Splunk Alert Project Report

Creating Splunk Alert
To Detect Failed Login Attempt
On A Windows Server

Prepared By:
Junaid AbdulRahman A
Cybersecurity Analyst

Date:23 November 2025

1. Project Overview

This project demonstrates how to create and trigger a security alert in Splunk Enterprise using data collected from a Windows Server via the Splunk Universal Forwarder. The alert identifies multiple failed login attempts (Event ID 4625), which can be indicative of brute-force attacks or unauthorized access attempts.

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 'host' with sourcetype 'WinEventLog:Security'.

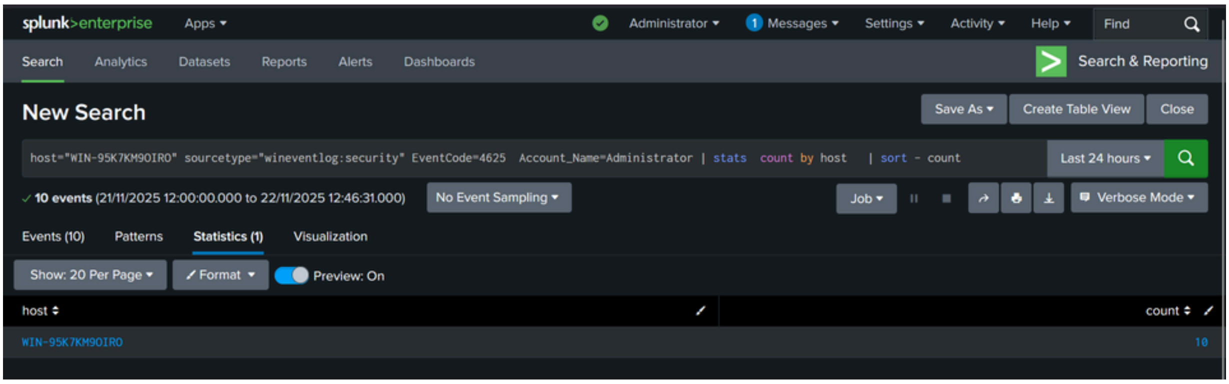
3. Objective

Trigger an alert when more than 5 failed login attempts (EventCode 4625) occur within a 15-minute window.

4. Splunk Search Query

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

host=WIN-95K7KM9OIRO sourcetype=WinEventLog:Security
EventCode=4625 Account_Name=Administrator
| stats count by host
| sort - count



New Search

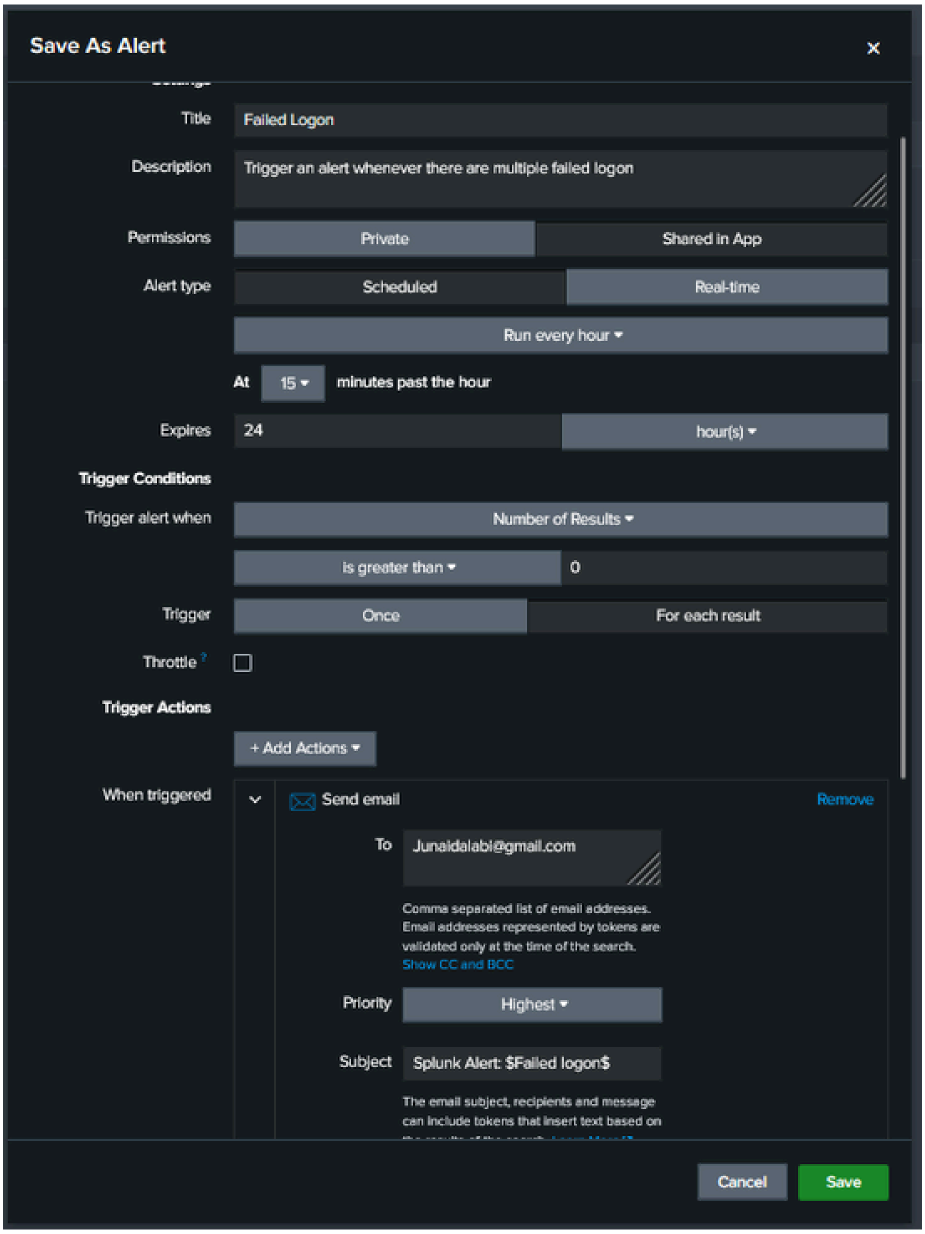
```
host="WIN-95K7KM9OIRO" sourcetype="wineventlog:security" EventCode=4625  Account_Name=Administrator | stats  count by host   | sort - count
```

✓ **10 events** (21/11/2025 12:00:00.000 to 22/11/2025 12:46:31.000)

host	count
WIN-95K7KM9OIRO	10

5. Alert Configuration

- Title: Failed Logon
- Type: Scheduled Alert (Every hour)
- Time Range: Last 15 minutes
- Trigger Condition: Number of results > 0
- Trigger Actions: Send Email (Configured via SMTP in Splunk Settings)



Save As Alert

Title: Failed Logon

Description: Trigger an alert whenever there are multiple failed logon

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour

At 15 minutes past the hour

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Number of Results

is greater than 0

Trigger: Once | For each result

Throttle ☐

Trigger Actions

When triggered: Send email

To: Junaidalabi@gmail.com

Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search.

Priority: Highest

Subject: Splunk Alert: $Failed logon$

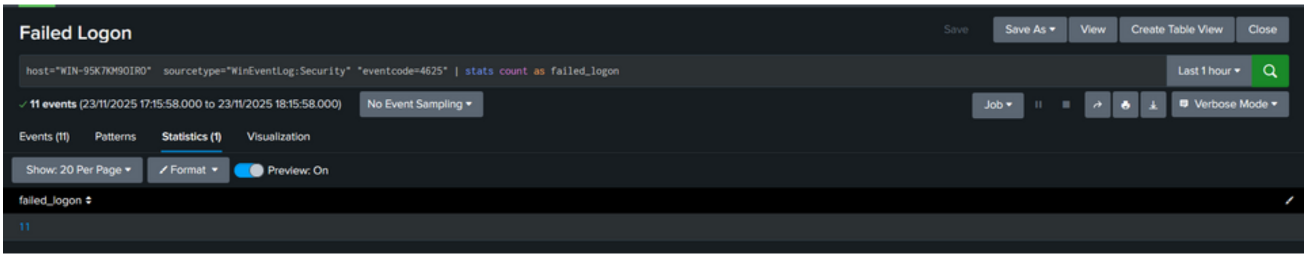
The email subject, recipients and message can include tokens that insert text based on

6. 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.

7. Validation & Output

The alert was successfully triggered after 11 failed login attempts. It appeared in the 'Alerts' section of Splunk and an email notification was received, confirming successful detection and
response.



Failed Logon

```
host="WIN-95K7KM9OIRO"  sourcetype="WinEventLog:Security" "eventcode=4625" | stats count as failed_logon
```

✓ 11 events (23/11/2025 17:15:58.000 to 23/11/2025 18:15:58.000)

failed_logon
11

Conclusion

The successful implementation of this Splunk alert has significantly enhanced the security monitoring capabilities, enabling swift incidence response and minimizing potential security breach. Continuous monitoring and refining the alert is required to ensure optimal performance and improve the overall security posture.