Cybersecurity SOC Portfolio Overview

by Alexander T. Ramos

Objective

This portfolio showcases practical, hands-on cybersecurity skills across SOC disciplines including log analysis, vulnerability management, phishing investigation, incident response, and home lab simulation. All artifacts reflect real-world workflows aligned with NIST 800-61, NIST 800-53, and MITRE ATT&CK; frameworks.

Portfolio Summary

Artifact	Folder	Deliverables (Key Files)	Focus
1 – SIEM Log Analysis	SIEM-Log-Analysis	Log_Investigation.md, Queries.txt, SIEM_Log_Analysis_Findings.pdf	Splunk log ingestion, correlation, and SOC triage
2 – Phishing Email Analysis	Phishing-Email-Analysis	Email_Investigation.md, IOCs.csv, Phishing_Report_Alexander_Ramos.pdf	Threat identification, phishing analysis, and documentation
3 – Vulnerability Scan	Vulnerability-Scan	Vuln_Scan_Report.md, Vuln_Scan_Results.pdf, Vulnerability_Remediation_Plan_Alexander_Ramos.pdf	Vulnerability identification, remediation, and validation
4 – Incident Response	Incident-Response	IR_Playbook.md, IR_Tech_Simulation.md, Case_Report_Alexander_Ramos.pdf	NIST 800-61 lifecycle, containment, and executive reporting
5 – Home Lab Environment	Home-Lab	Lab_Setup_Guide.md, Network_Topology.png, Home_Lab_Report_Alexander_Ramos.pdf	Virtual cybersecurity lab configuration and baseline logging
6 – SOC Incident Simulation	SOC-Incident-Simulation	SOC-Incident-Simulation.md, SOC_Report_Alexander_Ramos.pdf	End-to-end SOC simulation and escalation reporting

Tools & Frameworks

Technical Tools: Splunk, Kali Linux, VirtualBox, Metasploitable 2, Nmap, Nikto, Wireshark, Burp Suite
Frameworks & Methodologies: NIST 800-61, NIST 800-53, MITRE ATT&CK;, Incident Response Lifecycle, Vulnerability Management Lifecycle

About the Author

Alexander T. Ramos
Cybersecurity Analyst | CompTIA Security+ | Network+ | IT Essentials Certified
Focused on SOC operations, vulnerability management, and proactive cyber defense.

This portfolio demonstrates readiness for real-world cybersecurity roles, combining technical expertise and analytical communication.