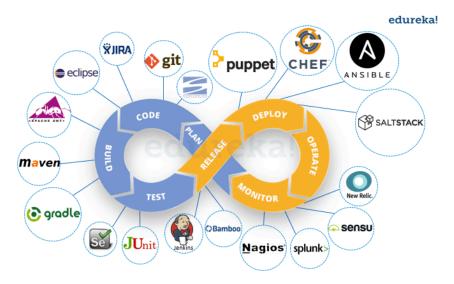
# Desarrollo de Código Seguro SecDevOps

#### 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

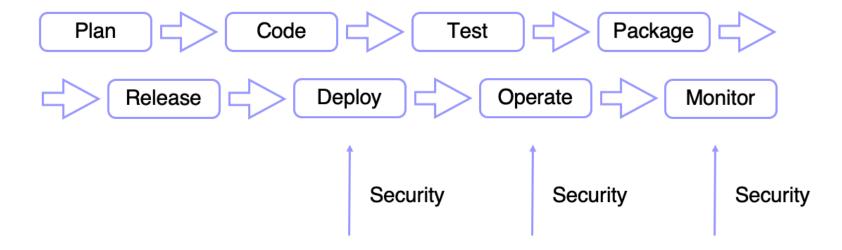


## DevOps

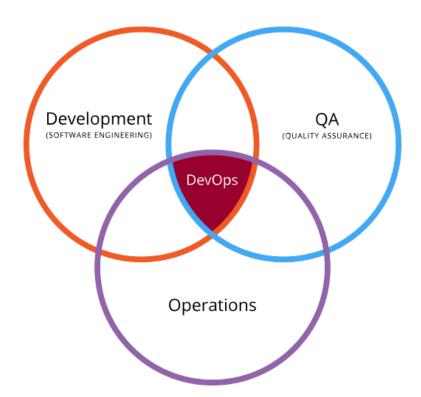


- Repositorios de código (Github, Gitlab, Bitbucket, etc)
- Infraestructura (Terraform, CloudFormation, etc)
- CI/CD (Jenkins, Bamboo, CircleCI, TravisCI, etc)
- Builds (Maven, Gradle, make, rake, etc)
- Test (\*unit, cucumber, protractor, etc)
- Repositorio de artefactos (Nexus, Artifactory, Docker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

## > DevOps

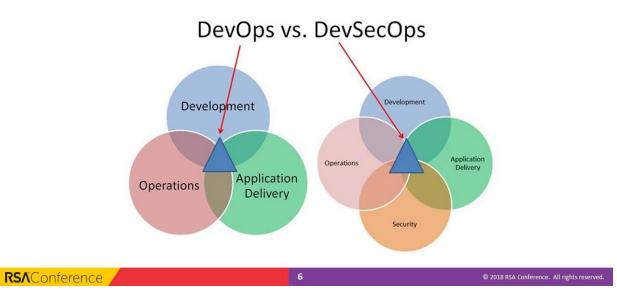


## > DevOps

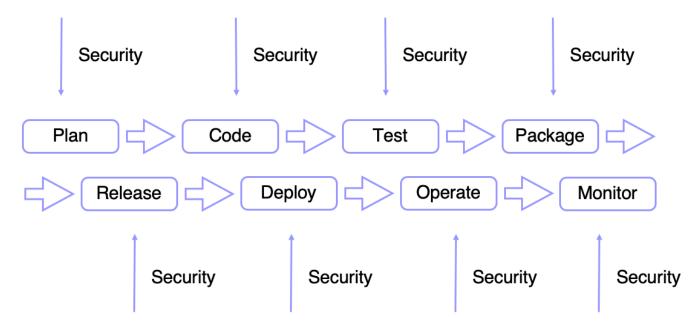


## > SecDevOps

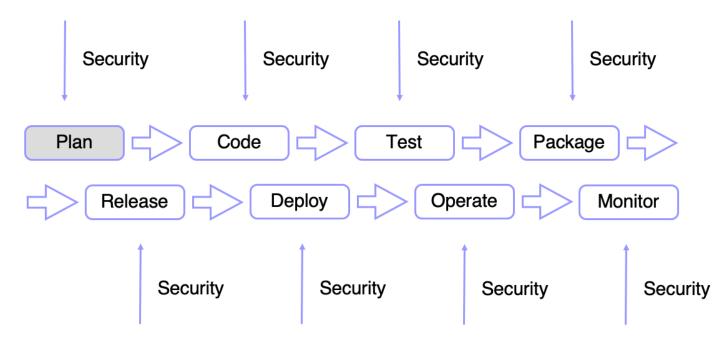
## DevOps vs DevSecOps



## > SecDevOps



## > SecDevOps. Design/Plan



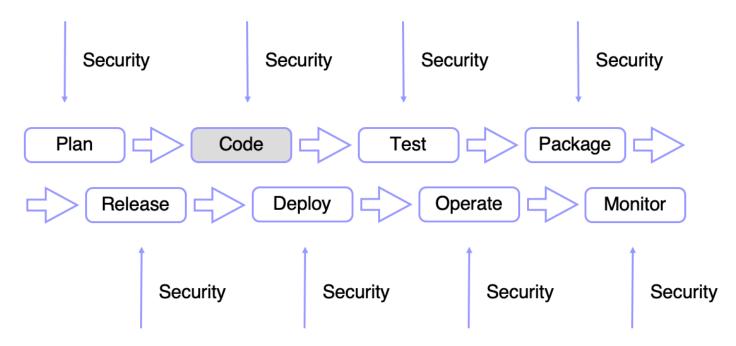
> SecDevOps. Design/Plan (Threat Modeling)

#### **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

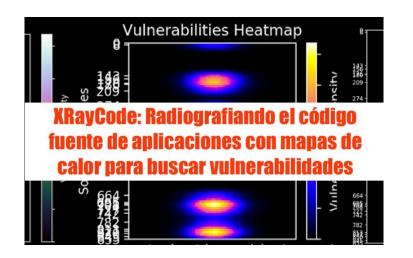
- git-secrets
- git-hound
- gofmt, yapf (Google), PMD, SonarQube, etc
- SAST
  - Brakeman (Ruby), SpotBugs+FindSecBugs (Java),
     Go AST (Go), Bandit (Python), etc
  - IDE Plugins

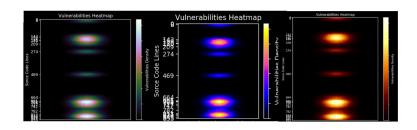
https://owasp.org/www-community/Source Code Analysis Tools

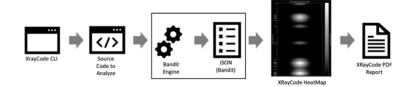


## > SecDevOps. Development / Code

#### **XRayCode**







https://github.com/ElevenPaths/x-ray\_code

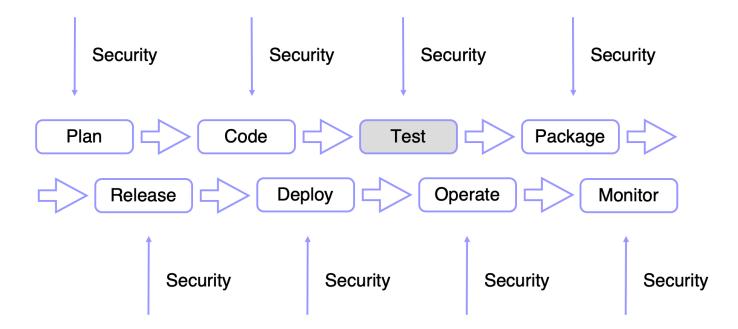
https://www.elladodelmal.com/2020/03/xraycode-radiografiando-el-codigo.html

## > SecDevOps. Development / Code

### XRayCode

aacircle.py.	aliens.py.	arraydemo. py.png	arrinter.py.	async_sub. py.png	audiocaptu re.py.png	base_test. py.png	blend_fill. py.png	blit_blends.	blit_test. py.png	boilerplate. py.png	bufferprox y_test.py. png	buftools. py.png	bundle_ docs.py. png
camera.py.	_camera_ opencv_ highgui.p	camera_ test.py.png	_camera_ vidcapture. py.png	cdrom_ tags.py.png	cdrom_ test.py.png	cherry_ picker.py. png	chimp.py.	colordict. py.png	color_test. py.png	compat.py.	compat_ test.py.png	conf.py.png	config.py.
config_ darwin.py. png	config_ msys.py. png	config_ unix.py.png	config_win. py.png	constants. py.png	constants_ test.py.png	cursors.py.	cursors_ test.py.png	customvers ion.py.png	display_ test.py.png	download_ win_ prebuilt	draw_ module_ example	draw_py. py.png	draw_test. py.png
dropevent. py.png	dummybac kend.py	edit_on_ github.py. png	endian.py.	eventlist. py.png	event_test. py.png	fake_1_ test.py.png	fake_2_ test.py.png	fake_3_ test.py.png	fake_4_ test.py.png	fake_5_ test.py.png	fake_6_ test.py.png	fastevents. py.png	fastevent_ tags.py.png
Fastevent_ test.py.png	font_tags. py.png	font_test. py.png	font_ viewer.py. png	fonty.py.	freetype. py.png	freetype_ misc.py. png	freetype_ tags.py.png	freetype_ test.py.png	ftfont.py.	ftfont_ tags.py.png	ftfont_test. py.png	gen_stubs. py.png	gen_stubs_ test.py.png
gfxdraw_ test.py.png	glcube.py. png	headers.py.	headless_ no_ windows	imageext_ tags.py.png	imageext_ test.py.png	image save_gl_ surface_t	image_ tags.py.png	image_test. py.png	incomplete _todo_test. _py.png	indexer.py.	initpy. _png	invisible_ tag_test. py.png	joystick_ calls.py.png
joystick_ test.py.png	key_test. py.png	liquid.py.	locals.py.	macosx.py. png	magic_tag_ test.py.png	main py.png	makeref. py.png	mask.py. png	mask_test. py.png	math_test. py.png	midi.py.png	midi_test. py.png	mixer_ music_tags. py.png
mixer_ music_test. py.png	mixer_tags. py.png	mixer_test. py.png	mouse_ test.py.png	moveit.py.	msysio.py. png	music_ drop_fade. py.png	no_ assertions_ _ret_cod	numpysnda rray.py.png	numpysurf array.py	overlay.py.	overlay_ tags.py.png	overlay_ test.py.png	pixelarray. py.png

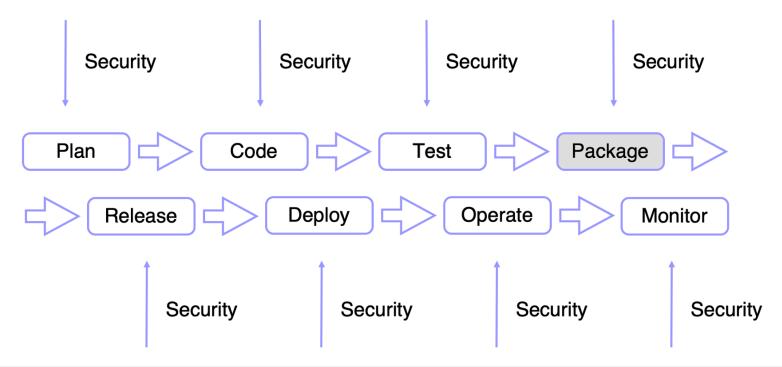
## > SecDevOps. Test



## > SecDevOps. Test

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

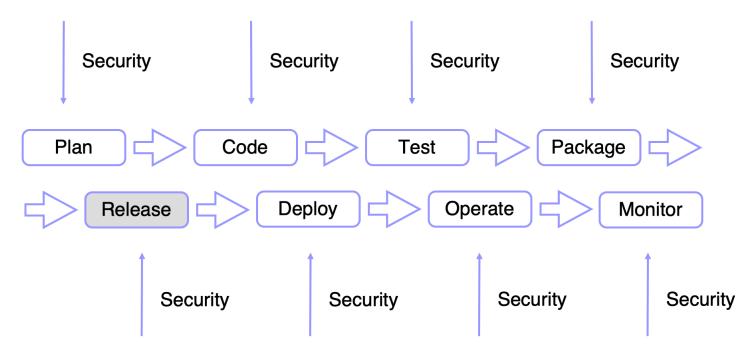
## > SecDevOps. Package



## > SecDevOps. Package

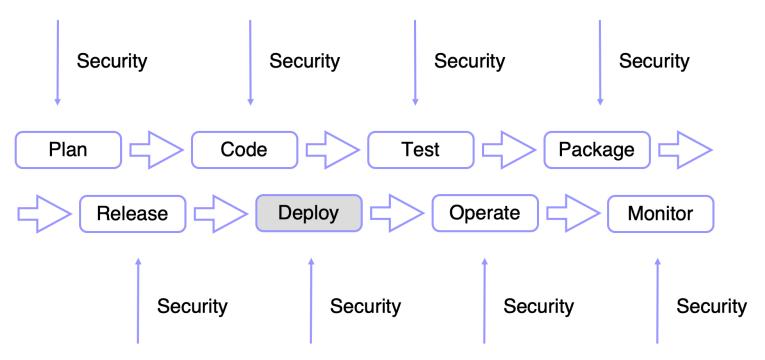
- bundler-audit (Ruby)
- OWASP Dependency Check (Java) Retire.js
- nsp (node)
- Retire.js (JS)
- Contenedores Docker:
  - Docker Bench
  - Clair
  - Dagda
    - https://github.com/eliasgranderubio/dagda

## > SecDevOps. Release



- > SecDevOps. Release
  - Manejo de secretos
    - Vault
    - AWS Secret Management
    - Azure Key Vault
    - Secret Manager (GCP)

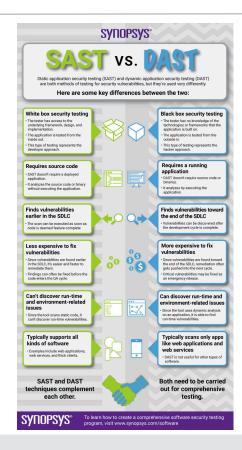
## > SecDevOps. Deploy



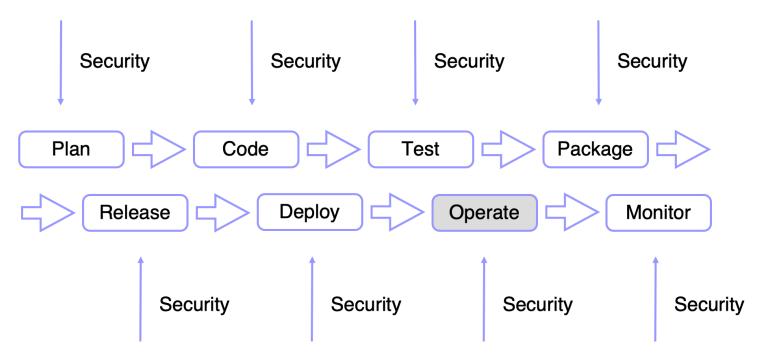
## > SecDevOps. Deploy

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

> SecDevOps. Deploy



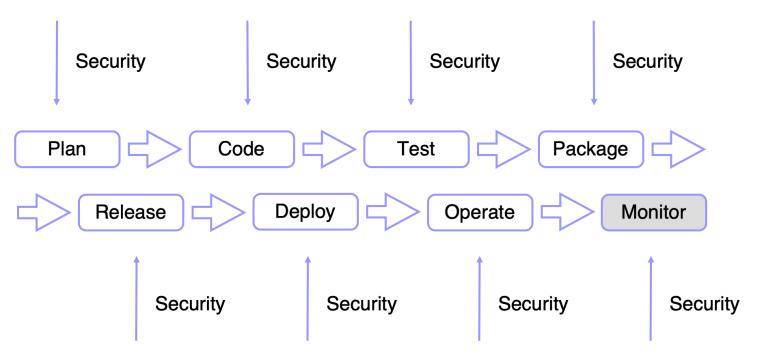
## > SecDevOps. Operate



## > 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