Yvonne Albert

yvonne.k.albert@gmail.com | 469-844-0233 | Texas

SKILLS & CERTIFICATIONS

- AWS Certified Cloud Practitioner
- CompTIA Security+
- Google Cybersecurity Professional Certificate: SQL, Splunk, Linux, Python
- ISC2 Certified in Cybersecurity
- Cybersecurity Compliance Frameworks & System Administration (IBM)
- Introduction to Cybersecurity Tools & Cyber Attacks (IBM)
- Security and Privacy by Design Foundations (IBM)
- Strong Technical reporting & presenting skills
- Agile Methodologies/Tools – Trello, Slack, Mural, Stand-ups, retrospectives

RELEVANT PROFESSIONAL HISTORY

Cyber Security Developer – Stretch Project September 2022 – April 2023
IBM

- Used automation to reduce manual controls mapping to NIST, PCI DSS by 100%.
- Successfully presented project results to global IBM security teams, demonstrating the value of implementing automation methods for controls mappings, which led to saving 30hrs per week.
- Collaborated closely with software development teams to design and implement highly effective automated processes for controls mapping, ensuring seamless integration into AI tool.
- Played a key role in the documentation process for the mappings tool, creating clear and comprehensive documentation that effectively communicates the tool's features and best practices to developers.
- Extracted over 150 controls with PostgreSQL database management tool.

Hardware Engineer, Infrastructure June 2021 – May 2023
IBM

- Conducted root cause analysis of semiconductor chip data to provide technical solutions, generating technical reports and making recommendations to cross-functional teams and management personnel.
- Developed storage solution plans, determined resources, and created a budget for continuous improvement of lab processes.
- Developed streamlined product archiving processes by creating a standard operating procedure, ensuring consistent and accurate documentation for future reference.
- Used project management skills to lead daily scrum meetings to manage product backlog.

Quality Control/Assurance Chemist November 2016 - July 2019
MEDISCA

- Reviewed compliance documents under USP-NF and generated 100+ technical reports.
- Collaborated with team and manager to discuss new project initiatives to advance the Chemistry department as well as train new hires.
- Spearheaded the buildout of Standard Operating Procedure (SOP) for lipid compounds resulting in reduced equipment cost by $10,000.
- Evaluated non-compliant results and initiated remediation processes leading to supplier recall.

CYBERSECURITY PROJECTS & BOOTCAMPS

Women in Cybersecurity (WiCyS) Training Scholarship (Sept 2024 - current)

- SANS institute cyber range CTF (**Tier 1**)
- TryHackMe security pathway training (**Tier 2**) – Jr Pen tester pathway, web app attacks and vulnerabilities.

AWS EC2 (July 2024)

- Configuring EC2 instances and security groups to deploy a website.

AWS IAM configuration (July 2024)

- Assigning users to groups, managing group/user permissions, updating passwords and reviewing user access.

Mastercard via Forage: Security Awareness (May 2024)

- Designed a phishing email simulation.
- Interpreted phishing email results and designed a presentation for departments affected.

Google Professional Cybersecurity Bootcamp Program (May 2023 – Feb 2024)

- Prioritized audit findings of simulated company's vulnerabilities to produce recommendations for critical discoveries in a stakeholder memorandum.
- Engaged in reporting cybersecurity incidents following the NIST CSF. This included a DNS and ICMP analysis and Wireshark TCP log analysis.
- Provided risk assessment report to recommend various network hardening tools and methods of implementation.
- Exposure to Splunk, Python, SQL and Linux command line.

Analyzing a proxy log – TryHackMe CTF (Dec 2023)

- Isolated suspicious web traffic logs in Linux terminal using sort, uniq and cut commands.
- Decoded with base64 to expose exfiltrated data located in the website parameter.

Amazon x WiCyS – Incident Response CTF (September 2023)

- Discovered threat actor identity via OSINT tactics (Social media reconnaissance).
- Utilized Wireshark to analyze compromised packet to extract .png file in multipart via cyberchef.
- Accurately identified hidden message in .png file using EXIF tool and cyberchef.

Target x WiCyS - Cyber Threat Intelligence CTF (June 2023)

- Protected against a simulated ransomware attack using brute force to decipher threat message.
- Conducted in-depth research using MITRE database to identify technique and procedures for nltest/ command, resulting in uncovering Domain Trust tactic.
- Researched ARIN database to resolve IP address, resulting in identifying attacker domain name used by threat actor.

EDUCATION

Masters in Materials Science & Engineering, The University of Texas – Arlington, Texas

Bachelors in Chemistry, Minor: Mathematics, Midwestern State University – Wichita Falls, Texas

VOLUNTEERING & INTERESTS

Black Girls Code | PTECH volunteer | Society of Women Engineers volunteer | 48in48 Women's Build | UTSA Cybersecurity Alumni Mentor | Women in Cybersecurity Mentor