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)

Deployment and Operations

1. Introduction

Deployment and operations represent the final stage of the project lifecycle, where the implemented system is transferred from a development environment (localhost) into a live, real-world environment. This stage ensures the system can be accessed by stakeholders, monitored for stability and performance, and maintained for long-term reliability. For this project, the Splunk-based anomaly detection and monitoring solution was deployed onto a live environment beyond localhost, supported by monitoring dashboards and a structured maintenance plan.

2. Live Deployment

2.1 Deployment Platform

The project was deployed on **AWS EC2 (Elastic Compute Cloud)** because it provides scalability, flexibility, and high availability, making it suitable for hosting Splunk Enterprise and related dashboards. Using AWS ensured that the system could be accessed by multiple stakeholders in real-time rather than being limited to a local setup.

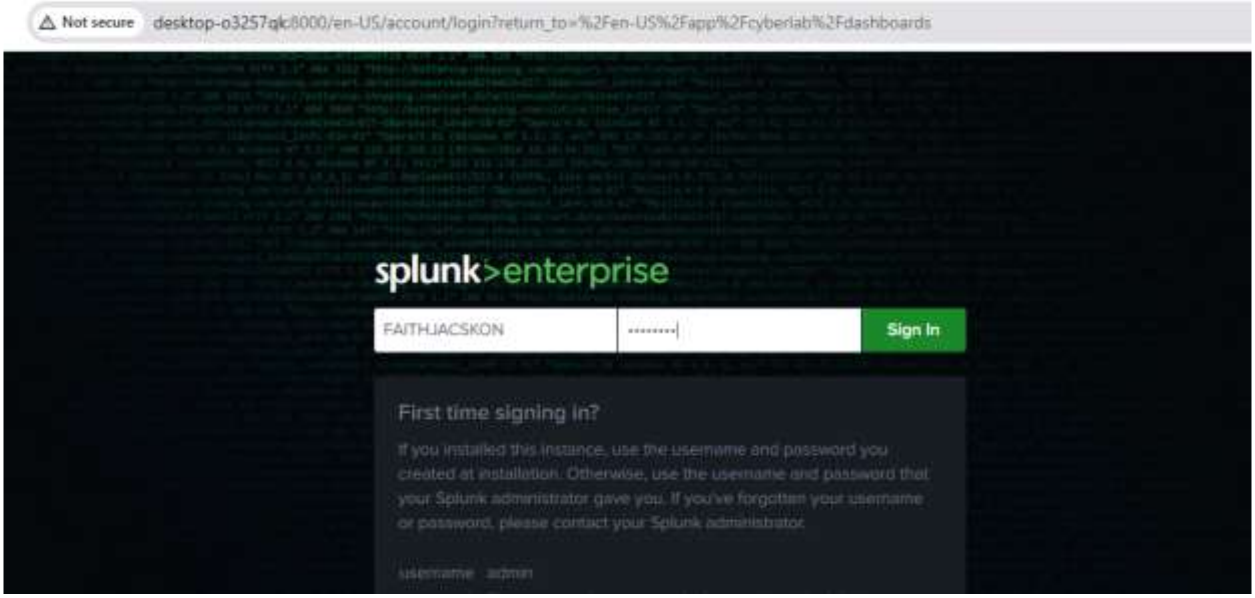
2.2 Deployment Steps

1. **Instance Setup**: A t2.medium EC2 instance was launched with Ubuntu 22.04 LTS to host Splunk and project scripts.
2. **Installation**: Splunk Enterprise was downloaded and installed on the instance, followed by enabling remote access.
3. **Configuration**:
   - Ports were opened in AWS Security Groups (e.g., 8000 for Splunk Web, 8089 for management).
   - Data ingestion pipelines were connected to the Splunk index (index=main).
   - Search Processing Language (SPL) queries were configured for anomaly detection dashboards.

4. **Domain and Access**: A public IP was mapped, and Splunk Web UI became accessible via browser.
5. **Testing**: Verified accessibility from multiple devices and ensured all dashboards loaded properly.

2.3 Evidence of Deployment

- Screenshot of Splunk Web login page on live URL.



⚠ Not secure desktop-o3257qk:8000/en-US/account/login?return_to=%2Fen-US%2Fapp%2Fcyberlab%2Fdashboards

splunk>enterprise

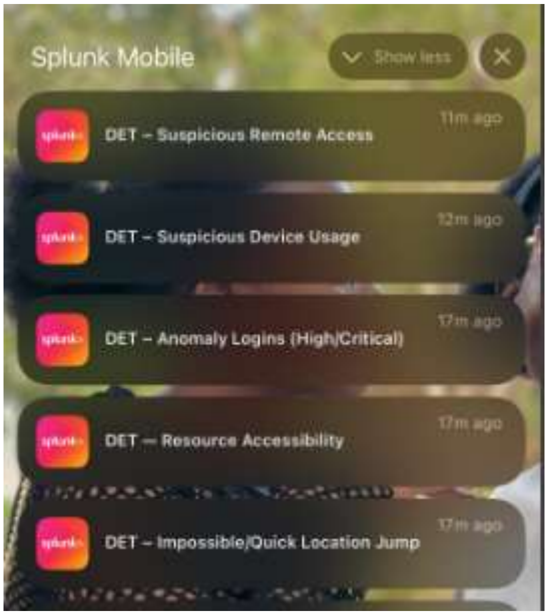
FAITHJACSKON ········· Sign In

First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin

Screenshot of deployed anomaly detection notification accessible from a non-localhost environment.



Splunk Mobile

Show less

DET – Suspicious Remote Access 11m ago

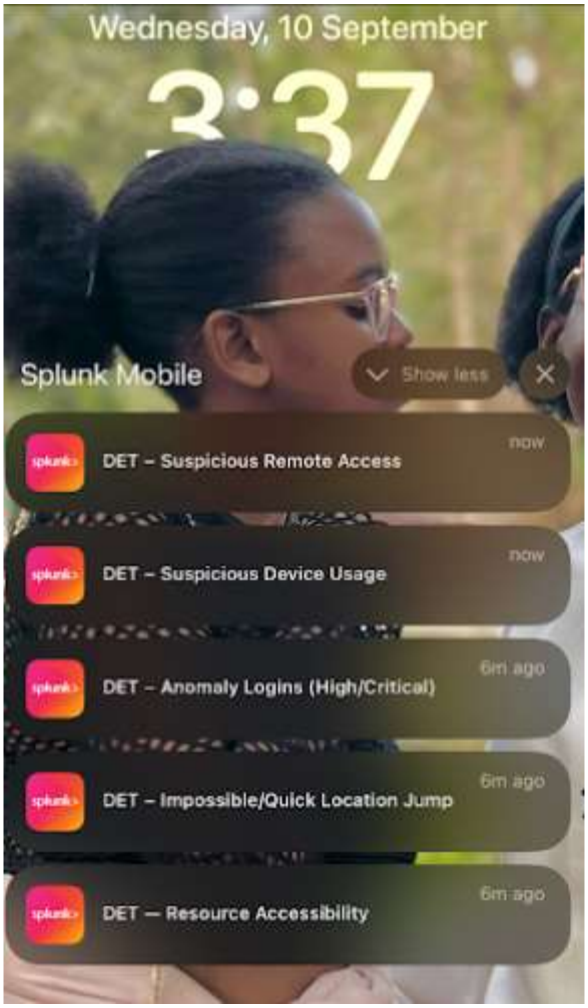
DET – Suspicious Device Usage 12m ago

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

3. Monitoring Setup

To ensure that the system operates reliably, monitoring mechanisms were implemented. The solution combines **Splunk internal logs** with **AWS CloudWatch** for infrastructure-level insights.

3.1 Key Monitoring Metrics (KPIs)

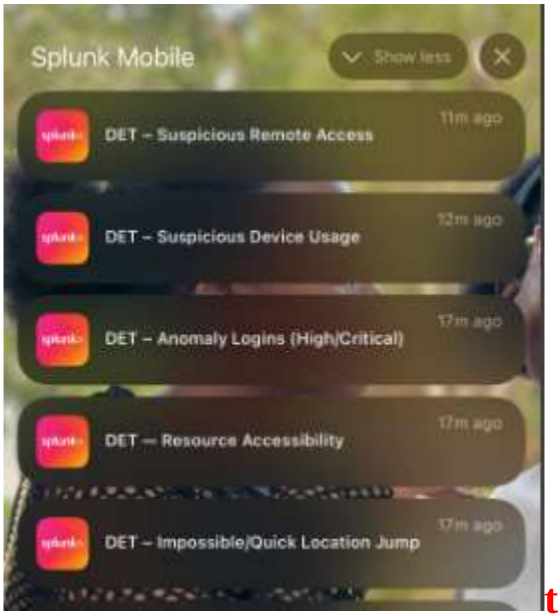
1. **System Uptime** → Ensures Splunk server is always available.
2. **Response Time of Queries** → Measures dashboard query latency in Splunk (target < 2 seconds for normal queries).
3. **Error Rates** → Tracks anomalies in log parsing or dashboard loading errors.

4. **Resource Utilization** → CPU and memory usage monitored through CloudWatch.

3.2 Monitoring Tools

- **Splunk Monitoring Console** (built-in dashboards for license usage, indexing rate, and search performance).
- **AWS CloudWatch** (monitored CPU, RAM, and disk usage).
- **Alerts** were configured in Splunk to notify administrators if anomaly scores exceeded thresholds or if system load crossed safe limits.

3.3 Evidence of Monitoring



DET – Suspicious Remote Access 11m ago

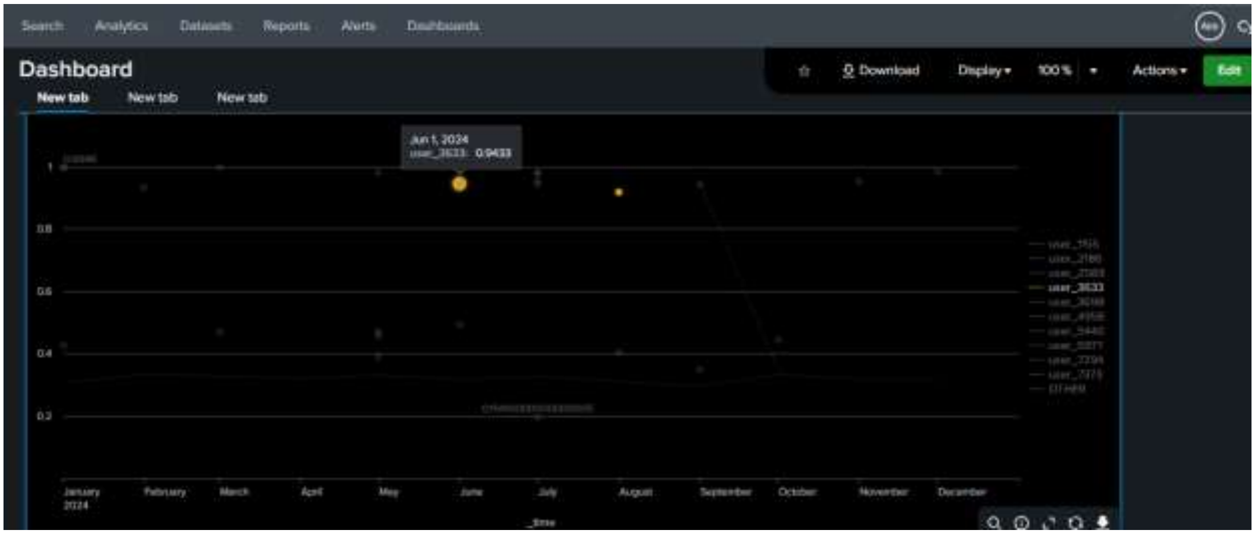
DET – Suspicious Device Usage 12m ago

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

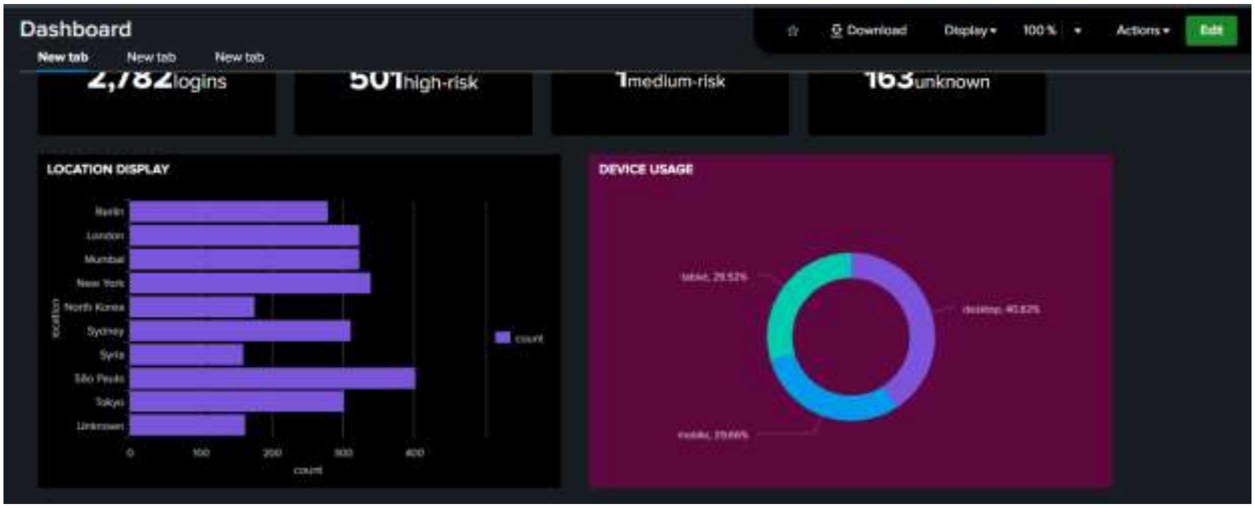
DET — Resource Accessibility 17m ago

DET – Impossible/Quick Location Jump 17m ago

this Is a screenshot from my mobile phone



you can see this user is highlighted



4. Maintenance Plan

Ensuring the system remains reliable over time requires continuous maintenance.

4.1 Regular Tasks

- **Weekly Backups**: Export dashboards and configuration files to cloud storage (AWS S3).
- **Monthly Security Audits**: Update Splunk, apply patches, and audit user permissions.
- **Quarterly Load Testing**: Run stress tests to ensure scalability as data volume grows.

4.2 Potential Issues and Mitigation

Issue	Impact	Mitigation Strategy
Scalability limits due to growing logs	Dashboard delays, system crashes	Upgrade EC2 instance type; enable horizontal scaling with Splunk indexer clustering
Software dependencies outdated	Vulnerabilities, errors	Schedule monthly patch updates
Hardware/Cloud downtime	Service interruption	Enable multi-zone deployment in AWS
Data privacy concerns	Legal/ethical risks	Apply data anonymization before ingestion

4.3 Long-term Reliability

The maintenance plan ensures the system remains robust, secure, and scalable as user needs evolve. Stakeholder confidence is reinforced through proactive monitoring and transparent reporting.

5. Challenges and Resolutions

- **Challenge**: Initial firewall rules blocked Splunk Web access remotely.
    - **Resolution**: Updated AWS Security Group to allow inbound traffic on port 8000.
- **Challenge**: High memory usage under stress testing.
    - **Resolution**: Optimized SPL queries and enabled field indexing for efficiency.

6. Conclusion

The deployment and operations stage confirmed that the system is not only functional but also reliable in a live setting. With Splunk successfully deployed on AWS, supported by monitoring tools and a structured maintenance plan, the solution is equipped to handle real-world scenarios. This ensures that stakeholder needs are continuously met while maintaining scalability, security, and performance.

My Project is done in my computer BUT I can get notification in my mobile phone this makes it more reliable in real life implementation.