INCIDENT RESPONSE REPORT

Security Alert Monitoring & Incident Response

---

1. Introduction

Security logs were monitored using Splunk SIEM. Multiple suspicious activities were detected, including malware alerts, failed login attempts, and unauthorized access. Incidents were analyzed, classified by severity, and remediation actions were recommended.

---

2. Tools Used

- SIEM Tool: Splunk Enterprise
- Log Source: Sample Syslog Files
- Index: log_check

---

3. KEY INCIDENTS IDENTIFIED

Incident	Description	Severity
Ransomware Detected	Malware activity detected	High
Trojan Detected	Trojan malware identified	High
Failed Login Attempts	Possible brute-force attack	Medium
Suspicious Connection Attempts	Repeated connection attempts	Low–Medium
External File Access	File accessed from external IP	Medium

---

4. Timeline (Sample)

- 09:10 AM – Ransomware behavior detected
- 05:45 AM – Trojan detected
- 09:02 AM – Login failed

- Multiple times – Connection attempts & file access

---

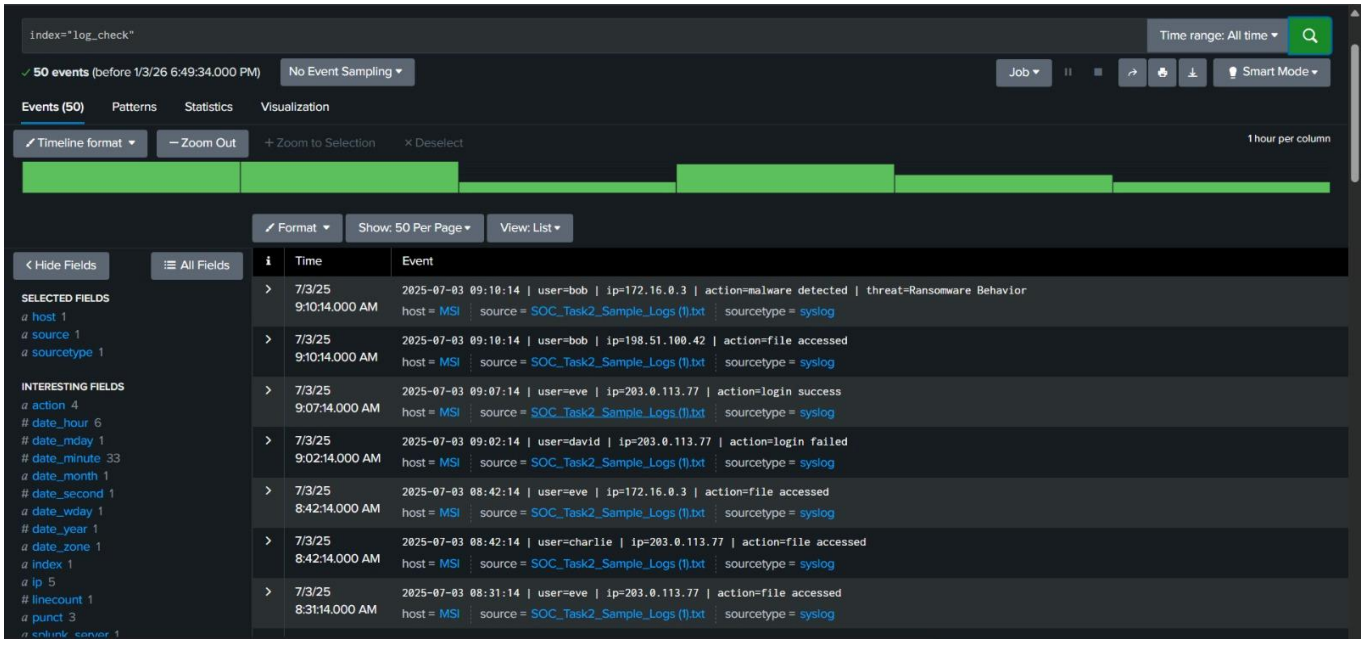
5. Impact

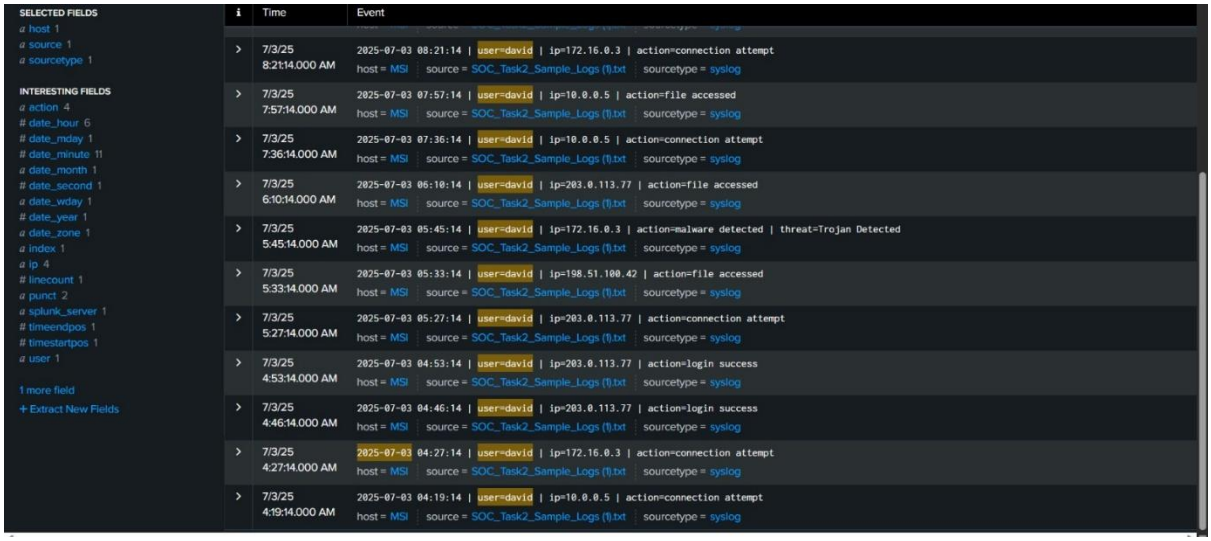
- Risk of system compromise
- Possible credential exposure
- Unauthorized access to files

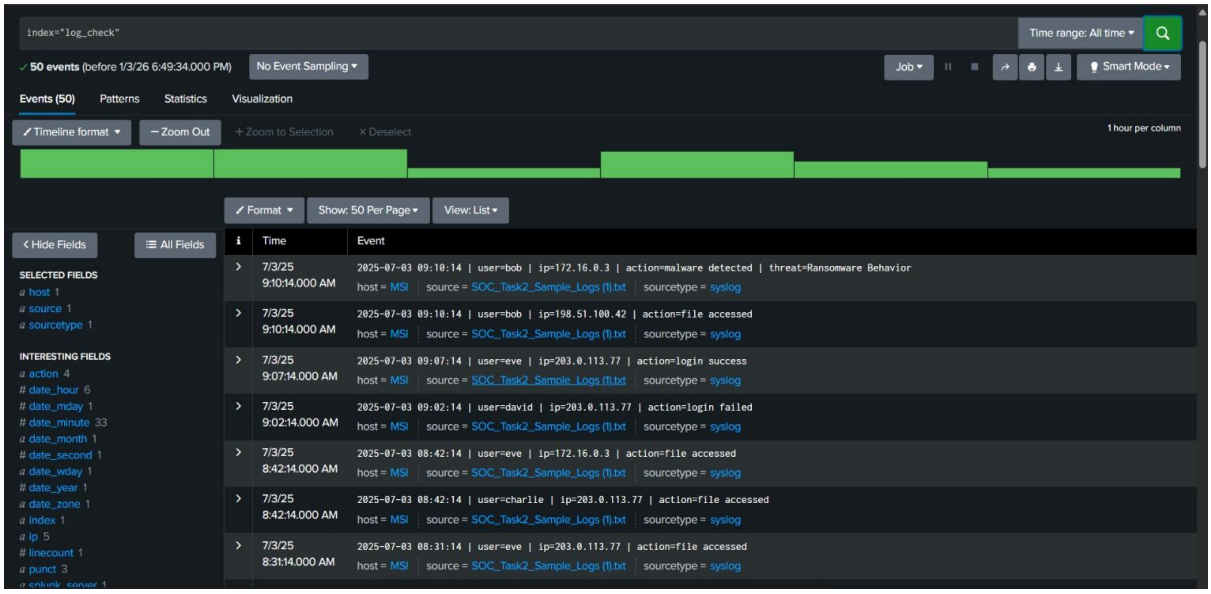
---

6. Response & Remediation

- Identified and reviewed malicious alerts
- Recommended isolating infected systems
- Blocking malicious IPs
- Resetting compromised credentials
- Enabling MFA and SIEM alerting




SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 4
date_hour 6
date_mday 1
date_minute 11
a date_month 1
date_second 1
a date_wday 1
date_year 1
a date_zone 1
a index 1
a ip 4
linecount 1
a punct 2
a splunk_server 1
timeendpos 1
timestartpos 1
a user 1
1 more field
+ Extract New Fields
Time
Event
7/3/25 8:21:14.000 AM 2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 7:57:14.000 AM 2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 7:36:14.000 AM 2025-07-03 07:36:14 | user=david | ip=10.0.0.5 | action=connection attempt host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 6:10:14.000 AM 2025-07-03 06:10:14 | user=david | ip=203.0.113.77 | action=file accessed host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 5:45:14.000 AM 2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 5:33:14.000 AM 2025-07-03 05:33:14 | user=david | ip=198.51.100.42 | action=file accessed host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 5:27:14.000 AM 2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connection attempt host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 4:53:14.000 AM 2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 4:46:14.000 AM 2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login success host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 4:27:14.000 AM 2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 4:19:14.000 AM 2025-07-03 04:19:14 | user=david | ip=10.0.0.5 | action=connection attempt host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog


index="log_check"
Time range: All time
50 events (before 1/3/26 6:49:34.000 PM)
No Event Sampling
Job
Smart Mode
Events (50)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 50 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 4
date_hour 6
date_mday 1
date_minute 33
a date_month 1
date_second 1
a date_wday 1
date_year 1
a date_zone 1
a index 1
a ip 5
linecount 1
a punct 3
a splunk_server 1
Time
Event
7/3/25 9:10:14.000 AM 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 9:10:14.000 AM 2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 9:07:14.000 AM 2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 9:02:14.000 AM 2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 8:42:14.000 AM 2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 8:42:14.000 AM 2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog
7/3/25 8:31:14.000 AM 2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed host = MSI source = SOC_Task2_Sample_Logs (1).txt sourcetype = syslog