Marilou Daara

Tulsa, OK 74136 | Phone: 918-8102793
Email: mariloudaara@gmail.com
LinkedIn: https://www.linkedin.com/in/mariloudaara

Objective

Dedicated cybersecurity professional with 12 years of nursing experience, driven by a passionate commitment to safeguarding individuals across both physical and digital realms. Seeking an entry-level position to leverage comprehensive cybersecurity training, including expertise in security concepts and incident response. The adaptability honed through years in healthcare enables rapid acquisition and application of cybersecurity skills, with a keen enthusiasm to fortify organizational security in an evolving digital landscape.

SKILLS

HTML | Bash Script | PowerShell Commands | Linux | Windows | Hashcat | Networkminer | Wireshark | Recon-Ng | Nessus | Metasploit | Kiwi (Mimikatz version) | Ethics and Confidentiality | Problem-Solving | Attention to details | Team Collaboration

CERTIFICATIONS

CompTIA Security+ pending, August 2024

PROJECTS

Project 1: Securing Cloud Applications
Technologies Used: Azure: {Keyvaults, App Services, Front Door, WAF}
PHP, HTML, Docker, OpenSSL

- Developed and designed a cyber-blog web application using Azure's Cloud services and Docker
- Created and stored SSL certificates in Azure's Key Vault, and bound them to secure the web application.
- Protected the web application by utilizing Azure's Security features, such as Azure's Front Door, WAF, and Security Center.

Project 2: Exploiting Vulnerabilities with Capture the Flag (CTF) Style Competition
Technologies Used: Web Application, Linux Server, Windows Server, Kali, Mimikatz

- Analyze the fictional organization’s web application for vulnerabilities.
- Execute exploits to uncover security weaknesses.
- Identify and collect flags representing successful exploits.
- Assess vulnerabilities specific to Linux servers within the organization’s infrastructure.
- Employ penetration testing techniques to exploit Linux server weaknesses.
- Locate and retrieve flags corresponding to successful intrusions.
- Evaluate the security posture of the fictional organization’s Windows servers.
- Employ methodologies to exploit vulnerabilities inherent to Windows operating systems.

Project 3: Building a Security Monitoring Environment
Technologies used: SIEM tool > Splunk, web lab Virtual Machine

- Utilize Splunk tools to craft a tailored monitoring solution for the fictional organization.
- Analyze provided logs of “normal” business activities to comprehend the organization’s operational context.
- Establish baselines using the collected data and develop custom alerts, reports, and dashboards, as instructed in class.
- Incorporate a Splunk “add-on” app of choice to enhance monitoring capabilities against diverse attack vectors.
- Evaluate the effectiveness of the monitoring solution by analyzing reports and dashboards.
- Assess the defensive choices made and their impact on mitigating or preventing simulated attacks.
- Address review and analysis questions to identify areas of improvement in the defensive strategy.
- Initiate preparation of presentation slides summarizing findings for the upcoming group presentation.
- Collaborate with peers to present the designed defensive solutions and their performance against simulated attacks.
- Discuss the efficacy of the implemented monitoring environment in safeguarding the organization.
- Engage in Q&A sessions to provide further insights into the defensive approach and its outcomes.

Project 4: Research Project > Honeypot Lab with Azure
Technologies used: Microsoft Azure Lab Environment, Log Analytic Workspace, Microsoft Defender for the Cloud, Microsoft Sentinel (SEIM tool), PowerShell Script.

- Constructed a virtual Security Information and Event Management (SIEM) environment using Microsoft Azure and Sentinel to analyze and visualize live cyber attacks. This involves intentionally exposing a virtual machine to global cyber threats to generate a real-time attack dashboard.
- Leverage the use of PowerShell script (courtesy of github.com Josh Madakor) and https://ipgeolocation.io/ for geolocating brute force attempts to create a global heatmap of cyber incursions. This serves as both a personal exploration into cybersecurity and an educational platform for visualizing and strategizing against live digital threats.
- Gain hands-on experience with essential tools within the Microsoft Azure ecosystem.
- Develop an understanding of the critical importance of securing both cloud and on-premise infrastructure.
- Explore best practices and practical insights for enhancing security measures in both cloud and on-premise environments.

WORK EXPERIENCE

Charged Nurse | Gracewood Health and Rehab

February 2016 - December 2023, Tulsa OK

- Monitored patient's health, observed for any significant conditions or symptoms, and utilized diagnostic tests and medical equipment, leading to an increase in patient recovery rates, early warning sign detection and improved patient outcomes.
- Conduct safety, neuro checks and risk assessments, reducing patient falls and incidents by about 10% year-over-year.

Charged Nurse PRN | Emerald Care Center

March 2022 - June 2022

- Maintain accurate patient records using Epic Software. Complete and update patient records in Epic within 30 minutes of patient interaction, ensuring 100% compliance with documentation standards.

Charged Nurse | Southern Hills Rehabilitation Center
May 2014 - February 2016, Tulsa, OK

- Effectively engaged with patients and their families to discuss health-related matters, utilizing patient education materials to drive improved health outcomes and gather feedback from the families.

Companions Care Center / Charged Nurse
May 2013 - May 2014, Tulsa, OK

- Assist in executing care plans developed by RNs and Physicians, ensuring 100% to treatment protocols.
- Provide guidance and oversight, ensuring tasks are completed efficiently and correctly, with a 95% task completion rate.

Leisure Village Health Care / Charge Nurse
December 2011 - May 2013, Tulsa, OK

- Proficient in wound vac dressing and medication administration via PEG Tube to enhance patient comfort and improve quality of life.
- Monitor patient vitals and report changes. Record vitals (e.g. blood pressure, pulse, temperature) every 4 hours and immediately report any significant changes.

EDUCATION

Certificate, Cybersecurity Bootcamp: Tulsa Community College | 2U/edX, Tulsa, OK

Certificate, Licensed Practical Nurse: Tulsa Tech, Tulsa, OK

Bachelor of Science in Business Administration major in Computer Science:
Central Colleges of the Philippines, Quezon City, Philippines

SCHOLARSHIP/ AWARD

Cyberskills Skills Center Scholarship Award
Microsoft Scholarship / Last Mile Fund Recipient