Incident Response Report

Name: Kumari Tulsi

Task 2: Multiple Security Alerts Detected Through Splunk SIEM

Program: Future Interns Cybersecurity Internship

Date: September 2025

Target Application: Splunk SIEM (Analyzed SOC_Task2_Sample_Logs.txt)

Task Summary

This task focused on monitoring and analyzing system logs using Splunk SIEM to identify suspicious activities such as failed logins, unusual IP addresses, and malware detection alerts. The objective was to simulate real-world SOC Analyst responsibilities: threat detection, incident triage, and drafting an incident response report.

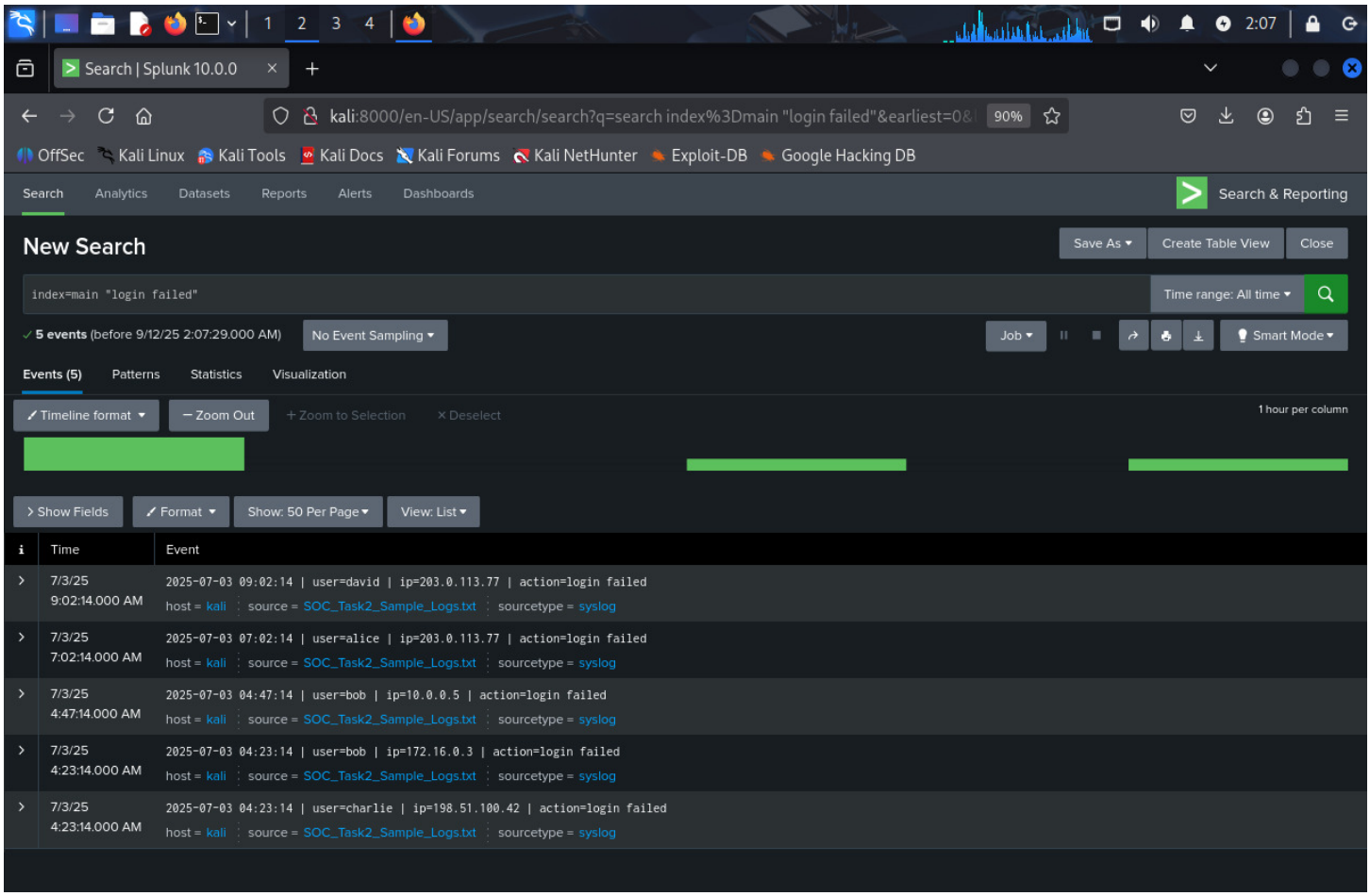
Tools Used

- **Splunk SIEM (Free Trial)** – For log ingestion and analysis
- **Kali Linux** – Host environment
- **SOC_Task2_Sample_Logs.txt** – Sample log dataset provided
- **Manual Analysis & Filtering (grep, Splunk queries)**

Findings

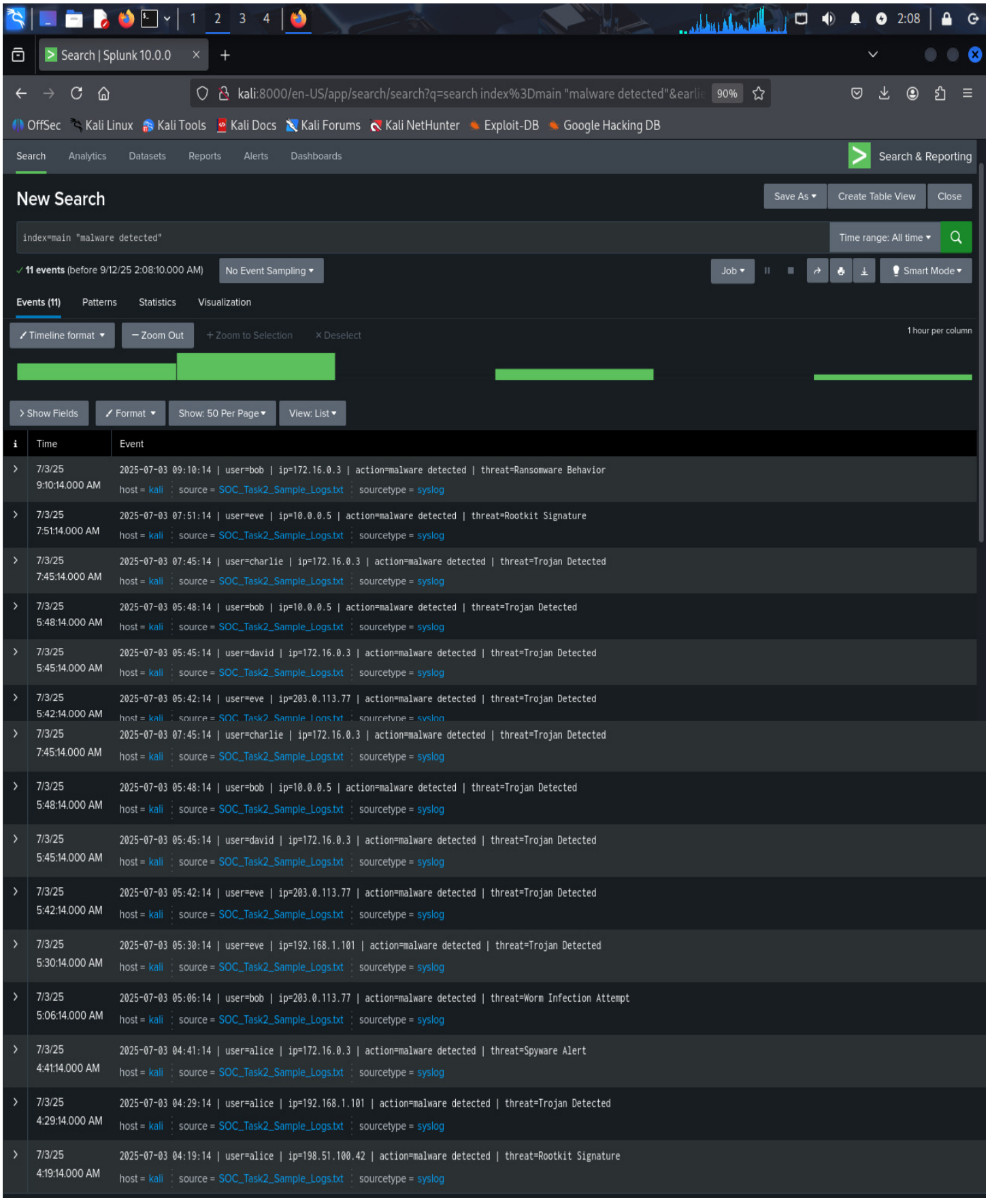
1. Failed Login Attempts

- Multiple failed logins observed from suspicious IPs.
- **Users:** alice, bob, charlie, david
- **IPs: 203.0.113.77, 10.0.0.5, 198.51.100.42**



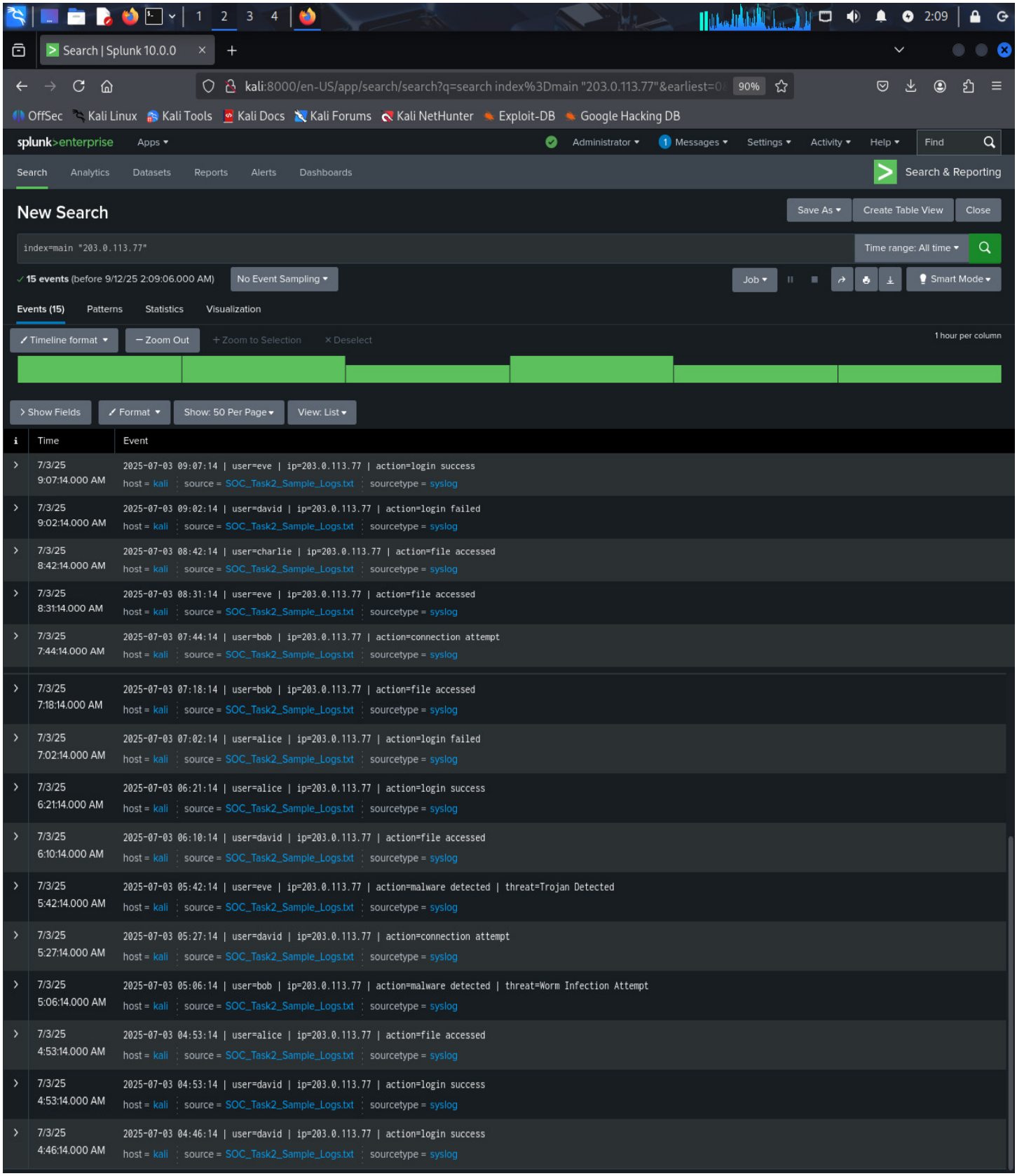
2. Malware Detection Events

- **Threats:** Ransomware, Rootkit, Trojan, Worm, Spyware
- **Users Involved:** bob, alice, eve, charlie, david
- **IPs Involved:** 172.16.0.3, 198.51.100.42, 192.168.1.101, 203.0.113.77, 10.0.0.5



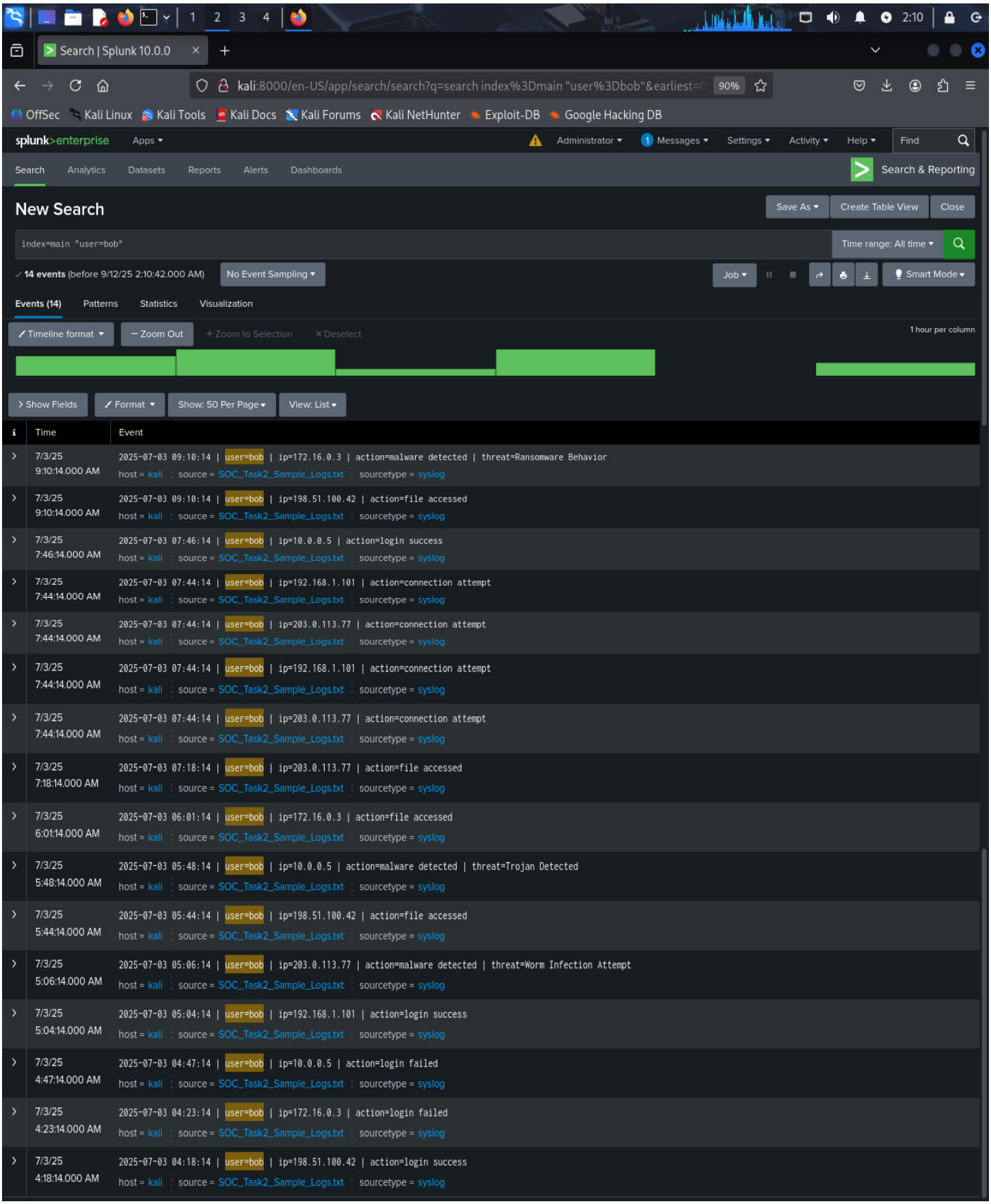
3. Suspicious External IPs

- IP **203.0.113.77** repeatedly flagged in malware + failed login logs.
- Indicates brute-force or coordinated external attack.



4. User Account Activity (user=bob)

- Logs specifically highlighted suspicious activity tied to **user=bob**.
- Bob's account appears in **ransomware detection** and **failed login attempts**, suggesting it was both **compromised and targeted**.
- **IPs linked to Bob:** 172.16.0.3 (internal system), 203.0.113.77 (external attacker).



Impact & Risk Assessment

- **Ransomware (bob – 172.16.0.3)** → High risk: Could encrypt data and cause loss.
- **Rootkit (alice – 198.51.100.42, eve – 10.0.0.5)** → High risk: Persistence + privilege escalation.
- **Failed logins (alice, bob, david, charlie)** → Medium risk: Possible brute-force attempts.
- **Suspicious IP 203.0.113.77** → High risk: Multiple attack types from one external source.
- **Compromised User bob** → Critical: Actively targeted + already infected.

Recommendations / Remediation

- Isolate infected systems immediately.
- Block suspicious IPs (esp. 203.0.113.77).
- Reset affected user credentials (Alice, Bob, Eve, Charlie, David).
- Enable MFA and account lockout policies.
- Perform full forensic analysis on compromised hosts.
- Patch and harden internal systems (172.16.0.3, 10.0.0.5, etc.).

Conclusion

Splunk SIEM log monitoring revealed multiple coordinated attacks including malware infections, brute-force login attempts, suspicious external IP activity, and targeted compromise of **user=bob**.
Immediate remediation and strict monitoring actions are required to secure the environment.