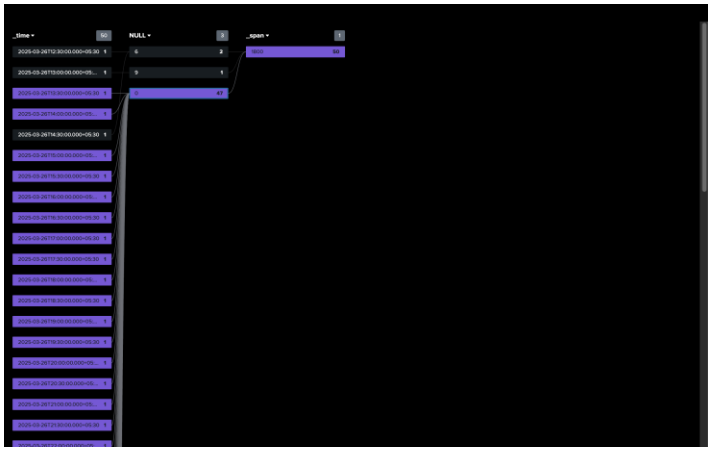
Mac Security Log Analysis Report

Objective:

Analyzed authentication failures and security logs on my personal Mac using Splunk to identify potential security threats and unauthorized access attempts.

Approach:

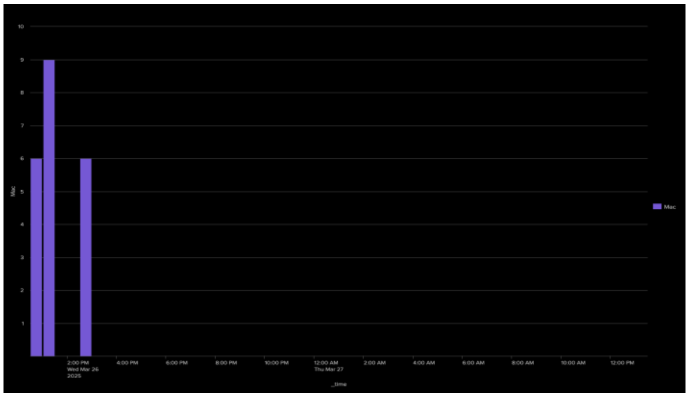
- Collected system logs (syslog) and filtered for authentication failures, errors, and security-related events.


_time ▾ 50
2025-03-26T12:30:00.000+05:30 1
2025-03-26T13:00:00.000+05:... 1
2025-03-26T13:30:00.000+05:30 1
2025-03-26T14:00:00.000+05:... 1
2025-03-26T14:30:00.000+05:30 1
2025-03-26T15:00:00.000+05:... 1
2025-03-26T15:30:00.000+05:30 1
2025-03-26T16:00:00.000+05:... 1
2025-03-26T16:30:00.000+05:30 1
2025-03-26T17:00:00.000+05:30 1
2025-03-26T17:30:00.000+05:30 1
2025-03-26T18:00:00.000+05:... 1
2025-03-26T18:30:00.000+05:30 1
2025-03-26T19:00:00.000+05:... 1
2025-03-26T19:30:00.000+05:30 1
2025-03-26T20:00:00.000+05:... 1
2025-03-26T20:30:00.000+05:... 1
2025-03-26T21:00:00.000+05:... 1
2025-03-26T21:30:00.000+05:30 1
2025-03-26T22:00:00.000+05:... 1
NULL ▾ 3
6 2
9 1
0 47
_span ▾ 1
1800 50

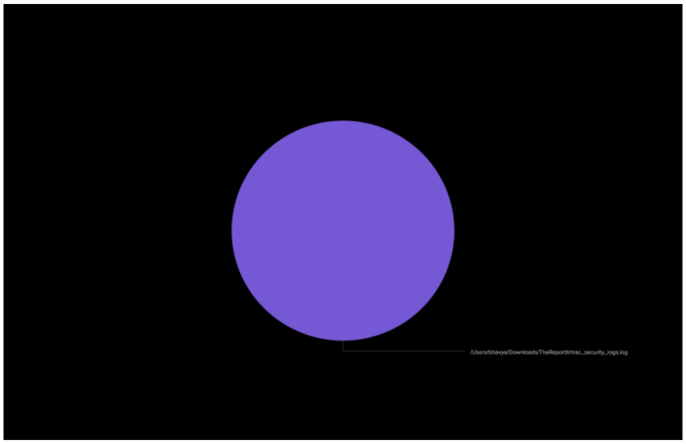
- Used Splunk queries to generate time-based trends and source-specific statistics.
- Identified failed login attempts, their frequency, and possible security vulnerabilities.

Findings:

- Observed multiple failed authentication attempts within a short timeframe.



- Most failures were from my user account, likely due to mistyped credentials or background processes.



- No external intrusion detected, but log monitoring is essential for future security.

Tools Used:

- Splunk for log analysis and visualization.

Conclusion:

This analysis demonstrates my ability to investigate system security issues, work with log data, and utilize Splunk for real-world cybersecurity monitoring.