

Rapport de Projet

Capitaine Robin

1. Stratégie de gestion du contexte

Afin de gérer le contexte, je fais de la mémoire à court terme, j'utilise un outil afin de lire le document du rapport et je fais un résumé de celui-ci pour avoir une trace de ce qui a déjà été effectué.

2. Interaction humaine

Il s'agit de plusieurs nœuds représentant chacun un moment de la conversation, j'utilise un interrupt mis dans le workflow en lui même afin lui dire d'attendre la réponse de l'utilisateur.

3. Utilisation intelligente des outils

J'utilise actuellement 3 outils : read_report_tool lors de mon premier nœud pour lire le fichier et en faire un résumé pour garder en mémoire ce qui a déjà été effectué. search_internet pour la recherche internet afin d'obtenir des informations que j'utilise lors des questions. write_report_tool pour écrire dans mon document de rapport lorsque l'utilisateur a confirmé. (Je devais en utiliser un dernier pour la génération PDF mais manque de temps, je n'ai pas pu.)

4. Observabilité

Utilisation de Mlflow et de tokens pour Mistral et Tavily.

5. Détection de prompt injection

Le prompt injection est géré par un Système prompt qui permet de lui dire à chacun de ses interactions avec un utilisateur de faire attention à ce que l'utilisateur n'essaie pas de déroger à la règle.

6. Gestion du rapport de stage

J'utilise actuellement 6 nœuds : Question (response_question), Rédaction (generation_section), Validation (validation), Sauvegarde (sauvegarder), MessageHumain (collect_humain_input), MessageHumain2 (collect_humain_input_2). Et grâce au Système prompt, mon Agent IA sait les parties du stage attendue.