

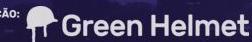
# mindthesec<sup>®</sup>

## /SÃO PAULO

MAIS UM  
EVENTO:



REALIZAÇÃO:



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

Rafael Santos

Analista de Segurança

# \$ whoami

Rafael dos Santos  @rafasantos5

[github.com/rafaveira3](https://github.com/rafaveira3)

 Volante Clássico (Camisa 5)

 OSCP + OSCE

 Analista de Segurança @

[globo.com](http://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 ...

10000000



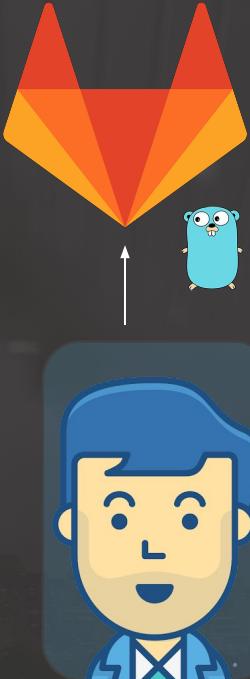
The news cards include:

- 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 Carlile, Timão tenta acelerar montagem de elenco**
- Sasha posa decotada e capricha no 'carão' para encantar fãs**
- Ghosn é acusado formalmente no Japão por violação financeira**
- Cobiçado por clubes do Brasil, Sassá seguirá no Cruzeiro, diz diretor**
- 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**

\* \* 00000001

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

10000000



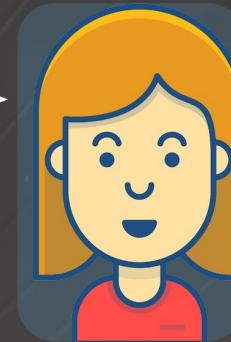
Nova feature!



Pipeline Jobs 8

Ci

- build
- iOS
- Android
- lint
- test



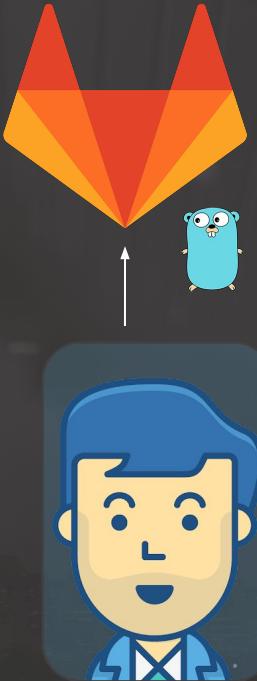
"Parece bom!"



mindthesec<sup>®</sup>  
/SÃO PAULO



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



Pipeline Jobs 8

Ci

- build
- ios
- Android
- lint
- test

Time de Segurança



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



Pipeline Jobs 8

Ci

- build
- ios
- Android
- lint
- test
- Gosec

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



Pipeline Jobs 8

Ci

- build
- ios
- Android
- lint
- test

Time de Segurança



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



Pipeline Jobs 8

Ci

- build
- ios
- Android
- lint
- test
- Brakeman

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



Nova feature!

Pipeline Jobs 8

Ci

- build
- ios
- Android
- lint
- test

Time de Segurança



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



Pipeline Jobs 8

Ci

- build
- ios
- Android
- lint
- test
- huskyCI

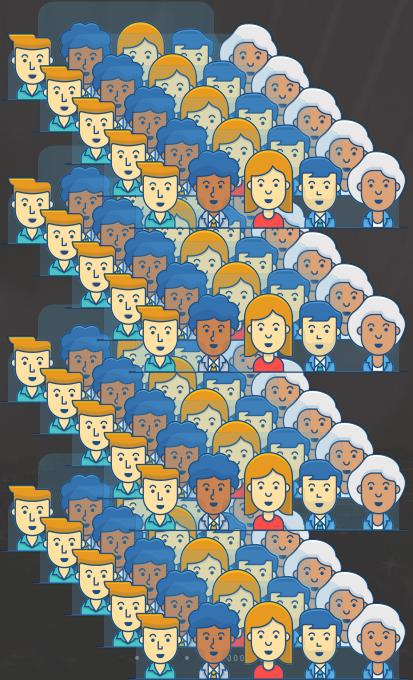


**Um dia na vida de uma grande organização ...**

# Um dia na vida de uma grande organização ...

10000000

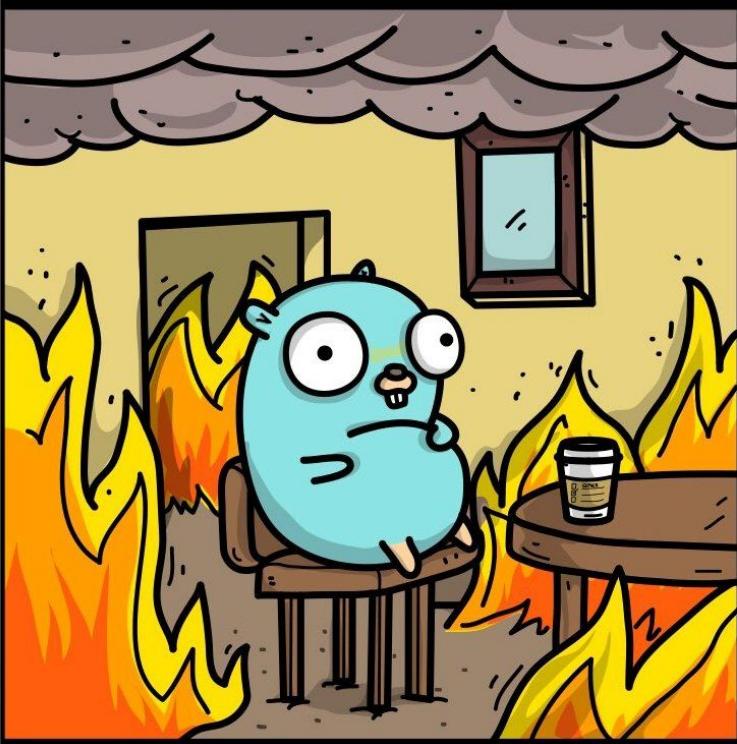
## Times de Desenvolvimento



## Time de Segurança

A circular collage containing several news snippets from a news website. The snippets include:

- Ronaldo chama Messi para jogar na Itália: '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 dectada e capricha no 'cárão' para encantar fãs
- Cobiçado por clubes do Brasil, Sessá seguirá no Cruzeiro, diz diretoria
- Gavassi mostra Bruna 'desesperada' em show de Sandy; vídeo
- Alok passa mal durante show no Festival de Verão e relata suspeita de zika



Let's hack! 



mindthesec<sup>®</sup>  
/SÃO PAULO

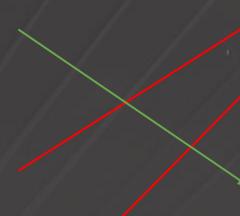
# Let's hack!

10000000

## Times de Desenvolvimento



## Time de Segurança



# Let's hack!

10000000

## Times de Desenvolvimento



## Time de Segurança



**mindthesec**  
/SÃO PAULO

\* \* \* 00000001

# Let's hack!

10000000

## Times de Desenvolvimento



## Time de Segurança



**mindthesec**  
/SÃO PAULO

\* \* \* 00000001

# Let's hack!

10000000

## Times de Desenvolvimento



## Time de Segurança



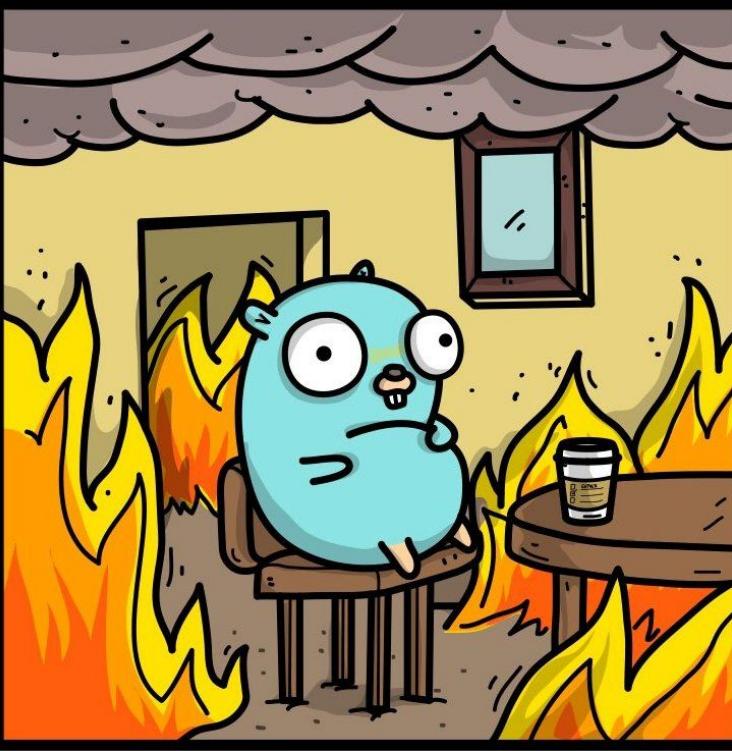
10000000  
00000001

# Beleza, mas quais linguagens usamos?



# Beleza, mas quais linguagens usamos?





mindthesec  
/SÃO PAULO

# Beleza, mas quais linguagens usamos?

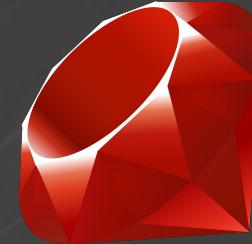
10000000



gosec  
00000001



Bandit  
00000001



Brakeman  
00000001

mindthesec<sup>®</sup>  
/SÃO PAULO

Como queremos construir esta ferramenta?



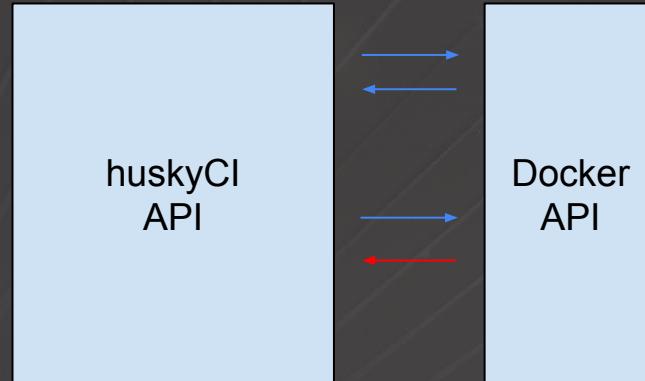
# Como queremos construir esta ferramenta?

Time de Desenvolvimento



# Como queremos construir esta ferramenta?

Time de Desenvolvimento



Time de Segurança

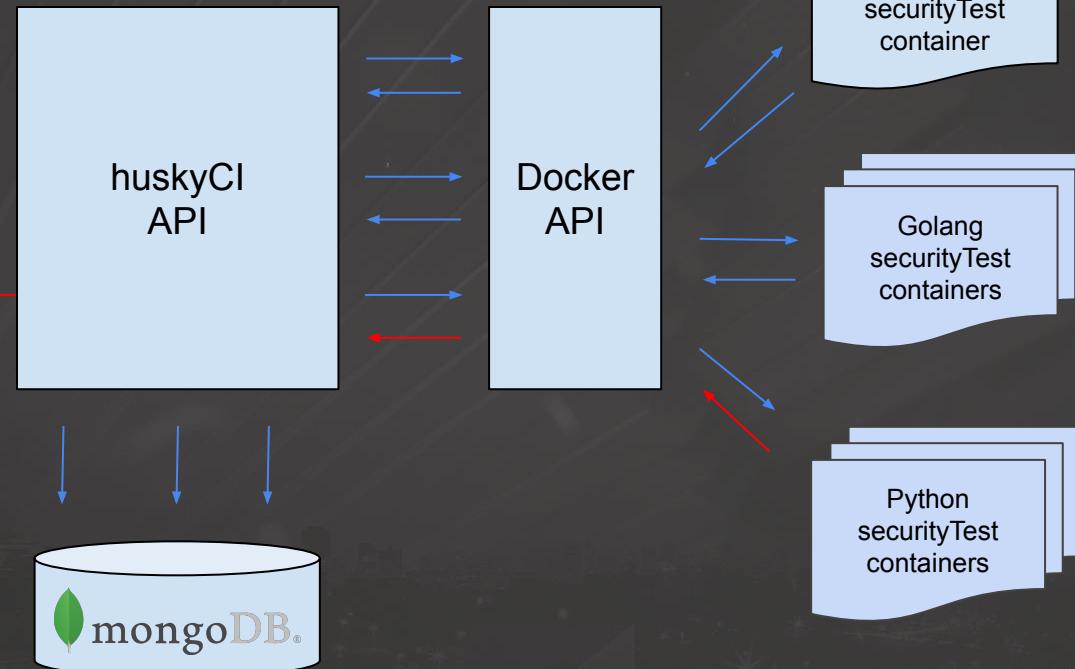


# Como queremos construir esta ferramenta?

Time de Desenvolvimento



Time de Segurança



E o que gostaríamos de ver? 

# E o que gostaríamos de ver?

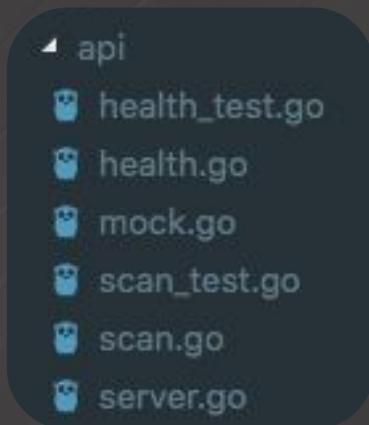
10000000



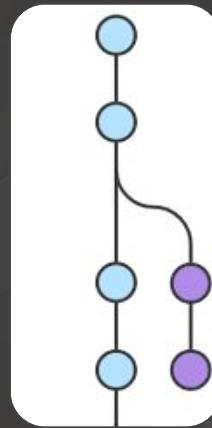
Autores de  
commit



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

HuskyCI: failed



HuskyCI: passed



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
▼	huskyresults	{ 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 (Entry + Gosec)

Resultados

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

# ! .gitlabci.yml ✘

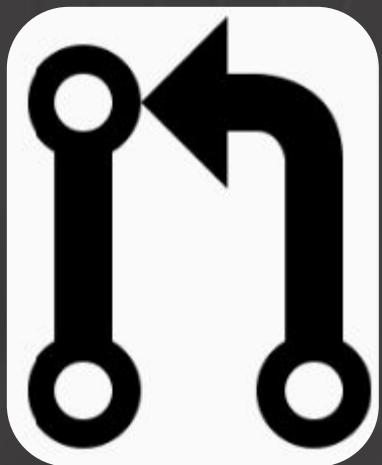
```
1 stages:
2   - HuskyCI
3
4 test-huskyci:
5   stage: HuskyCI
6   script:
7     - wget urlto.huskyci.com/huskyci-client
8     - chmod +x huskyci-client
9     - ./huskyci-client
10
```

Demo 🔥

# Resultados Globo.com (até agora)

# Resultados Globo.com (até agora)

10000000



projetos "beta" com  
huskyCI



~65 repositórios únicos

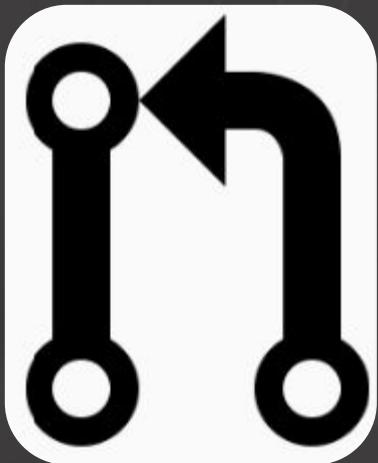
~30 análises por dia



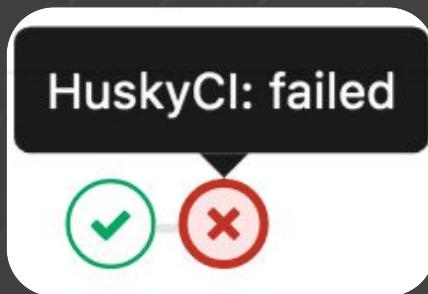
~180 branches únicas

# Resultados Globo.com (até agora)

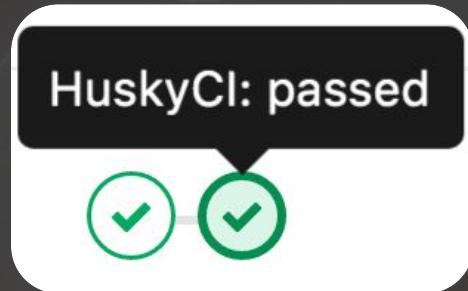
10000000



projetos "beta" com  
huskyCI



~20% falhou



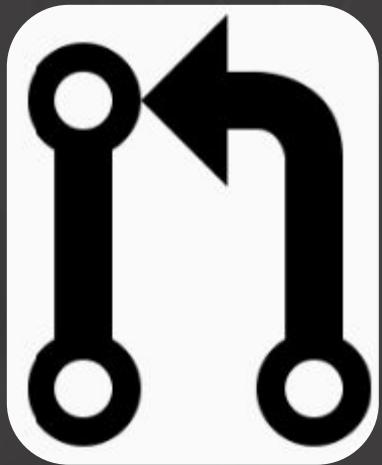
~52% passou

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

~28% errou

# Resultados Globo.com (até agora)

100000000



projetos "beta" com  
huskyCI



14.6  
segundos



13.8  
segundos



7.1  
minutos



7.1  
segundos



BANDIT  
13.2  
segundos

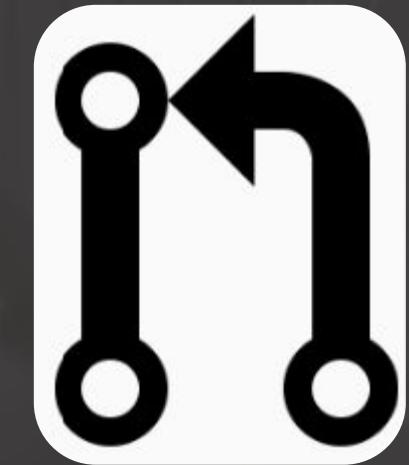


8.3  
segundos

mindthesec<sup>®</sup>  
/SÃO PAULO

00000001

# Resultados Globo.com (até agora)



projetos "beta" com  
huskyCI



"error unhandled"



dependências vulneráveis



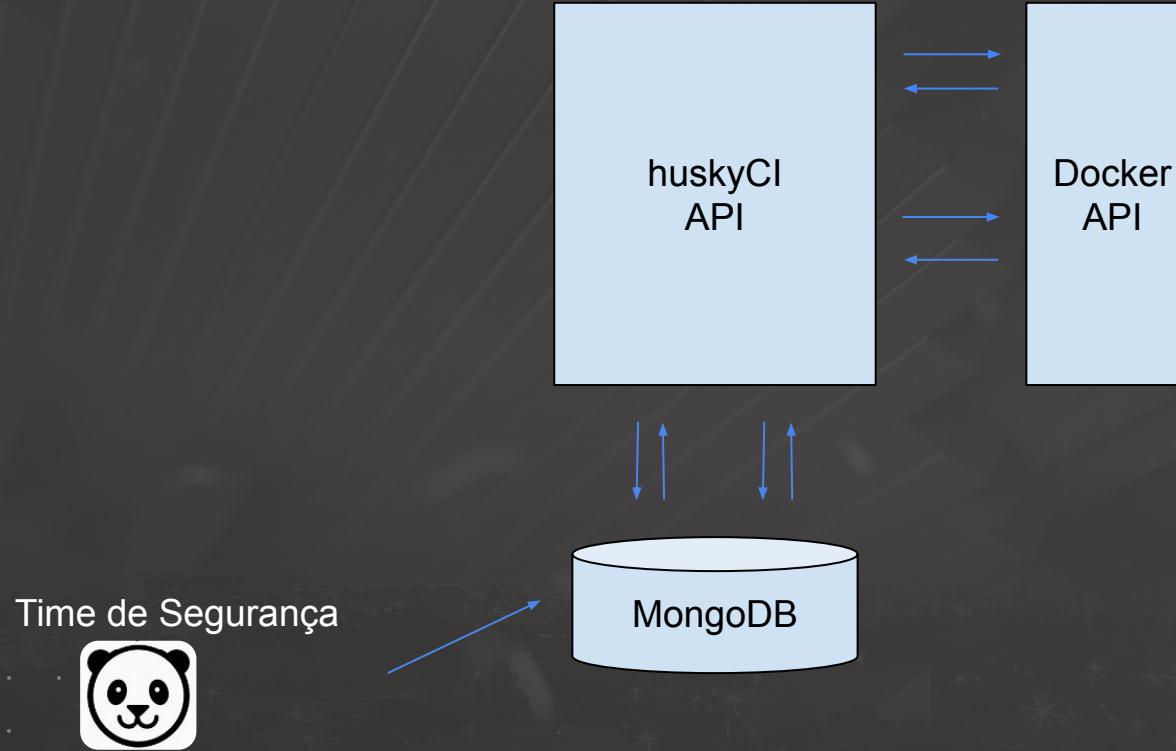
dependências vulneráveis



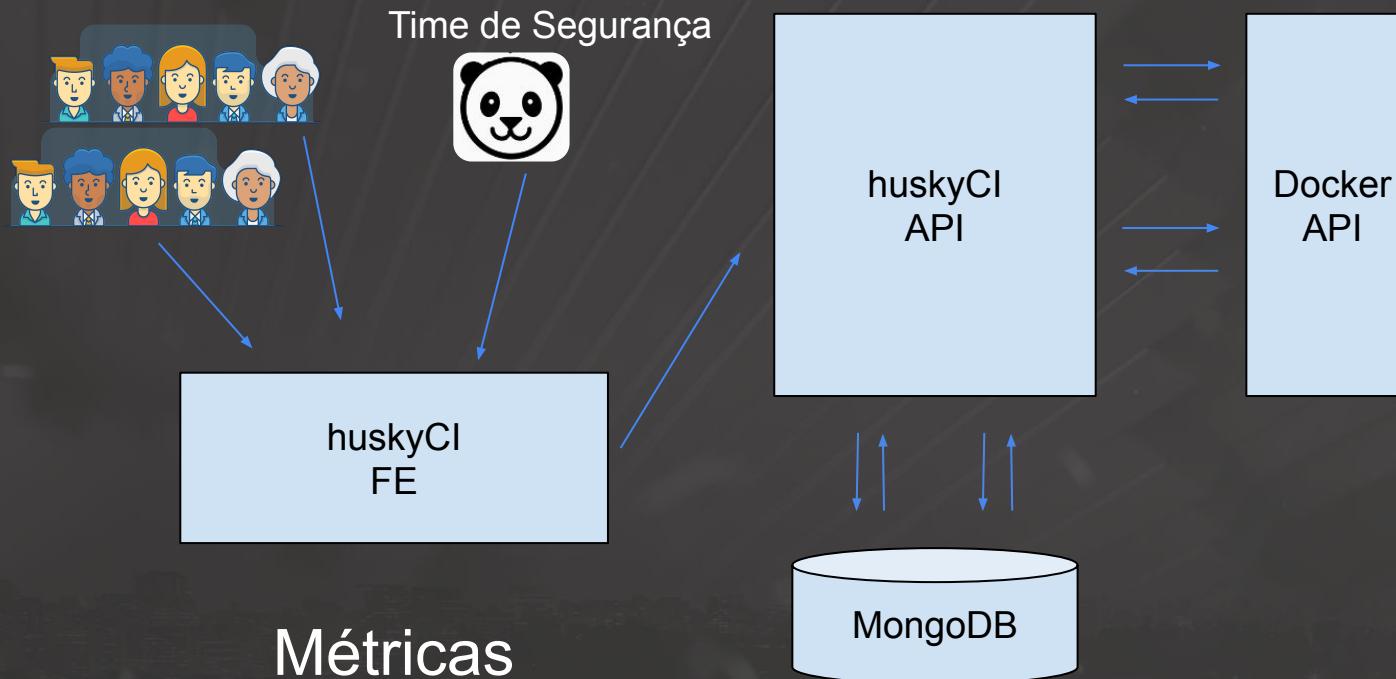
dependências vulneráveis

Próximas etapas 

# Próximas etapas: Front-end



# Próximas etapas: Front-end



# Próximas etapas: Integração com o SonarQube

10000000



0000001

# Próximas etapas: Suportar mais linguagens



# Próximas etapas: Contribuir para as ferramentas Open Source



Safety

Retire.js

# Próximas etapas: Adicionais mais Security Tests

10000000



## Security Code Scan



CHECKMARX

SpotBugs



Awesome Static Analysis!

Awesome DevSecOps 

00000001

mindthesec<sup>®</sup>  
/SÃO PAULO

# Próximas etapas: E muito mais!

10000000

<input type="checkbox"/> ⓘ 21 Open ✓ 95 Closed	Author ▾	Labels ▾	Projects ▾	Milestones ▾	Assignee ▾	Sort ▾
<input type="checkbox"/> ⓘ Use Qualitative Severity Rating Scale (CVSS 3.0) in HuskyCI/Vulnerabilities <span>feature-request</span> #316 opened 4 days ago by rafaveira3						
<input type="checkbox"/> ⓘ Refactor huskyCI-Client to consume new Analysis Output <span>refact</span> #314 opened 5 days ago by rafaveira3						
<input type="checkbox"/> ⓘ Add yarn support for other dependencies libraries <span>refact</span> #292 opened 18 days ago by Krlier						
<input type="checkbox"/> ⓘ Add commit author into Analysis struct <span>feature-request</span> #286 opened 19 days ago by rafaveira3						
<input type="checkbox"/> ⓘ Add container version into Container struct <span>feature-request</span> #259 opened on Jun 14 by rafaveira3					1	
<input type="checkbox"/> ⓘ Create an env var to enable or not containers to be "cleaned" after some time <span>feature-request</span> #252 opened on Jun 7 by rafaveira3						
<input type="checkbox"/> ⓘ Start building a huskyCI Front-End to consume database metrics <span>feature-request</span> <span>help wanted</span> 🙋 #251 opened on Jun 7 by gildasio					1	

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

**mindthesec**  
/SÃO PAULO

# Próximas etapas: E muito mais!



Open Source

huskyCI - Performing security tests inside your CI

huskyCI

coverage 20% PASSED chat on gitter

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.

<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/talentosqcom/>
- [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](https://gitlab.com/rafaveira3/appsec-defcon27-huskyci/merge_requests)

# PERGUNTAS

# AGRADECIMENTO

[rafael.santos@corp.globo.com](mailto:rafael.santos@corp.globo.com)

@rafasantos5

00000001