**FaithCollins E. Okogbuo**

Ikeja, Lagos | Phone: +2348102644557 | Email: faithcollinsokogbuo@gmail.com | LinkedIn: linkedin.com/in/faithcollinsokogbuo |

**Professional Summary**

Results-driven Security Analyst with expertise in cybersecurity operations, threat detection, and SOC workflows. Proficient in using tools like Splunk, Microsoft Sentinel, and Wireshark to monitor, analyze, and secure IT systems. Adept at conducting risk assessments, developing mitigation strategies, and leveraging frameworks such as MITRE ATT&CK, NIST, and ISO 27001 to fortify organizational security. Hands-on experience in advanced tasks like packet analysis, policy development, and AI-powered cybersecurity solutions.

**Key Skills**

* **Security Operations (SOC)**: Incident detection, threat hunting, log analysis.
* **Open-Source Tools:** Metasploit, OpenVAS, Wireshark, Nmap, Autopsy**.**
* **Forensic Tools:** FTK Imager, Volatility, CyberChef.
* **SIEM Tools:** Splunk, Microsoft Sentinel**.**
* **Frameworks**: PCI DSS, GDPR, MITRE ATT&CK, NIST Cybersecurity, ISO 27001.
* **Governance, Risk, and Compliance (GRC):** Policy development, risk assessment, and audit mapping.
* **Cloud and Automation:** Kubernetes, AWS, PowerShell, Bash**.**
* **Data Analysis:** Excel, Power BI, SQL.
* **Web Development:** HTML, CSS, JavaScript for secure application design**.**

**Professional Experience**

**BNS Cyberlab** | *Cybersecurity Intern* | Jan 2025 – Present

* Designed and implemented a network packet sniffer tool for analyzing and displaying IP addresses, protocols, and payload data ethically.
* Developed a password complexity checker to evaluate strength based on predefined criteria and provide user feedback.
* Created an image encryption tool using pixel manipulation techniques for enhanced data security.
* Contributed to building a risk assessment framework that evaluates organizational risks by likelihood and impact using Excel.
* Assisted in the creation of business continuity plans (BCP) and internal audit risk mapping tools with Power BI.

**CyberSafe Foundation (CyberGirl Fellowship)** | *Security Analyst* |Nov 2023 – Dec 2024

* Conducted risk assessments to identify and mitigate potential threats to IT infrastructure.
* Optimized SIEM tools (Splunk, Microsoft Sentinel) to monitor network traffic, achieving real-time anomaly detection and reducing false positives.
* Analyzed threat intelligence data to identify emerging cybersecurity threats, contributing to improved incident response protocols.

**CyberPatron, Remote** | *GRC Intern* | Feb 2024 – May 2024

* Drafted and implemented data privacy and security policies, reducing breaches by 5%.
* Researched and analyzed project data using Excel and SQL, improving operational efficiency by 20%.

**Projects**

**Network Packet Analyzer**

* Developed a tool to capture and analyze network packets, extracting and displaying key details such as source and destination IP addresses, protocols, and payload data.

**Password Complexity Checker**

* Created a tool to evaluate password strength based on criteria like length, special characters, and casing.

**Image Encryption Tool**

* Built an encryption utility that manipulated pixel values for securing images against unauthorized access.

**Risk Assessment Framework and Audit Mapping Tool**

* Designed frameworks and tools to prioritize organizational risks and identify high-risk areas during audits.

**Implementing MITRE ATT&CK Framework in SOC Operations**

* Developed custom detection rules aligned with MITRE ATT&CK tactics, improving threat detection by 80%.
* Automated SOC workflows using tools like Splunk and Microsoft Sentinel, reducing response time and enhancing efficiency.

**Education**

University of Uyo, Nigeria | *BSc, Library and Information Science* | 2024

* Achieved Second Class Honours, Upper Division(2:1)

**Certifications**

* Certified in Cybersecurity (CC) – (ISC)²
* Blue Team Level 1 (BTL1)
* CompTIA CySA+ – CompTIA
* CompTIA SEC+ – INFOSEC
* Linux+ – INFOSEC
* Cybergirl Fellowship Certificate
* THM Advent of cyber-Certificate

**Technical Tools**

* **Open-Source Tools:** Metasploit, OpenVAS, Wireshark, Autopsy
* **Forensics Tools**: FTK Imager, Volatility, CyberChef
* **Cloud & Automation:** Kubernetes, AWS, PowerShell, Bash
* **Data Analysis Tools:** Excel, Power BI, SQL
* **Frameworks**: PCI DSS, GDPR, MITRE ATT&CK, NIST, ISO 27001