SOC Task 2 - Incident Investigation Report

Prepared by: Nikhil Kumar Yadav

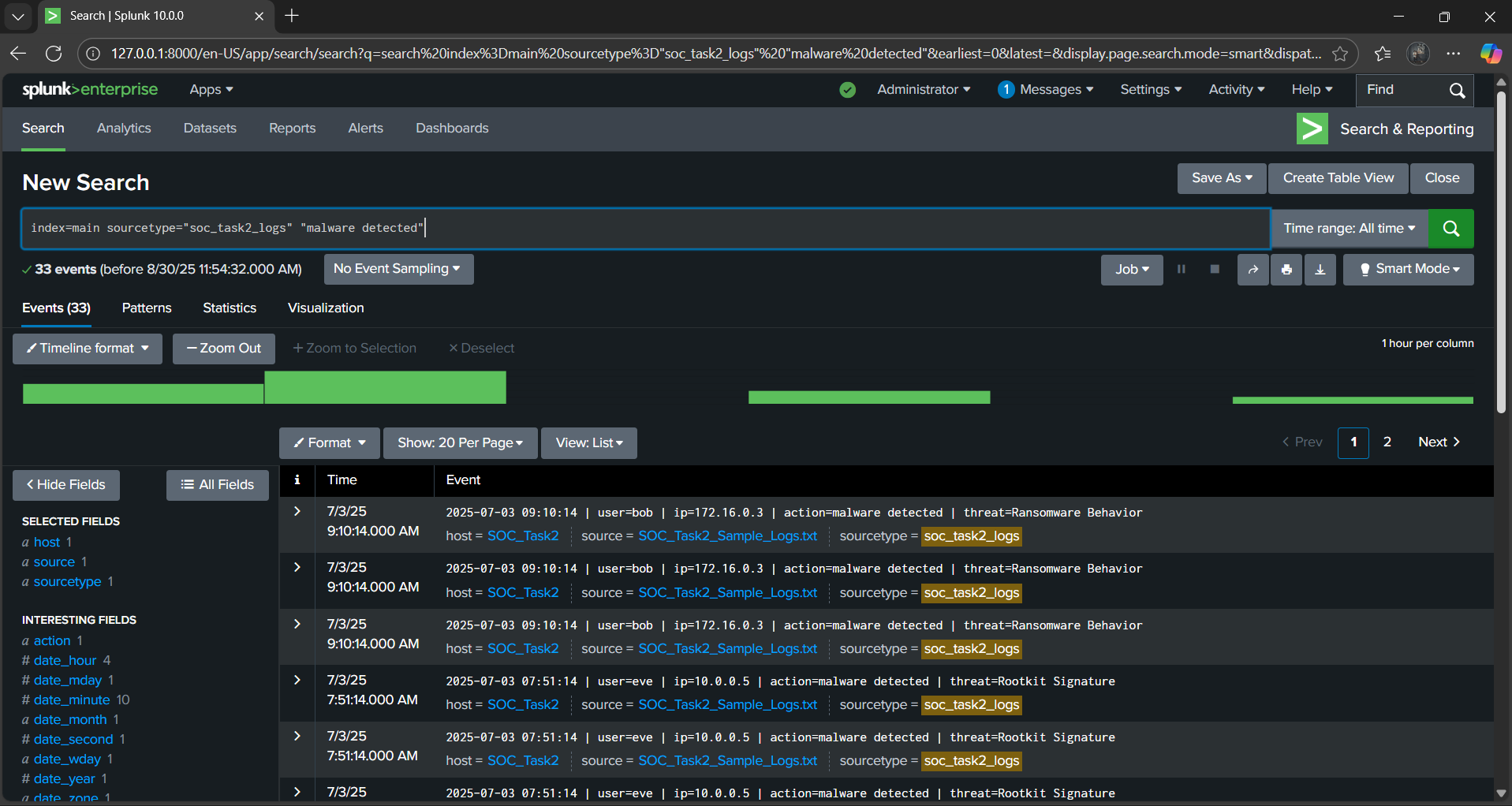
# Executive Summary

This report documents the results of the security operations analysis task. Multiple types of events were investigated using Splunk, including malware detections, file access activities, connection attempts, and failed logins. The purpose of this analysis was to identify suspicious or malicious activities within the monitored environment.

# Findings

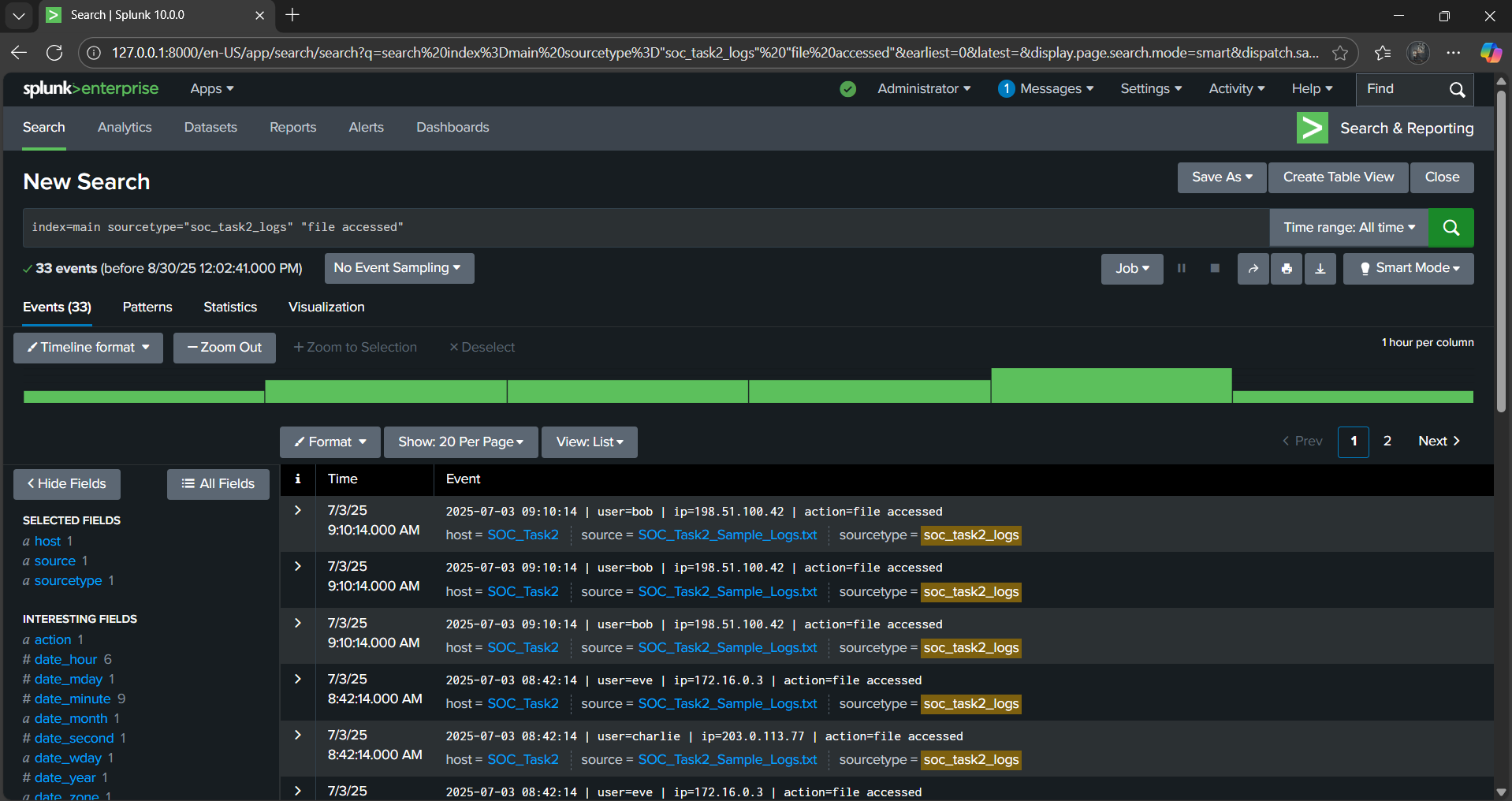
## 1. Malware Detection Events

The search for 'malware detected' events revealed multiple instances of potential malware activity. These events indicate that the environment may have been targeted or compromised by malicious software.



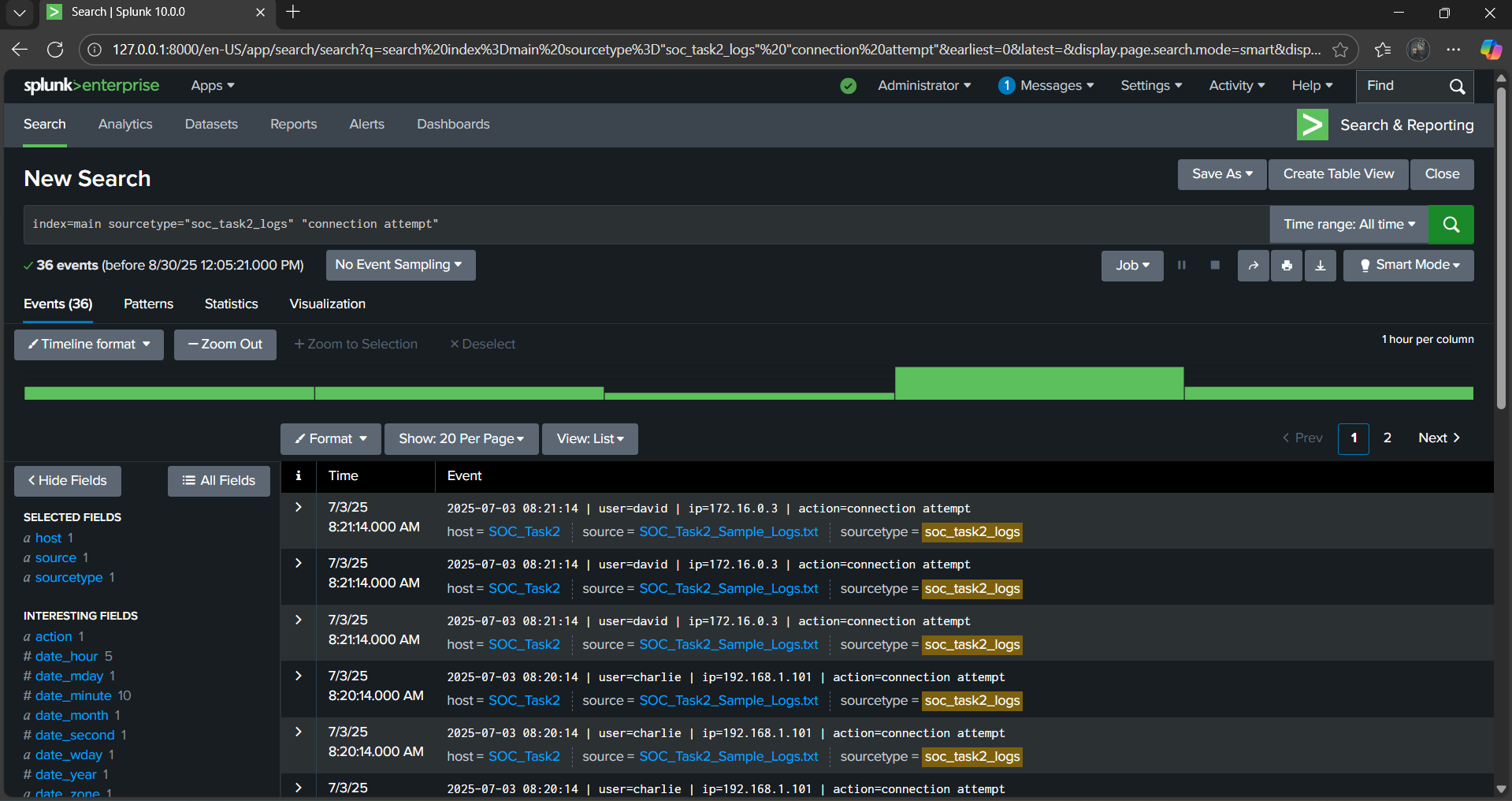
## 2. File Access Events

The search for 'file accessed' events showed records of users accessing files. While some file access may be normal, frequent or unusual access patterns may indicate insider threats or unauthorized activity.



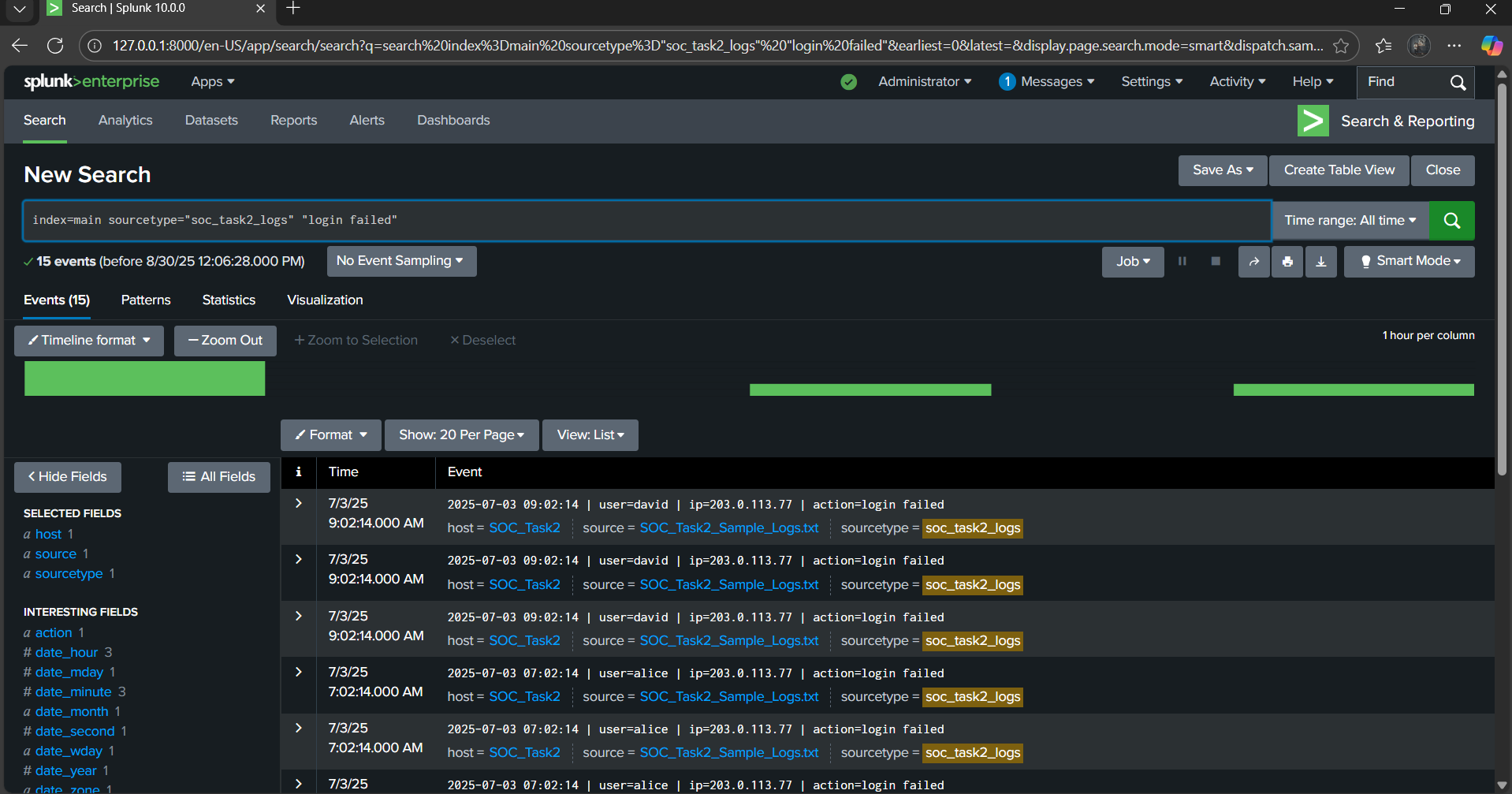
## 3. Connection Attempt Events

The search for 'connection attempt' events revealed multiple connection attempts from different users and IP addresses. These could be legitimate network activities, but repeated or failed attempts may point to reconnaissance or intrusion attempts.



## 4. Failed Login Events

The search for 'login failed' events identified several unsuccessful login attempts by multiple users. This could indicate brute force attacks or unauthorized access attempts.



# Conclusion

Based on the Splunk searches, suspicious activities were observed including malware detections, file access events, connection attempts, and failed logins. These findings highlight the importance of continuous monitoring and immediate remediation steps.

# Recommendations

- Investigate malware detection events in detail and isolate affected systems.  
- Review file access logs for anomalies and verify if access was authorized.  
- Monitor and restrict suspicious connection attempts.  
- Implement account lockout policies to prevent brute force login attempts.  
- Regularly update and patch systems to reduce vulnerabilities.