Incident Response Report

Task ID: FUTURE_CS_02

Tool Used: Splunk 9.4.3

Performed by: Kunal Phadtare

Date: 20 July 2025

Objective:

Monitor simulated security alerts using Splunk (a SIEM tool), detect suspicious activity, classify events based on severity, and document a professional incident response report.

Summary of Activities:

1. Log File Monitored: SOC_Task2_Sample_Logs.txt
2. Source Type Set: Custom 'task2' source type created for parsing.
3. Search Conducted:
   - Basic search on logs using source="SOC_Task2_Sample_Logs.txt" and sourcetype="task2".
   - Time-based and host-based analysis performed.
   - Internal Splunk errors examined using:
     index=_internal "error" NOT debug source=*splunkd.log*

Detected Suspicious Activities:

Timestamp (UTC)	User	IP Address	Action	Threat / Notes
2025-07-03 06:13	charlie	10.0.0.5	connection attempt	Unusual time
2025-07-03 05:04	bob	192.168.1.101	login success	Odd login hour
2025-07-03 04:27	david	172.16.0.3	login success	Off-hour access
2025-07-03 05:48	bob	10.0.0.5	malware detected	Trojan Detected
2025-07-03 09:10	bob	172.16.0.3	malware detected	Ransomware behavior flagged
2025-07-03 09:24	david	203.0.113.77	login failed	Repeated login failure

Classification of Events:

- Critical Incidents:

  - Ransomware behavior detected from IP 172.16.0.3 by user bob
  - Malware detection (Trojan) flagged earlier from user bob on 10.0.0.5

- Suspicious Incidents:
  - Login success by david and bob during non-working hours
  - Failed login attempts by david from an external IP

- Information Only:
  - Normal connection attempts by charlie
  - Internal Splunk service errors logged

Visualization:
- Host-based bar charts and time series visualizations created for:
  - Malware detection spikes
  - Error logs from splunkd.log (for Splunk monitoring)

Response Actions Taken:
- Malware detection alerts reviewed.
- Error logs checked from splunkd.log to ensure Splunk performance.
- Suspicious accounts and IPs flagged for further investigation.