Manju Kuah

manjukuah@gmail.com ❖ (503) 548-7109 ❖ manjukuah.github.io ❖ Portland, Oregon

PROFESSIONAL EXPERIENCE

Information Security Analyst Intern - Freddie Mac **Jan 2022 - June 2022**

Deployed, configured, integrated, and troubleshooted CyberArk Privileged Account Security product suite, including Enterprise Password Vault, Password Vault Web Access, Central Policy Manager, Privileged Session Manager, Application Identity Manager, and Privileged Threat Analytics.

- Consulted with over 50 clients to integrate PSM and CPM plugins, fortifying web-based applications, mitigating security risks, ensuring compliant user access, and enhancing overall organizational security.
- Published 100+ pages of comprehensive documentation, simplifying complex processes and code for non-technical comprehension. Enhanced process auditing and organizational transparency.

PROJECTS

SOC Infrastructure

Senior capstone project focused on designing infrastructure for the Oregon Research & Teaching Security Operations Center (ORTSOC) , a student-staffed SOC aimed at vocational teaching of students in SOC operations and security analysis.

- Designed infrastructure using zero-cost software such as Zeek, Elastic Stack, Ansible, and VSphere to minimize operating costs for clients.
- Enabled small organizations with limited resources to access valuable security services by providing a functional SOC alternative that they may not have been able to afford otherwise.
- Cultivated the expertise of hundreds of students, equipping them with proficiency in SOC capabilities. Its infrastructure continues to serve as a cornerstone for ongoing education and practical application.

Cyber Security Incident Response

- Leveraged NIST incident response framework and MITRE ATT&CK framework to respond to incidents
- Conducted proactive threat hunting for malicious activity across network and digital assets using a SIEM.
- Analyzed data sets and utilized various tools to identify indicators of malicious activity.
- Developed and implemented strategies to enhance incident response effectiveness and mitigate threats.
- Gained proficiency in ISO 27001, NIST SP800-61 + CSF, and Diamond Model of Intrusion Analysis.

SKILLS

Security

- SIEM: Splunk, Elastic Stack
- EDR: Wazuh, Sysmon
- Automation: Ansible, BladeLogic
- Vulnerability Scanning: Nessus, nmap
- Binary Exploitation: pwntools

Programming

- Scripting + Automation: Python, PowerShell, Bash
- C, C++
- x86 Assembly
- Java
- HTML/CSS/JavaScript
- YAML/XML/JSON
- VisualStudio/Eclipse/IntelliJ

Digital Forensics

- Malware Analysis + Reverse Engineering: IDA Pro/Hex-rays Decompiler, gdb
- Volatility
- FTK Imager
- RAM Capture
- Autopsy

EDUCATION + CERTIFICATIONS

Bachelor of Science in Computer Science & Certificate in CyberSecurity **Grad Date: June 10th, 2022**

CompTIA Security+ Certification **March 28st 2023 - March 28st 2026**