

## **TITLE**

**SECURITY ALERT MONITORING & INCIDENT  
RESPONSE USING SPLUNK ENTERPRISE**

**NAME : FOWSUNNISSA A.G**

**INTERNSHIP TRACK : CYBERSECURITY**

**TASK NUMBER : 2**

## **Abstract**

This project demonstrates the use of Splunk Enterprise as a Security Information and Event Management (SIEM) tool to monitor security events, visualize log data, identify suspicious activity patterns, and recommend appropriate incident response actions. The implementation focuses on log ingestion, data analysis, visualization, and dashboard creation to support SOC-level monitoring.

## **Objective**

The primary objective of this task is to:

- Monitor simulated security events using a SIEM tool
- Analyze log data for suspicious behavior
- Visualize security events using charts and dashboards
- Classify incidents based on severity
- Propose incident response and preventive measures

## Tool Used

- Splunk Enterprise (Free Trial)

Splunk Enterprise was selected due to its industry-wide adoption as a SIEM platform for real-time log analysis, alerting, and visualization.

## Log Sources

- System-generated security logs
- DNS / network-related event logs

The logs were ingested into Splunk and indexed for search and analysis.

## **Methodology**

1. Installed and configured Splunk Enterprise
2. Uploaded sample security log files
3. Verified data ingestion using SPL queries
4. Performed log analysis using Splunk Search Processing Language (SPL)
5. Created visualizations for security monitoring
6. Designed a centralized security dashboard
7. Analyzed event patterns and classified incidents
8. Documented incident response recommendations

## **Visualizations and Analysis**

### **1. Security Events Over Time**

Chart Type : Line Chart

Purpose:

To observe trends and spikes in security events over time, which may indicate abnormal or suspicious activity.

## **2. Event Distribution by Log Type**

Chart Type: Bar Chart

Purpose:

To understand the distribution of events across different log sources and identify dominant event types.

## **3. Top Hosts by Event Volume**

Chart Type: Pie Chart

Purpose:

To identify hosts generating a high volume of events, which could indicate misconfiguration or compromise.

## **4. Top Event Sources**

Chart Type: Column Chart

Purpose:

To analyze the most active event sources and detect potential anomalies.

## **Incident Classification**

Incident description	Severity
Sudden spike in event volume	Medium
Repeated events from same host	Medium
Abnormal source activity	High

## **Incident Response Actions**

### **Containment**

- Monitor and isolate suspicious sources
- Restrict access if required

### **Eradication**

- Investigate affected systems
- Remove malicious components

## Recovery

- Resume normal operations
- Validate system integrity

## Prevention

- Enable continuous monitoring
- Configure alerts in Splunk
- Apply security hardening policies

## Conclusion

This project successfully demonstrates the use of Splunk Enterprise for security alert monitoring and incident response. The created dashboard provides clear visibility into security events and supports effective analysis, making it suitable for SOC operations and cybersecurity monitoring tasks.