

## SOC LAB

I built this Splunk SOC home lab to get hands-on experience with how a SIEM actually operates in a real SOC-style environment. The goal was to investigate **Windows Authentication & Identity log dataset**

This lab focuses on defensive security, SIEM operations, and incident investigations

The task performed includes

Identify Failed Login Attempts

Detect Brute-Force Behavior

Detect Logins from External / Unusual IPs