Splunk Alert Project: Security Event Type Analysis Report

(Successful Logon on Windows Server 2022 – Event Code - 4624)

Prepared by: Dada Ojuko

(Cybersecurity Analyst)

Date: December 2025

1. Introduction

This report provides a summarized assessment of the monitoring and analysis of **Windows Security Event Code 4624**, which indicates a successful logon. Because this event is one of the most frequently generated security logs in Windows environments, analysing it is essential for detecting unauthorized access, account misuse, lateral movement, and early indicators of compromise (IOC). Leveraging **Splunk** as the SIEM platform enables real-time alerting, correlation, and visibility across authentication activities within the Windows Server 2022 environment.

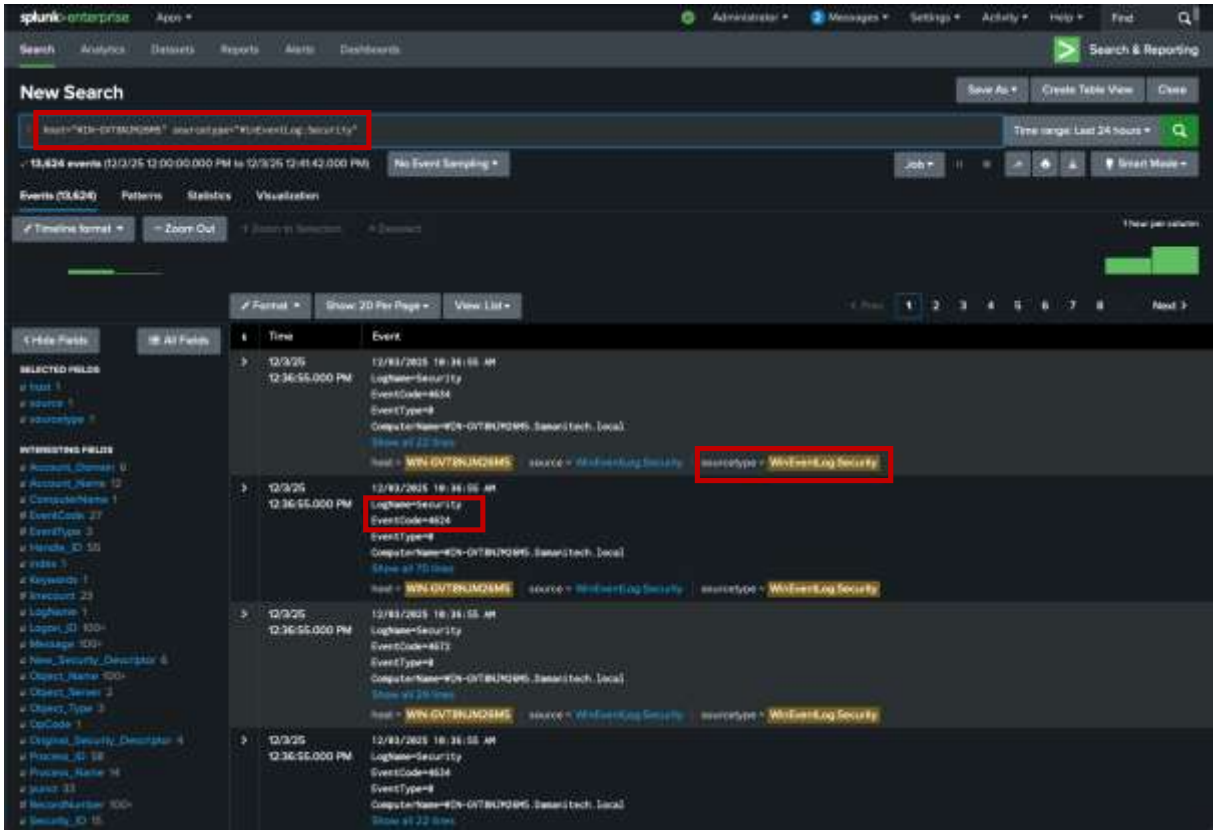
2. Project Overview

The project focuses on designing and implementing a Splunk-based detection and alerting workflow for Event Code 4624. The setup includes ingesting Windows security logs, parsing authentication fields, categorizing logon types (such as interactive, remote, network, and service logons), and establishing alert thresholds based on baseline user behaviour.

This project enhances the organization's ability to quickly identify suspicious logon patterns, such as unusual login hours, logons from abnormal hosts, high-volume login attempts, or logons involving privileged accounts.

3. Architecture and Setup

- **Data Sources:** Windows Server 2022 hosts sending Security Event Logs via WinEventLog/Forwarded Events.
- Splunk Enterprise installed on Host PC.
- **Forwarding Mechanism:** Windows Event Forwarding (WEF) or Universal Forwarder for log collection.
- Data indexed under 'main' index with sourcetype 'WinEventLog:Security'.



4. Objective

The core objective of this project is to improve authentication visibility and strengthen threat detection by analysing **Event Code 4624** within Splunk. This includes:

- ❖ Establishing a reliable log ingestion and parsing workflow.
- ❖ Identifying baseline logon behaviour for all users and systems.
- ❖ Detecting anomalies or indicators of suspicious activity.
- ❖ Providing actionable alerts for security operations teams.
- ❖ Enhancing situational awareness and supporting incident response.

Overall, the project aims to ensure timely identification of unauthorized or risky logon activity, helping maintain a secure and compliant Windows server environment.

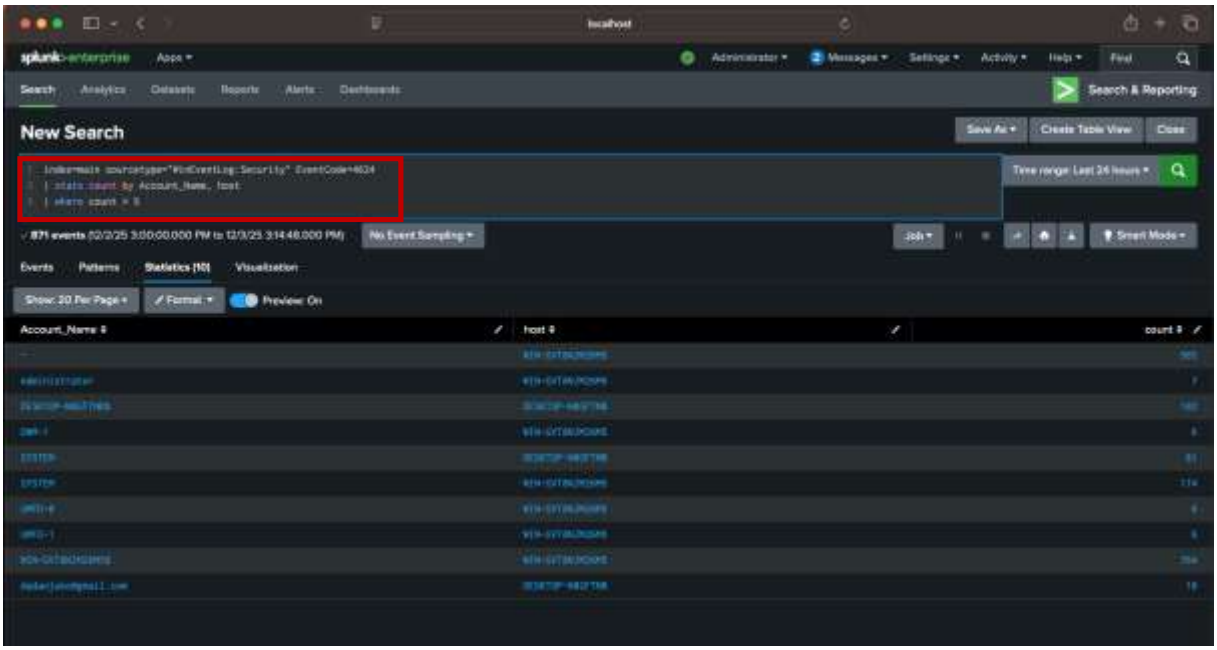
5. Splunk Search Query

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

index=main sourcetype=WinEventLog:Security EventCode=4624

| stats count by Account_Name, host

| where count > 5

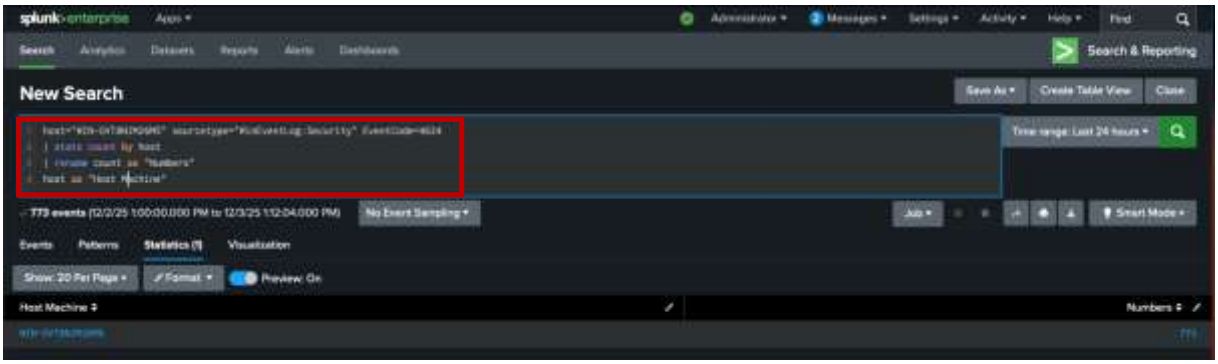


index=main sourcetype=WinEventLog:Security EventCode=4624

| stats count by host

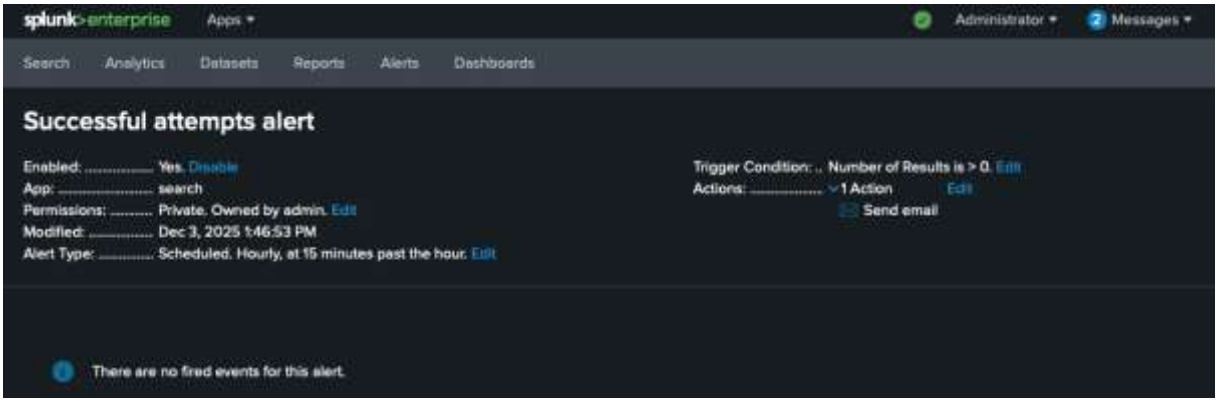
| rename count as ''Numbers''

host as ''Host Machine''



6. Configuring Alert

- Title: Successful Logon overview alert.
- Time Range: Last 15 minutes.
- Trigger Conditions: Number of results > 0.
- Trigger Actions: Send Email (Configured via SMTP in Splunk settings).

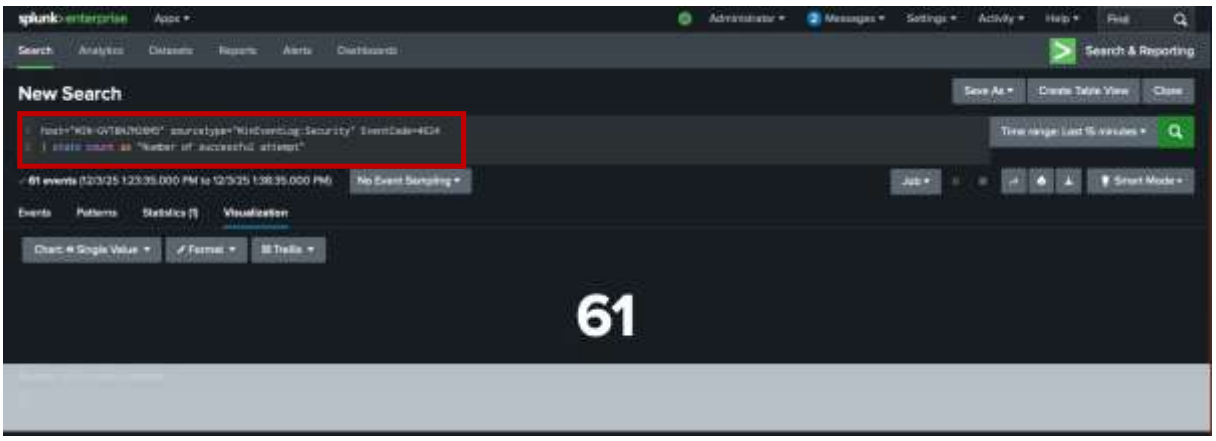


7. Simulating the Alert

Simulating an alert involves creating controlled conditions that trigger a predefined Splunk detection to verify that the alert logic, configurations, and response workflows function as expected. This process ensures that the alert is accurately tuned, effectively monitored, and operational before being deployed into a production environment.

The simulation typically includes generating specific log events—such as Windows Security **Event Code 4624 (Successful Logon)**—using test accounts, scheduled scripts, or controlled authentication attempts. These events were forwarded into Splunk through the Universal Forwarder. Once the logs appear, the correlation alert query is executed to confirm that Splunk correctly identifies the trigger input.

index=main sourcetype=WinEventLog:Security EventCode=4624
| stats count as ''Number of successful attempt''



8. Validation and Output

The alert triggered successfully after several successful login events were logged during the monitoring report. It appeared in the Triggered Alerts section in Splunk, an email notification was sent out which confirmed that the alert was detected and rightly processed.

9. Conclusion

Event Code 4624, which records successful logon activity in Windows environments, is one of the most valuable and frequently generated authentication events for security monitoring. Although it represents legitimate access, its high volume and detailed fields make it a critical data source for detecting abnormal behaviour, privilege misuse, lateral movement, and early (IOC) indicators of compromise.

By effectively ingesting, parsing, and analysing this event within Splunk, organizations can gain enhanced visibility into user authentication patterns across their Windows Server infrastructure. When combined with baselining and alerting mechanisms, Event Code 4624 becomes a powerful tool for identifying anomalous login activity, validating account behaviour, and strengthening the organization’s overall security posture.

Ultimately, the consistent monitoring of Event Code 4624 contributes to proactive threat detection, improved incident response readiness, and the establishment of a more resilient authentication ecosystem.