Escaneo de vulnerabilidades

Enrique Cuevas

Prácticas modernas para crear software con calidad y sabor

#SGVirtual

About me

- Ingeniero en Computación
- Staff Site Reliability Engineer @ Wizeline
- Cloud - Devops - Agile
- Hobbies: Outdoors🏔️ , music🎵, MTB🚵, RPis, woodworking🪵
- Don’t like politics 🙅🏽‍♂️

@rastangineer

Agenda

- What is vulnerabilities scanning?
- What are we going to do?
- Workshop
- Q&A

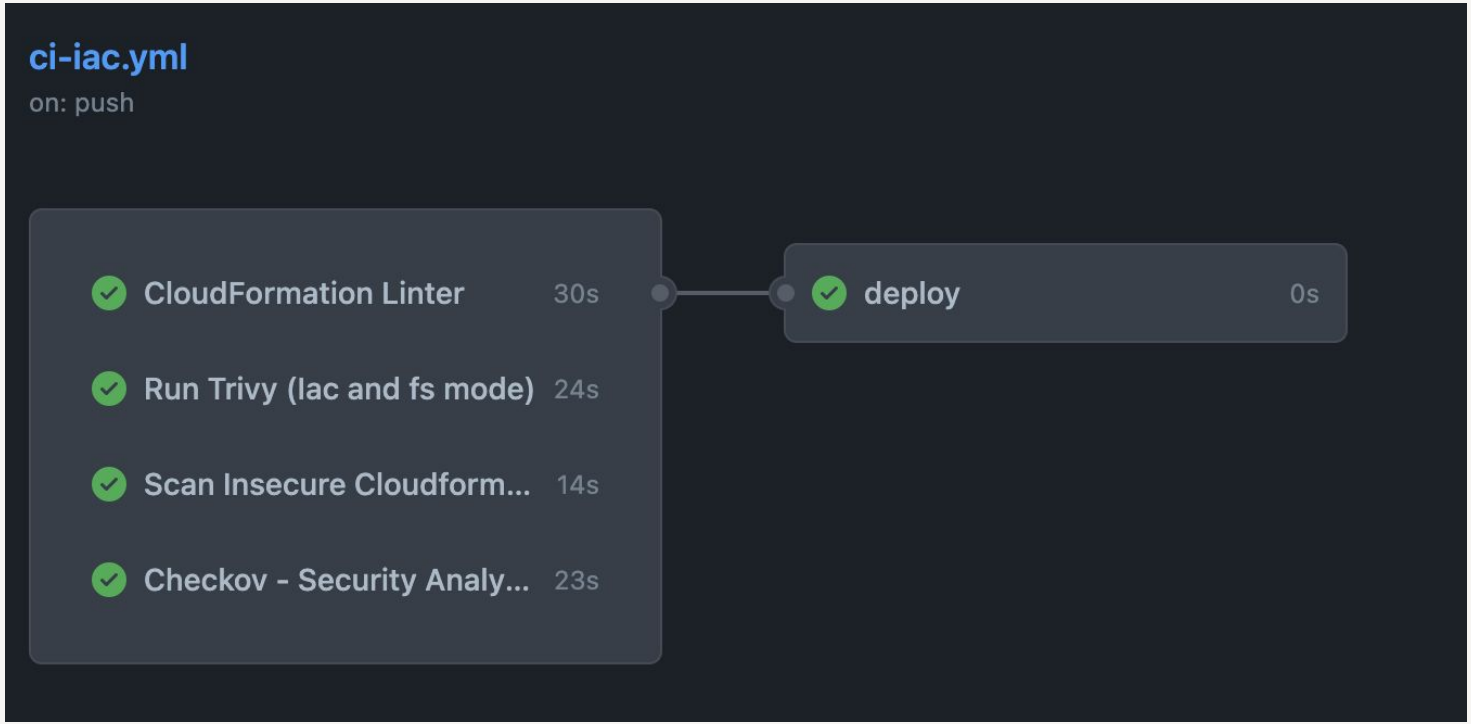
What is vulnerabilities scanning?

- It’s an **analysis** that compares the code to a predefined set of rules to identify **potential** security issues.

- Tries to **avoid injecting** security issues on our repositories

- Also known as Static Application Security Testing (SAST) Tools, can help analyze source code or compiled versions of code to help find security flaws

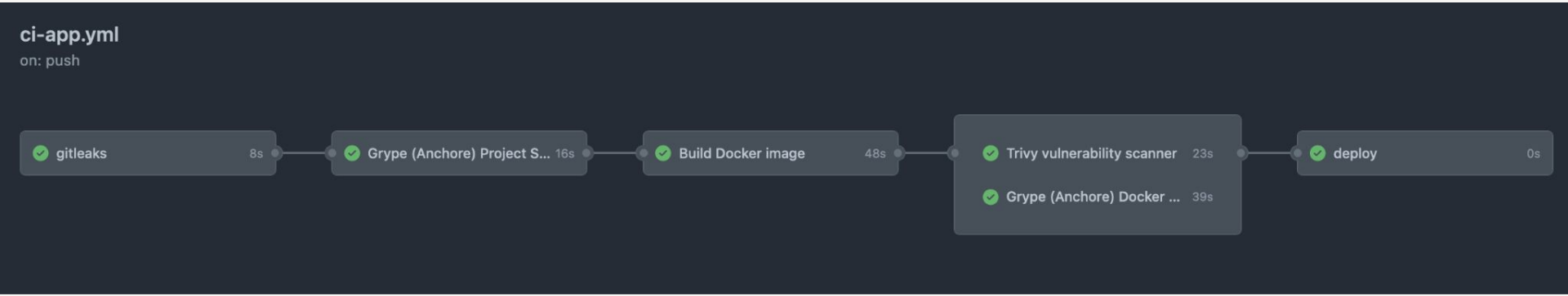
CI Pipeline for Infra as Code



What are we going to do?

- Infra as code
  - stelligent/cfn_nag looks for patterns in CloudFormation templates that may indicate insecure infrastructure.
  - bridgecrewio/checkov-action performs static security analysis of Terraform & CloudFormation Infrastructure code
- Application Code
  - gitleaks
  - Grype (Anchore) Project and Docker Scan
  - Pycharm-security
  - Trivy Vulnerability Scanning

CI Pipeline for App



Workshop time!

- bit.ly/escaneo-vulnerabilidades-sg2023

What is next?

- Pre-commits, scan before commit

¡Gracias!

¿Preguntas?

Contacto:

@rastangineer