Incident Response Report

Internship Track: Cyber Security
Task 2: Security Alert Monitoring & Incident Response

1. Executive Summary

During this task, simulated security alerts were monitored using Splunk. The objective was to analyze log data, identify suspicious activities, classify incidents, and propose remediation strategies. The investigation revealed brute-force login attempts, malware detection alerts, and multiple suspicious user activities, indicating potential system compromise attempts.

2. Objective

- Monitor simulated security alerts using Splunk.
- Detect anomalies and classify incidents.
- Draft an incident response report including findings and recommendations.

3. Tools Used

- Splunk (Free Trial) – for log collection and analysis
- Sample SOC Log Files – provided test data for monitoring

4. Log Analysis & Findings

1. Failed Login Attempts
- Multiple failed login attempts observed from IP 203.0.113.77 and 198.51.100.42.
- Indicates a potential brute-force attack.

2. Suspicious User Activity
- Users alice, bob, charlie, david, and eve generated unusual activity spikes.
- Possible insider threat or compromised accounts.

3. Malware Alerts
- Splunk logs flagged malware detections on endpoints.
- Critical priority incidents reported.

4. Network Anomalies
- Repeated unauthorized access attempts from unusual IP addresses.

5. Incident Classification

- Brute Force Attack Attempts: Unauthorized login attempts from external IPs.
- Malware Infection: Endpoints flagged with malware detection alerts.
- Suspicious Account Activity: Multiple flagged users showing abnormal log behavior.

6. Remediation Recommendations

- Block Malicious IPs: Immediately blacklist 203.0.113.77 and 198.51.100.42.
- Enforce MFA: Apply Multi-Factor Authentication for all accounts.
- Reset & Monitor Accounts: Force password reset for suspicious users (alice, bob, charlie, david, eve).
- Patch & Scan Systems: Apply latest security updates and run antivirus scans.
- Strengthen Monitoring: Configure Splunk alerts for brute-force thresholds and malware triggers.
- Employee Awareness: Conduct phishing and malware awareness training.

7. Conclusion

The incident monitoring exercise demonstrated the importance of proactive SIEM log analysis. By detecting brute-force attempts, malware alerts, and suspicious user behavior early, organizations can prevent security breaches and reduce risks.

Deliverables uploaded in this repository:
- Screenshots/ → Splunk screenshots of alerts
- Incident_Response_Report.pdf → This report
- Incident_Response_Report.md → GitHub-friendly report