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)

Ideation and Stakeholder Needs Analysis

I. Stakeholder Identification

The success of any ICT solution depends on its ability to serve the needs of its stakeholders. For the proposed Splunk-based cybersecurity anomaly detection project, the primary stakeholders include:

1. **Small and Medium Enterprises (SMEs):**
   SMEs face growing cybersecurity risks but often lack the financial and technical resources to deploy advanced SIEM (Security Information and Event Management) solutions. They require **cost-effective, easy to deploy monitoring systems** that provide visibility into cyber threats [1].

2. **Cybersecurity Analysts:**
   Security teams are burdened by a large volume of alerts, many of which are false positives. Analysts require **dashboards with contextual insights** that allow them to prioritize genuine threats quickly [2].

3. **Educational Institutions and Students:**
   Universities and training centers increasingly use Splunk as a learning tool. They require **hands-on platforms** to train students in real-world cybersecurity practices without compromising sensitive data [3].

4. **End-users (Employees and Customers):**
   While indirect stakeholders, they are impacted by security breaches. Their need is for **data privacy, trust, and protection** from insider misuse or external attacks [4].

II. Stakeholder Needs Analysis

A systematic review of reports and case studies highlights specific needs:

- **Affordability and Accessibility:** SMEs cannot always afford enterprise Splunk licenses; therefore, a lightweight, student/project-friendly version is needed [1].
- **Reduced Analyst Fatigue:** Research shows that over **45% of SOC analysts quit within 2 years** due to stress from false positives and alert overload [2]. This demonstrates the urgent need for **smart anomaly detection with reduced noise**.
- **Educational Relevance:** The demand for cybersecurity professionals is projected to grow by **32% by 2032**, according to the U.S. Bureau of Labor Statistics [5]. Educational institutions need practical platforms to train students in SOC (Security Operations Center) workflows.
- **Data Privacy and Ethics:** GDPR and similar laws mandate data anonymization. Stakeholders need assurance that monitoring does not compromise personal data [4].

III. Problem Statement

Based on stakeholder needs, the problem can be defined as follows:

“Small and medium enterprises, as well as educational institutions, lack affordable, user-friendly, and scalable cybersecurity monitoring systems that provide actionable insights while ensuring data privacy and reducing false positives in anomaly detection.”

IV. Solution Ideation

The ideation phase generated **three creative solutions** that address stakeholder needs:

1. **Splunk-Powered Anomaly Detection Dashboard**
    - A customizable Splunk dashboard that detects login anomalies, unusual session durations, and suspicious user behavior.
    - Meets stakeholder needs by providing **real-time visibility** with **interactive charts**.
    - Aligned with ICT trends in **SIEM and real-time analytics**.
2. **Anomaly Scoring with Machine Learning Toolkit (MLTK)**
    - Integration of Splunk MLTK for anomaly scoring and contextual alerts.
    - Reduces false positives by correlating behaviors (e.g., login from unusual geolocation + abnormal session length).
    - Aligned with ICT trends in **AI-driven analytics** [2].
3. **Lightweight Cloud-Based Deployment for SMEs and Universities**
    - Provides a **practical training ground** for students and a **low-cost security tool** for SMEs.
    - Aligned with ICT domains of **cloud computing and DevOps** [3].

V. Relevance to ICT Domain

The proposed solutions are strongly connected to current ICT trends:

- **Artificial Intelligence & Machine Learning:** Used in anomaly detection and predictive alerting.
- **Cloud Computing:** Ensures scalable and cost-effective deployment models.
- **Cybersecurity and Network Security:** Directly addresses global challenges in cyber defense.
- **Big Data and Visualization:** Splunk’s indexing and dashboards transform raw log data into actionable intelligence.

The project's potential impact includes:

- **For SMEs:** Affordable monitoring solutions to improve resilience.
- **For Analysts:** Reduced alert fatigue and improved efficiency.
- **For Education:** Realistic training platforms that prepare students for SOC environments.

VI. Conclusion

The ideation and stakeholder needs analysis demonstrate a clear demand for a Splunk based anomaly detection system that balances affordability, usability, and scalability. By focusing on the needs of SMEs, cybersecurity analysts, and educational institutions, the project is both **practically relevant** and **academically valuable**. The creative solution ideas real-time dashboards, anomaly scoring, and cloud deployment are well aligned with current ICT trends and address pressing cybersecurity challenges.

References

[1] Gartner, *Market Guide for Security Information and Event Management*, Gartner Inc., 2024.
[2] J. Kim et al., "Deep learning-based anomaly detection in cybersecurity: A survey," *IEEE Access*, vol. 9, pp. 140–156, 2021.
[3] Splunk Inc., *Splunk in Higher Education: A Practical Guide*, Whitepaper, 2023.
[4] European Union, *General Data Protection Regulation (GDPR)*, Official Journal of the EU, 2016.
[5] U.S. Bureau of Labor Statistics, "Information Security Analysts: Occupational Outlook Handbook," 2023.