Rahmah Khalil

(717) 634-1652 rmkhalil21@gmail.com
github.com/Rahmahk02 linkedin.com/in/rahmah-khalil

EDUCATION

Penn State World Campus World Campus (Online)

B.S. in Cybersecurity Analytics and Operations (Information Sciences and Technology) *Aug 2023 – May 2026*

Relevant Coursework: Intro App Development, Intermediate App development, Computer Literacy, Organization of Data, Cyber-Defense Studio, Information Security, Cyber Forensics, Network and Telecom

SKILLS

Certifications: Mastercard Cybersecurity Simulation, Qualys Vulnerability Management (in progress)
Technical Skills: Microsoft Office Suite, Linux, Python, Honeypots, Java, SQL, SIEM, Virtual Machine, PHP
Soft Skills: Teamwork, Communication, Problem-Solving, Technical Writing, Public Speaking
Languages: English (Native), Arabic (Elementary)

EXPERIENCE

Mastercard Cybersecurity virtual experience program on Forage January 2025 – January 2025

- Completed a job simulation as an analyst on Mastercard's Security Awareness Team
- Helped identify and report security threats such as phishing
- Analyzed and identified which areas of the business needed more robust security training and implemented training courses and procedures for those teams

Company: Al-Huda School Dec 2021 – Present
Title: Fundraiser Host/Emcee Speaker (Volunteer)

While volunteering at a private school, I helped set up event venues and served food during events. I also organized several fundraisers, including being an MC and hosting as a speaker.

PROJECTS (Personal)

SIEM Setup with Azure Feb 2025 – Feb 2025

- Used an RDP port as a decoy to monitor unauthorized access attempts following a SIEM deploy on Azure.
- Integrated Microsoft Sentinel on a VM with a non-personal IP address to log successful logins.
- Used SQL queries to analyze logins.
- Created a custom 'Security Incident' alert to flag suspicious activities in real-time.

Platforms and Technology Used: Microsoft Azure, Microsoft Sentinel

Honey Pot Installation Dec 2024 – Dec 2024

- Deployed and configured a Cowrie honeypot to capture and log unauthorized access attempts, including brute-force attacks and shell interactions.
- Set up a honeypot to monitor and log SSH and Telnet traffic, providing valuable insights into attack patterns and enhancing network security.

Source: https://github.com/Cowrie-Honeypot-Setup
Platforms and Technology Used: Akami, SSH, Telenet, Python