Security Alert Monitoring & Incident Response Report

Name: Okoro Destiny Nkem

Task 2: Security Alert Monitoring & Incident Response

Program: Future Interns Cybersecurity Internship

Tools Used:

- Splunk Enterprise (Free Trial)
- SOC_Task2 SampleLogs (Data Source)

Date: August 2025

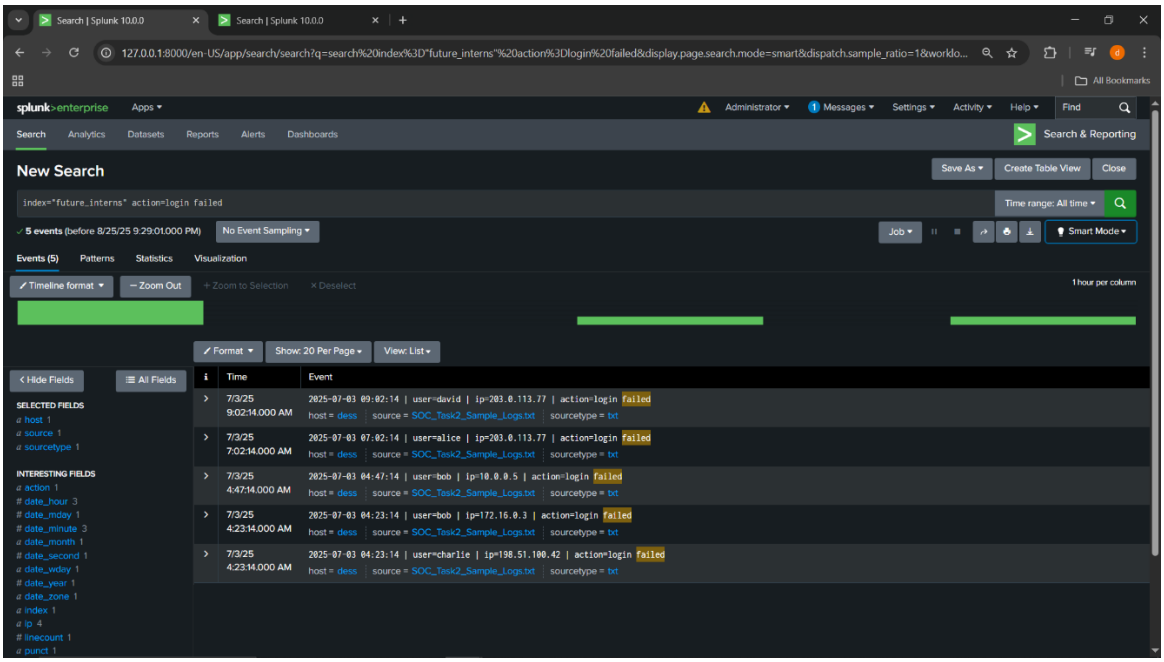
Task Summary

In this task, I successfully set up and explored Splunk as a SIEM tool to monitor and analyze security events. I generated a summary dashboard within Splunk to visualize security alerts and their status, and also triggered alert actions for suspicious events to simulate real time incident handling. And as part of communication best practices, I prepared an incident notification email template for management reporting. This exercise demonstrated key SOC analyst functions such as log monitoring, threat detection, alert response, and structured incident communication.

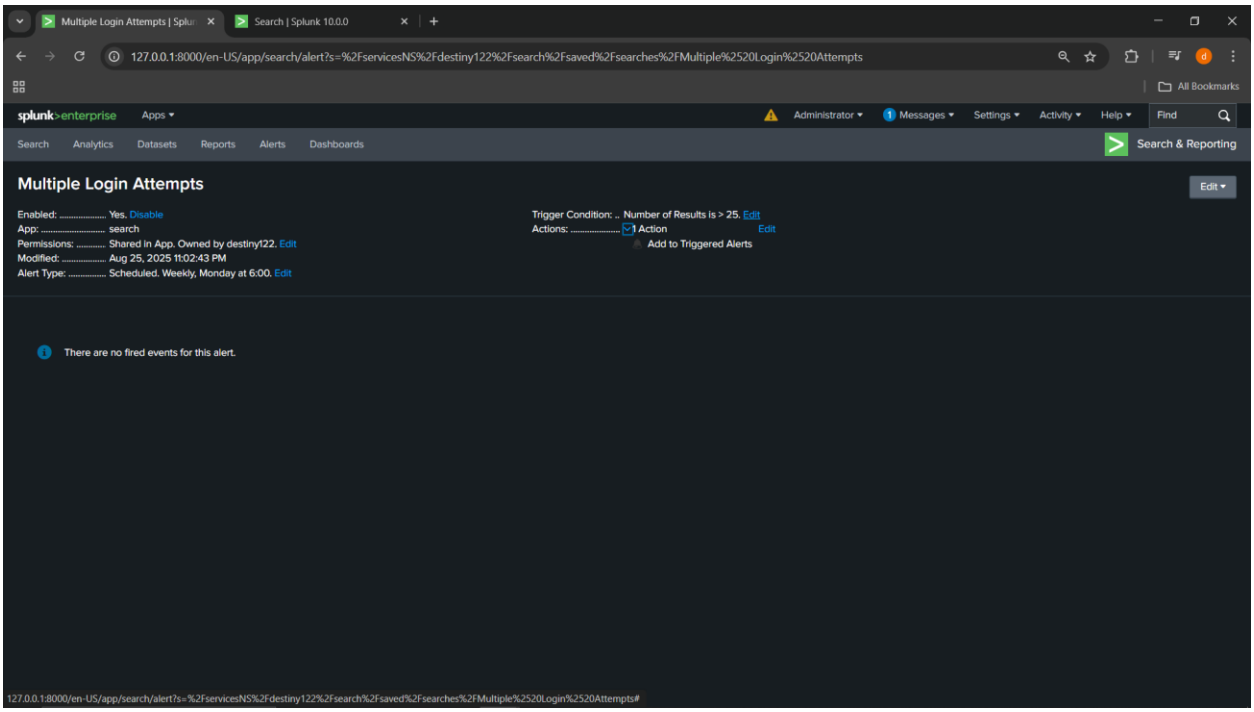
Identified Alerts

1. **Multiple Login Attempts**

Using Splunk, I identified several failed login attempts originating from multiple external IP addresses. The repeated failures from different sources suggest a potential brute-force attack or unauthorized access attempt targeting user accounts.



This activity was classified as a **High Priority** Alert due to the risk of account compromise. And in response to that, I triggered alert actions within Splunk to ensure immediate notification of security personnel.

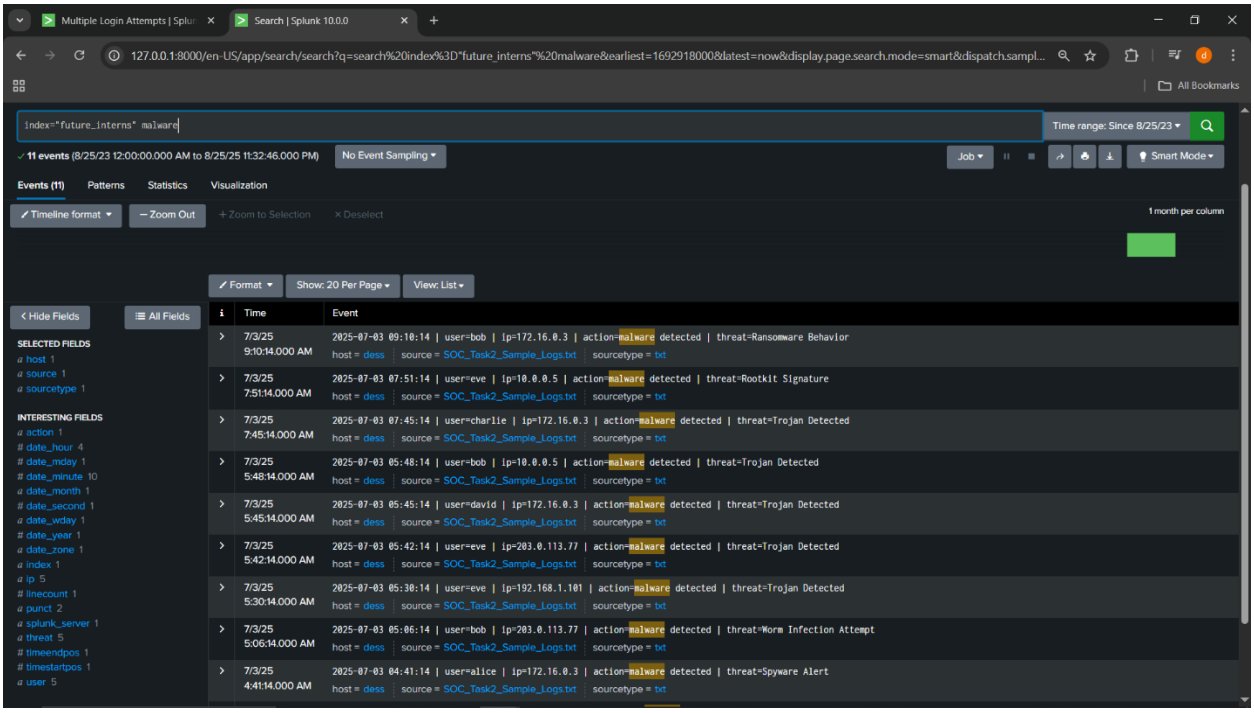


Remediation Suggestions:

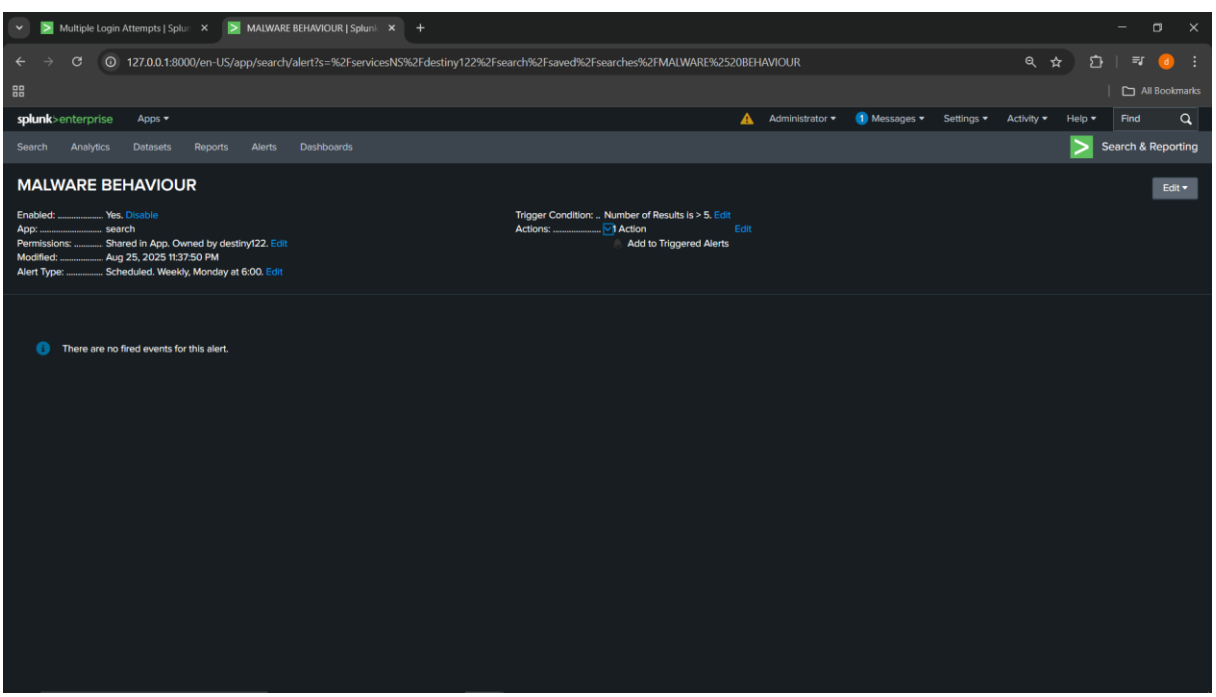
i. Implement account lockout policies after repeated failed attempts.
ii. Enforce Multi-Factor Authentication (MFA) for all user accounts.

2. **Malware detection alerts**

Using Splunk and applying Search Processing Language (SPL) queries, I filtered suspicious events related to malware activity. The logs revealed multiple detections, including ransomware behavior, rootkit signatures, trojan infections, worm activity, and spyware alerts. These events originated from different IP addresses and highlight potential compromise attempts across the environment.



This activity was classified as a **High Priority** Alert due to the severity of threats associated with malware infections. To simulate real-time SOC operations, I configured Splunk to trigger alert actions for immediate security team notification.

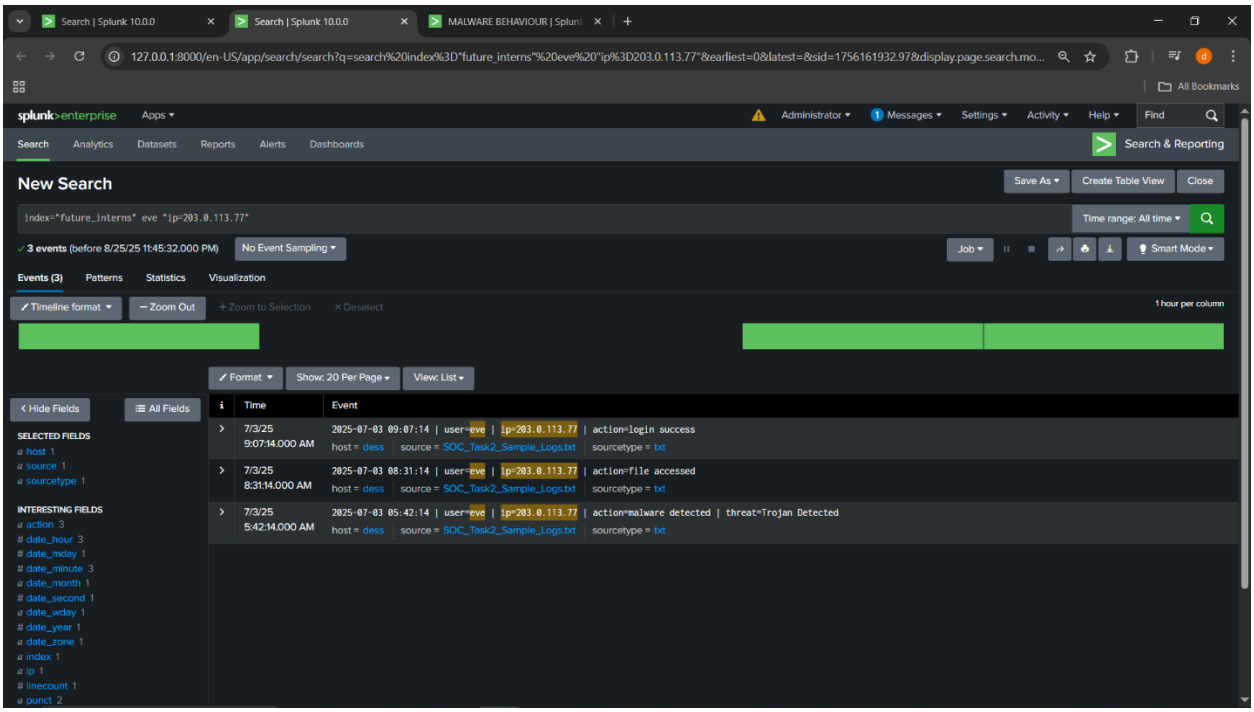


Remediation Suggestions:

i. Immediately isolate affected hosts to prevent malware propagation.
ii. Run full malware scans with updated signatures.

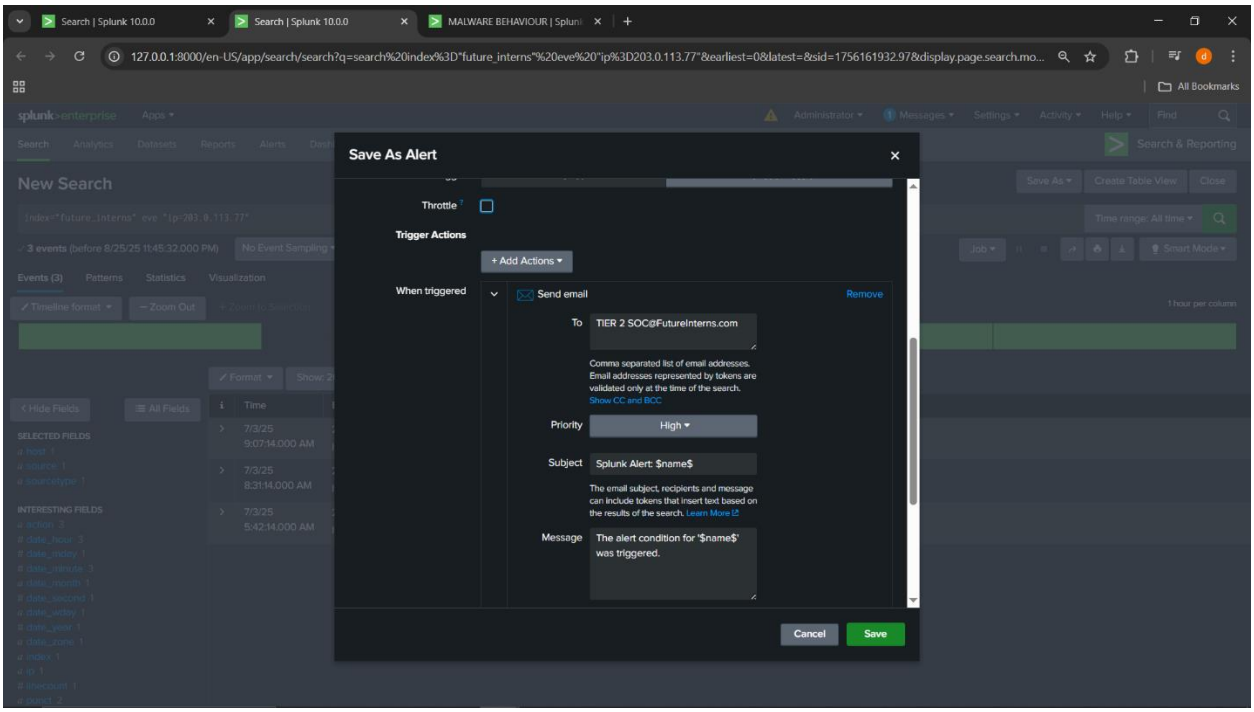
3. **Suspicious Host Activity**

Using Splunk SPL queries, I investigated events linked to a host with IP 203.0.113.77. The logs revealed a sequence of suspicious activity, a successful login, followed by file access, and later a malware detection (Trojan). This chain of events strongly suggests that the host may have been compromised after initial access.



This was classified as a **High-Priority** Alert because the activity indicates both successful authentication and possible malware execution, which together increase the risk of spread to other systems and data exfiltration.

Following the detection of suspicious activity from host 203.0.113.77 which included a successful login, file access, and subsequent malware detection , I configured an email alert in Splunk to escalate the incident details directly to the Tier 2 SOC team. This ensured that the event was formally reported to higher level analysts for deeper investigation and remediation actions.

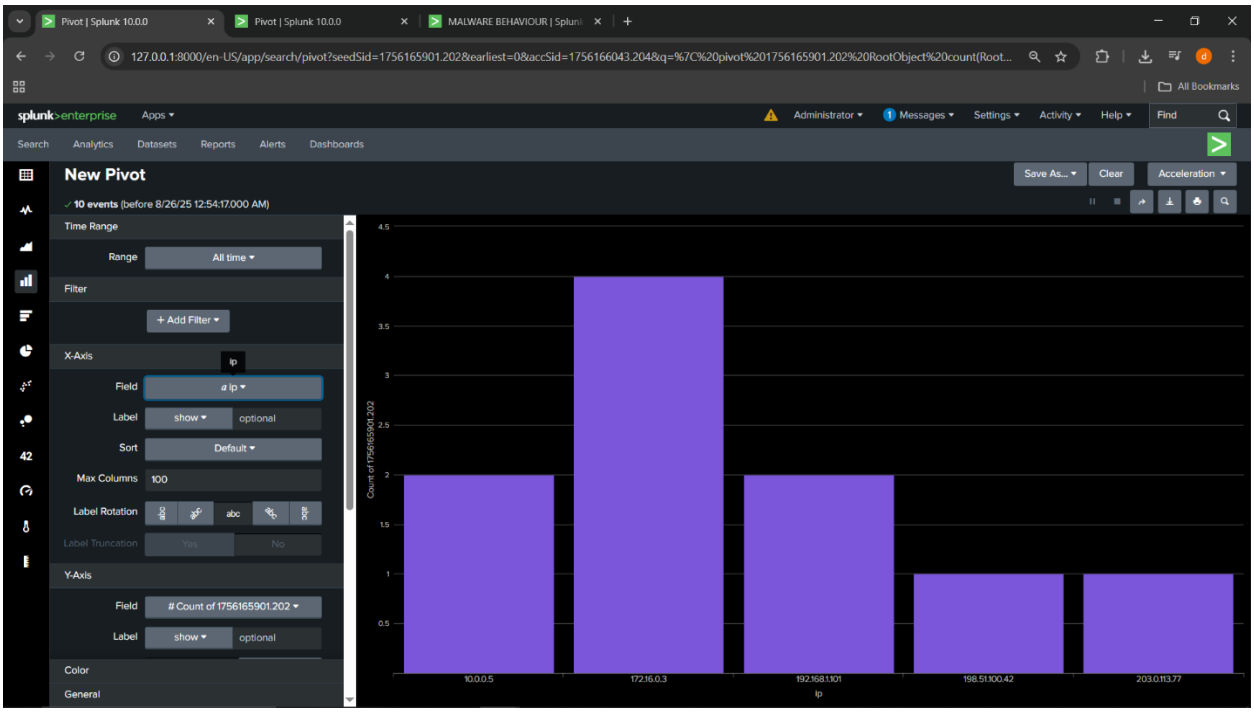


Remediation Suggestions:

i. Quarantine or isolate the host from the network.

ii. Conduct forensic investigation on login activity and accessed files.

Dashboard Summary



A column chart dashboard was generated in Splunk using an SPL query to visualize malware behavioral activity across multiple hosts. This representation provides clear insights into the distribution and frequency of malicious events, helping to quickly identify which systems were most affected and prioritize incident response efforts.

Optional Email to Management

Summary of Security Alert Monitoring & Response

Dear Security Lead,

I have completed the simulated security alert monitoring task using Splunk. During the exercise, several critical alerts were identified:

- Multiple failed login attempts from external IPs (potential brute-force attempts)
- Malware activity detections such as trojans, ransomware, and spyware
- Suspicious host activity (IP address: 203.0.113.77) involving successful login, file access, and malware execution.

Each of these incidents was classified according to severity, with High-Priority Alerts escalated to the Tier 2 SOC team via automated Splunk email alerts. I also documented the findings with timelines, potential impacts, and recommended response actions such as host isolation, account monitoring, and enhanced authentication controls.

Please advise if additional actions, reporting, or escalation are required.

Best regards,

Destiny Okoro.