

# Security Alert Monitoring & Incident Report Task-2

Intern name : Mithileshwaran

Internship domain : Cyber Security

Task title : Security Alert Monitoring & Incident Response

Date : August 2025

Tool used : Splunk Cloud Free Trail

## 1.Objective :

The objective of this task was to simulate real-world Security Operations Center (SOC) activities using Splunk. I uploaded and analyzed a simulated log file (SOC\_Task2\_Sample\_Logs.txt) containing various system events such as login attempts, malware alerts, IP connections, and host activity.

The goal was to identify security threats by running custom queries, classify alerts based on severity, and document findings through screenshots. This included detecting malware presence, high-volume host logs, failed login attempts, and possible port scanning behavior — mimicking how SOC teams monitor and respond to potential cyber incidents.

## 2. Log Source:

- **Log File Name:** SOC\_Task2\_Sample\_Logs.txt
- **Description:** Simulated system logs containing authentication attempts, usernames, IP addresses, malware alerts, and network activity.
- **Upload Platform:** Splunk Cloud (Free Trial)

### 3. Summary of Alerts:

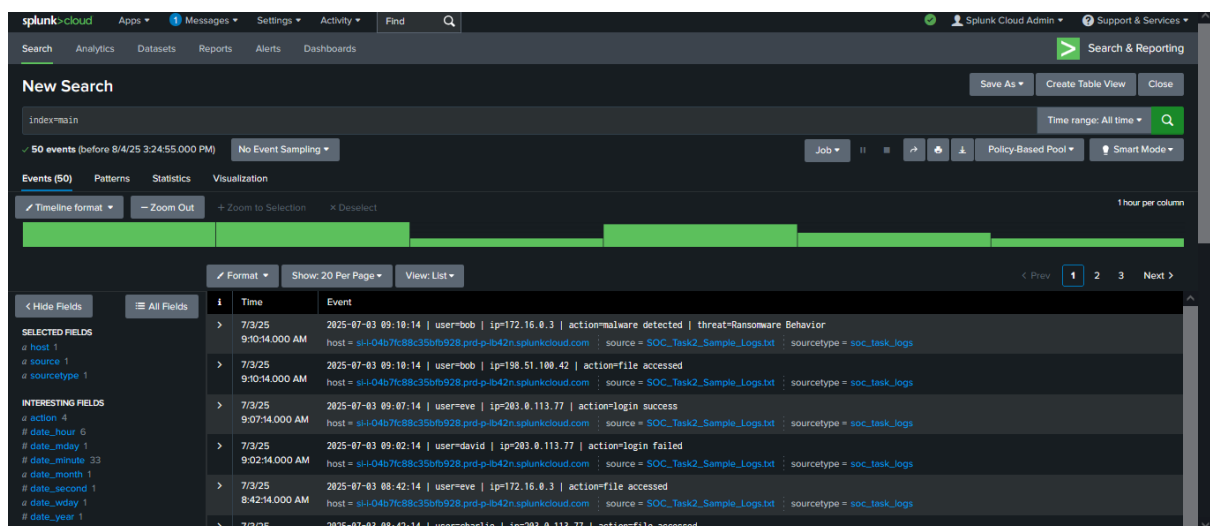
Alert ID	Type	Description	Severity
A01	Full Log View	Index-wide search to observe full logs (index=main)	Low
A02	Malware Detection	Trojan found in logs from Splunk	High
A03	High Host Activity	Host logged 50+ events — possible automation or misuse	Medium
A04	Failed Login Attempts	Multiple failed authentication attempts observed	High
A05	Port Scanning Detected	Repeated connections/port activity logged	Medium

### 4. Detailed Incident Analysis

#### A01 – Full Log Overview:

**Query Used:** `index=main`

A general log overview was performed to validate that log ingestion into Splunk was successful. This gave context for further threat hunting.



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 = si-I04b7fc88c35bf928-prd-p-b42n.splunkcloud.com : source = SOC_Task2_Sample_Logs.txt : sourcetype = soc_task_logs
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 = si-I04b7fc88c35bf928-prd-p-b42n.splunkcloud.com : source = SOC_Task2_Sample_Logs.txt : sourcetype = soc_task_logs
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 = si-I04b7fc88c35bf928-prd-p-b42n.splunkcloud.com : source = SOC_Task2_Sample_Logs.txt : sourcetype = soc_task_logs
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 = si-I04b7fc88c35bf928-prd-p-b42n.splunkcloud.com : source = SOC_Task2_Sample_Logs.txt : sourcetype = soc_task_logs
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 = si-I04b7fc88c35bf928-prd-p-b42n.splunkcloud.com : source = SOC_Task2_Sample_Logs.txt : sourcetype = soc_task_logs
7/3/25 8:42:14.000 AM	2025-07-03 08:42:14   user=charlie   ip=203.0.113.77   action=file accessed

## A02 – Malware Detection:

**Query Used:** `index=main malware OR trojan OR virus`

A Trojan was detected in the logs, suggesting possible system compromise. Malware should be isolated and removed immediately.

The screenshot shows the Splunk Cloud interface with a search query: `index=main malware OR virus OR trojan OR infected`. The results show 11 events. The visualization is a timeline format. The table below shows the first six events:

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 = si-i-04b7fc88c35bf9328-prd-p-b42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 7:51:14.000 AM	2025-07-03 07:51:14   user=veve   ip=10.0.0.5   action=malware detected   threat=Rootkit Signature host = si-i-04b7fc88c35bf9328-prd-p-b42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 7:45:14.000 AM	2025-07-03 07:45:14   user=charlie   ip=172.16.0.3   action=malware detected   threat=Trojan Detected host = si-i-04b7fc88c35bf9328-prd-p-b42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 5:48:14.000 AM	2025-07-03 05:48:14   user=Bob   ip=10.0.0.5   action=malware detected   threat=Trojan Detected host = si-i-04b7fc88c35bf9328-prd-p-b42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
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 = si-i-04b7fc88c35bf9328-prd-p-b42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 05:42:14	2025-07-03 05:42:14   user=veve   ip=203.0.113.77   action=malware detected   threat=Trojan Detected

## A03 – High Host Activity:

**Query Used:** `index=main | stats count by host`

One host (`si-i-04b7fc88c35bf9328-prd-p-b42n.splunkcloud.com`) generated over 50 logs, indicating abnormal or automated behavior. Monitoring of this host is advised.

The screenshot shows the Splunk Cloud interface with a search query: `index=main | stats count by host`. The results show 50 events. The visualization is a table format. The table below shows the first row:

host	count
si-i-04b7fc88c35bf9328-prd-p-b42n.splunkcloud.com	50

## A04 – Failed Login Attempts:

**Query Used:** index=main failed OR "login failed"

Multiple failed authentication attempts may indicate a brute-force attack. Lockouts or alerting mechanisms should be considered.

The screenshot shows the Splunk Cloud interface with a search query: `index=main failed OR "login failed" OR "authentication failure"`. The search results are displayed in a table format, showing 5 events. The table columns are Time and Event. The events are as follows:

Time	Event
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 = si-i-04b7c88c35bfb928.prd-p-lb42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 7:02:14.000 AM	2025-07-03 07:02:14   user=alice   ip=203.0.113.77   action=login failed   host = si-i-04b7c88c35bfb928.prd-p-lb42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 4:47:14.000 AM	2025-07-03 04:47:14   user=bob   ip=10.0.0.5   action=login failed   host = si-i-04b7c88c35bfb928.prd-p-lb42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 4:23:14.000 AM	2025-07-03 04:23:14   user=bob   ip=172.16.0.3   action=login failed   host = si-i-04b7c88c35bfb928.prd-p-lb42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 4:23:14.000 AM	2025-07-03 04:23:14   user=charlie   ip=198.51.100.42   action=login failed   host = si-i-04b7c88c35bfb928.prd-p-lb42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs

## A05 –Port Scan or Network Probe:

**Query Used:** index=main port OR scan OR connection

Logs revealed several port-related or connection attempts — common indicators of port scanning or reconnaissance by threat actors.

The screenshot shows the Splunk Cloud interface with a search query: `index=main port OR scan OR connection`. The search results are displayed in a table format, showing 12 events. The table columns are Time and Event. The events are as follows:

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 = si-i-04b7c88c35bfb928.prd-p-lb42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 8:20:14.000 AM	2025-07-03 08:20:14   user=charlie   ip=192.168.1.101   action=connection attempt   host = si-i-04b7c88c35bfb928.prd-p-lb42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 7:44:14.000 AM	2025-07-03 07:44:14   user=bob   ip=192.168.1.101   action=connection attempt   host = si-i-04b7c88c35bfb928.prd-p-lb42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 7:44:14.000 AM	2025-07-03 07:44:14   user=bob   ip=203.0.113.77   action=connection attempt   host = si-i-04b7c88c35bfb928.prd-p-lb42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 7:38:14.000 AM	2025-07-03 07:38:14   user=charlie   ip=172.16.0.3   action=connection attempt   host = si-i-04b7c88c35bfb928.prd-p-lb42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs
7/3/25 7:35:14.000 AM	2025-07-03 07:35:14   user=david   ip=10.0.0.5   action=connection attempt   host = si-i-04b7c88c35bfb928.prd-p-lb42n.splunkcloud.com   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_task_logs

## 5. Incident Report Summary:

Incident Type	IP Address	Severity	Notes
Malware Detection	172.16.0.3	High	Ransomware / Trojan detected
	10.0.0.5	High	Rootkit Signature
	172.16.0.3	High	Trojan Detected
	10.0.0.5	High	Trojan Detected
	203.0.113.77	High	Trojan Detected
Failed Login Attempts	203.0.113.77	Medium	Multiple login failures
	10.0.0.5	Medium	Brute-force suspected
	172.16.0.3	Medium	Failed login by user “bob”
	198.51.100.42	Medium	Unauthorized login attempt
High Host Activity	si-04b7fc88c35bfb928...	High	50+ log events from single host
Port Scan Activity	172.16.0.3	High	Multiple connection attempts
	192.168.1.101	High	Connection attempt – possible scan
	203.0.113.77	High	Scan behaviour
	10.0.0.5	High	Repeated scan signs

## 6. Conclusion:

- Used a **SIEM tool (Splunk)** for log analysis
- Wrote **basic SPL queries** to search and filter security events
- Detected **brute-force attacks** and **suspicious activities**
- Documented incidents in a **structured incident response report**

This forms the foundation of what real-world **Security Operations Center (SOC)** teams do for live incident monitoring and response.

