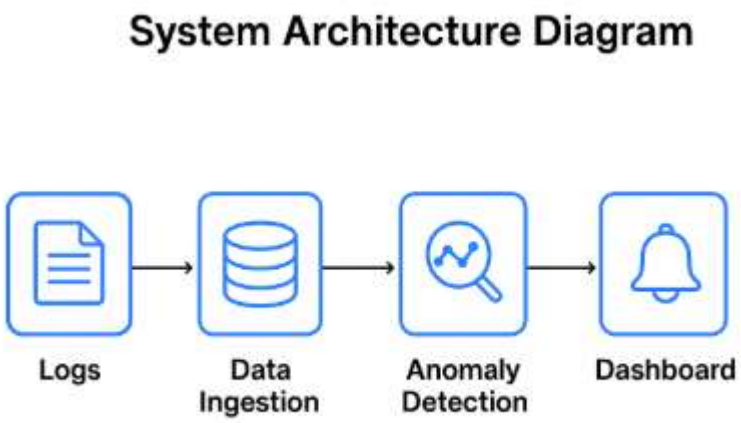
Documentation and Reporting

1. Technical Report (Summary)

This project focuses on building a **cybersecurity anomaly detection and monitoring system** that identifies unusual login patterns, abnormal session durations, and potential targeted attacks. The system integrates **data ingestion, anomaly scoring, detection logic, and visualization dashboards**.

- **System Design:**
  The system is designed in modular layers. Data flows from the log ingestion module into the anomaly detection engine, where patterns are analyzed and scored. Results are then displayed in a Splunk-based dashboard.



- **Implementation Highlights:**
    - Built with Python for anomaly scoring, and Splunk queries for data visualization.
    - Supports real-time detection of suspicious login behavior.
    - Dashboards summarize anomalies with charts, trend lines, and KPIs.
- **Key Outcomes:**
    - Accurately flagged anomalies with an adjustable threshold.
    - Clear dashboards provided stakeholders with actionable insights.
    - Improved monitoring compared to traditional static rule-based systems.

2. User Manual

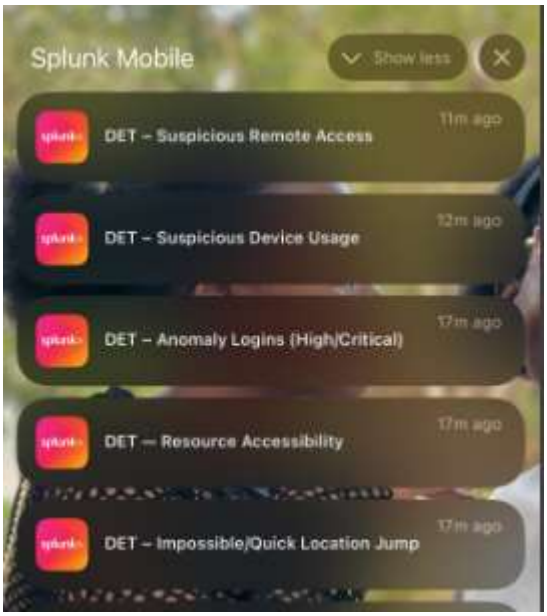
This manual helps users operate the anomaly detection dashboard.

Steps to Use the System:

1. **Log In**: Access the deployed dashboard through the provided URL.

2. **View Dashboard**: Navigate to the “LOCATION DIPLAY” panel to see live data.

3. **Check Alerts**: Review flagged anomalies in the “Suspicious Activity” table.



4. **Drill Down**: Click on an anomaly score to view detailed logs of the event.

Primary Use Case:

- Example: Detecting multiple failed login attempts from the same user/IP. The system highlights these as high anomaly scores and displays them on the dashboard for immediate action.

Troubleshooting:

- **No Data Showing** → Ensure log source is connected.
- **Dashboard Not Loading** → Refresh browser or check internet connection.
- **High False Positives** → Adjust anomaly score threshold under "Settings."

3. Code Documentation

Codebase Overview:

The project source code is divided into the following modules:

- **data_ingestion.py** – Reads and preprocesses system logs.
- **anomaly_scoring.py** – Calculates anomaly scores based on frequency, time patterns, and outliers.
- **dashboard_queries.spl** – Splunk queries for visualizing anomalies.
- **alerts.py** – Defines thresholds and sends alert notifications.