SOC Analyst Home Lab — SIEM Monitoring, Threat Detection & Incident Response

This document summarizes a home SOC (Security Operations Center) lab project designed to demonstrate foundational cybersecurity and monitoring skills.

Lab Components: - Virtual machines (Windows & Linux) used to simulate a real-world environment. - SIEM solution (Splunk or Wazuh) configured for log collection and monitoring.

Key Activities: - Ingested system, authentication, and security logs. - Detected failed login attempts, brute-force patterns, suspicious scripts, and abnormal behavior. - Created SIEM dashboards to visualize events and alerts. - Wrote a sample Incident Response Report for a simulated attack scenario.

This project demonstrates readiness for entry-level SOC Analyst roles and provides evidence of practical cybersecurity skills.