Splunk SOC Dashboard Projects

By Juwan Naylor

Generated: July 30, 2025

This document highlights three SOC-ready security dashboards built in Splunk. Each project includes live log ingestion, SPL query development, threat detection logic, and real-time visualization.

Projects included:

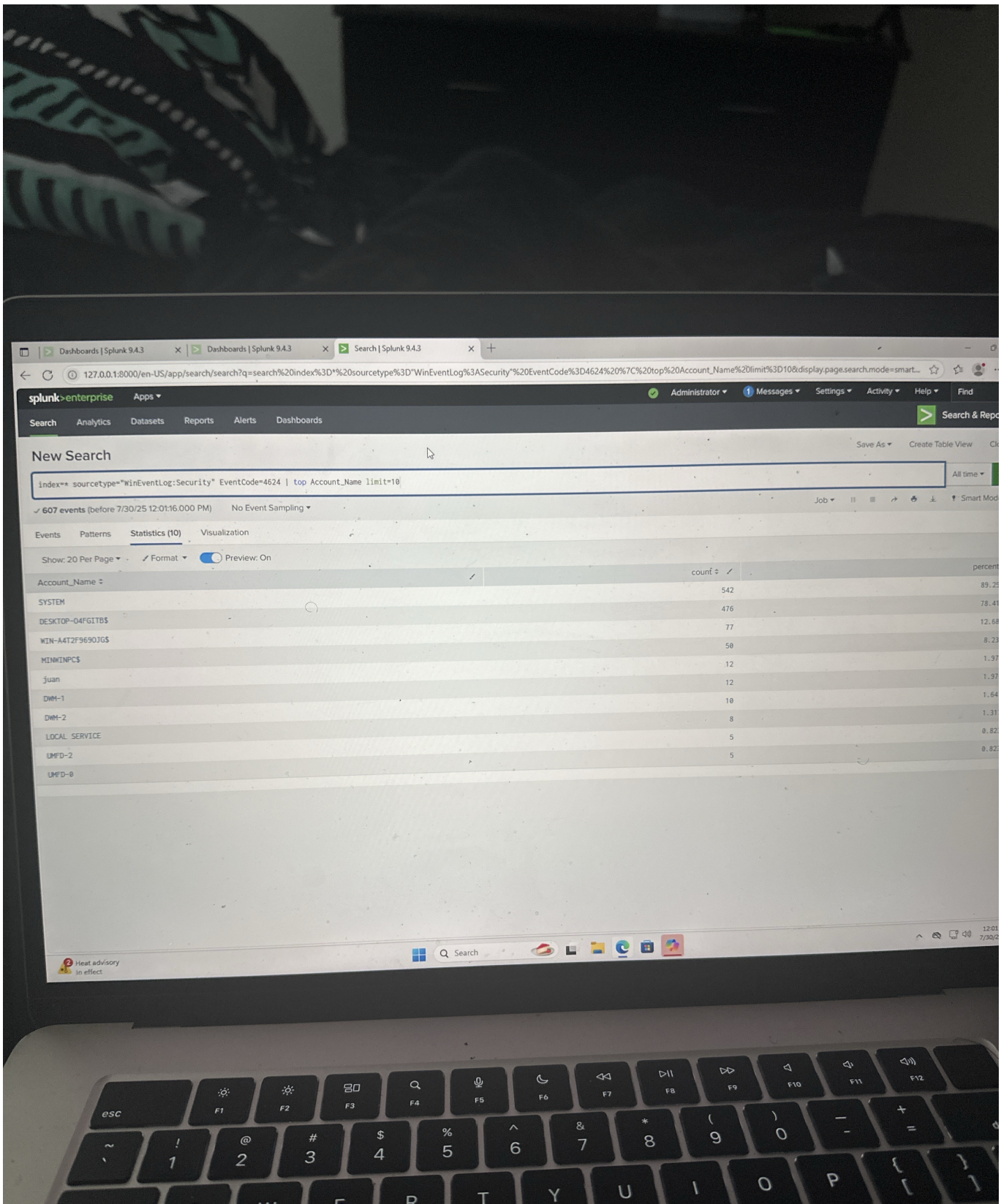
1. Windows Logon Activity Tracker
2. Failed Login Attempt Tracker
3. Brute Force Detection Tracker

1. Windows Logon Activity Tracker

Tracks successful Windows logons over time using EventCode 4624. Visualizes which user accounts are logging in and when, making it easier to spot normal vs. abnormal activity.

Search Query:

```
index=* sourcetype="WinEventLog:Security" EventCode=4624
| top Account_Name
```

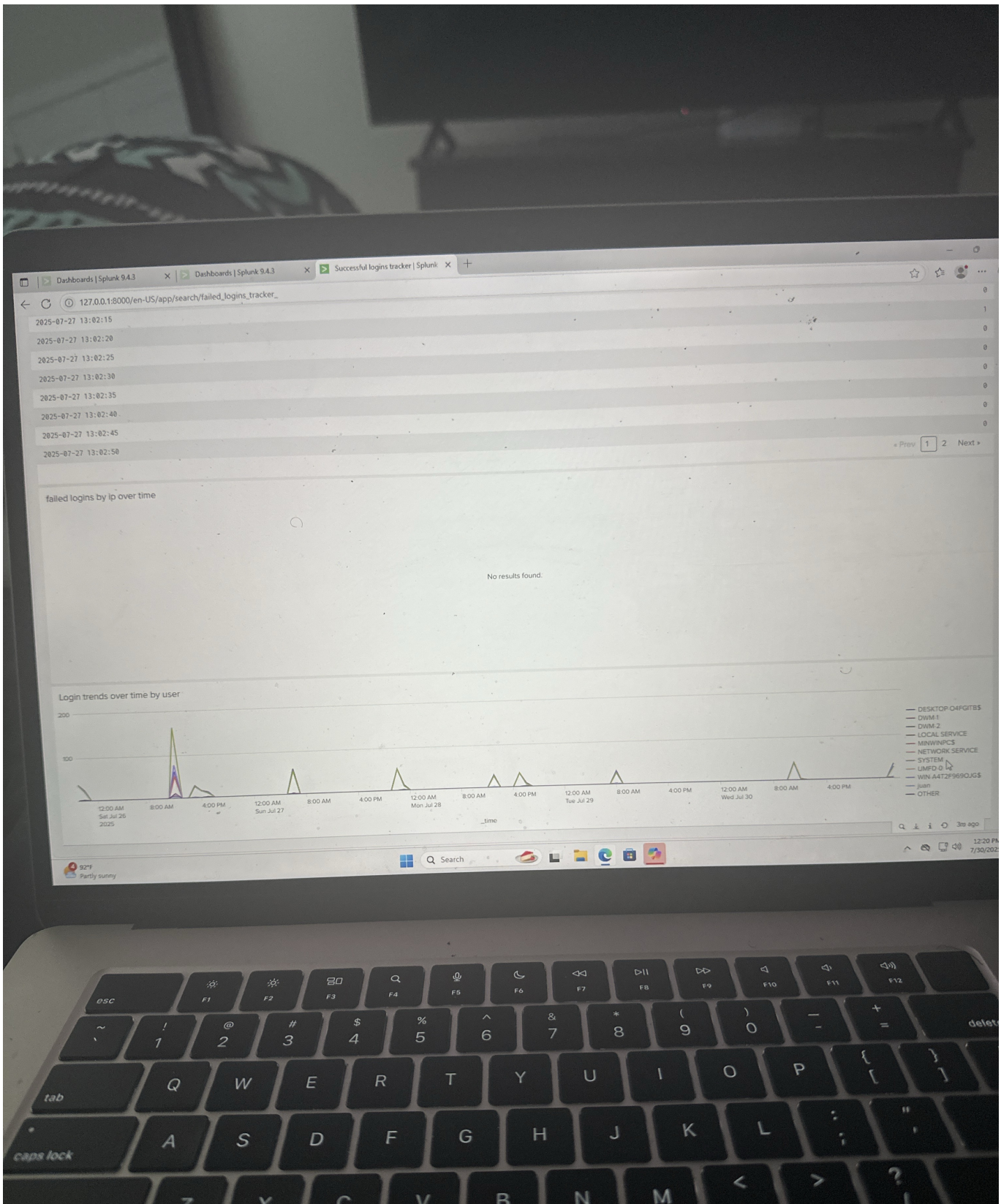


2. Failed Login Attempt Tracker

Monitors failed login attempts using Windows Security EventCode 4625. Helps detect authentication issues and signs of unauthorized access attempts.

Search Query:

```
index=* sourcetype="WinEventLog:Security" EventCode=4625
| timechart span=1h count by Account_Name
```



3. Brute Force Detection Tracker

Detects brute-force login attempts by identifying users with more than 5 failed login events (EventCode 4625) within a short time window. Includes bar chart visualization and alert-ready logic.

Search Query:

```
index=* sourcetype="WinEventLog:Security" EventCode=4625
| stats count by Account_Name, ComputerName
| where count > 5
```