



GTS 32 | SP 12/2018

HuskyCI:

Encontrando vulnerabilidades de código na Globo.com antes do deploy

Rafael Santos

rafael.santos@corp.globo.com

1. Motivações
2. Planejamento do projeto
3. Demo
4. Resultados obtidos
5. Próximos passos



1. Motivações

Times de Devs



Time de Segurança



Motorista nu bate em carro parado e capota veículo no Ceará



CR7 chama Messi para jogar na Itália: 'Como eu, aceite o desafio'



Ex-paquitas se reúnem para amigo secreto na casa de Xuxa



Executiva da Huawei presa pede libertação por motivos de saúde



Após anunciar Carille, Timão tenta acelerar montagem de elenco



Sasha posa decotada e capricha no 'carão' para encantar fãs



Ghosh é acusado formalmente no Japão por violação financeira



Cobiçado por clubes do Brasil, Sassá seguirá no Cruzeiro, diz diretoria



Gavassi mostra Bruna 'desesperada' em show de Sandy; vídeo

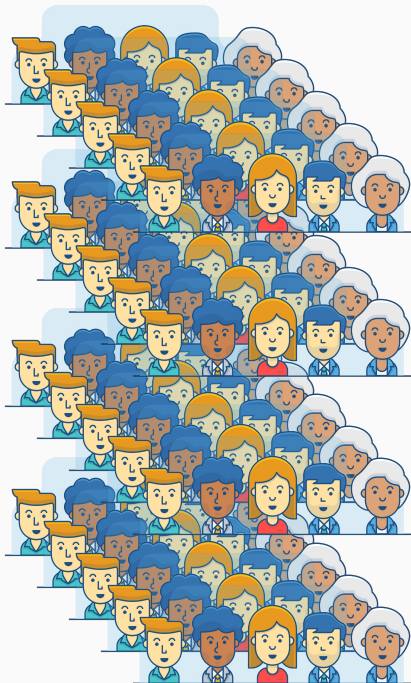
Operação mira suposto esquema de médicos e empresários para furar fila do SUS

Santos não tem avanços após 'não' de Abel e inicia semana decisiva por novo técnico

Alok passa mal durante show no Festival de Verão e relata suspeita de zika

1. Motivações: Realidade

Times de Devs



Time de Segurança



7 chama Messi para jogar na Iia: 'Como eu, aceite o desafio'



Ex-paquitas se reúnem para amigo secreto na casa de Xuxa



Após anunciar Carille, Timão tenta acelerar montagem de elenco



Sasha posa decotada e capricha no 'carão' para encantar fãs



Cobiçado por clubes do Brasil, Sassa seguirá no Cruzeiro, diz diretoria



Gavassi mostra Bruna 'desesperada' em show de Sandy; vídeo

tos não tem avanços após 'não' de Abel e a semana decisiva por novo técnico

Alok passa mal durante show no Festival de Verão e relata suspeita de zika

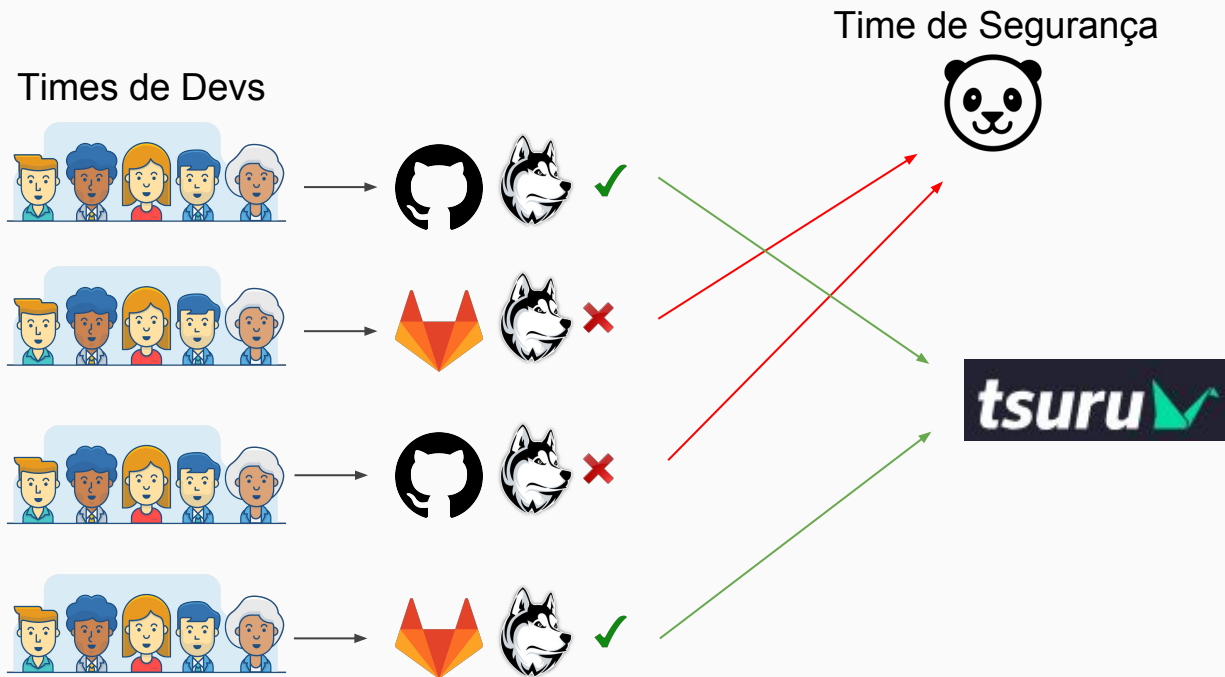
1. Motivações: Realidade



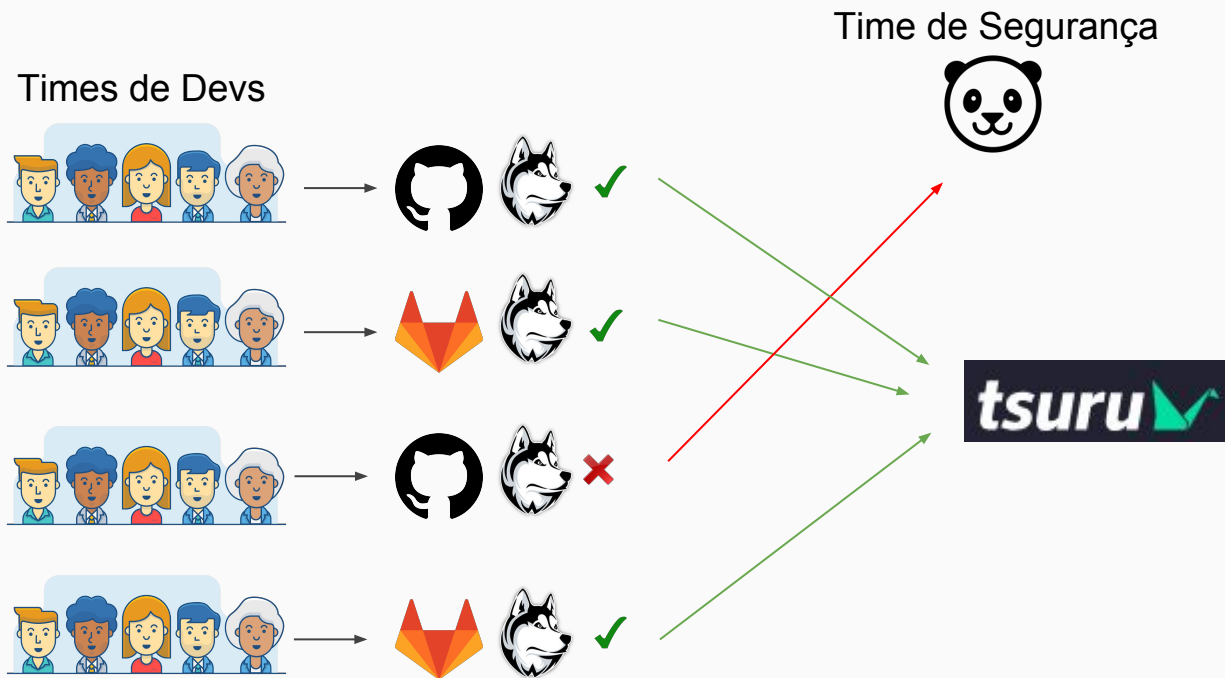
2. Planejamento do projeto



2. Planejamento do projeto: Fluxo ideal



2. Planejamento do projeto: Fluxo ideal

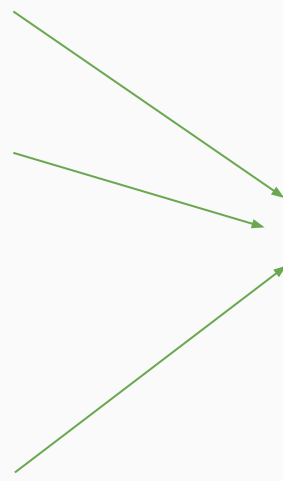


2. Planejamento do projeto: Fluxo ideal

Time de Segurança



Times de Devs



2. Planejamento do projeto: Fluxo ideal

Time de Segurança



Times de Devs



7 chama Messi para jogar na Iia: 'Como eu, aceite o desafio'



Ex-paquitas se reúnem para amigo secreto na casa de Xuxa



Após anunciar Carille, Timão tenta acelerar montagem de elenco



Sasha posa decotada e capricha no 'carão' para encantar fãs



Cobiçado por clubes do Brasil, Sassa seguirá no Cruzeiro, diz diretoria

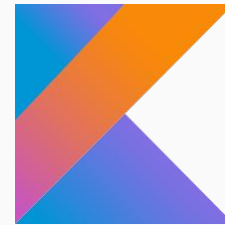
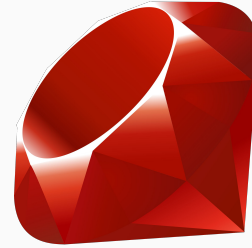


Gavassi mostra Bruna 'desesperada' em show de Sandy; vídeo

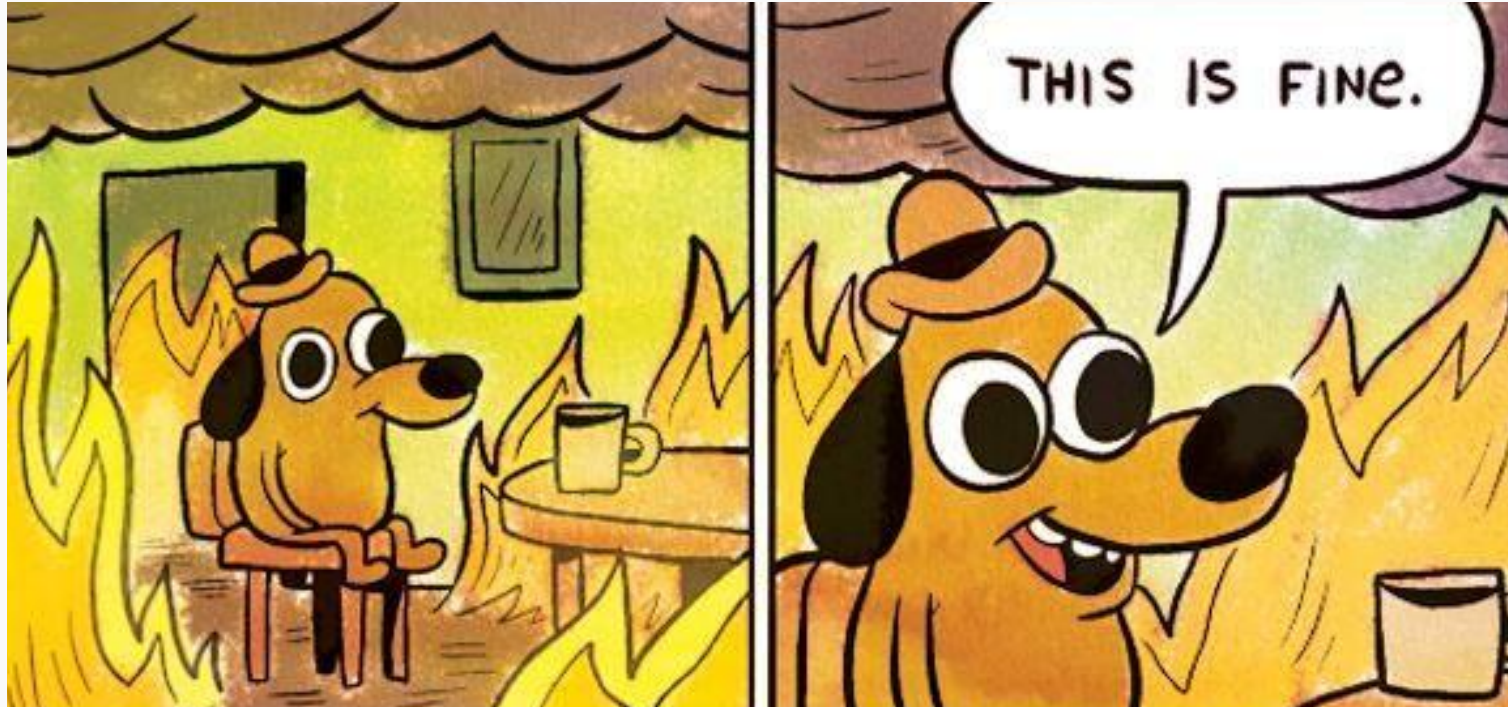
tos não tem avanços após 'não' de Abel e a semana decisiva por novo técnico

Alok passa mal durante show no Festival de Verão e relata suspeita de zika

Quais linguagens utilizamos na Globo.com?



2. Planejamento do projeto: Linguagens



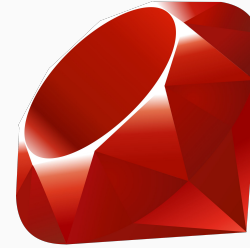
Ferramentas open source para análise de código?



GoSec



BANDIT



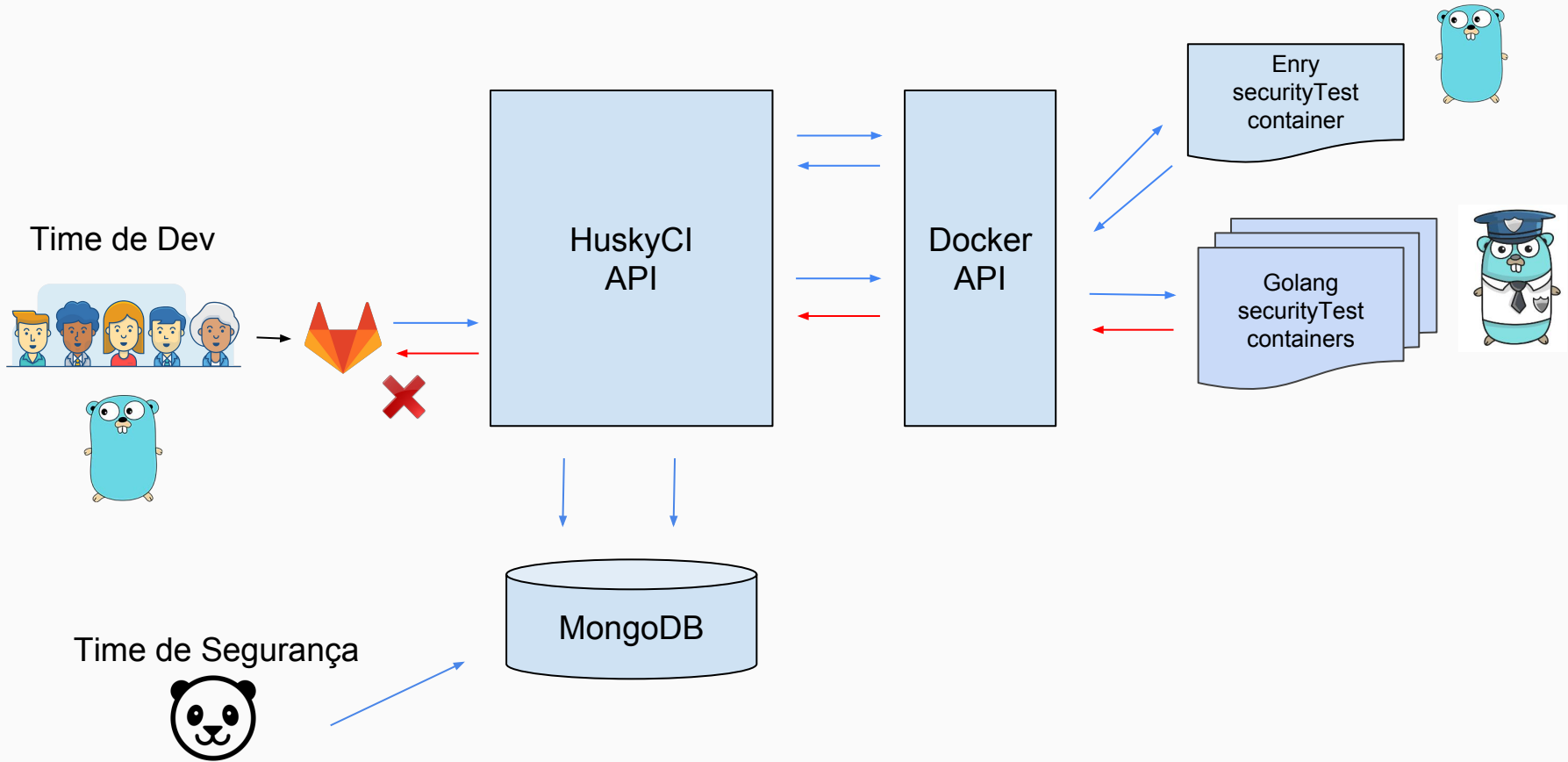
Brakeman

2. Planejamento do projeto: Arquitetura

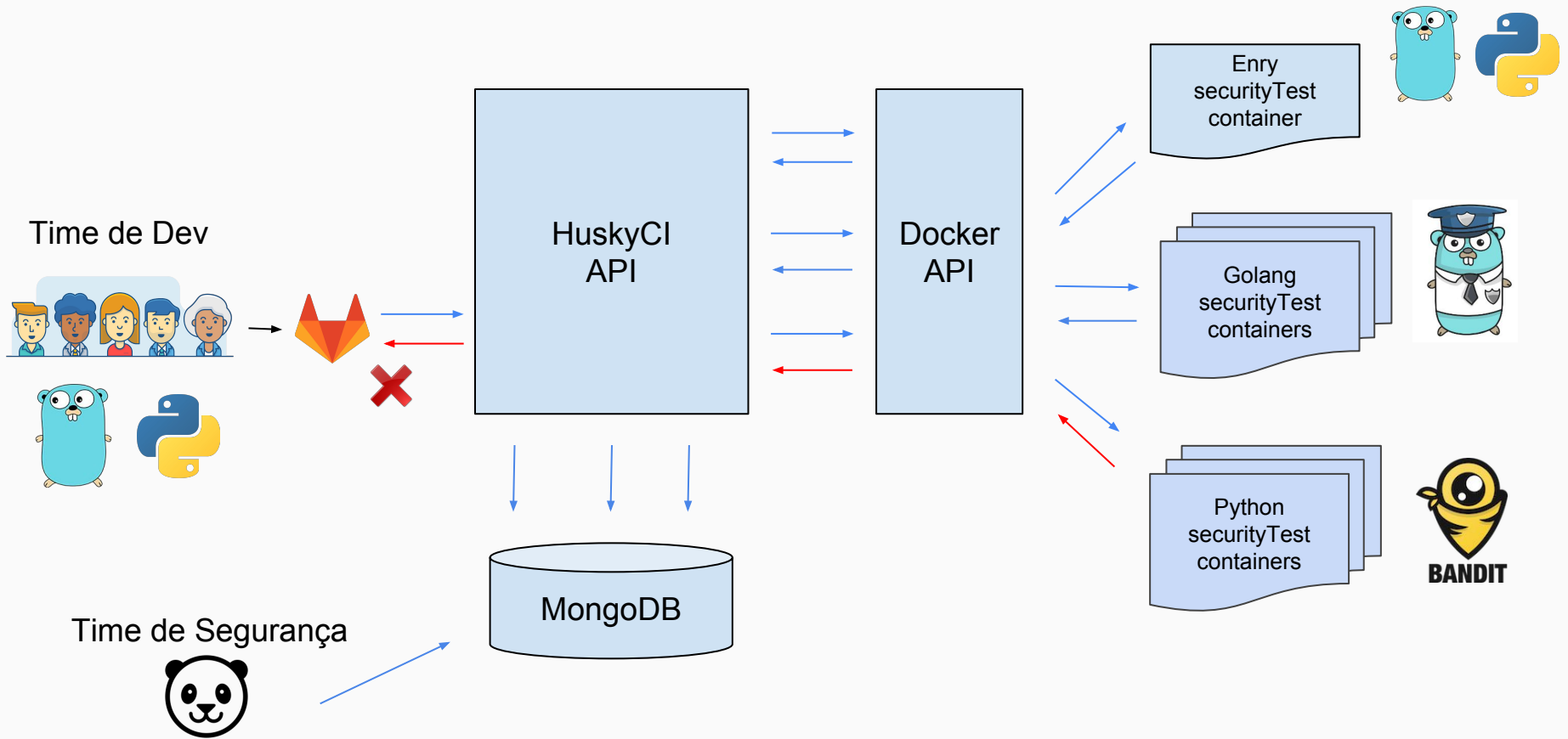
Time de Dev



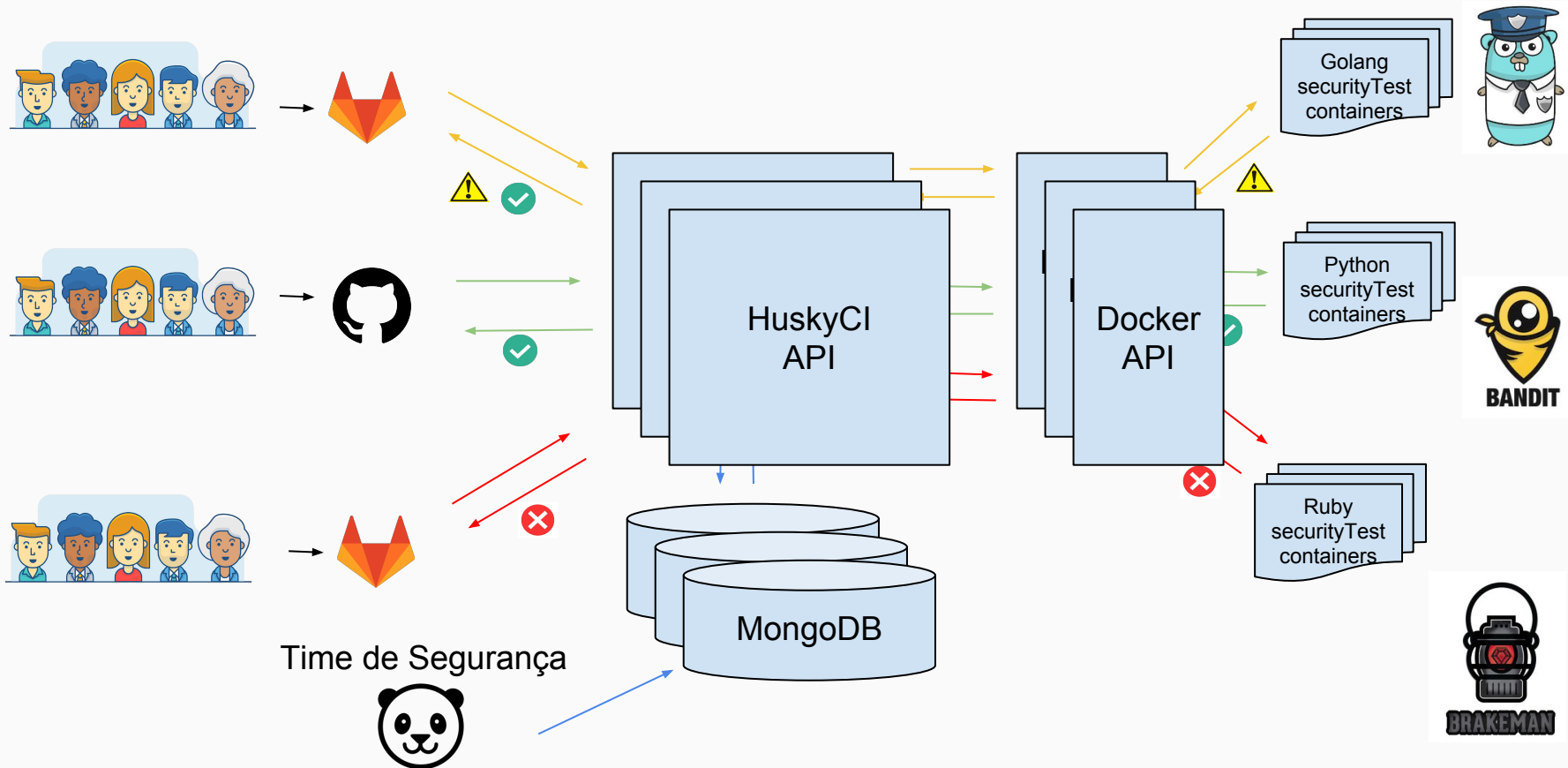
2. Planejamento do projeto: Arquitetura



2. Planejamento do projeto: Arquitetura



2. Planejamento do projeto: Escalabilidade



2. Planejamento do projeto: MongoDB

▼ (1) ObjectId("5c0fb0c243ef8c28590f5487")	{ 8 fields }	Object
_id	ObjectId("5c0fb0c243ef8c28590f5487")	ObjectId
RID	iyfYaADYICZzzgq9uXZoEGhdPWLbhwJT	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
▼ [0]	{ 8 fields }	Object
CID	b2649a16bf6f6b14fd3890117bd2aab7b2d1b97aa17ceb610d07c7c45afff51b	String
VM		String
▶ securityTest	{ 7 fields }	Object
cStatus	finished	String
cOutput	{"Dockerfile":["Dockerfile"],"Go":["api/health.go","api/health_test.go","api/mock.go","api/scan.go","api/sca...	String
cResult		String
startedAt	2018-12-11 12:42:43.433Z	Date
finishedAt	2018-12-11 12:42:46.841Z	Date
▼ [1]	{ 8 fields }	Object
CID	8bac8f4f825a57b28210e9acac476a06465e51b0f75c18a3efeb4e5de8fad2fd	String
VM		String
▶ securityTest	{ 7 fields }	Object
cStatus	finished	String
cOutput	{"Issues":{"severity":"LOW","confidence":"HIGH","rule_id":"G104","details":"Errors unhandled.","file":"/go/...	String
cResult	passed	String
startedAt	2018-12-11 12:42:47.982Z	Date
finishedAt	2018-12-11 12:43:00.909Z	Date

Repositório

Containers (Enry + Gosec)

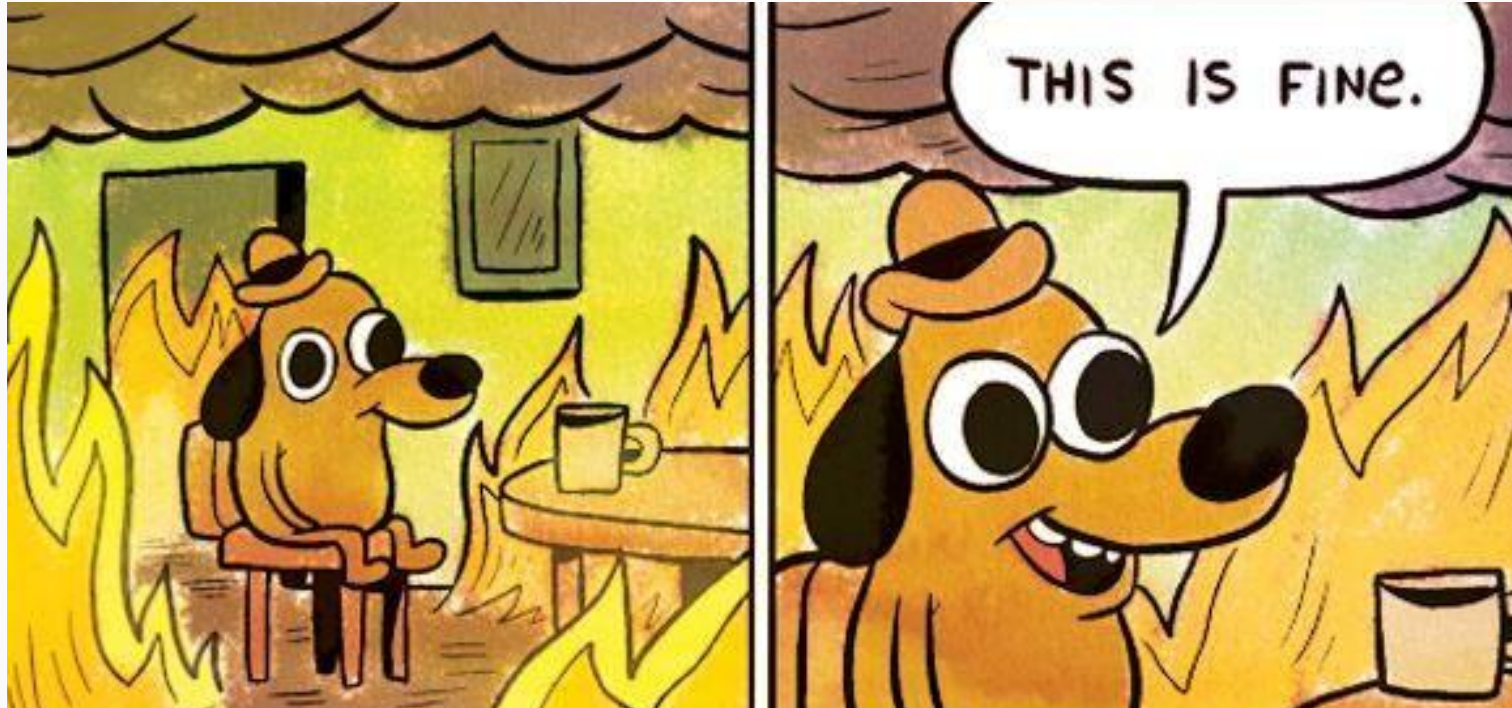
Resultados

2. Planejamento do projeto: CI config

! .gitlabci.yml x

```
1  stages:
2  |   - HuskyCI
3
4  test-huskyci:
5  |   stage: HuskyCI
6  |   script:
7  |     - wget urlto.huskyci.com/huskyci-client
8  |     - chmod +x huskyci-client
9  |     - ./huskyci-client
10
```

3. Demo



4. Resultados obtidos: SupSeg

```
Checking out 314357dd as master...
Skipping Git submodules setup
$ wget [REDACTED]/husky-ci-client
Connecting to [REDACTED]
husky-ci-client      77% | ***** | 5099k 0:00:00 ETA
husky-ci-client      100% | ***** | 6622k 0:00:00 ETA

$ chmod +x husky-ci-client
$ ./husky-ci-client
{"Issues":[{"severity":"MEDIUM","confidence":"HIGH","rule_id":"G304","details":"Potential file inclusion via variable","file":"/go/src/code/main.go","code":"os.Open(file)","line":"23"}],"Stats":{"files":1,"lines":29,"nosec":0,"found":1}}
ERROR: Job failed: exit code 1 ←
```

























4. Resultados obtidos: SupSeg

```
Cloning repository...
Cloning into '/builds/supseg/insecure-go-project'...
Checking out 53d5eed as master...
Skipping Git submodules setup
$ wget [REDACTED]/huskyci-client
Connecting to [REDACTED]
huskyci-client 100% |*****| 6658k 0:00:00 ETA

$ chmod +x huskyci-client
$ ./huskyci-client
[HUSKYCI] [*] master -> [REDACTED]/insecure-go-project.git
[HUSKYCI] [*] HuskyCI analysis started! pSMHgcM3hRlUCXHyoQsFNrWRquEw3i4R

[HUSKYCI] [*] :) ←
Job succeeded
```

4. Resultados obtidos: SupSeg

	#131230 by 	 master -> 0ed3b331  Merge branch 'update_or...	 
	#129655 by 	 master -> 2c639a76  Merge branch 'body_adju...	 
	#128972 by 	 master -> 9a15bfe3  Merge branch 'husky_feat...	 
	#128078 by  	 2.13.0 -> a5af906b  This change	 

4. Resultados obtidos: SupSeg

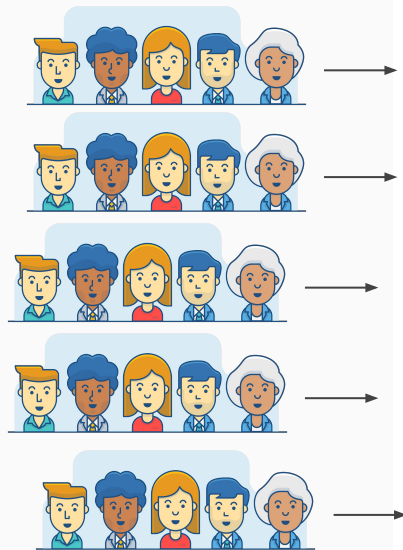
```
174 201 if __name__ == '__main__':
175     - app.config.update(
176     -     SECRET_KEY="fGh^5%21!hJ0)-pfasc23aodnaGTDAR [REDACTED]",
177     -     SESSION_COOKIE_NAME='Sessao',
178     -     PERMANENT_SESSION_LIFETIME=timedelta(minutes=60)
179     - )
```

```
157     -
158     -     db, err := util.GetDB()
159     -     if err != nil {
160     -         return nil, err
161     -     }
162     -
163     -     query := `SELECT id FROM token WHERE ` + field + ` = ? AND active = 1 `
```


4. Resultados obtidos: SupSeg

```
17 -  
18 - func openFile(file string) error {  
19 -     reader, err := os.Open(file) // vai filho  
20 -     if err != nil {  
21 -         return err  
22 -     }  
23 -     defer reader.Close()  
24 -     return nil  
25 - }
```

5. Próximos passos: Open Source!



Código Aberto!

GitHub, Inc. [US] | <https://github.com/globocom/huskyci>

README.md

HuskyCI

✓ PASSED

HuskyCI is an open source tool that performs security tests inside CI pipelines of multiple projects and centralizes all results into a database for further analysis and metrics.

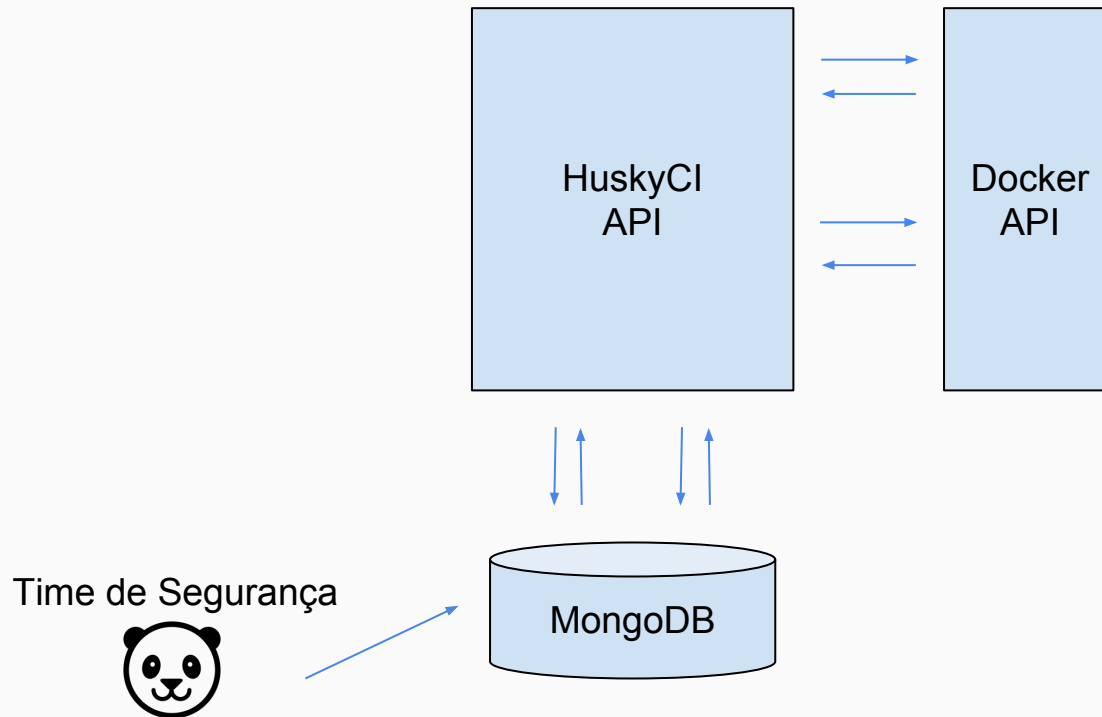
The main goal of this project is to help development teams improve the quality of their code by finding vulnerabilities as soon as possible.

How does it work?

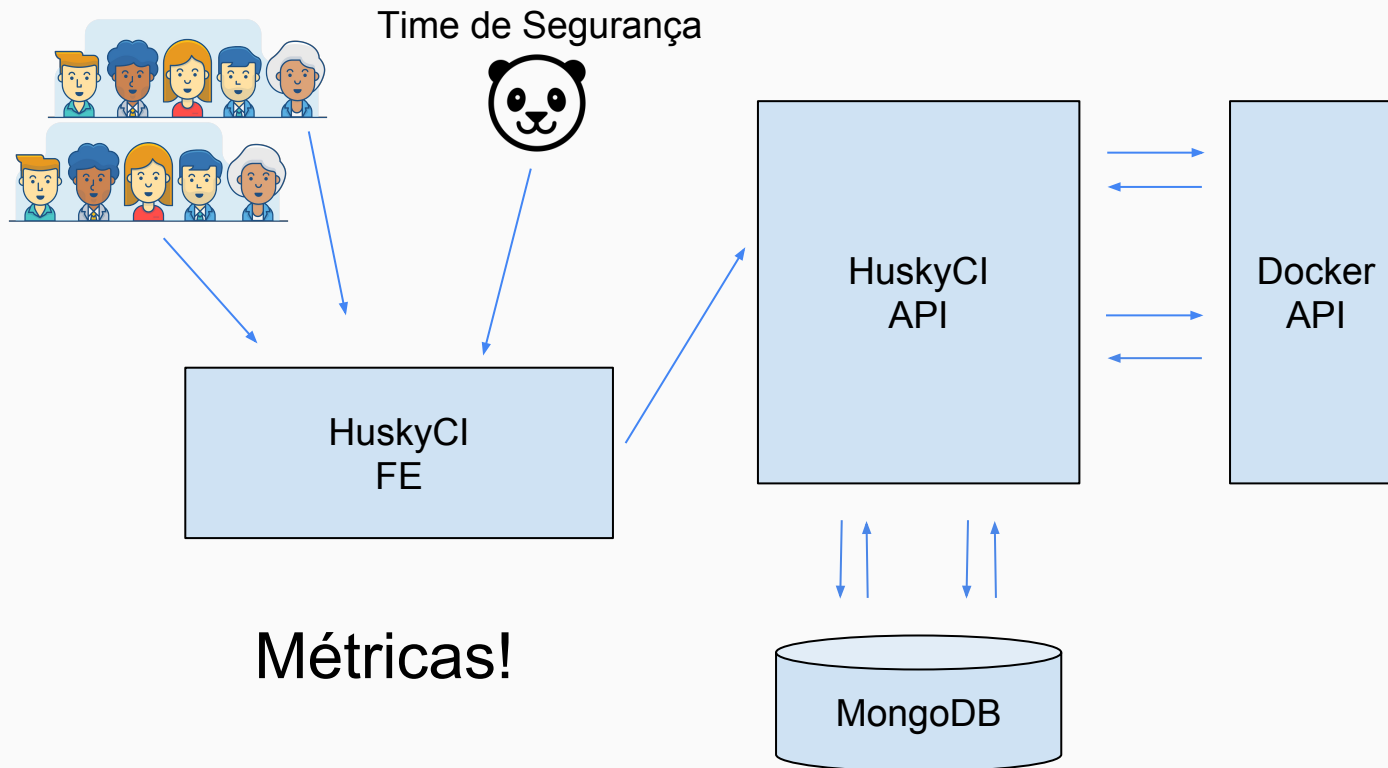
Imagine that an organization has projects like `awesome-golang-project`, `awesome-python-project` and `awesome-ruby-project`. In each project's CI configuration file, the following example code may be included:

<https://github.com/globocom/huskyci>

5. Próximos passos: Front-end

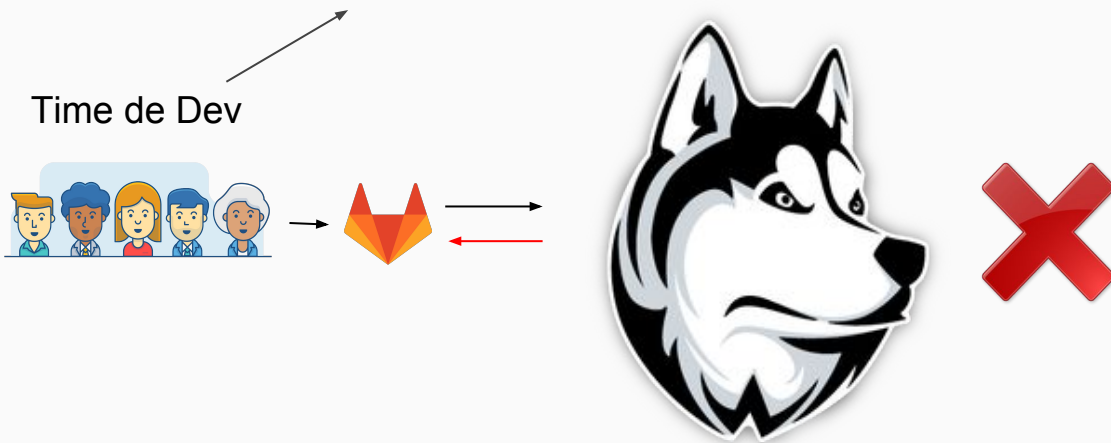


5. Próximos passos: Front-end

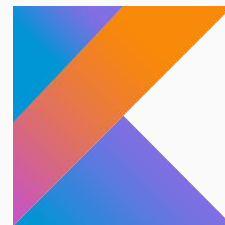


5. Próximos passos: Falso positivo

"FALSO POSITIVO! Não trave meu CI!"



5. Próximos passos: Outras linguagens



5. Próximos passos: E mais...

- Add a RetireJS security Test** feature
#127 opened 20 days ago by rafaveira3
- Adjust Makefile to stop/start/restart a single container** feature 1
#126 opened 21 days ago by rafaveira3
- Add authentication to HuskyCI** feature 1
#123 opened 21 days ago by rafaveira3
- Start documenting HuskyCI** docs let's open source!
#122 opened 26 days ago by rafaveira3
- Create an epic logo for HuskyCI** docs let's open source! 2
#120 opened 27 days ago by rafaveira3 Backlog
- Include _test files to perform tests in HuskyCI code** let's open source! test 1
#114 opened 27 days ago by rafaveira3 Backlog
- Verify if image exists and get image if it doesn't exist** feature refact
#81 opened on Oct 16 by carlosjr Super refactor ...
- Avoid connecting to MongoDB every time a huskydb.go function is called** bug 3
let's open source! refact
#76 opened on Oct 1 by rafaveira3 Super refactor ...
- Add numAnalysis into RepositoryCollection** feature 2
#73 opened on Sep 5 by rafaveira3 Backlog

<https://github.com/globocom/huskyci/issues>

globo
.com



GTS 32 | SP 12/2018

Perguntas?

Rafael Santos

rafael.santos@corp.globo.com



GTS 32 | SP 12/2018

HuskyCI:

Encontrando vulnerabilidades de código na Globo.com antes do deploy

Rafael Santos

rafael.santos@corp.globo.com