**Building a SIEM Dashboard using ELK Stack**

Submitted by: **TANISHA GUPTA**

College: United College of Engineering and Research  
Course Name: Cyber Security

Supervisor’s Name: Ayush Kumar

**ABSTRACT**

In the evolving landscape of cybersecurity, real-time monitoring and analysis of system logs is crucial. This project explores the creation of a Security Information and Event Management (SIEM) dashboard using the ELK Stack — Elasticsearch, Logstash, and Kibana.

The system ingests logs, parses and stores them efficiently, and visualizes them using Kibana dashboards for threat detection, anomaly monitoring, and alert generation.

The project demonstrates how open-source tools can build an effective SOC (Security Operations Center) solution.

**TABLE OF CONTENTS**

1. Introduction
2. Objectives
3. Technology Stack
4. System Architecture
5. Literature Review
6. Methodology and Approach
7. Dashboard Design
8. Results and Discussion
9. Conclusion

10.Future Scope

11.References

**INTRODUCTION**

Cybersecurity has become a critical area of concern for organizations. Detecting threats in real time using log analysis can prevent serious data breaches. This project focuses on building dashboards for a SIEM solution using the ELK Stack, providing a central platform for monitoring and alerting on suspicious events.

Through the integration of log data collected from diverse sources such as servers, applications, firewalls, and authentication systems, the project seeks to build insightful and interactive dashboards that deliver centralized visibility into organizational security posture. Real-time analysis of these logs not only enables threat detection but also empowers security teams to act swiftly and decisively. Kibana dashboards will serve as a dynamic interface for visualizing trends, identifying anomalies, and triggering alerts based on suspicious patterns and behavior. By leveraging the flexibility and scalability of the ELK Stack, this SIEM solution provides a cost-effective, open-source alternative to proprietary tools.

**OBJECTIVES**

* To understand and implement the ELK Stack for log analytics.
* To build real-time dashboards for visualizing system and network events.
* To detect security threats based on log patterns.
* To simulate and analyze real-world security scenarios using dashboards.

**LITERATURE REVIEW**

Security Information and Event Management (SIEM) systems have been a key tool for monitoring and analyzing security events across IT infrastructures. Prior research highlights the need for centralized log monitoring, real-time threat detection, and compliance reporting. Commercial SIEM solutions (e.g., Splunk, IBM QRadar) are widely used but often costly.

Studies suggest open-source alternatives like the ELK Stack as viable options for small to mid-sized organizations. According to [Elastic documentation](https://www.elastic.co/), ELK provides scalable, customizable log analytics capabilities. Research articles demonstrate successful applications of ELK Stack in building SOC environments, especially when configured with alerting tools and custom dashboards.

The literature emphasizes the importance of structured log collection, parsing using patterns (like GROK), and real-time data visualization for security use cases. Community forums, GitHub projects, and instructional platforms have also contributed significantly to knowledge sharing in this domain.

**TECHNOLOGY STACK**

* **Elasticsearch**: Distributed search and analytics engine.
* **Logstash**: Data processing pipeline for ingesting logs.
* **Kibana**: Visualization interface for Elasticsearch.
* **Beats (Filebeat)**: Lightweight log shipper.
* **Operating System**: Ubuntu (VM or local machine)
* **Wireshark/Zeek**: Network analysis tools for additional log sources in advance use cases.

**METHODOLOGY AND APPROACH**

**Overview of the ELK Stack**

* **Elasticsearch**: Stores, indexes, and enables efficient search of log data.
* **Logstash**: Ingests and processes data using filters and plugins.
* **Kibana**: Creates interactive visualizations and dashboards for analysis

**SYSTEM ARCHITECTURE**

* [Devices/Servers] --> [Filebeat] --> [Logstash] --> [Elasticsearch] --> [Kibana]

**Step-by-Step Implementation**

**1. Setup Environment**

* Installed Ubuntu on a virtual machine.
* Updated all packages and ensured the system was secure.

**2. Install and Configure ELK Stack**

* **Installed Elasticsearch:**

bash

sudo apt install elasticsearch

Configured elasticsearch.yml for network access.

* **Installed Logstash**:

bash

sudo apt install logstash

Created a pipeline to receive logs from Filebeat.

* **Installed Kibana:**

bash

sudo apt install kibana

Configured Kibana to connect to Elasticsearch.

**3. Install and Configure Filebeat**

* Installed Filebeat on the same system or remote machine.
* Configured it to monitor:
  + System logs: /var/log/syslog
  + Authentication logs: /var/log/auth.log
* Set Filebeat output to Logstash.

**4. Build Dashboards in Kibana**

* Connected Kibana to Elasticsearch index patterns.
* Created custom dashboards showing:
  + Failed login attempts
  + SSH activity
  + Top IP addresses
  + Log types over time (bar/line graphs)

**5. Test the Setup**

* Simulated SSH login failures.
* Monitored logs flowing through Filebeat → Logstash → Elasticsearch → Kibana.

**6. Analyzed and Interpreted Results**

* Used filters and queries in Kibana to analyze security logs.
* Verified alerts and log trends.

This process allowed me to build a complete SIEM system that can monitor and visualize system logs in real-time, helping detect potential threats efficiently.

**Data Flow Summary**

System Logs → Filebeat → Logstash (parse, enrich) → Elasticsearch (store, index) → Kibana (visualize)

**Security Detection Logic**

* Brute-force attacks: Monitored multiple failed logins in short intervals.
* Unauthorized access: Alerts triggered on unusual IP ranges.
* Service anomalies: Correlated system restarts with error logs.

**Evaluation Metrics**

* **Log latency**: Delay from generation to dashboard visualization.
* **Data integrity**: Accuracy of log parsing and field mapping.
* **Alerting efficiency**: Rate of true vs. false positives.
* **User feedback**: Usability of dashboards in incident response.

**DASHBOARD DESIGN**

Key dashboards designed in Kibana:

* **Login Attempts Overview**: Tracks successful and failed logins.
* **IP Geolocation Map**: Shows locations of external access attempts.
* **Top Alerting Hosts**: Highlights hosts with most events.
* **Brute Force Attack Panel**: Detects repeated login failures.
* **Hourly Event Timeline**: Identifies peak suspicious activity hours.
* **Threat Levels by Type**: Categorizes events by severity.

**RESULTS AND DISCUSSION**

* **Log Ingestion**: Achieved seamless ingestion of logs from multiple sources.
* **Parsing Accuracy**: GROK filters successfully extracted user, IP, and status fields.
* **Real-time Visualization**: Dashboards reflected data changes with minimal latency.
* **Anomaly Detection**: Brute-force scenarios, port scans, and unauthorized access were flagged.

**Discussion:**

* Dashboards improved incident response by highlighting patterns.
* Geolocation maps enabled quick identification of external threats.
* Some false positives occurred due to benign repetitive activity—refinements in filtering helped reduce this.

**CONCLUSION**

The ELK Stack proves to be a powerful and cost-effective solution for building SIEM dashboards. It provides real-time monitoring and forensic capabilities for security professionals. The project successfully demonstrated how logs can be transformed into actionable intelligence. Its flexibility and open-source nature make it a viable alternative to commercial SIEM tools for small to mid-sized organizations.

**FUTURE SCOPE**

* Integrate alerts via email or Slack using ElastAlert.
* Add machine learning-based anomaly detection using X-Pack.
* Scale the stack to handle enterprise-grade data flow.
* Ingest logs from cloud platforms (AWS, GCP).

**REFERENCES**

* Elastic.co Documentation (<https://www.elastic.co/guide/index.html>)
* Cybercademy: ELK for SIEM (<https://cybercademy.org/create-a-siem-with-the-open-source-elk-stack>)
* GitHub: SIEM Dashboards (<https://github.com/NiSan4844/SIEM-Visualization-using-ELK-Stack>)
* Studocu - SIEM Projects (<https://www.studocu.com/my/document/mara-university-of-technology-shah-alam/information-and-network-security/group-project-soc-siem/116089973>)