BMC Hackathon '24

Presented by Team Spartans

Team Members

1. Anish Dabhane
2. Sujal Bhor
3. Siddhesh Sangale
4. Avadhut Giri

BMC Hackathon '24 - Spartans

01

Problem Statement

Organizations spend significant time analyzing CIS, DISA, and PCI documents to create audit and remediation scripts for compliance templates. The documents are frequently updated for various OS versions, requiring careful analysis, which makes the process time-consuming and prone to duplicate work for similar rules with minor changes.

The challenge is to automate this process using AI/ML tools to generate scripts efficiently, ensuring accuracy, reliability, and compliance with updated guidelines.

02

Vision

Develop a comprehensive platform that serves as the go-to solution for retrieving compliance rules, fully compatible with all major compliance frameworks and organizations, while supporting multiple versions.

The platform will harness the power of open-source Large Language Models (LLMs) and state-of-the-art LLM inference technologies to significantly accelerate the generation of audit and remediation scripts, ensuring efficiency and adaptability.

03

Document


CIS Center for Internet Security
CIS Benchmarks™
CIS Ubuntu Linux 24.04 LTS Benchmark
v1.0.0 - 08-26-2024

04

Solution

01

Text extraction using built in python libraries and regex for separating the content.

02

Leveraging the power of LLM for audit and remedy script generation

03

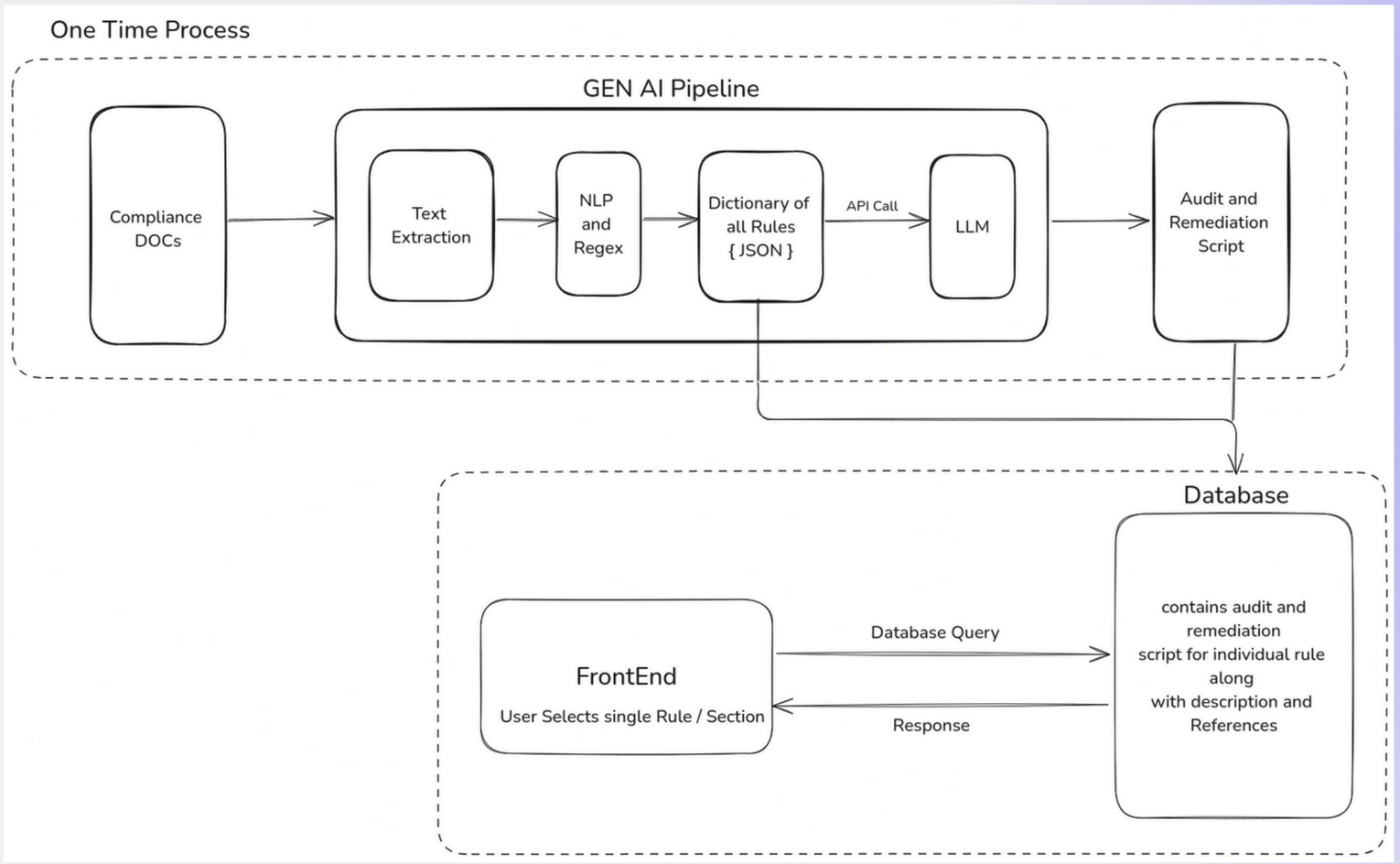
Using Database for Storing the scripts and other meta data associated with each rule

04

AI driven remediation script generation

05

Architecture



06

Tech Stack

LLM

LLaMA

together.ai

groq

Language

python™

Frontend

Streamlit

Backend

mongoDB.

FastAPI

USP

Leveraging Groq, the fastest LLM inference platform available, to deliver unparalleled processing speed. By storing scripts and metadata for each rule in a database, our solution minimizes API call costs while ensuring data reliability and accessibility.

01. **Speed**

02. **Cost Efficient**

03. **Reliability**

08

Future Scope

CLI

A command-line tool will assist users with specific commands, provide **warnings** for potentially harmful remediation actions, and **log** every command executed.
It will also generate a concise **audit summary** with pass/fail results.

Expansion

Extend the platform to support a wider range of compliance standards and frameworks beyond **CIS, DISA, and PCI,** ensuring broader applicability across industries and geographies.

Automation

Splitting PDF for to various sections and depth of rule ID, accordingly generating the

Optimizations

Optimizing text extraction with advanced OCR and AI techniques, along with **fine-tuning NLP models** for better rule recognition. Enhancing database efficiency through improved indexing, **caching**, and **partitioning** for faster data access and **reduced API costs.**

Thank You

Team Spartans