Incident Response Report – Task 2 (SOC Internship)

Table of Contents

1. Introduction

This report documents the findings from Task 2 of the SOC Internship Program, focused on Security Alert Monitoring and Incident Response using Splunk. The goal of this exercise is to analyze simulated log data, detect suspicious activities, and recommend appropriate incident response actions.

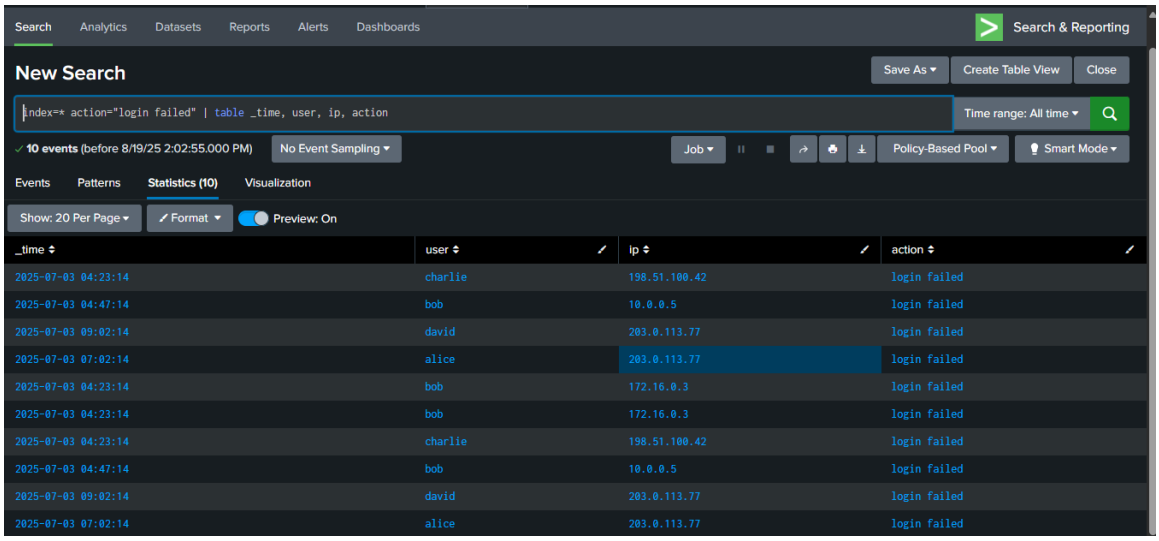
2. Incident Summary

During the analysis of provided system logs, several suspicious activities were identified, including repeated failed login attempts, multiple malware detections, and connections from unusual external IP addresses. These findings suggest potential brute-force attempts, malware infections, and possible unauthorized access from outside the network.

3. Detection and Analysis

3.1 Failed Login Attempts

Search Query:
index=* action="login failed" | table _time, user, ip, action

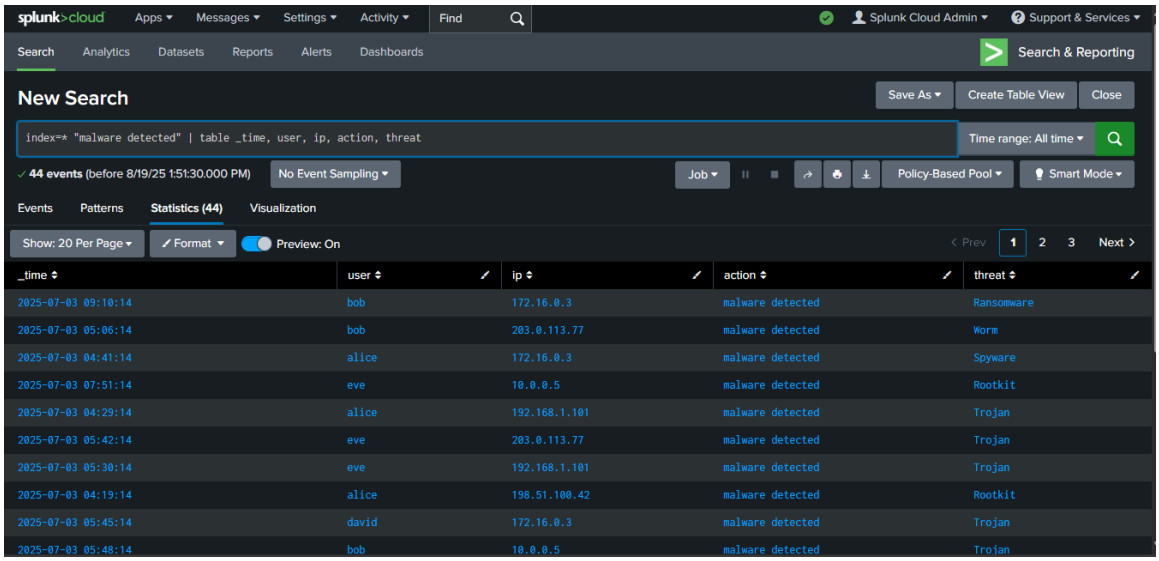


Analysis: Multiple failed login attempts were detected across different users. This pattern may indicate brute-force attack attempts or unauthorized users trying to guess credentials. Monitoring should be intensified for accounts with repeated failed attempts.

3.2 Malware Detection Alerts

Search Query:

index=* action="malware detected" | table _time, user, ip, threat



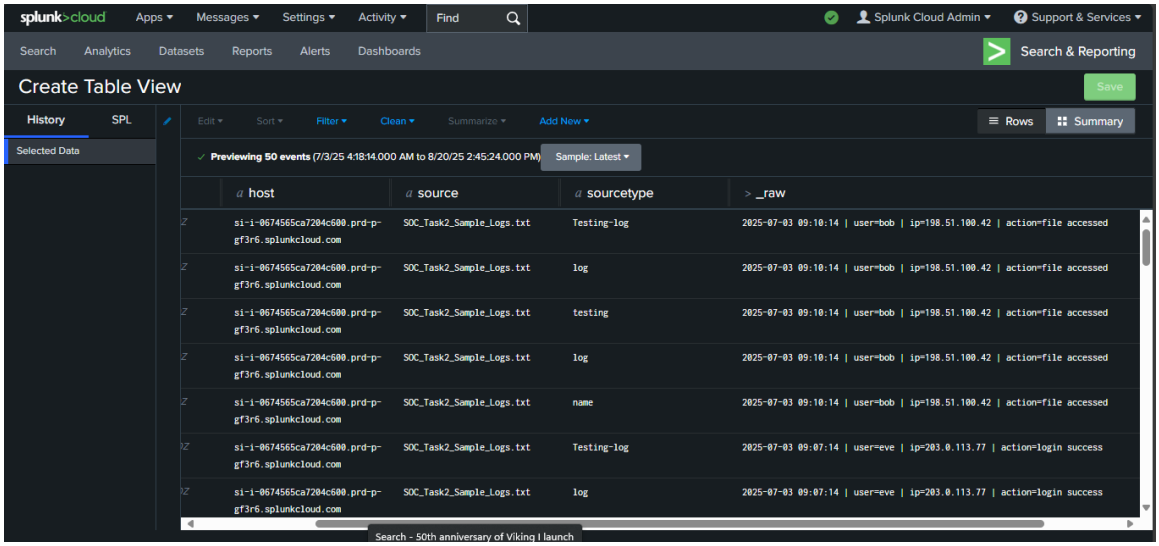
Analysis: Several malware alerts were triggered, including Trojan, Rootkit, and Ransomware detections. These represent high-severity threats that could compromise system integrity. Immediate containment and system scans are recommended to prevent lateral movement of threats.

3.3 External IP Connections

Search Query:

index=* source="SOC_Task2_Sample_Logs.txt"

NOT (ip="10.*" OR ip="192.168.*" OR ip="172.16.*")



Analysis: Logs show multiple connection attempts from external IP ranges such as 198.51.x.x and 203.0.x.x. These IPs are not part of the internal private ranges, suggesting potential unauthorized external access attempts. Such events should be investigated and blocked if necessary.

4. Containment, Eradication, and Recovery

Based on the detected incidents, the following actions are recommended:
- Block suspicious external IP addresses at the firewall level.
- Reset compromised user accounts and enforce multi-factor authentication.
- Quarantine affected machines and run full malware scans.
- Apply security patches and harden system configurations.

5. Lessons Learned

This task highlights the importance of proactive monitoring using SIEM tools like Splunk. Regular log analysis enables early detection of brute-force attempts, malware infections, and unauthorized access. Clear documentation and communication ensure faster incident response and minimize business impact.