Windows SOC Project using Splunk Enterprise

Objective

To simulate a **Security Operations Centre (SOC)** environment by collecting, analysing, and visualising **Windows Event Logs** on Splunk Enterprise. This project focuses on detecting **failed login attempts**, **brute-force attacks**, and **user-based anomalies**, helping build real-world SIEM skills relevant for cybersecurity job roles.

Setup (Tools Used)

Tool	Purpose
VMware Fusion / UTM	To run guest VMs
Windows 11 VM	Generates logs; runs Splunk Forwarder
Splunk Enterprise (60-day trial)	SIEM solution for indexing and dashboarding
Splunk Universal Forwarder	Installed on Win11 VM to send logs to Splunk
Windows Security Logs	Main source of telemetry (EventCode 4625, etc.)

Data Collection Steps

1. **Install Splunk Enterprise on macOS (localhost)**
   - Enabled port `9997` for receiving input.
2. **Set up Splunk Universal Forwarder on Windows 11 VM**
   - Configured with the deployment IP of the Splunk Enterprise instance.
   - Monitored these logs:
     - `WinEventLog://Security`
     - `WinEventLog://System`
3. **Created Splunk Index: `wineventlog`**
   - Mapped incoming logs to this index for query consistency.
4. **Simulated Attacks:**
   - Attempted multiple failed logins with fake users (admin, John, Randy).
   - Used native Windows login screen to trigger Event ID 4625.

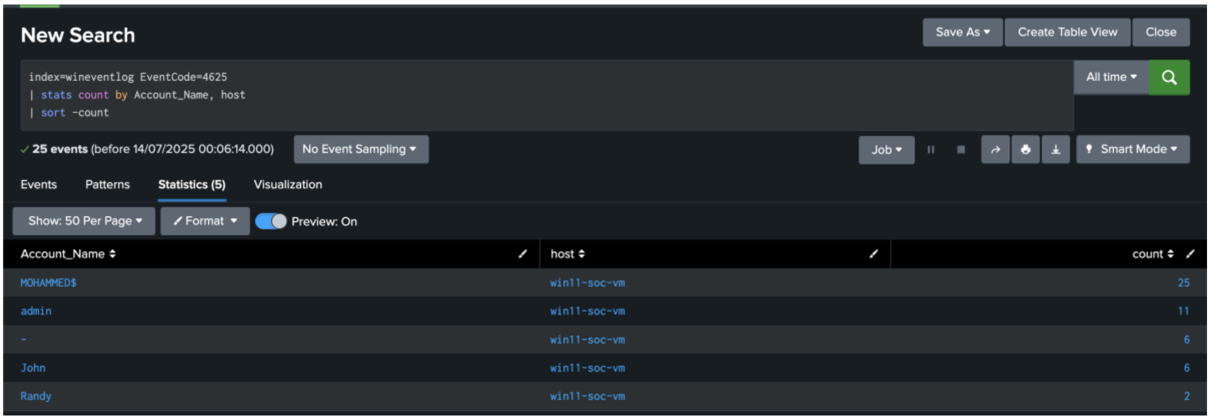
Detection Use Cases

1. Failed Login Attempts (Brute-force Detection)

Description:
Detection of repeated failed logins across multiple accounts could indicate brute-force attack attempts.

EventCode: `4625`
SPL Query:

```
index=wineventlog EventCode=4625
| stats count by Account_Name, host
| sort -count
```



```
index=wineventlog EventCode=4625
| stats count by Account_Name, host
| sort -count
```

✓ 25 events (before 14/07/2025 00:06:14.000)

Account_Name	host	count
MOHAMMED$	win11-soc-vm	25
admin	win11-soc-vm	11
-	win11-soc-vm	6
John	win11-soc-vm	6
Randy	win11-soc-vm	2

2. Account Enumeration Attempts

Description:
Monitoring login failures using non-existent usernames can indicate enumeration attempts by attackers.

SPL Query:

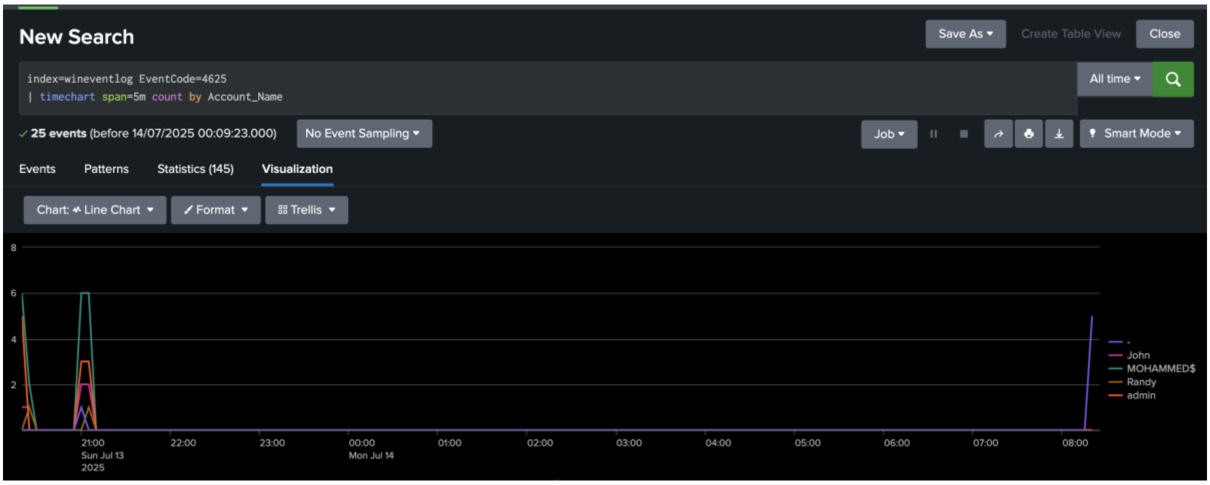
```
index=wineventlog source="WinEventLog: Security" EventCode=4625
| stats count by Account_Name, _time, host
| where Account_Name!="MOHAMMED$"
```

3. Login Failure Over Time

Description:
Track login failures minute by minute to identify spikes in failed authentication attempts.

SPL Query:

```
index=wineventlog EventCode=4625
| timechart span=1m count by Account_Name
```



```
index=wineventlog EventCode=4625
| timechart span=5m count by Account_Name
```

✓ **25 events** (before 14/07/2025 00:09:23.000)

SPL Queries (Collection)

Basic Failed Logins by Account

```
spl
CopyEdit
index=wineventlog EventCode=4625
| stats count by Account_Name, host
```

Failed Logins Over Time

```
spl
CopyEdit
index=wineventlog EventCode=4625
| timechart span=5m count
```

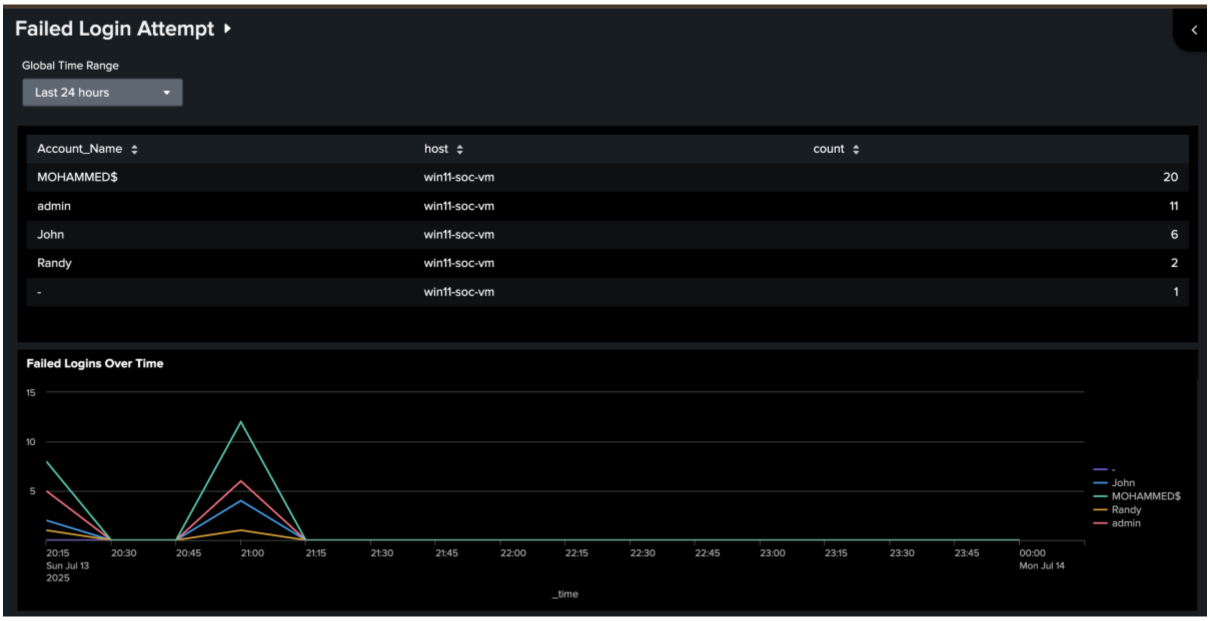
Filtered by Host/Source

```
spl
CopyEdit
index=wineventlog source="WinEventLog:Security" host="win11-soc-vm"
| stats count by Account_Name, _time
```

Dashboard Insights

Panel	Description
Top Failed Login Accounts	Highlights which users failed most
Login Failure Over Time	Brute-force detection
Hosts with Login Failures	Helps trace compromised systems
Real-time updates	Logs streamed via Splunk Forwarder

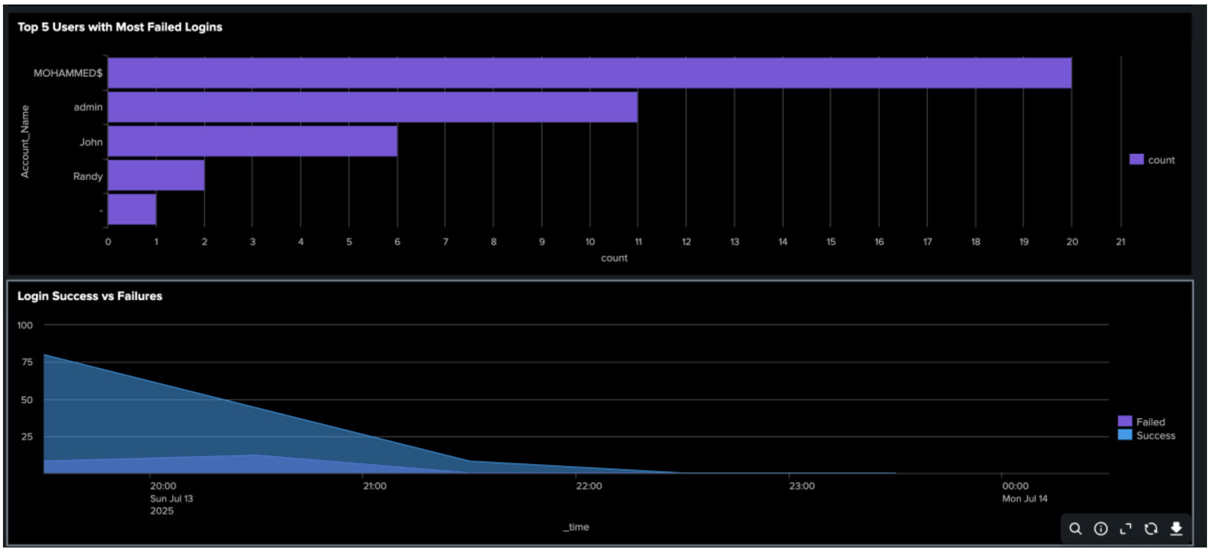
Screenshot:



Failed Login Attempt

Global Time Range: Last 24 hours

Account_Name	host	count
MOHAMMED$	win11-soc-vm	20
admin	win11-soc-vm	11
John	win11-soc-vm	6
Randy	win11-soc-vm	2
-	win11-soc-vm	1



Top 5 Users with Most Failed Logins
Account_Name
MOHAMMED$
admin
John
Randy
-
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
count
count
Login Success vs Failures
100
75
50
25
20:00
Sun Jul 13
2025
21:00
22:00
23:00
00:00
Mon Jul 14
_time
Failed
Success