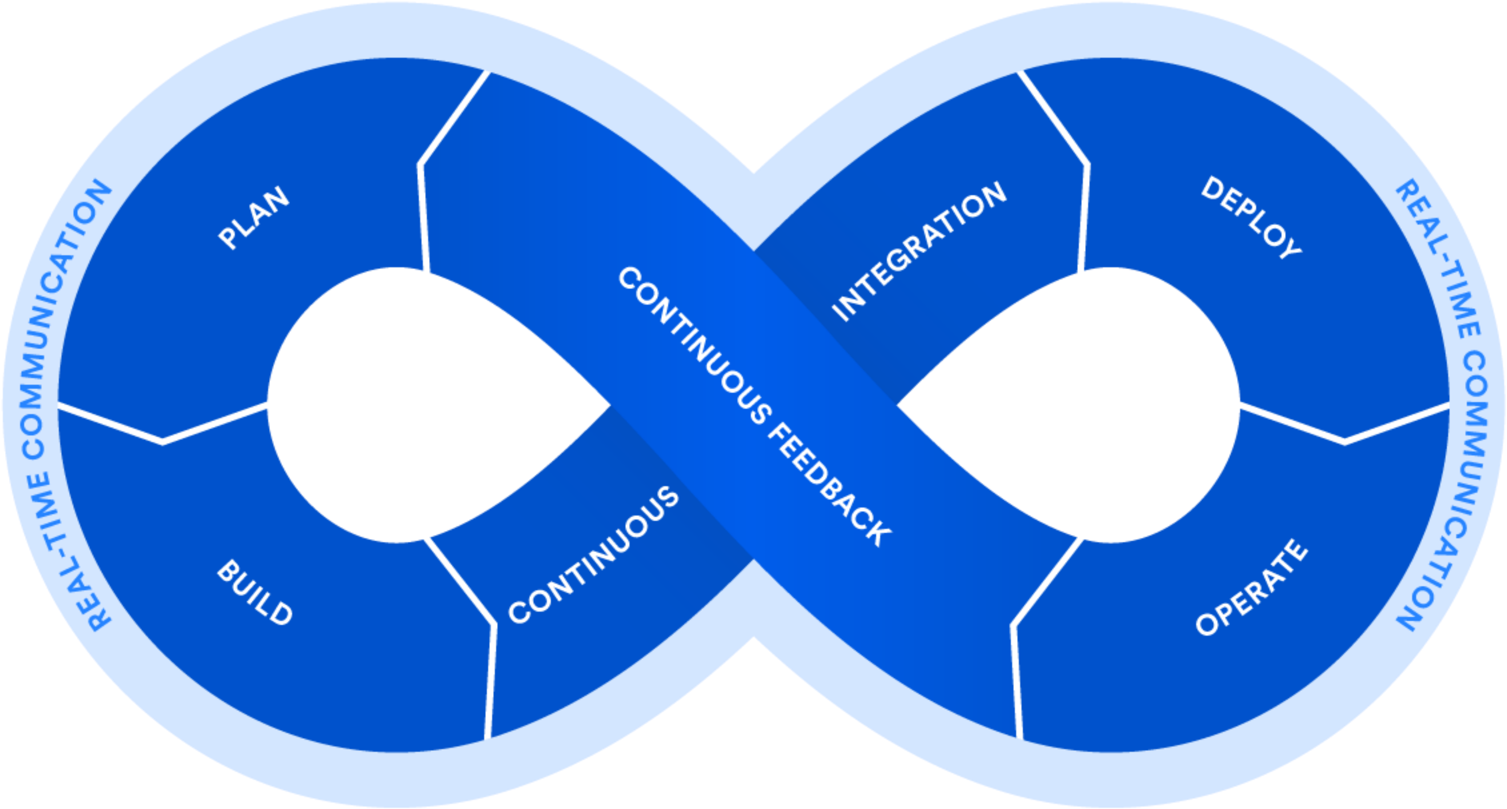
Network Intelligence India (NII)

Twitter **@CyberArmour**

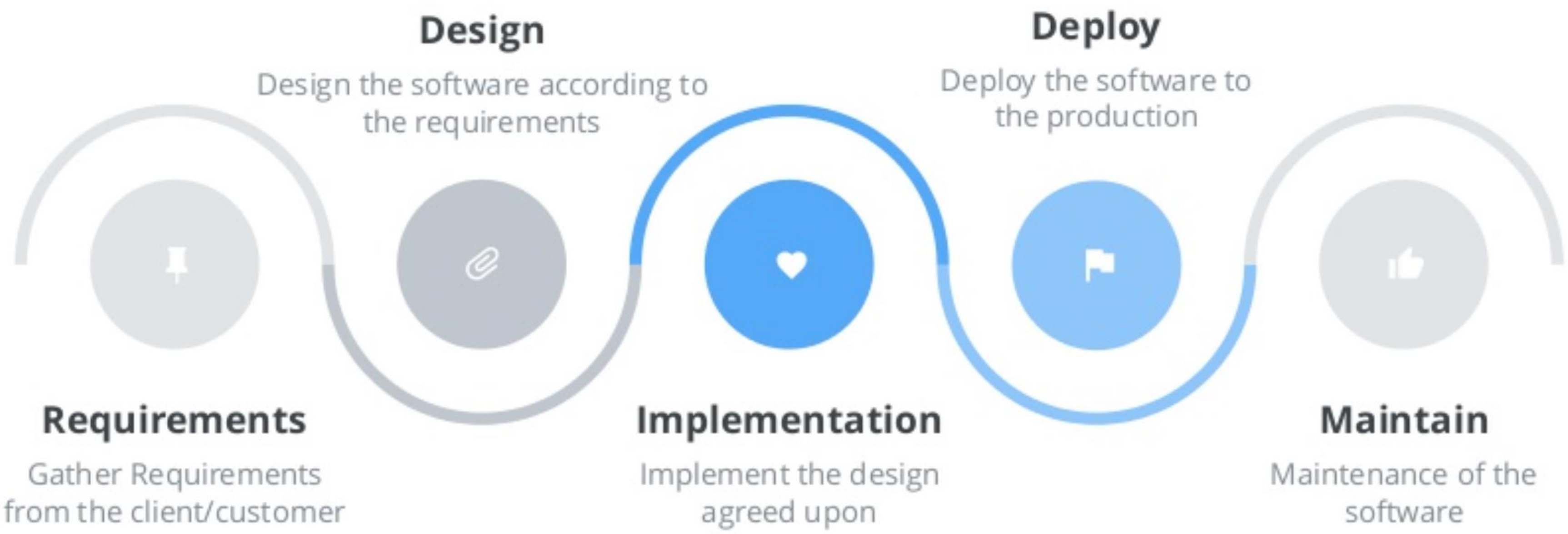
Agenda

- Introduction
- Traditional SDLC (Waterfall)
- Introduction DevOps and DevSecOps
- DevSecOps Principal.
- Important Factor.
- Secure SDLC

DevOps


REAL-TIME COMMUNICATION
PLAN
BUILD
CONTINUOUS
CONTINUOUS FEEDBACK
INTEGRATION
DEPLOY
OPERATE
REAL-TIME COMMUNICATION

Waterfall Model



Requirements

Gather Requirements from the client/customer

Design

Design the software according to the requirements

Implementation

Implement the design agreed upon

Deploy

Deploy the software to the production

Maintain

Maintenance of the software

Pitfalls Of Waterfall Model

- Long Release Cycles
- A lot of ”WIP”
- Functional Silos
- Incredible Rigid

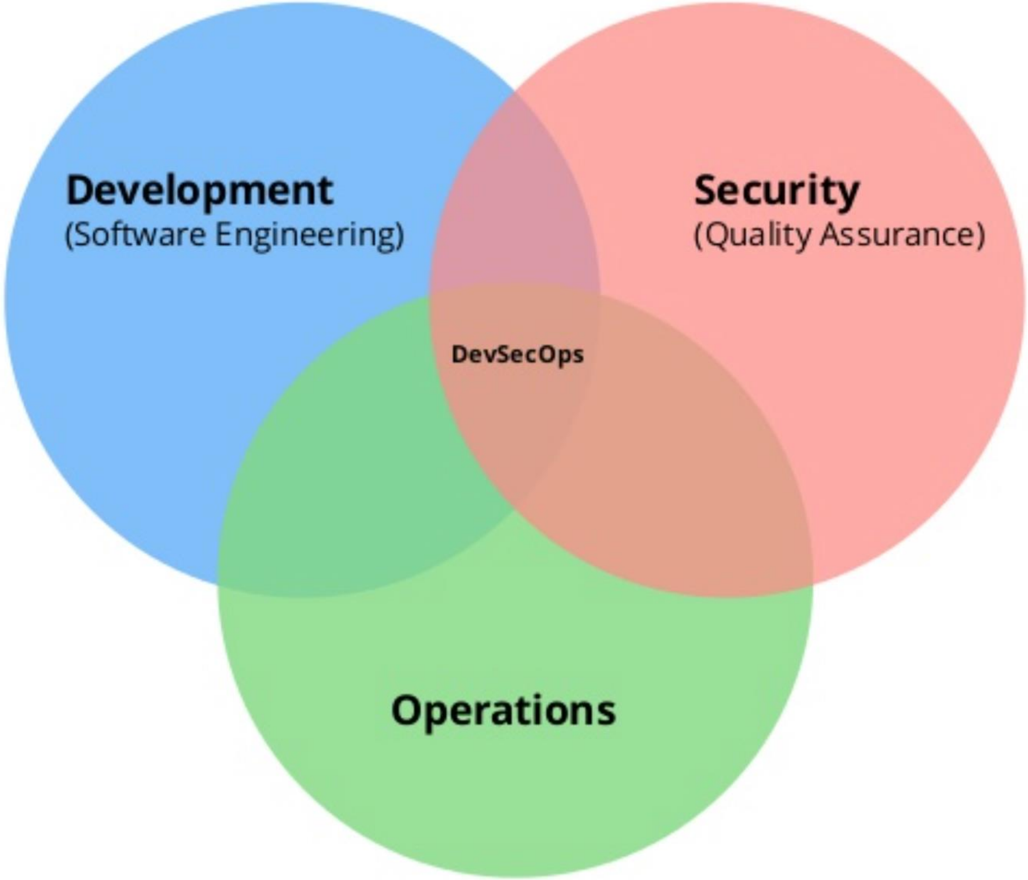
Then Agile Comes In …

- Shorter Release Cycle
- Smaller Batch Size
- Cross Functional Teams
- Incredibly Agile

What is DevOps

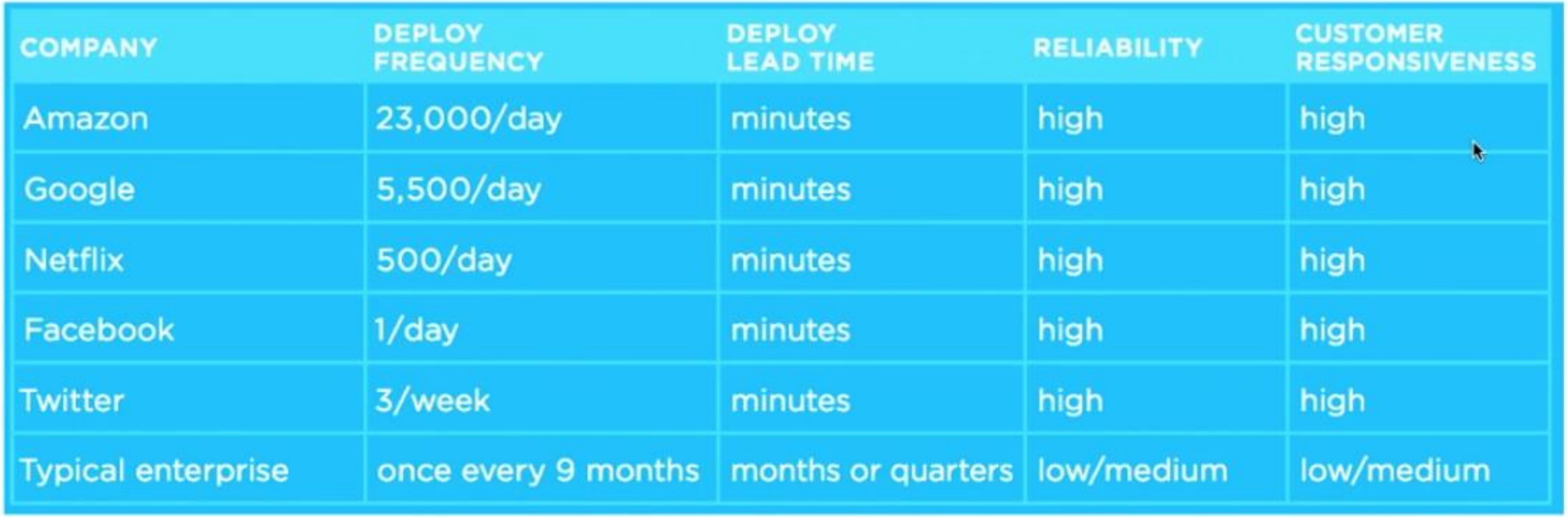
- Set of principles and practice for efficient communication and collaboration (Culture)
- Automated Deployment Pipeline (Process)
- Supporting Tool chains (Technology)

DevSecOps


Development
(Software Engineering)
Security
(Quality Assurance)
DevSecOps
Operations

Security Challenges In DevSecOps

- Target State
  - Enable organization to deliver inherently secure software at DevOps Speed



COMPANY	DEPLOY FREQUENCY	DEPLOY LEAD TIME	RELIABILITY	CUSTOMER RESPONSIVENESS
Amazon	23,000/day	minutes	high	high
Google	5,500/day	minutes	high	high
Netflix	500/day	minutes	high	high
Facebook	1/day	minutes	high	high
Twitter	3/week	minutes	high	high
Typical enterprise	once every 9 months	months or quarters	low/medium	low/medium

Source: https://xebialabs.com/assets/files/whitepapers/ITRev_DevOps_Guide_5_2015.pdf

DevSecOps Principles

- Culture
- Process
- Technology

Culture

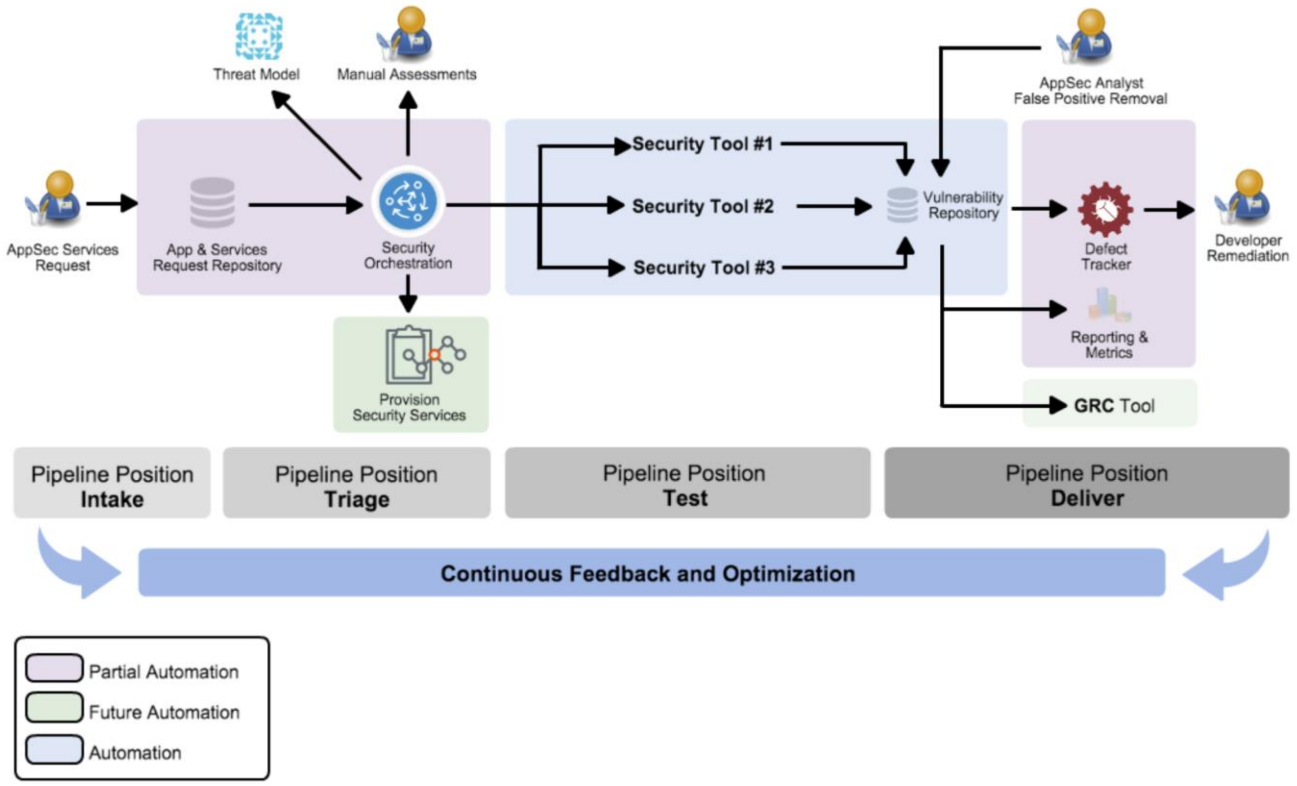
- Communication and transparency
- High trust environment
- Continues Improvement
- Security is everyone responsibility
- Automate as much as possible
- Everything as code

Process

- Training
- Understanding Requirements
- Architecture & Design
- Coding
- Testing
- Deployment
- Post Deployment

OWASP Appsec Pipeline

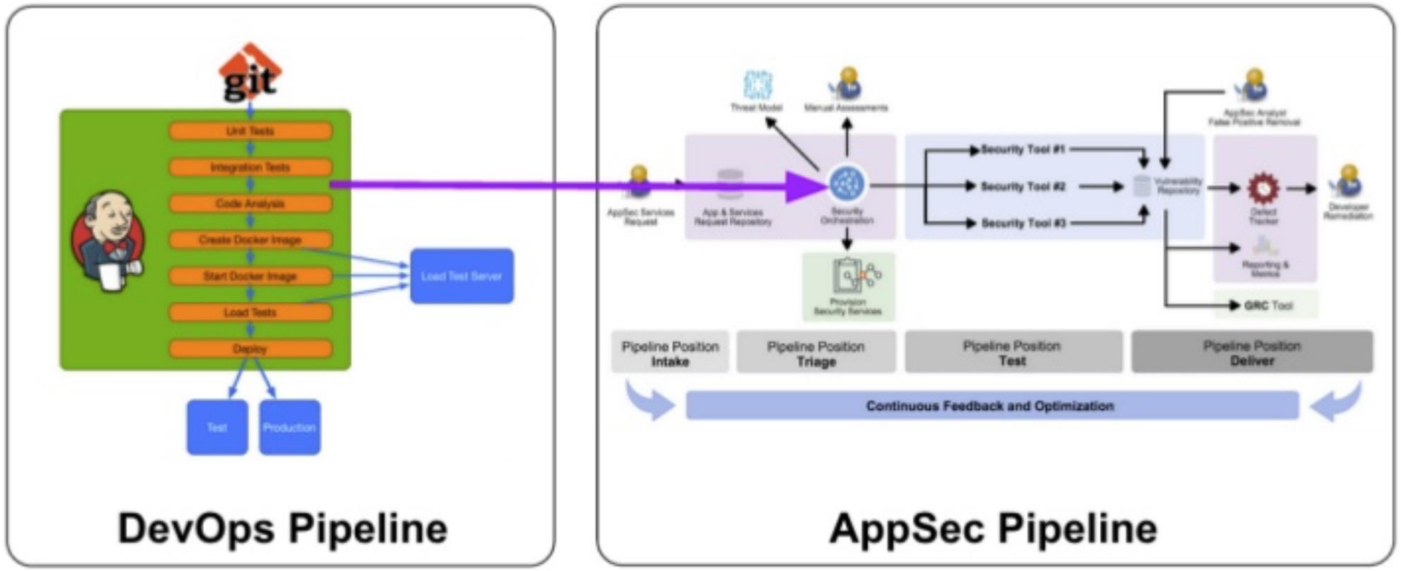
Rugged Devops - AppSec Pipeline Template



Aaron Weaver, CC ShareAlike 3.0

DevSecOps Pipeline

OWASP AppSec Pipeline



DevOps Pipeline

AppSec Pipeline

Technology

- Requirement
- Code (IDE plugins) => SAST
- Testing (Gautlt… burpsuite .. ZAP ..) => *AST
- Configure (Security As a Code)
- Maintenance (Patch Management)
- Monitoring (Audit, Attacks)

Summary

- Waterfall Model
- Agile
- DevOps
- DevOps v/s DevSecOps
- DevSecOps Principle (Culture, Process and Technology)

Thanks