Name: Temitope C Folowosele

Title: Splunk Project

Date: 11/26/2025

Introduction

This project examines Windows Event Logs in Splunk to review patterns linked to successful login activities (Event Code 4624). It highlights how Splunk searches and dashboards support visibility into authentication events and strengthen security monitoring.

Objectives

To apply Splunk to search, filter, and analyze Windows security logs.

To identify the pattern and frequency of successful logon attempts.

To create visual insights like timecharts and bar visualizations for easy interpretation.

To improve understanding of user authentication behavior within the environment.

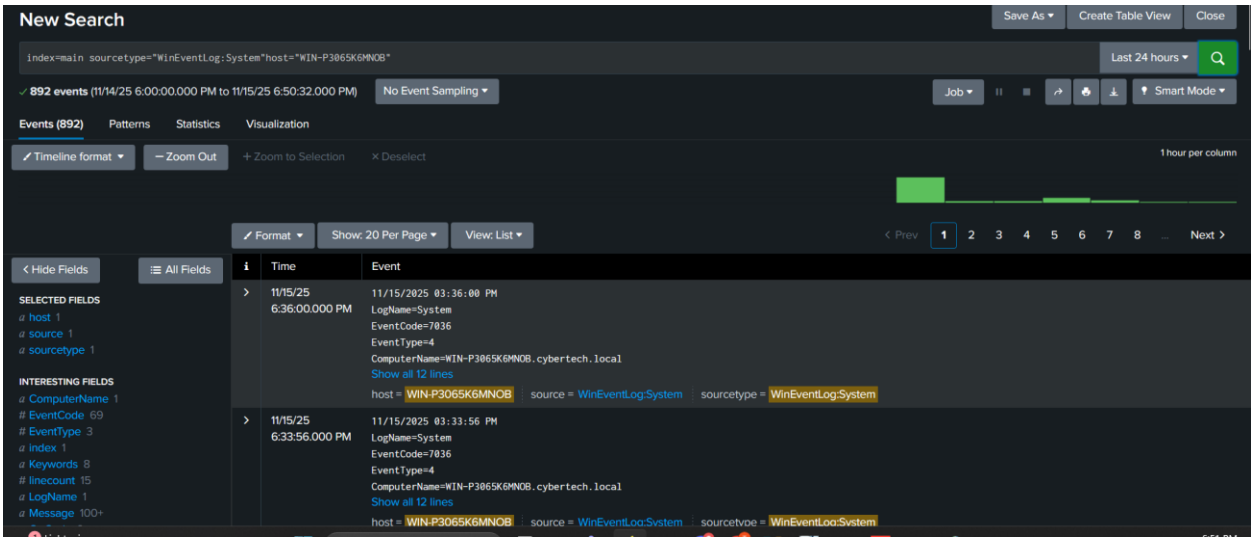
Goal

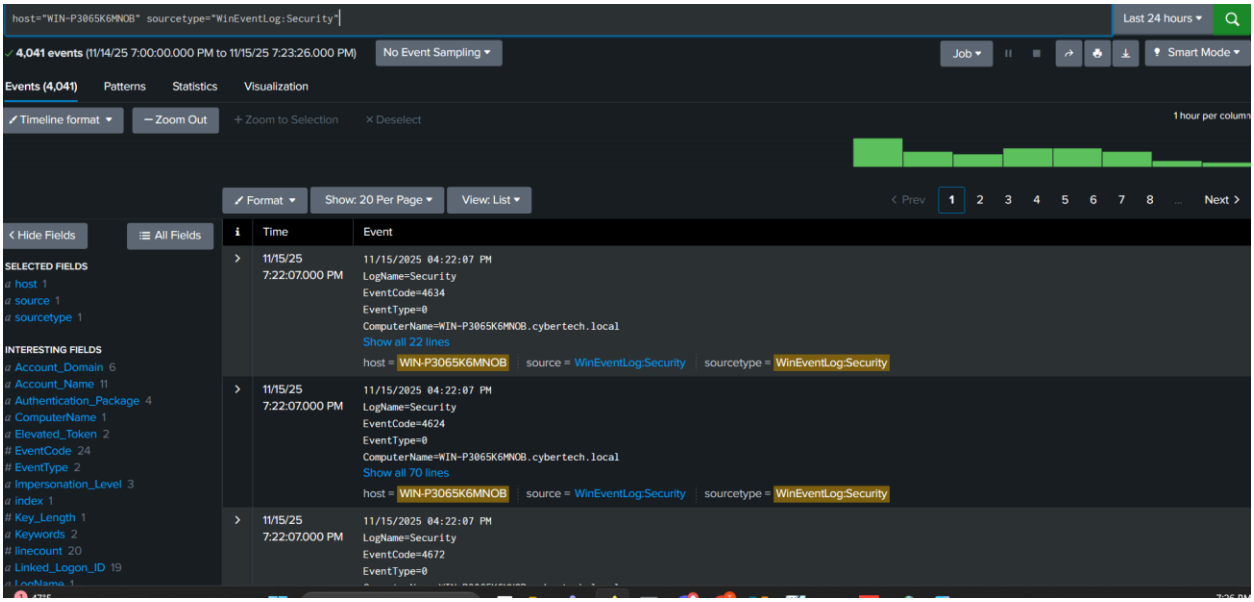
The goal is to use Splunk as a SIEM tool to gain clear insight into login events, detect unusual behavior, and support security operations by monitoring authentication activity.

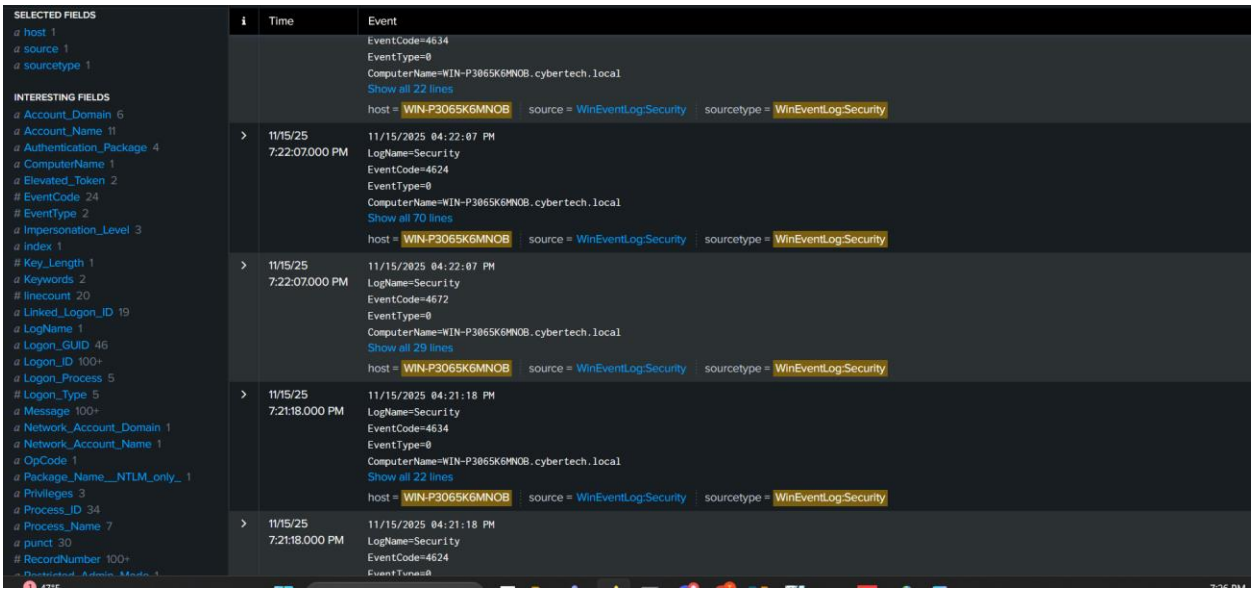
Data Ingestion

Windows security logs were ingested into Splunk for review.

Purpose: Provides the raw event data required for analysis.



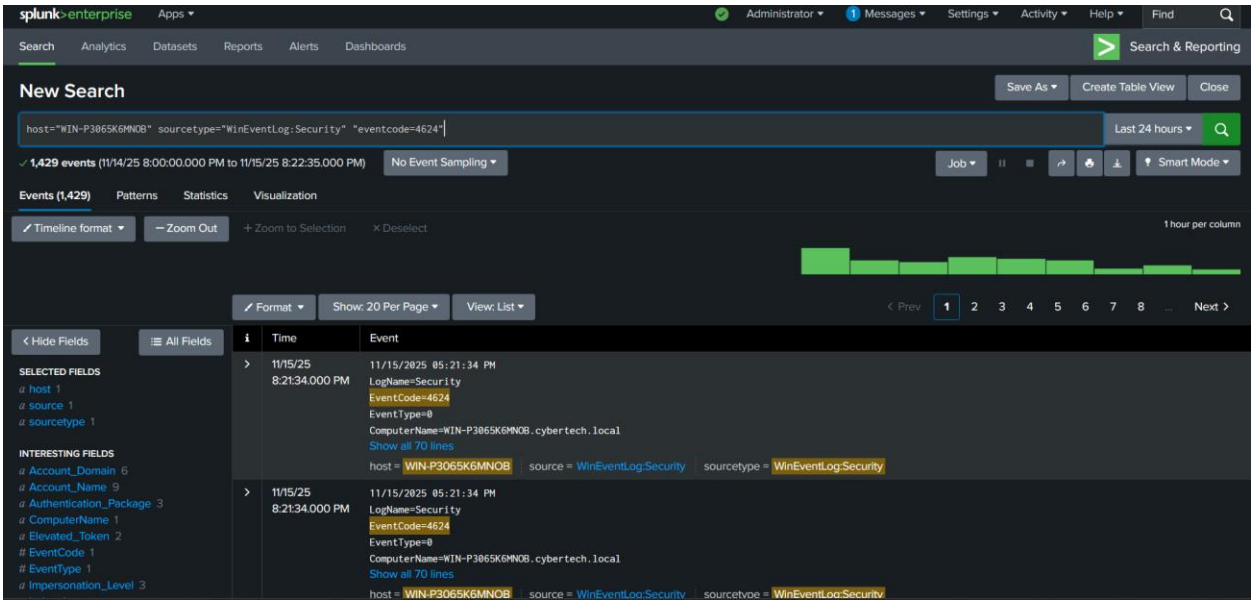


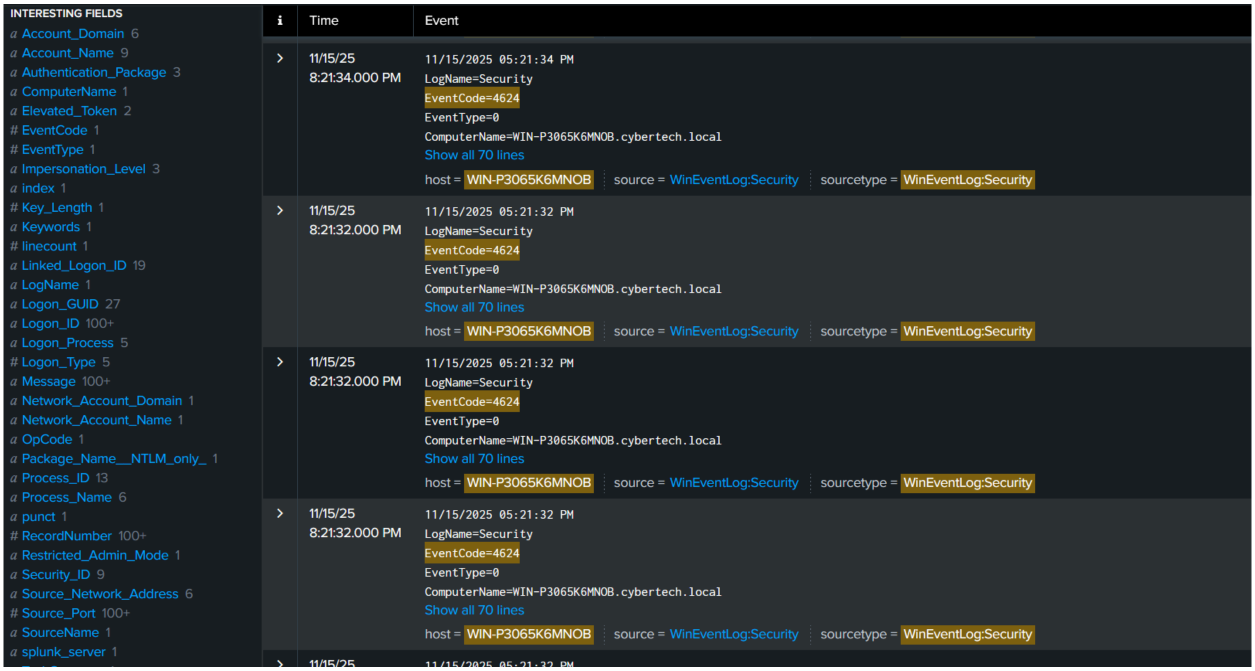


Using Search Query

A Splunk query was executed for EventCode = 4624.

Purpose: Isolates all successful logon events from the collected logs.

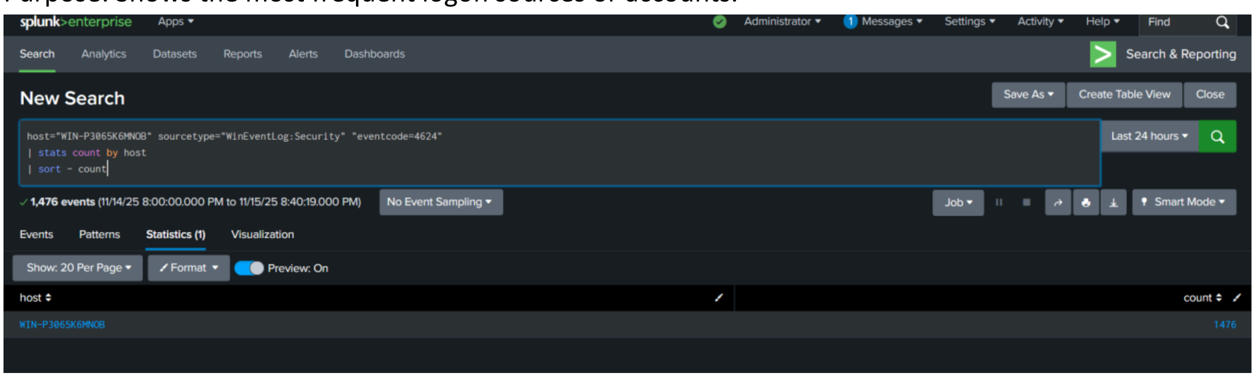


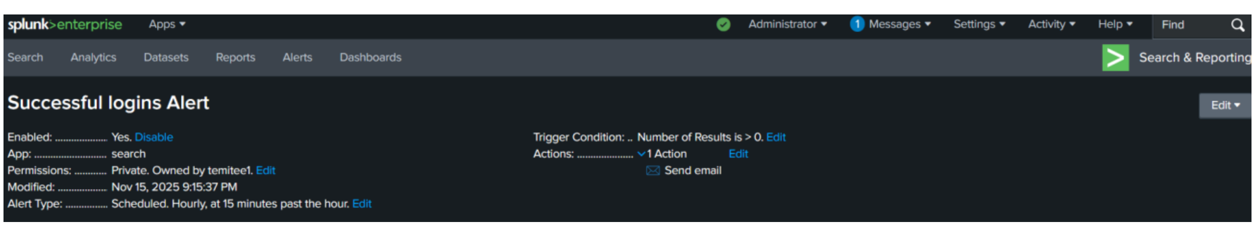


Sorting by Count

Events were organized according to their count.

Purpose: Shows the most frequent logon sources or accounts.

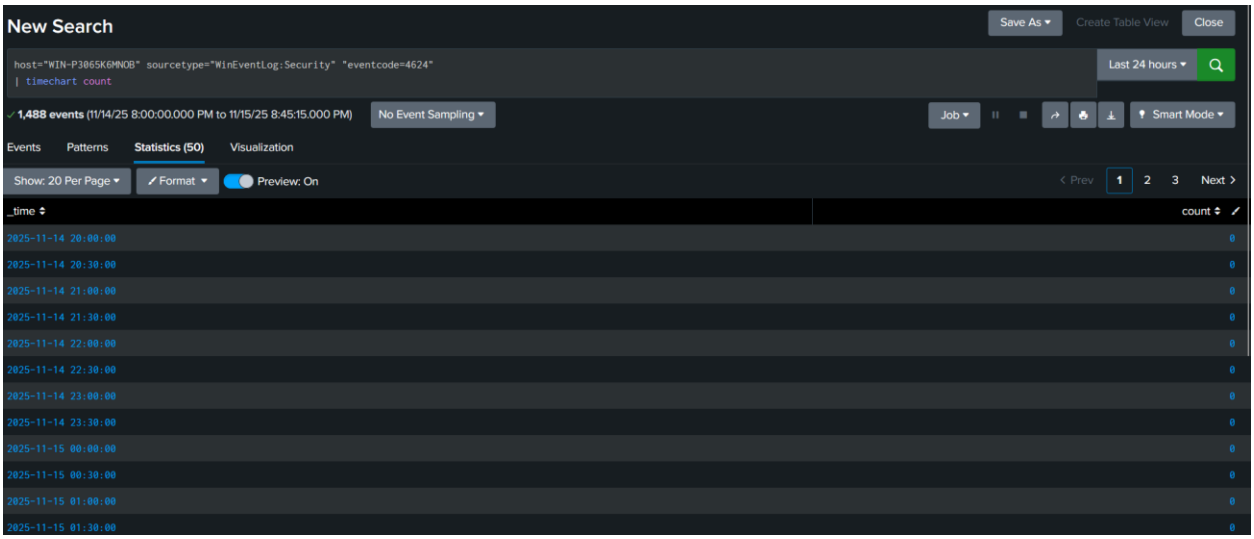




Dashboard Creation

The results were added to a dashboard for continuous observation.

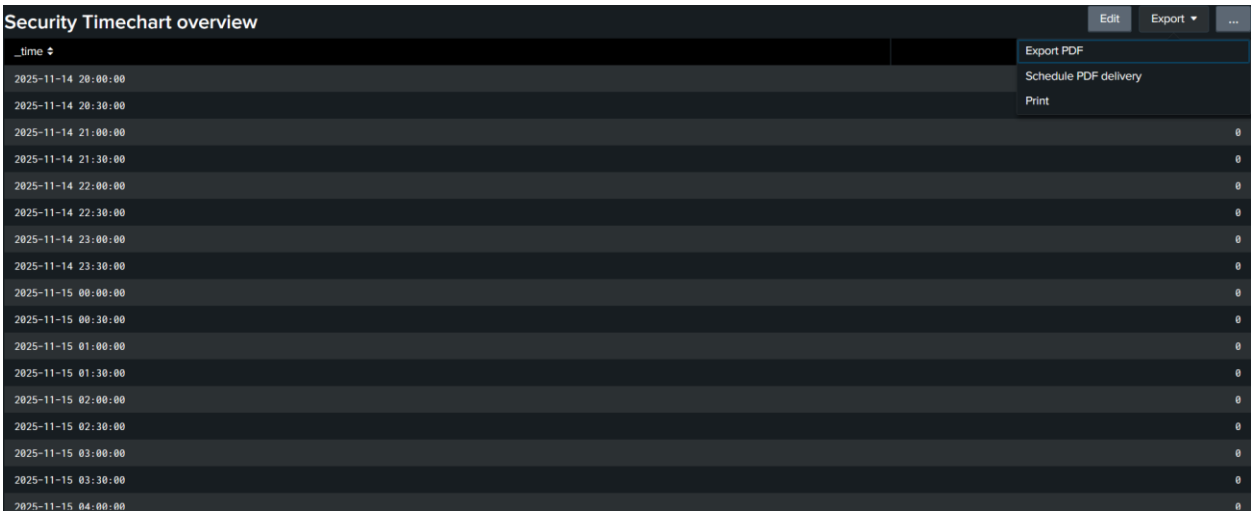
Purpose: Enables easy reporting and real-time monitoring.



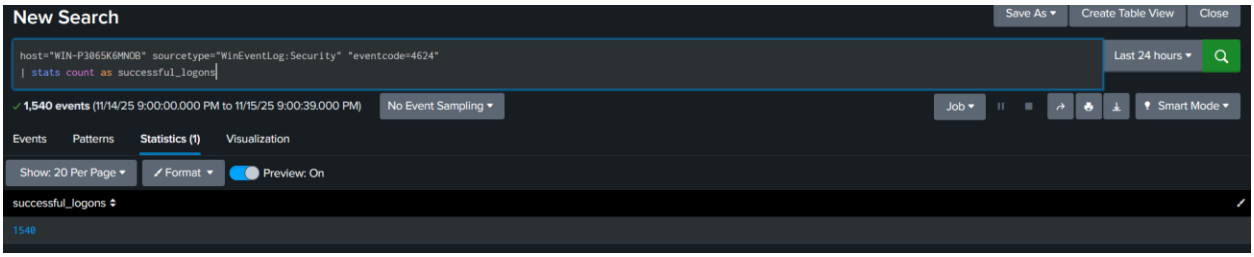
Visualization – Timechart

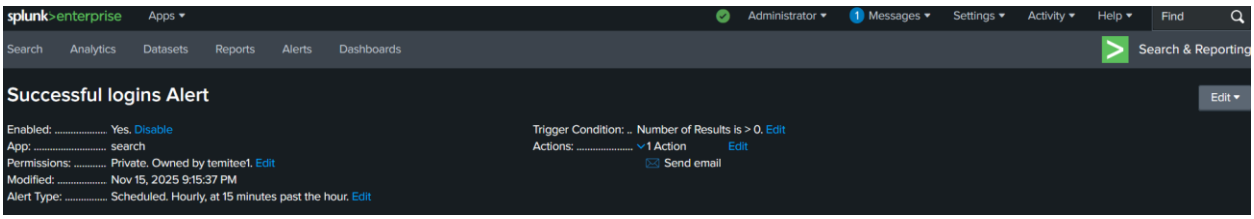
A timechart visualization was generated to display logon activity across time.

Purpose: Helps reveal spikes or abnormal login behavior.



Successful logons-1540





Recommendation

Maintain ongoing monitoring of 4624 and related login event codes to detect unusual patterns.

Set up alerts for irregular login times, repeated failed attempts, or suspicious accounts.

Review authentication trends frequently to enhance incident response and improve access controls.

Conclusion

This project shows how Splunk efficiently analyzes Windows authentication logs. By reviewing and visualizing successful logons, organizations can enhance visibility, detect threats earlier, and reinforce their overall security monitoring capabilities.