INCIDENT RESPONSE REPORT

Title:
Security Operations Center (SOC) – Incident Response Report
Task: Cyber Security Task 2 – Alert Monitoring & Incident Simulation
Dataset Used: SOC_Task2_Sample_Logs

---

1. Executive Summary

Security monitoring using Splunk revealed several high-severity and medium-severity alerts within the environment. These included malware detections (Trojans, Rootkits, Worms, Ransomware), repeated connection attempts, credential failures, and suspicious file-access behavior.
These collectively indicate attempted compromise, probing, or early-stage lateral movement.

The SOC analysis team performed alert triage, classification, and recommended remediation actions.

---

2. Tools Used

- Splunk Enterprise SIEM
- Log dataset: SOC_Task2_Sample_Logs
- Splunk Dashboard Studio
- OSINT references (AbuseIPDB, VirusTotal)
- Google Docs (report creation)

---

3. SIEM Dashboard Overview

Insert your Screenshot #5 (Dashboard Overview) here
This dashboard contains:

- Timechart of event activity
- Single-value display for total malware detections
- Pie/Bar chart showing distribution of actions/events

---

4. Alerts Identified

Alert 1 — Malware Detections

Multiple malware alerts detected, including:

- Trojan Detected
- Rootkit Signature
- Worm Infection Attempt
- Ransomware Behavior

Severity: High
Risk: System compromise, payload deployment, lateral spread.

Insert Screenshot #1 here

Alert 2 — Repeated Connection Attempts

Several users performed repeated connection attempts across various hosts, suggesting probing or enumeration.

Severity: Medium–High
Risk: Possible internal scanning or command-and-control attempts.

Insert Screenshot #2 here

Alert 3 — Login Failures

Multiple invalid login attempts across different IPs, indicating potential brute force or credential-stuffing attempts.

Severity: Medium–High

Insert Screenshot #3 here

Alert 4 — Suspicious File Access

File-access events occurred across various hosts and users in a pattern that suggests reconnaissance or unauthorized activity.

Severity: Medium

Insert Screenshot #4 here

---

5. Alert Classification Table

Alert Type	Severity	Evidence Source	Status
Malware detections	High	Malware signatures	Contained / Review
Connection attempts	Medium–High	Network logs	Monitoring
Login failures	Medium–High	Authentication logs	Investigating
Suspicious file access	Medium	File activity logs	Monitoring

---

6. Timeline of Events

Time Window	Activity Observed
04:18–05:50	Malware events (Trojan, Rootkit, Worm)
04:23–09:02	Login failures
04:19–09:07	Repeated connection attempts
07:45–09:10	Ransomware/Worm detections
08:00–09:10	Suspicious file access across hosts

---

7. Impact Assessment

- High probability of attempted account compromise
- Active malware behavior suggests infection attempts
- Repeated connection attempts point to network probing
- Possible lateral movement indicated by file access patterns

Overall Risk Level: High

---

8. Recommended Remediation

Immediate Actions

- Quarantine suspicious hosts
- Reset affected user credentials
- Block malicious IPs
- Enable MFA across all accounts
- Perform full system AV/EDR scans

Mid-term Measures

- Strengthen authentication policies
- Monitor outbound traffic for anomalies
- Review access rights and group memberships
- Log and SIEM tuning for better detection

---

9. Final Summary

The analysis shows a coordinated or automated malicious activity pattern within the monitored system. Immediate containment and strengthened authentication controls are recommended to prevent further compromise.