# Detecting Suspicious Login Attempts Using Splunk SIEM

\*\*Project Type:\*\* SOC Simulation | \*\*Tool:\*\* Splunk (Simulated) | \*\*Level:\*\* Beginner-to-Intermediate

## Project Overview

This project simulates the role of a SOC Analyst monitoring authentication events through Splunk SIEM. A spike in failed login attempts is identified, originating from a suspicious IP address, indicating a possible brute-force attack.

## Objectives

- Ingest sample Windows authentication logs into Splunk (simulated)  
- Create alerts for failed login thresholds  
- Identify suspicious IPs and user accounts  
- Recommend mitigation steps

## Simulated Data Summary

The simulation uses anonymized Windows Security Event logs showing repeated Event ID 4625 (failed logon attempts). A particular external IP appears in over 20 failed login events within a 5-minute window.

## Detection Logic in Splunk

Search Query (simulated):  
```sourcetype="WinEventLog:Security" EventCode=4625 | stats count by src\_ip, user | where count > 10```

An alert was configured to trigger when any IP or user had more than 10 failed login attempts within 5 minutes.

## Screenshots (Simulated)

• Splunk Dashboard - Failed Logins by IP (sample)  
• Alert Configuration Window (sample)  
• Alert Trigger Example (simulated)

## Response Steps & Recommendations

- Investigate the source IP address using threat intel sources (e.g., AbuseIPDB, VirusTotal)  
- Lock affected user accounts  
- Notify IT team for forensic review  
- Update firewall rules or add to blocklist  
- Educate users on strong password practices

## Conclusion

This simulation demonstrates how a beginner SOC Analyst can use Splunk to detect brute-force login attempts. It builds foundational skills in log analysis, alert creation, and incident response planning.