DFD Level-1: Log-Driven Incident Response System

In **Level-1 DFD**, the main process *"Log-Driven Incident Response System"* is decomposed into multiple sub-processes to show internal working and data movement.

External Entities

- **Apps / Servers**
- **System Executor**
- **On-Call Engineer**
- **Notification System**

Data Stores

- **D1: Log Repository** – Stores incoming application/server logs
- **D2: Rule Store** – Stores incident detection and response rules
- **D3: Incident Records** – Stores detected incidents and their status

---

Processes

1.0 Log Collection

- **Input:** Logs from Apps / Servers
- **Operation:** Collects and normalizes logs
- **Output:** Structured logs
- **Data Store:** Saves logs into **Log Repository (D1)**

Data Flow:

- Apps / Servers → 1.0 Log Collection → D1 Log Repository

2.0 Log Analysis & Failure Detection

- **Input:** Logs from Log Repository
- **Operation:** Analyzes logs to detect errors, anomalies, or failures
- **Output:** Failure events / incident candidates

Data Flow:

- D1 Log Repository → 2.0 Log Analysis

3.0 Rule Evaluation & Decision Engine

- **Input:**
  - Detected failures
  - Rules from System Executor
- **Operation:** Matches failures against rules to decide actions
- **Data Stores:**
  - Reads rules from **Rule Store (D2)**
  - Writes incidents to **Incident Records (D3)**

Data Flow:

- System Executor → D2 Rule Store
- 2.0 Log Analysis → 3.0 Rule Evaluation
- 3.0 Rule Evaluation → D3 Incident Records

4.0 Incident Handling

- **Input:** Incident data from Incident Records
- **Operation:**
  - Determines whether automation or manual approval is required
  - Handles incident lifecycle (new, ongoing, resolved)

Data Flow:

- D3 Incident Records → 4.0 Incident Handling

5.0 Manual Approval & Review

- **Input:** Critical incidents requiring human intervention
- **Operation:** On-Call Engineer reviews and approves/overrides actions
- **Output:** Approval or rejection decision

Data Flow:

- 4.0 Incident Handling → On-Call Engineer
- On-Call Engineer → 4.0 Incident Handling

6.0 Alert & Notification Management

- **Input:** Confirmed incidents and actions taken

- **Operation:** Sends alerts and updates
- **Output:** Notifications to engineers and systems

Data Flow:

- 4.0 Incident Handling → 6.0 Alert Management
- 6.0 Alert Management → Notification System
- Notification System → Apps / Servers