Dec, 2019

Performing Security Tests Inside Your CI

Rafael dos Santos 🇧🇷 @rafasantos5

huskyCI

github.com/globocom/huskyCI

$ whoami

Rafael dos Santos 🇧🇷 @rafasantos5

github.com/rafaveira3

⚽ Flamengo Fan

☕ OSCP + OSCE

🐼 Security Engineer @ globo.com

🚀 Security Tools

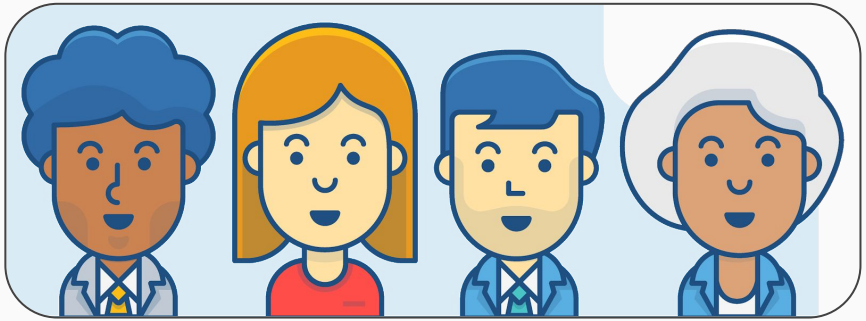
huskyCI

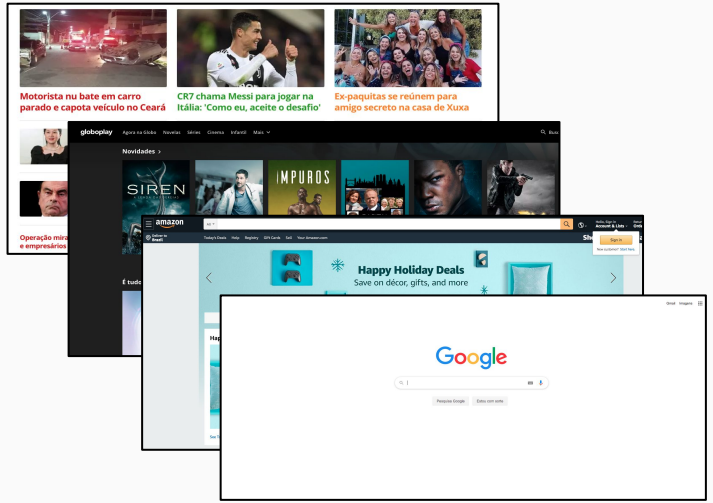
github.com/globocom/huskyCI

A day in the life of a…
development team

A day in the life of a… DEV team

huskyCI
github.com/globocom/huskyCI

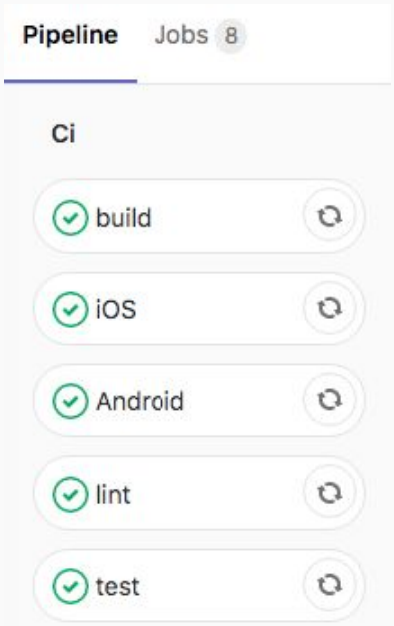


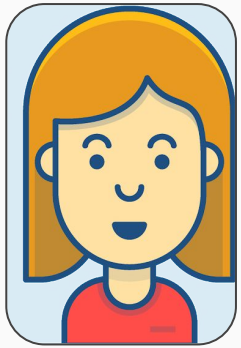


A day in the life of a… DEV team

huskyCI
github.com/globocom/huskyCI

"Awesome feature!!!!"





"Sounds good to me!"

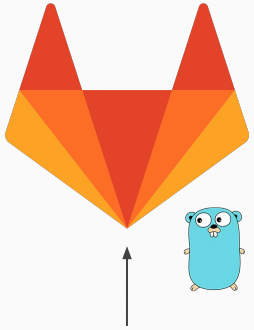
huskyCI

github.com/globocom/huskyCI

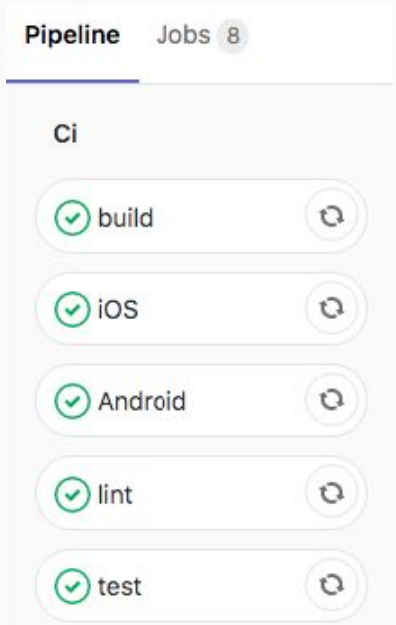
Security Team?

A day in the life of a… DEV team

huskyCI
github.com/globocom/huskyCI

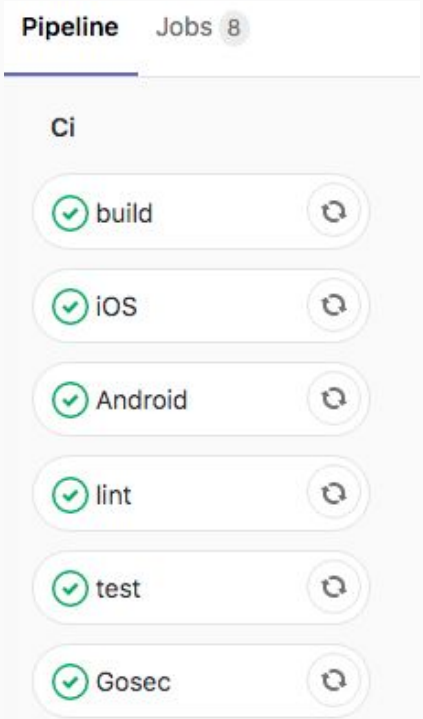


"Awesome feature!!!!"



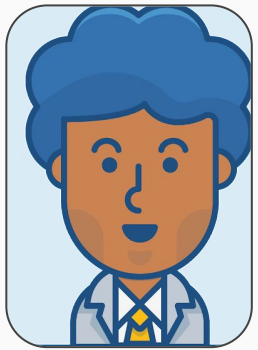
Security Team

"Hey, what about using **Gosec**?"

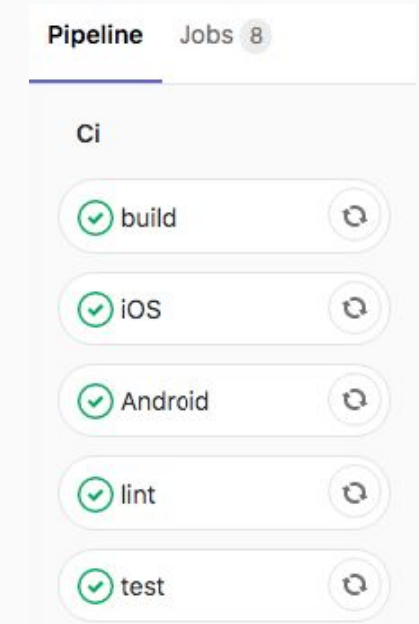


A day in the life of a… DEV team

huskyCI
github.com/globocom/huskyCI

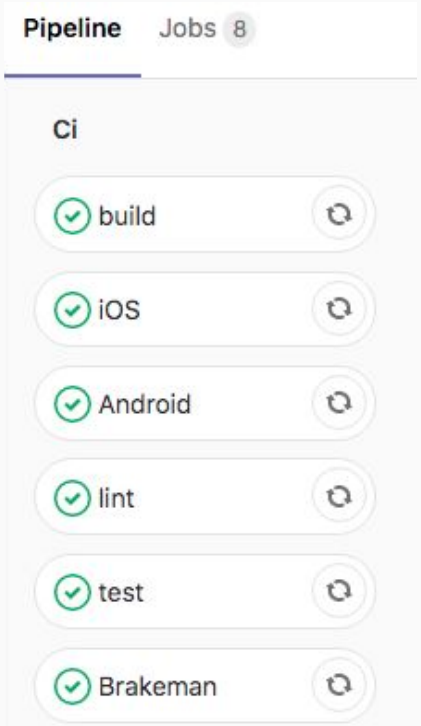


"Awesome feature!!!!"



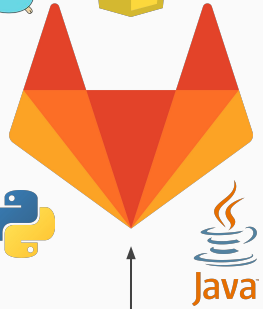
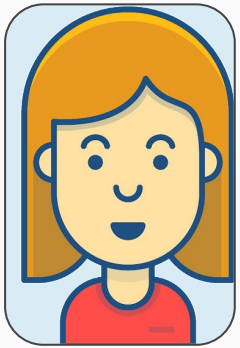
Security Team

"Hey, what about using **Brakeman**?"

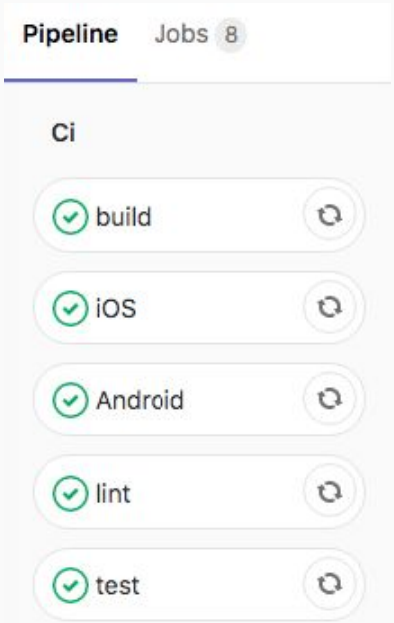


A day in the life of a… DEV team

huskyCI
github.com/globocom/huskyCI

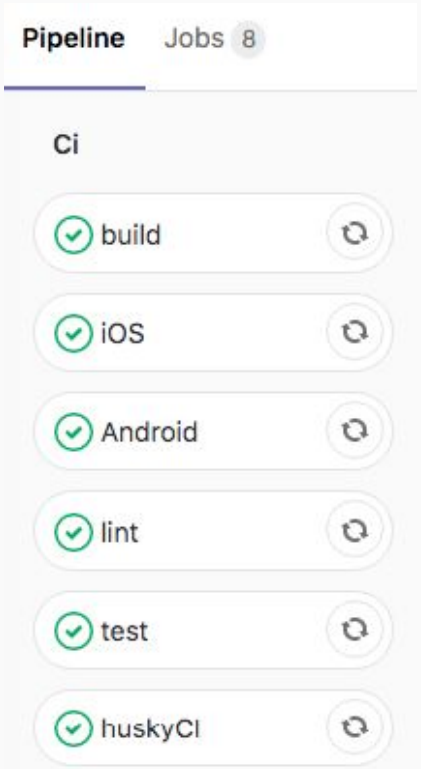



"Awesome feature!!!!"



Security Team

"Hey, what about using … ?"



huskyCI

github.com/globocom/huskyCI

huskyCI

github.com/globocom/huskyCI

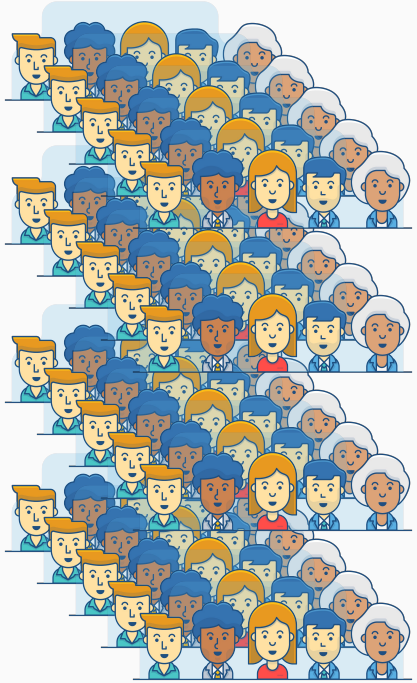
A day in the life of a…
big organization

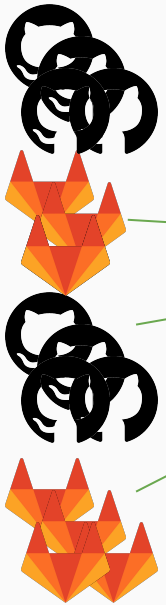
A day in the life of a… BIG organization

huskyCI

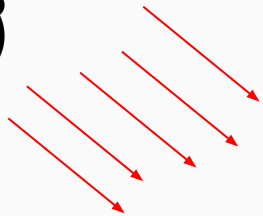
github.com/globocom/huskyCI

Development Team





Security Team



tsuru

huskyCI

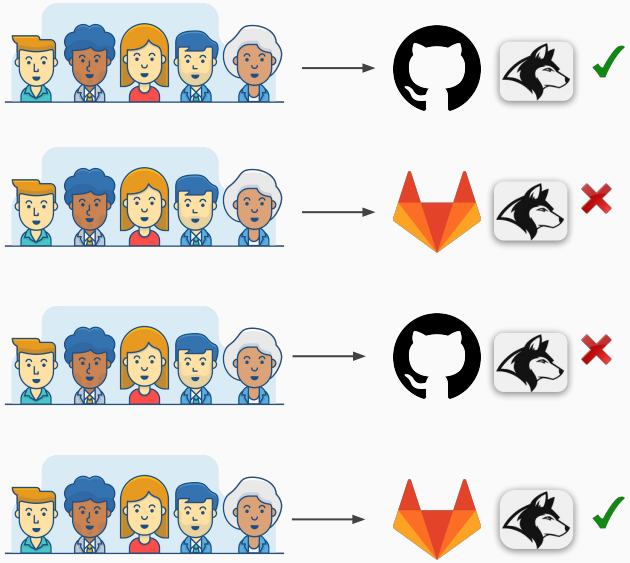
github.com/globocom/huskyCI

Let's hack!

huskyCI

github.com/globocom/huskyCI

Development Team



Security Team

Ok, what are we coding?

huskyCI
github.com/globocom/huskyCI









Ok, what are we coding?

huskyCI
github.com/globocom/huskyCI

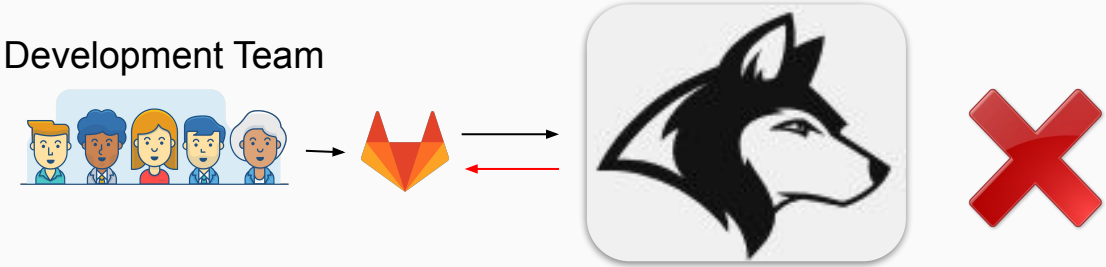
gosec

Bandit

Brakeman

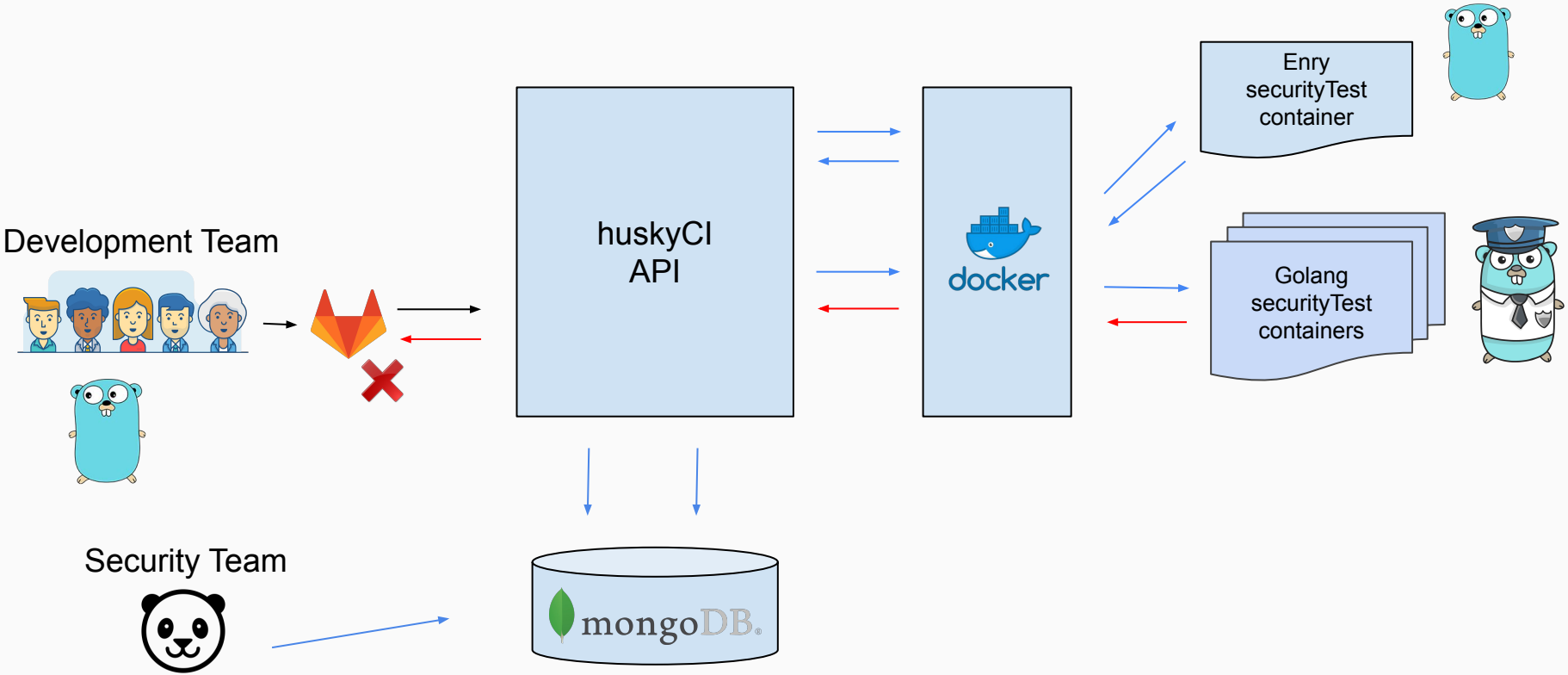
How can we build this?

huskyCI
github.com/globocom/huskyCI



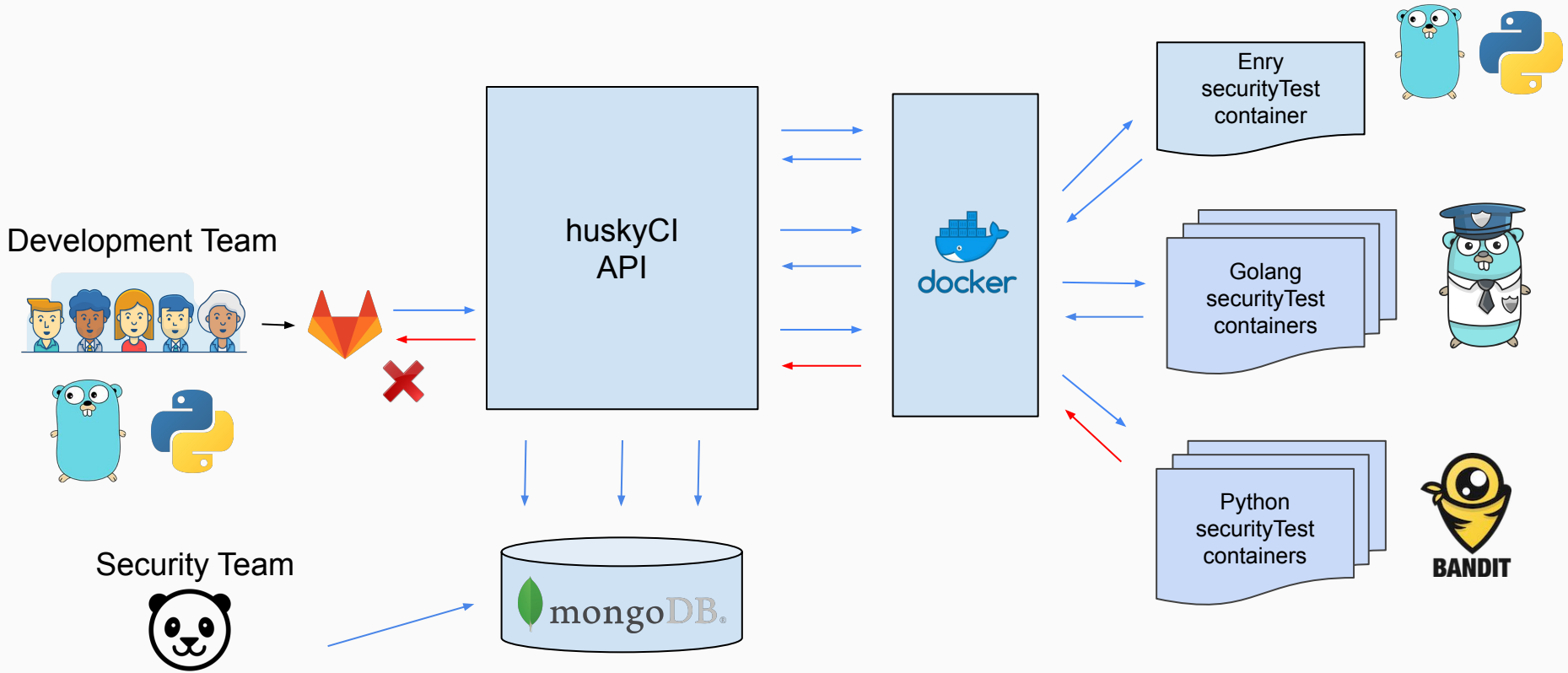
How can we build this?

huskyCI
github.com/globocom/huskyCI



How can we build this?

huskyCI
github.com/globocom/huskyCI



Add a new stage in your CI

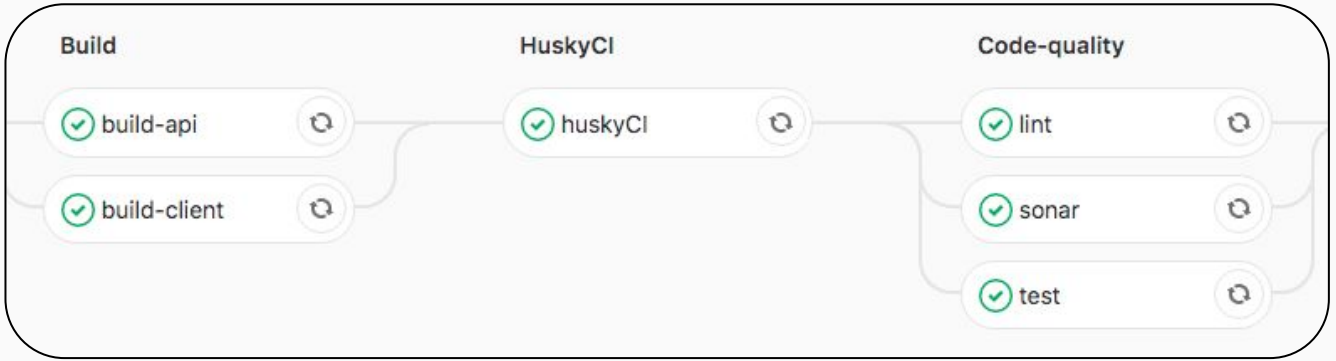
huskyCI

github.com/globocom/huskyCI

.gitlabci.yml

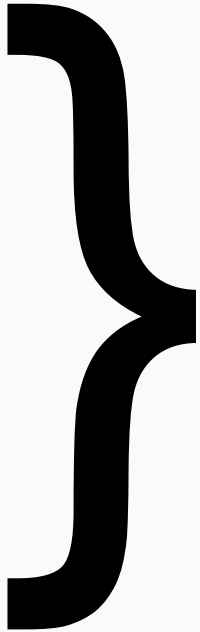
```yaml
stages:
  - HuskyCI

test-huskyci:
  stage: HuskyCI
  script:
    - wget urlto.huskyci.com/huskyci-client
    - chmod +x huskyci-client
    - ./huskyci-client
```



Add a new stage in your CI

huskyCI
github.com/globocom/huskyCI



~ 4 minutes

huskyCI

github.com/globocom/huskyCI

Demo 🔥

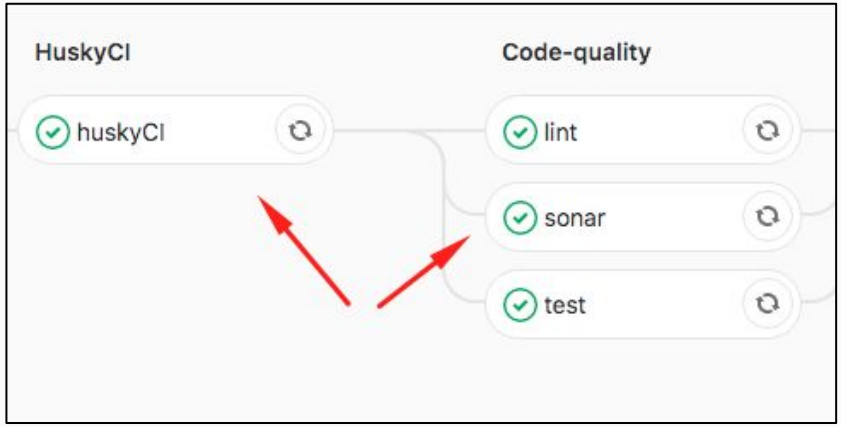
Quick Metrics

huskyCI
github.com/globocom/huskyCI

https://github.com/globocom/huskyCI-dashboard

Sonar Integration

huskyCI
github.com/globocom/huskyCI



Gemfile.lock

https://github.com/flavorjones/loofah/issues/144loofah gem 2.1.1 is vulnerable (CVE-2018-8048). Upgrade to 2.2.1 See Rule huskyCI
2 years ago L707
Vulnerability Info Open Not assigned 0min effort Comment
No tags

https://groups.google.com/d/msg/rubyonrails-security/tP7W3kLc5u4/uDy2Br7xBgAJrails-html-sanitizer 1.0.3 is vulnerable (CVE-2018-3741). Upgrade to rails-html-sanitizer 1.0.4 See Rule huskyCI
3 years ago L775
Vulnerability Info Open Not assigned 0min effort Comment
No tags

Supported Languages + Sec Tests

huskyCI
github.com/globocom/huskyCI

Supported Languages





Available Security Tests

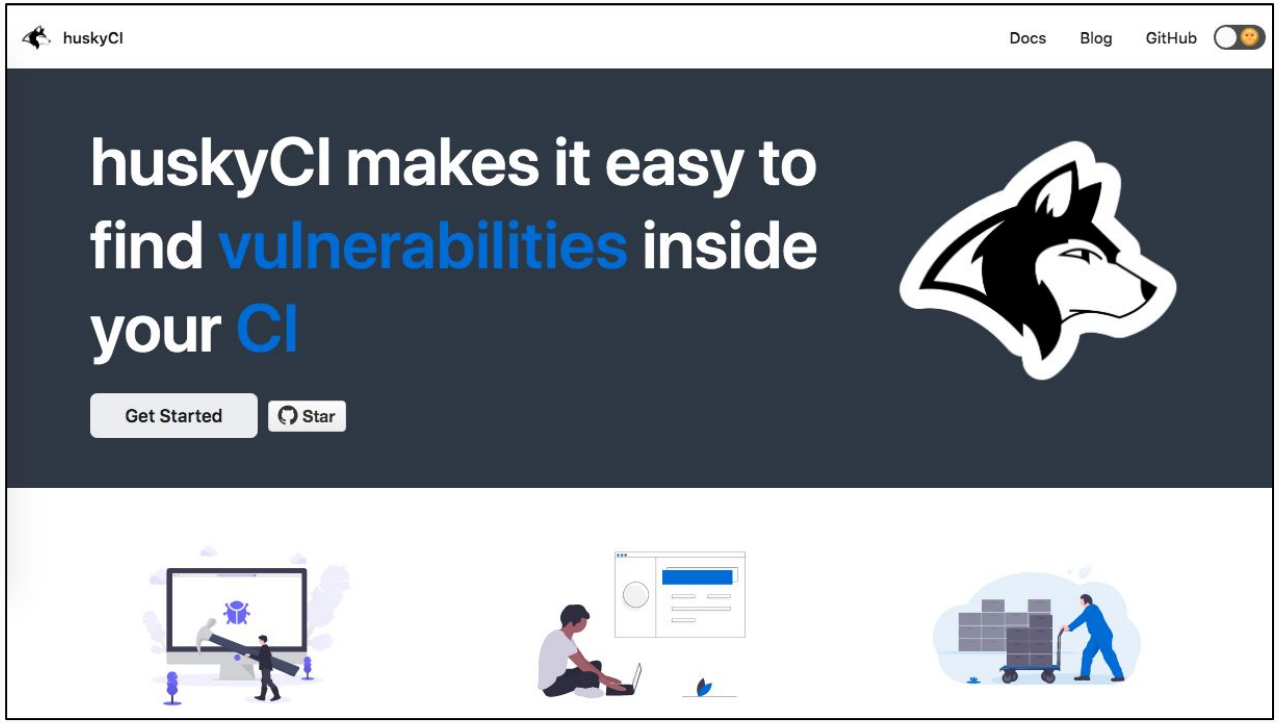


Gitleaks

Give it a try!

huskyCI

github.com/globocom/huskyCI



https://github.com/globocom/huskyCI

Dec, 2019

Questions? Thanks!

🤔 🙃

github.com/globocom/huskyCI

Rafael dos Santos 🇧🇷 @rafasantos5

References 📖

huskyCI

github.com/globocom/huskyCI

- [huskyCI] https://github.com/globocom/huskyCI
- [huslyCI-dashboard] https://github.com/globocom/huskyCI-dashboard
- [enry] https://github.com/src-d/enry
- [Safety] https://github.com/pyupio/safety
- [Bandit] https://github.com/PyCQA/bandit
- [gosec] https://github.com/securego/gosec
- [Brakeman] https://github.com/presidentbeef/brakeman
- [npm audit] https://docs.npmjs.com/cli/audit
- [yarn audit] https://yarnpkg.com/lang/en/docs/cli/audit/
- [gcom Hackday] https://www.instagram.com/talentosgcom/
- [Docker API] https://docs.docker.com/engine/api/v1.24/
- [SonarQube] https://www.sonarqube.org
- [SpotBugs] https://github.com/spotbugs/spotbugs
- [Awesome-Static-Analysis] https://github.com/mre/awesome-static-analysis
- [Awesome DevSecOps] https://github.com/devsecops/awesome-devsecops
- [huskyCI POC] https://gitlab.com/rafaveira3/appsec-defcon27-huskyci/merge_requests