INCIDENT RESPONSE REPORT

Prepared for: Future Interns

Prepared by: K. Gautham Naga Ravi

Date: 29 August 2025

Objective

This report provides an **incident response analysis** of simulated security alerts generated using **SIEM tools** (Elastic Stack and Splunk Free Trial). The exercise focused on monitoring log data, identifying suspicious activities, classifying security incidents, and providing remediation recommendations to improve organizational security posture.

Scope

The Scope of this Report was limited to:

- Monitoring simulated alerts using **Elastic Stack (ELK)** and **Splunk**.
- Analyzing sample log files (web server logs, authentication logs, and network traffic logs).
- Identifying **suspicious activities and anomalies**.
- Classifying incidents based on severity and potential business impact.
- Providing actionable recommendations for remediation

Alert Analysis and Findings

1. Multiple Failed Login Attempts

Description: Authentication logs in Splunk revealed repeated failed login attempts on multiple user accounts within a short time frame.
Suspicious Activity: Possible brute force attack.
Incident Classification: High Severity – Authentication Threat.
Recommendation: Enforce account lockouts, implement multi-factor authentication (MFA), and monitor for further brute force attempts.

---

2. Unusual File Access Patterns

Description: ELK dashboard flagged repeated access to sensitive files outside normal business hours.
Suspicious Activity: Potential insider threat or compromised account.
Incident Classification: Medium Severity – Data Access Anomaly.
Recommendation: Review user activity logs, restrict access to sensitive files, and enforce time-based access policies.

---

3. Suspicious Outbound Traffic

Description: Network logs detected high-volume outbound connections to an untrusted external IP.
Suspicious Activity: Possible data exfiltration attempt.
Incident Classification: High Severity – Network Threat.
Recommendation: Block suspicious IPs at the firewall, analyze destination domain, and perform endpoint forensics on affected systems.

---

4. Privilege Escalation Event

Description: Splunk flagged multiple privilege escalation commands executed by a user with standard rights.
Suspicious Activity: Unauthorized privilege escalation attempt.
Incident Classification: Critical Severity – System Compromise Attempt.
Recommendation: Terminate the affected user session, reset credentials, investigate persistence mechanisms, and patch privilege escalation vulnerabilities.

---

5. Malware Indicators in Uploaded Files

Description: File upload logs analyzed in ELK showed hash matches against known malware signatures.
Suspicious Activity: Malicious file upload attempt.
Incident Classification: High Severity – Malware Threat.
Recommendation: Quarantine suspicious files, enable antivirus scanning at upload, and restrict executable file types.

Conclusion

The SIEM simulation demonstrated the importance of continuous monitoring, alert correlation, and rapid incident response. High-severity alerts such as brute force attempts, suspicious outbound traffic, and privilege escalation attempts require immediate response to prevent compromise.

Suggesstions :

- deploy automated alerting and correlation rules in ELK/Splunk.
- Enforce stricter authentication controls (MFA, lockout policies).
- Strengthen file upload security (antivirus scanning, file type restrictions).
- Implement network monitoring and geolocation-based anomaly detection.
- Conduct periodic red team/blue team exercises to test SIEM effectiveness.
