

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.

New Search Save As Create Table View Close

index=main sourcetype="WinEventLog:System" host="WIN-P3065K6MNOB" Last 24 hours Q

✓ 892 events (11/14/25 6:00:00.000 PM to 11/15/25 6:50:32.000 PM) No Event Sampling Job || ↶ ↷ ⬇ ⬆ Smart Mode

Events (892) Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection X Deselect 1 hour per column

Format Show: 20 Per Page View: List < Prev 1 2 3 4 5 6 7 8 ... Next >

	i	Time	Event
	>	11/15/25 6:36:00.000 PM	11/15/2025 03:36:00 PM LogName=System EventCode=7036 EventType=4 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 12 lines host = WIN-P3065K6MNOB source = WinEventLog:System sourcetype = WinEventLog:System
	>	11/15/25 6:33:56.000 PM	11/15/2025 03:33:56 PM LogName=System EventCode=7036 EventType=4 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 12 lines host = WIN-P3065K6MNOB source = WinEventLog:System sourcetype = WinEventLog:System

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a ComputerName 1
EventCode 69
EventType 3
a index 1
a Keywords 8
Linecount 15
a LogName 1
a Message 100+

host="WIN-P3065K6MNOB" sourcetype="WinEventLog:Security" Last 24 hours Q

✓ 4,041 events (11/14/25 7:00:00.000 PM to 11/15/25 7:23:26.000 PM) No Event Sampling Job || ↶ ↷ ⬇ ⬆ Smart Mode

Events (4,041) Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection X Deselect 1 hour per column

Format Show: 20 Per Page View: List < Prev 1 2 3 4 5 6 7 8 ... Next >

	i	Time	Event
	>	11/15/25 7:22:07.000 PM	11/15/2025 04:22:07 PM LogName=Security EventCode=4634 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 22 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	11/15/25 7:22:07.000 PM	11/15/2025 04:22:07 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 70 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	11/15/25 7:22:07.000 PM	11/15/2025 04:22:07 PM LogName=Security EventCode=4672 EventType=0

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 6
a Account_Name 11
a Authentication_Package 4
a ComputerName 1
a Elevated-Token 2
EventCode 24
a Impersonation_Level 3
a index 1
Key_Length 1
a Keywords 2
Linecount 20
a Linked_Logon_ID 19
a LogName 1

SELECTED FIELDS	i	Time	Event
# host 1 # source 1 # sourcetype 1 # Account_Domain 6 # Account_Name 11 # Authentication_Package 4 # ComputerName 1 # Elevated_Token 2 # EventCode 24 # EventType 2 # Impersonation_Level 3 # Index 1 # Key_Length 1 # Keywords 2 # Linecount 20 # Linked_Logon_ID 19 # LogName 1 # Logon_GUID 46 # Logon_ID 100+ # Logon_Process 5 # Logon_Type 5 # Message 100+ # Network_Account_Domain 1 # Network_Account_Name 1 # OpCode 1 # Package_Name__NTLM_only_ 1 # Privileges 3 # Process_ID 34 # Process_Name 7 # punct 30 # RecordNumber 100+ # ...			EventCode=4634 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 22 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	11/15/25 7:22:07.000 PM	11/15/2025 04:22:07 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 70 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	11/15/25 7:22:07.000 PM	11/15/2025 04:22:07 PM LogName=Security EventCode=4672 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 29 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	11/15/25 7:21:18.000 PM	11/15/2025 04:21:18 PM LogName=Security EventCode=4634 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 22 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	11/15/25 7:21:18.000 PM	11/15/2025 04:21:18 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 70 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security

Using Search Query

A Splunk query was executed for EventCode = 4624.

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

splunk enterprise			
Search			
New Search			
host="WIN-P3065K6MNOB" sourcetype="WinEventLog:Security" "eventcode=4624"			
1,429 events (11/14/25 8:00:00.000 PM to 11/15/25 8:22:35.000 PM)			
Events (1,429) Patterns Statistics Visualization			
Timeline format Zoom Out Zoom to Selection Deselect			
Format Show: 20 Per Page View: List			
Time	Event		
11/15/25 8:21:34.000 PM	11/15/2025 05:21:34 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 70 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security		
11/15/25 8:21:34.000 PM	11/15/2025 05:21:34 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 70 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security		

INTERESTING FIELDS	i	Time	Event
Account_Domain 6 Account_Name 9 Authentication_Package 3 ComputerName 1 Elevated_Token 2 EventCode 1 EventType 1 Impersonation_Level 3 Index 1 Key_Length 1 Keywords 1 Linecount 1 Linked_Logon_ID 19 LogName 1 Logon_GUID 27 Logon_ID 100+ Logon_Process 5 Logon_Type 5 Message 100+ Network_Account_Domain 1 Network_Account_Name 1 OpCode 1 Package_Name__NTLM_only_ 1 Process_ID 13 Process_Name 6 punct 1 RecordNumber 100+ Restricted_Admin_Mode 1 Security_ID 9 Source_Network_Address 6 Source_Port 100+ SourceName 1 splunk_server 1	>	11/15/25 8:21:34.000 PM	11/15/2025 05:21:34 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 70 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	11/15/25 8:21:32.000 PM	11/15/2025 05:21:32 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 70 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	11/15/25 8:21:32.000 PM	11/15/2025 05:21:32 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 70 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	11/15/25 8:21:32.000 PM	11/15/2025 05:21:32 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MNOB.cybertech.local Show all 70 lines host = WIN-P3065K6MNOB source = WinEventLog:Security sourcetype = WinEventLog:Security

Sorting by Count

Events were organized according to their count.

Purpose: Shows the most frequent logon sources or accounts.

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

```
host="WIN-P3065K6MNOB" sourcetype="WinEventLog:Security" "eventcode=4624"
| stats count by host
| sort - count
```

Last 24 hours

✓ 1,476 events (11/14/25 8:00:00.000 PM to 11/15/25 8:40:19.000 PM) No Event Sampling Job

Events Patterns Statistics (1) Visualization

Show: 20 Per Page Format Preview: On

host	count
WIN-P3065K6MNOB	1476

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

Successful logins Alert

Edit

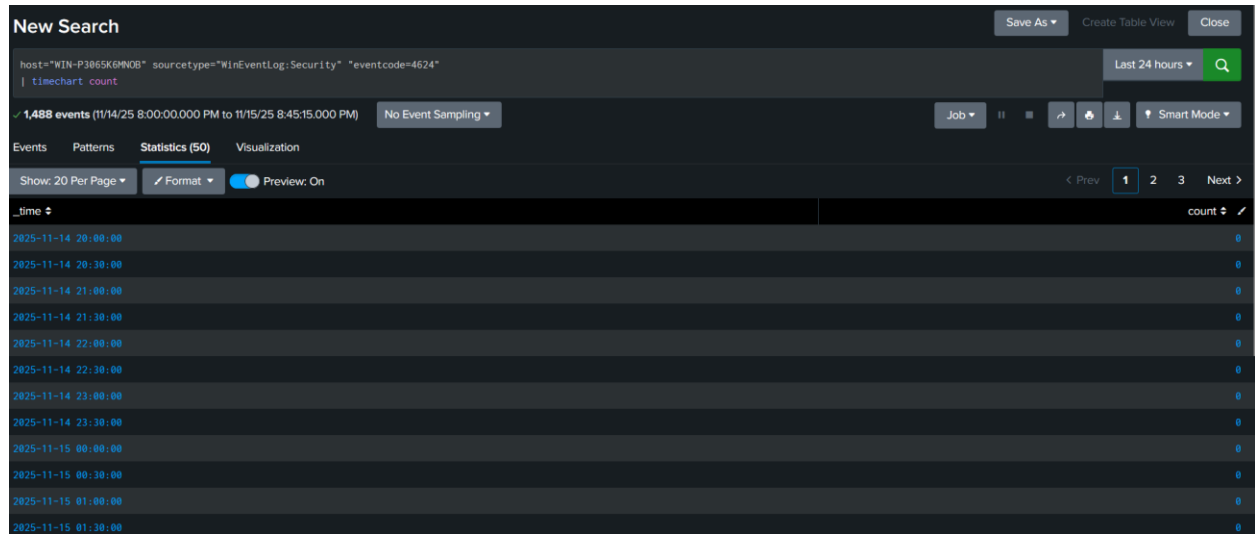
Enabled: Yes Disable
 App: search
 Permissions: Private. Owned by temitee1. Edit
 Modified: Nov 15, 2025 9:15:37 PM
 Alert Type: Scheduled. Hourly, at 15 minutes past the hour. Edit

Trigger Condition: Number of Results is > 0. Edit
 Actions: 1 Action Edit
 Send email

Dashboard Creation

The results were added to a dashboard for continuous observation.

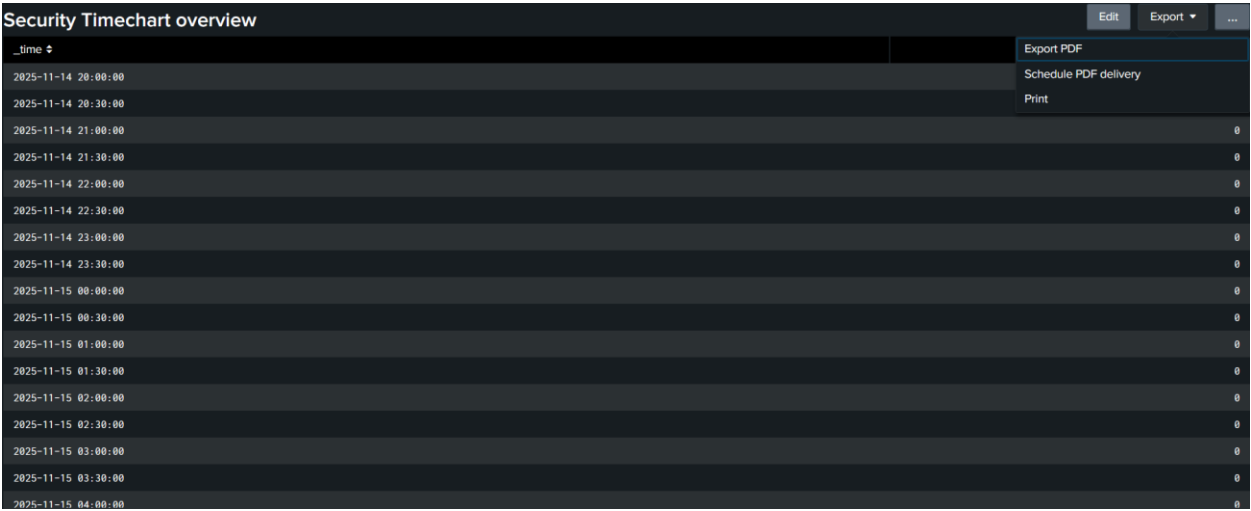
Purpose: Enables easy reporting and real-time monitoring.



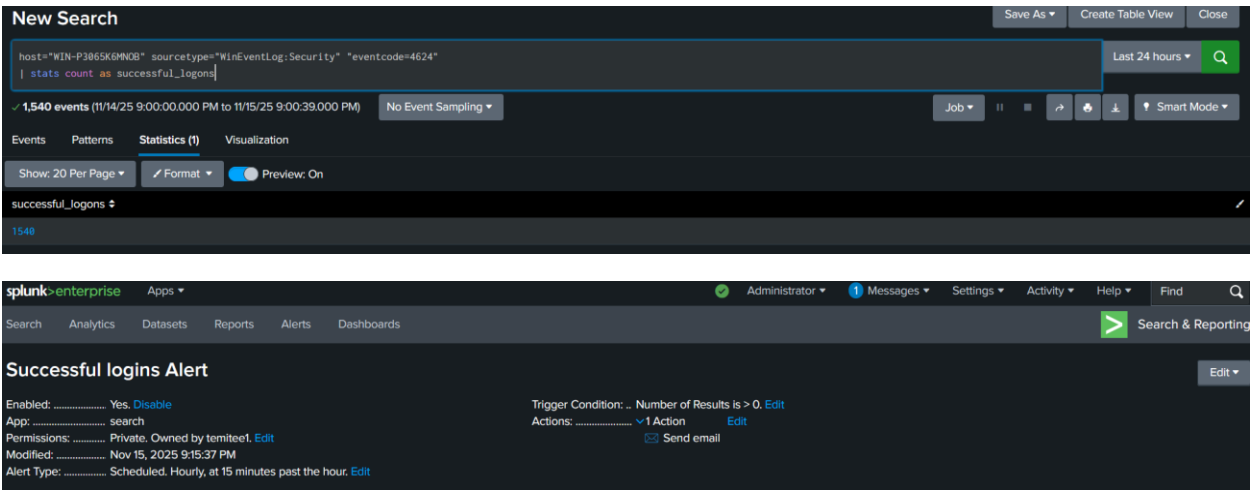
Visualization – Timechart

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.