# SODUNKE ABDULSAMOD

**Cybersecurity Engineer | Penetration Tester | Ethical Hacker | SOC Analyst | Information Security Specialist | AWS Cloud Security Engineer**
Abeokuta, Ogun State, Nigeria
+2349160599833 | [abdulsamodsodunke@gmail.com](mailto:abdulsamodsodunke@gmail.com) | [ [LinkedIn Profile](#) ]

## PROFESSIONAL SUMMARY

Innovative and detail-oriented Cybersecurity Engineer with 4+ years of experience in designing, implementing, and maintaining robust security systems and infrastructure. Expert in penetration testing, ethical hacking, vulnerability assessment, and AWS cloud security. Skilled in configuring and optimizing Security Operations Center (SOC) systems, SIEM solutions, and information security controls. Demonstrated success reducing Mean Time to Detect (MTTD) by 20% and Mean Time to Respond (MTTR) by 25% through advanced threat hunting and incident response techniques. Strong knowledge of security protocols, encryption techniques, and frameworks including NIST CSF, ISO 27001, and MITRE ATT&CK. Holds certifications in CompTIA Security+ and CEH with CISSP in progress. Adept at leveraging analytical skills to identify, assess, and resolve complex security challenges in enterprise environments.

## TECHNICAL SKILLS

- **Penetration Testing & Ethical Hacking**: Vulnerability scanning, exploit development, red team operations, OWASP methodology, social engineering
- **Security Operations (SOC)**: SIEM implementation (Splunk, QRadar, Microsoft Sentinel), threat hunting, incident response, security monitoring
- **Information Security**: Data protection, encryption, DLP, CASB, governance, risk & compliance
- **AWS Cloud Security**: AWS Security Hub, GuardDuty, CloudTrail, IAM, S3 security, VPC configuration, CSPM, CWPP
- **Vulnerability Management**: Nessus, Qualys, Burp Suite, risk assessment, mitigation strategies
- **Network Security**: Firewalls, IDS/IPS, VPNs, Wireshark, packet analysis, network traffic monitoring
- **Application Security**: Secure SDLC, static/dynamic code analysis, API security assessment
- **Security Frameworks**: NIST CSF, ISO 27001, MITRE ATT&CK, CIS Controls
- **Scripting & Automation**: Python, PowerShell, Bash, security automation workflows
- **Endpoint Security**: CrowdStrike, Carbon Black, EDR/XDR implementation

## 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 security risks by 25%
- Conducted comprehensive penetration tests and ethical hacking exercises against corporate infrastructure, identifying and remediating 50+ critical vulnerabilities
- Deployed and configured AWS cloud security controls including GuardDuty, Security Hub, and CloudTrail, ensuring compliance with industry standards
- Monitored and analyzed security incidents using Splunk and QRadar SIEM platforms, leveraging advanced analytics to reduce MTTD by 20% and MTTR by 25%
- Configured and maintained SOC infrastructure and 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 across the enterprise

## 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 penetration tests against AWS cloud environments, identifying and remediating security misconfigurations and access control vulnerabilities
- Performed information security risk assessments and implemented security measures to protect digital assets, improving system efficiency by 25%
- Monitored SOC/SIEM systems for potential threats, using analytical skills to ensure timely detection and response in a 24/7 operational environment
- Provided technical support and actionable security solutions to clients, enhancing their understanding of network security posture and threat landscape

## Ethical Hacker

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

- Conducted penetration testing, ethical hacking, and malware analysis, integrating Indicators of Compromise (IOCs) into the incident response pipeline
- Performed AWS cloud security assessments, identifying and remediating misconfigurations in IAM, S3, and VPC security settings

- Developed and implemented incident response playbooks for phishing and ransomware scenarios, reducing response times by 30%
- Established information security controls and protocols aligned with industry best practices
- Partnered with IT teams to evaluate and improve security operations controls, using analytical skills to align solutions with business objectives

# KEY PROJECTS

### Advanced Threat Hunting & Penetration Testing

- Conducted regular internal and external penetration tests against corporate infrastructure, identifying critical vulnerabilities before exploitation
- Identified and analyzed potential threats in real-time using SIEM tools, leveraging analytical skills to reduce MTTD by 20% and MTTR by 25%
- Performed ethical hacking exercises to validate security controls and identify weaknesses in the security posture
- Conducted malware analysis and integrated IOCs into the incident response pipeline, improving threat intelligence capabilities

### SOC & SIEM Implementation and Optimization

- Designed and deployed a comprehensive Security Operations Center (SOC) with integrated SIEM capabilities
- 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
- Implemented AWS CloudTrail and GuardDuty for cloud security monitoring and automated alerting

### AWS Cloud Security Architecture

- Designed and implemented comprehensive AWS security architecture incorporating Security Hub, GuardDuty, and CloudTrail
- Conducted security assessments of AWS environments, focusing on IAM policies, S3 bucket configurations, and VPC security groups
- Developed automation scripts for continuous monitoring and remediation of AWS security vulnerabilities
- Implemented AWS security best practices for data protection, access management, and compliance monitoring

# EDUCATION

**Bachelor of Computer Science**

**Olabisi Onabanjo University** | Mar 2022 – Apr 2024
*Graduated with Distinction (Top 10% of Class)*
*Relevant Coursework: Threat Analysis, Penetration Testing, Ethical Hacking, Incident Response, SIEM/SOC Monitoring, AWS Cloud Security, Information Security Management*

# CERTIFICATIONS

- Certified Ethical Hacker (CEH)
- CompTIA Security+
- Certified Information Systems Security Professional (CISSP) – In Progress
- Certified Information Security Manager (CISM) – In Progress
- AWS Certified Security – Specialty (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, penetration testing, ethical hacking, incident response, and SIEM/SOC monitoring
- Designed training programs to improve participants' understanding of AWS cloud security, AI-automated systems, and cybersecurity principles