Steven Song – Cybersecurity Analyst

Fullerton, CA – StevenSong0812@gmail.com – https://portfolio-st.pages.dev/

SUMMARY

New grad cybersecurity analyst with hands-on experience through self-directed homelab environments and simulated SOC workflows. Skilled in log analysis, threat hunting, vulnerability management, and compliance monitoring, with additional exposure to red-team tooling. Previously supported public-facing cybersecurity education and simulations.

EXPERIENCE

Orange County Cyber Innovations Clinic, *Intern*

JAN 2025 - MAY 2025

- Created and delivered cybersecurity awareness presentations for older adults through the Osher Lifelong Learning Institute (OLLI), reaching 100+ participants.
- Designed phishing simulation scenarios and educational materials to improve understanding of social engineering risks.
- Provided mentorship and training to OCCIC trainees in CompTIA Security+ preparation, achieving a 100% certification pass rate.

PROJECTS

Proxmox Homelab

- Designed a multi-VLAN Proxmox homelab using pfSense to segment management, Windows, containerized services, and vulnerable machine subnets for controlled experimentation.
- Emulated enterprise operations by configuring Windows AD and GPOs, and performing vulnerability, threat, and compliance assessments with patching and remediation workflows.
- Executed adversarial simulations by hosting vulnerable web services via Docker and deploying intentionally vulnerable machines (e.g., Metasploitable) to practice penetration testing and malware analysis.

Simulated SOC

- Configured Wazuh agents on enterprise Windows machines collecting over 20,000 user event logs and detecting 1,400+ vulnerabilities.
- Patched over 200 failed controls related to Active Directory and Group Policy configurations to achieve compliance with CIS Microsoft Windows Server 2022 Benchmark.
- Performed adversarial operations through MITRE Caldera and analyzed resulting logs and alerts to inform alert triaging and detection rule development.

Chiron Compliance Management

- Led a four-person team to design and develop a compliance management platform enabling secure storage, tracking, and review of organizational compliance.
- Researched and incorporated cybersecurity compliance frameworks (e.g., ISO 27001, GDPR, CIS Controls) into the system's configured assessments.
- Implemented and monitored a CI/CD pipeline with GitHub Actions, using Jira for sprint planning and tracking.

EDUCATION

California State University, Fullerton - *Computer Science, Cybersecurity Concentration, B.S.*

AUG 2021 - DEC 2025

CERTIFICATIONS

CompTIA - *Security+ (SY0-701)*

AUG 2024 - AUG 2027

SKILLS

Threat Hunting and IR (Splunk, Wazuh), Vulnerability Mgmt (Nessus, OpenVAS), Frameworks (NIST, ISO, CIS, MITRE), Operating Systems (Windows, Linux), Scripting & Automation (Python, Bash), Penetration Testing (Kali Linux, Burp Suite), Networking (TCP/IP, OSI, Wireshark), Virtualization (Proxmox, VirtualBox, VMware), Cloud (AWS, Azure)