Application Components of the Project

1. Log Ingestion Service

- Accepts raw unstructured logs.
- Validates and forwards logs for processing.
- Acts as system entry point.

2. Log Processing Service

- Parses raw logs.
- Normalizes logs into structured LogEvent.
- Prepares data for detection analysis.

3. Detection Service

- Applies rule-based detection.
- Performs anomaly detection.
- Generates DetectionSignal objects.

3.1) Rule Engine

- Matches known log patterns.
- Identifies predefined failure scenarios.

3.2) Anomaly Engine

- Detects unusual behavior (e.g., error spikes).
- Identifies unknown or abnormal events.

4. Incident Management Service

- Correlates detection signals.
- Creates and updates incidents.
- Maintains incident lifecycle (Open, Escalated, Resolved).

5. Response Automation Engine

- Selects appropriate playbooks.
- Applies safety and approval policies.
- Decides auto-execution or manual intervention.

6. Playbook Module

- Stores predefined response strategies.
- Contains ordered recovery steps (PlaybookStep).

7. Response Executor

- Executes approved playbook steps.
- Interacts with system actuators.

8. Notification Service

- Notifies analysts about incidents.
- Sends alerts for escalations or failures.

9. Audit Service

- Records system actions and decisions.
- Maintains compliance logs and reports.

10. System Actuator (Interface)

- Executes system-level actions (e.g., restart service).
- Supports extensibility for future integrations.