

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

index=main sourcetype="WinEventLog:System" host="WIN-P3065K6MNOB"

892 events (11/14/25 6:00:00.000 PM to 11/15/25 6:50:32.000 PM) No Event Sampling

Last 24 hours

Events (892) Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection Deselect

Format Show: 20 Per Page View: List

1 2 3 4 5 6 7 8 ... Next

INTERESTING FIELDS

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
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

SELECTED FIELDS

All Fields

host source sourcetype

INTERESTING FIELDS

ComputerName EventCode EventType Index Keywords LineCount LogName Message

host source sourcetype

host="WIN-P3065K6MNOB" sourcetype="WinEventLog:Security"

4,041 events (11/14/25 7:00:00.000 PM to 11/15/25 7:23:26.000 PM) No Event Sampling

Last 24 hours

Events (4,041) Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection Deselect

Format Show: 20 Per Page View: List

1 2 3 4 5 6 7 8 ... Next

INTERESTING FIELDS

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
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
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

SELECTED FIELDS

All Fields

host source sourcetype

INTERESTING FIELDS

Account_Domain Account_Name Authentication_Package ComputerName Elevated_Token EventCode EventType Impersonation_Level Index Key_Length Keywords LineCount Linked_Logon_ID LogName

host source sourcetype

SELECTED FIELDS	i	Time	Event
host 1 source 1 sourcetype 1			EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MN0B.cybertech.local Show all 22 lines
INTERESTING FIELDS	>	11/15/25 7:22:07:000 PM	host = WIN-P3065K6MN0B source = WinEventLog:Security sourcetype = WinEventLog:Security
# 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+ # sessionid_Authentication 1	>	11/15/2025 04:22:07 PM 7:22:07:000 PM	LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MN0B.cybertech.local Show all 70 lines
	>	11/15/25 7:22:07:000 PM	host = WIN-P3065K6MN0B source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	11/15/25 7:21:18:000 PM	11/15/2025 04:22:07 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MN0B.cybertech.local Show all 22 lines
	>	11/15/25 7:21:18:000 PM	host = WIN-P3065K6MN0B 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 EventTime=0 EventTzOffset

Using Search Query

A Splunk query was executed for EventCode = 4624.

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

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `host="WIN-P3065K6MN0B" sourcetype="WinEventLog:Security" eventcode=4624`. The results panel displays 1429 events from November 14, 2025, to November 15, 2025. The interface includes a timeline chart at the bottom, search and reporting buttons, and various navigation and configuration options.

SELECTED FIELDS	i	Time	Event
host 1 source 1 sourcetype 1	>	11/15/25 8:21:34:000 PM	11/15/2025 05:21:34 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MN0B.cybertech.local Show all 70 lines
INTERESTING FIELDS	>	11/15/25 8:21:34:000 PM	host = WIN-P3065K6MN0B source = WinEventLog:Security sourcetype = WinEventLog:Security
# Account_Domain 6 # Account_Name 9 # Authentication_Package 3 # ComputerName 1 # Elevated_Token 2 # EventCode 1 # EventType 1 # Impersonation_Level 3	>	11/15/25 8:21:34:000 PM	11/15/2025 05:21:34 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-P3065K6MN0B.cybertech.local Show all 70 lines

INTERESTING FIELDS	i	Time	Event
a_Account_Domain 6 a_Account_Name 9 a_Authentication_Package 3 a_ComputerName 1 a_Elevated_Token 2 # EventCode 1 # EventType 1 a_Impersonation_Level 3 a_index 1 # Key_Length 1 a_Keywords 1 # linecount 1 a_Linked_Logon_ID 19 a_LogName 1 a_Logon_GUID 27 a_Logon_ID 100+ a_Logon_Process 5 # Logon_Type 5 a_Message 100+ a_Network_Account_Domain 1 a_Network_Account_Name 1 a_OpCode 1 a_Package_Name__NTLM_only_ 1 a_Process_ID 13 a_Process_Name 6 a_punct 1 # RecordNumber 100+ a_Restricted_Admin_Mode 1 a_Security_ID 9 a_Source_Network_Address 6 # Source_Port 100+ a_SourceName 1 a_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
	>	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	11/15/2025 05:21:32 PM

Sorting by Count

Events were organized according to their count.

Purpose: Shows the most frequent logon sources or accounts.

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** host="WIN-P3065K6MNOB" sourcetype="WinEventLog:Security" "eventcode=4624" | stats count by host | sort -count
- Results Summary:** 1,476 events (11/14/25 8:00:00:000 PM to 11/15/25 8:40:19:000 PM) | No Event Sampling
- Statistics Tab:** Selected. Shows 1,476 events over the specified time range.
- Results Table:** A table showing the count of events for each host. The top result is WIN-P3065K6MNOB with a count of 1476.

The screenshot shows the configuration for a successful logins alert:

- Enabled:** Yes. Disable
- App:** search
- Permissions:** Private. Owned by temiteel1. 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.

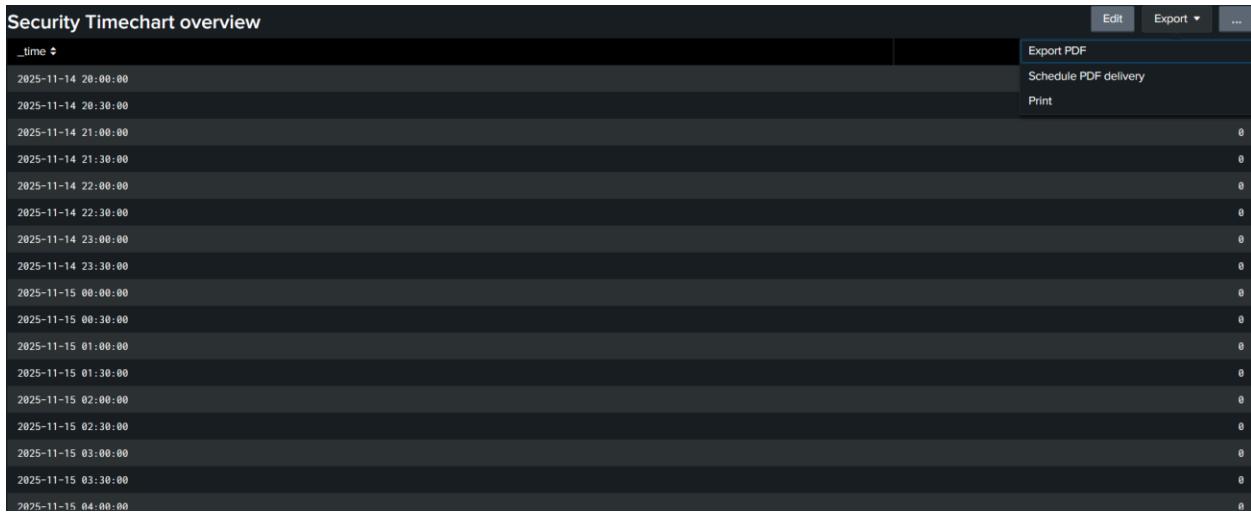
A screenshot of a Splunk search interface titled "New Search". The search bar contains the query: "host='WIN-P3065K6MN0B' sourcetype='WinEventLog:Security' eventcode=4624 | timechart count". The results show 1,488 events from November 14, 2025, to November 15, 2025. The "Statistics (50)" tab is selected. The table lists the time range and the count of events for each hour. The count is zero for all entries.

Time	Count
2025-11-14 20:00:00	0
2025-11-14 20:30:00	0
2025-11-14 21:00:00	0
2025-11-14 21:30:00	0
2025-11-14 22:00:00	0
2025-11-14 22:30:00	0
2025-11-14 23:00:00	0
2025-11-14 23:30:00	0
2025-11-15 00:00:00	0
2025-11-15 00:30:00	0
2025-11-15 01:00:00	0
2025-11-15 01:30:00	0

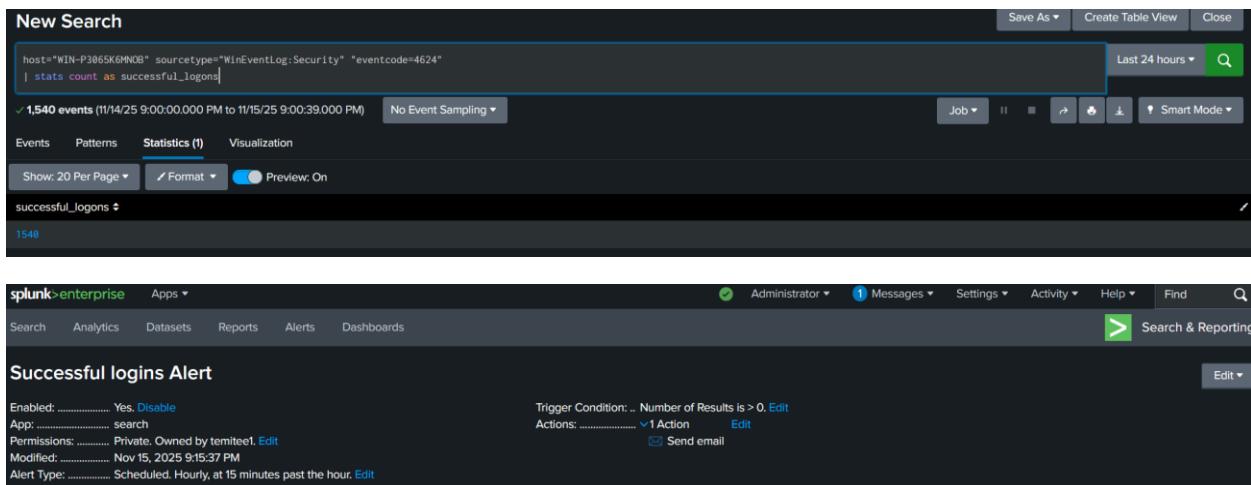
Visualization – Timechart

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.