
mindthesec
/SÃO PAULO
MAIS UM EVENTO:
Flipside
SECURITY BEYOND TECHNOLOGY
REALIZAÇÃO:
Green Helmet

huskyCI: Encontrando vulnerabilidades de código na Globo.com antes do deploy

Rafael Santos

Analista de Segurança

mindthesec /SÃO PAULO

$ whoami

Rafael dos Santos 🇧🇷 @rafasantos5

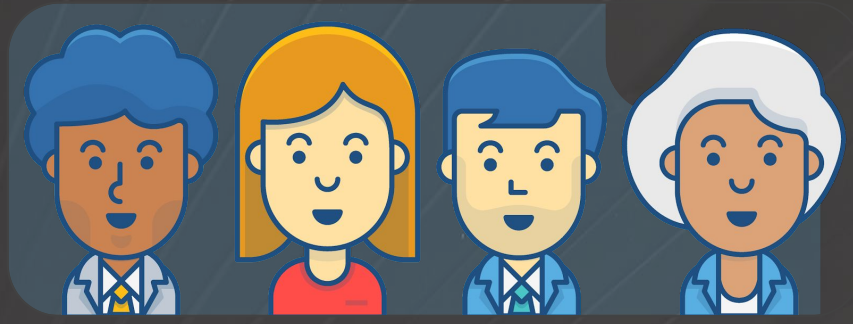
github.com/rafaveira3

⚽ Volante Clássico (Camisa 5)

☕ OSCP + OSCE
🐼 Analista de Segurança @ globo.com
🚀 Sec Tools + Desenvolvimento de Exploits

Um dia na vida de um time de desenvolvimento ...

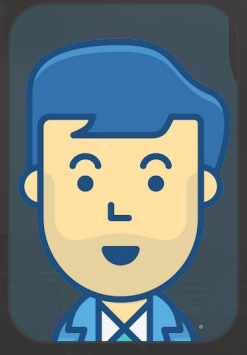
Um dia na vida de um time de desenvolvimento ...



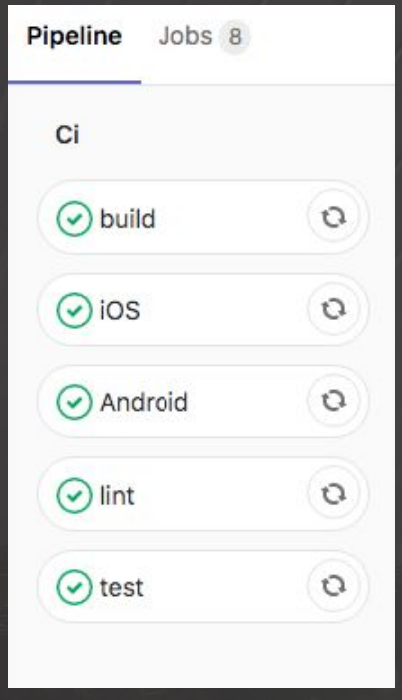
tsuru

mindthesec /SÃO PAULO

Um dia na vida de um time de desenvolvimento ...

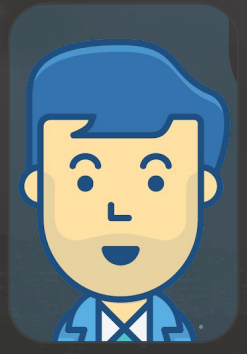


Nova feature!

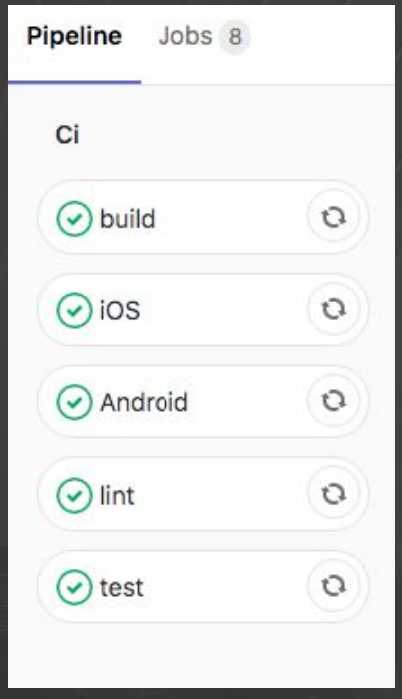


"Parece bom!"

Um dia na vida de um time de desenvolvimento ...

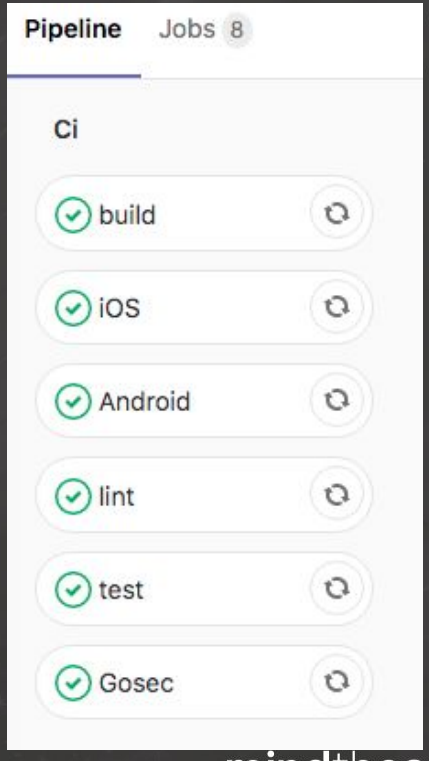


Nova feature!



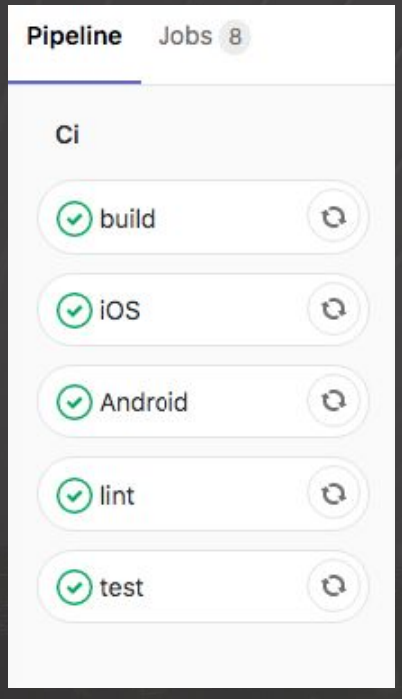
Time de Segurança

"Opa, o que acham de usar o Gosec?"



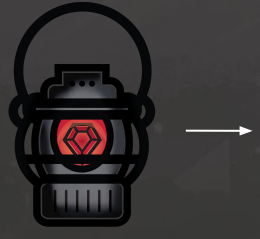
Um dia na vida de um time de desenvolvimento ...

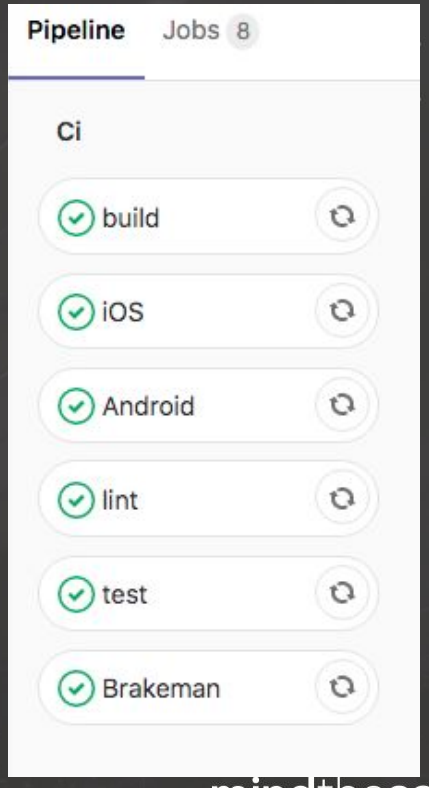
Nova feature!



Time de Segurança

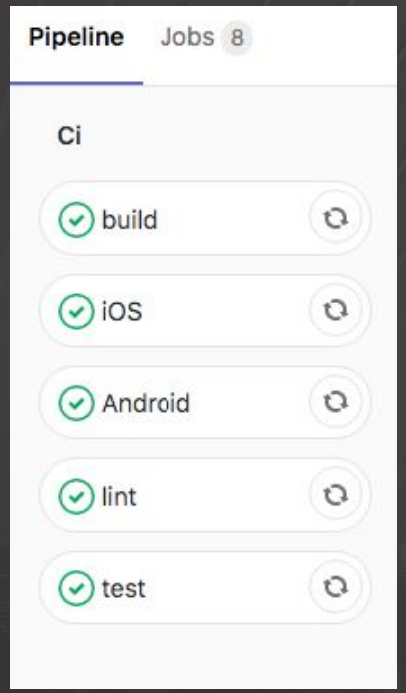
"Opa, o que acham de usar o Brakeman?"





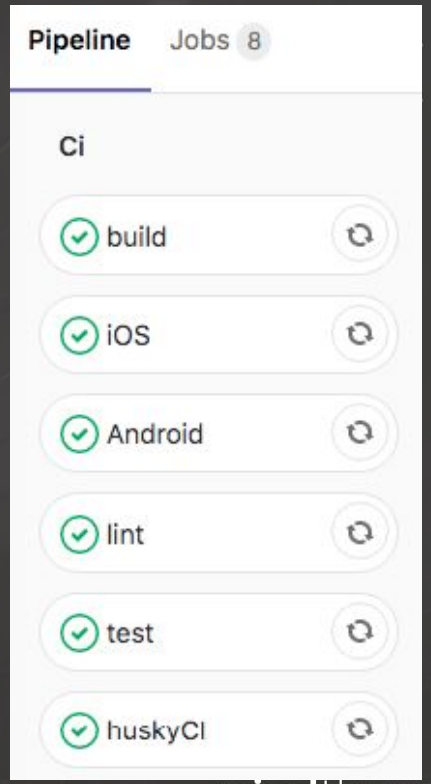
Um dia na vida de um time de desenvolvimento ...

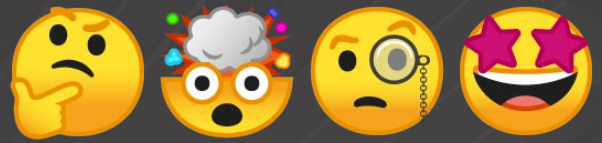
Nova feature!



Time de Segurança

"Opa, o que acham de usar o ... ?"

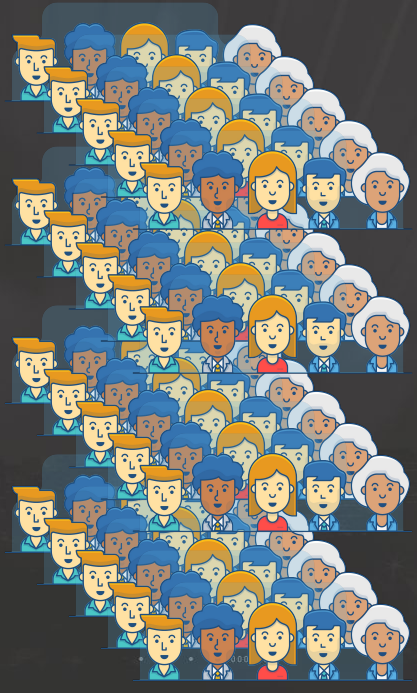




Um dia na vida de uma grande organização ...

Um dia na vida de uma grande organização ...

Times de Desenvolvimento



Time de Segurança


THIS IS FINE
GOPHER

Let's hack! 


The Hack Day

Let's hack!

Times de Desenvolvimento

Time de Segurança

tsuru

Let's hack!

Times de Desenvolvimento

Time de Segurança

tsuru

mindthesec /SÃO PAULO

Let's hack!

Times de Desenvolvimento

Time de Segurança

tsuru

mindthesec /SÃO PAULO

Let's hack!

Times de Desenvolvimento

Time de Segurança

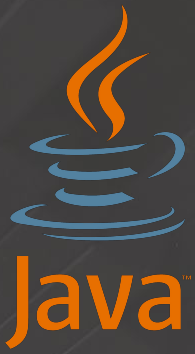
tsuru

mindthesec /SÃO PAULO

Beleza, mas quais linguagens usamos? 

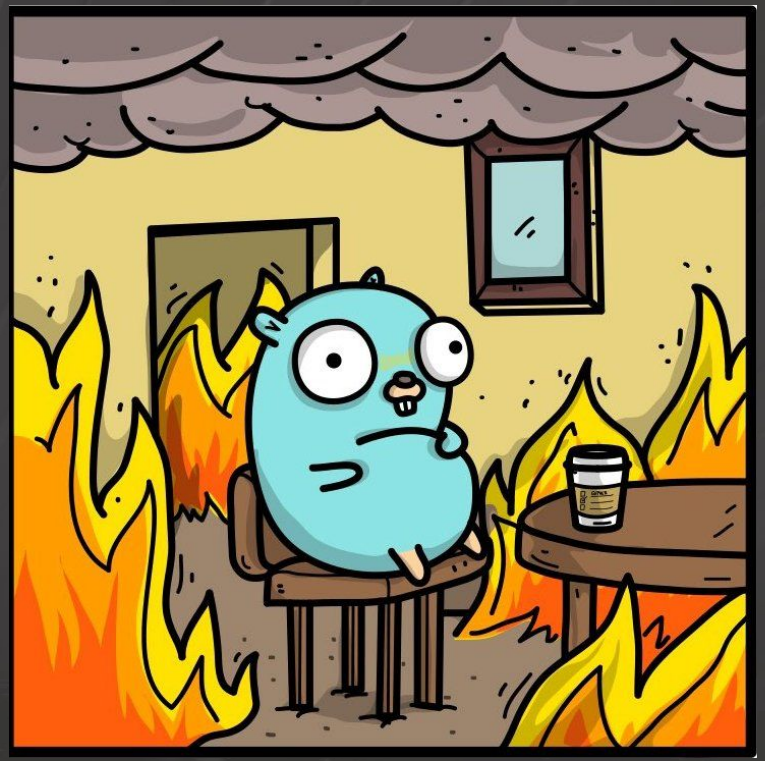
Beleza, mas quais linguagens usamos?







Beleza, mas quais linguagens usamos?

gosec

Bandit

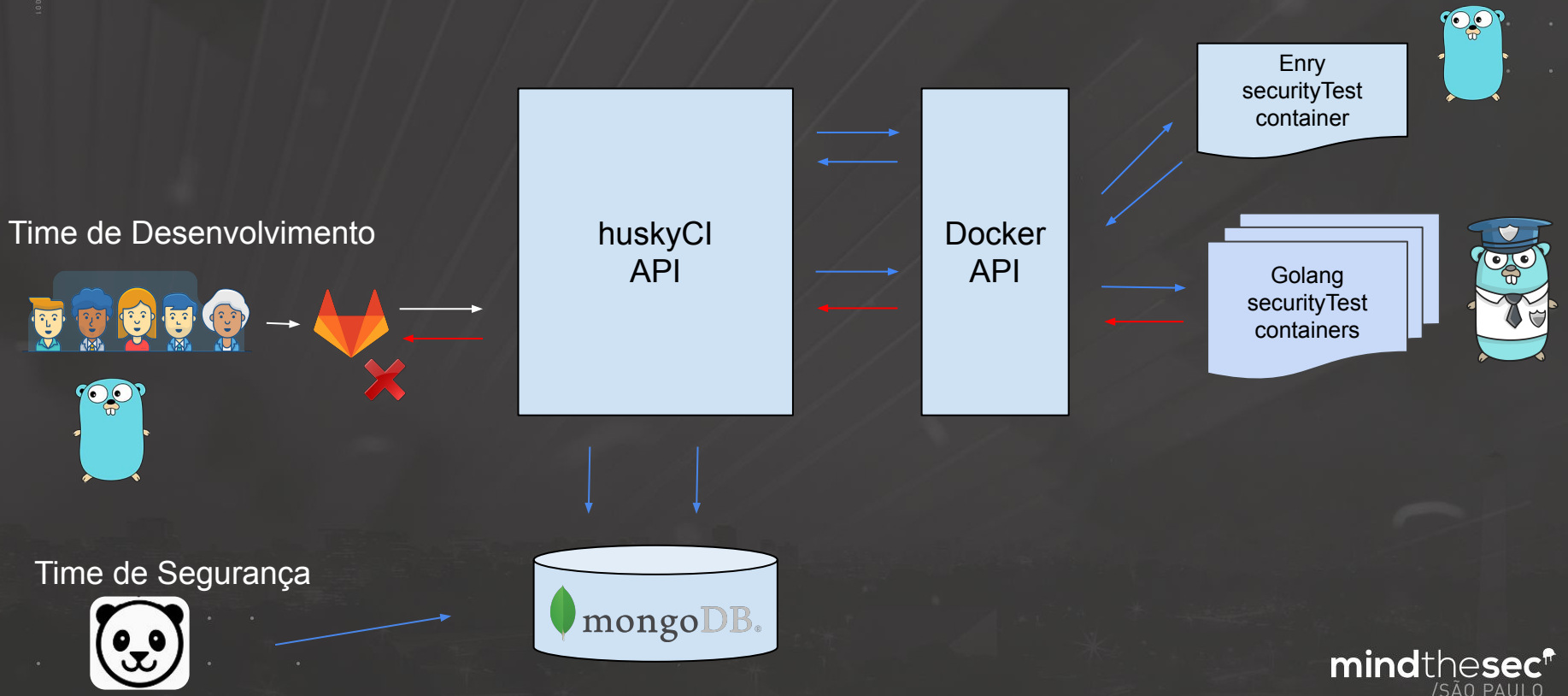
Brakeman

Como queremos construir esta ferramenta? 🛠️

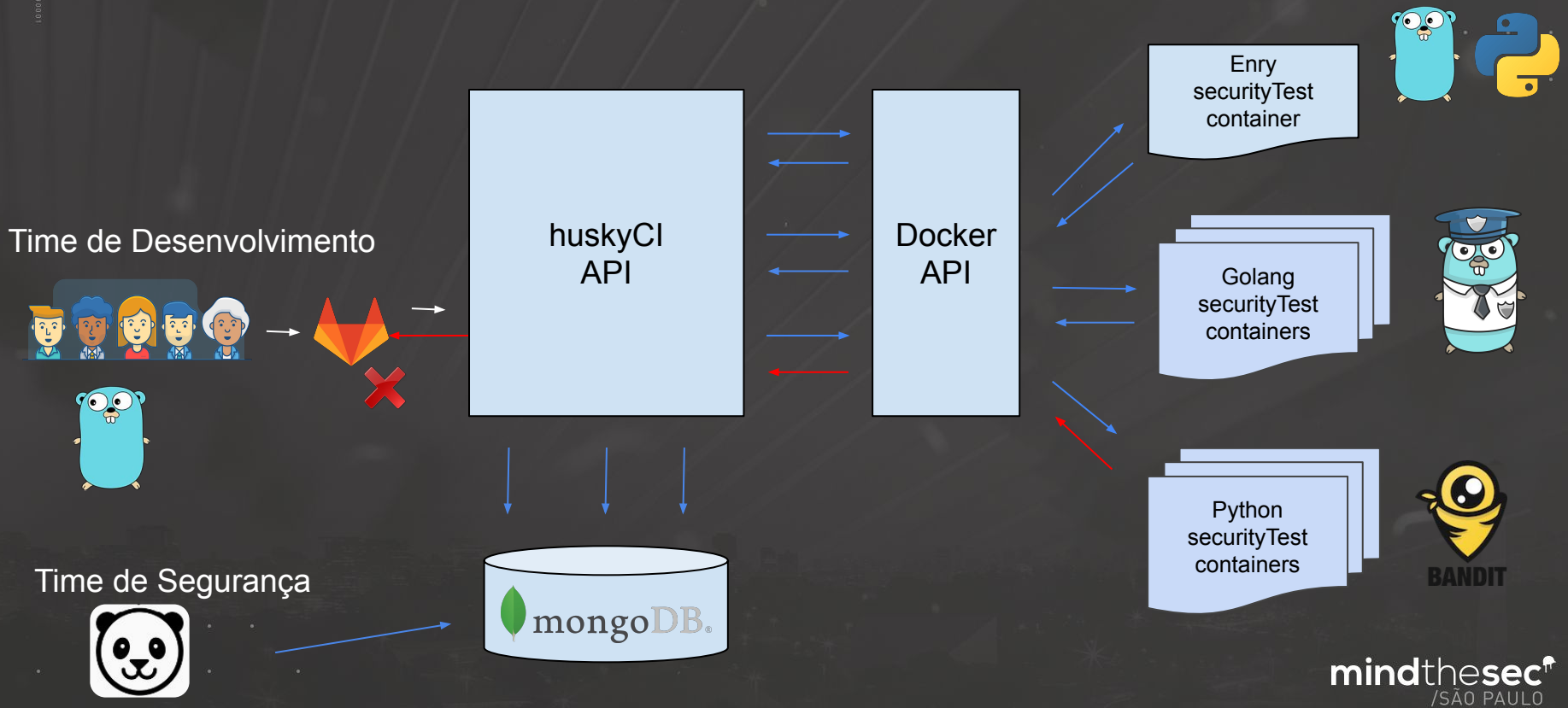
Como queremos construir esta ferramenta?

Time de Desenvolvimento

Como queremos construir esta ferramenta?



Como queremos construir esta ferramenta?

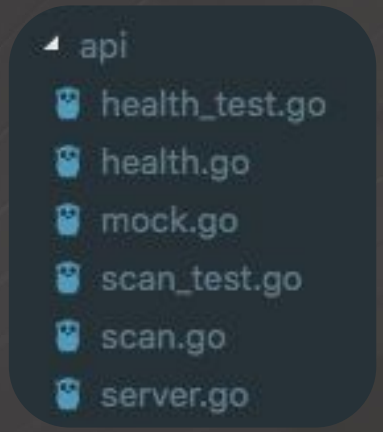


E o que gostaríamos de ver? 👀

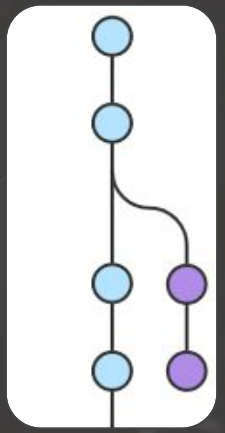
E o que gostaríamos de ver?

Autores de commit

Linguagem do repositório



Arquivos encontrados

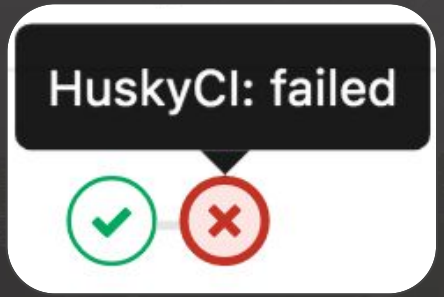


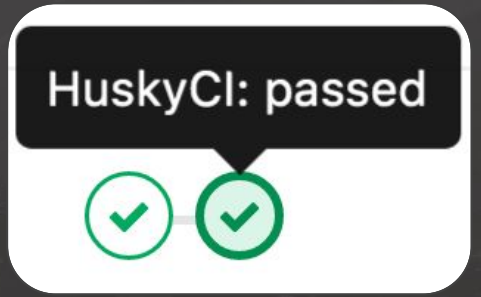
Nome da Branch

E o que gostaríamos de ver?

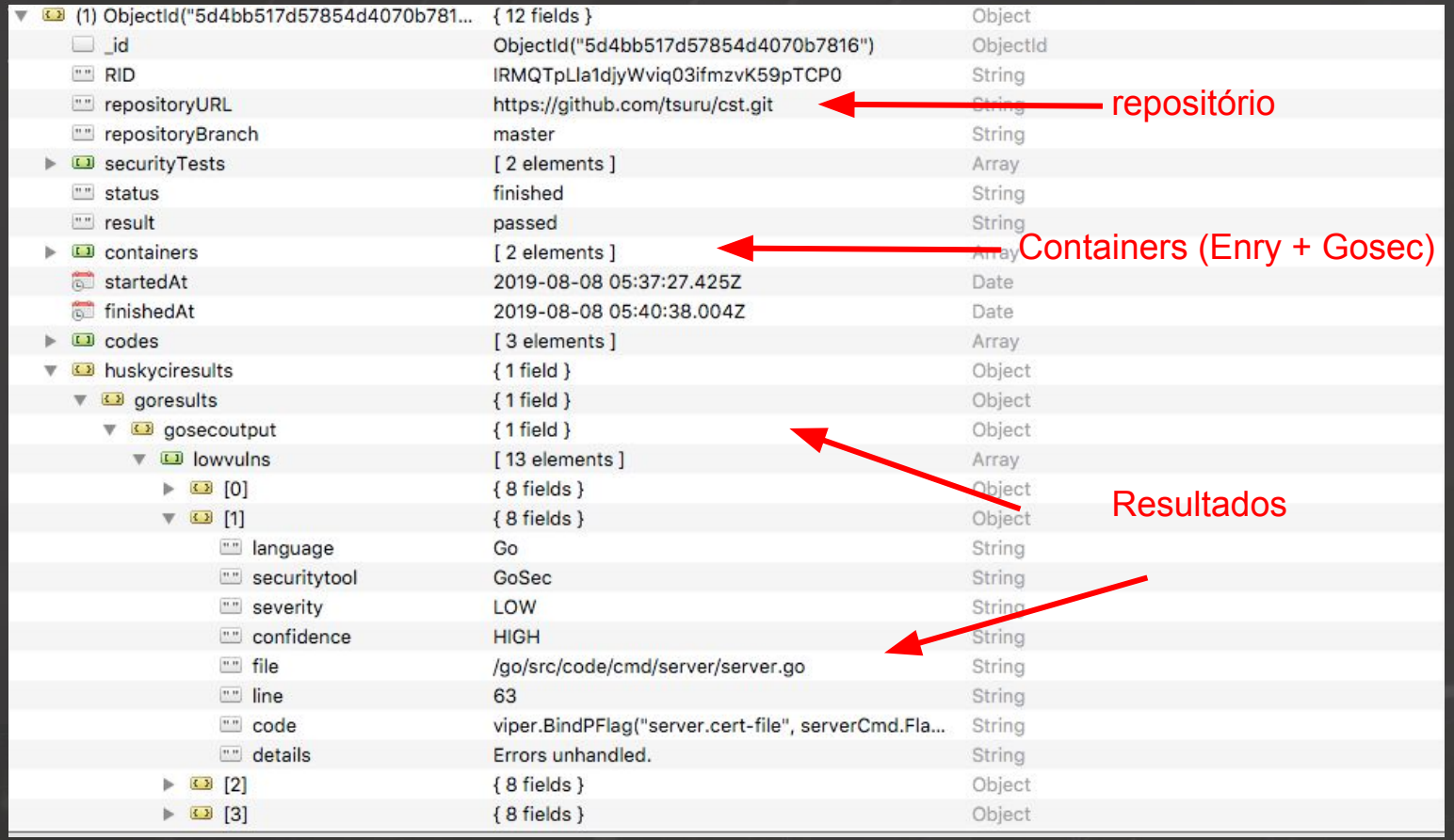
```
[HUSKYCI][!] Severity: MEDIUM
[HUSKYCI][!] Confidence: HIGH
[HUSKYCI][!] Details: Blacklisted import crypto/sha1: weak cryptographic primitive
[HUSKYCI][!] File: /go/src/code/api/token.go
[HUSKYCI][!] Line: %!d(string=6)
[HUSKYCI][!] Code: "crypto/sha1"
```

Vulnerabilidades Encontradas





Mitigação feita


(1) ObjectId("5d4bb517d57854d4070b781... { 12 fields } Object
_id ObjectId("5d4bb517d57854d4070b7816") ObjectId
RID IRMQTpLla1djyWviq03ifmzvK59pTCP0 String
repositoryURL https://github.com/tsuru/cst.git String
repositoryBranch master String
securityTests [2 elements] Array
status finished String
result passed String
containers [2 elements] Array
startedAt 2019-08-08 05:37:27.425Z Date
finishedAt 2019-08-08 05:40:38.004Z Date
codes [3 elements] Array
huskyciresults { 1 field } Object
goresults { 1 field } Object
gosecoutput { 1 field } Object
lowvulns [13 elements] Array
[0] { 8 fields } Object
[1] { 8 fields } Object
language Go String
securitytool GoSec String
severity LOW String
confidence HIGH String
file /go/src/code/cmd/server/server.go String
line 63 String
code viper.BindPFlag("server.cert-file", serverCmd.Fla... String
details Errors unhandled. String
[2] { 8 fields } Object
[3] { 8 fields } Object
repositório
Containers (Enry + Gosec)
Resultados

DEV, "vem tranquilo"... Pode focar no desenvolvimento ❤️‍🩹

.gitlabci.yml

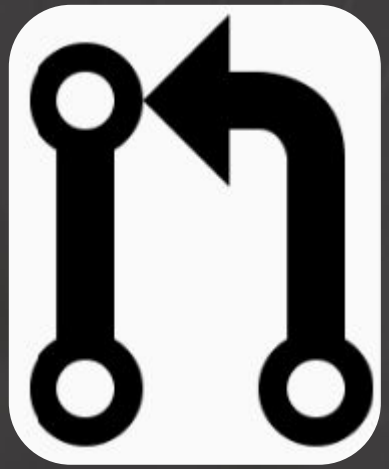
```yaml
stages:
  - HuskyCI

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

Demo 🔥

Resultados Globo.com (até agora) 🚀

Resultados Globo.com (até agora)



projetos "beta" com huskyCI

Big Brother Brasil

CartolaFC

~65 repositórios únicos

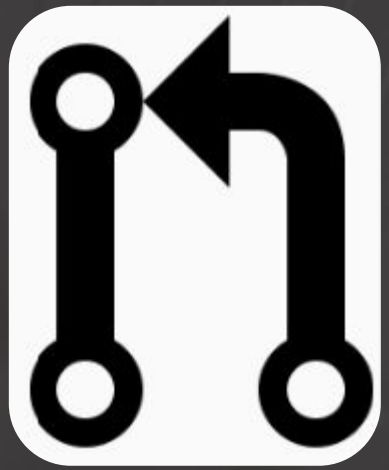
~30 análises por dia

GLOBOPLAY

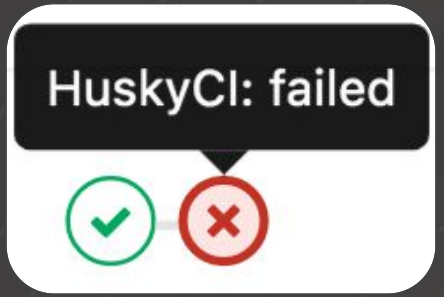
the Voice Brasil

~180 branches únicas

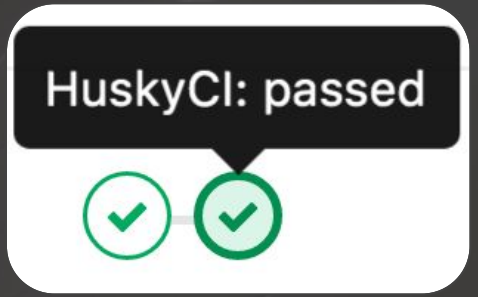
Resultados Globo.com (até agora)



projetos "beta" com huskyCI



~20% falhou

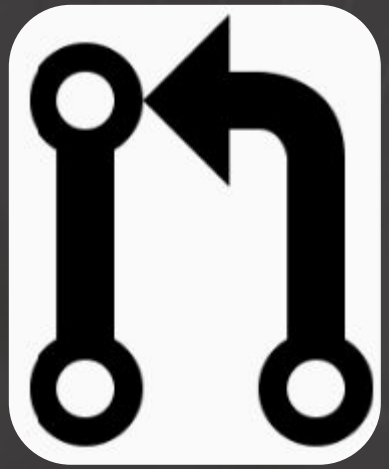


~52% passou

```
$ chmod +x huskyci-client
$ ./huskyci-client
[HUSKYCI][ERROR] Check environment variables:
ERROR: Job failed: exit code 1
```

~28% errou

Resultados Globo.com (até agora)



projetos "beta" com huskyCI

14.6 segundos

13.8 segundos

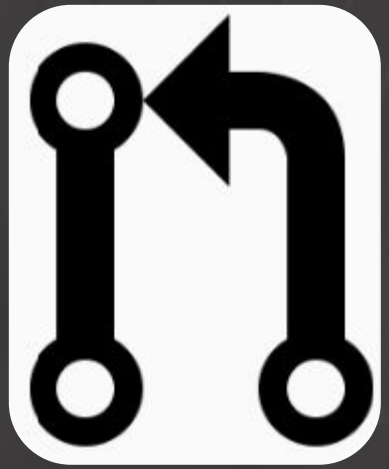
7.1 minutos

7.1 segundos

13.2 segundos

8.3 segundos

Resultados Globo.com (até agora)



projetos "beta" com huskyCI

“error unhandled”

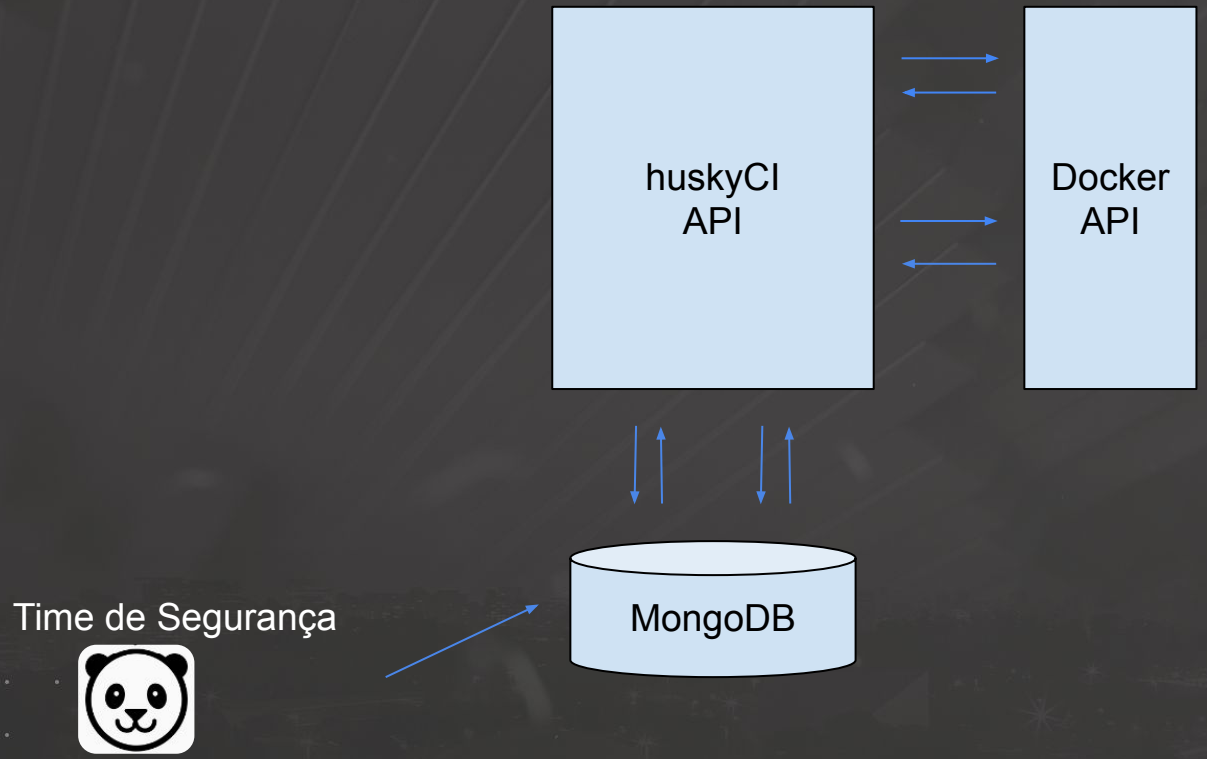
dependências vulneráveis

dependências vulneráveis

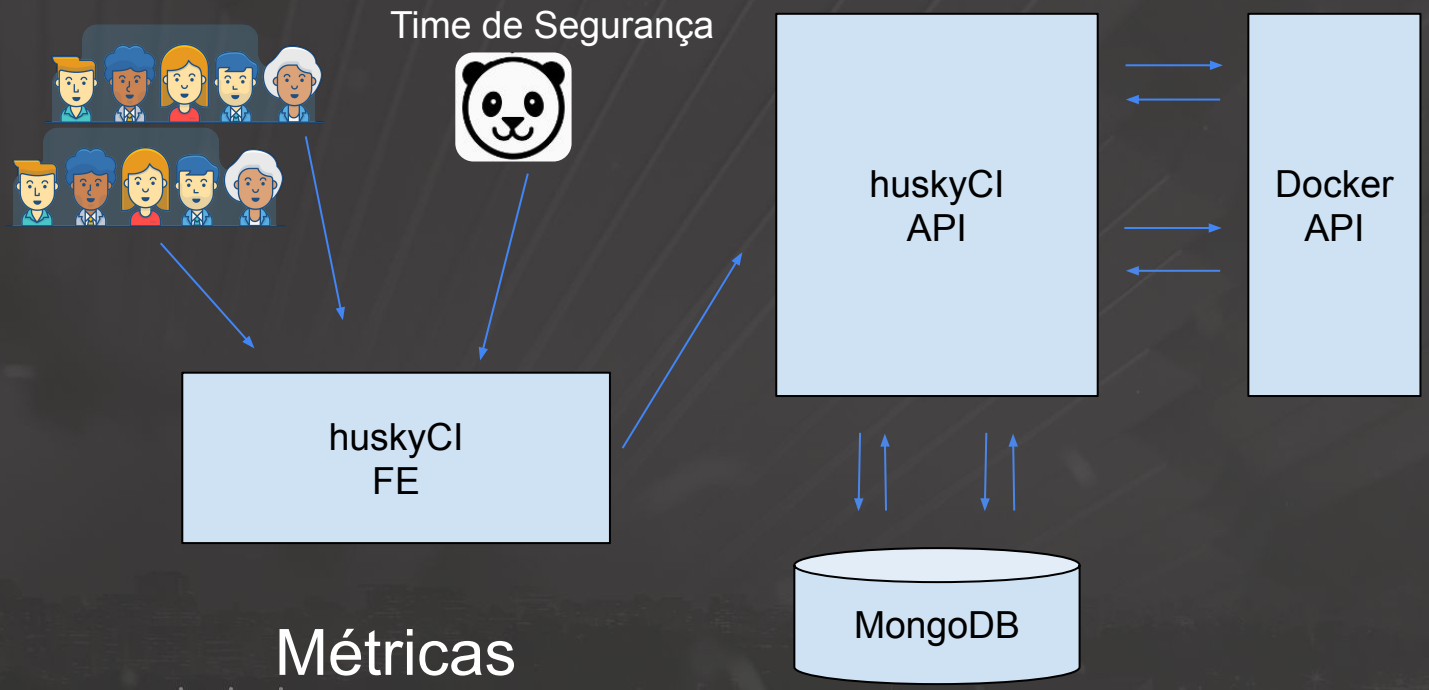
dependências vulneráveis

Próximas etapas ⭐

Próximas etapas: Front-end



Próximas etapas: Front-end



Métricas

Próximas etapas: Integração com o SonarQube

Próximas etapas: Suportar mais linguagens

Próximas etapas: Contribuir para as ferramentas Open Source

npm

Safety

Retire.js

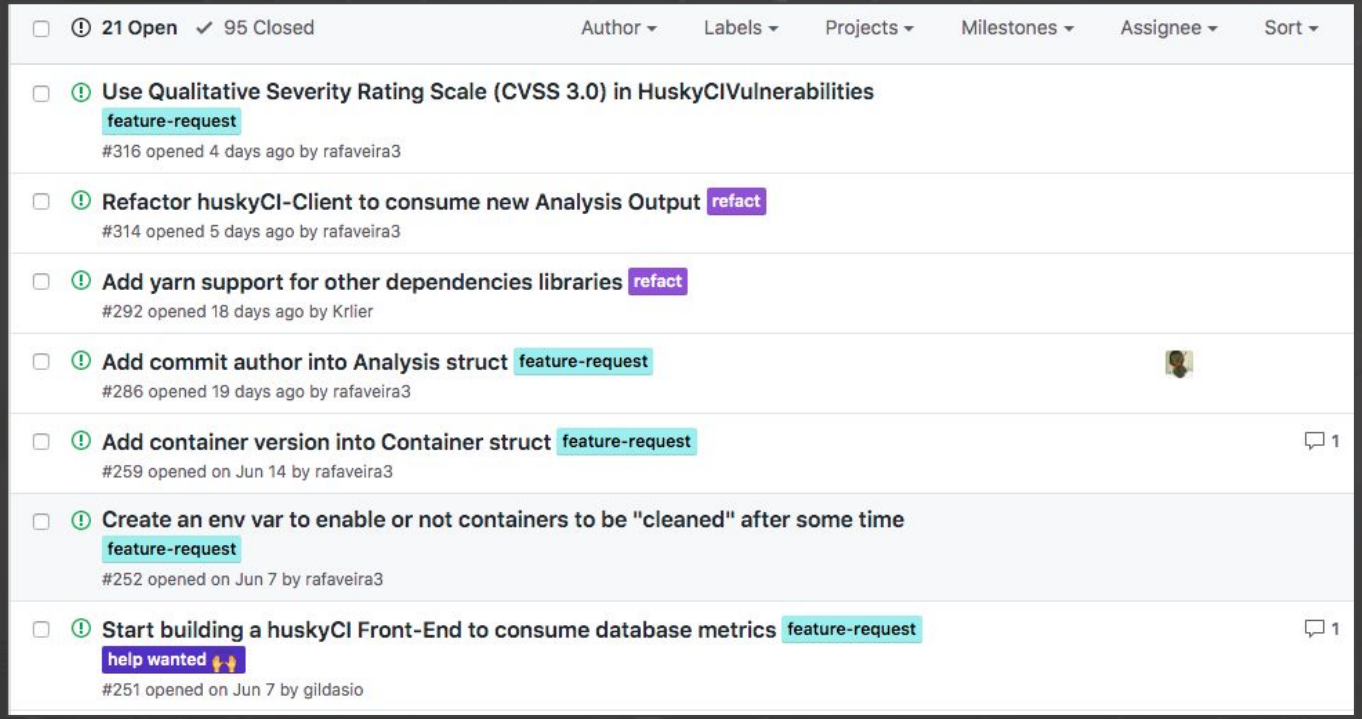
Próximas etapas: Adicionais mais Security Tests

Security Code Scan

SpotBugs

Awesome DevSecOps awesome

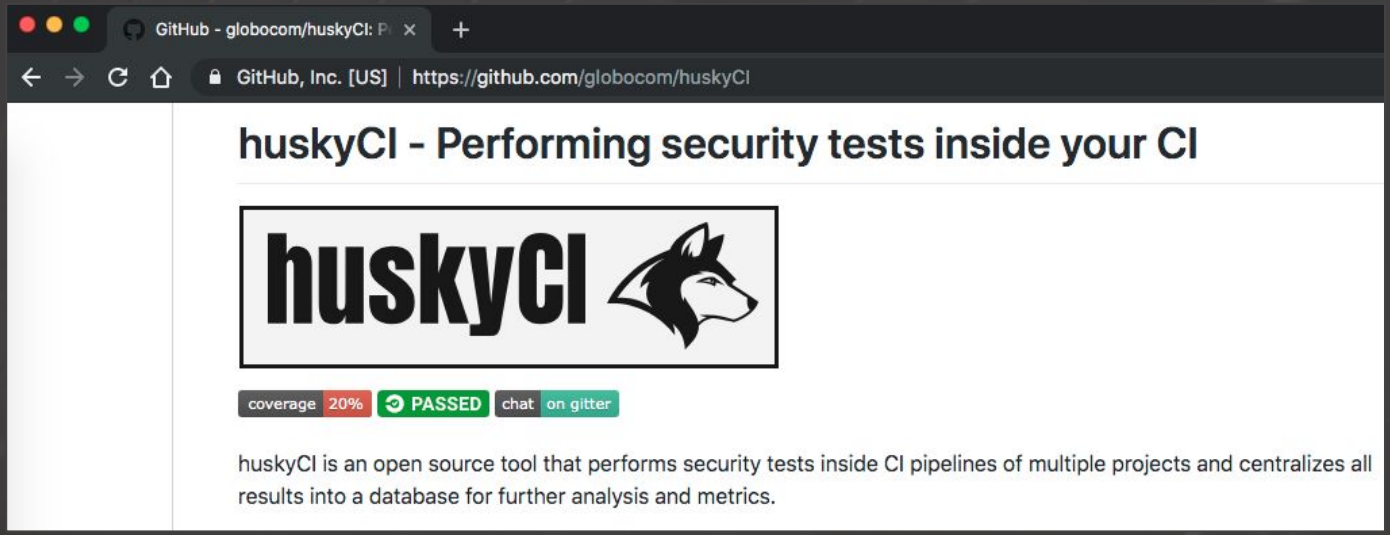
Próximas etapas: E muito mais!



https://github.com/globocom/huskyCI/issues

Próximas etapas: E muito mais!

Open Source



https://github.com/globocom/huskyCI

Referências 📖

- [huskyCI] https://github.com/globocom/huskyCI
- [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
- [gcom Hackday] https://www.instagram.com/talentosgcom/
- [Docker API] https://docs.docker.com/engine/api/v1.24/
- [SonarQube] https://www.sonarqube.org
- [Infer] http://fbinfer.com
- [SpotBugs] https://github.com/spotbugs/spotbugs
- [Security Code Scan] https://security-code-scan.github.io/
- [Checkmarx] https://www.checkmarx.com/
- [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

PERGUNTAS

AGRADECIMENTO

rafael.santos@corp.globo.com
@rafasantos5