

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: SOC_Task2_Sample_Logs	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. The search bar contains the query `index=soc_task2 sourcetype=soc_task2_logs`. The search results are displayed in a table view, showing 50 events. The table has columns for `_time`, `host`, `source`, `sourcetype`, and `action`. The results show four events, all from the host `Anki2003` and source `SOC_Task2_Sample_Logs.txt`. The actions are `malware detected`, `file`, `login`, and `login`.

#	_time	host	source	sourcetype	action
1	7/3/25 9:10:14.000 AM	Anki2003	SOC_Task2_Sample_Logs.txt	soc_task2_logs	malware detected
2	7/3/25 9:10:14.000 AM	Anki2003	SOC_Task2_Sample_Logs.txt	soc_task2_logs	file
3	7/3/25 9:07:14.000 AM	Anki2003	SOC_Task2_Sample_Logs.txt	soc_task2_logs	login
4	7/3/25 9:02:14.000 AM	Anki2003	SOC_Task2_Sample_Logs.txt	soc_task2_logs	login

Observation:

The screenshot shows the Splunk Enterprise Search interface. The search bar contains the query: `index=soc_task2 sourcetype=soc_task2_logs | stats count by ip | sort - count`. The results are displayed in a table with 50 events. The table has two columns: `ip` and `count`. The results are sorted by count in descending order.

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 query: `index=soc_task2 sourcetype=soc_task2_logs threat=* | table _time host user ip threat action | sort _time`. The results are displayed in a table with 11 events. The table has six columns: `_time`, `host`, `user`, `ip`, `threat`, and `action`. The results are sorted by `_time` in ascending order.

_time	host	user	ip	threat	action
2025-07-03 04:19:14	Ark12003	alice	198.51.100.42	Rootkit	malware detected
2025-07-03 04:29:14	Ark12003	alice	192.168.1.101	Trojan	malware detected
2025-07-03 04:41:14	Ark12003	alice	172.16.0.3	Spyware	malware detected
2025-07-03 05:06:14	Ark12003	bob	203.0.113.77	Worm	malware detected
2025-07-03 05:30:14	Ark12003	eve	192.168.1.101	Trojan	malware detected
2025-07-03 05:42:14	Ark12003	eve	203.0.113.77	Trojan	malware detected
2025-07-03 05:45:14	Ark12003	david	172.16.0.3	Trojan	malware detected
2025-07-03 05:48:14	Ark12003	bob	10.0.0.5	Trojan	malware detected
2025-07-03 07:45:14	Ark12003	charlie	172.16.0.3	Trojan	malware detected
2025-07-03 07:51:14	Ark12003	eve	10.0.0.5	Rootkit	malware detected
2025-07-03 09:10:14	Ark12003	bob	172.16.0.3	Ransomware	malware detected

6.5 Severity Level

Observation:

New Search

Save AsCreate Table ViewClose

index=soc_task2 sourcetype=soc_task2_logs

| eval Severity=case(
 threat="ransomware behavior","Critical",
 threat="malware detected","High",
 action="login_failed","Medium",
 true(),"Low"
)

| table _time user ip host action threat Severity

Time range: All time

50 events (before 11/10/25 11:52:27000 AM)No Event SamplingJob

Events (50)PatternsStatistics (50)Visualization

Show: 50 Per PageFormatPreview: On

_time	user	ip	host	action	threat	Severity
2025-07-03 09:10:14	bob	172.16.0.3	Ank12003	malware detected	Ransomware	Low
2025-07-03 09:10:14	bob	198.51.100.42	Ank12003	file		Low
2025-07-03 09:07:14	eve	203.0.113.77	Ank12003	login		Low
2025-07-03 09:02:14	david	203.0.113.77	Ank12003	login		Low
2025-07-03 08:42:14	eve	172.16.0.3	Ank12003	file		Low
2025-07-03 08:42:14	charlie	203.0.113.77	Ank12003	file		Low
2025-07-03 08:31:14	eve	203.0.113.77	Ank12003	file		Low
2025-07-03 08:30:14	eve	172.16.0.3	Ank12003	login		Low
2025-07-03 08:21:14	david	172.16.0.3	Ank12003	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.