Project Name: Agentic Multi-Source Log Correlation for Incident Analysis

Project Proposer: Alison Yao alisonyao821@gmail.com

Open Source: Yes

Mentors: Alison Yao alisonyao821@gmail.com

Preferred Experience

Required for all members: Python, Git, Experience with LLMs

Required for at least one member: Experience with ML/NLP/prompting, Experience with cloud

Valuable: Experience with agent-based or multi-step LLM workflows, Experience with building data pipelines

Nice to have: Knowledge of causal reasoning

Project Background

Incidents in real-world systems rarely manifest in a single log stream. Failures often involve multiple subsystems, such as authentication services, host processes, network activity, and infrastructure metrics. Effective incident triage requires correlating signals across these sources and reasoning about their relationships.

This project explores agentic approaches to incident analysis, where different agents specialize in analyzing different log sources and collaborate to identify correlations, thereby revealing the full picture of incidents.

Project Description

The team will build an agent-based system that:

1. Ingests logs from multiple sources (e.g., host logs, authentication logs, network logs, metrics)
2. Aligns events temporally across sources
3. Uses specialized LLM-based agents to analyze each source independently
4. Introduces a correlation agent that:
    - identifies cross-source relationships

    - proposes candidate explanations or hypotheses
    - ranks likely causes or contributing components
5. Produces a structured incident narrative describing what happened and why

The project explicitly focuses on correlation and reasoning, not automated remediation or full root cause resolution.

Learning Outcomes

Students will gain experience in:

- Designing multi-agent LLM systems
- Correlating heterogeneous data sources in distributed systems
- Handling temporal alignment and partial observability
- Applying LLMs for reasoning and hypothesis generation
- Building explainable incident analysis tools
- Understanding real-world challenges in incident triage and observability