Incident Response Report – Task 2

Prepared by:Harshika Haresh Gangan (Cybersecurity Intern)

Date: June 25, 2025

# Executive Summary

This report presents the analysis of simulated security alerts captured using a Security Information and Event Management (SIEM) tool. Using the Elastic Stack (ELK) and/or Splunk, sample log data was ingested and analyzed to identify potential security incidents. The goal was to simulate SOC-level alert triage and incident response processes.

# Tools Used

- Elastic Stack (ELK)

- Sample system, network, and application log files

# Alert Analysis and Incident Classification

## Brute Force Login Attempts Detected

Classification: Credential Access

Log Source: Authentication logs

SIEM Tool: Splunk

Analysis:

Multiple failed login attempts observed from a single IP over a short time window. Pattern matches brute force behavior. Source IP: 192.168.1.101

Recommendations:

Block source IP, enforce account lockout policy, enable 2FA

## Unauthorized Access to Admin Panel

Classification: Privilege Escalation

Log Source: Web server logs

SIEM Tool: Elastic Stack (Kibana)

Analysis:

Admin panel access recorded from non-admin user without elevated privileges. Suspicious URI accessed: /admin/config.php

Recommendations:

Review access control list (ACL), revoke compromised credentials

## Unusual Data Exfiltration Patterns

Classification: Data Exfiltration

Log Source: Network traffic logs

SIEM Tool: Elastic Stack (Logstash)

Analysis:

Large outbound traffic to an external IP observed outside of business hours. Volume exceeds baseline norms. Destination IP: 45.77.23.88

Recommendations:

Alert DLP system, investigate endpoint activity, isolate affected host

# Conclusion

The simulated SIEM analysis exercise successfully demonstrated core skills in security alert triage, log analysis, and incident classification. Timely identification of suspicious activities, appropriate classification, and mitigation recommendations are essential components of an effective incident response process in modern Security Operations Centers (SOCs).