Sprint Review: Setup do Ambiente

Uma análise detalhada do setup técnico e da arquitetura do middleware para garantir a segurança e privacidade em aplicações com LLMs.

Introdução ao Projeto

Este projeto aborda a Segurança da Informação em aplicações que utilizam Modelos de Linguagem de Aprendizado Profundo (LLMs). A equipe visa assegurar que as soluções implementadas respeitem os princípios de segurança, privacidade.

Objetivo da Sprint

Este projeto aborda a Segurança da Informação em aplicações que utilizam Modelos de Linguagem de Aprendizado Profundo (LLMs). A equipe visa assegurar que as soluções implementadas respeitem os princípios de segurança, privacidade.

Diagrama da Arquitetura da PoC

O diagrama ilustra o fluxo de dados completo da Prova de Conceito, destacando como a aplicação middleware, executada em Docker, processa cada requisição. Com cinco camadas de controle efetivas, garantimos a segurança e a conformidade antes de interagir com a API externa do Gemini.

Ambiente e Ferramentas (Tech Stack)

01 Ambiente de Execução: Docker e Docker Compose

02 Linguagem: Python 3.10+

03 Servidor da PoC: FastAPI

04 LLM: Google Gemini 2.5

05 Embeddings: Google text-embedding-004

06 Vector DB (RAG): ChromaDB

07 Módulos de Segurança: presidio-analyzer

08 Orquestração: langchain

09 RBAC e Firewall: Módulos Python customizados

Fluxo de Dados na Prova de Conceito

O fluxo de dados na nossa Prova de Conceito é cuidadosamente estruturado para assegurar que cada requisição do usuário seja tratada de forma segura e eficiente. As etapas incluem a sanitização da entrada, controle de acesso adaptativo, e a aplicação de um firewall LLM, culminando com a sanitização da saída antes de retornar a resposta ao usuário.

Módulos de Segurança Implementados

01 Sanitização de Dados Sensíveis

02 Controle de Acesso Rigoroso

03 Proteção com Firewall LLM

04 Repositório de Acesso RAG

05 Registro de Conformidade

Conclusão e Próximos Passos

Os resultados da Sprint demonstraram a validação do setup técnico e a eficácia da arquitetura de middleware implementada. Para os próximos passos, focaremos na implementação dos módulos de segurança restantes e na realização de testes extensivos para garantir a conformidade e a segurança do sistema.