Complete SOC Portfolio

SOC ANALYST COMPLETE PORTFOLIO

Includes:

- KQL Threat Hunting (20+ queries)
- Incident Response Playbook (NIST/SANS)
- BEC Attack Simulation
- Detection Rule Pack (PowerShell, LSASS, Kerberoasting)
- Windows Forensics (Sysmon-based)
- Azure AD Identity Attack Investigations
- SOC Skillset Summary
- GitHub Repository Structure Overview

This document provides a consolidated overview of all SOC capabilities and projects.