Desarrollo de Código Seguro

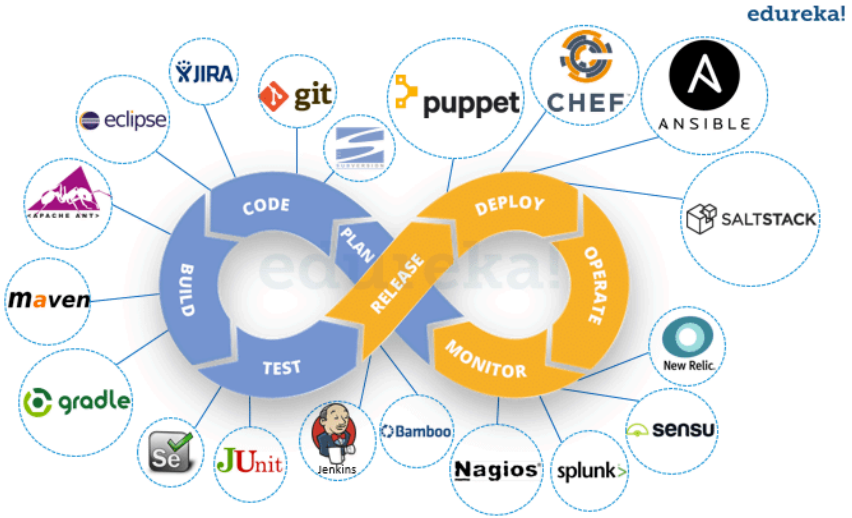
SecDevOps

viu | Universidad Internacional de Valencia

SecDevOps.

Ciclo de vida de un desarrollo de código seguro

- DevOps
- SecDevOps
- Fases del ciclo SecDevOps
- Herramientas



https://www.edureka.co/blog/devops-tutorial

DevOps

Pilares

- Colaboración
- Automatización
- Feedback continuo

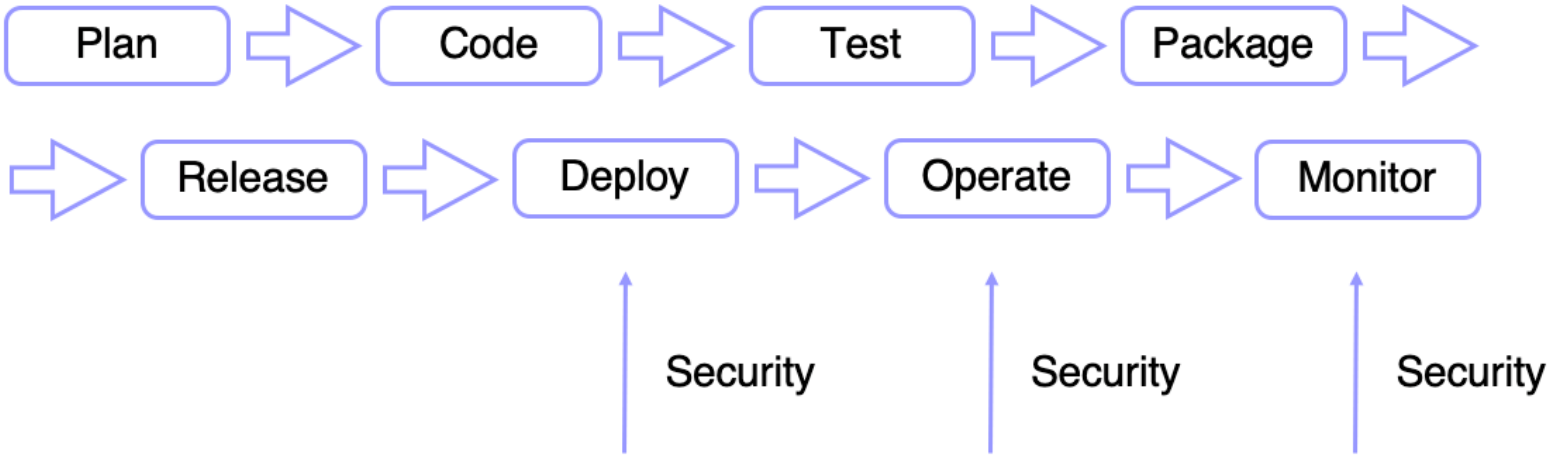
https://www.edureka.co/blog/devops-tutorial

DevOps

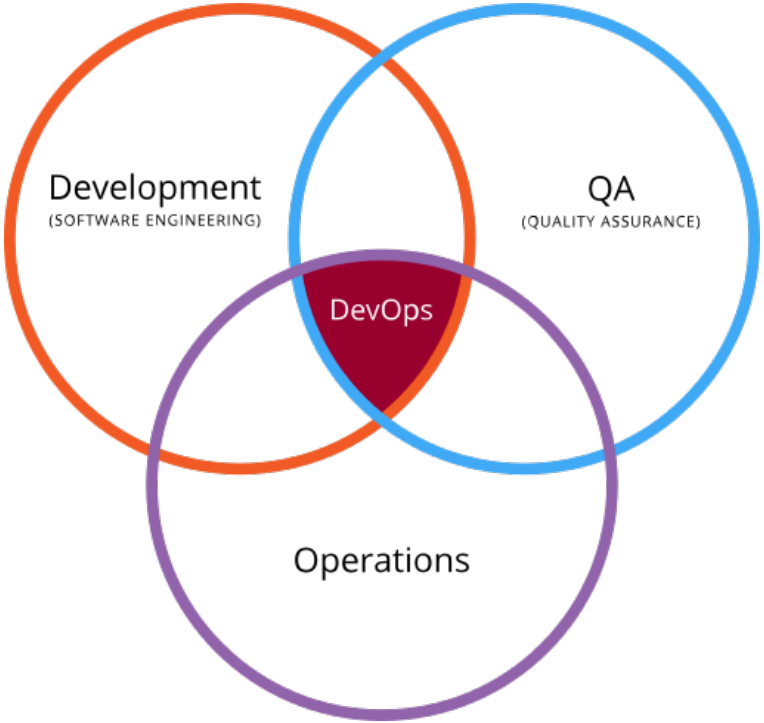
Tools

- Repositorios de código (Github, Gitlab, Bitbucket, etc)
- Infraestructura (Terraform, CloudFormation, etc)
- CI/CD (Jenkins, Bamboo, CircleCI, TravisCI, etc)
- Builds (Maven, Gradle, make, rake, etc)
- Test (*unit, cucumber, protractor, etc)
- Repositorio de artefactos (Nexus, Artifactory, Docker Hub, S3, etc)
- Despliegue (Ansible, Puppet, Chef, etc)
- Monitorización (NewRelic, AppDynamics, Sysdig, etc)
- Logging (Splunk, ELK, etc)
- Comunicación (Slack, HipChat, etc)

DevOps

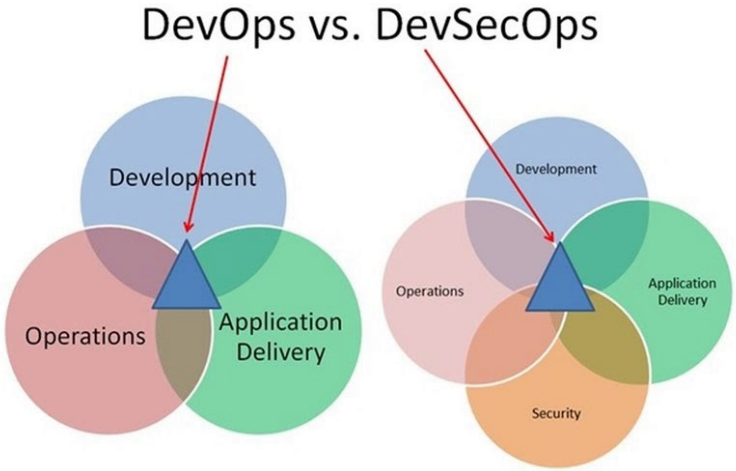

Plan
Code
Test
Package
Release
Deploy
Operate
Monitor
Security
Security
Security

DevOps

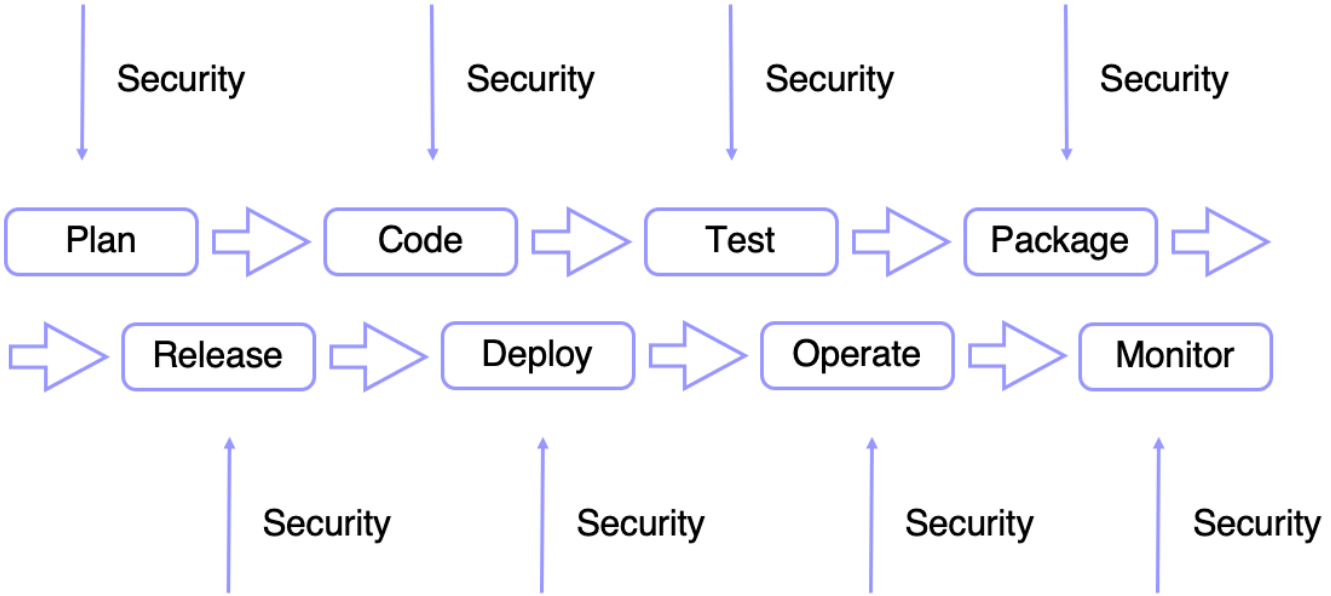


SecDevOps

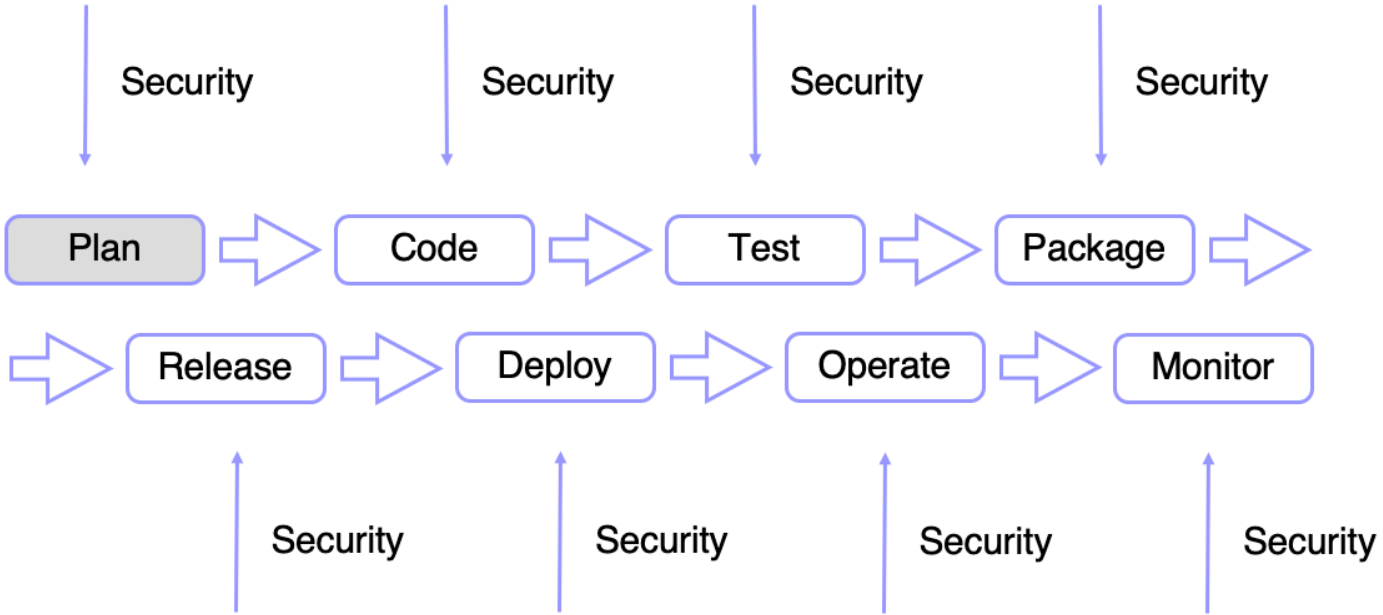
DevOps vs DevSecOps



SecDevOps



SecDevOps. Design/Plan

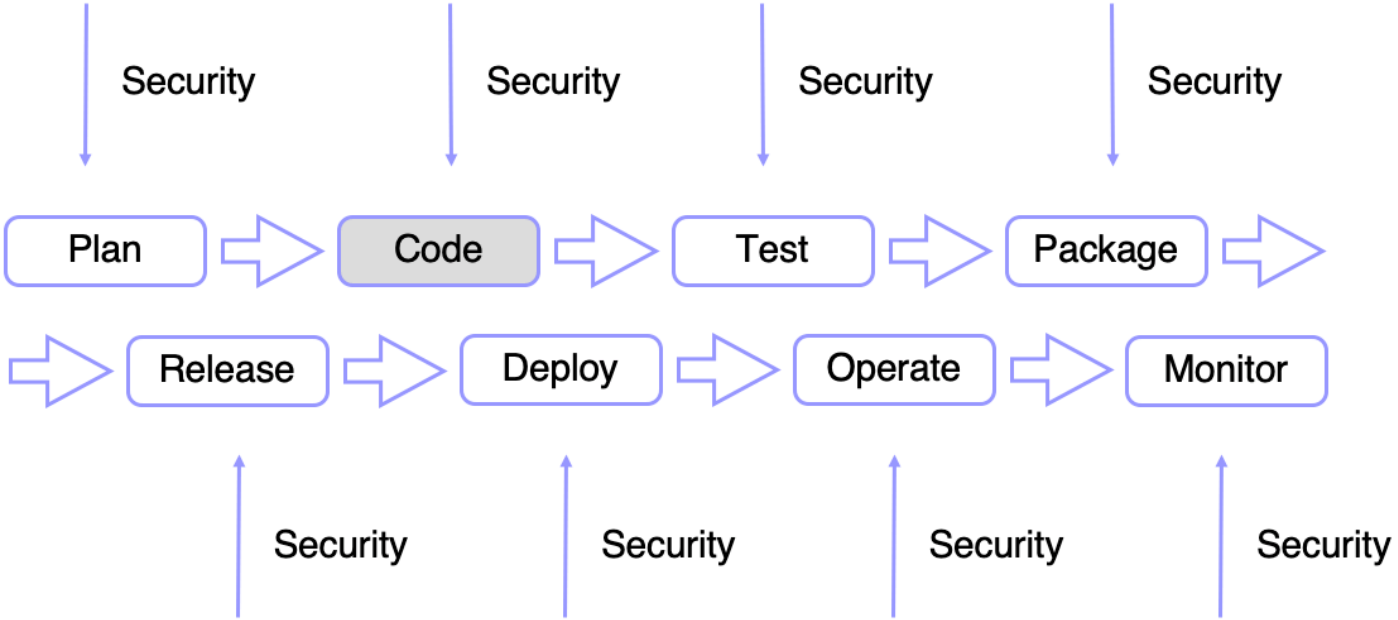


SecDevOps. Design/Plan (Threat Modeling)

GOTO Clase Anterior …

- OWASP Application Threat Modeling
  - https://www.owasp.org/index.php/Application_Threat_Modeling
- Don´t forget EVIL user stories
  - https://www.owasp.org/index.php/Agile_Software_Development:_Don't_Forget_EVIL_User_Stories
- OWASP Security Verification Standard
  - https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
- Mozilla Rapid Risk Assessment
  - https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment.html

SecDevOps. Code



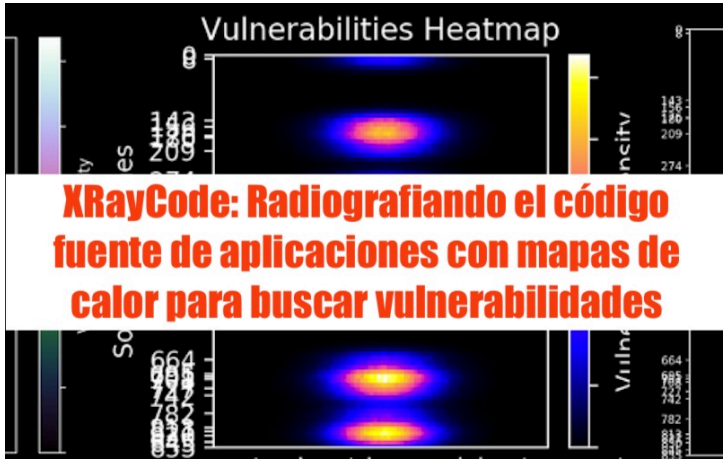
SecDevOps. Development / Code

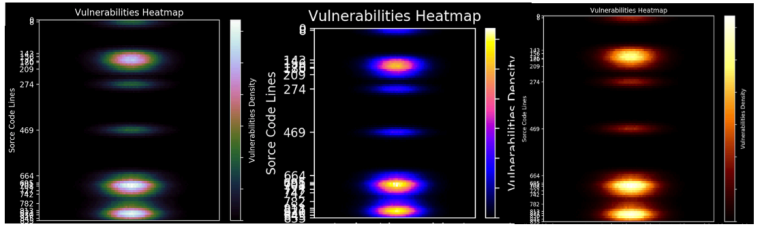
- git-secrets
- git-hound
- gofmt, yapf (Google), PMD, SonarQube, etc
- **SAST**
  - Brakeman (Ruby), SpotBugs+FindSecBugs (Java), Go AST (Go), Bandit (Python), etc
  - IDE Plugins

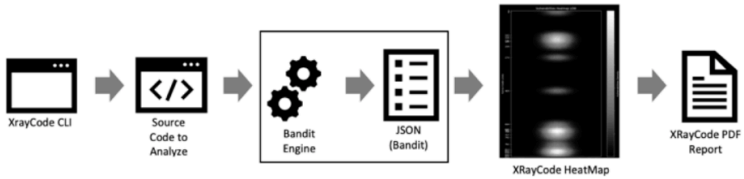
https://owasp.org/www-community/Source_Code_Analysis_Tools

SecDevOps. Development / Code

XRayCode





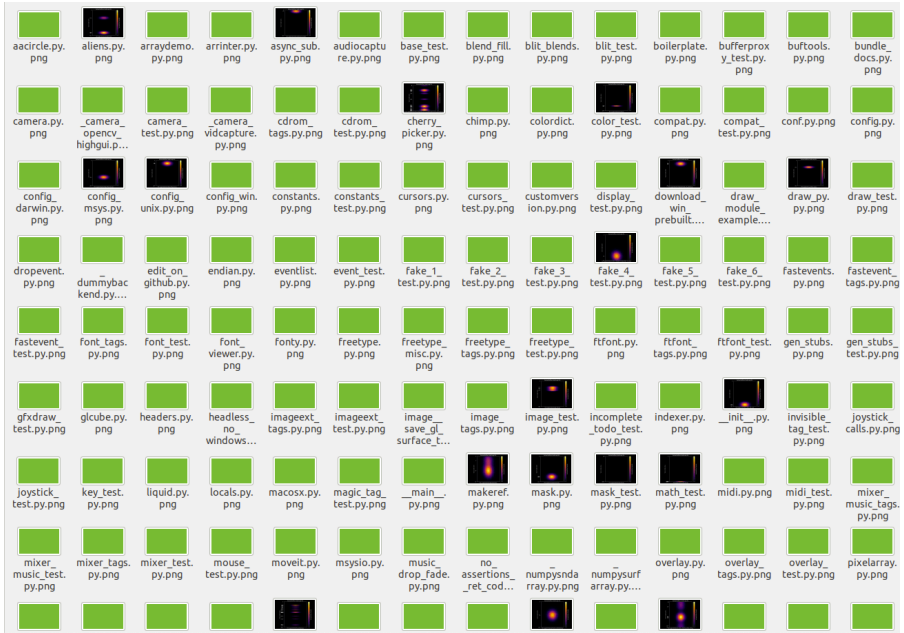


https://github.com/ElevenPaths/x-ray_code

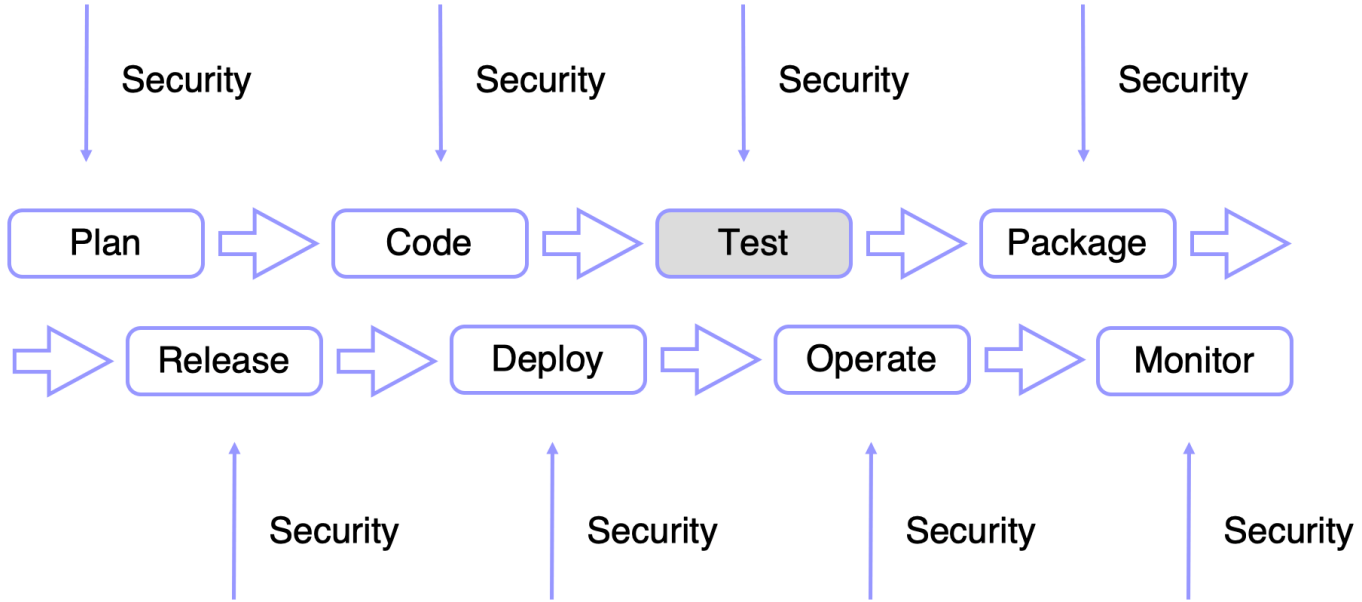
https://www.elladodelmal.com/2020/03/xraycode-radiografiando-el-codigo.html

SecDevOps. Development / Code

XRayCode



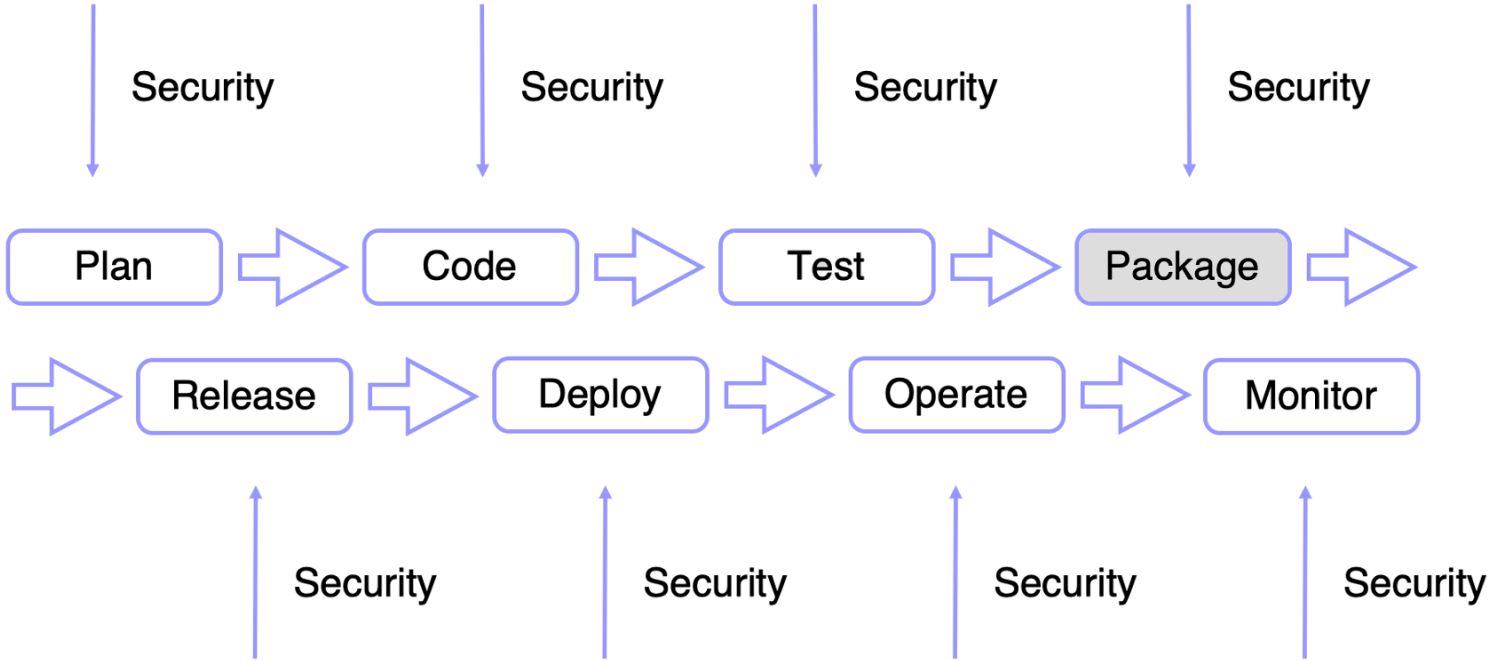
SecDevOps. Test



SecDevOps. Test

- Tests específicos de seguridad
- Testcontainers - https://www.testcontainers.org

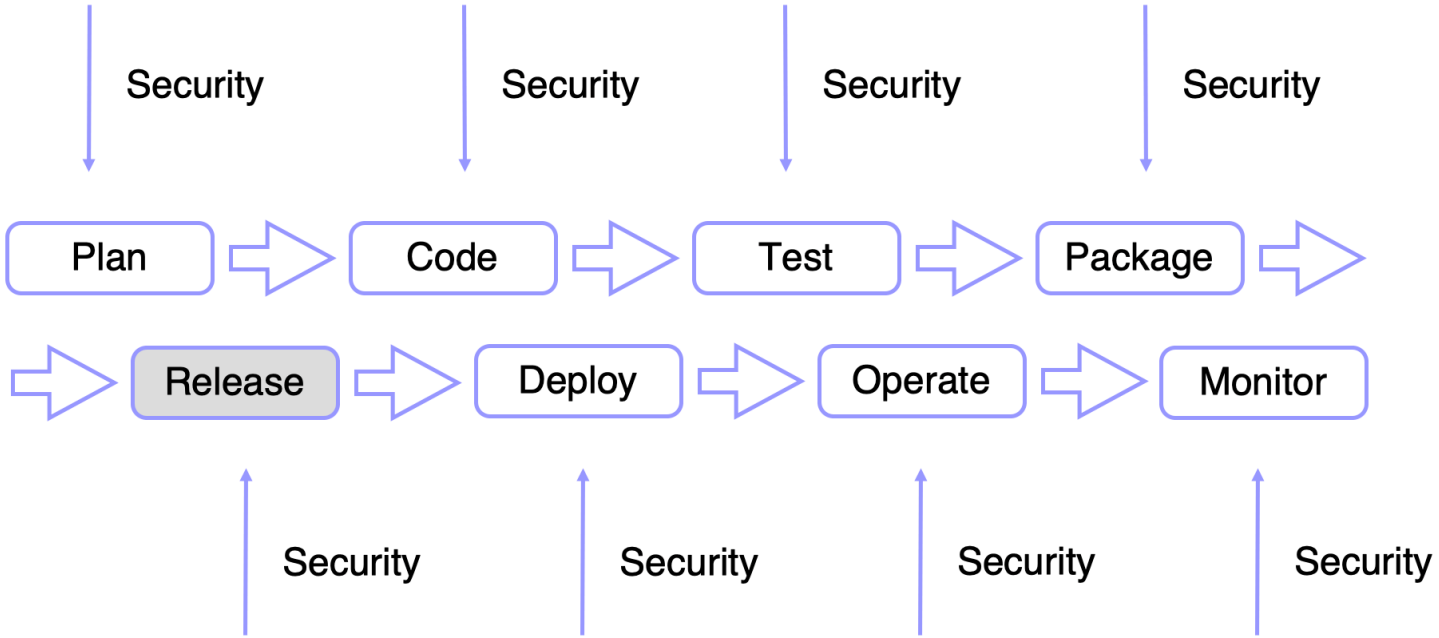
SecDevOps. Package



SecDevOps. Package

- bundler-audit (Ruby)
- OWASP Dependency Check (Java) – Retire.js
- nsp (node)
- Retire.js (JS)
- Contenedores Docker:
  - Docker Bench
  - Clair
  - Dagda
    - https://github.com/eliasgranderubio/dagda

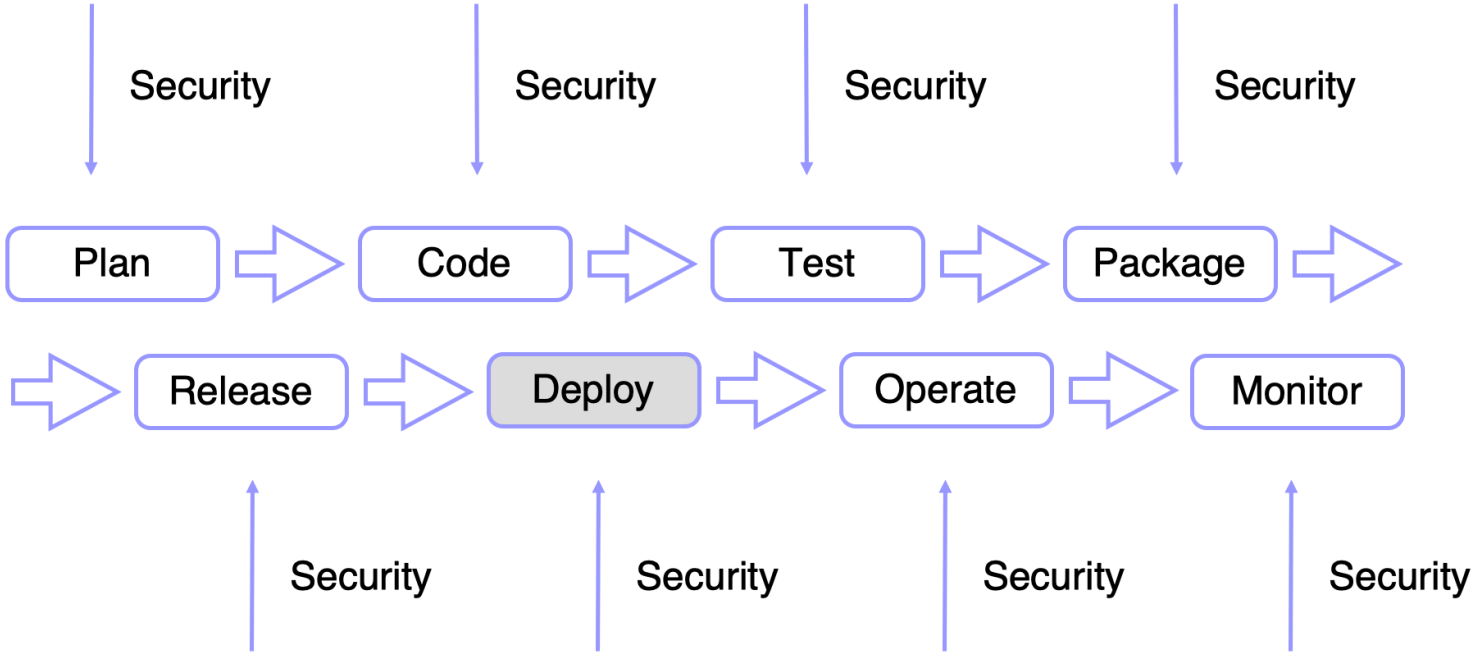
SecDevOps. Release



SecDevOps. Release

- Manejo de secretos
  - Vault
  - AWS Secret Management
  - Azure Key Vault
  - Secret Manager (GCP)

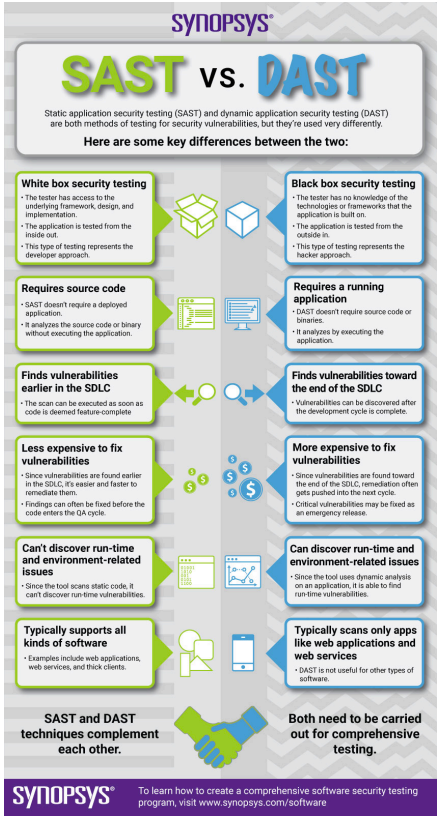
SecDevOps. Deploy



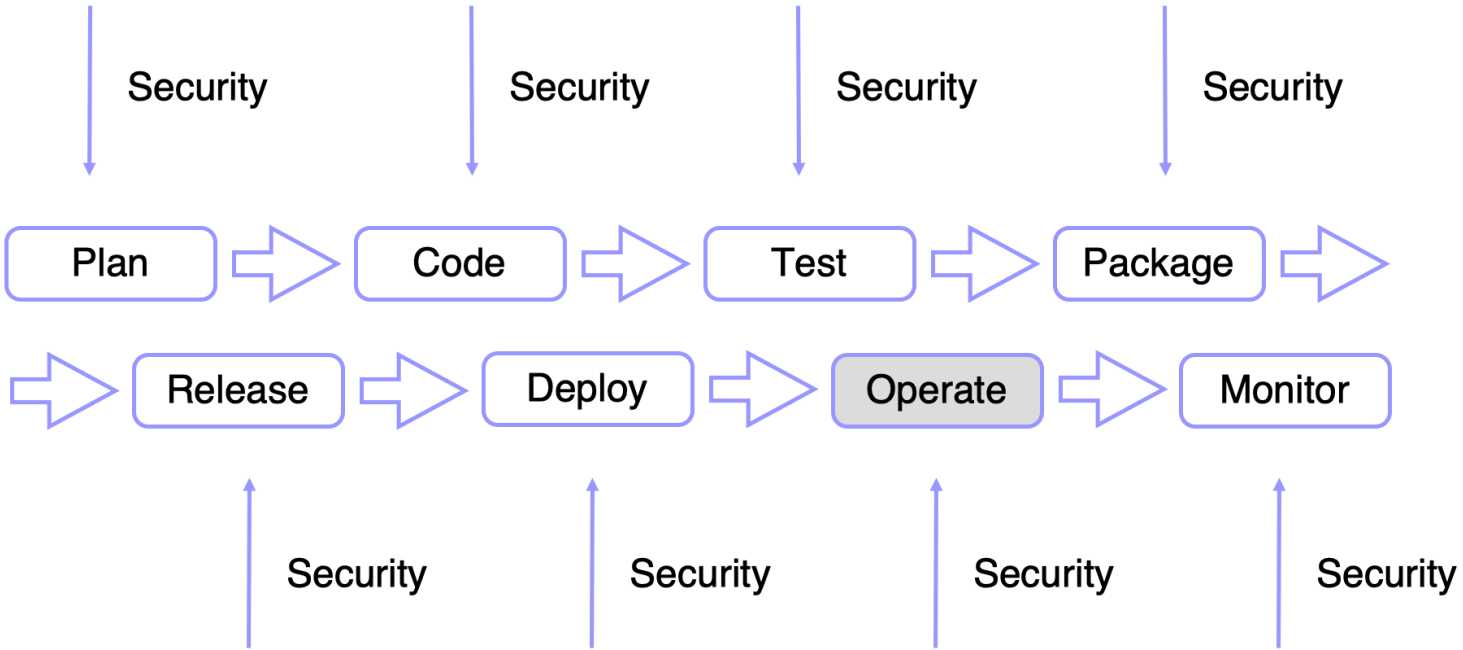
SecDevOps. Deploy

- DAST:
  - Nikto
  - ZAP
  - sqlmap
  - nmap
  - Arachni
  - Gauntlt (BDD style for automation)

SecDevOps. Deploy



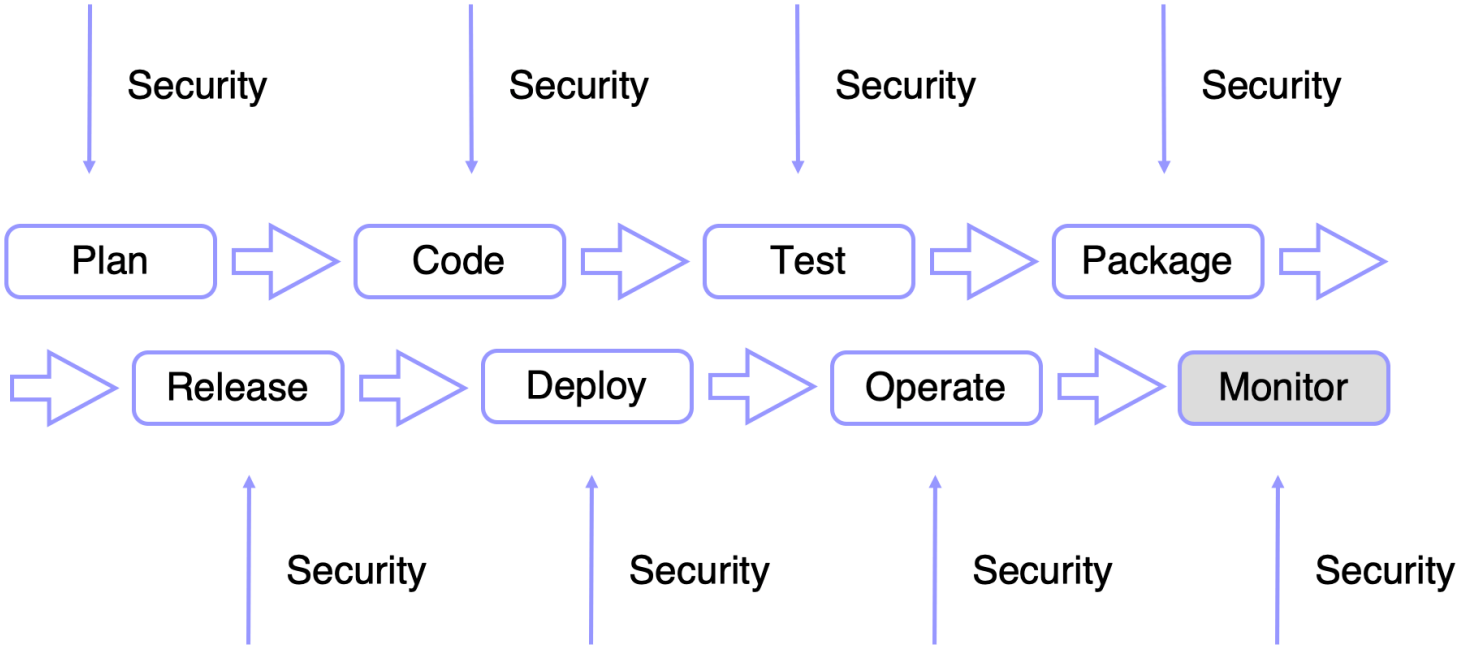
SecDevOps. Operate



SecDevOps. Operate

- Chaos Engineering
- Circuit Breaker
- Instrumentation (NewRelic, AppDynamics, Contrast, etc)
- Red Team
- Bug Bounties
- WAF

SecDevOps. Monitor



SecDevOps. Monitor

- Splunk
- ELK
- Datadog
- Pagerduty
- …

SecDevOps

OpsDevSec OpsSecDev

DevSecOps

… llámalo como quieras, pero pon siempre el "Sec" ;)

Gracias

viu | Universidad Internacional de Valencia