

SOC INCIDENT RESPONSE REPORT

Prepared by: Murtaza Sukhsarwala
Cybersecurity Internship Project

Executive Summary

- This report summarizes key suspicious alerts detected using Splunk SIEM.
- High severity malware, failed logins, and unusual file access indicate attempted compromise.

Top Suspicious Alerts

- Ransomware Behavior – High
- Rootkit Detection – High
- Trojan Detection – High
- Failed Login Attempts – Medium
- Suspicious File Access – High

Incident Timeline

- 04:19 – Rootkit detected
- 05:48 – Trojan detected
- 07:02 – Failed logins
- 08:42 – Suspicious file access
- 09:10 – Ransomware detected

Impact & Risk

- Multiple high-risk malware infections detected.
- Signs of credential theft and brute-force attempts.
- Possible lateral movement inside the network.

Recommended Actions

- Immediate: Isolate hosts, block malicious IPs.
- Short-Term: Reset passwords, analyze logs.
- Long-Term: Implement SIEM rules, deploy EDR.

SIEM Dashboard Screenshot

The screenshot shows a Splunk Cloud search interface with the following details:

- Search Bar:** source="50C_Task2_Sample_Logs.txt" host="si-i-09025a8f6447aef4.prd-p-29yt2.splunkcloud.com" sourcetype="sample".
- Results Summary:** 50 events (before 11/22/25 5:57:24.000 AM) No Event Sampling.
- Time Range:** All time.
- Visualizations:** A timeline visualization showing a green bar for the threat category. A tooltip indicates "5 Values, 22% of events".
- Event Details:** A table showing top values for threat types: Trojan (54.545%), Rootkit (18.182%), Ransomware (9.091%), Spyware (9.091%), and Worm (9.091%).
- Interesting Fields:** A list of fields including action, date_hour, date_mday, date_minute, date_month, date_second, date_wday, date_year, date_zone, host, index, ip, linecount, punct, source, sourcetype, splunk_server, timeendpos, timestamppos, and user.
- Logs:** A list of log entries related to threat detection, such as file accessed, login success, and connection attempt.

SIEM Dashboard Screenshot

SIEM Dashboard Screenshot