Level-1 DFD Description:

Log-Driven Incident Response System

The Level-1 Data Flow Diagram expands the overall system shown in the Level-0 DFD into detailed internal processes. It explains how raw logs are collected, analyzed, converted into incidents, and handled through automated and manual response mechanisms.

External Entities

- **Log Source**: Generates raw logs and alerts from applications, servers, or infrastructure.
- **System Administrator**: Maintains and modifies response playbooks.
- **Analyst**: Receives notifications and handles escalated incidents.
- **Notification Service**: Sends alerts and updates to analysts and administrators.

Processes and Data Flow

1.0 Log Ingestion

This process collects **raw logs and alerts** from the Log Source. It acts as the entry point of the system and ensures continuous ingestion of log data for further analysis.

Output: Raw logs

2.0 Log Parsing & Normalization

The raw logs are parsed and normalized into a consistent structured format. This makes logs easier to analyze and compare.

Data Store Used:

- **D1: Log Repository** – stores processed and normalized logs.

3.0 Detection Service

This process analyzes processed logs to detect anomalies, errors, or suspicious patterns using predefined rules or detection logic.

Output: Incident context

4.0 Incident Management Service

Based on the detected incident context, this process creates and manages incidents. It assigns severity, tracks status, and stores incident details.

Data Store Used:

- **D2: Incident Store** – maintains incident records throughout their lifecycle.

5.0 Playbook Selection & Execution

The system selects an appropriate response playbook based on the incident type and severity, then executes predefined actions.

Data Store Used:

- **D3: Playbook Store** – contains automated response workflows.
- The **System Administrator** can modify or update playbooks when required.

6.0 Response Actuation

This process executes the selected response actions, such as restarting services, blocking IPs, or isolating components, and tracks action execution status.

Output: Action status

7.0 Failure Handling & Escalation

If automated actions fail or exceed safety limits, the incident is escalated. Notifications are sent to analysts via the Notification Service for manual intervention.

Output: Escalation records

8.0 Reporting & Audit Logging

All actions, decisions, and escalations are logged for compliance, auditing, and analysis purposes.

Data Store Used:

- **D4: Audit Log Store** – stores audit trails and reports.

Overall Flow Summary

1. Logs are ingested and normalized.
2. Potential incidents are detected and managed.
3. Automated playbooks are executed where possible.
4. Failures trigger escalation and analyst involvement.
5. All activities are logged for auditing and reporting.