

# Security Operations Center (SOC) Internship Report

## Task: Security Alert Monitoring & Incident Response Simulation

### 1. Introduction

This report documents the activities performed during the SOC internship project focused on **security alert monitoring and incident response simulation**.

The objective of this task was to learn how a SOC Analyst monitors logs, detects suspicious events, triages alerts, and communicates incidents to stakeholders.

### 2. Project Scope

During the task, simulated security logs were analyzed to detect:

- Failed authentication attempts
- Unusual network connections
- Malware alerts
- Suspicious user behavior

A SIEM tool was used to view, filter, and analyze the logs to identify potential threats.

### 3. Tools & Resources Used

Tool	Purpose
Splunk / ELK (SIEM Tool)	Log monitoring and alert analysis
Sample Log File: <b>SOC_Task2_Sample_Logs</b>	Contained authentication, network, and malware events
Word / Google Docs	For creating the incident response report

### 4. Skills Developed

- Basic **log analysis** and event interpretation
- **Alert triage** and severity classification
- Use of **SIEM dashboards** to visualize threat activity
- Understanding key **cybersecurity terminology**
- **Incident response documentation and communication**

## 5. Data Analyzed

The dataset included:

- System event timestamps
- Network connections with IP addresses
- Successful & failed login attempts
- Malware detection alerts

## 6. SIEM Search Commands Used

### 6.1 View All Logs

```
index=soc_task2 sourcetype=soc_task2_logs  
| table _time user ip host action threat  
| sort _time
```

Obsevation:

The screenshot shows the Splunk Enterprise search interface. At the top, there's a navigation bar with 'splunk>enterprise' and various dropdown menus like 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search bar. Below the navigation is a 'Search & Reporting' section with 'Save As', 'Create Table View', and 'Close' buttons. A 'Time range: All time' dropdown is also present. The main area is titled 'New Search' and displays a search bar with 'index="soc\_task2"' and 'No Event Sampling'. Below the search bar, it says 'Events (50)' and shows a timeline from 7/3/25 9:07:14.000 AM to 7/3/25 9:02:14.000 AM. The timeline is represented by a horizontal bar divided into green segments. Underneath the timeline, there's a table view with columns: '\_time', 'host', 'source', 'sourcetype', and 'action'. The table contains five rows of log data. On the left side, there are sections for 'SELECTED FIELDS' and 'INTERESTING FIELDS' with their respective counts.

	_time	host	source	sourcetype	action
>	7/3/25 9:07:14.000 AM	Anik2003	SOC_Task2_Sample_Logs.txt	soc_task2_logs	malware detected
>	7/3/25 9:07:14.000 AM	Anik2003	SOC_Task2_Sample_Logs.txt	soc_task2_logs	file
>	7/3/25 9:07:14.000 AM	Anik2003	SOC_Task2_Sample_Logs.txt	soc_task2_logs	login
>	7/3/25 9:02:14.000 AM	Anik2003	SOC_Task2_Sample_Logs.txt	soc_task2_logs	login

**SELECTED FIELDS**  
a action 4  
a host 1  
a source 1  
a sourcetype 1

**INTERESTING FIELDS**  
# date\_hour 6  
# date\_mday 1  
# date\_minute 33  
# date\_month 1  
# date\_second 1  
# date\_wday 1

Splunk > enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Search Analytics Datasets Reports Alerts Dashboards

New Search

Index=soc\_task2 sourcetype=soc\_task2\_logs  
| table \_time user ip host action threat  
| sort \_time

50 events (before 11/10/25 11:44:47.000 AM) No Event Sampling ▾

Save As ▾ Create Table View Close

Time range: All time ▾

Events (50) Patterns Statistics (50) Visualization

Show: 50 Per Page ▾ Format ▾ Preview: On

_time	user	ip	host	action	threat
2025-07-03 04:18:14	bob	198.51.100.42	Anki2003	login	
2025-07-03 04:19:14	david	10.0.0.5	Anki2003	connection	
2025-07-03 04:19:14	alice	198.51.100.42	Anki2003	malware detected	Rootkit
2025-07-03 04:23:14	bob	172.16.0.3	Anki2003	login	
2025-07-03 04:23:14	charlie	198.51.100.42	Anki2003	login	
2025-07-03 04:27:14	david	172.16.0.3	Anki2003	connection	
2025-07-03 04:29:14	alice	192.168.1.101	Anki2003	malware detected	Trojan
2025-07-03 04:41:14	alice	172.16.0.3	Anki2003	malware detected	Spyware
2025-07-03 04:46:14	david	203.0.113.77	Anki2003	login	
2025-07-03 04:47:14	bob	10.0.0.5	Anki2003	login	
2025-07-03 04:53:14	alice	203.0.113.77	Anki2003	file	

## 6.2 Login Detection

index=soc\_task2 sourcetype=soc\_task2\_logs action="connection"

### Observation:

New Search

index=soc\_task2 sourcetype=soc\_task2\_logs "connection"

12 events (before 11/10/25 11:57:09.000 AM) No Event Sampling ▾

Save As ▾ Create Table View Close

Time range: All time ▾

Events (12) Patterns Statistics Visualization

Timeline format ▾ Zoom Out ▾ + Zoom to Selection ▾ Deselect

1 hour per column

Format ▾ Show: 50 Per Page ▾ View: Raw ▾

< Hide Fields ▾ All Fields ▾

SELECTED FIELDS

- a action 1
- a host 1
- a ip 4
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- # date\_hour 5
- # date\_minute 10
- # date\_minute 10
- # date\_month 1
- # date\_second 1
- # date\_weekday 1
- # date\_year 1
- # date\_zone 1
- a Index 1
- # linecount 1
- a next 1

	Event
>	2025-07-03 08:21:14   user=david   ip=172.16.0.3   action=connection attempt
>	2025-07-03 08:20:14   user=charlie   ip=192.168.1.101   action=connection attempt
>	2025-07-03 07:44:14   user=bob   ip=192.168.1.101   action=connection attempt
>	2025-07-03 07:44:14   user=bob   ip=203.0.113.77   action=connection attempt
>	2025-07-03 07:38:14   user=charlie   ip=172.16.0.3   action=connection attempt
>	2025-07-03 07:36:14   user=david   ip=10.0.0.5   action=connection attempt
>	2025-07-03 07:22:14   user=charlie   ip=192.168.1.101   action=connection attempt
>	2025-07-03 06:13:14   user=charlie   ip=10.0.0.5   action=connection attempt
>	2025-07-03 05:49:14   user=charlie   ip=192.168.1.101   action=connection attempt
>	2025-07-03 05:27:14   user=david   ip=203.0.113.77   action=connection attempt
>	2025-07-03 04:27:14   user=david   ip=172.16.0.3   action=connection attempt
>	2025-07-03 04:19:14   user=david   ip=10.0.0.5   action=connection attempt

## 6.3 Suspicious IP Activity

index=soc\_task2 sourcetype=soc\_task2\_logs

| stats count by ip

| sort -count

## **Observation:**

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: `index=soc_task2 sourcetype=soc_task2_logs | stats count by ip | sort - count`. The results section shows 50 events from before 11/10/25 at 11:47:44.000 AM. The Statistics tab is selected, displaying a table of IP addresses and their counts. The table includes:

ip	count
203.0.113.77	15
172.16.0.3	12
10.0.0.5	8
198.51.100.42	8
192.168.1.101	7

## **6.4 Malware Alerts**

```
index=soc_task2 sourcetype=soc_task2_logs threat=*
| table _time host user ip threat
| sort _time
```

## **Obsevation:**

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: `index=soc_task2 sourcetype=soc_task2_logs threat=* | table _time host user ip threat action | sort _time`. The results section shows 11 events from before 11/10/25 at 11:49:04.000 AM. The Statistics tab is selected, displaying a table of malware threats and actions. The table includes:

_time	host	user	ip	threat	action
2025-07-03 04:10:14	Ank12003	alice	198.51.100.42	Rootkit	malware detected
2025-07-03 04:29:14	Ank12003	alice	192.168.1.101	Trojan	malware detected
2025-07-03 04:41:14	Ank12003	alice	172.16.0.3	Spyware	malware detected
2025-07-03 05:06:14	Ank12003	bob	203.0.113.77	Worm	malware detected
2025-07-03 05:30:14	Ank12003	eve	192.168.1.101	Trojan	malware detected
2025-07-03 05:42:14	Ank12003	eve	203.0.113.77	Trojan	malware detected
2025-07-03 05:45:14	Ank12003	david	172.16.0.3	Trojan	malware detected
2025-07-03 05:48:14	Ank12003	bob	10.0.0.5	Trojan	malware detected
2025-07-03 07:45:14	Ank12003	charlie	172.16.0.3	Trojan	malware detected
2025-07-03 07:51:14	Ank12003	eve	10.0.0.5	Rootkit	malware detected
2025-07-03 09:10:14	Ank12003	bob	172.16.0.3	Ransomware	malware detected

## **6.5 Severity Level**

## **Observation:**

_time	user	ip	host	action	threat	Severity
2025-07-03 09:10:14	bob	172.16.0.3	Anki2003	malware detected	Ransomware	Low
2025-07-03 09:10:14	bob	198.51.100.42	Anki2003	file		Low
2025-07-03 09:07:14	eve	203.0.113.77	Anki2003	login		Low
2025-07-03 09:02:14	david	203.0.113.77	Anki2003	login		Low
2025-07-03 08:42:14	eve	172.16.0.3	Anki2003	file		Low
2025-07-03 08:42:14	charlie	203.0.113.77	Anki2003	file		Low
2025-07-03 08:31:14	eve	203.0.113.77	Anki2003	file		Low
2025-07-03 08:30:14	eve	172.16.0.3	Anki2003	login		Low
2025-07-03 08:21:14	david	172.16.0.3	Anki2003	connection		Low

## **7. Identified Incidents & Findings**

### **Incident #1 — Multiple Failed Login Attempts**

- User:** David
- Source IP:** 10.0.0.5
- Description:** Several failed login attempts were recorded, indicating a possible brute-force attack.
- Severity:** low
- Action:** User account monitored and login attempts reviewed.

### **Incident #2 — Suspicious External IP Connection**

- IP:** 203.0.113.77
- Severity:** low
- Action:** Flagged for further investigation, recommended firewall block if repeated.

### **Incident #3 — Malware Detection Alert**

- Threat Type:** Ransomware Behavior
- Host:** workstation-04
- Severity:** Critical
- Action Taken:** Host isolated and malware scan recommended.

## 8. Incident Response Summary Table

Incident	Indicators	Severity	Response
Failed Login Attempts	Multiple login failures from same IP	low	Monitor and verify user activity
Suspicious IP Connection	New / unknown IP access attempt	low	Investigate & restrict access
Malware Detection	Ransomware alert triggered	low	Isolate host & perform malware removal

## 9. Communication to Stakeholders (Email Template)

**Subject:** Security Alert Notification — Incident Under Review

**Message:**

A security event has been detected and is currently under investigation. Our SOC team has identified abnormal login activity and a malware alert on one workstation. The affected system has been isolated and further analysis is in progress. Additional updates will be shared upon completion of the investigation.

## 10. Conclusion

This internship task provided practical exposure to SOC analyst responsibilities, including alert monitoring, log analysis, threat identification, and incident response documentation. The activity reinforced the importance of early detection, structured triage, and effective communication in cybersecurity operations.