SECURITY ALERT MONITORING & INCIDENT RESPONSE REPORT

Name: Odita Chukwudumebi Tobechukwu

Task 2: Security Alert Monitoring & Incident Response

Program: Future Interns Cybersecurity Internship

Date: September 2025

Task Summary

For this task, I was given a set of sample SOC logs to analyze for potential threats. My objective was to carefully study user activities, connection attempts, login outcomes, file access records, and malware detections in order to simulate the daily responsibilities of a SOC Analyst.

I used Splunk to ingest and query the logs. To make the findings clearer, I also designed a dashboard summarizing alert frequencies across different users and IP addresses. This allowed me to quickly spot patterns of compromise and escalation.

Finally, I drafted an incident report in the form of a management email to demonstrate how SOC teams escalate findings and ensure that critical issues are communicated effectively.

This task really helped me build confidence in log correlation, malware identification, and structured security reporting, which are all critical SOC analyst skills.

Tools Used:

- Splunk Enterprise (Trial)
- SOC_Task2_Sample_Logs.txt (Log Source)

Steps & Procedure

1. **Log Preparation & Splunk Setup**
   I started by preparing the provided log file for ingestion into Splunk. Once indexed, I ran SPL queries to filter by users, IP addresses, actions, and malware events. This step allowed me to transform raw text logs into structured and searchable data.
2. **Exploring Login Events**
   I first examined login events to differentiate between normal behavior and anomalies. I paid attention to repeated login failures, logins from unusual IP ranges, and cases where successful logins were immediately followed by suspicious actions.

3. **Correlating Malware Detections**
   I queried specifically for “malware detected” actions to see which users and hosts were repeatedly affected. This was important because repeated detections could indicate that a particular system or user account was compromised.

4. **Event Sequencing**
   I didn’t just look at single events, I studied the sequence of activities. For example, if a login success was followed by a file access and then a malware alert, that sequence is a strong sign of a breach in progress.

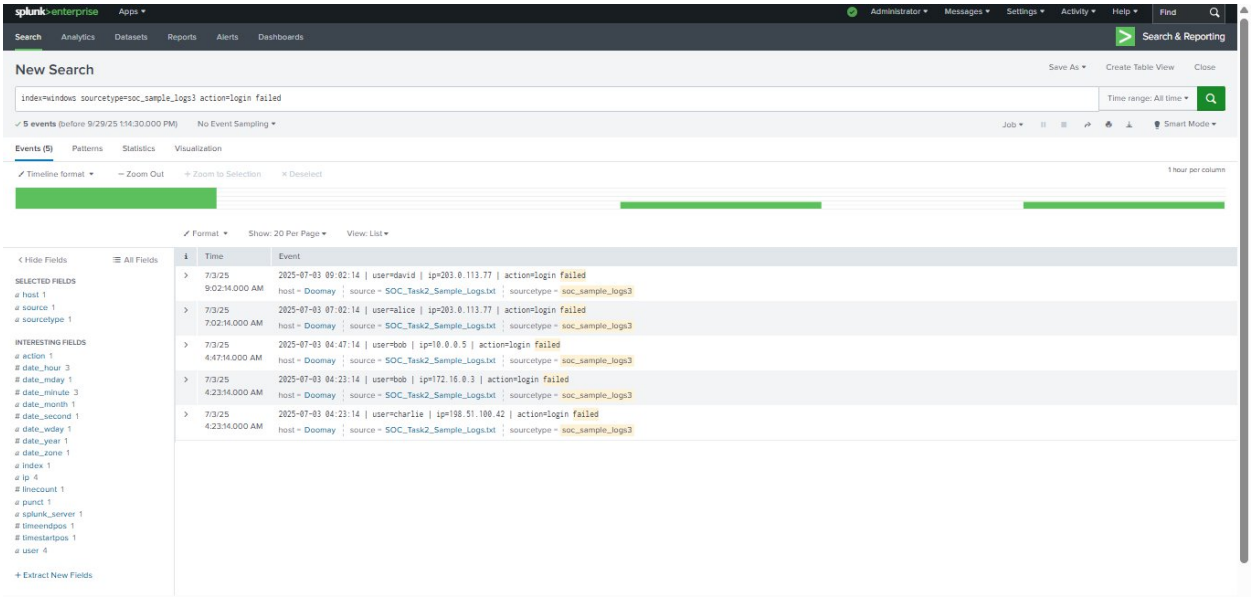
5. **Reporting & Escalation**
   After documenting all key alerts, I drafted a management email summarizing my findings, ensuring it was concise but highlighted the most critical threats and suggested actionable next steps.

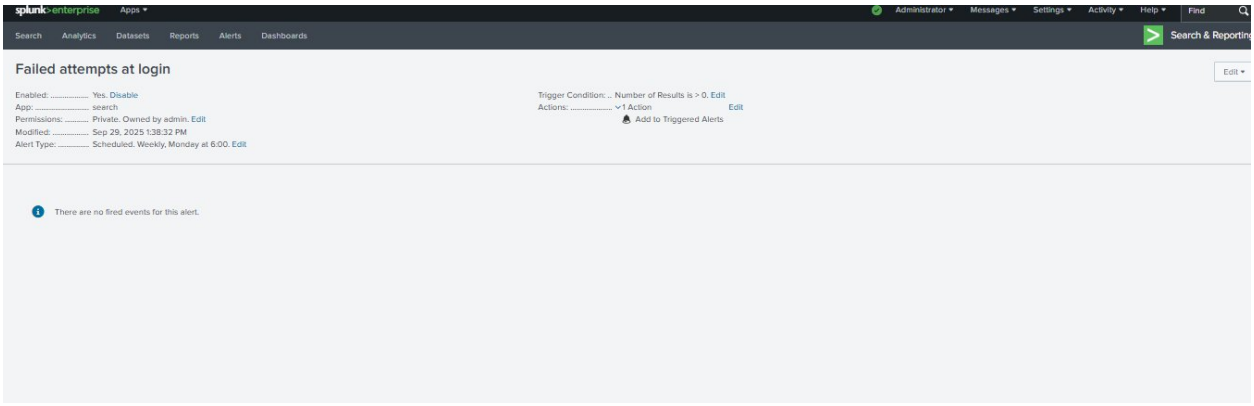
Identified Alerts

1. Multiple Login Attempts

During my review with Splunk, I noticed several failed login attempts across different IP addresses. For example, IP 203.0.113.77 and 198.51.100.42 generated repeated failures, and in some cases, a successful login later followed these failures.

This pattern stood out to me because it strongly resembles brute-force attacks**,** where attackers try multiple passwords until one works. The fact that some of these accounts eventually showed successful logins indicates that at least one attempt may have worked.





<u>Why this is concerning</u>**:** Unauthorized access could allow attackers to blend in as legitimate users.

Remediation Suggestions:

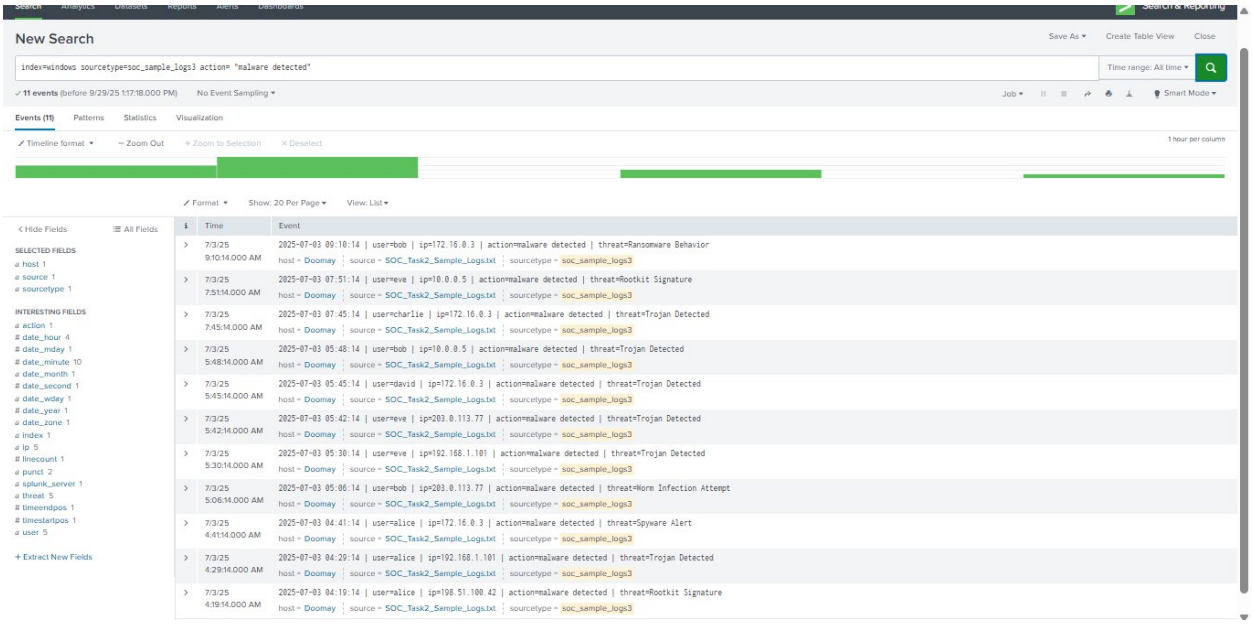
- Enforce Multi-Factor Authentication (MFA) immediately to make stolen credentials less useful.
- Apply account lockout policies to slow down brute-force attempts.

2. Malware Detection Alerts

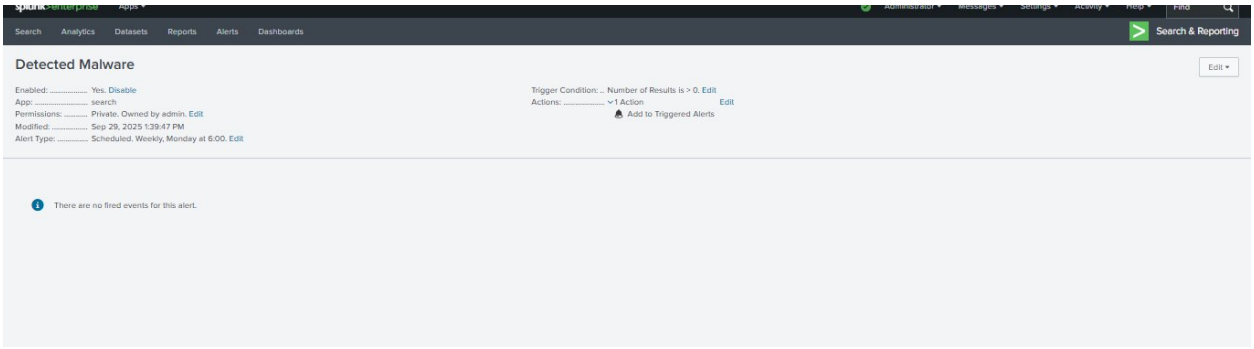
Using Splunk's Search Processing Language (SPL) I was able to point out the fact that malware alerts were widespread in the logs. I identified detections for:

- Trojans – suggesting backdoor or remote access attempts
- Rootkits – indicating stealthy persistence methods
- Spyware – possible data exfiltration attempts
- Worms – attempting to spread laterally
- Ransomware Behavior – particularly dangerous as it could encrypt files

These were spread across several users and hosts (notably Alice, Bob, and Eve).This indicates either their accounts were compromised or their systems were repeatedly targeted.



Why this is concerning**:** A single type of malware might be manageable, but seeing **f**ive distinct malware categories suggests that the environment is under coordinated attack or has multiple infection vectors.

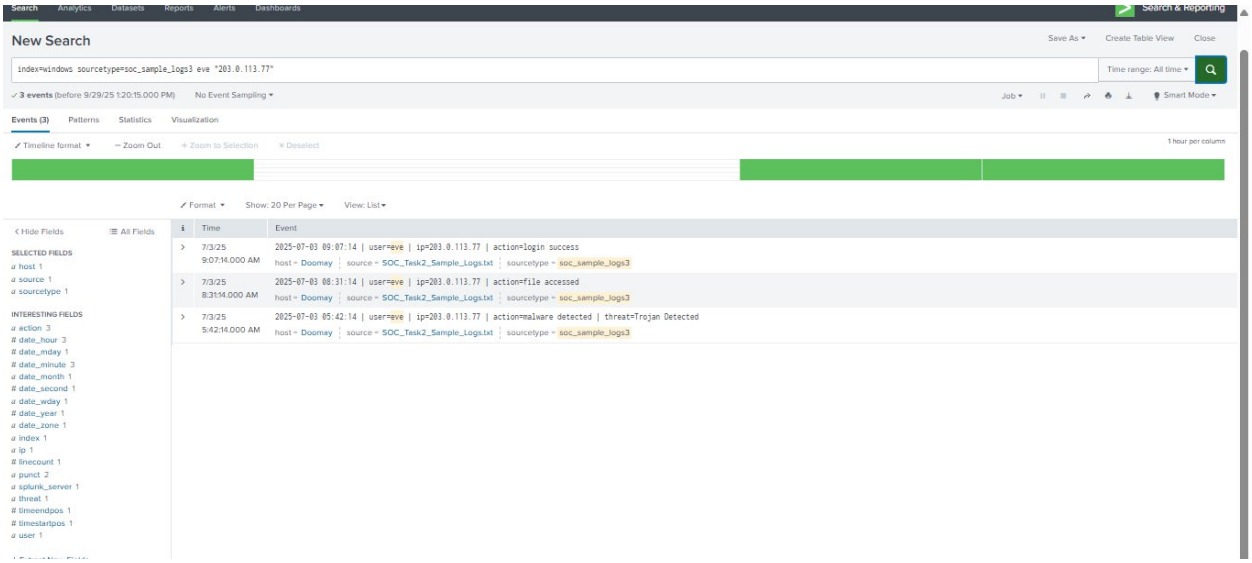


Remediation Suggestions:

- Immediately isolate compromised hosts.
- Conduct full malware scans with updated definitions.
- Strengthen endpoint protection.
- Perform threat-hunting to check for persistence mechanisms.

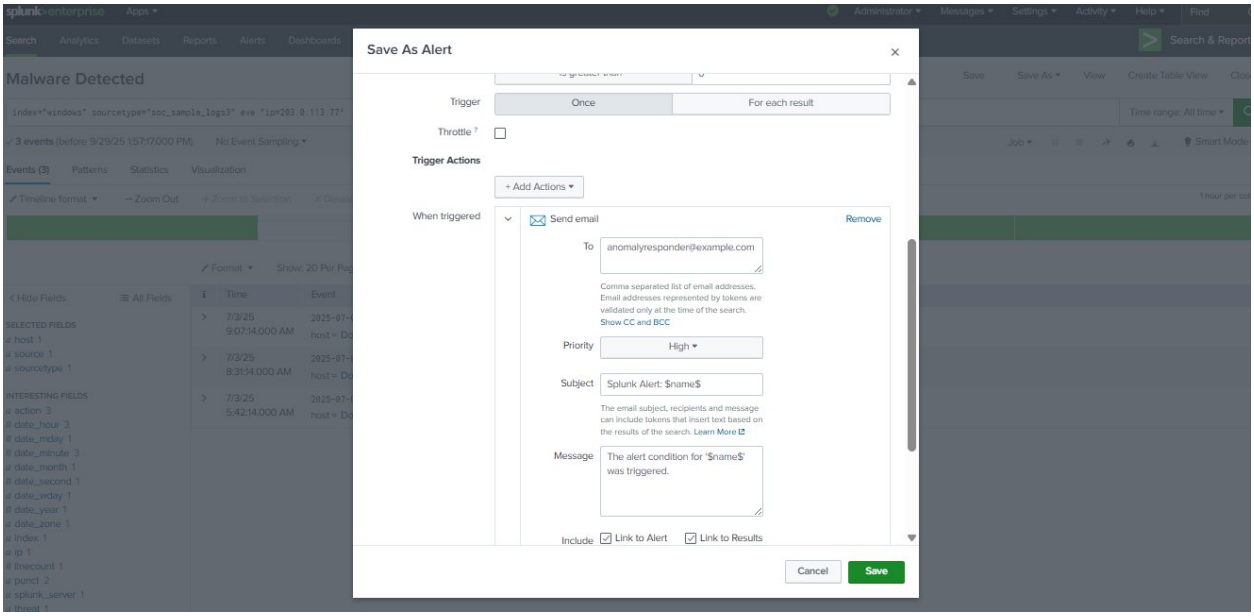
3. Suspicious Host Activity

Using Splunk's Search Processing Language (SPL), I investigated a sequence of suspicious events, one notable case involved host 203.0.113.77, where a successful login was followed by file access and then a Trojan detection. This event sequence strongly indicates a compromised host with potential lateral movement.



Why this is concerning: This is classic post-exploitation behavior**,** gaining access, moving through the system, and then executing malicious payloads.

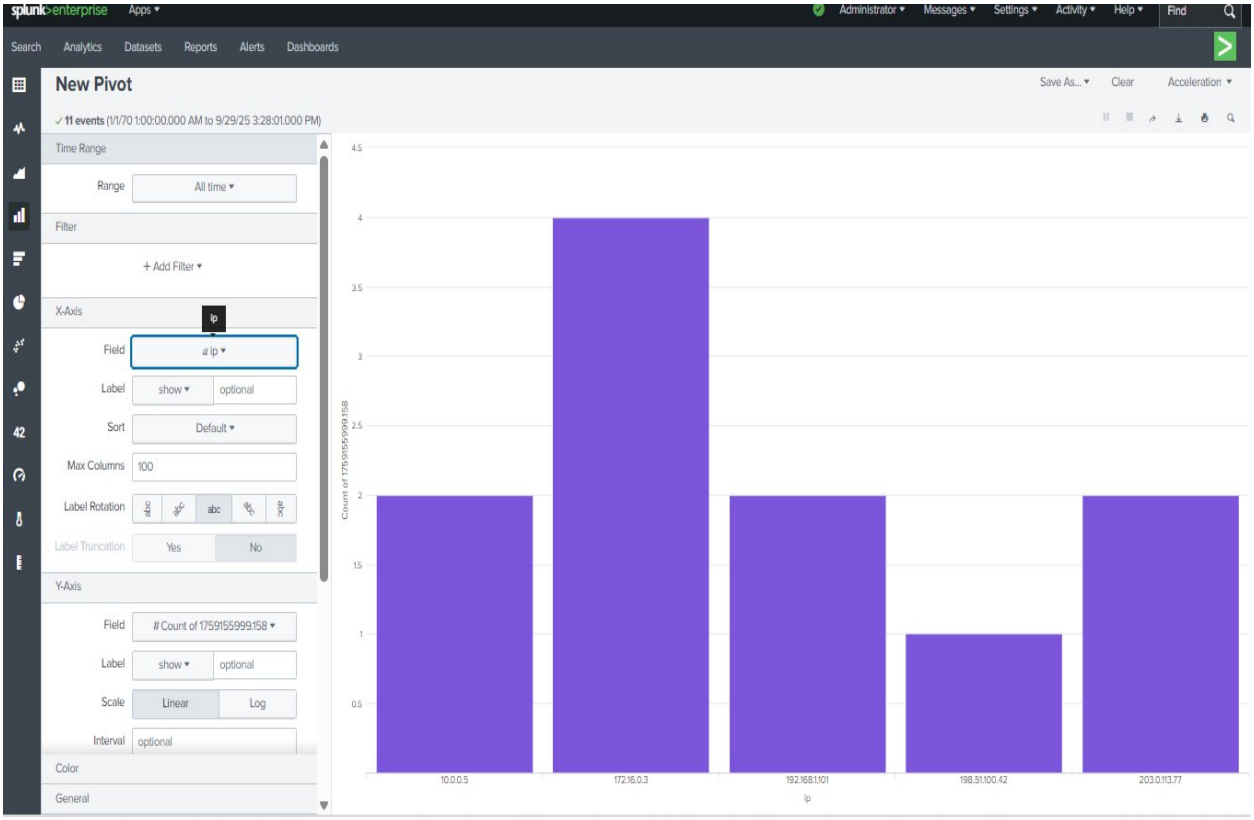
This activity was classified as a High Priority Alert because it indicates a dangerous combination of both successful authentication and malware execution. This pairing significantly increases the risk of malware propagation to other systems and the potential for data exfiltration. Following the detection 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.



Remediation Suggestions:

- Quarantine the affected host.
- Investigate accessed files for exfiltration.
- Review user account for credential compromise.

Dashboard Summary



The dashboard I created provided a visual breakdown of malware activity across users and hosts. This visualization made it clear which accounts were most repeatedly attacked and where the bulk of infections were coming from. Having this bird's-eye view was helpful to prioritize which systems needed urgent remediation.

Optional Email to Management

Security Alert Monitoring & Response

Dear Security Lead,

I have completed the simulated security alert monitoring task using Splunk. During the recent security log monitoring exercise, several high-priority incidents were detected that require immediate attention:

Brute-Force Attempts**:** Multiple failed login attempts were recorded from suspicious IP addresses, some of which were followed by successful logins. This indicates a high likelihood of credential compromise.

Malware Activity**:** Alerts were triggered for various malware types, including Trojans, Rootkits, Worms, Spyware, and Ransomware. These infections were observed across multiple user accounts and hosts, suggesting coordinated or widespread attack activity.

Compromised Host: A clear compromise was identified on host **203.0.113.77**, where a successful login was immediately followed by file access and a Trojan detection. This sequence of events is highly indicative of unauthorized access and malware execution.

Each of these incidents was classified based on its severity and escalated as a high-priority alert to the Tier 2 SOC team via automated Splunk email alerts. I have documented my findings, including timelines, potential impacts, and recommended response actions such as host isolation, account monitoring, and implementing enhanced authentication controls. Please let me know if any additional actions, reporting, or escalation are required.

Sincerely,

Chukwudumebi Odita