GT-LFI - *Learn from Incidents - Sistema de Ensino-Aprendizagem, Gamificação e Classificação a partir de Incidentes*

Apresentação final - RNP - 16/12/2025

Coordenador - Prof. Dr. Rodrigo Sanches Miani - FACOM/UFU

Incidentes de Segurança

O que é um incidente?

Evento que compromete a **confidencialidade**, **integridade** e/ou **disponibilidade**.

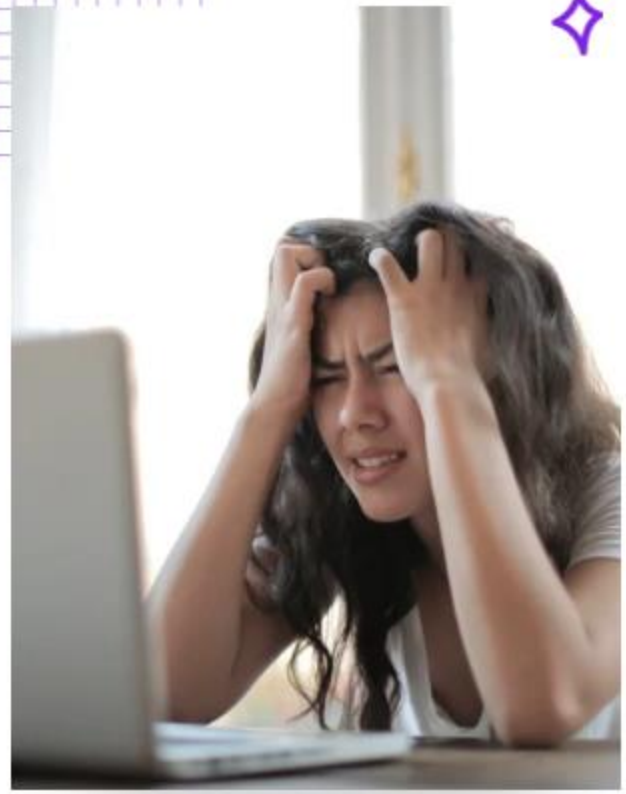
Cenário Atual

700M de ataques no Brasil em 2024 (2° país mais atacado da América Latina).

Impacto

Sobrecarga em CSIRTs, PoPs e empresas. Demanda por profissionais qualificados!

Problema



A resposta a incidentes é lenta, manual e não escalável!

Faltam profissionais qualificados!

4,8 milhões de vagas! 90% dos entrevistados apontam falta de habilidades (especialmente em resposta a incidentes).

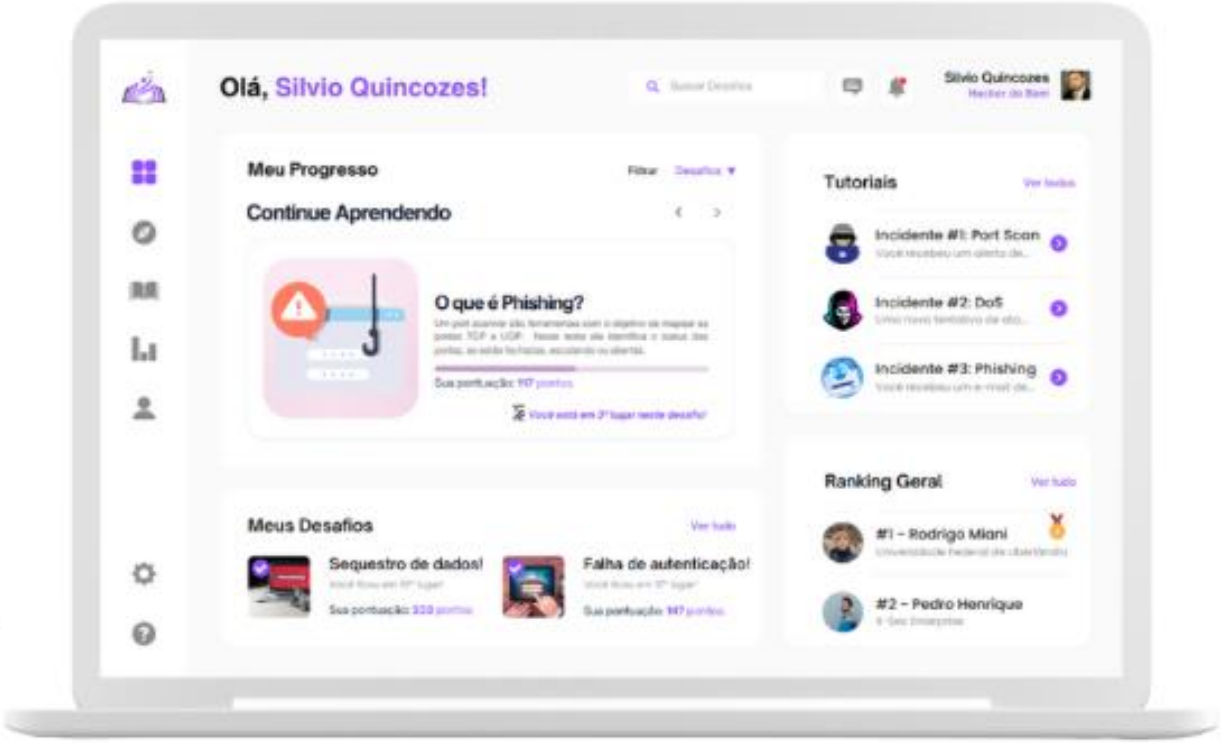
Treinamento ineficiente

Cursos com foco teórico, desconectados da prática e pouco efetivos para a realidade.

Como resolver o problema? - Parte 1

Plataforma de Aprendizagem

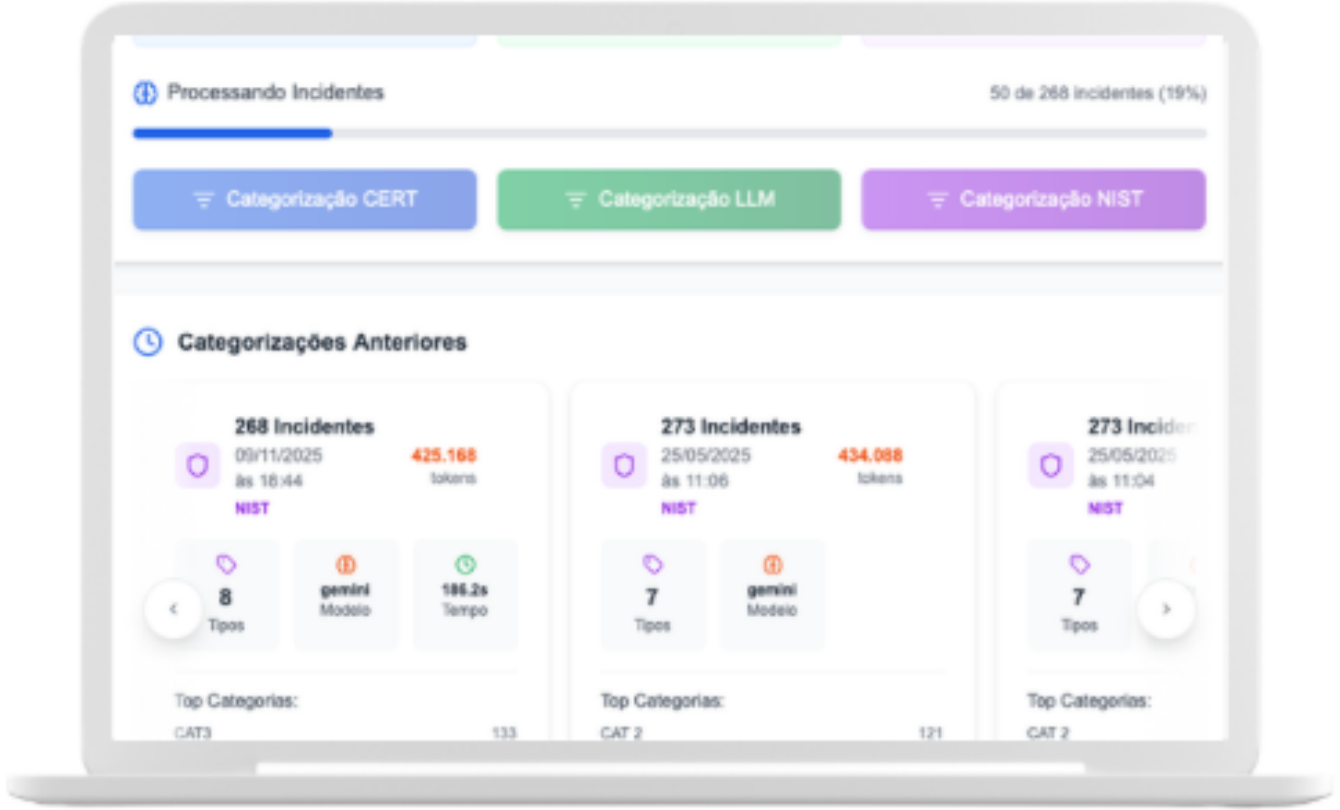
- Experiência **prática** e **envolvente** no aprendizado de resposta a incidentes.
- Aprendizado contínuo e **gamificado** com **ranking**, **missões** e **trilhas** de aprendizagem.
- Simulação de incidentes com **inteligência artificial** a partir de **dados reais e atualizados**.



Como resolver o problema? - Parte 2

Classificação e geração automática de playbooks

- **Tickets** de incidentes são basicamente formados por **textos**.
- IAs, em particular **LLMs**, podem ser usadas para auxiliar em **tarefas** que demandam **tempo dos analistas:** classificação de incidentes e geração de playbooks
- Considerando a sensibilidade dos dados, é importante inserir o analista no processo (**human-in-the-loop**).



Proposta

RNP

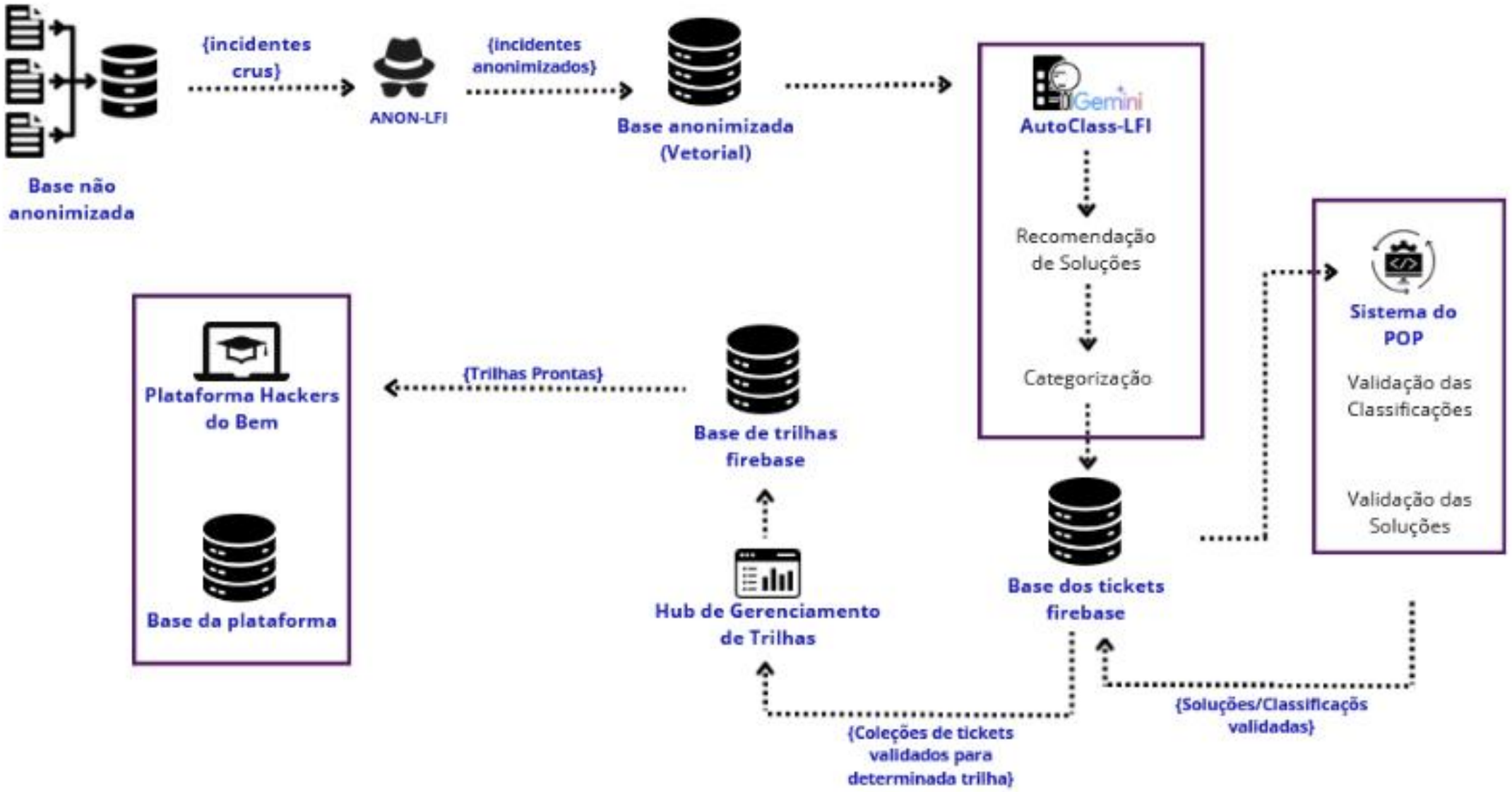
HACKERS DO BEM

GT-LFI

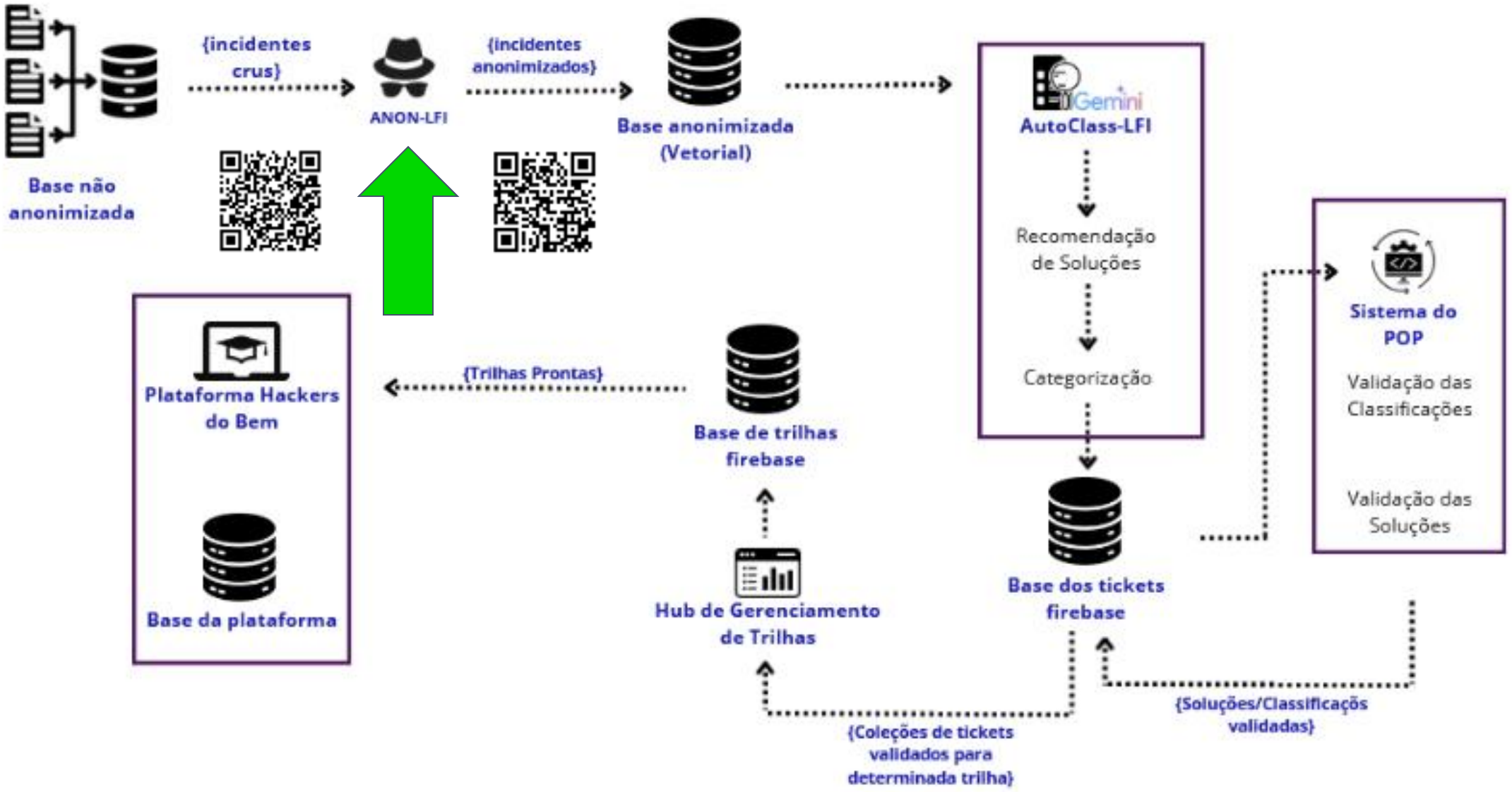
Learn From Incidents

"Formando quem responde aos desafios do mundo digital"

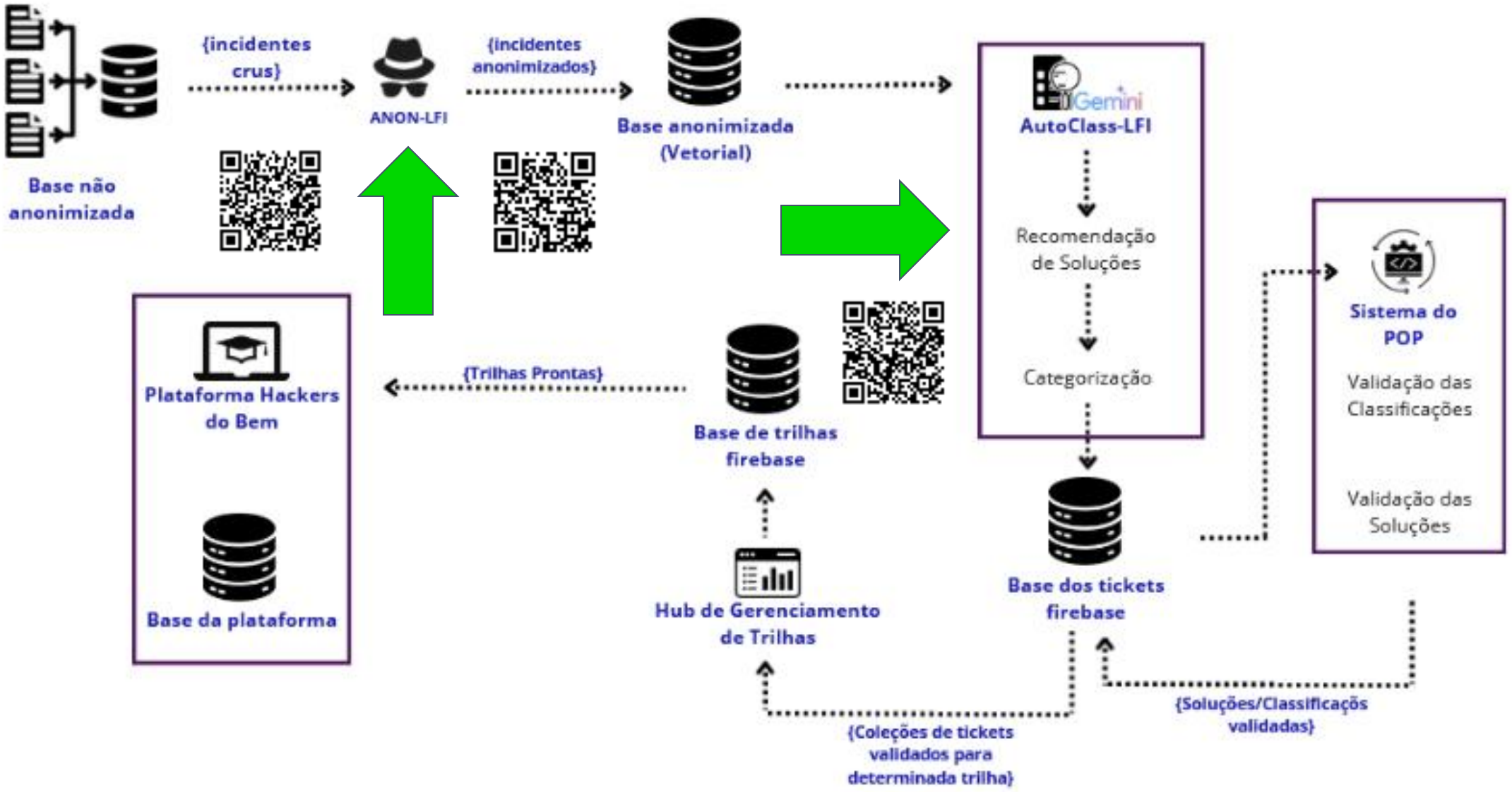
Arquitetura



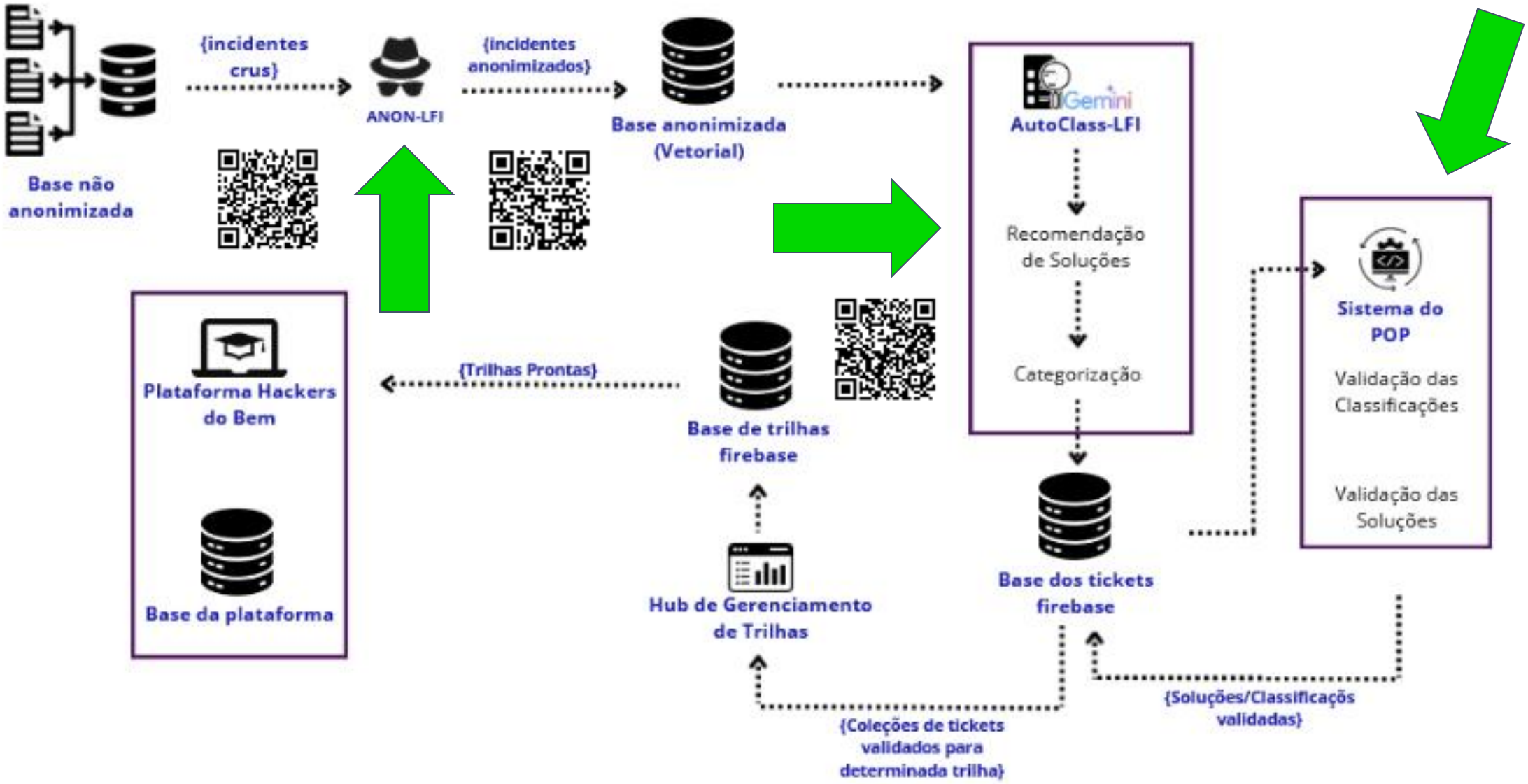
Arquitetura



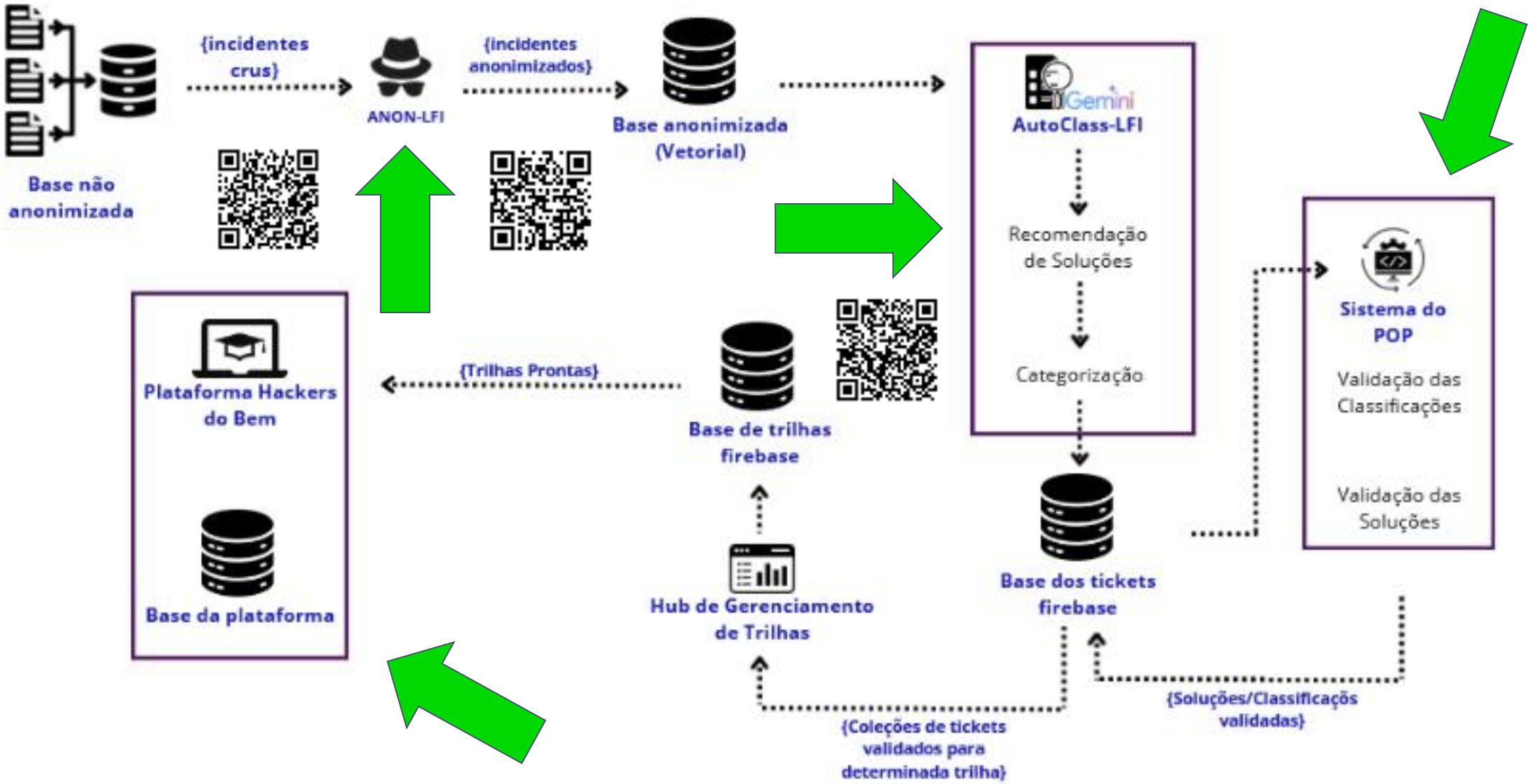
Arquitetura



Arquitetura



Arquitetura



Entregáveis

Anon

Autoclass

usuário:
usuario@gtlfi.com
senha:
AbC$#@!1234

PoP

HdB

Resultados

Desenvolvemos uma **solução inovadora** para o **treinamento** em resposta a incidentes:

- Dados reais anonimizados
- Uso de IA para fornecer soluções automáticas de classificação e playbooks
- Gamificação
- Flexibilidade na criação de novas trilhas de aprendizado

A solução permite que módulos como Anon e Autoclass/PoP possam ser usados **individualmente** por equipes de **CSIRTs** para resolver problemas como compartilhamento de incidentes e classificação de incidentes.

Próximos passos

Nos próximos **seis meses** trabalharemos nas seguintes atividades:

- Testes com os residentes do HdB
- Testes com estudantes e profissionais selecionados
- Trabalhar com a geração de dados sintéticos de incidentes
- Explorar as possibilidades de criação de startup ou transferência de tecnologia

Equipe

Coordenação

Dr. Rodrigo Sanches Miani

Coordenador Geral

Dr. Silvio Ereno Quincozes

Dr. Diego Luis Kreutz

Dr. Leandro Bertholdo

Dr. Rafael Dias Araújo

Coordenadores Locais

Equipe

Bolsistas e colaboradores

Felipe Scherer

Felipe Nestor Dresch

Sebastião de Jesus

Carolina Bandel

Alvaro Santana

João Pedro Esteves

Beatriz Machado

Agradecimentos

Demonstração

https://drive.google.com/file/d/1DmyNNi6WT0w7K9120ZfhqSbZoOHqRkLb/view?usp=sharing

Processamento de Texto

Análise rápida de entidades e anonimização em um fluxo unificado.

Texto

Cole o texto aqui

Extrair Entidades

Anonimizar Texto

Upload de Dataset

Pré-visualize, selecione colunas e processe seus tickets com segurança.

Selecionar arquivo CSV


HACKERS
DO
BEM