SODUNKE ABDULSAMOD

Cybersecurity Engineer | SOC Analyst | Information Security Analyst
Toronto, Ontario, Canada
+1 416 605 9983 | abdulsamodsodunke@gmail.com
LinkedIn

Professional Summary

Innovative and detail-oriented Cybersecurity Engineer with 4+ years of experience in designing, implementing, and maintaining cybersecurity systems. Proficient in application security, network security, and information security, with expertise in vulnerability assessment, security incident monitoring, and risk mitigation. Skilled in configuring and optimizing SIEM/SOC systems, endpoint security, and cloud security (AWS, Azure). Proven track record of reducing Mean Time to Detect (MTTD) by 20% and Mean Time to Respond (MTTR) by 25%. Strong knowledge of security protocols, encryption techniques, and frameworks such as NIST CSF, ISO 27001, and MITRE ATT&CK. Holds a Bachelor's degree in Computer Science and certifications including CompTIA Security+, CEH, and CISSP (in progress). Adept at leveraging analytical skills to identify, assess, and resolve complex security challenges in fast-paced environments.

Key Skills

Application Security: Secure coding practices, vulnerability scanning, penetration testing
Network Security: Firewalls, IDS/IPS, VPNs, Wireshark
Information Security: Data protection, encryption, DLP, CASB
Cybersecurity: Threat analysis, incident response, malware analysis
Vulnerability Assessment: Nessus, Qualys, risk assessment, mitigation strategies
Security Tools: Splunk, QRadar, Microsoft Sentinel, CrowdStrike, Carbon Black
Frameworks: NIST CSF, ISO 27001, MITRE ATT&CK
Scripting & Automation: Python, PowerShell, Bash
Cloud Security: AWS, Azure, CSPM, CWPP
Analytical Skills: Data analysis, root cause analysis, threat intelligence, risk evaluation

Soft Skills: Problem-solving, communication, collaboration

Professional Experience

Cybersecurity Engineer
SECURESPHERE FOUNDATION | Remote
Sep 2023 – Dec 2023

- **Designed and implemented application security measures, including secure coding practices and vulnerability scanning, reducing risks by 25%.**
- **Conducted vulnerability assessments using tools like Nessus and Qualys, identifying and mitigating 50+ high-priority vulnerabilities.**
- **Monitored and analyzed security incidents using Splunk and QRadar, leveraging analytical skills to reduce MTTD by 20% and MTTR by 25%.**
- **Configured and maintained network security systems, including firewalls, IDS/IPS, and VPNs, ensuring compliance with NIST CSF and ISO 27001.**
- **Collaborated with software engineering teams to integrate encryption techniques and improve information security controls.**

Cybersecurity Analyst
THEREDUSERS | Remote
Sep 2023 – Oct 2023

- **Evaluated and improved endpoint security controls using CrowdStrike and Carbon Black, mitigating 50+ high-priority incidents through analytical threat assessment.**
- **Conducted risk assessments and implemented security measures to protect digital assets, improving system efficiency by 25%.**
- **Monitored SIEM/SOC systems for potential threats, using analytical skills to ensure timely detection and response.**
- **Provided technical support and actionable solutions to clients, enhancing their understanding of network security states.**

Ethical Hacker
CFSS Cyber & Forensics Security Solutions | Remote
Aug 2023 – Sep 2023

- **Conducted penetration testing and malware analysis, integrating Indicators of Compromise (IOCs) into the incident response pipeline.**

Developed and implemented incident response playbooks for phishing and ransomware scenarios, reducing response times by 30%.
Partnered with IT teams to evaluate and improve security controls, using analytical skills to align solutions with business objectives.

Key Projects

Threat Analysis and Mitigation

Identified and analyzed potential threats in real-time, leveraging analytical skills to reduce MTTD by 20% and MTTR by 25%.
Conducted malware analysis and integrated IOCs into the incident response pipeline, improving threat intelligence.

SIEM/SOC System Optimization

Collaborated with AI teams to optimize automated features of the SIEM/SOC system, improving threat detection accuracy by 30%.
Monitored and maintained SIEM/SOC systems, using analytical skills to ensure timely detection and response to potential threats.

Customer Support and Solutions

Assisted customers in understanding their security network state, providing tailored solutions to enhance their security posture.
Developed and implemented incident response playbooks, improving response times by 30%.

Education

Bachelor of Computer Science
Olabisi Onabanjo University | Mar 2022 – Apr 2024
Graduated with Distinction (Top 10% of Class)
Relevant Coursework: Threat Analysis, Incident Response, SIEM/SOC Monitoring, AI-Automated Systems

---

Certifications

Certified Ethical Hacker (CEH)
CompTIA Security+
Certified Information Systems Security Professional (CISSP) – In Progress
Certified Information Security Manager (CISM) – In Progress

Languages

English: Native/Bilingual (Professional Communication, Documentation, and Technical Reports)
Arabic: Proficient (Intermediate Proficiency, able to communicate technically and document in Arabic)

Volunteer Experience

Cybersecurity Mentor | Cloud Mavins
Aug 2023 – Sep 2023

Mentored junior analysts in threat analysis, incident response, and SIEM/SOC monitoring.
Designed training programs to improve participants' understanding of AI-automated systems and cybersecurity principles.