

Splunk Security Event Analysis Report

Prepared by: Maximiliano Emmer Belmar

Date: March 2025

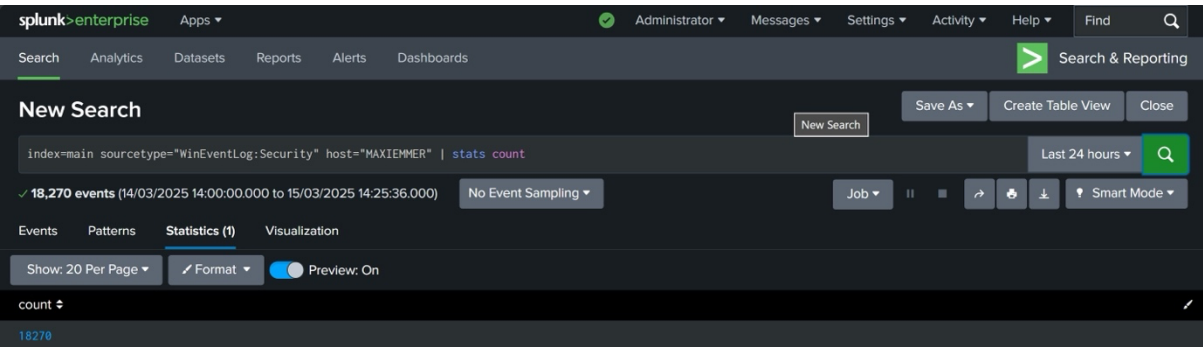
Subject: Windows Security Log Analysis & Threat Detection

1. Introduction

This report presents a comprehensive analysis of security event trends derived from Windows Event Logs. The objective is to monitor authentication activities, privilege assignments, and user enumeration attempts, providing actionable insights to enhance security monitoring and incident detection.

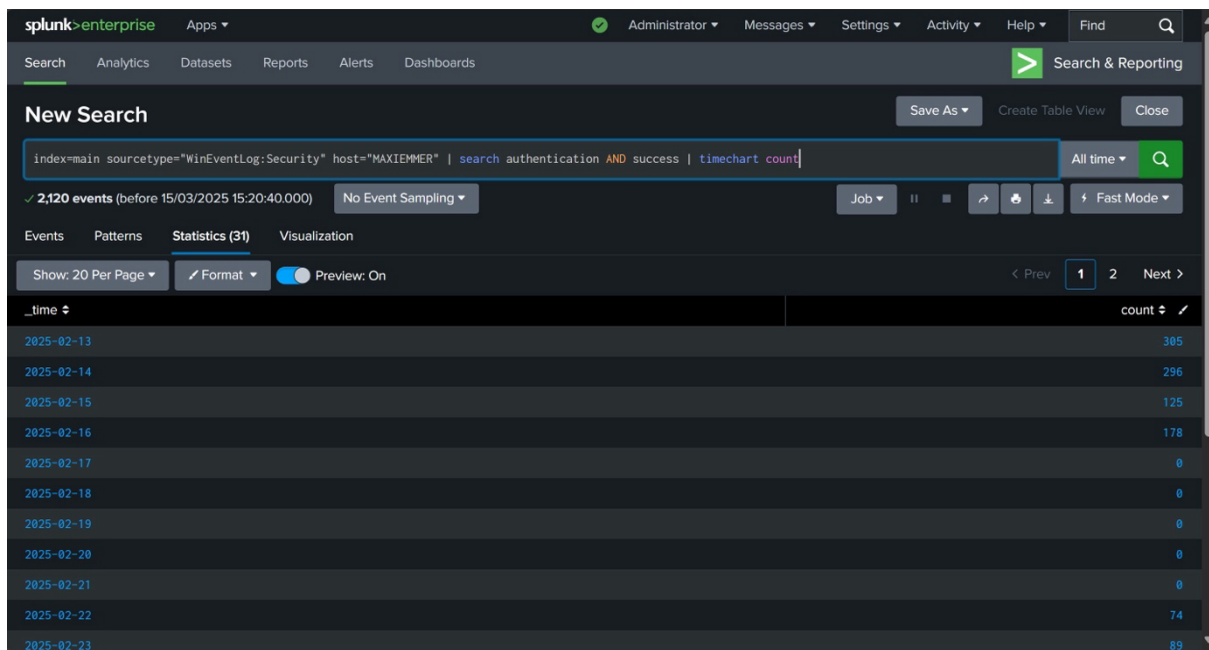
2. Key Findings

2.1 Total Events Analyzed



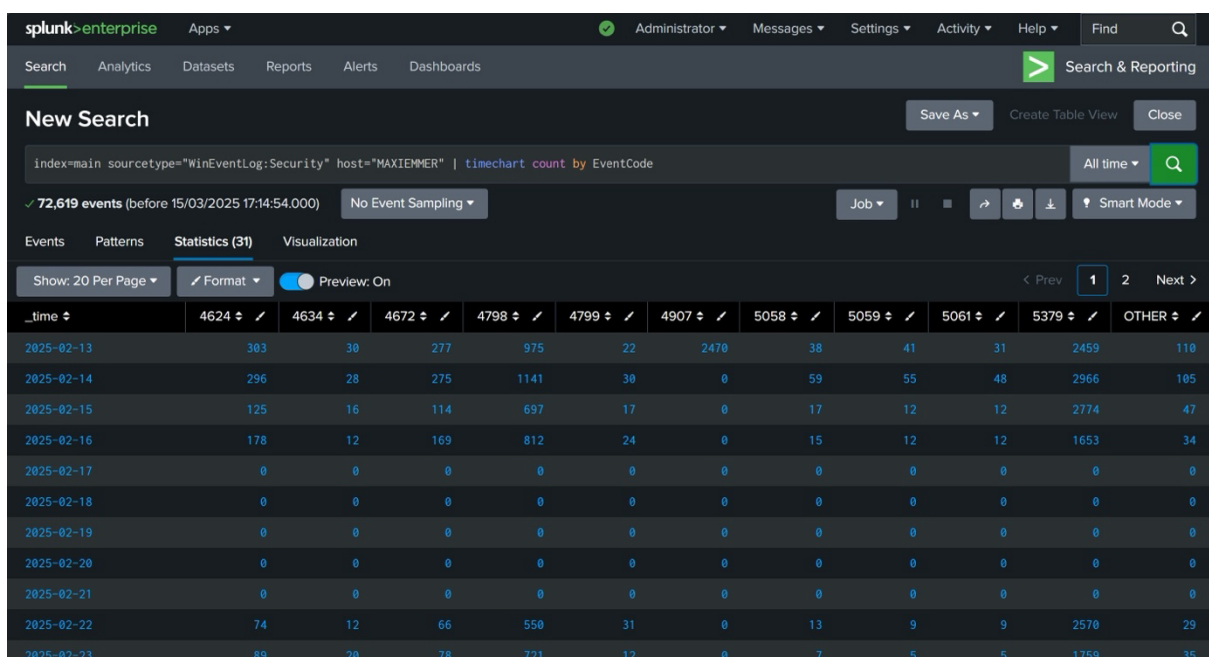
A total of 18,270 security events were recorded in the analysed timeframe. The distribution of these events provides valuable insight into authentication patterns and potential security threats.

2.2 Authentication Success Trends



The authentication success rate indicates normal user login activity trends. Peaks in successful logins were observed on February 13 and February 14, followed by a sudden drop after February 16. This anomaly may indicate potential logging issues, security policy changes, or abnormal authentication behaviour requiring further investigation.

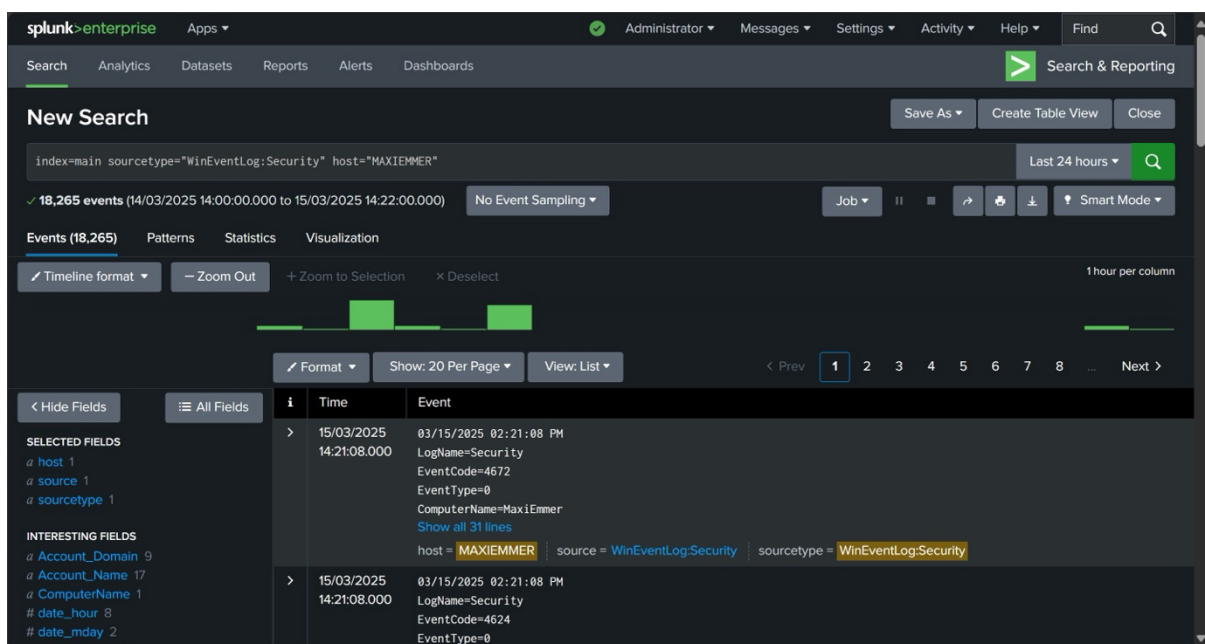
2.3 Event Code Breakdown



A breakdown of Windows Event Codes highlights critical security events, including:

- **4624 – Successful Logins:** Indicates legitimate access attempts.
- **4625 – Failed Logins:** Represents authentication failures (potential brute force or unauthorized access).
- **4672 – Privileged Logins:** Identifies elevated access attempts requiring scrutiny.
- **4798 – User Enumeration:** Possible reconnaissance activity that may indicate internal or external scanning attempts.

2.4 Log Entries



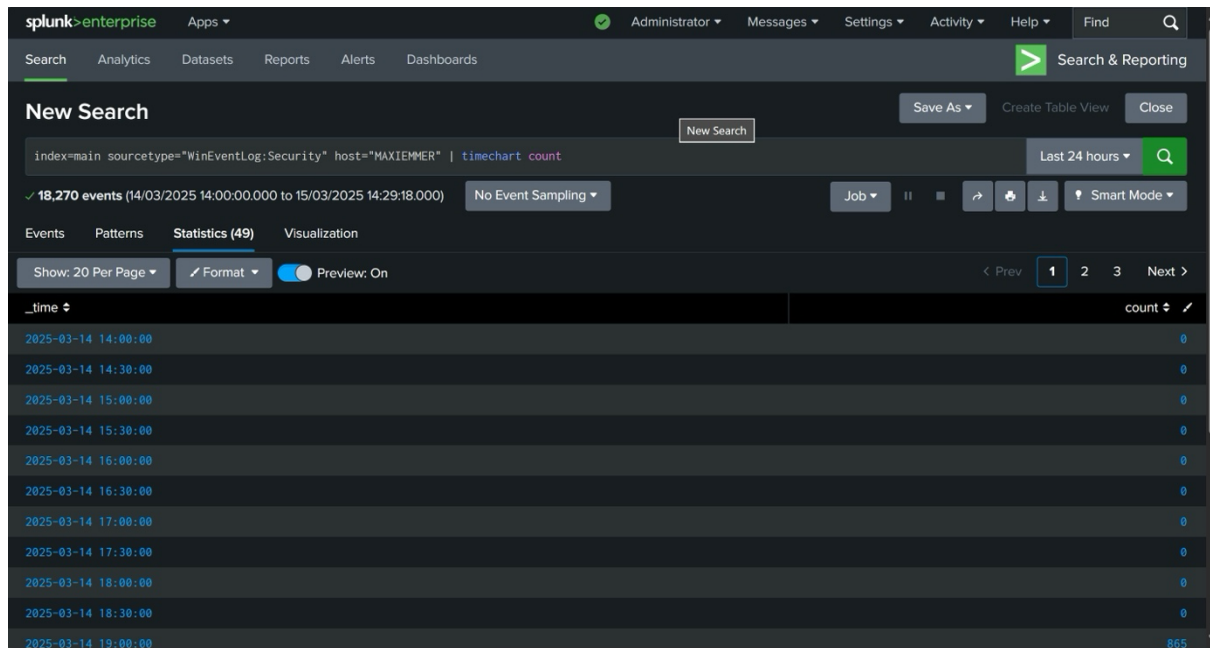
The screenshot displays the Splunk Enterprise interface for a search query: `index=main sourcetype="WinEventLog:Security" host="MAXIEMMER"`. The search results show 18,265 events from 14/03/2025 14:00:00.000 to 15/03/2025 14:22:00.000. The interface includes a search bar, a timeline visualization, and a table of results. The table shows two events:

Time	Event
15/03/2025 14:21:08.000	03/15/2025 02:21:08 PM LogName=Security EventCode=4672 EventType=0 ComputerName=MaxiEmmer Show all 31 lines host = MAXIEMMER source = WinEventLog:Security sourcetype = WinEventLog:Security
15/03/2025 14:21:08.000	03/15/2025 02:21:08 PM LogName=Security EventCode=4624 EventType=0

The collected raw log entries provide a detailed timeline of security-related events, including user authentication attempts, access control changes, and system interactions.

By analysing these logs, security teams can correlate security incidents, identify potential anomalies, and detect early indicators of compromise (IoC).

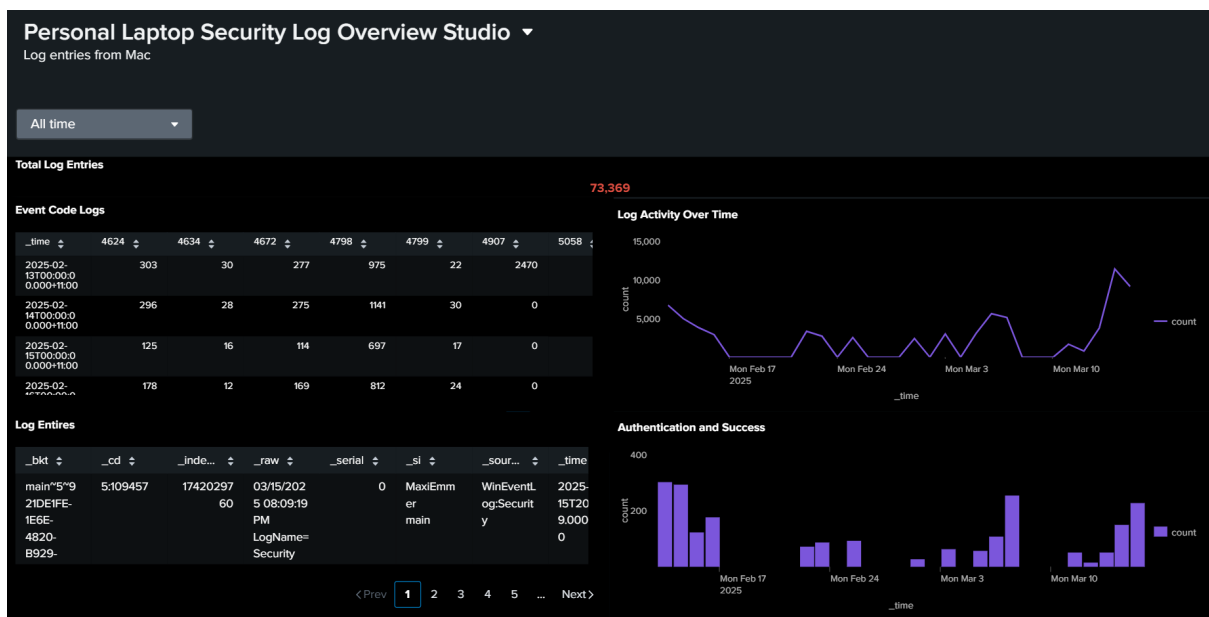
3. Security Event Trends



The analysis of security event trends revealed the following observations:

- Successful and Privileged Logins remained stable but dropped significantly after February 16, warranting an investigation into possible system logging misconfigurations or policy changes.
- User Enumeration Events (4798) peaked on February 14, suggesting potential unauthorized reconnaissance or lateral movement attempts.
- The sudden decrease in total events after February 16 may indicate an issue with log collection, security monitoring, or system inactivity, which should be verified with additional log sources.

4. Recommendations



Based on the findings, the following security recommendations should be implemented to enhance log monitoring and threat detection:

a) Investigate the Logging Drop After February 16

- Verify whether logging misconfigurations, system outages, or retention policies caused the sudden decline in recorded security events.
- Conduct a cross-check with alternative log sources (firewall, endpoint monitoring, SIEM) to ensure continuous visibility.

b) Monitor User Enumeration Attempts (Event 4798)

- Establish real-time alerts to detect and mitigate potential reconnaissance or lateral movement attempts.
- Review logs for correlated suspicious activities, such as repeated failed login attempts or privilege escalation attempts.

c) Implement Alerts for Failed Logins (Event 4625)

- Configure threshold-based alerts for multiple failed login attempts within short timeframes to identify potential brute-force or credential-stuffing attacks.

- Analyze trends in failed authentication attempts to determine if they originate from legitimate users or unauthorized actors.

d) Ensure Comprehensive Log Coverage

- Verify that all critical security events are being captured, including privilege escalation, group membership changes, and suspicious logins from external locations.
- Conduct log integrity checks to prevent data loss due to retention policies or storage limitations.

This security event analysis provides valuable insights into authentication patterns, privilege access activities, and potential security risks. By implementing the recommended monitoring enhancements, alert configurations, and log integrity checks, we can strengthen the organization's security posture and incident response capabilities.

5. Conclusion

This security event analysis provides a comprehensive overview of authentication activities, privilege access events, and potential security threats. Key findings indicate a significant drop in logging after February 16, a peak in user enumeration attempts on February 14, and stable yet notable privileged login activities.

To mitigate risks and enhance security monitoring, we recommend investigating logging gaps, implementing real-time alerts for failed logins and reconnaissance attempts, and ensuring continuous log coverage. Strengthening log integrity and alerting mechanisms will enable proactive threat detection and a more resilient security posture.

By acting on these insights, security teams can improve incident response, reduce the risk of unauthorized access, and enhance overall cybersecurity resilience.