

Splunk Alert Project: Detecting Failed Logins on

❖ **Designed by Jaytech enterprises**

➤ *Windows Server (2022)*

➤ **Project Overview**

Using Windows authentication logs obtained from a Windows server using the Splunk Universal Forwarder, this project shows how to create and initiate a security alert in Splunk Enterprise. The alert identifies a pattern that is frequently linked to brute-force assaults or illegal access attempts: several unsuccessful login attempts (Event ID 4625) followed by a successful login (Event ID 4624). This application demonstrates Splunk's capacity to provide proactive incident detection in Windows settings, correlate security events, and offer real-time monitoring.

➤ **Architecture & Setup**

- Windows Server has Splunk Universal Forwarder installed.
- The host PC has Splunk Enterprise installed.
- A forwarder set up to transport Splunk Enterprise Windows Security logs.
- Data with the source type "WinEventLog:Security" is indexed under the "main" index.

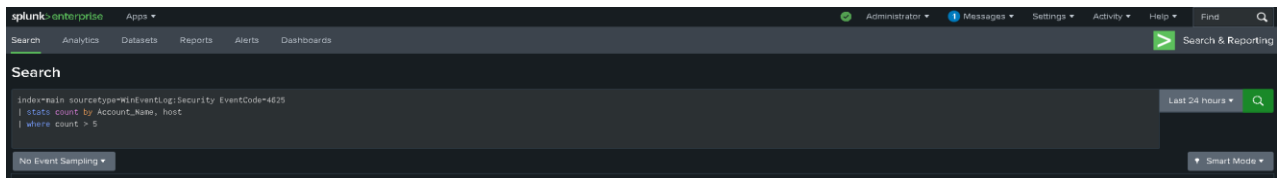
• **Objective**

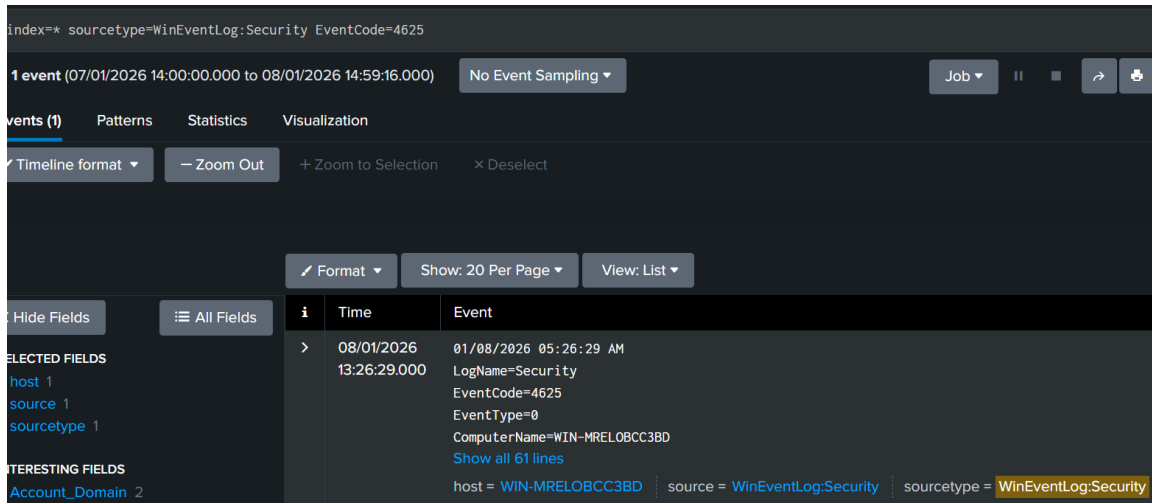
Trigger an alert when more than 5 failed login attempts (EventCode 4625) occur within a 10-minute window.

• **Splunk Search Query**

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

```
index=main sourcetype=WinEventLog:Security EventCode=4625  
/ stats count by Account_Name, host  
/ where count > 5
```





- **Alert Configuration**

- Title: Failed 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)

- **Simulating the Alert**

To simulate real-world conditions, failed login attempts were manually triggered on the Windows Server using the `runas` command with incorrect credentials. This ensured multiple Event ID 4625 logs were generated and forwarded to Splunk for processing.

- **Validation & Output**

The alert was successfully triggered after 6 failed login attempts. It appeared in the 'Triggered Alerts' section of Splunk and an email notification was received, confirming successful detection and response.

Edit Alert

Throttle ? ☐

Trigger Actions

+ Add Actions ▾

When triggered ▾

✉ Send email

Remove

To jayman@local.com

Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search. [Show CC and BCC](#)

Priority High ▾

Cancel

Save

index=* sourcetype=WinEventLog:Security EventCode=4625

1 event (07/01/2026 14:00:00.000 to 08/01/2026 14:59:16.000)

No Event Sampling ▾

Job ▾

▮

↗

📄

Events (1)

Patterns

Statistics

Visualization

Timeline format ▾

Zoom Out

+ Zoom to Selection

× Deselect

Format ▾

Show: 20 Per Page ▾

View: List ▾

Hide Fields

All Fields

	i	Time	Event
>		08/01/2026 13:26:29.000	<div>01/08/2026 05:26:29 AM</div> <div>LogName=Security</div> <div>EventCode=4625</div> <div>EventType=0</div> <div>ComputerName=WIN-MRELOBCC3BD</div> <div>Show all 61 lines</div>

SELECTED FIELDS

host 1

source 1

sourcetype 1

INTERESTING FIELDS

Account_Domain 2

host = WIN-MRELOBCC3BD

source = WinEventLog:Security

sourcetype = WinEventLog:Security

- ## Conclusion

This project shows how Splunk can be used practically for real-time log monitoring and alerting, allowing for continuous system activity visibility and the prompt identification of suspicious or security-related events.