

INCIDENT RESPONSE REPORT

NAME: AFOLABI ADESOYE THEOPHILUS

Task 02: SOC Alert Monitoring & Incident Response

Target: Splunk SIEM (Analyzed SOC_Task2_Sample_Logs.txt)

Program: Future Interns Cybersecurity Internship

DATE: 10/20/2025

Task Summary

This task focused on monitoring and analyzing system logs using **Splunk SIEM** to identify key security incidents, including **malware detections, failed login attempts, trojan activity, and ransomware behavior**. The objective was to demonstrate practical SOC analyst functions by detecting, assessing, and responding to these simulated threats through effective log analysis and incident reporting.

Tools Utilized

- Splunk SIEM (Free Trial) – For log ingestion and Analysis
- Sample log file (SOC_Task2_Sample_Logs.txt) – Sample log dataset
Provided

FINDINGS FROM THE SYSTEM LOGS

1. MALWARE DETECTIONS

(source="SOC_Task2_Sample_Logs.txt" host="AFOLABIADESOYE" sourcetype="SOC_Task2_Sample_Logs" action="malware detected")

Splunk SIEM analysis detected 11 malware-related alerts. These incidents affected several users and systems, pointing to a coordinated network-wide attack.

Threat Types Identified: Ransomware, Rootkit, Trojan, Worm, Spyware
Affected Users: Bob, Eve, Charlie, David, Alice

Involved IP Addresses: 172.16.0.3, 10.0.0.5, 192.168.1.101, 203.0.113.77, 198.51.100.42

Notably, user Bob was associated with both Ransomware and Worm alerts, indicating a potentially compromised account actively spreading malware.

source="SOC_Task2_Sample_Logs.txt" host="AFOLABIADESOYE" sourcetype="SOC_Task2_Sample_Logs" action="malware detected"

11 events (before 10/20/25 11:06:05.000 PM)

No Event Sampling

Events (11)

Patterns

Statistics

Visualization

Timeline format

Zoom Out

+ Zoom to Selection

✕ Deselect

Format

Show: 50 Per Page

View: List

< Hide Fields

All Fields

	i	Time	Event
SELECTED FIELDS	>	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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs
a host 1	>	7/3/25 7:51:14.000 AM	2025-07-03 07:51:14 user=eve ip=10.0.0.5 action=malware detected threat=Rootkit Signature host = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs
a source 1	>	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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs
a sourcetype 1	>	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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs
INTERESTING FIELDS	>	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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs
a action 1	>	7/3/25 5:42:14.000 AM	2025-07-03 05:42:14 user=eve ip=203.0.113.77 action=malware detected threat=Trojan Detected host = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs
a date_hour 4	>	7/3/25 5:30:14.000 AM	2025-07-03 05:30:14 user=eve ip=192.168.1.101 action=malware detected threat=Trojan Detected host = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs
a date_mday 10	>	7/3/25 5:06:14.000 AM	2025-07-03 05:06:14 user=bob ip=203.0.113.77 action=malware detected threat=Worm Infection Attempt host = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs
a date_month 1	>	7/3/25 4:41:14.000 AM	2025-07-03 04:41:14 user=alice ip=172.16.0.3 action=malware detected threat=Spyware Alert host = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs
a date_second 1	>	7/3/25 4:29:14.000 AM	2025-07-03 04:29:14 user=alice ip=192.168.1.101 action=malware detected threat=Trojan Detected host = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs
a date_wday 1	>	7/3/25 4:19:14.000 AM	2025-07-03 04:19:14 user=alice ip=198.51.100.42 action=malware detected threat=Rootkit Signature host = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_Logs
a date_year 1			
a date_zone 1			
a index 1			
a ip 5			
a linecount 1			
a punct 2			
a splunk_server 1			
a threat 5			
a timeendpos 1			
a timestartpos 1			
a user 5			

+ Extract New Fields

2. FAILED LOGIN ATTEMPTS

(index=main "login failed")

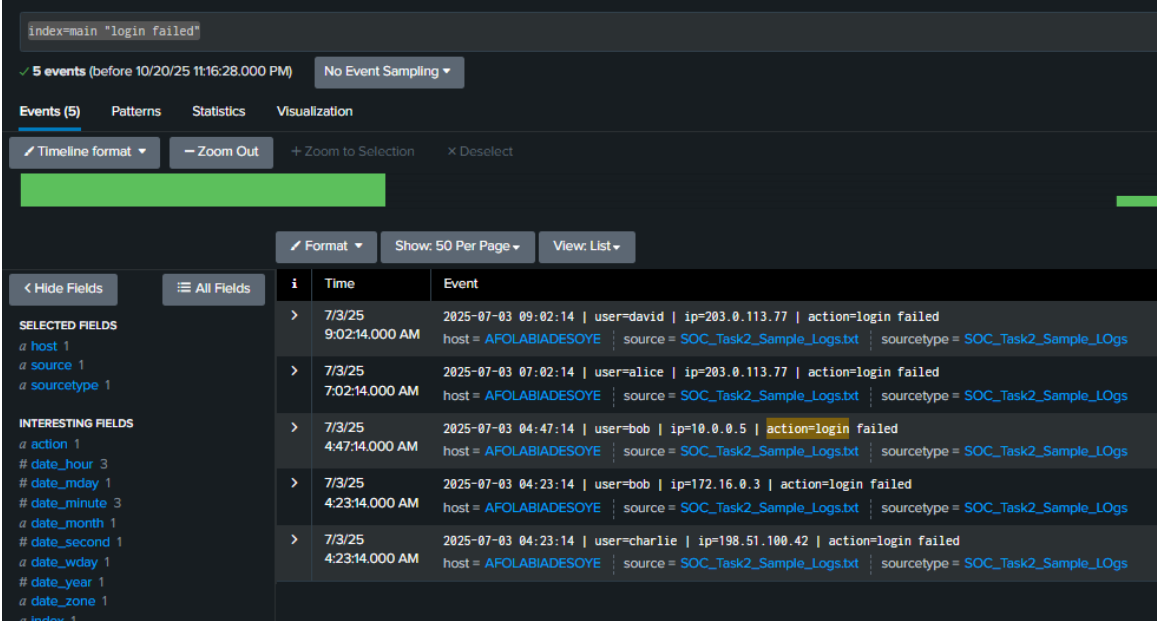
Splunk analysis recorded multiple failed login attempts on July 3, 2025, originating from various IPs and user accounts. These repeated authentication failures may indicate password-guessing or brute-force activity targeting network accounts.

Threat Type: Brute-force / Unauthorized Access Attempt

Affected Users: Bob, Alice, Charlie, David

Involved IP Addresses: 203.0.113.77, 10.0.0.5, 172.16.0.3, 198.51.100.42

Observation: User Bob had multiple failed logins from two different IPs within minutes, suggesting a compromised or targeted account.



The screenshot shows a Splunk search interface with the query `index=main "login failed"`. It displays 5 events. The left sidebar shows 'SELECTED FIELDS' (host, source, sourcetype) and 'INTERESTING FIELDS' (action, date_hour, date_mday, date_minute, date_month, date_second, date_wday, date_year, date_zone, index). The main table lists the events with columns for index, time, and event details.

i	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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_LOgs

3. TROJAN DETECTED

```
(source="SOC_Task2_Sample_Logs.txt" host="AFOLABIADESOYE" sourcetype="SOC_Task2_Sample_LOgs" action="malware detected" | search "Trojan Detected" |)
```

Splunk SIEM analysis revealed multiple Trojan detections across several user systems, indicating infection attempts through malicious executables. The activity suggests initial compromise vectors that could enable remote access or data exfiltration.

Threat Type: Trojan / Remote Access Malware

Affected Users: Alice, Bob, Charlie, David, Eve

Involved IP Addresses: 172.16.0.3, 10.0.0.5, 203.0.113.77, 192.168.1.101

Observation: Repeated Trojan detections from multiple user hosts suggest a widespread infection attempt. User Eve's system triggered two alerts from different IPs, implying possible network propagation or dual-host compromise.

The screenshot shows a Splunk search interface with the following search query: `source="SOC_Task2_Sample_Logs.txt" host="AFOLABIADESOYE" sourcetype="SOC_Task2_Sample_LOgs" action="malware detected" | search "Trojan Detected"`. The results show 6 events. The interface includes tabs for Events (6), Patterns, Statistics, and Visualization. Below the search bar, there are controls for Timeline format, Zoom Out, Zoom to Selection, and Deselect. A table of results is displayed with columns for Time and Event. The table lists six events, each with a timestamp, user, IP address, action, and threat. The events are as follows:

Time	Event
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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_LOgs
7/3/25 5:42:14.000 AM	2025-07-03 05:42:14 user=eve ip=203.0.113.77 action=malware detected threat=Trojan Detected host = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_LOgs
7/3/25 5:30:14.000 AM	2025-07-03 05:30:14 user=eve ip=192.168.1.101 action=malware detected threat=Trojan Detected host = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_LOgs
7/3/25 4:29:14.000 AM	2025-07-03 04:29:14 user=alice ip=192.168.1.101 action=malware detected threat=Trojan Detected host = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_LOgs

4. RANSOMWARE BEHAVIOR DETECTED

```
(source="SOC_Task2_Sample_Logs.txt" host="AFOLABIADESOYE" sourcetype="SOC_Task2_Sample_LOgs" action="malware detected" | search "Ransomware Behavior" |)
```

Splunk SIEM analysis identified a Ransomware Behavior alert on July 3, 2025. This detection indicates possible encryption or file manipulation activity consistent with ransomware attack patterns.

Threat Type: Ransomware

Affected User: Bob

Involved IP Address: 172.16.0.3

Observation: The alert originated from user Bob's system, which had also been linked to previous malware detections. This correlation suggests Bob's host may be compromised and actively exhibiting ransomware traits, requiring immediate isolation and forensic analysis.

The screenshot displays the Splunk SIEM interface with a search bar at the top containing the query: `source="SOC_Task2_Sample_Logs.txt" host="AFOLABIADESOYE" sourcetype="SOC_Task2_Sample_LOgs" action="malware detected" | search "Ransomware Behavior" |`. Below the search bar, a status bar indicates "1 event (before 10/20/25 11:41:38.000 PM)" and "No Event Sampling". The interface shows a single event in a table format. The event details are as follows:

Time	Event
2025-07-03 09:10:14 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 = AFOLABIADESOYE source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_Sample_LOgs

The interface also includes a sidebar with "SELECTED FIELDS" (host 1, source 1, sourcetype 1) and "INTERESTING FIELDS" (action 1, date_hour 1, date_mday 1, date_minute 1).

Incident Summary

- **Malware Detections:** Multiple malware alerts (Trojan, Rootkit, Spyware, Ransomware) were detected across several user systems, indicating widespread infection attempts.
- **Failed Login Attempts:** Repeated failed logins were observed for multiple users, suggesting possible brute-force or unauthorized access attempts.
- **Trojan Detected:** Several Trojan detections occurred across different users and IPs, showing potential malware spread within the network.
- **Ransomware Behavior Detected:** Ransomware-like activity was identified on Bob's system, pointing to possible file encryption or data tampering.

Impact & Risk Assessment (Alert Classification)

- **Malware Detections:** High
- **Failed Login Attempts:** Medium
- **Trojan Detected:** High
- **Ransomware Behavior Detected:** Critical

Remediation Suggestions

- **Malware Detections**
 - Isolate affected hosts and scan for infections.
 - Update antivirus definitions and security patches.
- **Failed Login Attempts**
 - Enforce account lockout and MFA.
 - Review login sources and patterns.
- **Trojan Detected**
 - Quarantine infected devices and remove malicious files.
 - Monitor outbound traffic for suspicious connections.
- **Ransomware Behavior Detected**
 - Disconnect and contain the infected system.
 - Restore clean backups.

EMAIL TEMPLATE TO MANAGEMENT

To: Management Team
Cc: IT Security Department, SOC Team
From: Afolabi Adesoye Theophilus, Security Analyst
Date: July 3, 2025

Dear Management,

This is to notify you of multiple security incidents identified during recent log analysis in Splunk SIEM. The investigation revealed four key findings requiring attention:

Malware Detections: Multiple malware alerts (Trojan, Rootkit, Spyware, Ransomware) were observed across several systems, suggesting potential network compromise.

Failed Login Attempts: Unusual failed login activities were recorded across user accounts, indicating possible unauthorized access attempts.

Trojan Detected: Several Trojan infections were detected, showing signs of internal spread and potential data exposure.

Ransomware Behavior: One system (User: Bob) exhibited ransomware-like activity that could lead to file encryption and data loss.

Immediate actions have been initiated, including system isolation, malware scans, and policy enforcement. Further forensic analysis is ongoing to confirm the infection sources and ensure full remediation.

We recommend maintaining heightened vigilance, verifying data backups, and scheduling a brief review meeting to discuss additional containment and recovery strategies.

Best Regards,
Afolabi Adesoye Theophilus
Security Operations Center (SOC) Analyst