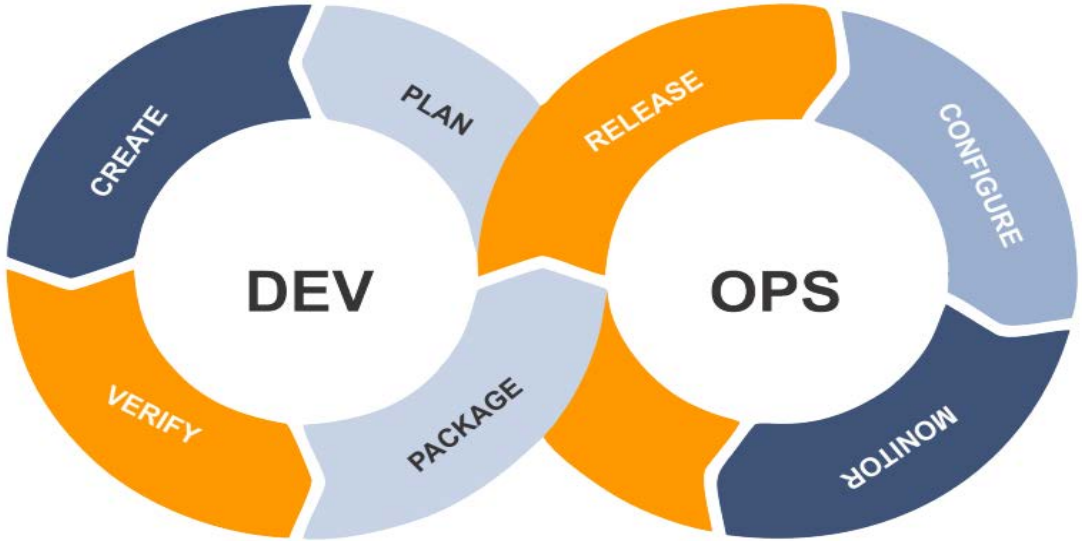
# How Security Best Practices Enable DevOps Data Transformation - DevSecOps

2019 QSC India Conference

Deepak Naik I Vice President | Security Engineering
Axis Bank

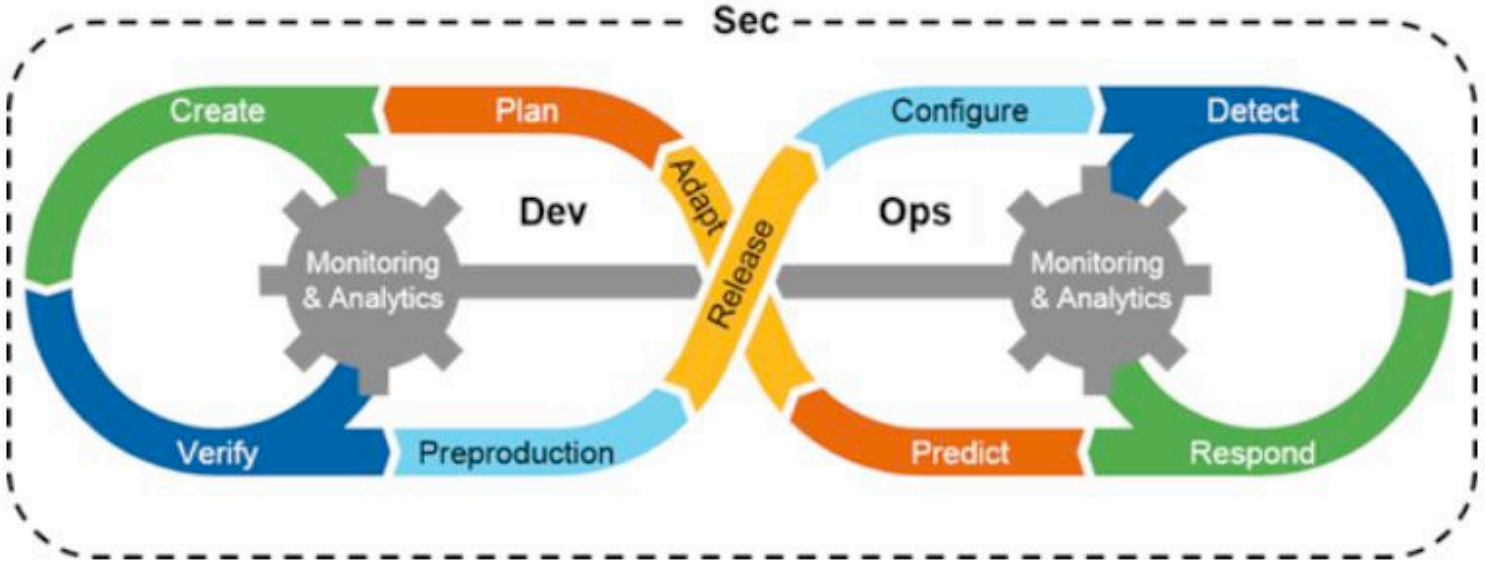
# What is DevOps?

DevOps ensures the collaboration between the teams (development and operations) by eliminating the common challenges they face while following other traditional models, say Waterfall Model. DevOps aims at shortening the systems development life cycle while delivering features, fixes, and updates at a faster pace in close alignment with business objectives.

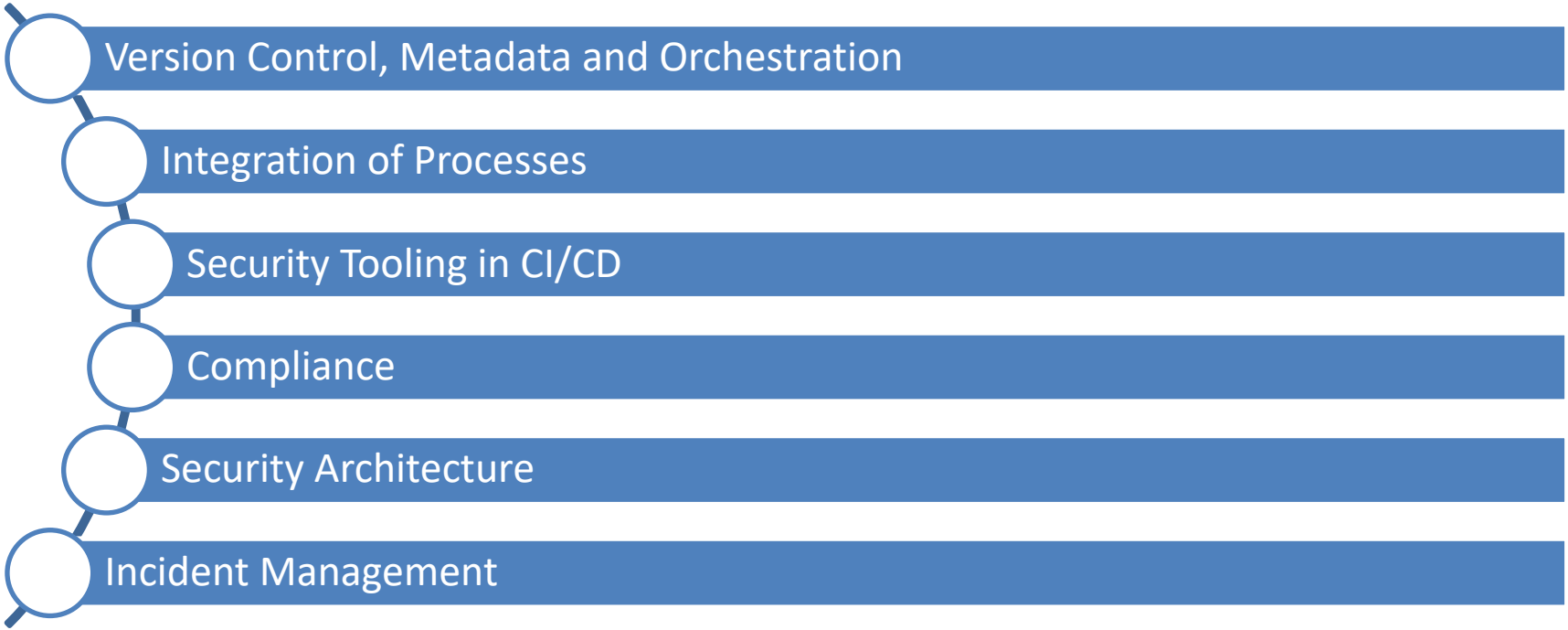


# What is DevSecOps?

It was introduced for integrating security extension with DevOps approach. Hence DevSecOps approach involves creating a 'Security as Code' culture with ongoing, flexible collaboration between security engineers and security teams.



# Different DevSecOps Process





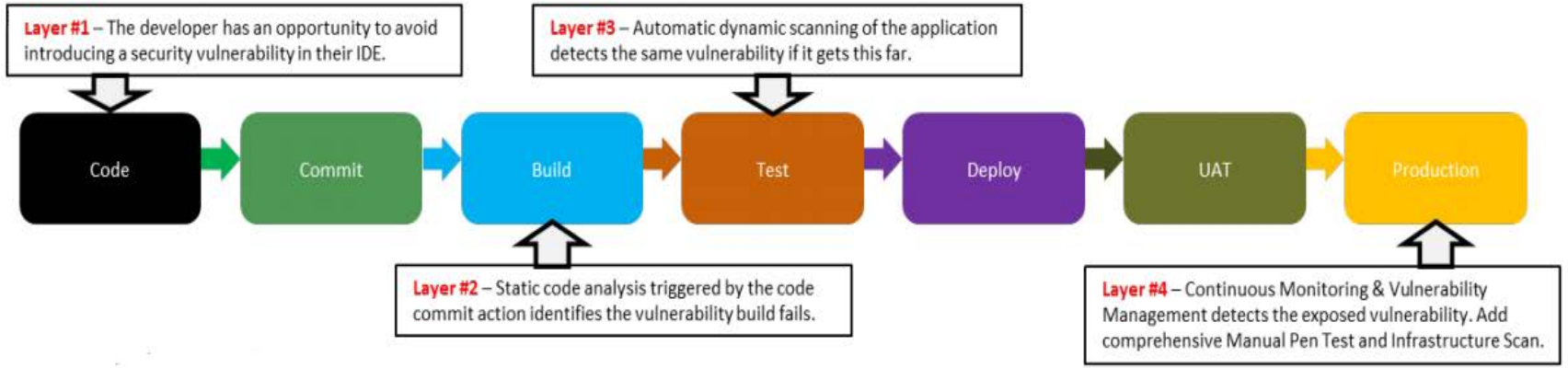

Qualys.

# Security integration in CI/CD methodology

Continuous Integration (CI), a set of processes defined as a part of a pipeline called 'Build Pipeline'.

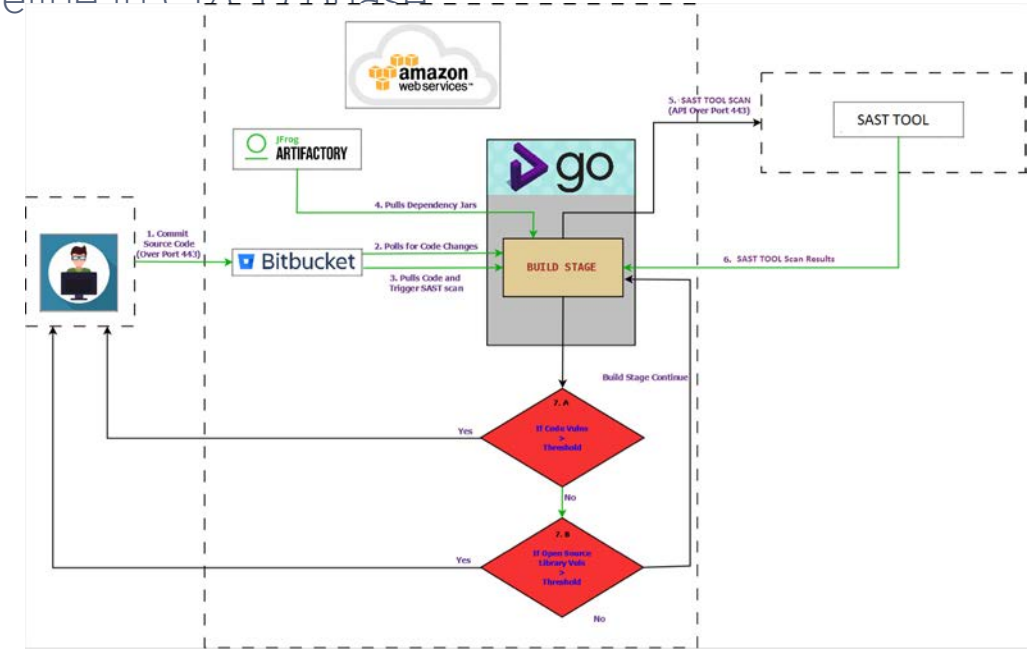
Continuous Delivery (CD), an extension of Continuous Integration (CI) that ensures new releases are to be delivered in a sustainable way.

Organizations can bring security into CI/CD by integrating various security tools to the existing pipeline.



# SAST (Static Application Security Testing)

SAST process analyzes source code to find security vulnerabilities in the application before the code is compiled. SAST can be automated and integrated to the build pipeline in CI/CD phase



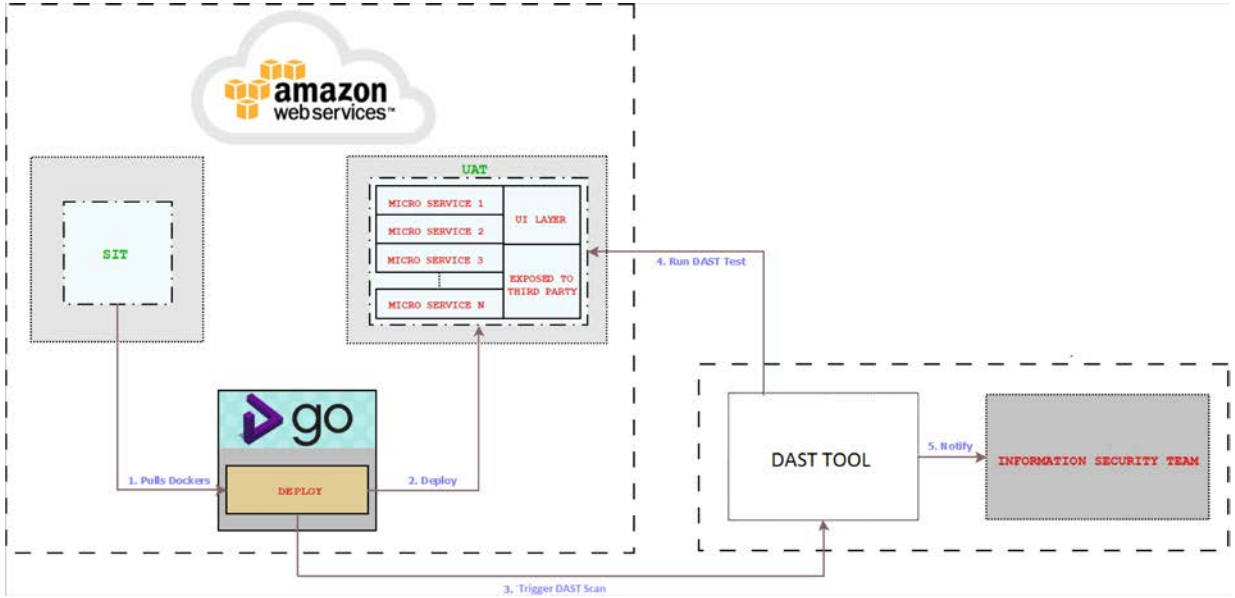



Qualys.

# DAST (Dynamic Application Security Testing)

DAST helps you to identify the vulnerabilities when the application is running and is accessible to the tester as a normal application user.

Grey Box methodology can be used here where the tester has access to application with valid user credentials and test coverage can be ensured for all the pages.

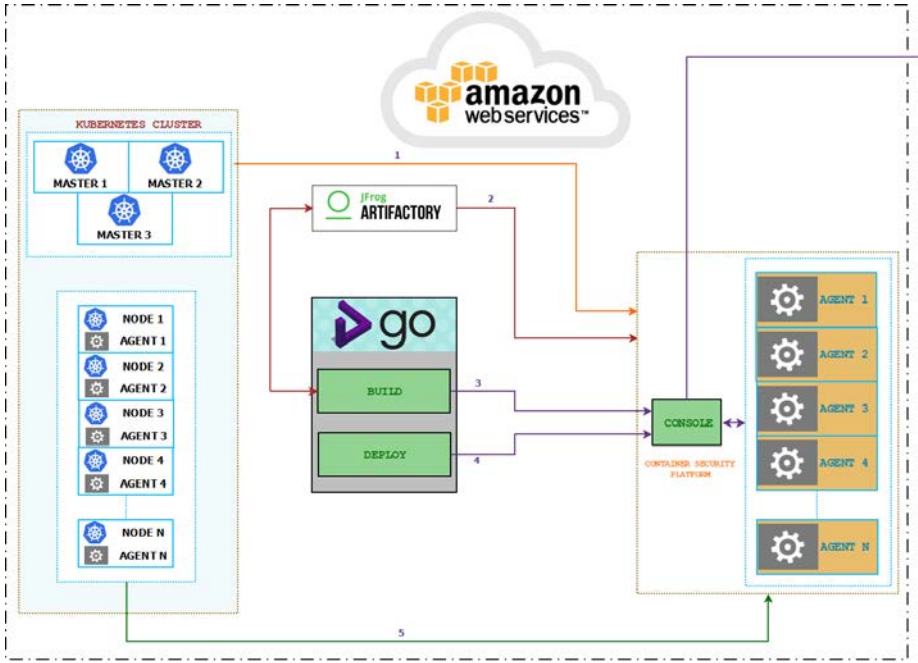





Qualys.

# Container Security Scanning

Container environment is dynamic and multiple containers spun up and down in various phases of the software release lifecycle in an automated way. The lifetime of a container may vary from few seconds to days.




1. Orchestrating Environment Hardening
2. Artifactory Scanning for Base Images
3. Enforcing Builds Restriction
4. Enforcing Restriction on Deploying Vulnerable Image
5. Host Environment Hardening



Qualys.

# Challenges in Container Security

- Vulnerability Assessment
- Access Controls
- Secure Configuration and Hardenings
- Real-time visibility and control of the container runtime environment
- Auditing and Logging
- Secret Management



Qualys.

Qualys®

Continuous Security

# Thank You

Deepak Naik