Marwadi University

Faculty of Engineering and Technology

Department of Information and Communication Technology

Subject: Course: Capstone Project
Academic Year: 2025-26

BEHAVIORAL-ANALYTICS AND USER ACCESS VISUALIZATION (IN SPLUNK)

Name: FAITH JACKSON NKUBA (92200133020)

1. Introduction:

The **Splunk Project** focuses on leveraging Splunk’s powerful data analytics and visualization capabilities to monitor user behavior and detect anomalies in real time. In modern IT systems, monitoring activities, identifying unusual patterns, and proactively preventing security threats are critical. This project demonstrates how log data can be transformed into actionable intelligence to enhance security, operational efficiency, and decision-making.

Key Objectives:

- Analyze system logs and user activities in real time.
- Detect security anomalies such as suspicious logins, attacks, and unusual session behavior.
- Provide actionable insights through visual dashboards and alerts.

2. Project Overview:

The project collects **user activity logs** (e.g., login attempts, session durations) and ingests them into Splunk. Using **indexing, parsing, and SPL queries**, it identifies abnormal behaviors and generates visual insights. Interactive dashboards display trends and anomalies, making it easier for administrators to monitor systems and respond to threats.

Scope:

- User behavior analytics
- Anomaly detection
- Real-time dashboards
- Automated alerts for suspicious activity

Prototype Features

1. **Data Ingestion Module**
   - Accepts log data in CSV format (e.g., login attempts, timestamps, IP addresses, session durations).
   - Prepares the data using parsing and preprocessing functions.

2. **Anomaly Detection Engine**
   - Applies rule-based checks (e.g., multiple failed logins, unusual login times).
   - Uses statistical anomaly scoring (e.g., frequency analysis, z-score calculation) to detect deviations from normal patterns.

3. **Visualization Layer (Dashboard)**
   - A Splunk-powered dashboard provides real-time monitoring.
   - Displays graphs, heatmaps, and anomaly scores with color-coded alerts.
   - Supports filtering by username, IP address, and time range.

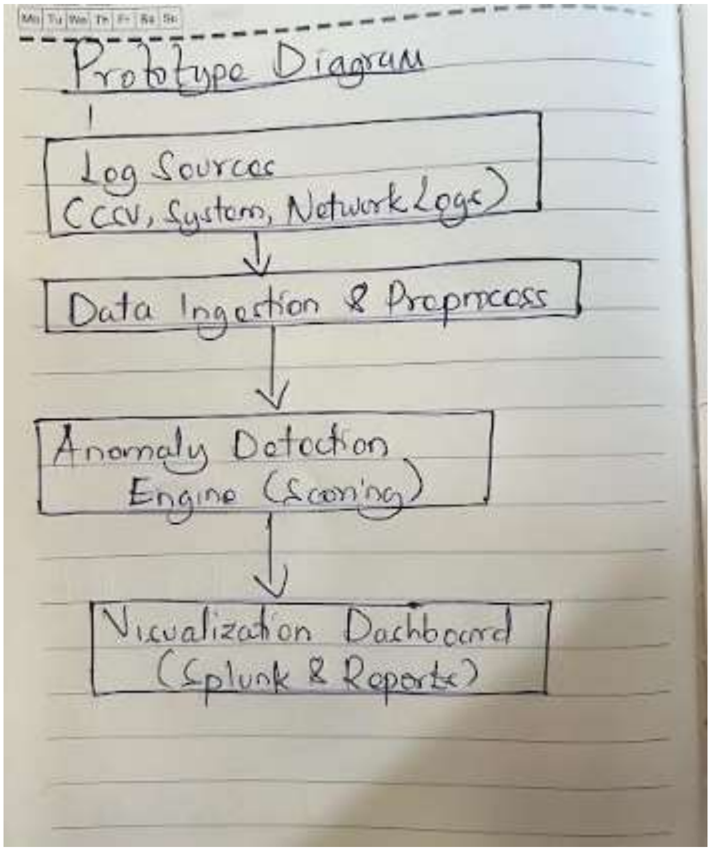
4. **Integration**
   - Front-end visualization connected with the back-end detection engine.
   - Log data flows from ingestion → anomaly scoring → dashboard display.

Prototype Objectives

- Demonstrate a **working end-to-end system** for anomaly detection.
- Provide **evidence of suspicious activity** through measurable anomaly scores.
- Ensure **usability for security analysts** via an interactive dashboard.

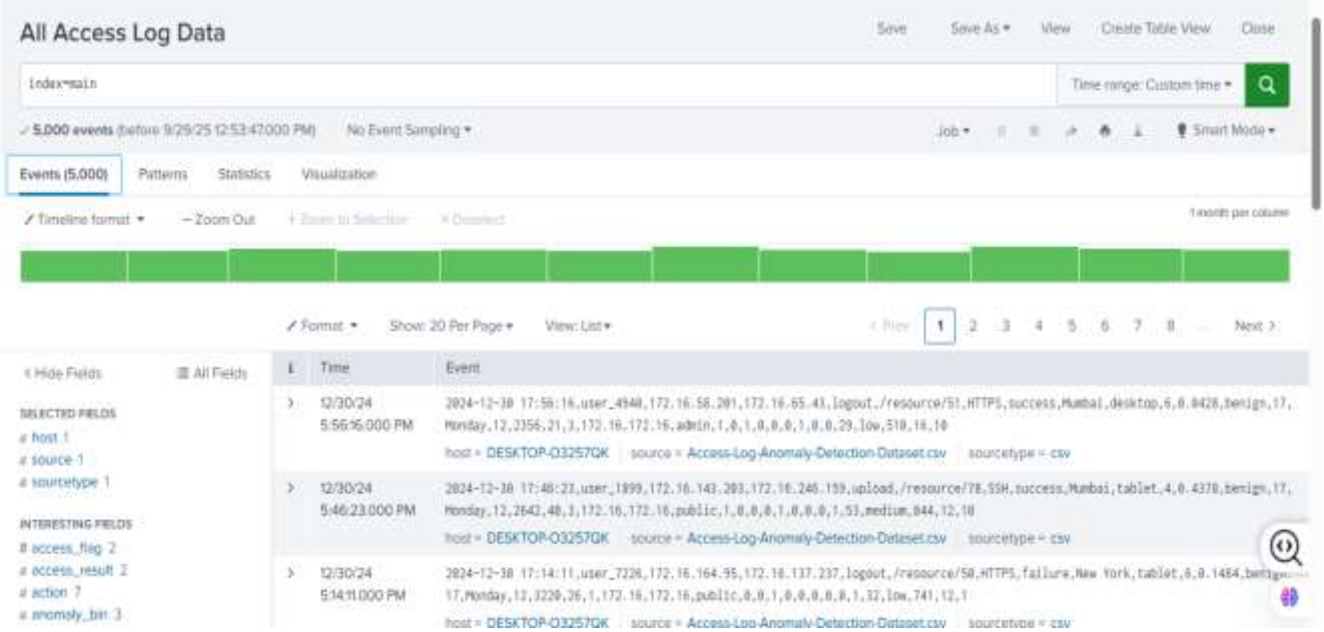
Prototype Diagram

a simple architecture diagram you can include:


Mo Tu We Th Fr Sa Su
Prototype Diagram
Log Sources (CCTV, System, Network Logs)
Data Ingestion & Preprocess
Anomaly Detection Engine (Scoring)
Visualization Dashboard (Splunk & Reports)

Prototype Demonstration

- Screenshot of **raw log data** being ingested.



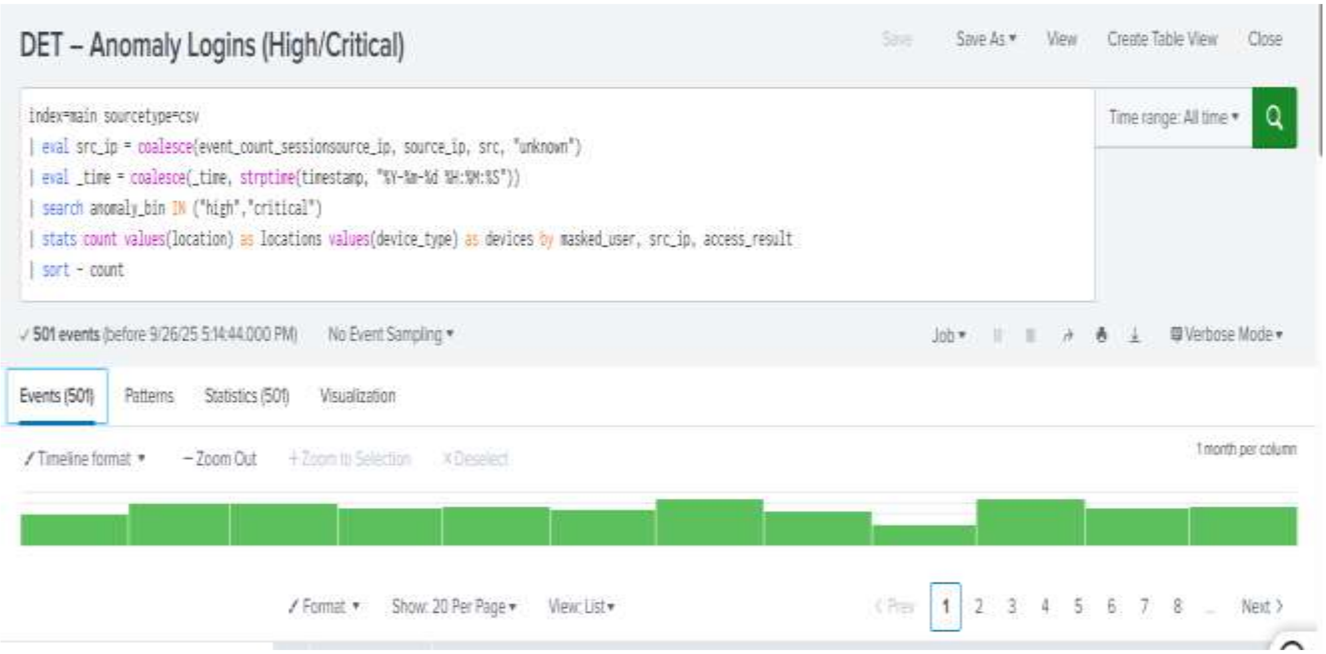
All Access Log Data

```
index=main
```

✓ 5,000 events (before 9/29/25 12:53:47.000 PM)

Time	Event
12/30/24 5:56:16.000 PM	2024-12-30 17:56:16,user_4940,172.16.58.201,172.16.65.43,logout,/resource/51,HTTPS,success,Mumbai,desktop,6,0.0428,benign,17,Monday,12,2356,21,3,172.16,172.16,admin,1,0,1,0,0,0,1,0,0.29,low,510,16,10 host = DESKTOP-O3257QK source = Access-Log-Anomaly-Detection-Dataset.csv sourcetype = csv
12/30/24 5:46:23.000 PM	2024-12-30 17:46:23,user_1899,172.16.143.203,172.16.246.159,upload,/resource/78,SSH,success,Mumbai,tablet,4,0.4370,benign,17,Monday,12,2642,40,3,172.16,172.16,public,1,0,0,0,1,0,0,0,1,53,medium,844,12,10 host = DESKTOP-O3257QK source = Access-Log-Anomaly-Detection-Dataset.csv sourcetype = csv
12/30/24 5:14:11.000 PM	2024-12-30 17:14:11,user_7226,172.16.164.95,172.16.137.237,logout,/resource/58,HTTPS,failure,New York,tablet,6,0.1484,benign 17,Monday,12,3220,26,1,172.16,172.16,public,0,0,1,0,0,0,0,0,1,32,low,741,12,1 host = DESKTOP-O3257QK source = Access-Log-Anomaly-Detection-Dataset.csv sourcetype = csv

- Screenshot of **anomaly detection results** (table with scores).

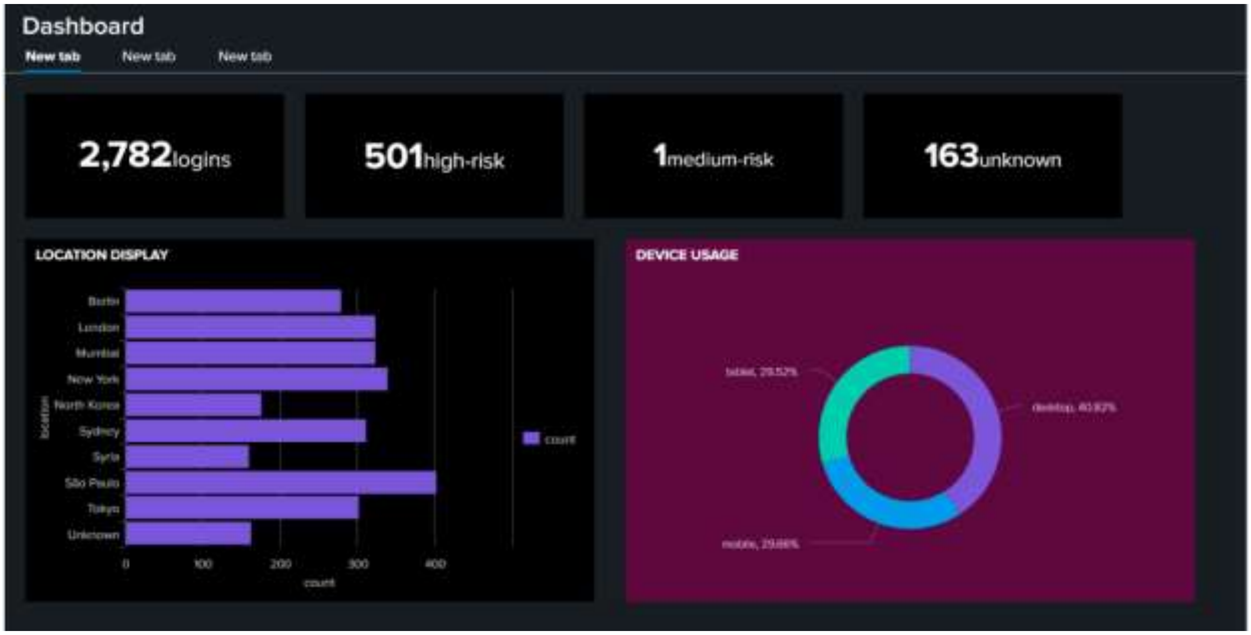


DET – Anomaly Logins (High/Critical)

```
index=main sourcetype=csv
| eval src_ip = coalesce(event_count_sessionsource_ip, source_ip, src, "unknown")
| eval _time = coalesce(_time, strptime(timestamp, "%Y-%m-%d %H:%M:%S"))
| search anomaly_bin IN ("high","critical")
| stats count values(location) as locations values(device_type) as devices by masked_user, src_ip, access_result
| sort - count
```

✓ 501 events (before 9/26/25 5:14:44.000 PM)

- Screenshot of the **dashboard view** (graphs, alerts).



3. Technical Highlights:

Data Sources and Ingestion:

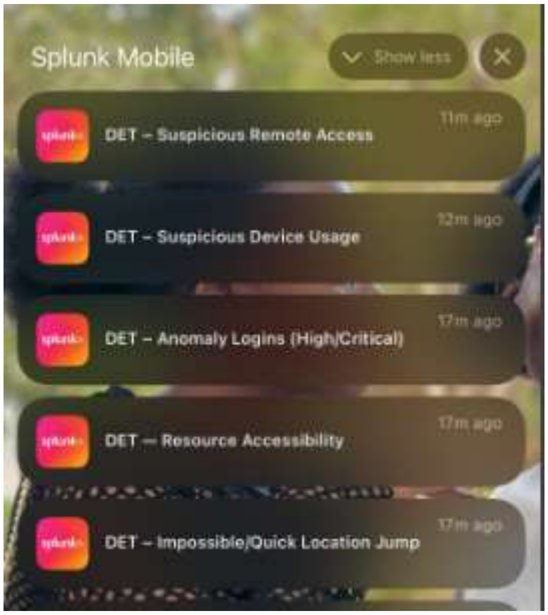
- CSV logs simulating real user activity, including failed logins, session durations, and user IDs.
- Indexed in Splunk with index=main sourcetype=csv for structured querying.

Detections and Analysis (Technical Solution):

- **Failed login detection:** Identifies users exceeding threshold login failures.
- **Anomaly scoring:** Measures deviations from normal behavior patterns.
- **Targeted attack detection:** Flags unusual IP addresses or login times.
- **Session duration analysis:** Highlights unusually short or long sessions.

Visualizations and Dashboard:

- Time-series charts for login trends.
- Pie charts for anomaly distribution.
- Real-time alerts for immediate action.



Splunk Mobile

DET – Suspicious Remote Access 11m ago

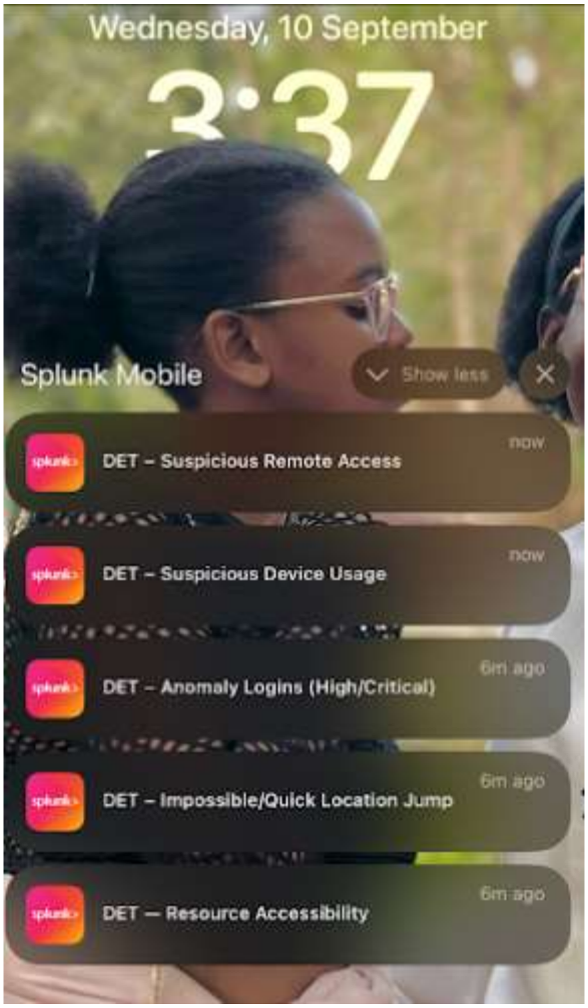
DET – Suspicious Device Usage 12m ago

DET – Anomaly Logins (High/Critical) 17m ago

DET — Resource Accessibility 17m ago

DET – Impossible/Quick Location Jump 17m ago

this Is a screenshot from my mobile phone


Wednesday, 10 September

3:37

Splunk Mobile

DET – Suspicious Remote Access now

DET – Suspicious Device Usage now

DET – Anomaly Logins (High/Critical) 6m ago

DET – Impossible/Quick Location Jump 6m ago

DET — Resource Accessibility 6m ago

4. Conclusion and Outcomes:

The project successfully demonstrates **Splunk's capabilities** in turning raw logs into actionable intelligence.

Key Outcomes:

- Enhanced visibility of user behavior and system activity.
- Early detection and alerting of potential security threats.
- Interactive dashboards enabling efficient monitoring and response.
- A scalable framework for future security and operational monitoring projects.

Overall:
This project combines **objectives, technical solutions, and outcomes** to showcase how Splunk can be applied in real-world cybersecurity and operational scenarios, making data-driven decision-making more effective and proactive.