CDW Documentation

Suggestions

Suggestions

- Give explanation for why each monitoring test failed – 'Toxicity test failed due to these words:'
- Functionality for running multiple initial monitoring tests at once or creating a queue.
- Ability to evaluate models against the framework packs, rather than a simple checklist
- Key vault within the tool to store model secrets, reference the secrets when onboarding model
- Automatically pull the AI Model inventory from AWS/Azure/GCP instead of manually onboarding models
- Variety in test prompts so that the same exact prompt is not used every time to yield the same exact result – shouldn’t need to manually create/add every prompt.
- Need more automation in general - manually onboarding models, manually designing prompts, etc. is too much

Issues

- 'Create Report' button didn’t always work in AI Models section
- In 'AI Monitoring' → 'Audit Logs': User and User ID are both random character strings
- 'View Audit Log' in the test results: the screen would be blank
- Sending the same prompt over and over would likely lead to the same results