First M. Lastname

Phone: *(123)456-7890*

Email: *user.name@domain.com*

GitHub: *https://github.com/Alias*

LinkedIn: *https://www.linkedin.com/in/user-name*

Professional Summary

A cybersecurity professional and enthusiast, with 4 years experience from various roles in the field, after building other technical and interpersonal skills, spanning over 15 years and several industries.

Cybersecurity Experience

Vulnerability Scanning Analyst [redacted] *(Mar 2024 – Present)*

The CISA Cyber Hygiene Vulnerability Scanning (CyHy VS) services uses tools such as Nessus, Nmap, pshtt, SSLyze, and trustymail to conduct regular assessments and provide comprehensive reports to our stakeholders each week. As total stakeholders increased by more than 2,000 entities over one year, I improved the efficacy and efficiency our small team needed to accommodate this by:

- Automating data collection required for false positive analysis, pulling information from multiple MongoDB collections and scraping variable information from internet repositories using Python scripting, saving an immeasurable amount of time;
- Developing GUI tools for non-technical staff to have ability to change scanning/reporting configurations, update the CyHy database, and collect data for statistical analysis;
- Updating training frameworks for investigating Binding Operational Directive (BOD) compliance for Federal Civilian Executive Branch (FCEB) Agencies (specifically BOD 18-01 and 19-02);
- Updating and pruning deprecated records, across multiple sources and between cross-functional decentralized teams, by leveraging platforms like GitHub and ServiceNow.

Risk Operations Analyst [redacted] *(Mar 2023 – Mar 2024)*

The main focus of our CISA Risk Operations team was to identify and track vulnerabilities which could detrimentally impact our nation's critical infrastructure. Once identified, notifications were issued to those CI entities, including special notification when vulnerabilities had been associated with ransomware deployments (CISA's RVWP). My contributions included:

- Automated the vulnerability prevalence scanning with several Python scripts, which leveraged signature tracking through the Shodan API, reducing time needed for analysis and resulting in doubling the number of notifications able to be issued;
- Added the Ransomware boolean to CISA KEV database entries, improving the utility in risk analysis for stakeholders (completed by leveraging Ransomware intelligence through platforms like Bitsight, Black Kite, Mandiant TIP, and Palo Alto Xpanse/ILI);
- Provided technical summary for how organizations can improve their security posture by leveraging the 'security.txt' file (RFC 9116), which was utilized to publish a CISA Blog Post.

Continuous Monitoring Engineer [redacted] *(Jan 2022 – Mar 2023)*

Though the operations of our team was focused on the continuous network performance monitoring for the US Coast Guard, using the SolarWinds Orion platform, we were also responsible for the security and compliance of our SolarWinds, Microsoft SQL Server, and IIS tech stack. So, in addition to learning technical skills of network engineering, this also provided me unique opportunities:

- Developed a repeatable and continuous process for ACAS vulnerability scan analysis, mitigation testing, and implementation for ContMon servers;
- Collected more appropriate documentation and artifacts for DISA STIG compliance;
- Mapped the Continuous Monitoring SOP to NIST SP 800-53 controls.

Cybersecurity Internship [redacted] *(May – Sept, 2021)*

- This opportunity was my introduction to the vast scope of cybersecurity focuses and their interdependancies. It provided exposure to several platforms, cybersecurity tooling, and compliance frameworks, which I would love the opportunity to discuss.
- My major contribution adding value to their products was providing 3 – 5 technical summaries per week to their Hive-IQ community. Using OSInt research, these briefings discussed details on how recent cyber attacks were carried out, by whom, and how to defend against them.

Other Professional Experience

Adjunct Instructor (Linux+ Prep) [redacted] *(Fall 2023)*

- Sharpened teaching, project planning, and Linux Server Admin technical skills.

Certified Applications Counselor [redacted] *(2019 – 2022)*

- Developed proficiency in tailoring explanations of complex concepts to align with the audience's level of understanding, and meet them where they are.

Mobile Device Sales [redacted] *(2014 – 2019)*

- Established foundational understanding IT and troubleshooting concepts;
- Included four years of Retail Store and Sales Management experience.

Education

Community College – *Associate of Applied Science in Cybersecurity*

Other Technical Proficiency

Cyber Security:	BURP Suite, Censys, Firewalls, Metasploit, Netcat, OpenVAS, OWASP ZAP, Qualys, SCAP-CC, Security Onion, Snort, Splunk, Wazzuh, and Wireshark
Platforms:	AWS, Docker Containers, ELK Stack, InfoBlox, Jira, and Remedy
Certifications:	CompTIA – PenTest+, Security+, and Linux+
Clearances:	Secret and Pubic Trust