Building Your First DevSecOps Pipeline

[Karan Sharma]

$ whoami

- Founder @ Wise Fox Security
- CDP | OSWE | OSCP | eWPTX certified
- Passion - Web/Mobile | DevSecOps | Code Auditing
- Twitter - @W1S3F0X
- YouTube Channel - Wise Fox Security

OWASP
NEW
ZEALAND
owasp.org.nz

QUANTUM
SECURITY

AUT

CyberCX

DATACOM

snyk

Auth0

Checkmarx

HCL AppScan

kordia®

LATERAL
SECURITY

MICRO
FOCUS®

Pulse Security
www.pulsesecurity.co.nz

RedShield

Flux

SEQA™
Information Security

Cobalt

LACEWORK

SecureFlag

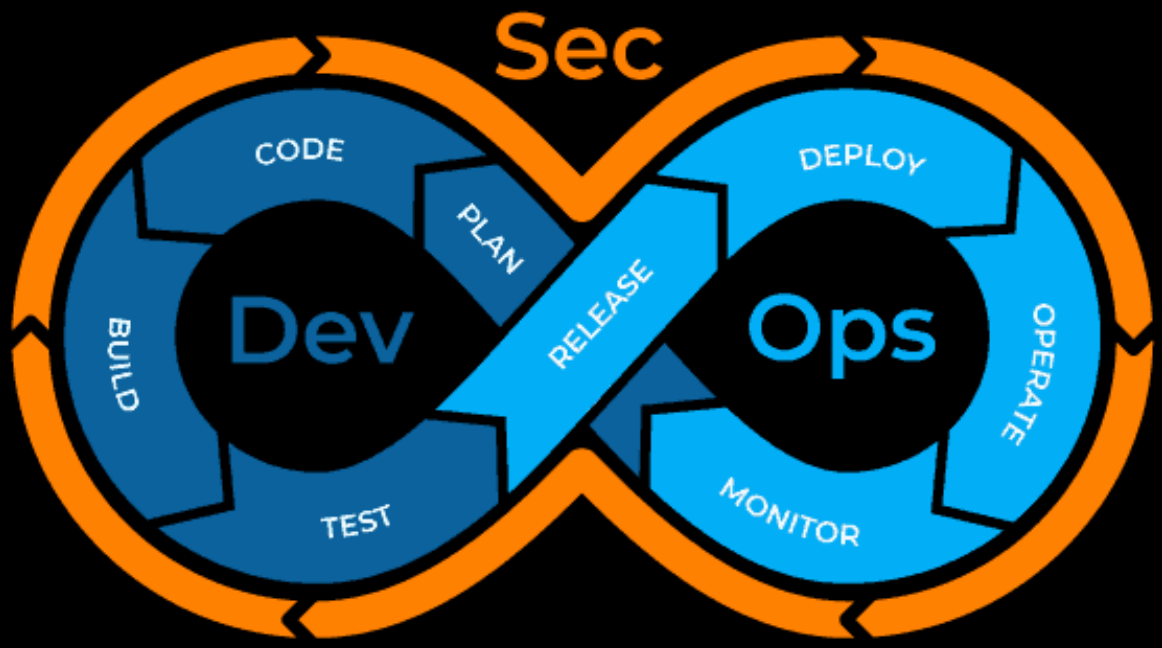
Without them, OWASP New Zealand Day couldn't happen

Agenda

- What & Why DevSecOps?
- DevSecOps Buzzwords
- CI/CD Pipeline Overview
- Traditional Security vs Shift Left Approach
- Practical Walkthrough

What is DevSecOps?

- Short for Development, Security, and Operations.
- Automates the integration of security at every phase of the software development lifecycle.
- From initial design through integration, testing, deployment, and software delivery.



Why DevSecOps?

- We want to catch security issues as early as possible.
- High visibility of security threats.
- It helps shorten development cycles.
- Development teams see security as an enabler, not an impediment.

DevSecOps Buzzwords

- ***SAST:*** *Static Application Security Testing*
  - *It is also known as white box testing. It allows you to find security vulnerabilities in the application source code earlier in the software development life cycle.*
    E.g. SonarQube, Snyk, Veracode etc.

- ***DAST:*** *Dynamic Application Security Testing*
  - *It can find security vulnerabilities and weaknesses in a running application, typically web apps.*
    E.g. AppScan, Checkmarx.

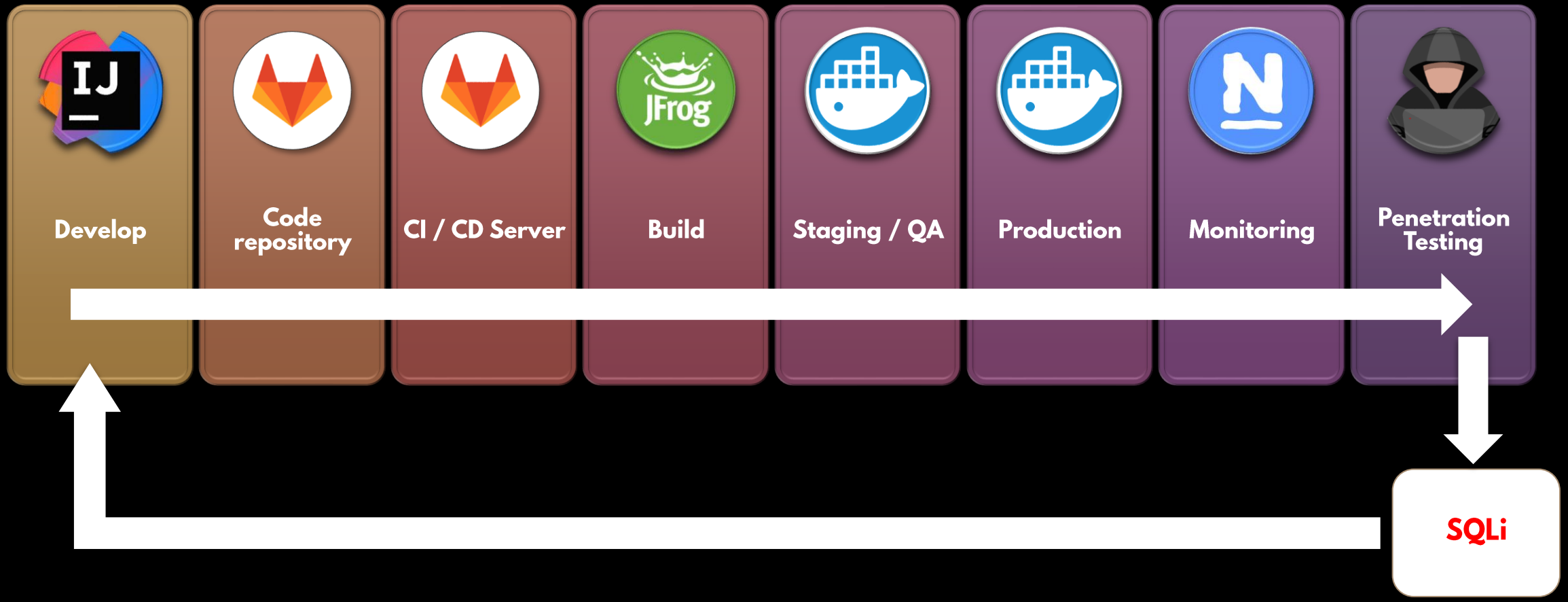
- ***RASP:*** *Runtime Application Security Protection*
  - *It's a security technology that is built or linked into an application or application runtime environment, and is capable of controlling application execution and detecting and preventing real-time attacks.*
    E.g. Sqreen (now Datadog), OpenRASP by Baidu.

- ***IAST:*** *Interactive Application Security Testing*
  - *Analyzes code for security vulnerabilities while the app is run by an automated test, human tester, or any activity "interacting" with the application functionality.*
    E.g. Seeker by Synopsys, Contrast Assess.

- ***SCA:*** *Software Composition Analysis*
  - *Identifies all the open source libraries and extensions used in a codebase and maps that inventory to a list of current known vulnerabilities.*
    E.g. RetireJS, Safety, Snyk etc.

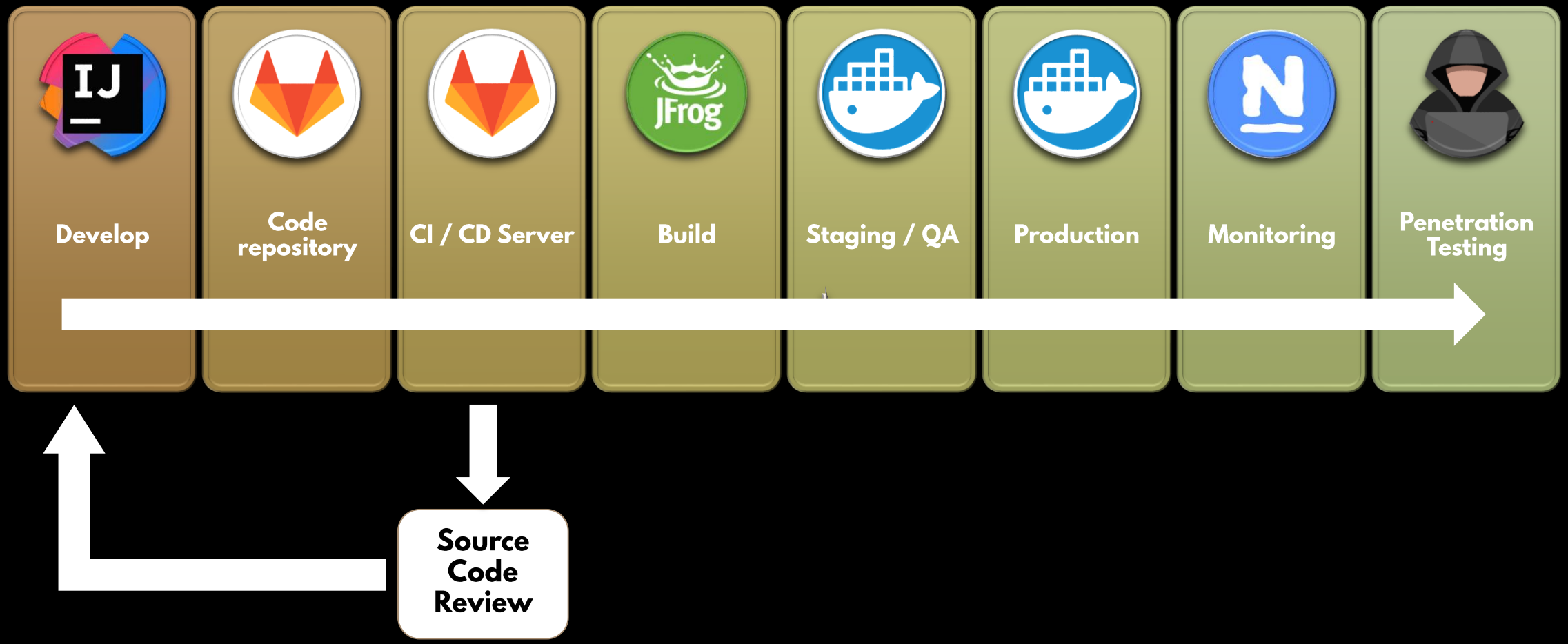
- ***IaC:*** *Infrastructure as Code*
  - *It is the managing and provisioning of the infrastructure through code instead of manual processes.*
  - *With IaC, configuration files are created that contain your infrastructure specifications, which makes it easier to edit and distribute configurations.*
    E.g. AWS CloudFormation, Red Hat Ansible, Chef, Puppet, Terraform and so on..

Traditional Process

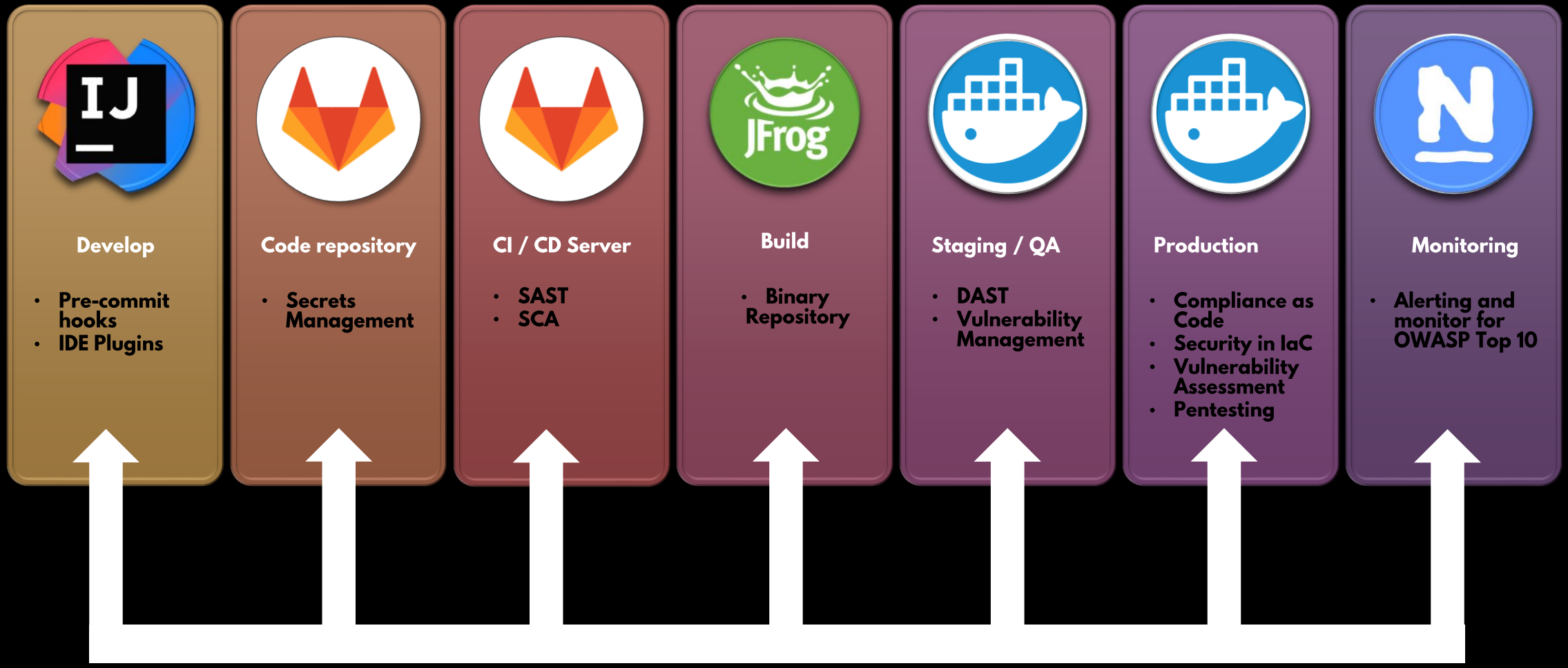


https://notsosecure.com/achieving-devsecops-open-source-tools

The Shift Left Approach

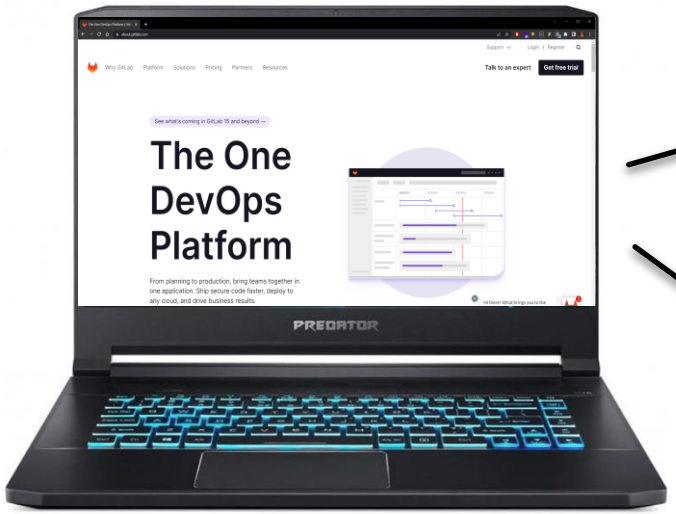


https://notsosecure.com/achieving-devsecops-open-source-tools



https://notsosecure.com/achieving-devsecops-open-source-tools

Lab Setup



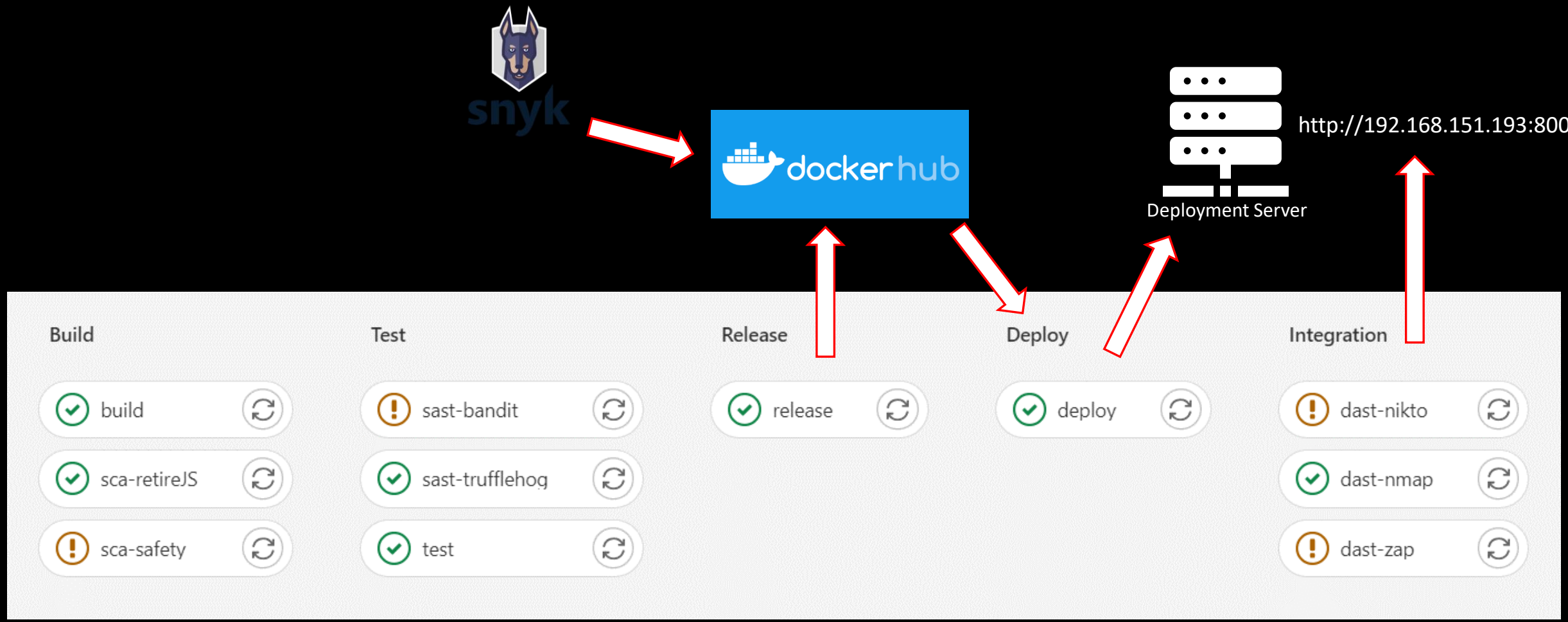
Host Machine

GitLab

VM1 - GitLab Runner

VM2 - Deployment Server

Pipeline Overview


snyk
docker hub
Deployment Server
http://192.168.151.193:8000
Build
build
sca-retireJS
sca-safety
Test
sast-bandit
sast-trufflehog
test
Release
release
Deploy
deploy
Integration
dast-nikto
dast-nmap
dast-zap

@W1S3F0X