

SOC Task Report

Future interns- Cybersecurity internship

Task Title: Security operations center (SOC) simulation-log
Analysis & incident Response

Name: Adebowale Emmanuel Okikiola

CIN ID: FIT/JUL25/CS2572

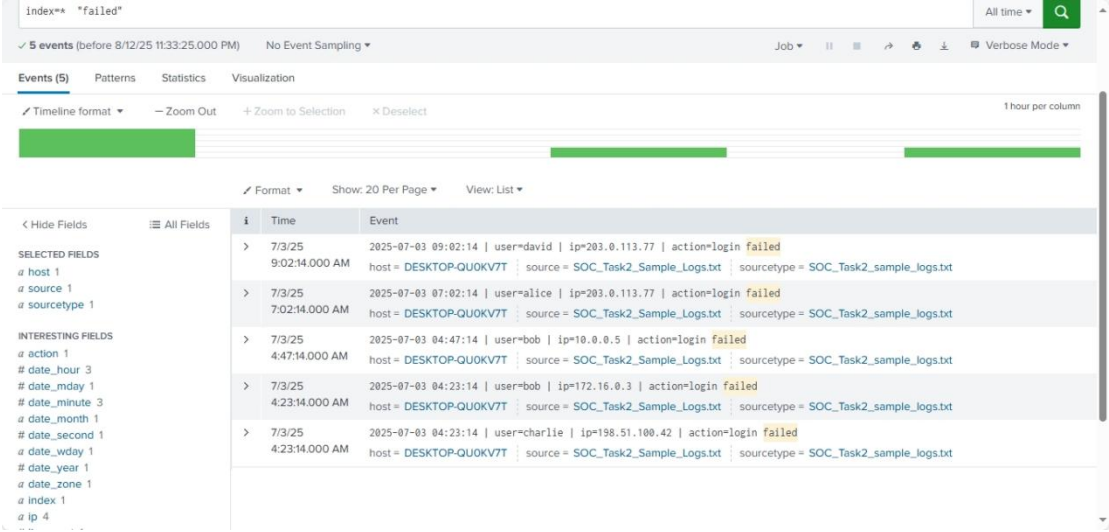
Date: August 2025

Executive Summary

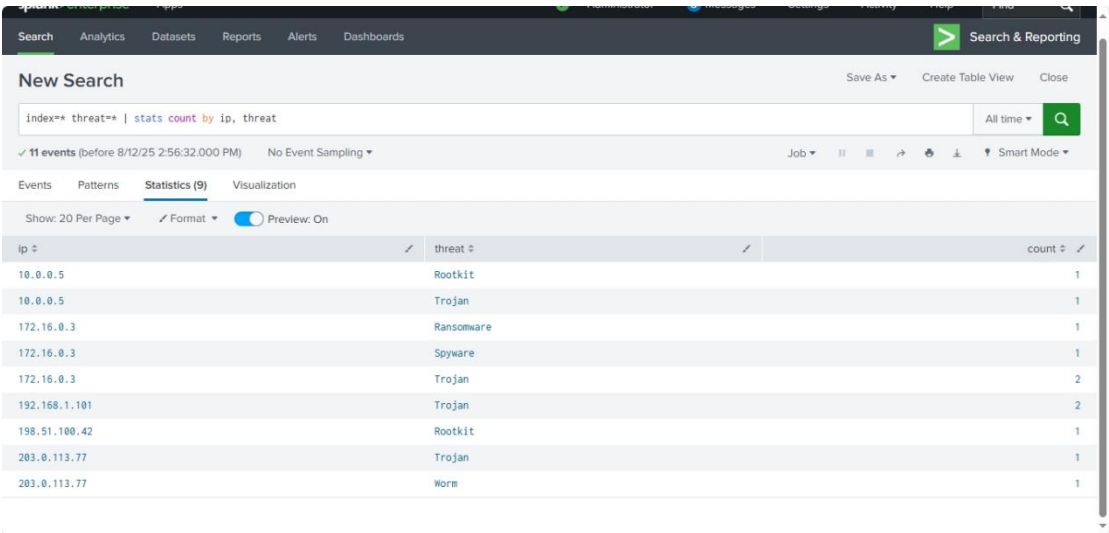
This SOC simulation task involve monitoring and analyzing security alerts using Splunk, identifying suspicious activities such as failed logins, repeated ip addresses, and malware threats. The task includes classifying incidents by severity, drafting an incident response report, and providing recommendations to mitigate the risks.

Splunk Analysis Screenshots

1. Failed login attempts



2. Suspicious repeated ip addresses



3. Malware threats detection

< Hide Fields		≡ All Fields	✓ Format ▾	Show: 20 Per Page ▾	View: List ▾
SELECTED FIELDS			i	Time	Event
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 = DESKTOP-QUOKV7T source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_sample_logs.txt
a source 1					
a sourcetype 1					
INTERESTING FIELDS					
a action 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 = DESKTOP-QUOKV7T source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_sample_logs.txt
# date_hour 4					
# date_mday 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 = DESKTOP-QUOKV7T source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_sample_logs.txt
# date_minute 10					
# date_month 1			>	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 = DESKTOP-QUOKV7T source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_sample_logs.txt
# date_second 1					
# date_wday 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 = DESKTOP-QUOKV7T source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_sample_logs.txt
# date_year 1					
# date_zone 1			>	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 = DESKTOP-QUOKV7T source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_sample_logs.txt
a index 1					
a ip 5			>	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 = DESKTOP-QUOKV7T source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_sample_logs.txt
# linecount 1					
a punct 2			>	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 = DESKTOP-QUOKV7T source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_sample_logs.txt
a splunk_server 1					
a threat 5			>	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 = DESKTOP-QUOKV7T source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_sample_logs.txt
# timeendpos 1					
# timestartpos 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 = DESKTOP-QUOKV7T source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Task2_sample_logs.txt
a user 5					
+ Extract New Fields					

Suspicious Findings Table

IP Address	Threat Type	Count	Severity
10.0.0.5	Rootkit	1	High
10.0.0.5	Trojan	1	High
172.16.0.3	Ransomware	1	Critical
172.16.0.3	Spyware	1	High
172.16.0.3	Trojan	1	High
192.168.1.101	Trojan	2	High
198.51.100.42	Rootkit	2	High
203.0.113.77	Trojan	1	High
203.0.113.77	Worm	1	High

Incident Response Report

Timeline:

[8/3/2025 12:00]

Description of incident:

Multiple security threats detected, including brute-force login attempts, repeated suspicious ip addresses, and various malware detection (rootkit, trojan, ransomware, spyware, worm).

Impacts Assessment:

These threats could lead to unauthorized access, data theft, and possible systems compromise if not contained.

Remediation Suggestions:

- Block malicious IP addresses at the firewall
- Patch vulnerable systems
- Reset affected user password
- Run full antivirus and anti-malware scans
- Review and tighten login security measures