Village

Aug, 2019

Finding security flaws in CI before deploying them

Rafael dos Santos 🇧🇷 @rafasantos5

$ whoami

Rafael dos Santos 🇧🇷 @rafasantos5
github.com/rafaveira3

⚽ Left Winger

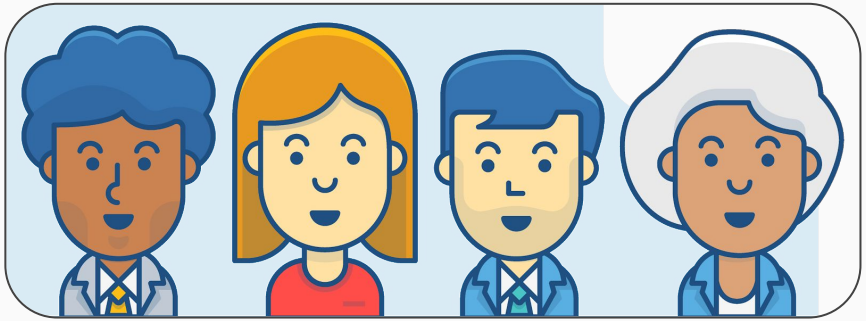
☕ OSCP + OSCE

🐼 Security Engineer @ globo.com

🚀 Sec Tools + Exploit Development

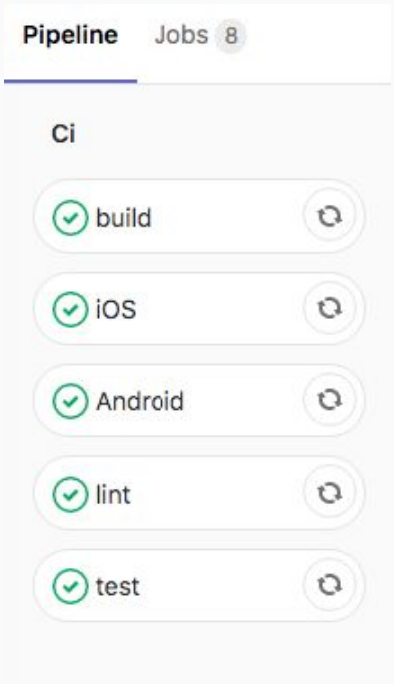
A day in the life of a…
development team

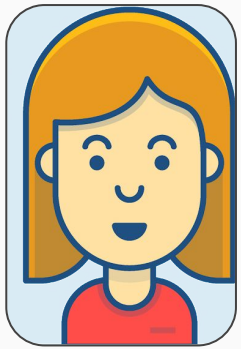
A day in the life of a... development team



A day in the life of a... development team

"Awesome feature!!!!"

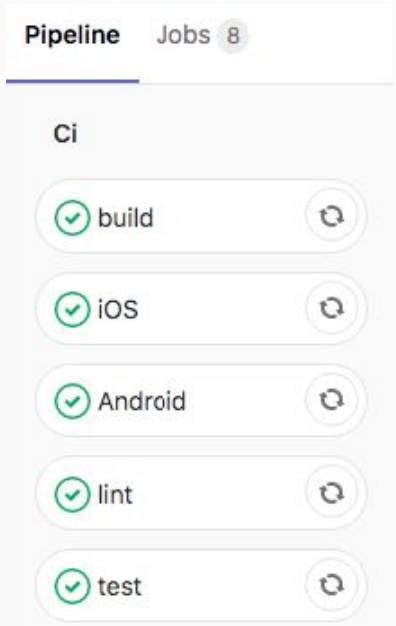




"Sounds good to me!"

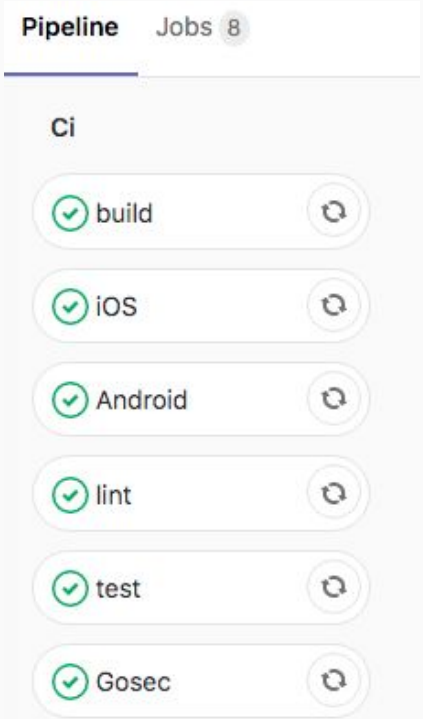
A day in the life of a... development team

"Awesome feature!!!!"

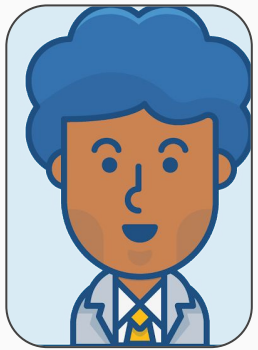


Security Team

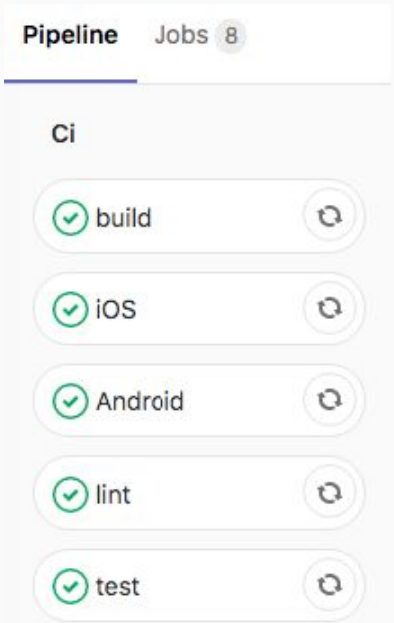
"Hey, what about using **gosec**?"



A day in the life of a... development team

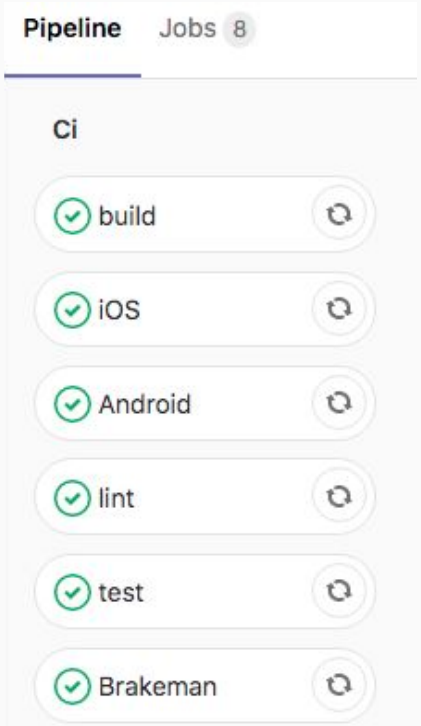


"Awesome feature!!!!"

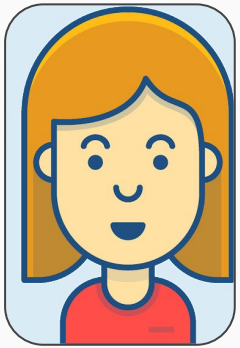


Security Team

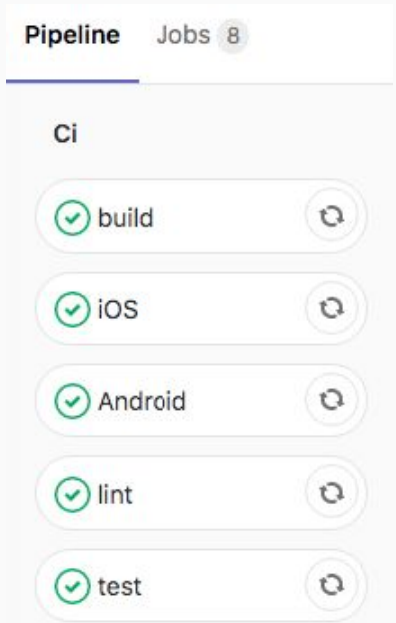
"Hey, what about using **Brakeman**?"



A day in the life of a... development team

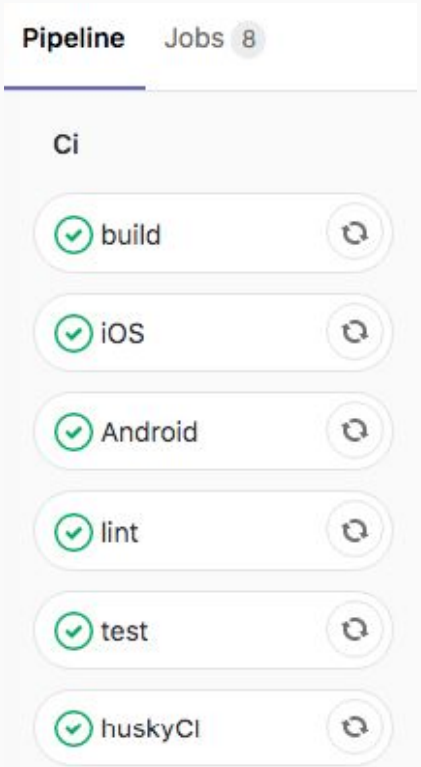


"Awesome feature!!!!"



Security Team

"Hey, what about using ... ?"

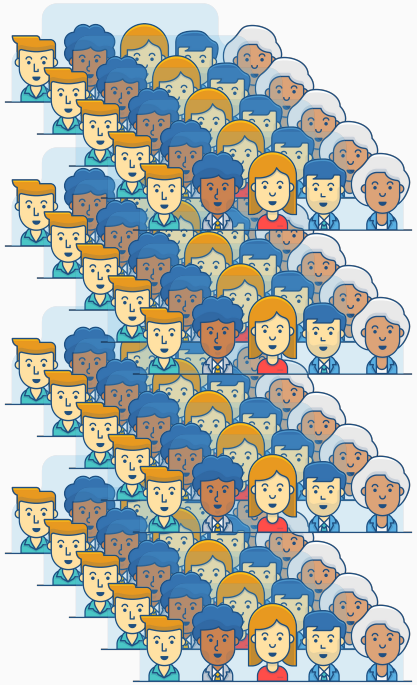


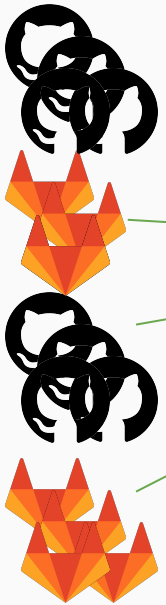
A day in the life of a…
big organization

A day in the life of a... big organization

Village

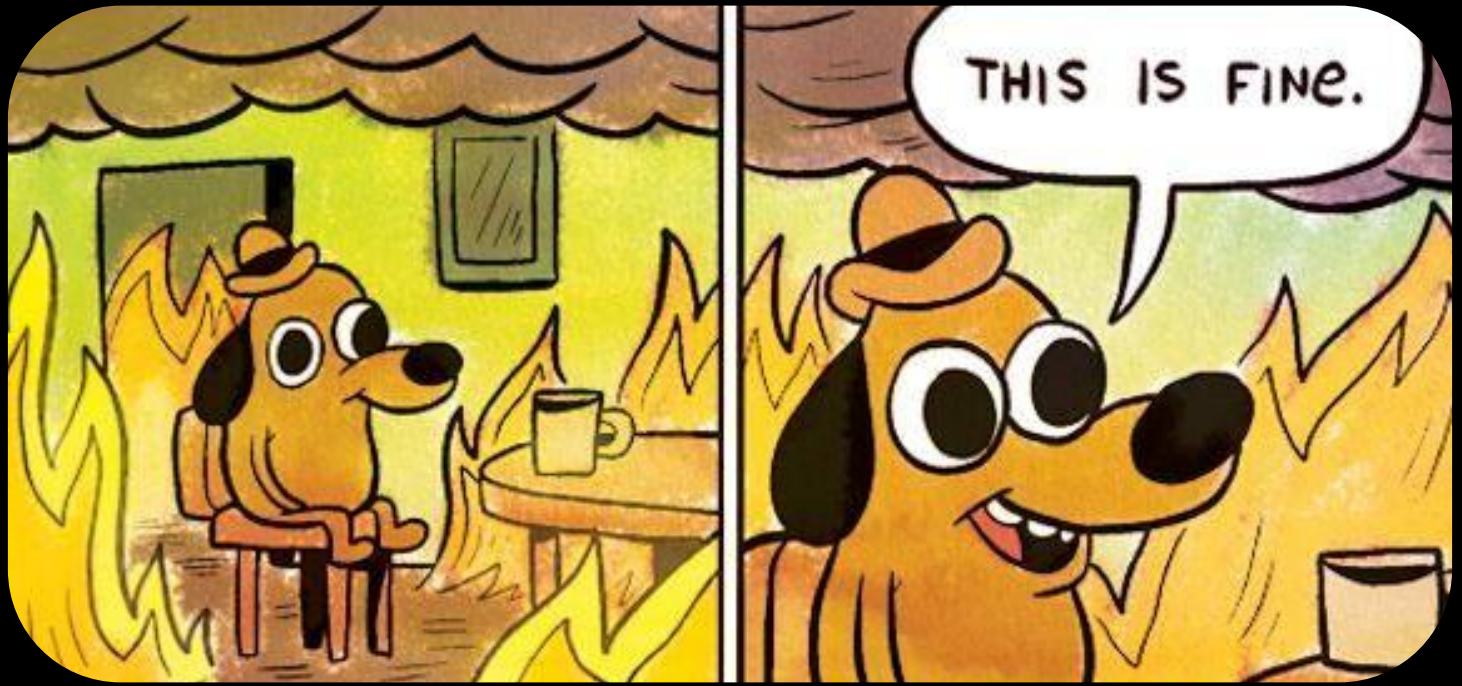
Development Teams





Security Team

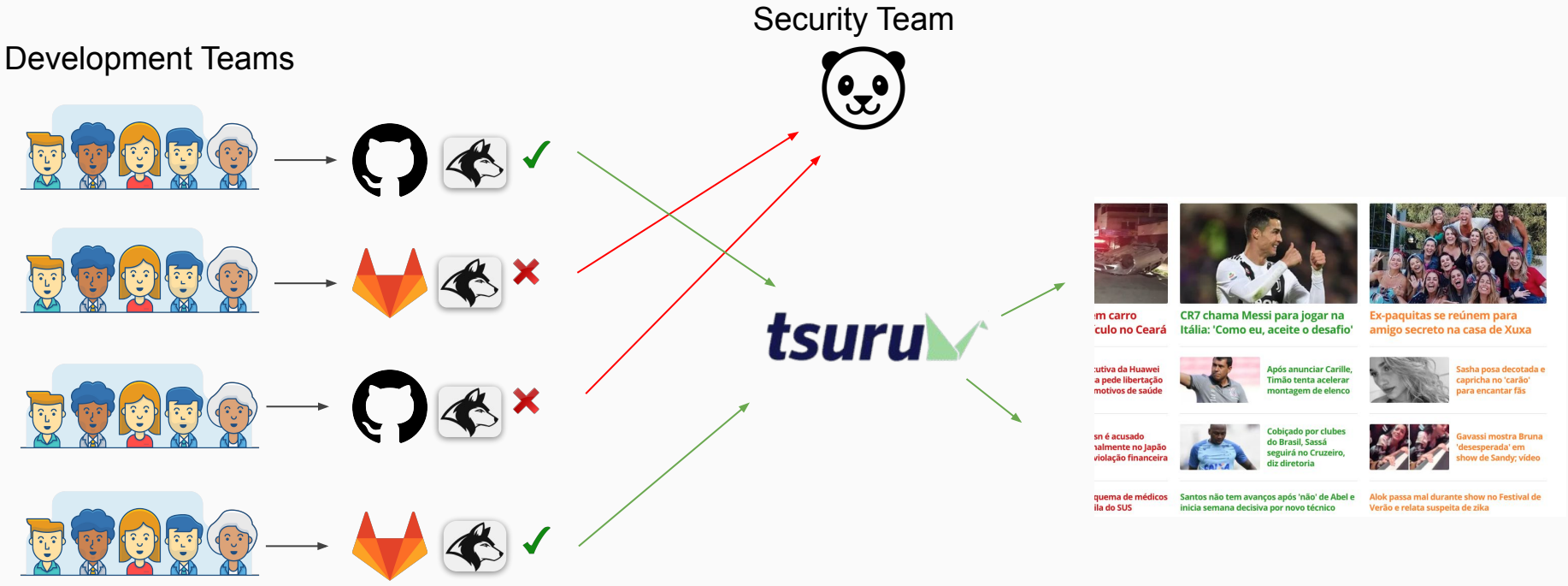
tsuru


THIS IS FINE.

Let's hack! 🐼

Let's hack!

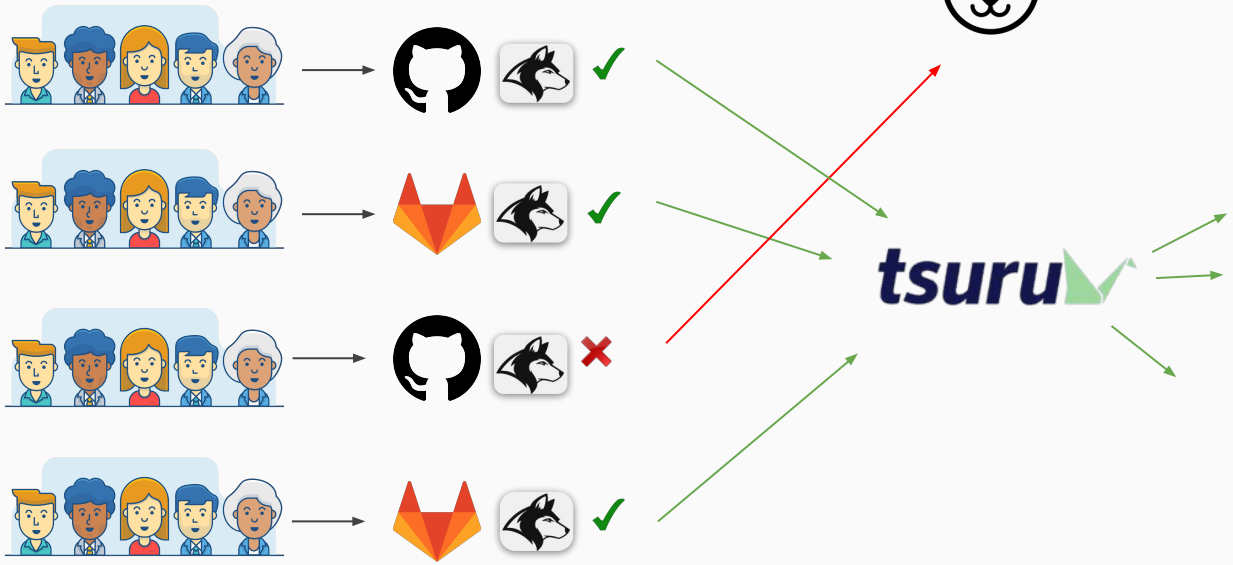
Let's hack!


Development Teams
Security Team
tsuru
CR7 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 decotada e capricha no 'carão' para encantar fãs
Cobiçado por clubes do Brasil, Sassá seguirá no Cruzeiro, diz diretoria
Gavassi mostra Bruna 'desesperada' em show de Sandy; vídeo
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

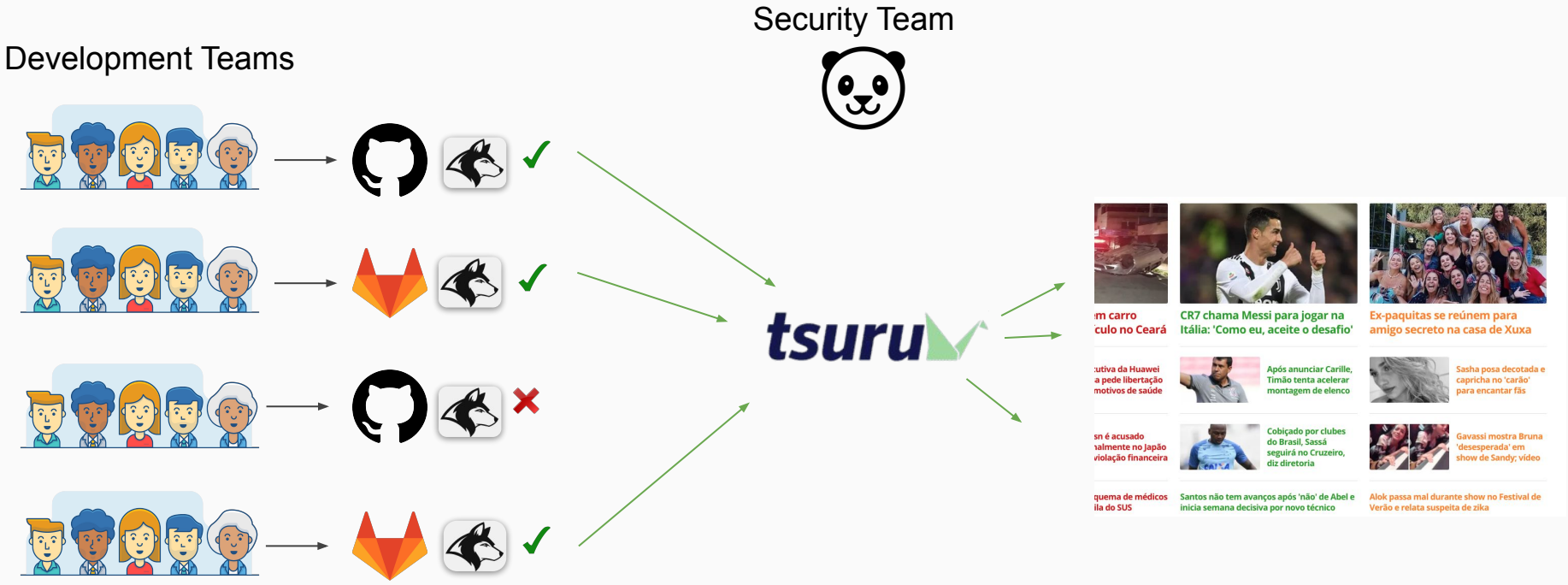
Let's hack!

Development Teams

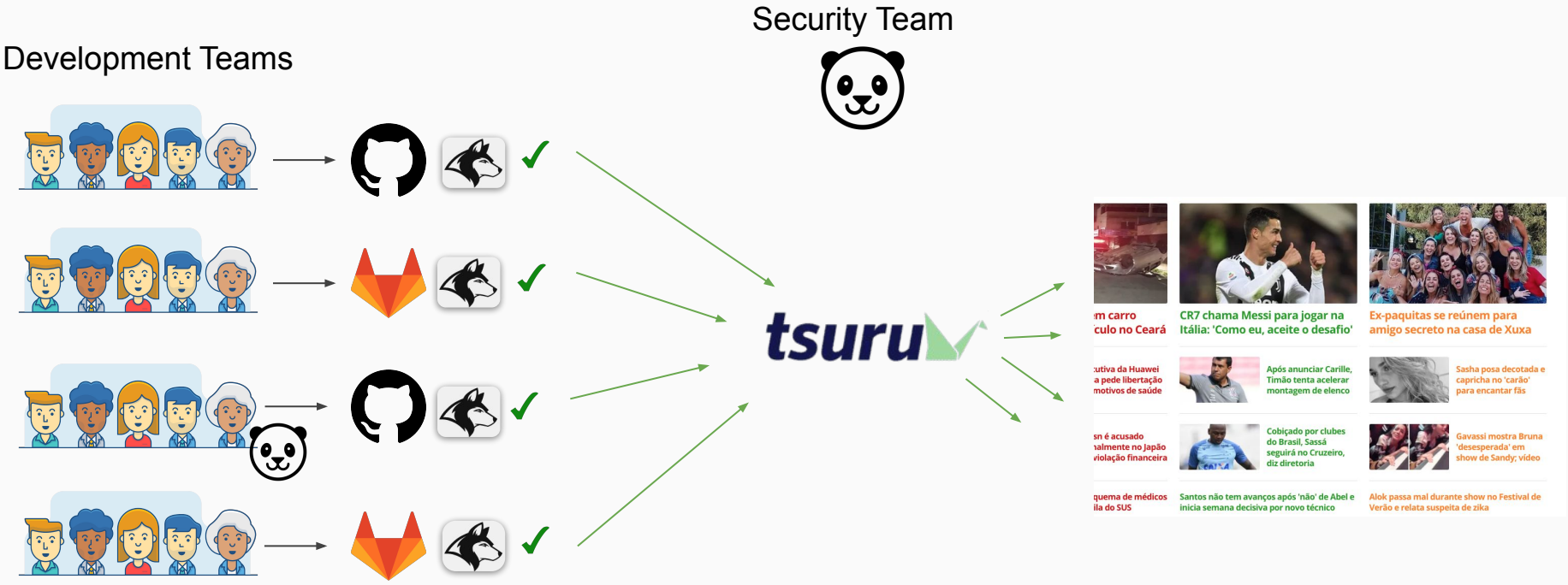
Security Team



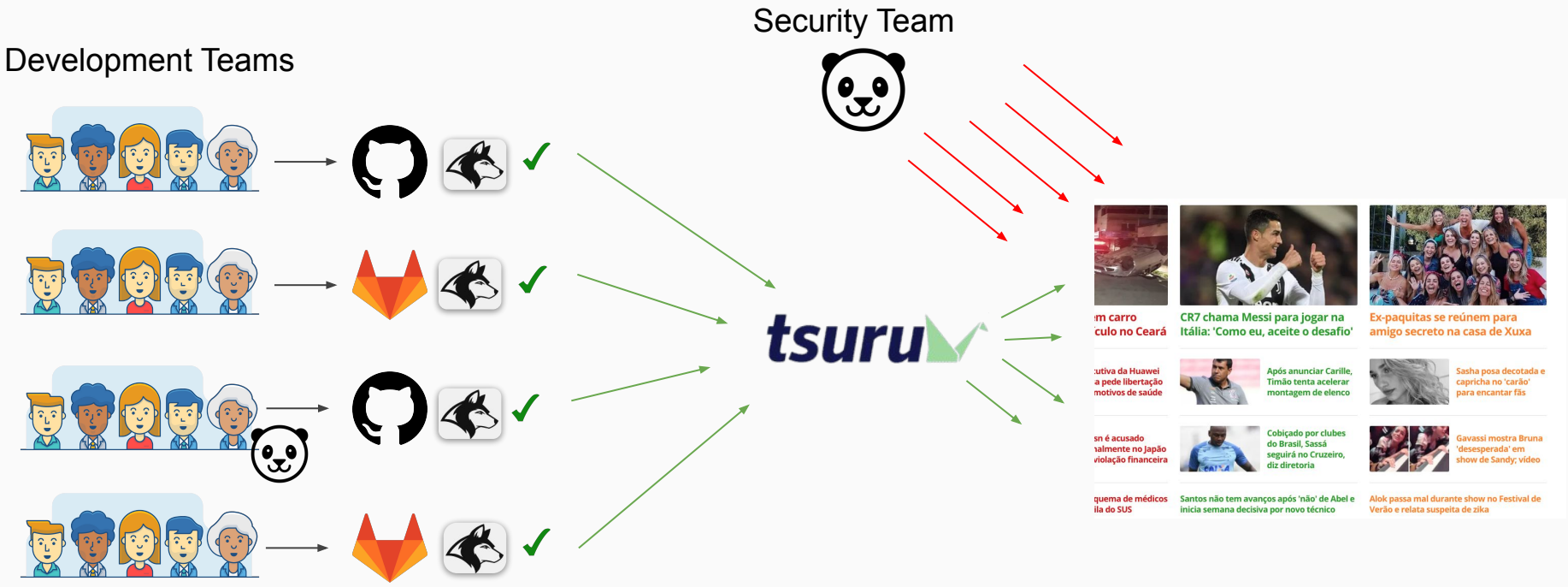
Let's hack!


Development Teams
Security Team
tsuru
CR7 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 decotada e capricha no 'carão' para encantar fãs
Cobiçado por clubes do Brasil, Sassá seguirá no Cruzeiro, diz diretoria
Gavassi mostra Bruna 'desesperada' em show de Sandy; vídeo
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

Let's hack!

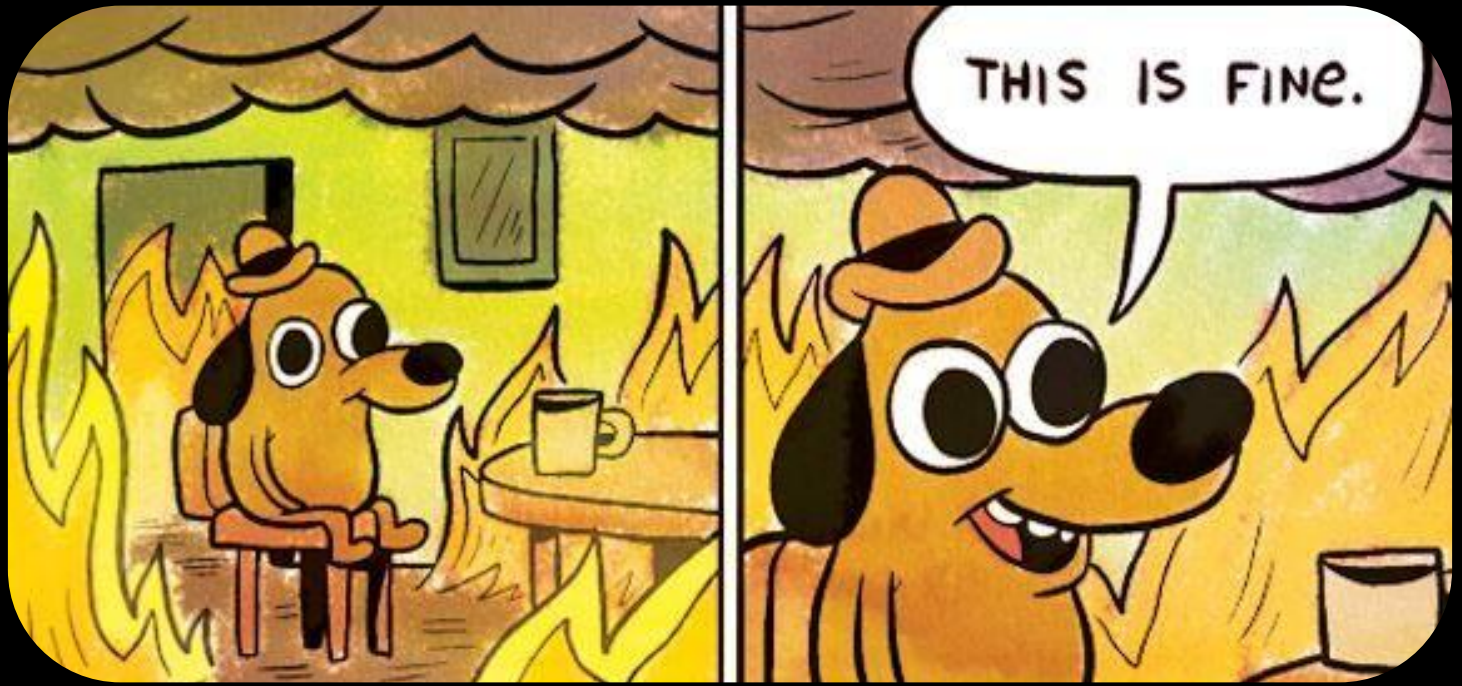

Development Teams
Security Team
tsuru
CR7 chama Messi para jogar na Itália: 'Como eu, aceite o desafio'
Ex-paquitas se reúnem para amigo secreto na casa de Xuxa
Após anunciar Carille, Timão tenta acelerar montagem de elenco
Sasha posa decotada e capricha no 'carão' para encantar fãs
Cobiçado por clubes do Brasil, Sassá seguirá no Cruzeiro, diz diretoria
Gavassi mostra Bruna 'desesperada' em show de Sandy; vídeo
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

Let's hack!


Development Teams
Security Team
tsuru
CR7 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 decotada e capricha no 'carão' para encantar fãs
Cobiçado por clubes do Brasil, Sassá seguirá no Cruzeiro, diz diretoria
Gavassi mostra Bruna 'desesperada' em show de Sandy; vídeo
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

Ok, what are we coding? ☕

Ok, what are we coding?


THIS IS FINE.

Ok, what are we coding?

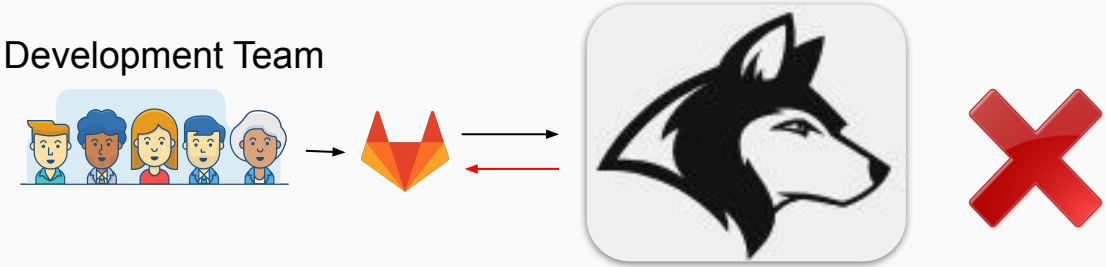
gosec

Bandit

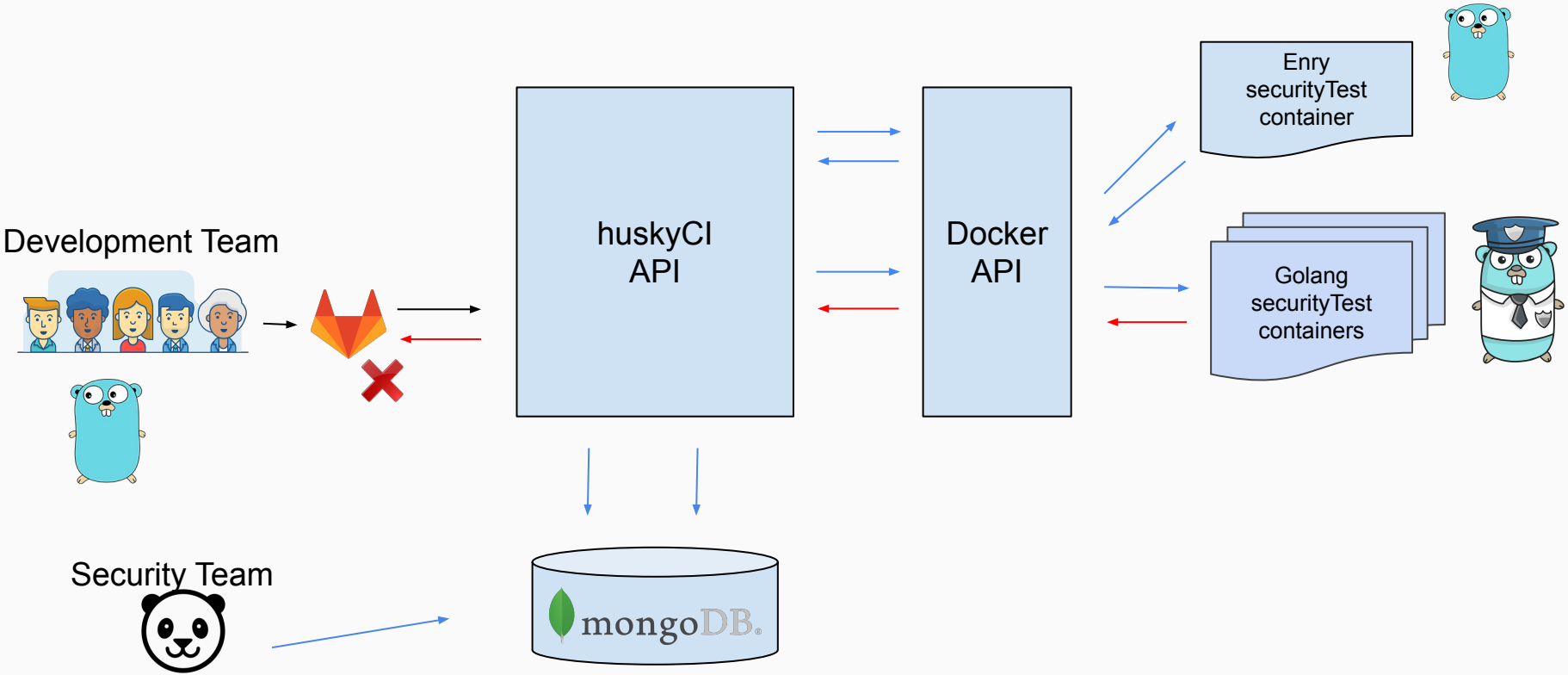
Brakeman

How can we build this? 🛠️

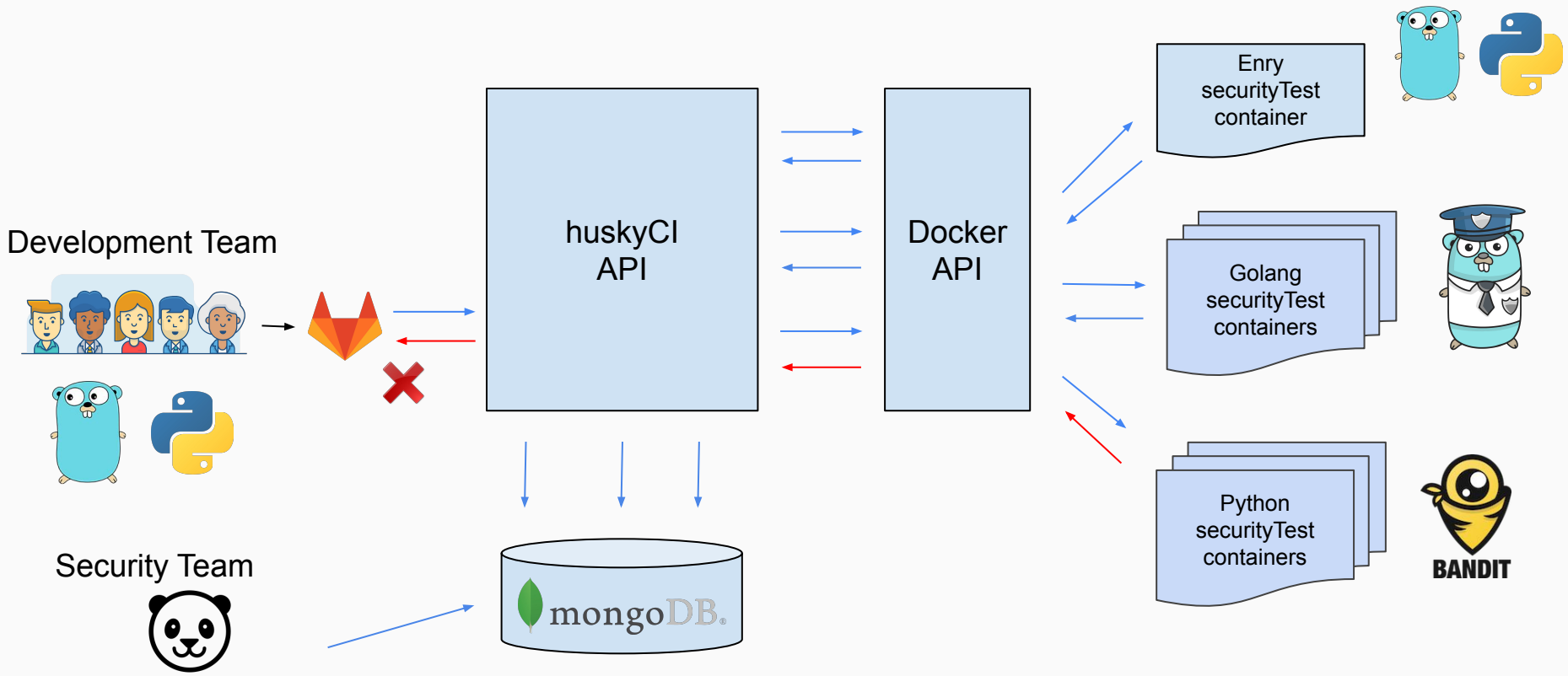
How can we build this?



How can we build this?



How can we build this?

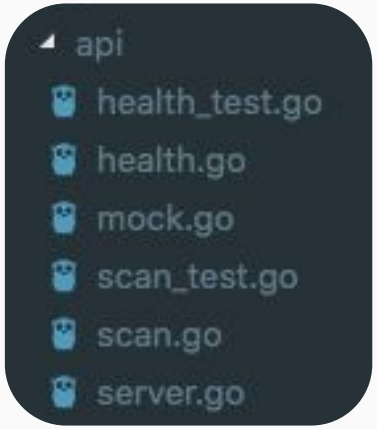


And what would we like to see? 👀

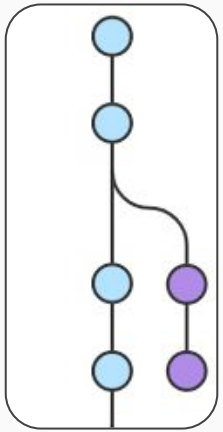
And what would we like to see?

Commit Author(s)

Repository Language(s)



File(s) Found

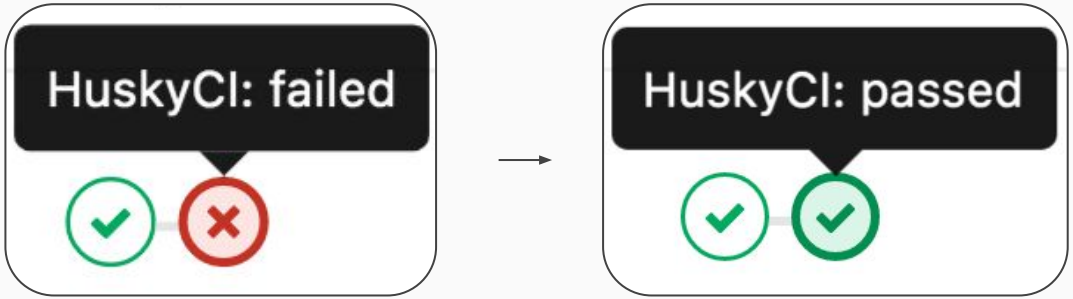


Branch Name

And what would we like to see?

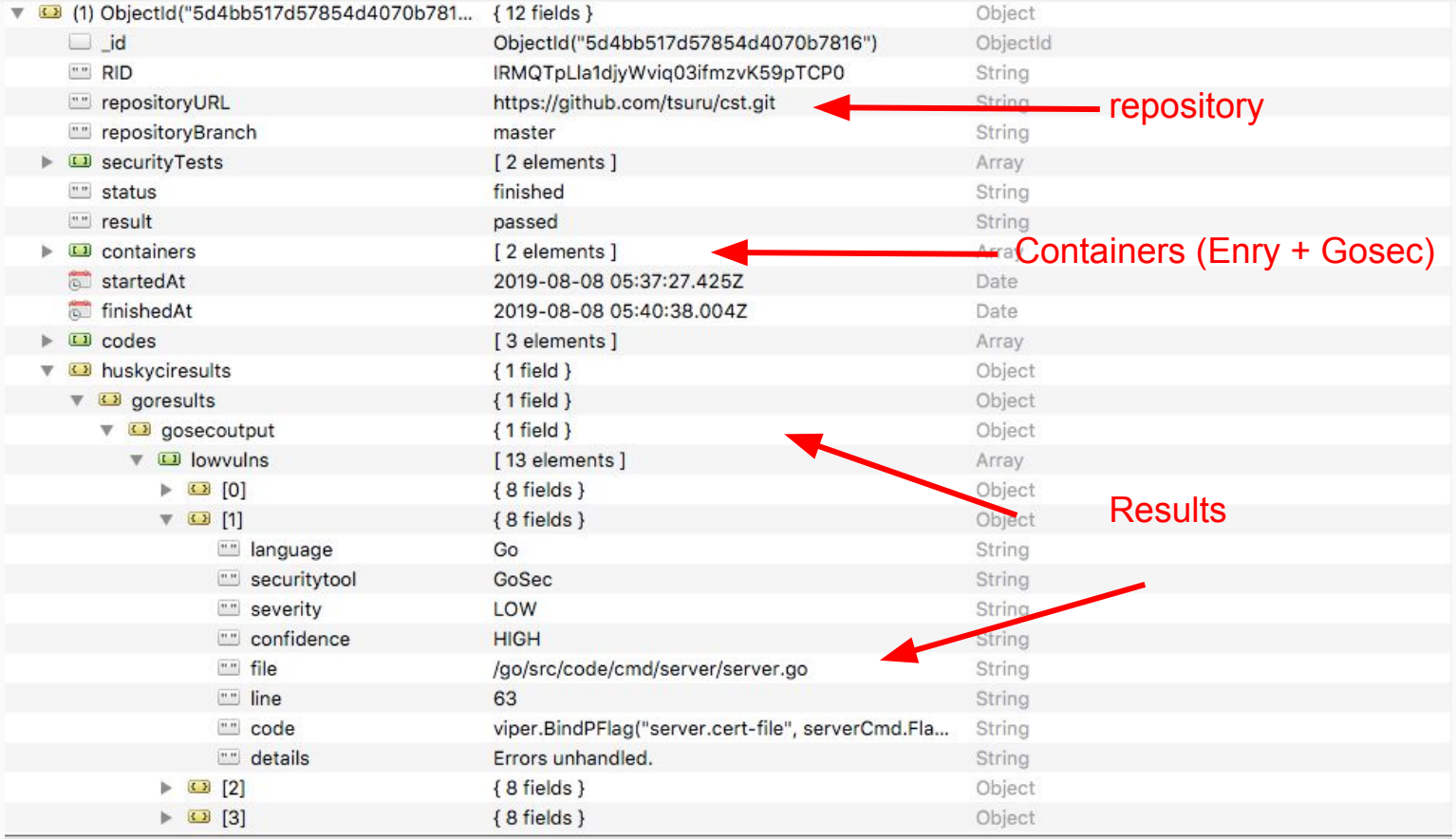
```
[HUSKYCI][!] Severity: MEDIUM
[HUSKYCI][!] Confidence: HIGH
[HUSKYCI][!] Details: Blacklisted import crypto/sha1: weak cryptographic primitive
[HUSKYCI][!] File: /go/src/code/api/token.go
[HUSKYCI][!] Line: %!d(string=6)
[HUSKYCI][!] Code: "crypto/sha1"
```

Vulnerabilities



Mitigations

And what would we like to see?



(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

And what would we like to see?


```
✔ [02:37] rafael.santos@labs:~/go/src/github.com/globocom/huskyCI (master)
$ make run-client-json
{"goresults":{"gosecoutput":[{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/cmd/server/server.go","line":"61","code":"serverCmd.MarkFlagRequired(\"database\")","details":"Errors unhandled."},{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/cmd/server/server.go","line":"63","code":"viper.BindPFlag(\"server.cert-file\", serverCmd.Flags().Lookup(\"cert-file\"))","details":"Errors unhandled."},{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/cmd/server/server.go","line":"64","code":"viper.BindPFlag(\"server.key-file\", serverCmd.Flags().Lookup(\"key-file\"))","details":"Errors unhandled."},{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/cmd/server/server.go","line":"65","code":"viper.BindPFlag(\"server.port\", serverCmd.Flags().Lookup(\"port\"))","details":"Errors unhandled."},{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/cmd/server/server.go","line":"66","code":"viper.BindPFlag(\"server.database\", serverCmd.Flags().Lookup(\"database\"))","details":"Errors unhandled."},{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/cmd/server/server.go","line":"67","code":"viper.BindPFlag(\"server.insecure\", serverCmd.Flags().Lookup(\"insecure\"))","details":"Errors unhandled."},{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/cmd/worker/worker.go","line":"45","code":"workerCmd.MarkFlagRequired(\"database\")","details":"Errors unhandled."},{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/cmd/worker/worker.go","line":"46","code":"workerCmd.MarkFlagRequired(\"clair-address\")","details":"Errors unhandled."},{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/cmd/worker/worker.go","line":"48","code":"viper.BindPFlag(\"worker.database\", workerCmd.Flags().Lookup(\"database\"))","details":"Errors unhandled."},{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/cmd/worker/worker.go","line":"49","code":"viper.BindPFlag(\"worker.clair.address\", workerCmd.Flags().Lookup(\"clair-address\"))","details":"Errors unhandled."},{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/scan/worker/default.go","line":"35","code":"job.Error(err)","details":"Errors unhandled."},{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/scan/worker/default.go","line":"61","code":"job.Error(err)","details":"Errors unhandled."},{"language":"Go","securitytool":"GoSec","severity":"LOW","confidence":"HIGH","file":"/go/src/code/scan/worker/default.go","line":"66","code":"job.Success(results)","details":"Errors unhandled."}]},"pythonresults":{},"javascriptresults":{},"rubyresults":{},"summary":{"repositoryURL":"https://github.com/tsuru/cst.git","repositoryBranch":"master","RID":"IRMQTpLla1djyWviq03ifmzvK59pTCP0","gosecsummary":{"foundinfo":true,"lowvuln":13},"banditsummary":{},"safetysummary":{},"retirejssummary":{},"npmauditsummary":{},"brakemansummary":{},"totalsummary":{"foundinfo":true,"lowvuln":13}}}
✔ [02:41] rafael.santos@labs:~/go/src/github.com/globocom/huskyCI (master)
$
```

Focus on coding... We got you, dev

❤️

Focus on coding... We got you, dev

.gitlabci.yml

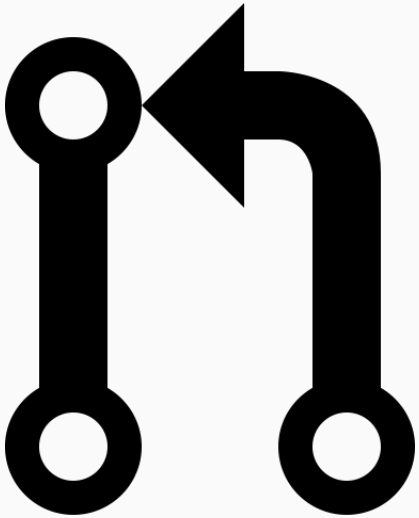
```
stages:
  - HuskyCI

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

Demo 🔥

Show me what you got (so far) 🚀

Show me what you got (so far)

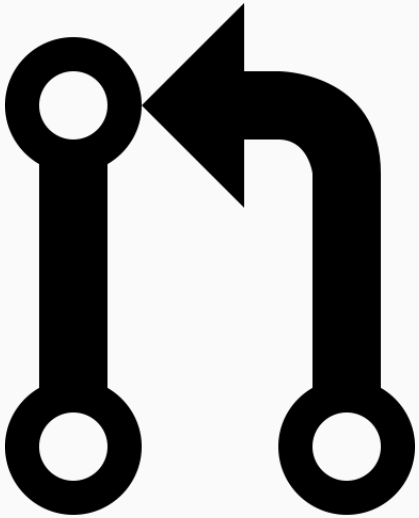


beta globo.com
projects with huskyCI

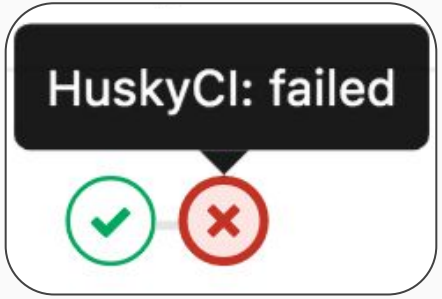
~65 unique repositories

~180 unique branches

Show me what you got (so far)



beta globo.com
projects with huskyCI



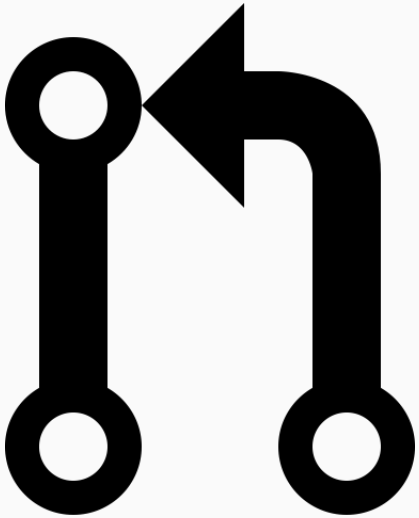
~20% failed

~52% passed

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

~28% errors

Show me what you got (so far)



beta globo.com
projects with huskyCI

14.6
seconds

13.8
seconds

7.1
minutes

Safety

7.1
seconds

13.2
seconds

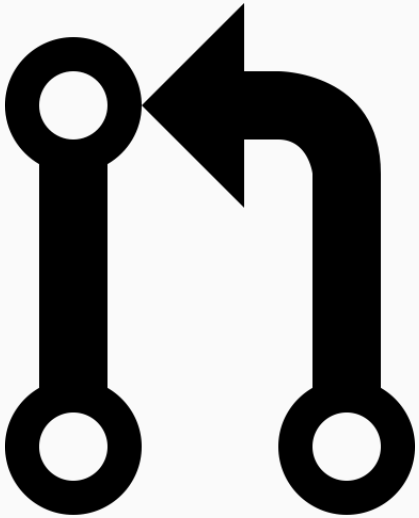
npm

8.3
seconds

Retire.js

3
minutes

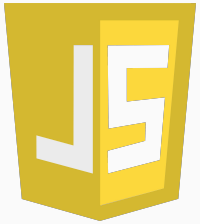
Show me what you got (so far)



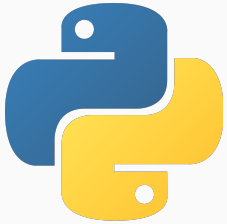
beta globo.com
projects with huskyCI

error unhandled

vulnerable dependencies



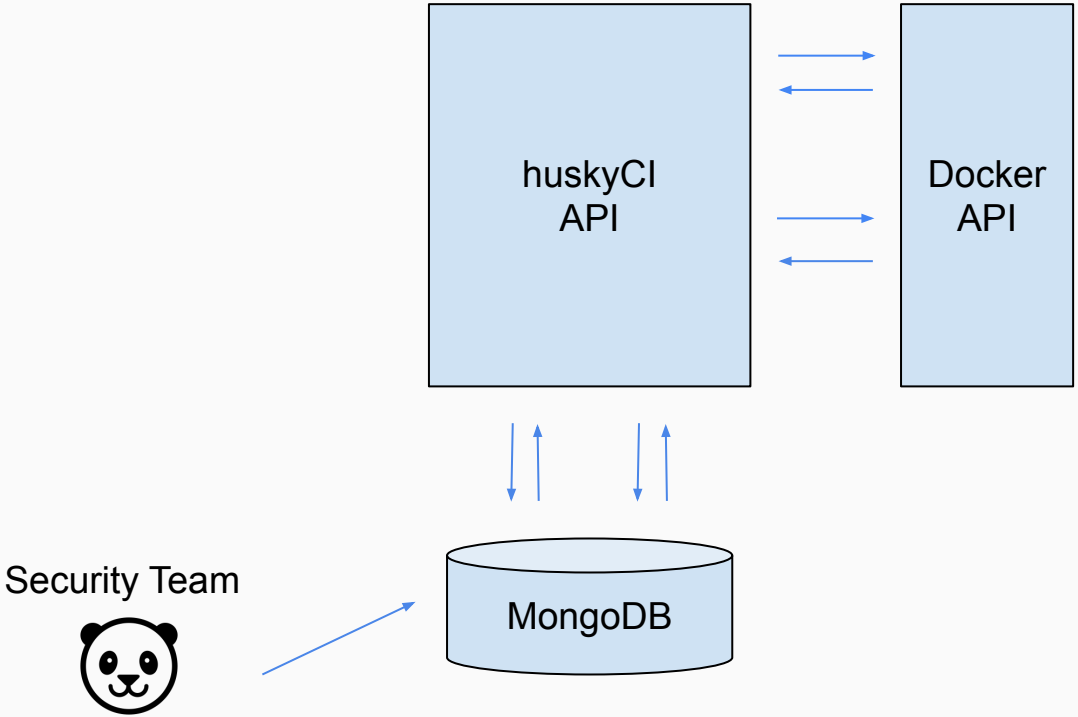
vulnerable dependencies



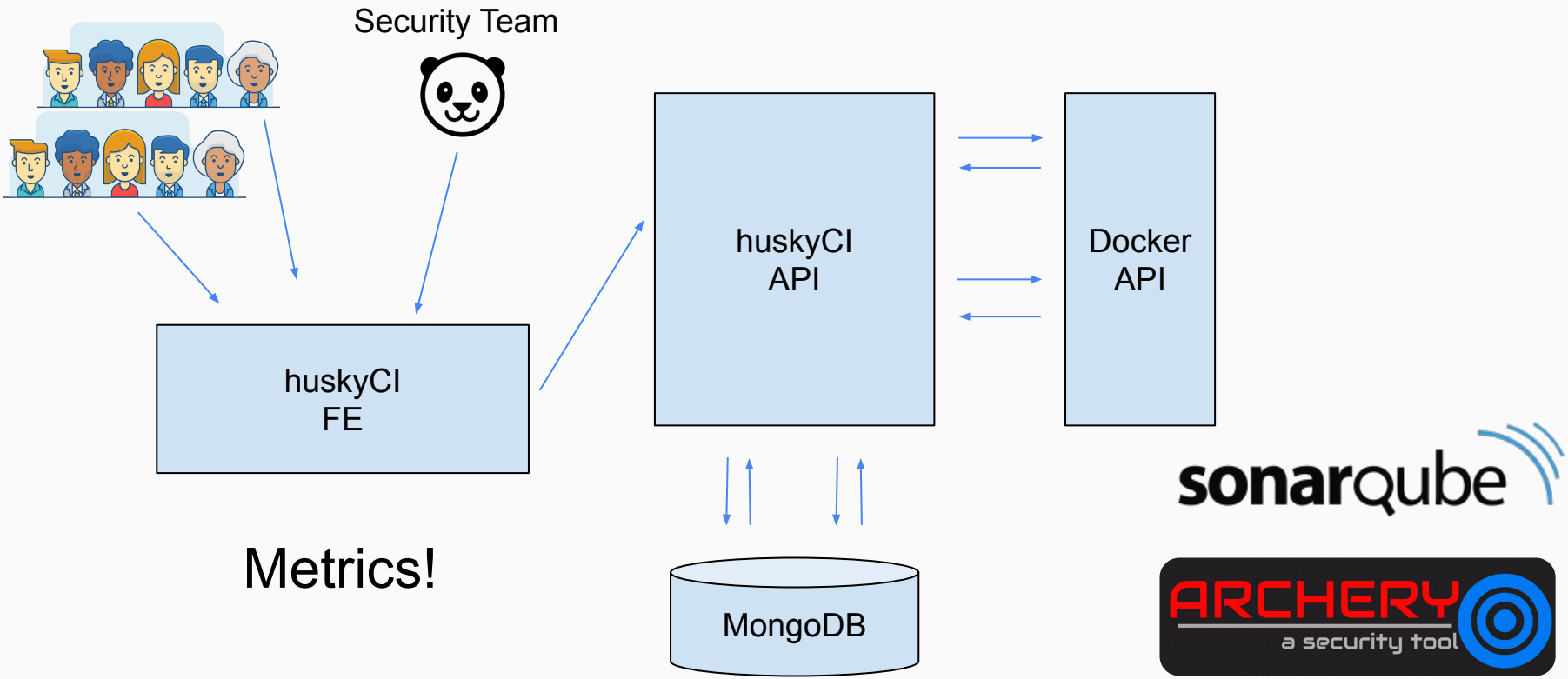
vulnerable dependencies

Next steps 😎

Next steps: Front-end

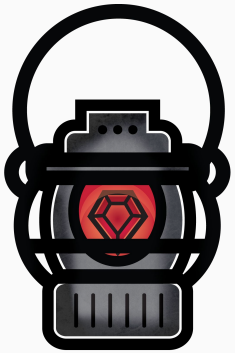


Next steps: Front-end



Next steps: Support other languages

Next steps: Contribute to open source tools

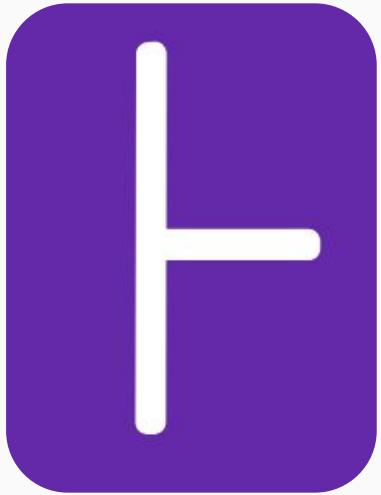


npm

Safety

Retire.js

Next steps: Add more security tests tools!



Security Code Scan

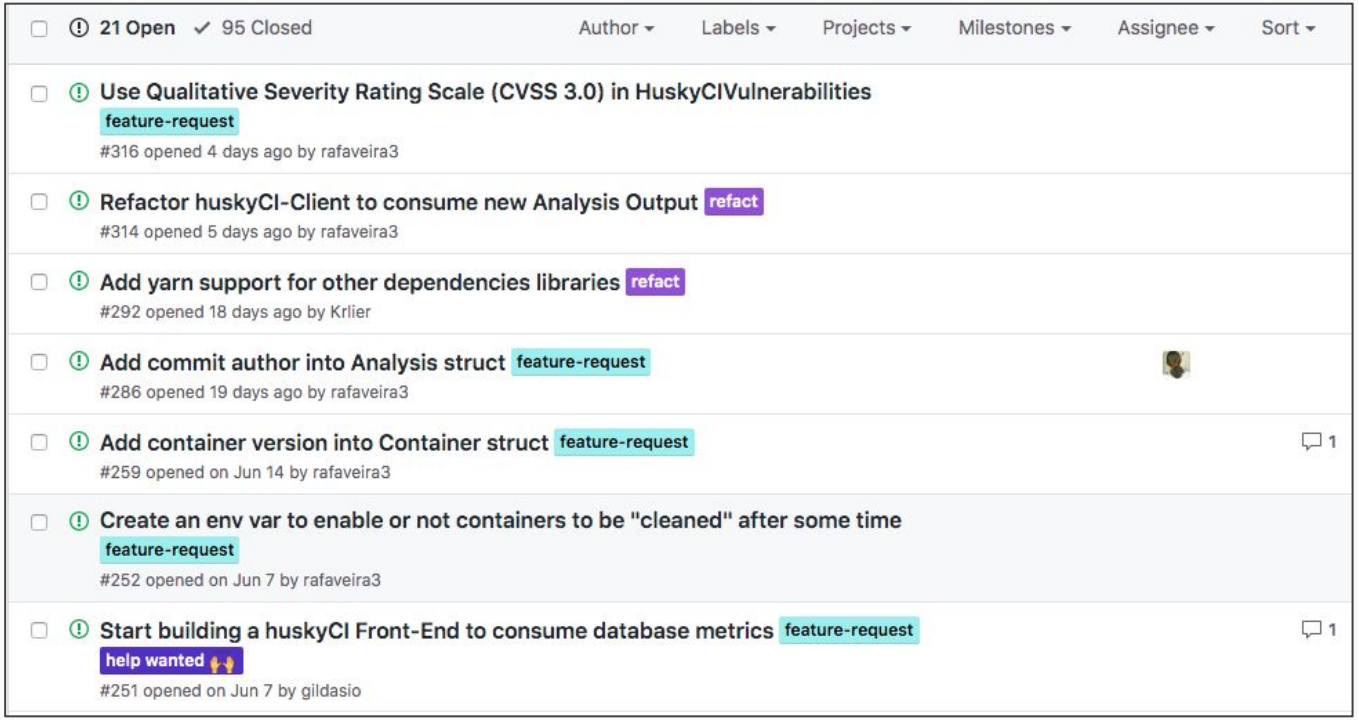
CHECKMARX

SpotBugs

Awesome Static Analysis!

Awesome DevSecOps awesome

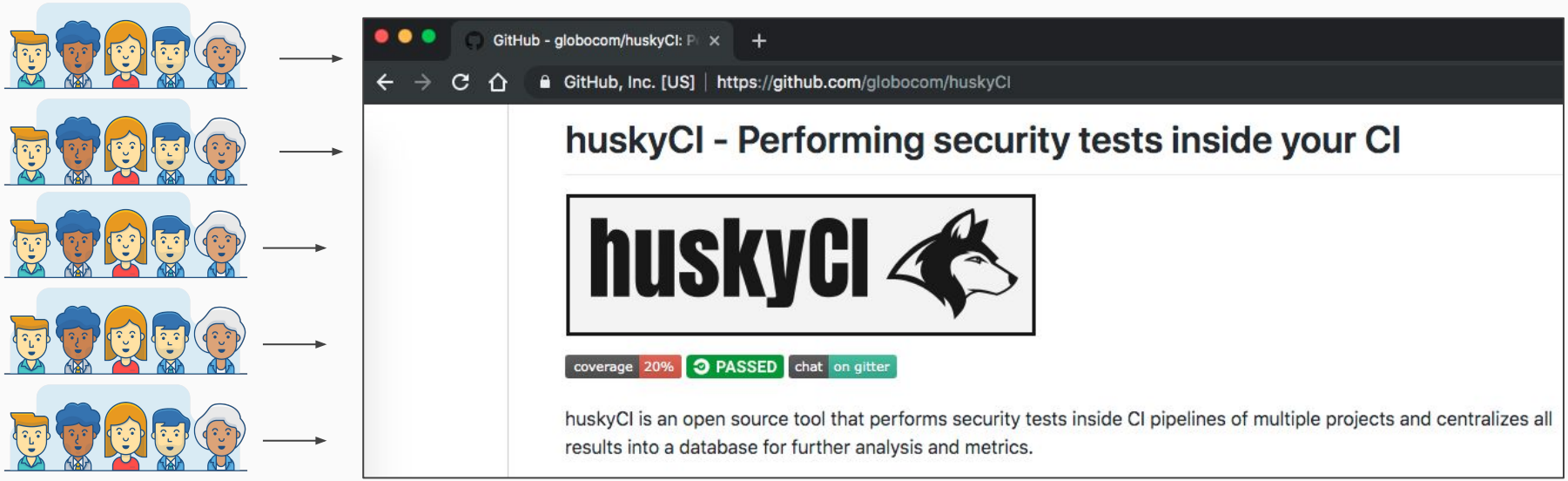
Next steps: And many more...



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

Give huskyCI a chance! 🐼

Give huskyCI a chance!



Open Source

https://github.com/globocom/huskyCI

References 📖

- [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

Village

Aug, 2019

Questions? 🤔

github.com/globocom/huskyCI

Rafael dos Santos 🇧🇷 @rafasantos5

Village

Aug, 2019

Thanks! 🙃

github.com/globocom/huskyCI

Rafael dos Santos 🇧🇷 @rafasantos5