LLM Apps

LLMOps Solutions

LLMOps solutions in the market

- The market for LLMOps tools is very recent and in full expansion, with new alternatives appearing frequently.

- There are more comprehensive tools like WhyLabs and more specific ones like Guardrails AI. In this lesson, we will analyze two popular products from WhyLabs: LangKit and LLM Security Management.

- While LangKit focuses on extracting actionable insights for content moderation and observability, LLM Security Management focuses on protecting LLM applications against a wider range of security risks, including prompt injections, data leaks, and misinformation.

Main features of LangKit, from WhyLabs

- Uses natural language techniques to extract actionable insights from prompts and responses, identifying and mitigating malicious prompts, sensitive data, toxic responses, problematic topics, hallucinations, and jailbreak attempts.
- Allows defining limits and detecting problematic prompts and responses in real-time, taking appropriate actions in case of failures.
- Validates how LLMs respond to known prompts, both continuously and ad-hoc, to ensure consistency when modifying prompts or changing models.
- Extracts key telemetry data and compares it with intelligent baselines over time, aiding in debugging and fine-tuning of the LLM application.
- Integrates easily with public APIs or proprietary models.
- Provides over 50 telemetry signals to assess the quality, relevance, sentiment, and safety of prompts and responses.

Features of LLM Security Management, from WhyLabs

- Protection Against Malicious Attacks.
- Prevention of Data Leaks.
- Defense Against Prompt Injections.
- Mitigation of Disinformation.
- Adoption of Best Security Practices: Implements telemetry to capture security risks defined in the "OWASP Top 10 for LLM Applications", allowing inline guardrails, continuous evaluations, and observability.
- Handling Various Security Risks: Addresses a range of vulnerabilities, including insecure handling of outputs, training data poisoning, denial of service, supply chain issues, and over-reliance on LLMs.
- Guardrails and Customizable Logging: Implements inline guardrails with customizable metrics, thresholds, and actions, and logs each prompt/response pair.