



Modelagem de ameaças utilizando IA

A FIAP Software Security, empresa de Segurança de Sistemas, está analisando a viabilidade de uma nova funcionalidade para otimizar seu software de análise de vulnerabilidades em arquitetura de sistemas.

O objetivo da empresa é usar novas tecnologias para identificar e tratar vulnerabilidades que possam colocar em risco a segurança dos sistemas criados por arquitetos(as) e desenvolvedores(as).

Um dos desafios é utilizar Inteligência Artificial para realizar automaticamente a modelagem de ameaças, baseado na metodologia STRIDE de um sistema a partir de um diagrama de arquitetura de software em imagem. A empresa tem o objetivo de validar a viabilidade dessa feature, e para isso, será necessário fazer um MVP para detecção supervisionada de ameaças.

Objetivos

- Desenvolver uma IA que interprete automaticamente um diagrama de arquitetura de sistema, identificando os componentes (ex.: usuários, servidores, bases de dados, APIs, etc);
- Gere um Relatório de Modelagem de Ameaças, baseado na metodologia STRIDE;
- Construir ou buscar um Dataset contendo imagens de Arquitetura de Software;
- Anotar o Dataset para treinar o modelo supervisionado, para que ele seja capaz de identificar os diversos componentes de arquitetura de Software;
- Treinar o modelo;
- Desenvolver um sistema que seja capaz de buscar as vulnerabilidades relacionadas a cada componente e as contramedidas específicas para cada ameaça.

Avaliação

Para avaliar o código desenvolvido, nós utilizaremos arquiteturas de teste como os descritos abaixo:

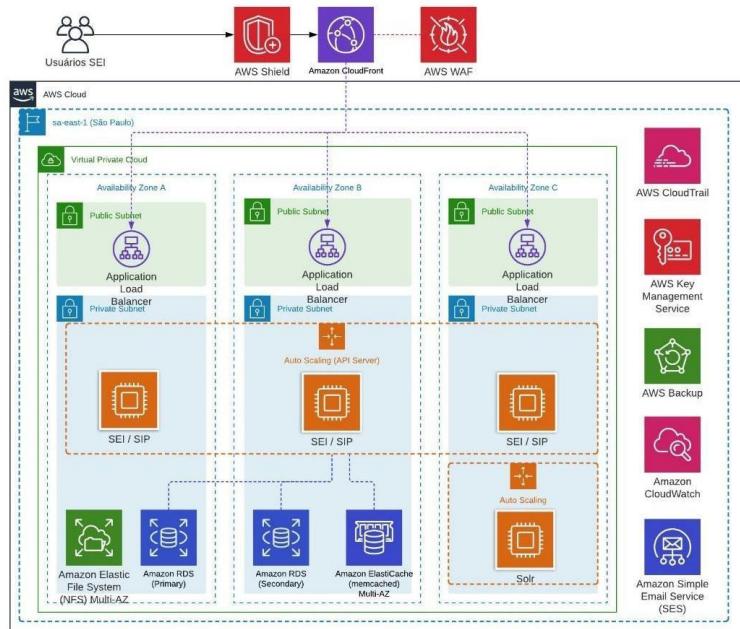


Figura 1 – Arquitetura 1

Fonte: elaborado pelo autor (2025)

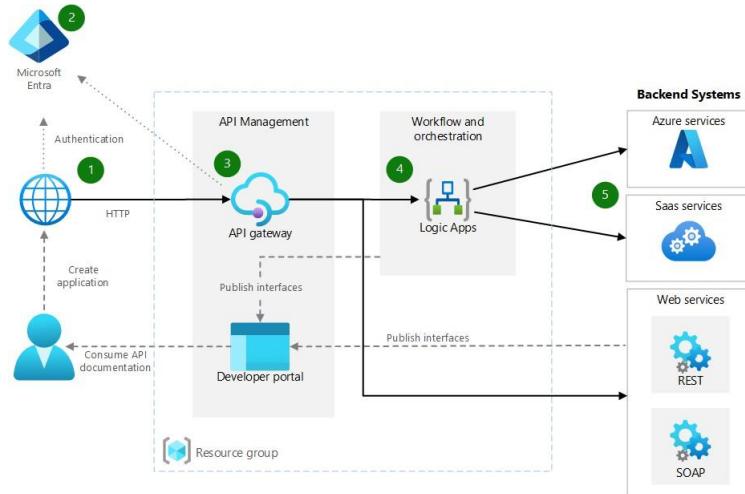
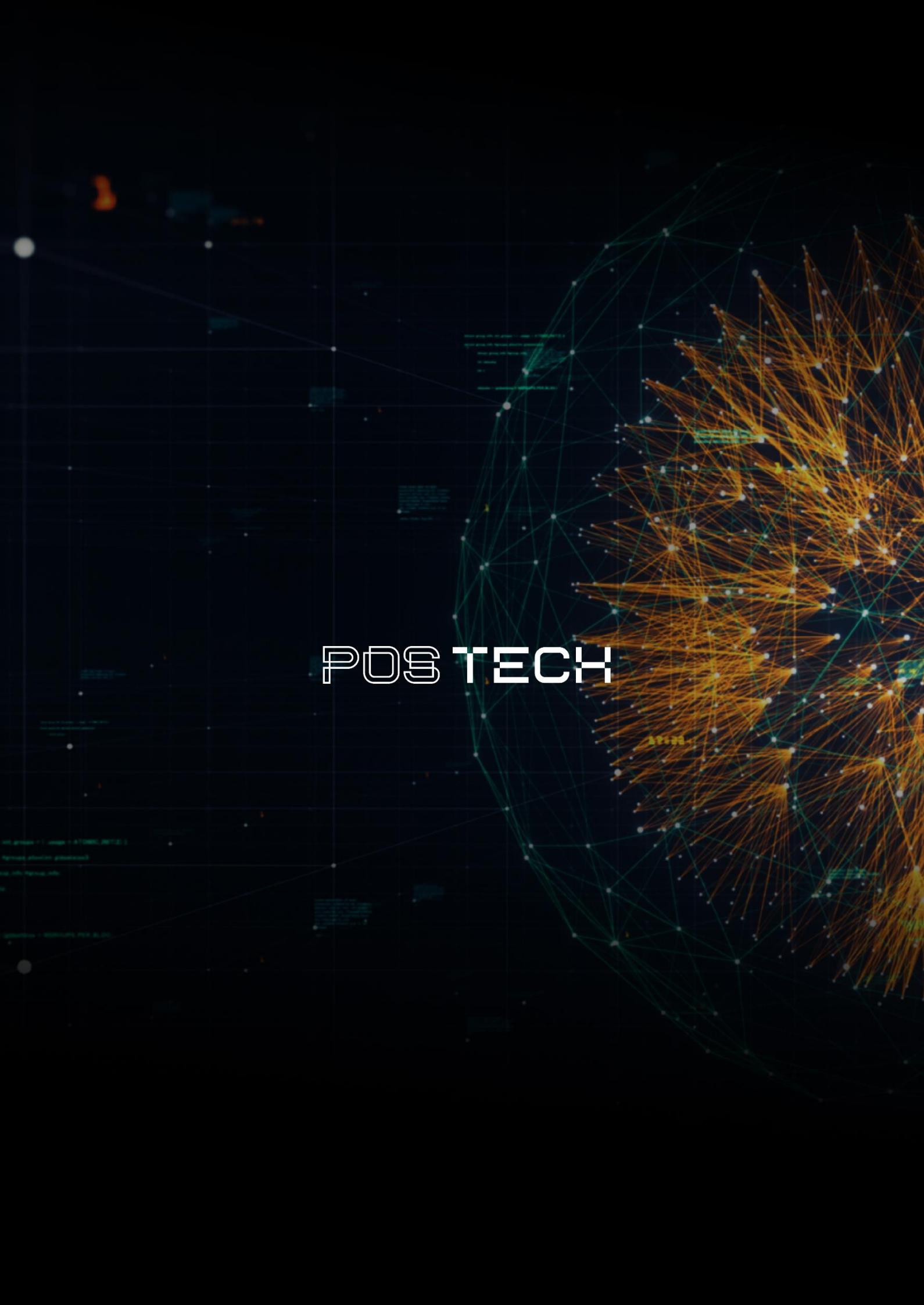


Figura 2 – Arquitetura 2

Fonte: elaborado pelo autor (2025)

Entregáveis

- Documentação detalhando o fluxo utilizado para o desenvolvimento da solução;
- Vídeo de até 15 minutos explicando a solução proposta;
- Link do Github do projeto.



POSTECH