HuskyCI: Um orquestrador de testes de segurança em software para ciclos ágeis de desenvolvimento

Thiago Lotufo Macedo
DSc Sérgio de Medeiros Câmara

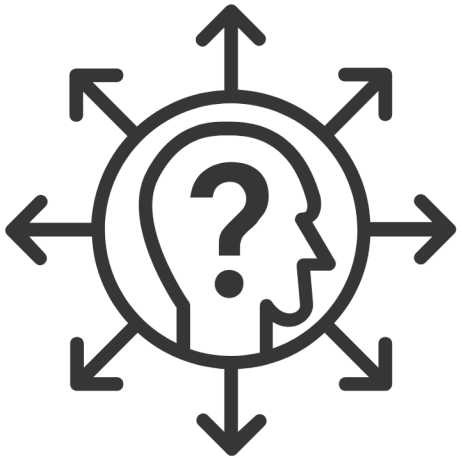
Globo

Antes de começar...

O que é um SAST?

Por que desenvolver um orquestrador de ferramentas SAST?

Desafios



- Escalabilidade
- Complexidade de implementação
- Resultados descentralizados

Desafios

Múltiplas linguagens

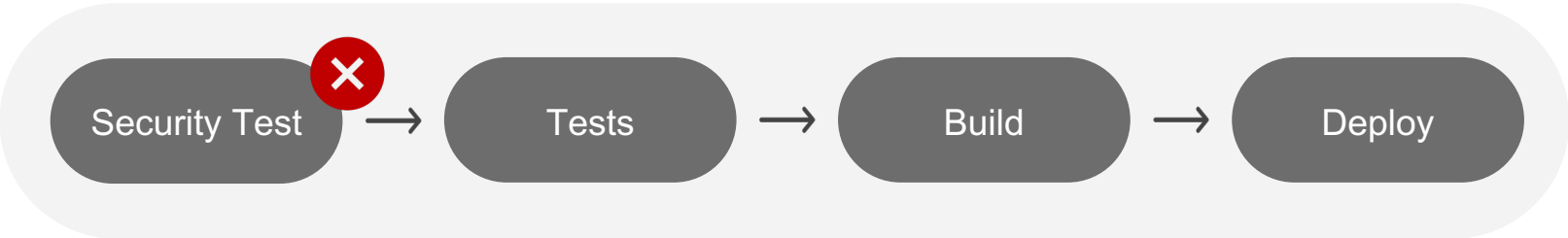
Desafios

Tempo de execução

+

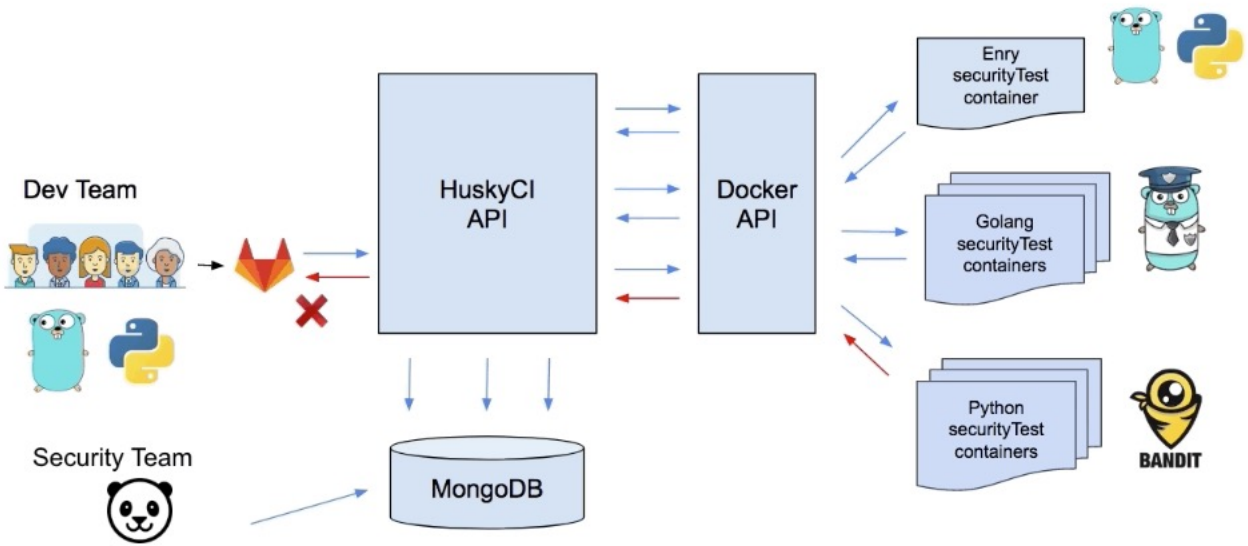
Complexidade de Implementação

> Impacto negativo nas pipelines



Solução Proposta

Aplicação escrita em Go, que pode ser executada utilizando Containers, tornando-se escalável e de fácil implementação.



Vantagens

Fácil de Implementar

A implementação nas pipelines é feita de forma transparente, não sendo necessário conhecer as linguagens do repositório.

Escalável

Como os testes de segurança rodam paralelamente em containers, a aplicação pode executar N análises simultâneas.

Tempo de execução

Como as análises rodam em paralelo, um repositório com diversas linguagens pode rodar N ferramentas simultâneas.

Execução

Para executar o HuskyCI, basta clonar o repositório *https://github.com/globocom/huskyCI* e executar os seguintes comandos:

- **make install**
- **source .env**
- **make run-client**

```
[HUSKYCI][*] main -> https://github.com/thiagolotufo/huskyCI.git
[HUSKYCI][*] huskyCI analysis started! yMMMCNkBjJaslr9GptIvQHmDvo81Lkbf
[HUSKYCI][!] Hold on! huskyCI is still running...

[HUSKYCI][*] main -> https://github.com/thiagolotufo/huskyCI.git
[HUSKYCI][*] huskyCI analysis started! yMMMCNkBjJaslr9GptIvQHmDvo81Lkbf
[HUSKYCI][!] Hold on! huskyCI is still running...

[HUSKYCI][*] The following securityTests were executed and no blocking vulnerabilities were found:
[HUSKYCI][*] [huskyci/gitleaks:v.7.6.1 huskyci/gosec:v2.3.0]
[HUSKYCI][*] No issues were found.
```

Melhorias

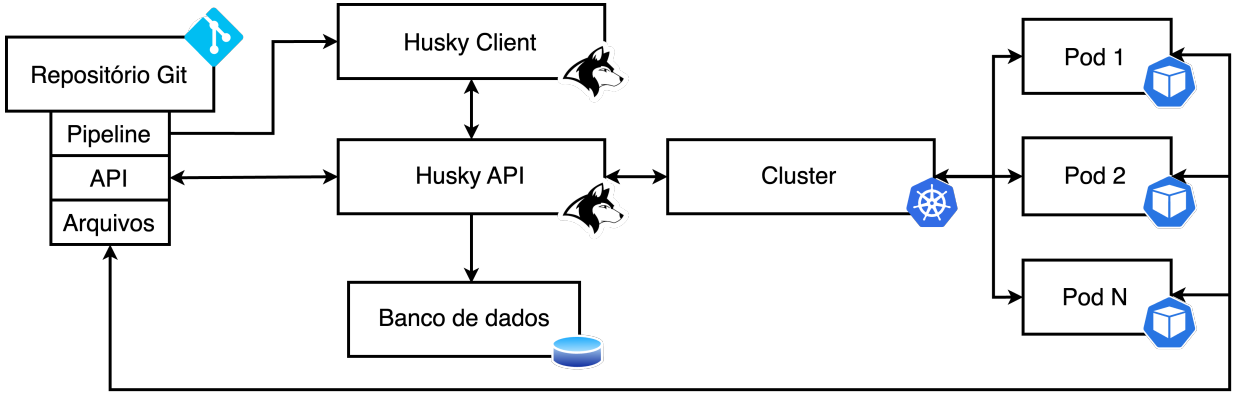
Utilizando a ferramenta, identificamos alguns pontos de melhoria no tempo de execução. Realizamos uma análise dos resultados e pontuamos algumas modificações a serem executadas.

- Alto tempo de execução em projetos grandes;
- Clone do mesmo repositório em duas etapas diferentes;
- Clone de todo o repositório Git;
- Infraestrutura mal dimensionada.

- Reconfiguramos os testes de segurança para aumentar a performance;
- Utilização da API do Github/Gitlab para obter as linguagens;
- Clone apenas do último commit;
- Redimensionamos a infraestrutura.

Melhorias

Novo fluxo do HuskyCI com as principais melhorias implementadas.



Trabalhos futuros

- Melhoria contínua da ferramenta;
- Monitorar o tempo de execução para garantir menor impacto nas pipelines;
- Melhoria nos erros e status da ferramenta.

Obrigado!

- Thiago Lotufo Macedo
  - https://linkedin.com/in/thiago-lotufo
- DSc Sérgio de Medeiros Câmara
  - https://linkedin.com/in/sergio-camara