

Splunk Alert Project: Security Event Analysis Report (Event Code 4624 - Successful Logon)

**Prepared by: Bamidele Olaleke
(Cybersecurity Analyst)**

Date: November 2025

Introduction

As part of my ongoing cybersecurity monitoring and log analysis practice, I analyzed Windows Security Event Code **4624**, which records successful logon activities. Leveraging my experience as a Cybersecurity Analyst, this report reflects a personalized and practical breakdown based on real-world environments I work with, including Windows Server monitoring and SIEM event correlation. Event Code **4624** is generated when an account logs on successfully to a Windows system. Monitoring this event is crucial in security operations as it helps analysts validate legitimate access, detect suspicious authentication behavior, and investigate potential unauthorized access that may appear normal. This report provides a professional breakdown of Event ID 4624, including its significance, fields of interest, security implications, and recommendations.

1. Project Overview

This project showcases the end-to-end process of generating and detecting a security alert in Splunk Enterprise by leveraging log data collected from a Windows Server through the Splunk Universal Forwarder. The alert is designed to identify patterns of successful logon activity (Event ID 4624), which can help security teams validate legitimate access, monitor authentication behavior, and detect potentially suspicious or unauthorized logon events..

2. Architecture & Setup

- Splunk Universal Forwarder installed on Windows Server.
- Splunk Enterprise installed on Host PC.
- Forwarder configured to send Windows Security logs to Splunk Enterprise.
- Data indexed under 'main' index with sourcetype 'WinEventLog:Security'.

3. Objective

Purpose of Monitoring Event Code 4624

From my security operations perspective, monitoring Event ID 4624 provides visibility into authentication behavior across systems I manage. This enables proactive threat detection and supports investigations related to unauthorized access, abnormal login times, and privilege escalation attempts. Event 4624 is useful for:

- Tracking successful authentication activities.
- Establishing baselines for normal user login patterns.
- Detecting logons occurring at unusual times or from unexpected sources.
- Investigating lateral movement and unauthorized access attempts.
- Supporting correlation in SIEM tools such as Splunk, ELK, and Microsoft Sentinel.

4. Splunk Search Query

The following SPL query was used to detect successful login attempts:

**index=main sourcetype=WinEventLog:Security
EventCode=4624
| stats count by Account_Name=CYBERTECH, Logon_Type,
Source_Network_Address**

index=main sourcetype=WinEventLog:Security EventCode=4624
| stats count by Account_Name, Logon_Type, Source_Network_Address

✓ 114 events (11/30/25 10:00:00.000 PM to 12/1/25 10:49:20.000 PM) No Event Sampling ▾ Job ▾ Last 24 hours ▾ Verbose Mode ▾

Events (114) Patterns Statistics (4) Visualization

✓ Timeline format ▾ - Zoom Out + Zoom to Selection × Deselect 1 hour per column

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

< Hide Fields	All Fields	i Time	Event
SELECTED FIELDS		> 12/1/25 10:42:07.000 PM	12/01/2025 10:42:07 PM LogName=Security EventCode=4624 EventType=0 ComputerName=CyberTech Show all 71 lines host = CYBERTECH source = WinEventLog:Security sourcetype = WinEventLog:Security
a host 1		> 12/1/25 10:42:06.000 PM	12/01/2025 10:42:06 PM LogName=Security EventCode=4624 EventType=0 ComputerName=CyberTech Show all 71 lines host = CYBERTECH source = WinEventLog:Security sourcetype = WinEventLog:Security
a source 1			
a sourcetype 1			
INTERESTING FIELDS			
a Account_Domain 3			
a Account_Name 3			
a Authentication_Package 1			
a ComputerName 1			
a Elevated_Token 2			
# EventCode 1			
# EventType 1			
a Impersonation_Level 1			
a index 1			

index=main sourcetype=WinEventLog:Security EventCode=4624
| stats count by Account_Name=CYBERTECH, Logon_Type, Source_Network_Address

✓ 114 events (11/30/25 10:00:00.000 PM to 12/1/25 10:49:20.000 PM) No Event Sampling ▾ Job ▾ Last 24 hours ▾ Verbose Mode ▾

Events (114) Patterns Statistics (4) Visualization

✓ Timeline format ▾ - Zoom Out + Zoom to Selection × Deselect 1 hour per column

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

< Hide Fields	All Fields	i Time	Event
SELECTED FIELDS		> 10:33:24.000 PM	10:33:24.000 PM LogName=Security EventCode=4624 EventType=0 ComputerName=CyberTech Show all 71 lines host = CYBERTECH source = WinEventLog:Security sourcetype = WinEventLog:Security
a Keywords 1		> 12/1/25 10:13:33.000 PM	12/01/2025 10:13:33 PM LogName=Security EventCode=4624 EventType=0 ComputerName=CyberTech Show all 71 lines host = CYBERTECH source = WinEventLog:Security sourcetype = WinEventLog:Security
# linecount 1		> 12/1/25 10:13:33.000 PM	12/01/2025 10:13:33 PM LogName=Security EventCode=4624 EventType=0 ComputerName=CyberTech Show all 71 lines host = CYBERTECH source = WinEventLog:Security sourcetype = WinEventLog:Security
a Linked_Logon_ID 7		> 12/1/25 10:13:28.000 PM	12/01/2025 10:13:28 PM LogName=Security EventCode=4624 EventType=0 ComputerName=CyberTech Show all 71 lines host = CYBERTECH source = WinEventLog:Security sourcetype = WinEventLog:Security
a LogName 1		> 12/1/25 10:01:03.000 PM	12/01/2025 10:01:03 PM LogName=Security EventCode=4624 EventType=0 ComputerName=CyberTech Show all 71 lines host = CYBERTECH source = WinEventLog:Security sourcetype = WinEventLog:Security
a Logon_GUID 1			
a Logon_ID 7			
a Logon_Process 2			
# Logon_Type 2			
a Message 7			
a Network_Account_Domain 1			
a Network_Account_Name 1			
a OpCode 1			
a Package_Name__NTLM_only_1			
a Process_ID 2			
a Process_Name 2			
a punct 1			
# RecordNumber 100+			
a Remote_Credential_Guard 1			
a Restricted_Admin_Mode 1			
a Security_ID 2			
a Source_Network_Address 2			
a Source_Port 2			
a SourceName 1			
a splunk_server 1			
a TaskCategory 1			
a Transited_Services 1			
a Type 1			
a Virtual_Account 1			
... 114 more ...			

5. Alert Configuration

Title: Successful Logins Alert

Type: Scheduled Alert (Every 10 minutes)

Time Range: Last 10 minutes

Trigger Condition: Number of results > 0

Trigger Actions: Send Email (Configured via SMTP in Splunk Settings)

The screenshot shows the 'Save As Alert' dialog box. The 'Rule' field contains 'Successful logon'. The 'Description' field is 'Optional'. Under 'Permissions', 'Private' is selected. The 'Alert type' is 'Scheduled'. The 'Run every week' dropdown is set to 'Run every week'. The 'On' dropdown shows 'Monday' and 'at' '6:00'. The 'Expires' field shows '10 minute(s)'. In the 'Trigger Conditions' section, 'Trigger alert when' is set to 'Number of Results' 'is greater than' '0'. At the bottom right are 'Cancel' and 'Save' buttons.

6. Simulating the Alert and TimeChart

Successful logins on the Windows Server using valid credentials generated multiple Event ID 4624 entries. These events were forwarded to Splunk via the Universal Forwarder and visualized using a timechart for monitoring and alert validation.

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with links for Apps, Search, Analytics, Datasets, Reports, Alerts, and Dashboards. On the right side of the header, there are links for Administrator, Messages, Settings, Activity, Help, and a Find bar. Below the header, a search bar says "Search & Reporting".

The main area displays an alert titled "Successful logon". The alert details are as follows:

- Enabled: Yes, Disable
- App: search
- Permissions: Private, Owned by bammycybertech. Edit
- Modified: Dec 2, 2025 12:41:49 AM
- Alert Type: Scheduled, Hourly, at 15 minutes past the hour. Edit

Trigger Condition: Number of Results is > 0. Edit
Actions: 1 Action Edit Add to Triggered Alerts

A message below states: "There are no fired events for this alert."

Below this, a "New Search" window is open. The search bar contains the query: "index=main sourcetype=WinEventLog:Security EventCode=4624 | timechart count by host". The search results show 119 events from Nov 30 to Dec 1, 2025, with a count of 0 for each event. The search results table has columns for _time and count, with 119 rows of data.

7. Validation & Output

The alert was successfully triggered after multiple successful login events were recorded during the monitoring period. It appeared in the *Triggered Alerts* section of Splunk, and an

email notification was generated, confirming that the alert was detected and processed correctly.

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for 'splunk>enterprise', 'Apps ▾', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search icon. Below the navigation is a secondary header with 'Search & Reporting' and a green 'Search' button.

The main content area displays two alert cards:

- Successful logon**: An alert card for a successful logon. It includes fields for 'Enabled' (Yes, Disable), 'App' (search), 'Permissions' (Private, Owned by bammmycybertech), 'Modified' (Dec 2, 2025 12:41:49 AM), and 'Alert Type' (Scheduled, Hourly, at 15 minutes past the hour). It also shows a trigger condition: 'Number of Results is > 0' and an action: '1 Action'. There's a note stating 'There are no fired events for this alert.'
- Successful login**: An alert card for a successful login. It includes the event code 4624. The table below lists three log entries:

i	Time	Event
>	12/2/25 1:10:10.000 AM	12/02/2025 01:10:10 AM LogName=Security EventCode=4624 EventType=0 ComputerName=CyberTech Show all 71 lines host = CYBERTECH source = WinEventLog:Security sourcetype = WinEventLog:Security
>	12/2/25 12:55:38.000 AM	12/02/2025 12:55:38 AM LogName=Security EventCode=4624 EventType=0 ComputerName=CyberTech Show all 71 lines host = CYBERTECH source = WinEventLog:Security sourcetype = WinEventLog:Security
>	12/2/25	12/02/2025 12:44:16 AM

6. Potential Security Concerns

Even though 4624 indicates success, it can be associated with suspicious activity:

- Successful logons after many failed attempts.

- Logons outside business hours.
- Privileged accounts logging in interactively.
- RDP logons from unknown or external IP addresses.
- Service accounts used with unexpected logon types.

7. Recommendations

- **Enable correlation alerts** combining 4624 and 4625 events.
- **Monitor privileged accounts**
- **Whitelist known service accounts** to reduce noise.
- **Alert on foreign or unusual IP addresses.**
- **Track repeated logon activity** from the same source.
- **Use multi-factor authentication (MFA)** to reduce misuse of credentials.

8. Conclusion

This project demonstrates the practical use of Splunk for real-time log monitoring and alerting. Event Code 4624 is a vital telemetry source for identifying valid and suspicious logons. When incorporated into a security monitoring strategy, it enables organizations to detect credential misuse, lateral movement, and unauthorized access attempts. Proper analysis strengthens the overall security posture and enhances incident investigation capabilities.