SOC Analyst Portfolio Summary

SOC ANALYST PORTFOLIO SUMMARY

Core Competencies:

- SIEM Monitoring (Microsoft Sentinel)

- KQL Threat Hunting

- Incident Response (NIST/SANS)

- EDR Investigations (Defender for Endpoint)

- Identity Security (Azure AD / Entra ID)

- Detection Engineering & MITRE ATT&CK; Mapping

Projects:

1. KQL Threat Hunting Workbook (20+ queries)

2. Business Email Compromise (BEC) Investigation Simulation

3. Ransomware Pre-encryption Detection Playbook

4. Windows Forensics using Sysmon

5. Detection Rule Pack (PowerShell, LSASS, Kerberoasting)

Tools:

Sentinel, MDE, Splunk, Sysmon, Wireshark, AD, PowerShell

Value:

This portfolio demonstrates end-to-end SOC readiness: detection, investigation, containment, and reporting.