ZAALIMA DEVELOPMENT

ZAALIMA
DEVELOPMENT

PYTHON DEVELOPMENT INTERNSHIP

A PROJECT PPT Presentation ON

“Sentinel – Real-time log Monitoring & Anomaly Detection”

Presented by

Ayisha Arbin MJ

Under the guidance of

Zaalima Development Team

Introduction

Modern applications generate thousands of logs every second.

Manually checking logs is slow, boring, and risk-prone.

Sentinel solves this using automatic real-time monitoring + ML-based detection.

Suspicious logs are instantly sent to Slack as alerts.

Problem Statement

Companies struggle with :

Missed critical errors

System failures

Security attacks hidden in logs

No real-time notifications

Goal: Build a system that watches logs continuously, detects anomalies, and alerts instantly.

Project Objective

Develop a real-time log monitoring system.

Detect unusual patterns using a machine learning model.

Send immediate alerts to Slack channels.

Create an end-to-end workflow similar to real DevOps environments.

Tools & Technologies

Python

Pandas

Scikit-Learn (Isolation Forest)

Slack Webhooks

Requests Library

VS Code / Terminal

System Architecture

1. Log Source → Read log file in real-time
2. Preprocessing → Clean + encode log data
3. ML Model → Isolation Forest detects anomalies
4. Alert Module → Slack webhook triggers alert
5. User → Receives "⚠ Anomaly Detected" in Slack

Workflow Diagram

1. Log file updates
2. Script detects new log lines
3. Model predicts anomaly
4. If anomaly = true
5. Slack alert sent to channel
6. User views alert instantly

Key Features

Real-time monitoring

Smart ML-based anomaly detection

Instant Slack alert system

Lightweight and easy to run

Industry-like DevOps workflow

Fully automated

What Makes Sentinel Unique?

Real-time automation (not static)

Slack integration (professional & practical)

Uses a real ML model, not dummy logic

Solves an actual real-world DevOps problem

Scalable for future integration

Shows skills in ML + Python + Automation + API integration

Sample Output

Terminal Output:

⚠ ANOMALY DETECTED!

🚨 Slack Alert Sent Successfully!

Slack Output:

🚨 Sentinel Alert

Anomaly Detected in Logs

timestamp: 5

level: 0

message: 3

Advantages

Faster issue response

Prevents major system failures

Detects unknown or hidden issues

No manual monitoring needed

Boosts reliability of applications

Limitations

Needs structured log format

Model accuracy improves with more data

Requires internet for Slack alerts

Future Enhancements

Add severity levels (low/medium/high)

Build a dashboard (Streamlit / Power BI)

Add SMS & email notifications

Train model on more diverse logs

Add multiple log sources (multi-file monitoring)

Conclusion

Successfully built SENTINEL, a real-time log monitoring + anomaly detection system.

Integrated Slack for instant alerting.

Demonstrates strong automation, ML, and API integration skills.

Real-world ready project useful in DevOps, Security, and IT Operations.