SOC Task Report
Future interns- Cybersecurity internship
Task Title: Security operations center (SOC) simulation-log Analysis & incident Response

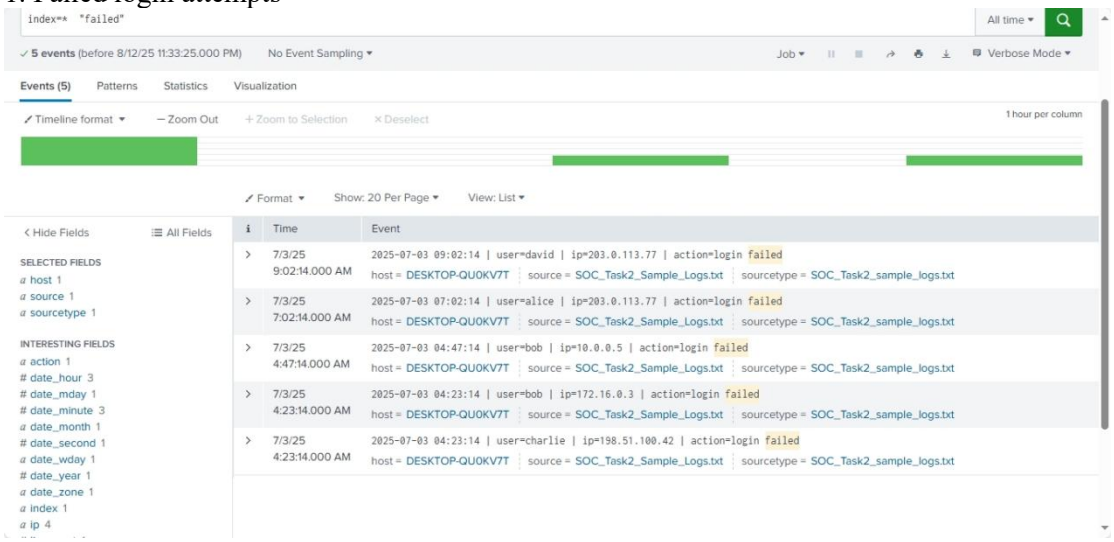
Name: Adebowale Emmanuel Okikiola
CIN ID: FIT/JUL25/CS2572
Date: August 2025

Executive Summary

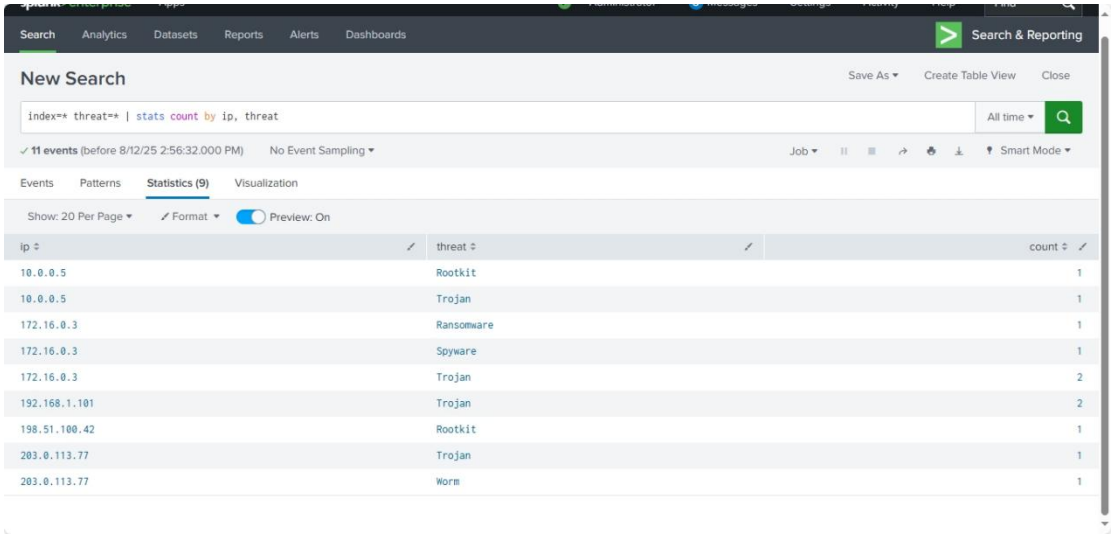
This SOC simulation task involve monitoring and analyzing security alerts using Splunk, identifying suspicious activities such as failed logins, repeated ip addresses, and malware threats. The task includes classifying incidents by severity, drafting an incident response report, and providing recommendations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

Splunk Analysis Screenshots

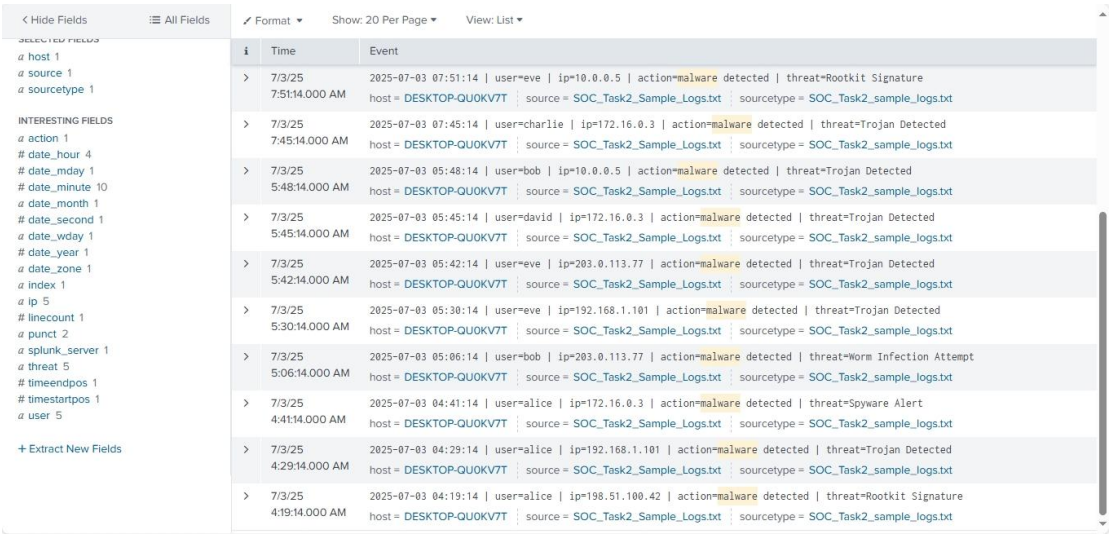
1. Failed login attempts



2. Suspicious repeated ip addresses



3. Malware threats detection



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