External Entities

1. **Apps / Servers**
    - Generate operational and error logs.
    - Receive update notifications or recovery status from the system.
2. **System Executor**
    - Defines, creates, and updates response rules and automation logic.
    - Provides configuration data to the incident response system.
3. **On-Call Engineer**
    - Receives incident details.
    - Performs manual review and approval for critical incidents.
4. **Notification System**
    - Delivers alerts and notifications to engineers and systems.

Main Process

Log-Driven Incident Response System

- Collects logs from apps/servers.
- Analyzes logs to detect failures or anomalies.
- Applies predefined rules to decide responses.
- Triggers alerts and notifications.
- Supports manual intervention when required.

Data Flows

1. **Apps / Servers → Log-Driven Incident Response System**
    - *Data:* Logs (error logs, performance logs, system events)
2. **System Executor → Log-Driven Incident Response System**
    - *Data:* Automation rules, response policies, updates
3. **Log-Driven Incident Response System → Notification System**
    - *Data:* Failure alerts, incident notifications
4. **Notification System → Apps / Servers**
    - *Data:* Update notifications, recovery actions, status messages
5. **On-Call Engineer ↔ Log-Driven Incident Response System**

- *Data:* Incident review, manual approval, override decisions