OpenSearchCon INDIA

AI Investigation Agents for Debugging Live Incidents Using OpenSearch

Aman Kimothi, Jai Mashalkar & Ashish Gupta

Oracle Cloud Infrastructure

OCI Search Service with OpenSearch

OpenSearchCon INDIA

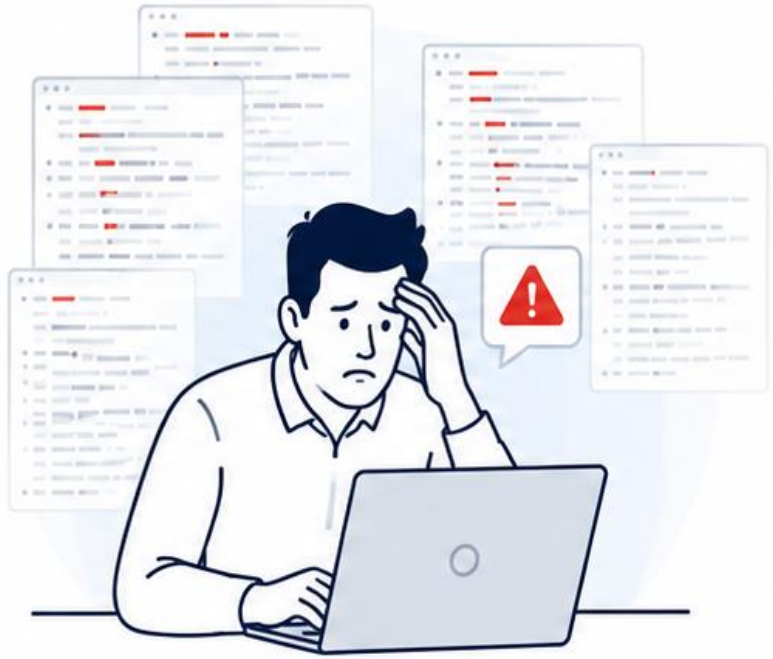
Aman Kimothi
Senior Software Engineer
LinkedIn

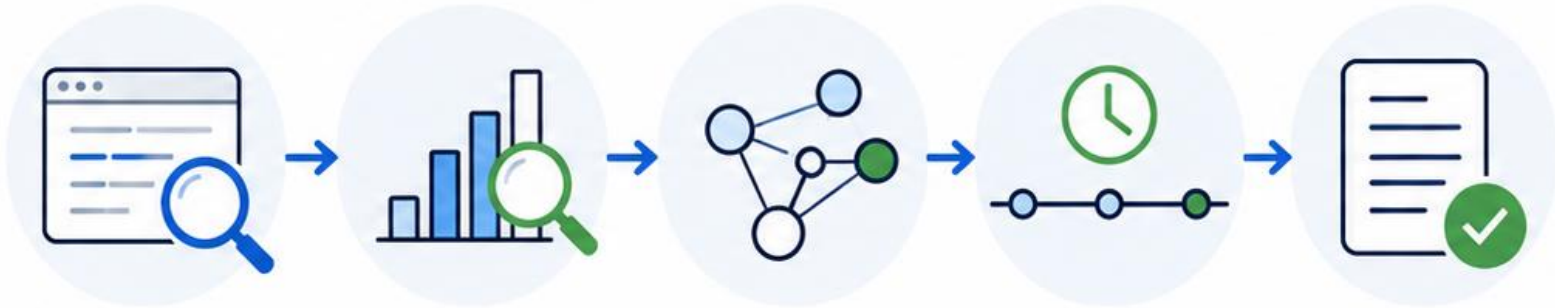
Jai Mashalkar
Senior Software Engineer
LinkedIn

Ashish Gupta
Senior Engineering Manager
LinkedIn

Problem Statement

Debugging production incidents in distributed systems is hard.





Logs
Collect relevant telemetry

Patterns
Identify dominant error patterns

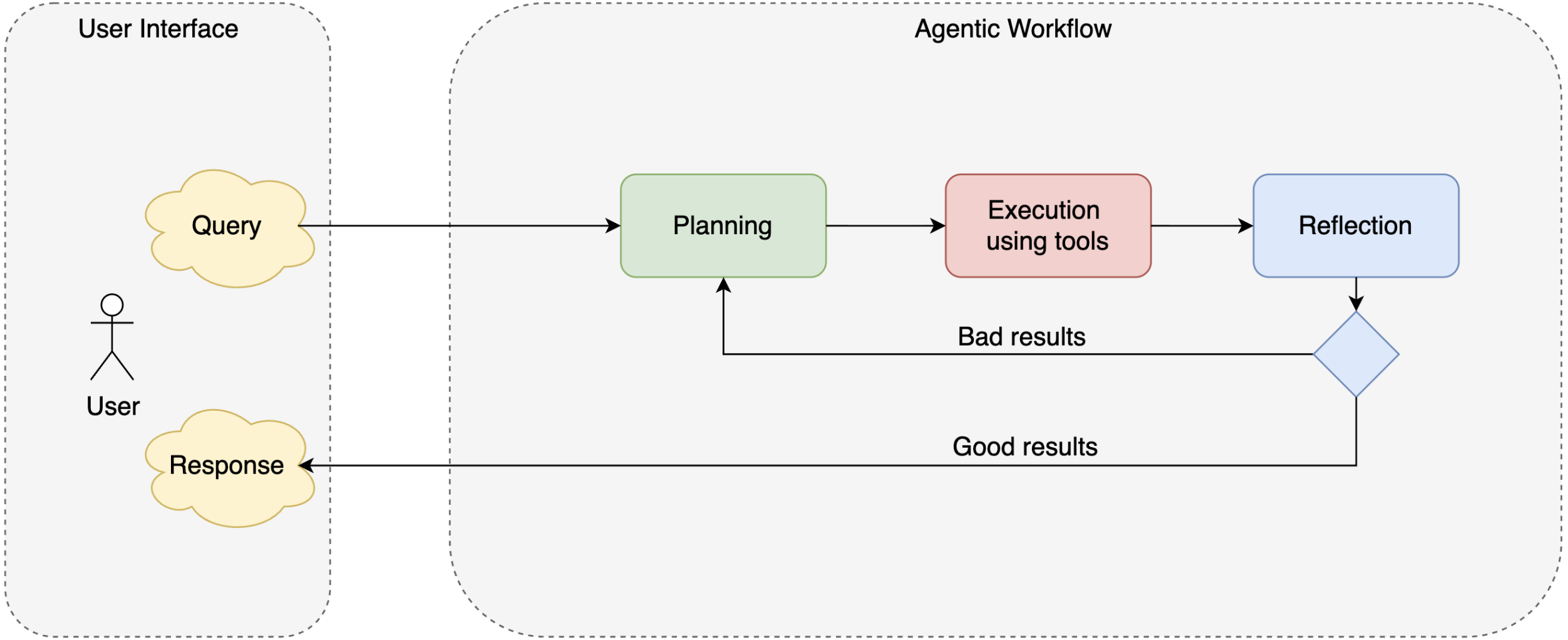
Correlation
Correlate events across services

Timeline
Reconstruct the sequence of events

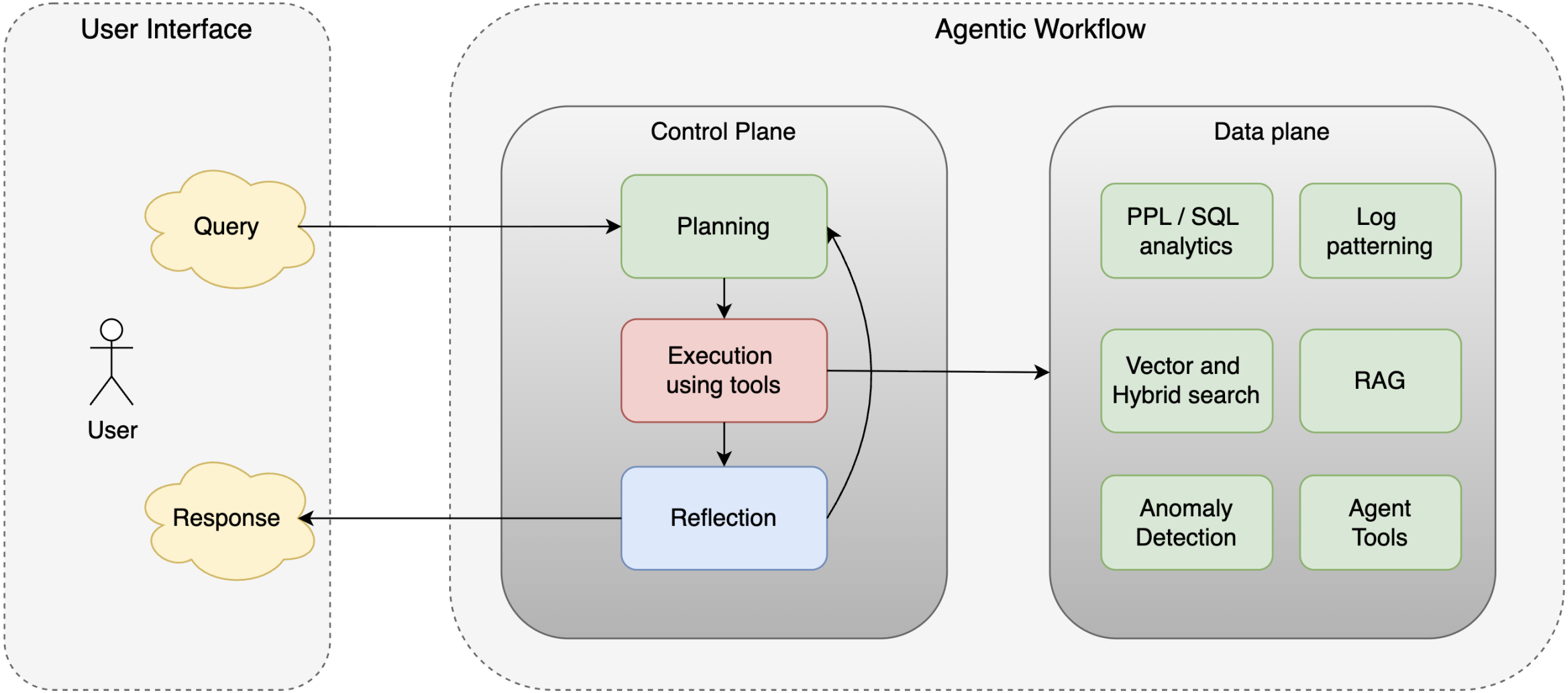
RCA
Explain root cause with evidence

From noise to **understanding**. From searching to **solving**.

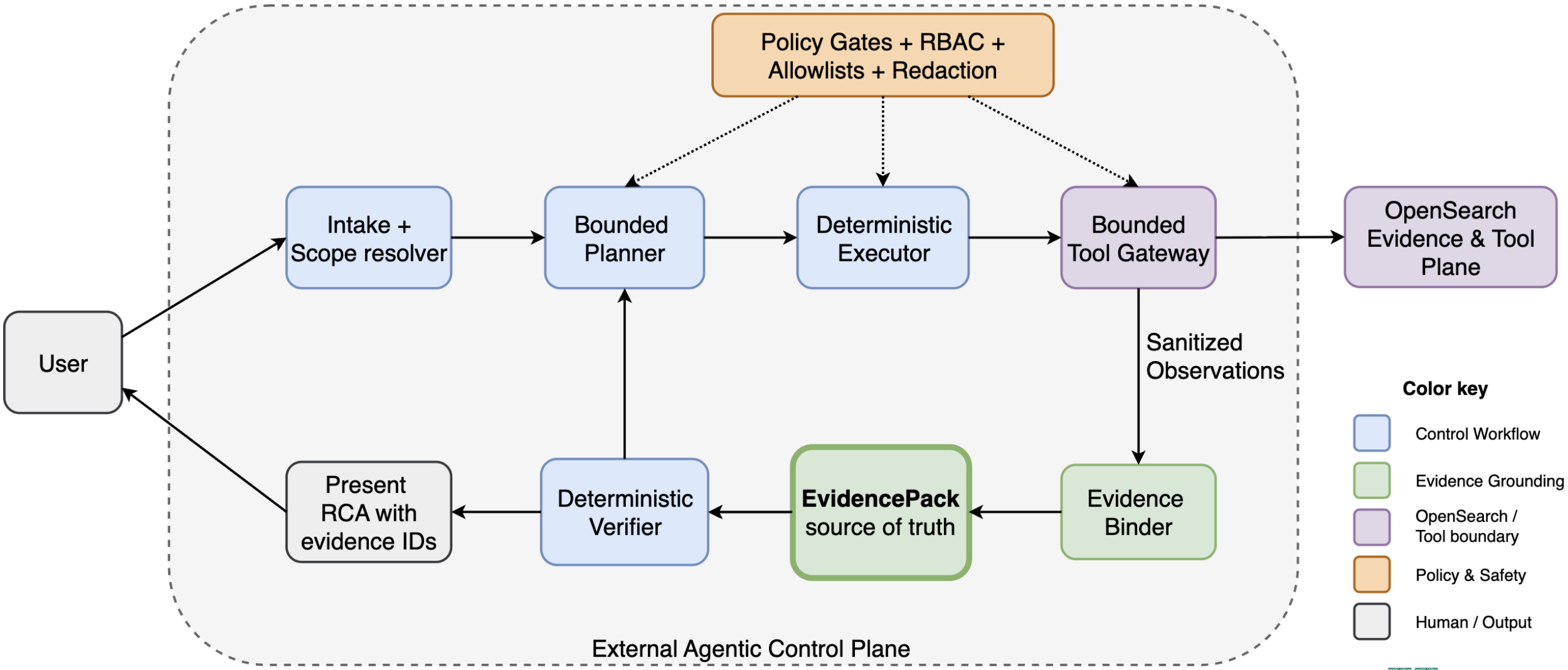
Agentic Workflow



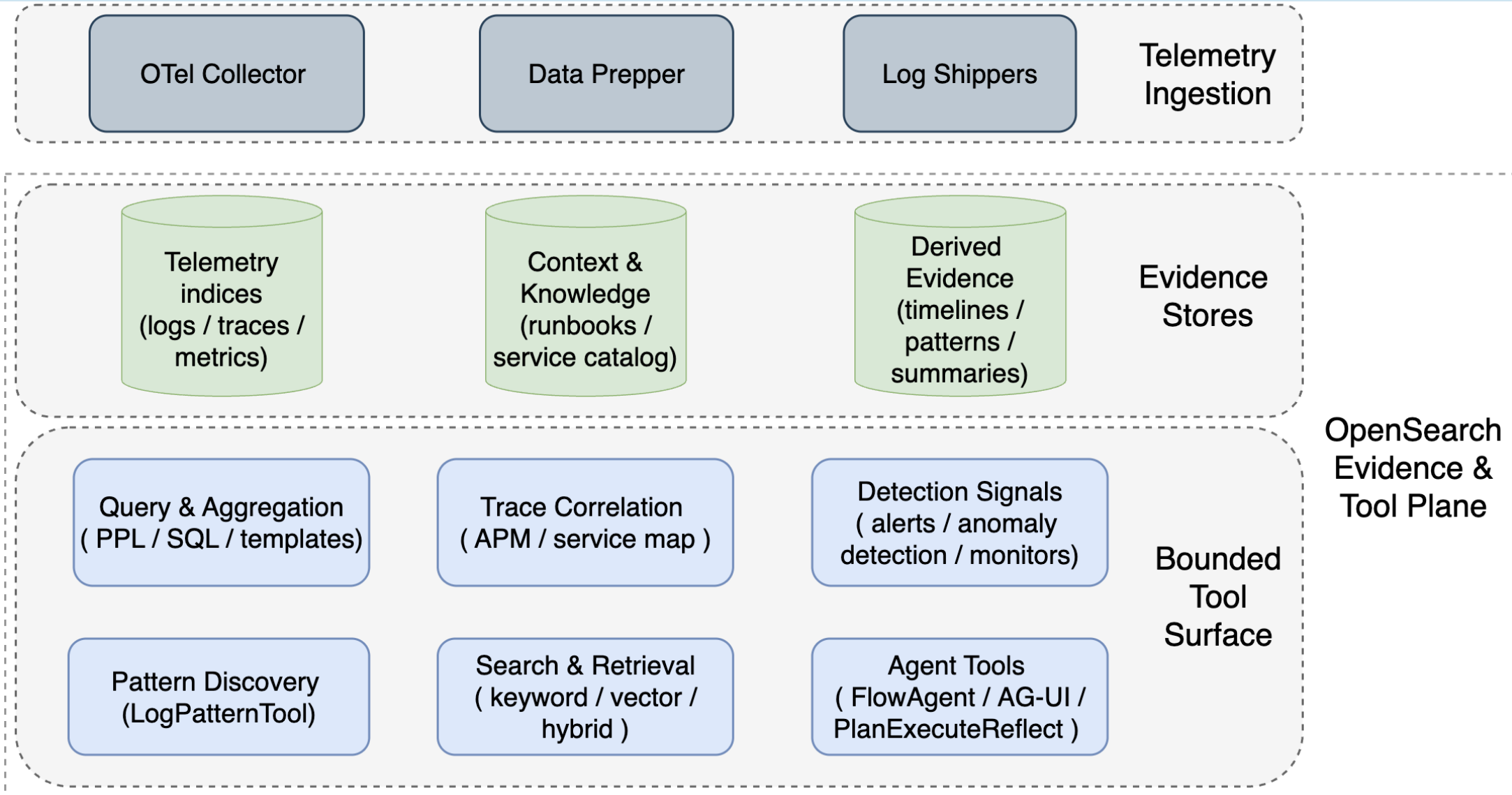
Investigation agent using OpenSearch



Implementation: External Agentic Control Plane



OpenSearch Evidence & Tool Plane

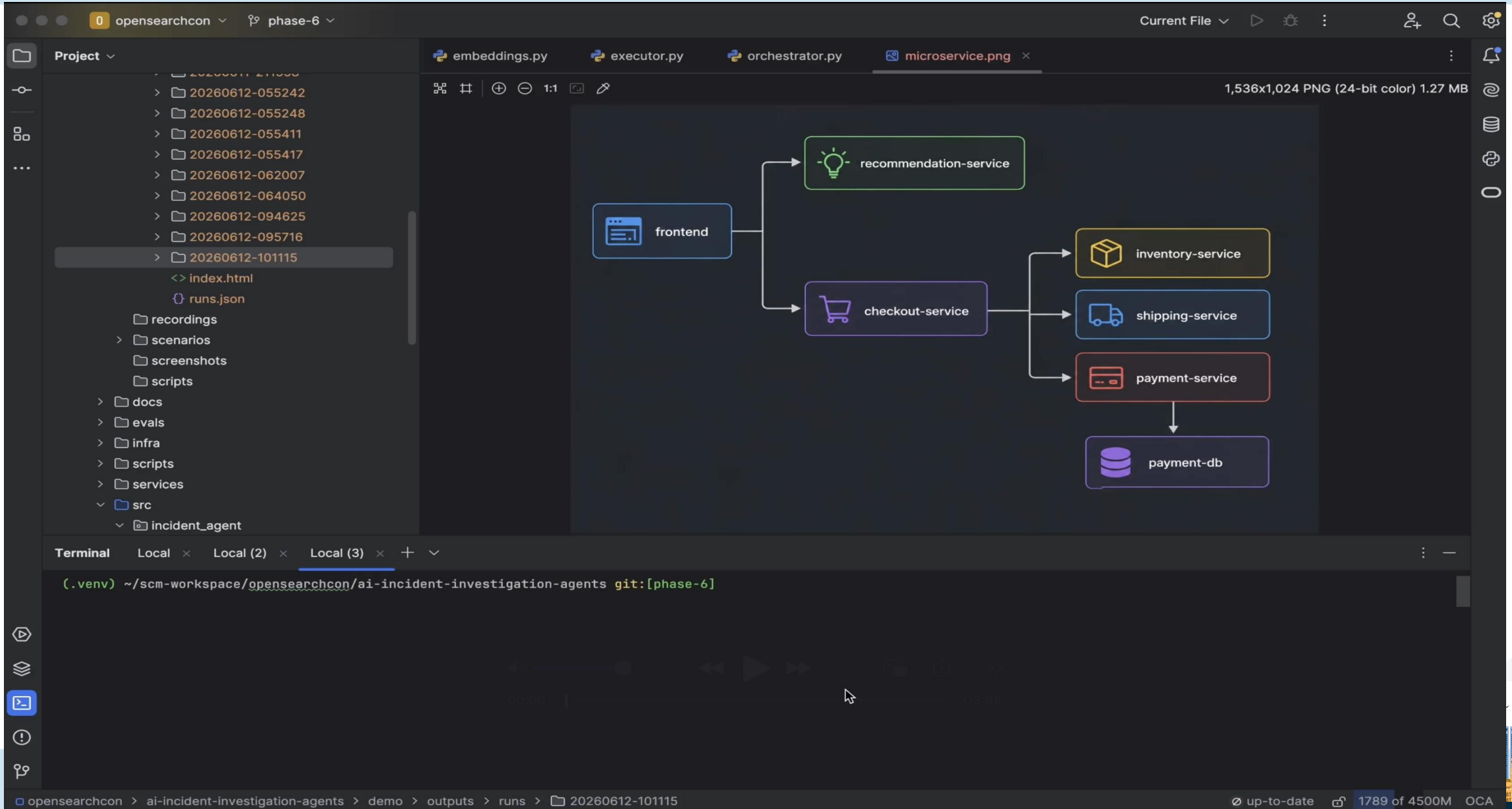


Design choices for large scale workflow system

- Use strictly **bounded** time windows and service scoping
- Use typed **search templates** rather than arbitrary planner-generated DSL/PPL queries
- Use **PIT** (Point in time) for multi-step consistency
- Keep **raw telemetry** separate from derived investigation artefacts.
- Use query **quotas**, **retries**, and **circuit breakers** at the orchestration layer

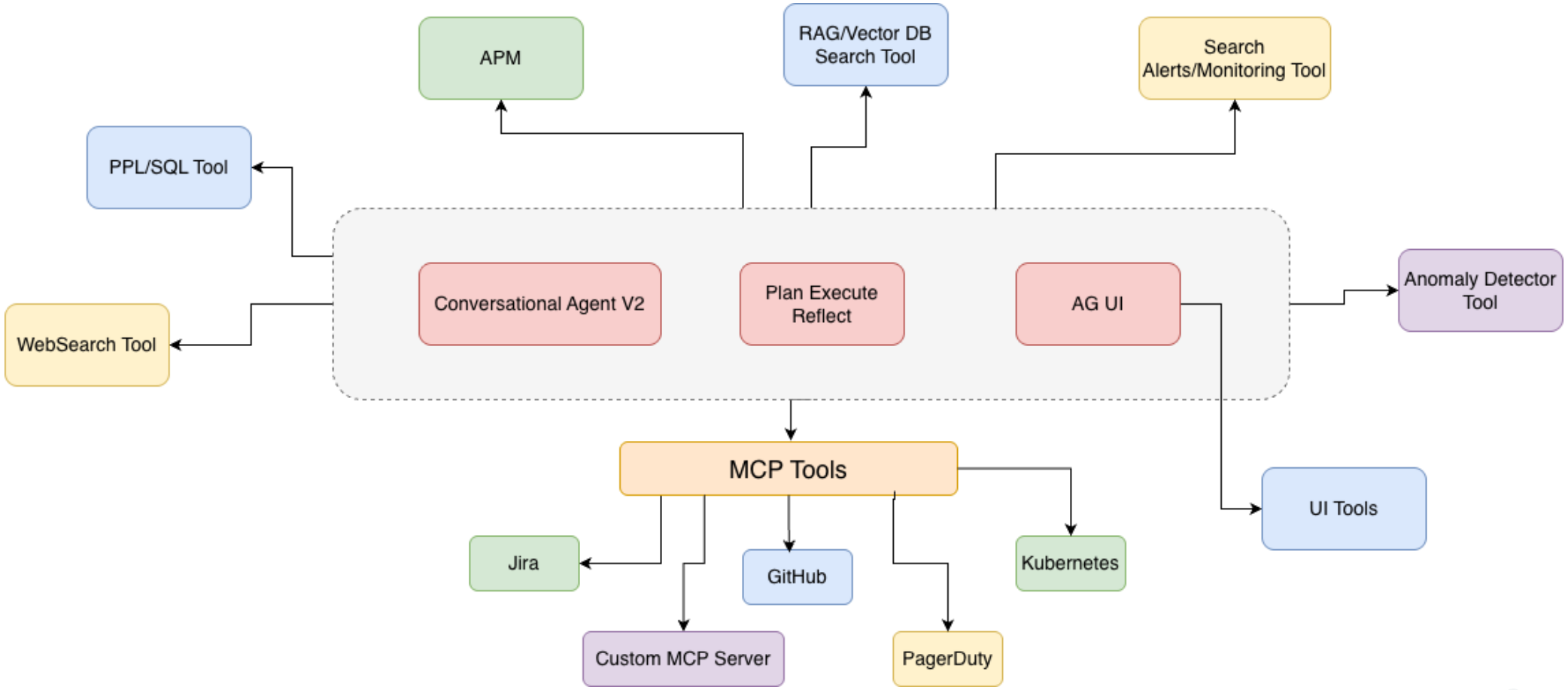
Demo for external agentic orchestration with OpenSearch

OpenSearchCon INDIA

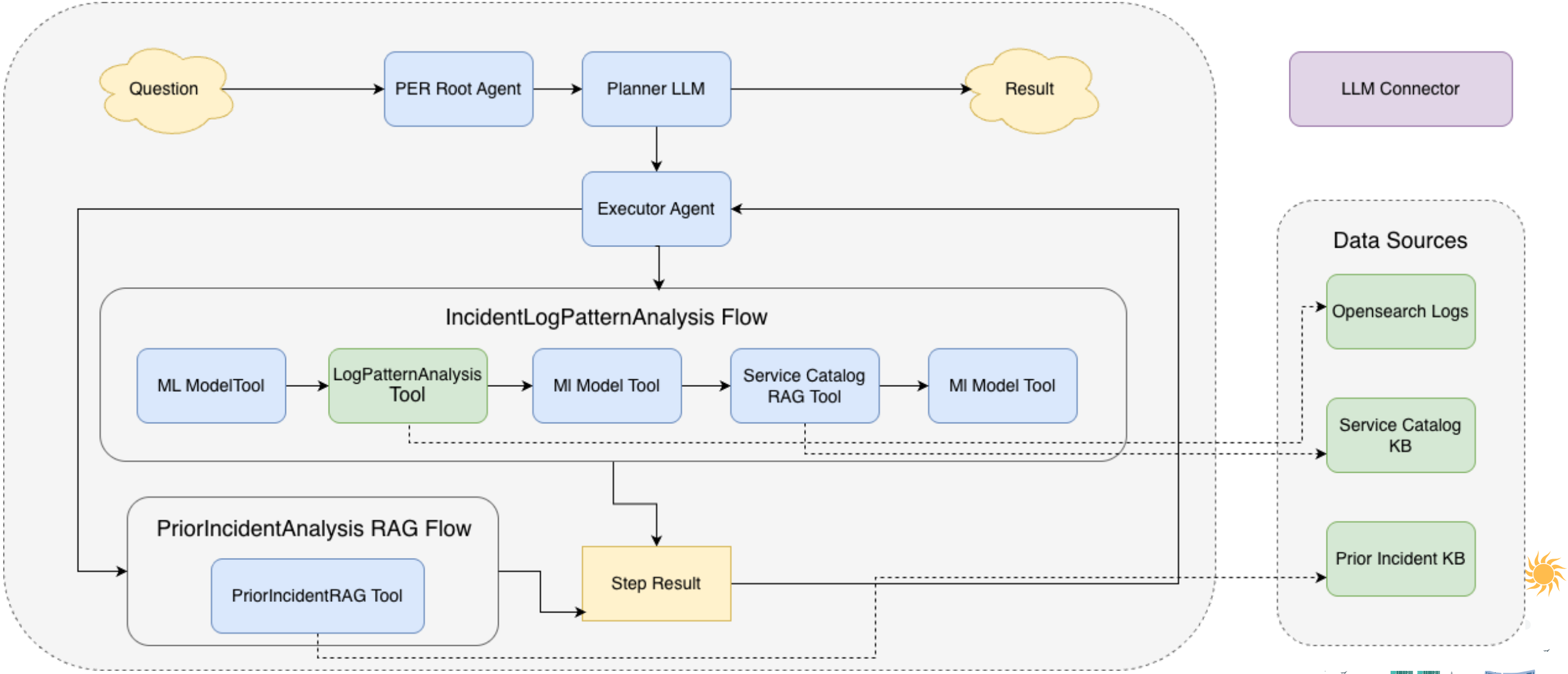


Agentic Tooling in OpenSearch

OpenSearchCon INDIA



Agentic Flow using Plan Execute Reflect Agent



Prominent Features

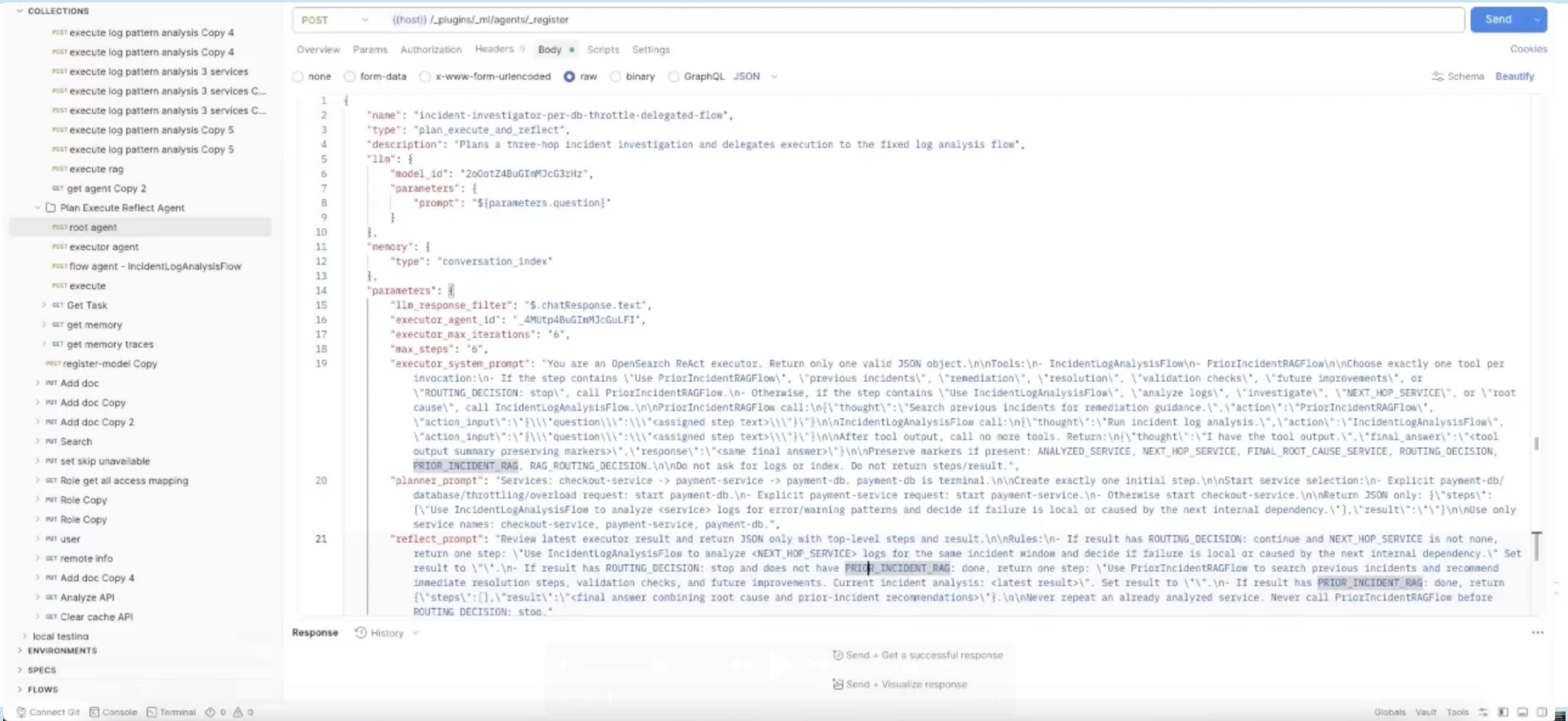
- **Extensible Plug and Play Architecture:** A baseline framework that can be extended through plug-and-play knowledge sources for service dependencies, ownership, error patterns, and log locations, reducing the complexity of the prompts.

- **Continuous Operational Learning:** Operators can refine the system over time by curating resolved incidents, runbooks, and lessons learned into the incident and service knowledge bases.

- **Hybrid Agent Orchestration:** PER agent handles adaptive, evidence-driven investigation, while flow agents execute deterministic analysis paths such as structured log search.

Demo for Plan Execute Reflect Agent

OpenSearchCon INDIA



Reflections

OpenSearchCon INDIA

Dimension	OpenSearch Agentic Tools	External Agentic Tools
Scope of solution	Best for focused, end-to-end investigation inside OpenSearch using native tools, logs, alerts, search, and ML Commons agents.	Better for broader workflows spanning many enterprise systems, custom APIs, ticketing, deployment systems, and external state.
Scale	Suitable for smaller flows with limited parallel execution and checkpointing needs.	Better manageability for large-scale, parallel, long-running, and resumable workflows.
Guardrails	Guardrails depend on tool permissions, prompts, connector controls, and OpenSearch security boundaries.	Stronger control over action approval, policy enforcement, retries, checkpoints, and audit gates.
Complexity	Planner is prompt-driven and simple to set up, making it fast for POCs and bounded investigation flows.	Supports elaborate rules, explicit workflow logic, state machines, and custom orchestration patterns.

Questions & Answers

OpenSearchCon INDIA