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

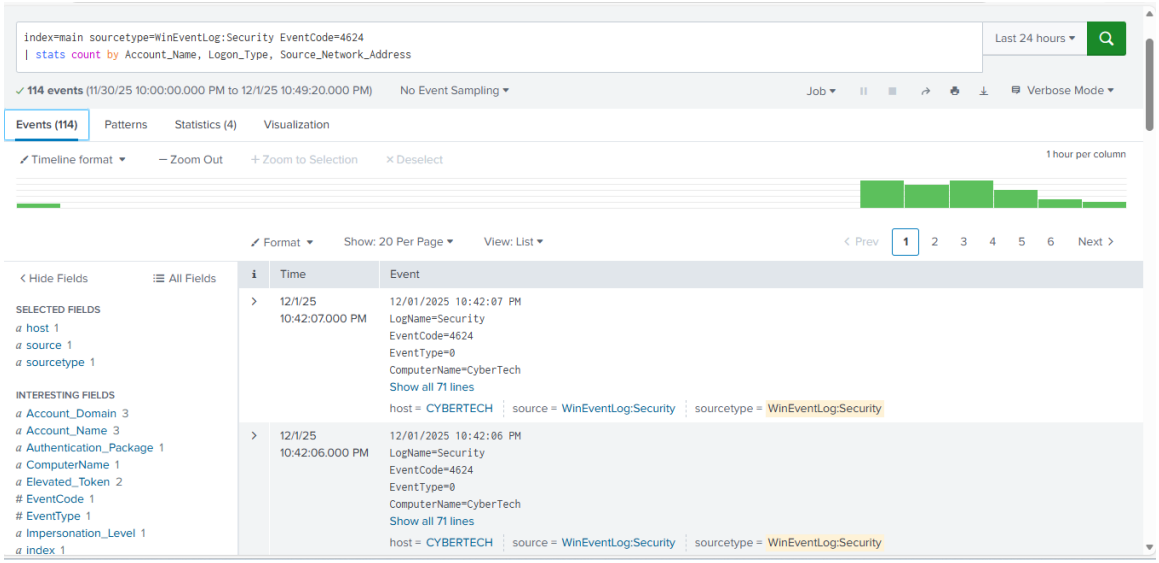
From my security operations perspective, monitoring Event ID 4624 provides visibility into authentication behavior across systems I manage. This enables proactive threat detection and supports investigations related to unauthorized access, abnormal login times, and privilege escalation attempts. Event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

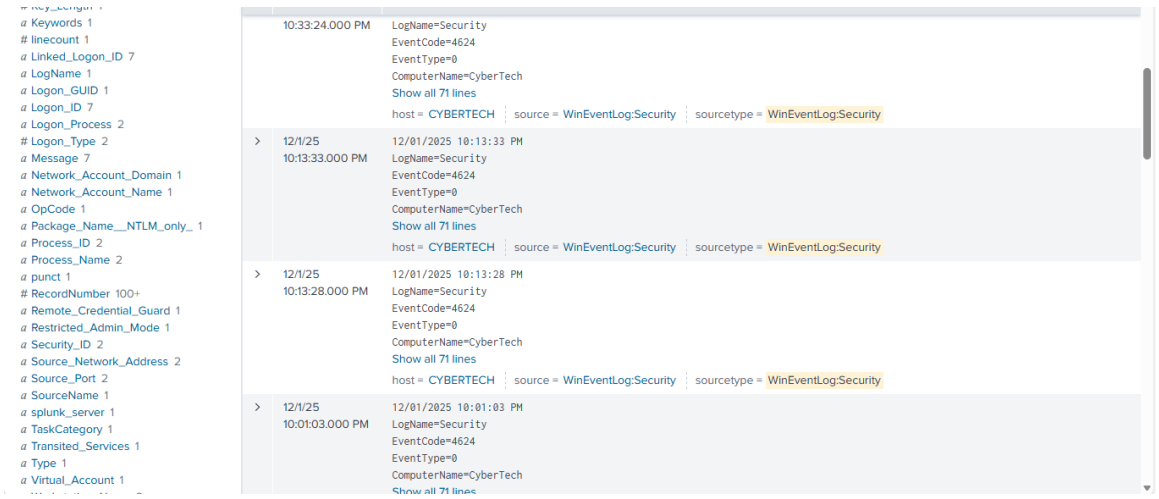
- Tracking successful authentication activities.
- Establishing baselines for normal user login patterns.
- Detecting logons occurring at unusual times or from unexpected sources.
- Investigating lateral movement and unauthorized access attempts.
- Supporting correlation in SIEM tools such as Splunk,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





5. Alert Configuration

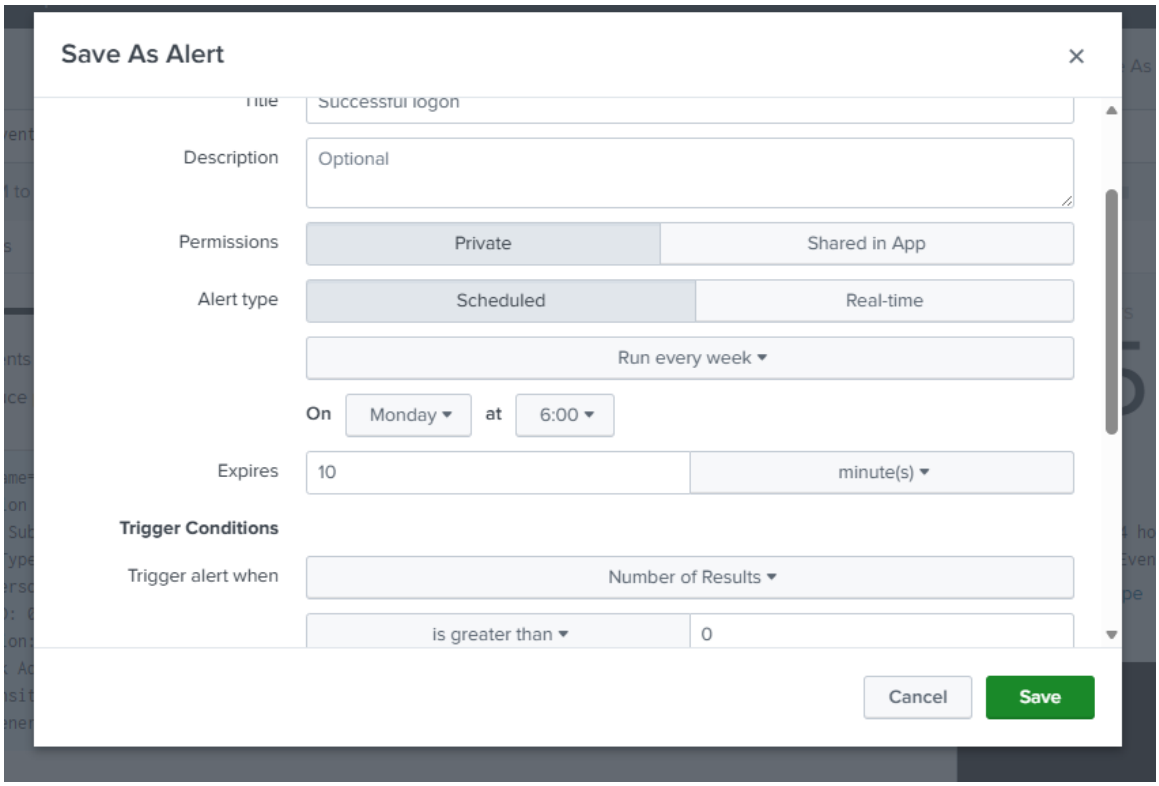
Title: Successful Logins Alert

Type: Scheduled Alert (Every 10 minutes)

Time Range: Last 10 minutes

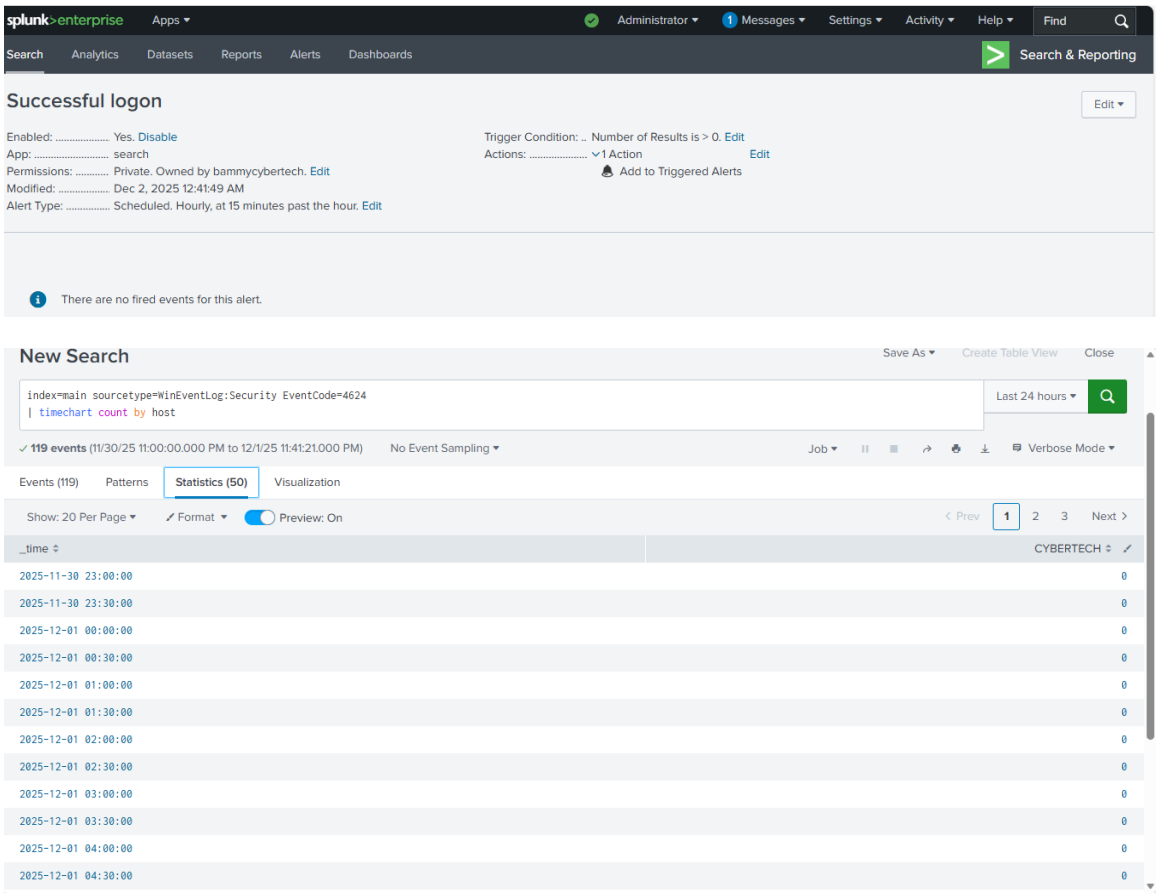
Trigger Condition: Number of results > 0

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



6. Simulating the Alert and TimeChart

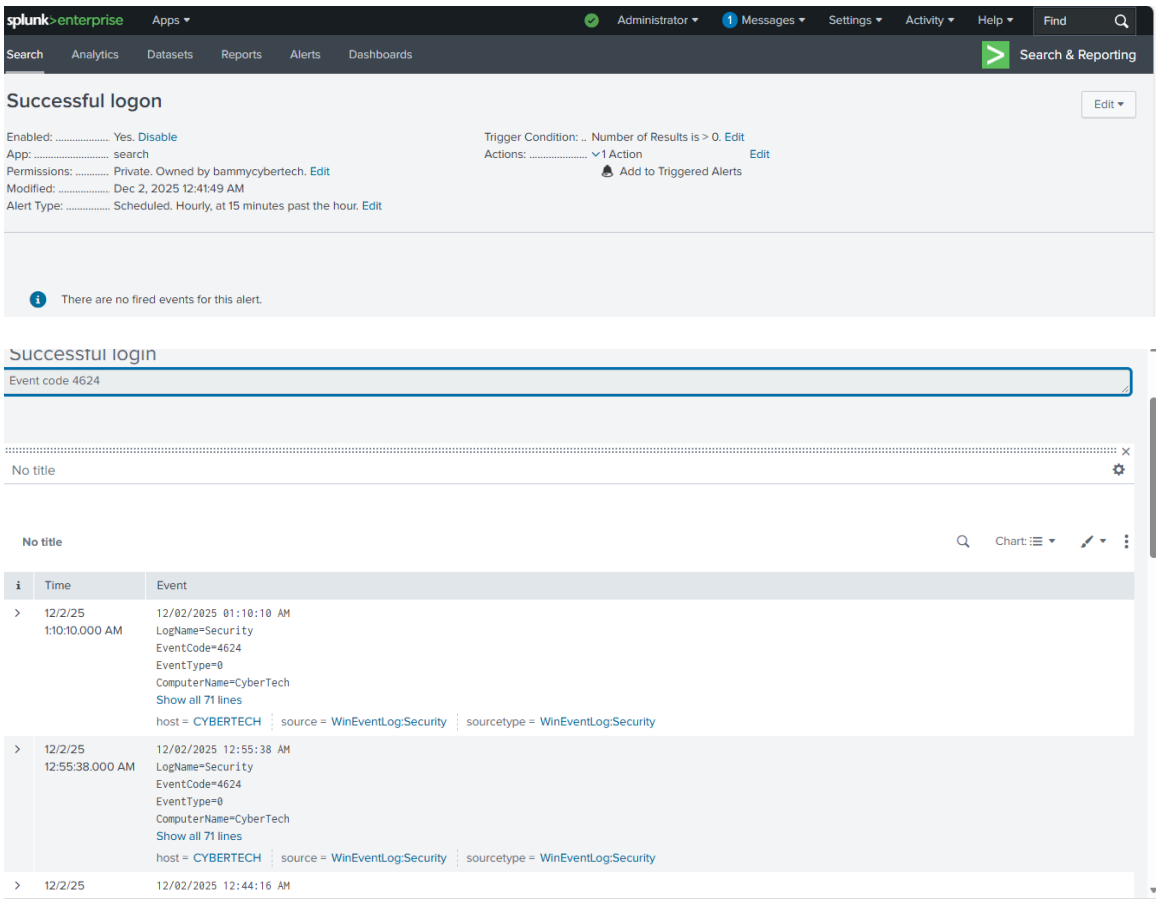
Successful logins on the Windows Server using valid credentials generated multiple Event ID 4624 entries. These events were forwarded to Splunk via the Universal Forwarder and visualized using a timechart for monitoring and alert validation.



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.



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.