Level 1 DFD — Automated Log Analysis & Incident Management System

```
Log Source / Agent
        │ Log Data
        ▼
   ● 1.0 Ingest Logs
        │
        ▼
   [Raw Log DB]
        │
        ▼
   ● 2.0 Parse & Normalize
        │ Normalized Logs
        ▼
   [Normalized Logs DB] ────────── Log Data ──────────┐
        │                                              │
        ▼                                              │
   ● 3.0 Analyze Logs                                  │
        │                                              │
        ▼                                              │
   ● 4.0 Detect Incidents                              │
        │ Store Incident                               │
        ▼                                              │
   [Incident DB]                                       │
        │ Incident Data                                │
        ▼                                              ▼
                          ● 9.0 Reporting & Search
   View Reports   Report Request   Filtered Results   Search Query   View Request   Display Reports   Store Generated Reports
        │              │                 │                │              │                │                    │
      [Admin]                        [Analyst]        [Viewer]                                          [Reports DB]
        │                                 │               │
        ▼                                 ▼               │
   ● 8.0 Manage Rules          ● 7.0 Manage Users & Auth
        │                            │ Authentication
        ▼                            ▼                ▼
   [Rules DB]                  [Auth Service]     [User DB]
        │ Risk Rules
        ▼
   ● 5.0 Classify Risk
        │
        ▼
   ● 6.0 Generate Alerts
        │ Alert Notification
        ▼
   [Notification Service]          [Audit Logs]
```