Threat Hunting Summary – Splunk SIEM

This simulated project demonstrates a basic threat hunting workflow using Splunk in a lab environment. The focus was on identifying Indicators of Compromise (IOCs) from sample network logs and simulating SOC operations.

Findings:
• Multiple failed login attempts from IP 192.168.1.10 were detected, indicating potential brute-force activity.
• DNS queries to suspicious external IPs (e.g., 8.8.8.8) observed outside normal operating hours.
• Anomalies in login timestamps suggest unauthorized access patterns.

Recommendations:
• Implement account lockout policies after 3 failed login attempts.
• Restrict DNS traffic to trusted resolvers only.
• Enable multi-factor authentication (MFA) for user accounts.
• Continue monitoring using Splunk dashboards and alert rules.

This exercise provided hands-on experience with log analysis, detection logic, and basic response procedures, reinforcing foundational skills for SOC roles and threat analysis.