

Automatiq.ai Home Assignment

Overview

CyFortis discovered that its annual cybersecurity training program had become chaotic: employees constantly forgot which videos they'd completed, and the CISO's team was drowning in requests for status checks. To streamline compliance and reduce operational friction, the company launched an initiative to build an AI assistant that could answer training-related questions in natural language for both employees and the CISO.

You've been assigned to build a **AI agent**:

1. Employee perspective:
 - a. Checks whether it finished the training or not.
 - b. If the employee didn't finish the training – the agent will list the missing videos.
2. CISO perspective:
 - a. For a specific employee:
 - i. Checks if finished the training or not.
 - ii. Produce a summary and current status (NOT_STARTED, IN_PROGRESS, FINISHED).
 - b. For all employees:
 - i. Given a status (NOT_STARTED, IN_PROGRESS, FINISHED) list all employees.
 - ii. Produce a summary (max/min/average time to finish training, fastest employee, slowest employee).
3. The Employee/CISO talks in natural language with the agent, they don't have access to the DB table.
4. The Employee/CISO must authenticate before "talking" with the agent (ID + Employee name).

Requirements

- Frontend: React (TypeScript preferred) - chat interface for user-agent interaction.
- Backend: Python + FastAPI - manages the chat flow, model calls, and recommendation logic.
- Model: Either Local model (e.g., gpt-oss, llama3, qwen), or Hosted LLM API (OpenAI, Anthropic, etc.).

Functionality

- The agent must understand from the natural language which query to execute.
- Add some guards that the agent talks only on the task (security training course) and not on any other topic.
- **Bonus:** make sure that the agent cannot perform actions that will affect the entire state.

Deliverables

- GitHub repo containing:
 - frontend/ and backend/ directories
 - README.md with setup and design notes
 - Dockerfile or docker-compose.yml
 - .env.example for environment variables
 - PDF file with explanations what you did and why you did (**IMPORTANT!**)

Additional Notes

- A SQLite with employees table is attached to the assignment with a basic python script exploring the DB.
- Extra thoughtfulness, creativity, and initiative are encouraged and will be appreciated. There's room for experimentation as long as the core requirements are met.

Example

Alice: "Which videos did I finished?"

Agent: "You must provide your name and ID in order to continue this conversation"

Alice: "My name is Alice"

Agent: "Hey Alice, I must get your ID also"

Alice: "123456789"

Agent: "Hi Alice, how can I help you?"

Alice: "Which videos did I finish?"

Agent: "You've finished video 1 and 2"

Alice: "How long it took me to finish video 1?"

Agent: "It took you 10 minutes to finish"