USE CASE DESCRIPTION

Automated Log Analysis and Incident Response System

Primary Actors

- Application / Server – Generates logs
- On-call Engineer – Provides manual approval and intervention
- System Executor – Executes automated recovery actions
- Notification System – Receives alerts and updates

Description

This use case describes how the system ingests logs from application servers, analyzes them using rule-based and anomaly-based techniques, correlates events into incidents, and performs automated recovery actions using predefined playbooks. For high-risk actions or failed automation, the system involves an on-call engineer and sends notifications through an external notification system.

Preconditions

- Application services are running and generating logs
- Detection rules and response playbooks are configured
- System executor and notification system are available

Trigger

An application or server generates log entries during normal operation or failure conditions.

Main Flow (Normal Scenario)

1. Application / Server generates log data.
2. Logs are ingested and analyzed internally by the system.
3. Known failures are identified using rule-based analysis.
4. Unknown or abnormal behavior is detected using anomaly detection.
5. The system correlates detected signals and creates or updates an incident.
6. The Incident Manager determines whether the incident can be handled automatically.
7. The system executes the appropriate response playbook.
8. The Automated Response is performed using the System Executor.

9. The incident is updated and recorded.
10. Notifications are sent to the Notification System.

Alternate Flow A – Manual Approval Required (<<extend>>)

1. The Incident Manager identifies a high-impact or risky recovery action.
2. The system requests manual approval from the On-call Engineer.
3. The On-call Engineer reviews the incident details.
4. Upon approval, the response playbook is executed.
5. The incident status is updated and notifications are sent.

Alternate Flow B – Failure or Exception (<<extend>>)

1. The automated response fails during execution.
2. The failure or exception is recorded by the system.
3. The incident is escalated for manual intervention.
4. A notification is sent to the On-call Engineer through the Notification System.

Postconditions

- The incident is resolved automatically or escalated to the On-call Engineer
- Incident details, actions, and outcomes are recorded
- Notifications reflect the current incident status

Business Value

- Reduces Mean Time To Recovery (MTTR)
- Enables safe and controlled automation
- Minimizes alert fatigue and manual intervention
- Provides consistent, auditable incident handling