Cybersecurity Professional Portfolio Sample

Name

Fremont, OH | @email.com | LinkedIn: linkedin.com/in/ | GitHub: github.com/

Professional Summary

Recent Information Technology graduate specializing in cybersecurity with hands-on experience in network security, vulnerability assessment, risk analysis, and security monitoring. Strong foundation in defensive security practices, threat mitigation, and system hardening. Seeking an entry-level Cybersecurity Analyst or Security Operations Center (SOC) role where I can contribute to protecting organizational assets and reducing cyber risk.

Core Cybersecurity Competencies

- Network Security Fundamentals
- Threat Detection & Incident Response
- Vulnerability Assessment
- Risk Management Principles
- Security Policy & Compliance Basics
- Security Awareness Training Development
- Log Analysis & Monitoring

Technical Skills

Security Tools:

Wireshark, Nmap, Splunk (basic), Microsoft Defender, Kali Linux

Operating Systems:

Windows Server, Windows 10/11, Linux (Ubuntu, Kali)

Networking:

TCP/IP, Subnetting, VLANs, Firewall Configuration Basics

Scripting:

Python (automation scripts), Basic PowerShell

Cybersecurity Projects

Vulnerability Assessment Lab

Conducted internal vulnerability scan of a simulated lab network using Nmap and Kali Linux. Identified open ports and potential attack surfaces, documented findings, and recommended mitigation strategies. Produced a professional vulnerability assessment report outlining risk levels and remediation steps.

Security Log Analysis Project

Imported simulated security logs into Splunk to identify suspicious login attempts and detect brute-force attack patterns. Created dashboards for visual threat monitoring and documented response recommendations.

Password Policy & System Hardening Implementation

Configured password complexity requirements and account lockout thresholds in Windows Server using Group Policy. Documented policy changes and tested enforcement effectiveness to improve system security posture.

Phishing Email Detection Script

Developed a Python script to flag suspicious email content using keyword detection and pattern matching. Implemented alert messaging to simulate automated threat notifications.

Internship Experience

IT Security Intern – SecureTech Solutions (Summer 2025)

Assisted SOC team with monitoring security alerts, reviewed firewall logs, supported phishing awareness campaigns, and participated in tabletop incident response exercises.

Certifications

- CompTIA Security+ (Planned – June 2026)
- Google Cybersecurity Certificate
- CompTIA Network+

Career Goals

Short-Term Goal:

Obtain CompTIA Security+ certification and secure a Junior Cybersecurity Analyst or SOC Analyst role.

Long-Term Goal:

Advance into a Security Engineer or Threat Intelligence Analyst role focusing on proactive defense strategies.

Professional Development Plan

- Build and maintain a home cybersecurity lab

- Participate in Capture the Flag (CTF) competitions
- Contribute to open-source security tools
- Attend cybersecurity conferences and workshops
- Stay updated on emerging threats and vulnerabilities

Personal Brand Statement

I am a cybersecurity-focused IT graduate dedicated to protecting systems, identifying vulnerabilities, and strengthening organizational security posture. I am passionate about continuous learning and committed to staying ahead of evolving cyber threats.