GT-CRIVO – Pitch para Discussão

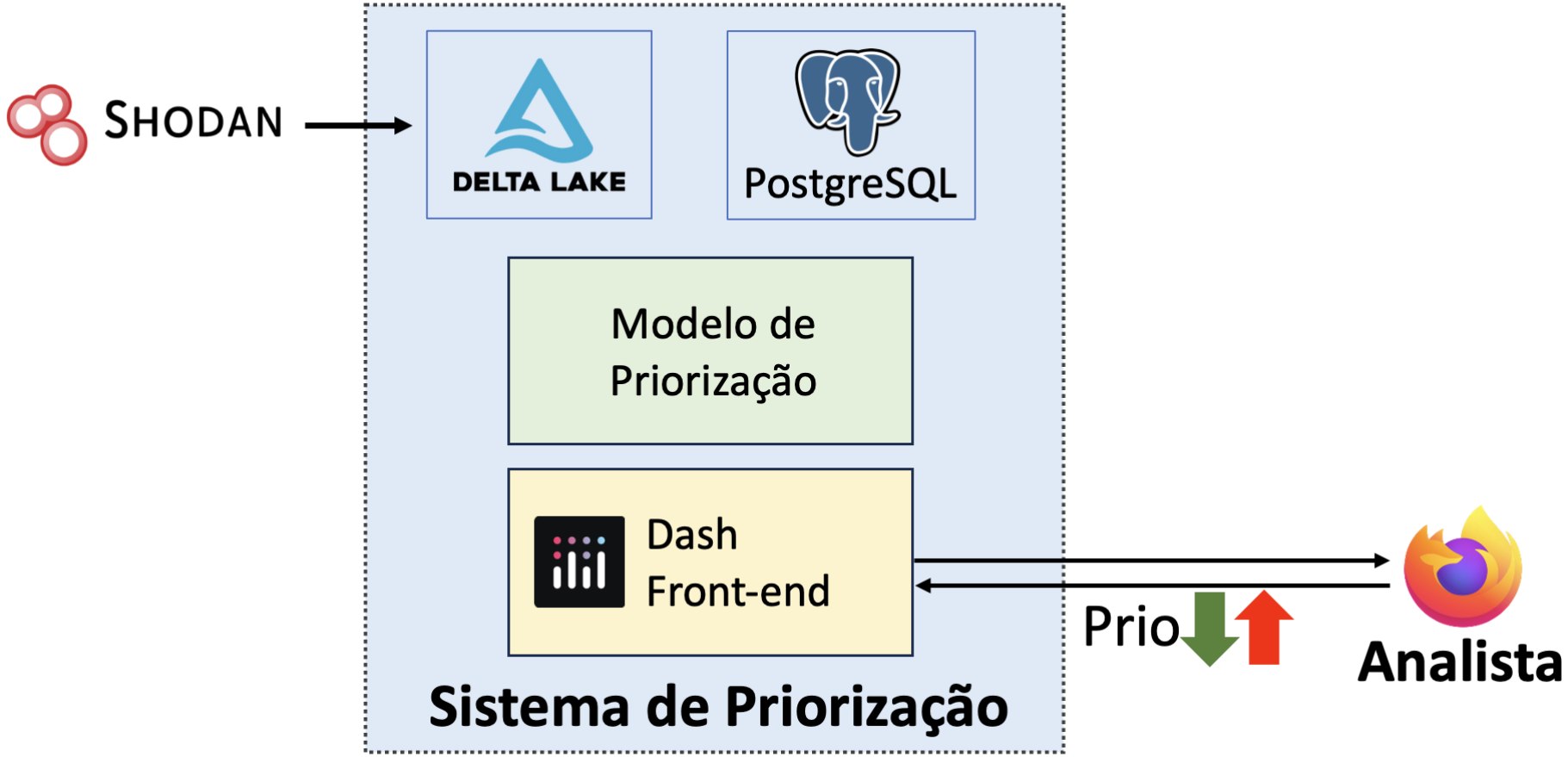
Priorização Contextualizada de Vulnerabilidades Orientada a Negócio

Ítalo Cunha

Francisco Aragão, Gabriel Pains, Leonardo Maia,
Lucas Sacramento, Pedro Almeida, Thiago Souza

Universidade Federal de Minas Gerais

Priorização de agrupamento de vulnerabilidades



Implantação do modelo de priorizações e agrupamento de vulnerabilidades

- Integração com DefectDojo pode levar a adoção naturalmente
  - Outros sistemas de interesse?
  - Como aumentar a abrangência?

Implantação do modelo de priorizações e agrupamento de vulnerabilidades

- Integração com DefectDojo pode levar a adoção naturalmente
  - Outros sistemas de interesse?
  - Como aumentar a abrangência?

- Integração com sistemas de gerência de vulnerabilidades da RNP
  - Transparente e opcional para os analistas!
  - Qual sistema?
  - Como fazer interação com desenvolvedores e analistas da RNP?
    - Modificações no banco
    - Modificações no front-end
    - Integração do modelo de predição
    - Acesso aos dados (e.g., incidentes)

Aplicação das soluções em novos contextos

- Parcerias com o CERT.br e startup do ramo de segurança

- Quais desafios enfrentados pela RNP e clientes na área de segurança?
- Como é a atuação do CAIS?
  - Compartilhamento de experiência para orientar nossos esforços

Potencializar o aprendizado dos alunos do Hackers do Bem

- Inúmeras frentes de análise e pesquisa com mais dados

- Plano atual: Aprendizado sobre vulnerabilidades para participantes do programa de residência
  - Atividades relacionadas a segurança nos PoPs?
  - Existe algum sistema de gerência de vulnerabilidades em uso?

Melhorias de classificação com modelos maiores

	CPU	GPU	CPU + GPU	2 GPUs	3 GPUs
Tamanho máximo	256GiB	24GiB	88GiB	48GiB	72GiB
Modelo	70B	9B	70B 4b-quant	70B 4b-quant	70B 6b-quant
Qualidade	Boa	Regular	Boa	Boa	Boa
Tempo de execução	45min	30s	3min	40s	40s

- Infra-estrutura para execução de grandes modelos de linguagem
- Treinamento (especialização) de novos modelos