Kate Amarachuwku Igwilo

Abuja, Nigeria | kateigwilo@gmail.com | +2349118283716 | www.linkedin.com/in/itskatieconnect | https://github.com/itskatieconnect

PROFILE

Dynamic SOC Analyst with proven expertise in cyber threat detection, incident response, and security monitoring. Skilled in utilizing advanced cybersecurity tools, including SIEM platforms (Splunk, Azure), for threat mitigation and risk management. Strong collaborator, excelling in communication and problem-solving, with a focus on enhancing organizational security posture. Seeking a challenging role to leverage my skills and drive proactive security measures.

CERTIFICATION

Microsoft Certified Security Operations Analyst (in-view)
Certified in Cybersecurity, $(ISC)^2$
SIEM Architecture and Process (Infosec)
Windows Registry Forensic (Infosec)
Applied ChatGPT for Cybersecurity (Infosec)

TECHNICAL SKILLS

- Security Operations: Incident Response, Threat Detection and Mitigation, SIEM Tools (Splunk, Azure)
- Network Security: Forensics and Malware Analysis (Wireshark, Network Miner), Vulnerability Assessment
- Security Strategy: Compliance (HIPAA), Security Monitoring, Security Strategy Development
- Scripting: PowerShell, JavaScript, HTML/CSS

SOFT SKILLS: Communication, Teamwork, Problem-Solving, Attention to Detail

EDUCATION

B. Sc, Biochemistry, University of Nigeria **2023**

- **4.1/5.0, Second Class Honours, Upper Division**

WORK HISTORY

Cybersafe Foundation - CyberGirls Fellowship **March 2024 – Present**

Position: SOC Analyst tier 1 Trainee

- Developed practical skills in network security, threat analysis, incident response, and vulnerability assessment.
- Performed root cause analysis for detected incidents using Splunk and Wireshark, contributing to system hardening efforts and preventing further breaches
- Developed playbooks for incident response, which reduced response time by 30%, ensuring swift containment of potential threats.
- Gained exposure to critical domains such as Cloud Security, DevSecOps, and Digital Forensics, strengthening incident-handling capabilities.

PROJECTS

1. **Incident Response Plan for Healthcare Organization (HIPAA Compliance)**

- Created and implemented an Incident Response Plan, ensuring compliance with HIPAA regulations and minimising risks to patient data.
- Collaborated with teams to define response strategies for ransomware and cyber threats, reducing potential attack surface by 20%

2. **Endpoint Network Forensics Using Wireshark and Network Miner**

- Performed deep packet inspections and traffic analysis to detect malicious activities and support incident investigations.
- Produced forensic reports used for further analysis and threat mitigation, strengthening overall endpoint security.

3. **In-depth Analysis of TCP/IP and IOS Models**

- Conducted a detailed analysis of vulnerabilities within the TCP/IP and IOS models, leading to recommendations for protocol enhancements.
- Provided security solutions that improved data flow efficiency and mitigated protocol-based attacks.