



códigofacilito



# Seguridad en DevOps

Fernando Garcia





# Conceptos (Application Security Testing)



SAST  
DAST  
IAST



# ☰ Static Application Security Testing (SAST)

## >\_ Análisis de código

Detección de bugs

Detección de Vulnerabilidades

Análisis de calidad de código



# 📋 Dynamic Application Security Testing (DAST)

## > Runtime Testing

Detección de bugs

Simulación de ataques (SQL injection, XSS)





## Ventajas

> Integración con CI/CD

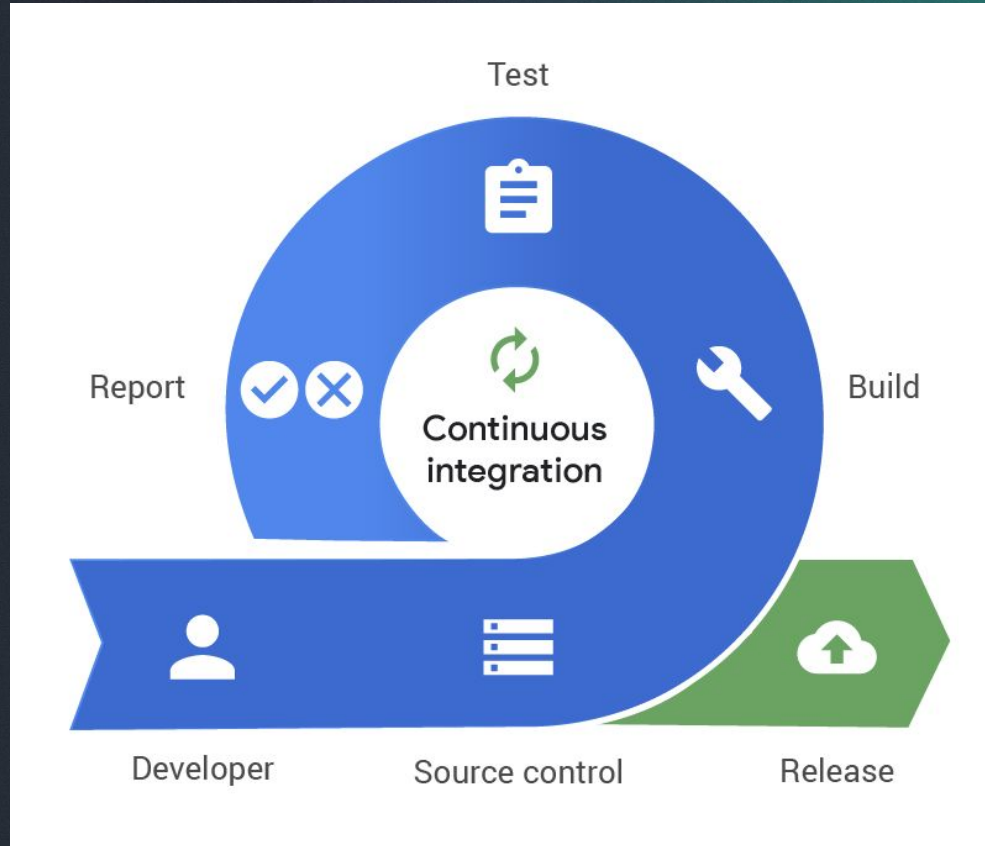
Automatización Code Review


















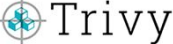



















Policy Enforcement

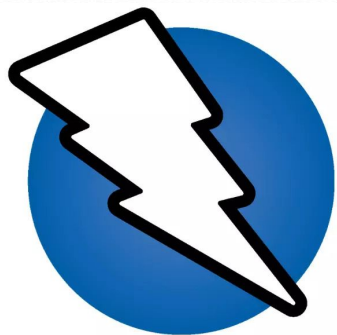
Feedback Loop



# Integración continua

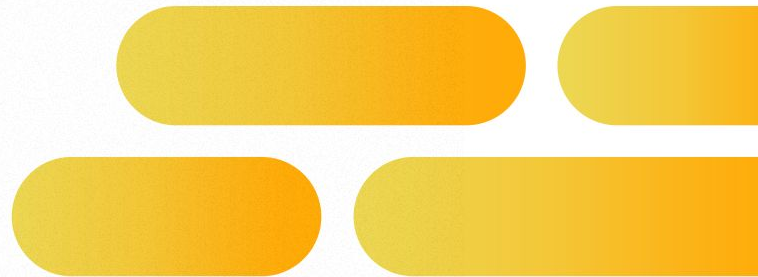


Issue Management	Source Code & DevSecOps Management	Security Scanning & Unit Testing	Continuous Integration & Build	Infrastructure as Code & Configuration Management	508 Compliance & Other Testing	Containerization & Continuous Deployment	Continuous Monitoring & Alerts
 GH Project Planner	 GitHub	 sonarqube	 Jenkins	 HashiCorp Terraform	 Selenium	 Jenkins	 Nessus vulnerability scanner
 Jira Software	 Federal GovCloud DevSecOps	 DEPENDENCY-CHECK	 Maven	 ANSIBLE	 Pa11y	 kubernetes	 WhiteSource
 ZenHub Enterprise		 Trivy	 MS Build		 Microsoft Cloud Security Center		
 Azure Boards		 sonarlint	 Sequelize		 SendGrid	 docker	 splunk
		 JUnit 5	 redgate			 GH Actions	
		 GH Advanced Security	 docker			 Azure DevOps	
		 JFrog ARTIFACTORY EDGE	 GH Actions				
		 Nessus vulnerability scanner	 JFrog XRAY				
			 Azure DevOps				



**OWASP ZAP**

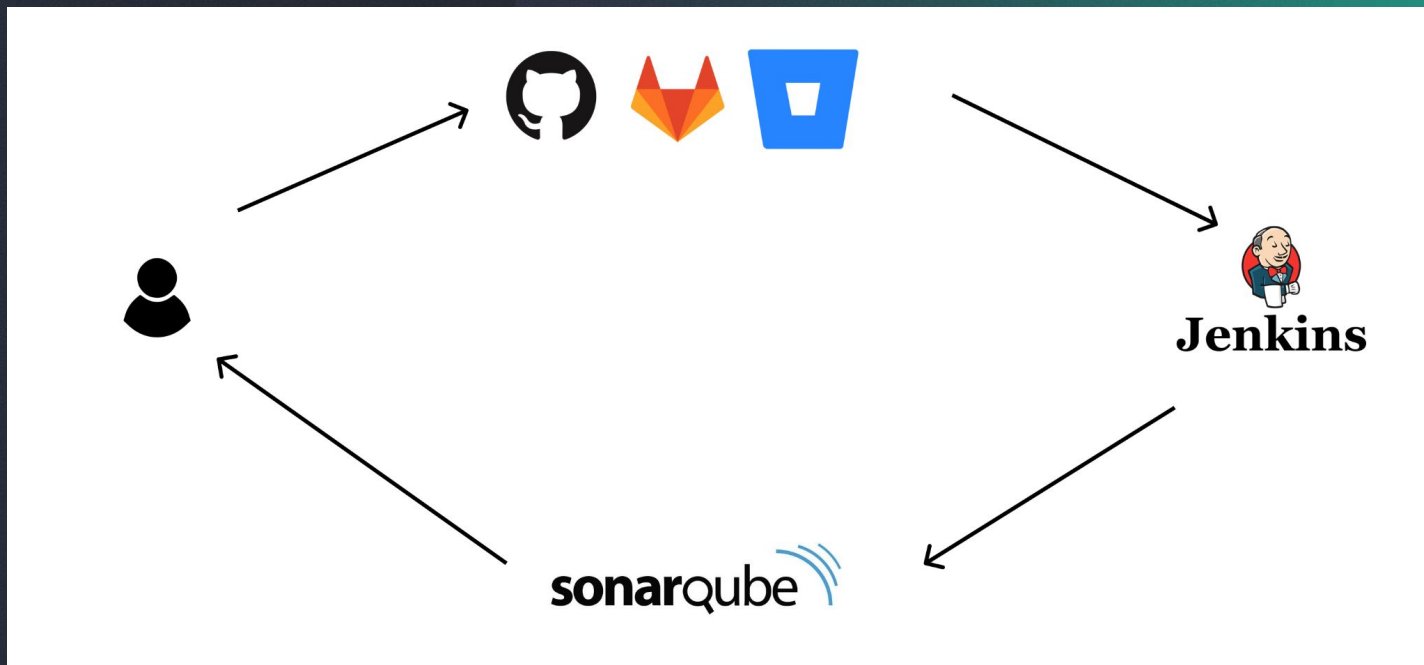
**sonarqube** 





# ☰ ¿Cómo funciona ?

>\_



.....  
.....  
.....  
.....

## Características principales de SonarQube:

- >\_ Soporte Multilenguaje (29 lenguajes)
- Integración con CI/CD
- Plataforma web
- Reglas de Calidad y Seguridad



# ☰ Instalación

>\_ Instalación con Java

Docker :)

