

SODIQ ADEWALE BABAYEMI

CYBERSECURITY & IT PROFESSIONAL | CYBERSECURITY TRAINER | SOC | SECURITY OPERATIONS | NETWORK SECURITY

Nigeria | +234 814 888 9996 | sodiqadewalebabayemi@gmail.com | Remote, Hybrid & International Opportunities

PROFESSIONAL SUMMARY

Cybersecurity and IT professional with practical experience developed through AI Info Tech Limited, paid client engagements, cybersecurity training, technical research, and hands-on security laboratories. Experienced in cybersecurity education, SOC and security operations, security monitoring, network security, vulnerability assessment, ethical hacking, IT infrastructure, systems support, Windows Server, technical documentation, and practical lab development. Experienced in planning and delivering structured training through remote, hybrid, and practical learning environments, supporting learners with demonstrations, exercises, troubleshooting, and feedback. Currently pursuing a B.Sc. in Computer Science at the University of the People.

CORE COMPETENCIES

Cybersecurity Training & Facilitation • Curriculum / Lesson Development • Practical Lab Development • SOC Operations • Security Monitoring • SIEM • Log Analysis • Alert Triage • Incident Analysis • Vulnerability Assessment • Ethical Hacking • Security Testing • Reconnaissance • Enumeration • Network Security • Routing & Switching • VPN Monitoring • Firewalls • Network Troubleshooting • Windows Server • Linux • Systems Administration • IT Infrastructure • Virtualization • Threat Detection • Threat Analysis • MITRE ATT&CK; • Security Awareness • GRC Fundamentals • Risk & Compliance • Policy Documentation • Technical Documentation • Client Engagements • Learner Mentoring • Technical Communication

TECHNICAL TOOLS & TECHNOLOGIES

Splunk • Wazuh • Nmap • Metasploit • Wireshark • Kali Linux • Hack The Box • Cisco IOS • Cisco Packet Tracer • Sophos • ManageEngine • VMware • UniFi • Windows Server • Python • Scikit-learn • Git • GitHub • OWASP Juice Shop

PROFESSIONAL EXPERIENCE

AI Info Tech Limited — Founder / Cybersecurity & IT Consultant | Nigeria | January 2019 – Present

- Lead cybersecurity, IT, technical training, research, and client-facing technology engagements through AI Info Tech Limited.
- Plan, coordinate, and deliver cybersecurity and IT training covering SOC operations, defensive security, offensive security, GRC, network security, vulnerability assessment, and infrastructure security.
- Design and develop structured course content, lesson plans, practical exercises, demonstrations, laboratory scenarios, and supporting training documentation.
- Deliver instructor-led sessions and practical demonstrations, explain technical concepts clearly, answer learner questions, and provide guidance during hands-on exercises.
- Mentor learners through practical cybersecurity activities and support the development of troubleshooting, analytical, security-testing, and problem-solving skills.
- Develop practical security laboratories and learning environments using SIEM, network monitoring, vulnerability assessment, ethical hacking, and systems administration technologies.
- Develop technical documentation, research materials, security curricula, client deliverables, and structured technical solutions based on project requirements.
- Build and maintain professional client relationships while translating technical requirements into practical cybersecurity and IT solutions.
- Support applied projects involving fraud detection, security monitoring, risk analysis, network security, and digital-security awareness.
- Conduct authorized security work and document technical findings, methodologies, observations, and recommendations for client-facing delivery.

AI Info Tech Learning — Cybersecurity Trainer / Technical Educator | Nigeria | Training Function within AI Info Tech | 2019 – Present

- Deliver structured cybersecurity education through theory sessions, demonstrations, practical exercises, and guided laboratory activities.
- Prepare and organize learning materials, practical scenarios, exercises, and supporting documentation for different learner levels.
- Facilitate learner interaction, respond to technical questions, clarify difficult concepts, and provide practical guidance during training.
- Use tools including Splunk, Wazuh, Wireshark, Nmap, Kali Linux, and related technologies to demonstrate security concepts in controlled environments.

- Mentor learners in practical troubleshooting, analytical thinking, security operations, vulnerability assessment, and ethical-hacking methodologies.
- Review learner performance and adapt explanations, demonstrations, and exercises to improve understanding and practical competence.

SELECTED TRAINING ENGAGEMENTS

Fushure Consulting — Cybersecurity Trainer / Remote Training Consultant | Fully Remote | 1 September 2024 – November 2024

- Delivered cybersecurity training remotely through live virtual sessions for learners engaged by Fushure Consulting.
- Prepared and organized training content, lesson materials, demonstrations, practical exercises, and supporting learning resources for online delivery.
- Facilitated virtual classroom sessions, explained technical concepts, answered learner questions, and guided participants through practical activities.
- Adapted training delivery and demonstrations to a fully remote environment while maintaining learner engagement and structured session flow.
- Provided learner support and clarification during and after sessions, helping participants understand technical concepts and practical tasks.
- Maintained professional communication and training documentation associated with the engagement.

Immonex — Professional Ethical Hacking (Entry Level) Trainer | Hybrid | 4 February – 28 March 2025 | 8 Weeks

Schedule: Wednesdays (Theory) | Saturdays (Practical) **Trainer:** Sodiq Babayemi Adewale

- Delivered an 8-week Professional Ethical Hacking (Entry Level) training programme through a hybrid training format.
- Facilitated weekly theory sessions on Wednesdays and practical sessions on Saturdays, connecting conceptual learning with hands-on activities.
- Prepared and delivered instructional materials, demonstrations, practical exercises, and guided lab activities for entry-level ethical-hacking learners.
- Explained ethical-hacking concepts in a structured and accessible manner and supported learners during practical exercises.
- Provided hands-on guidance, troubleshooting support, learner feedback, and clarification throughout the training programme.
- Managed the transition between in-person and remote participation requirements inherent in the hybrid delivery format.
- Supported learner development by emphasizing responsible security practice, practical problem-solving, and controlled security testing.

SELECTED CLIENT / APPLIED PROJECT EXPERIENCE

Cybersecurity Lab Assessment — UK-Based Client | AI Info Tech Limited | Paid Client Engagement | Remote

- Delivered authorized, paid cybersecurity assessment work involving the Hack The Box Rapid and Liberty environments.
- Performed practical reconnaissance, enumeration, vulnerability identification, exploitation analysis, and privilege-escalation activities within authorized lab environments.
- Documented technical findings, methodologies, and security observations for client-facing delivery.
- Applied offensive-security techniques in controlled environments while maintaining the agreed project scope and authorization.

Adaptive Fraud Protection in a Rapidly Digitalised Payment Ecosystem — Research / Applied Project

- Developed a research and technical prototype exploring machine learning, behavioural analysis, and adaptive risk scoring for digital-payment fraud protection.
- Performed data exploration, preprocessing, class-imbalance analysis, model development, and evaluation using a public credit-card fraud dataset.
- Investigated and mitigated a data-leakage problem by applying SMOTE only to training data and evaluating the resulting model on held-out test data.
- Evaluated a LightGBM no-leakage model with reported fraud-class precision of 0.79, recall of 0.72, and F1-score of 0.75.

HANDS-ON CYBERSECURITY LABS

Hack The Box — Rapid & Liberty

- Practical authorized lab work covering reconnaissance, enumeration, vulnerability identification, exploitation methodology, privilege escalation, and attack-path analysis; completed as part of a paid UK client engagement.

SOC & Security Monitoring Labs

- Practiced SIEM/log analysis, alert investigation, threat detection, incident analysis, and Windows/Linux security telemetry.
- Applied Splunk, Wazuh, Wireshark, and related technologies in controlled training environments.

Offensive Security & Vulnerability Assessment Labs

- Practiced reconnaissance, network scanning, vulnerability assessment, web-security testing, and ethical-hacking methodologies in controlled environments.
- Used Kali Linux, Nmap, Metasploit, and OWASP Juice Shop to develop practical security-testing skills.

EDUCATION

University of the People — Bachelor of Science (B.Sc.), Computer Science | Currently Pursuing

- Building formal foundations in computer science, programming, computing systems, databases, mathematics, ethics, privacy, and security.

CERTIFICATIONS & PROFESSIONAL DEVELOPMENT

- Cisco CCNA
- Sophos Certified Engineer / Technician
- Microsoft Certified Professional / Microsoft Windows Server training
- Network+ / Security+ training
- ManageEngine Product Associate
- Ethical Hacking & Cybersecurity practical training

PUBLICATION & THOUGHT LEADERSHIP

Author — The Invisible War, Volume I: The Invisible Attacker | AI Info Tech Learning

- Cybersecurity-focused publication exploring offensive cybersecurity concepts, reconnaissance, ethical hacking, digital threats, and responsible security practice.

PROFESSIONAL PORTFOLIO

- GitHub: <https://github.com/sodiqbabayemi>
- YouTube: <https://www.youtube.com/channel/UCgEypwPHbrFfBMOIbP8qZjw>

TRAINING DELIVERY PROFILE

Experienced in remote, hybrid, and practical classroom delivery, with emphasis on structured lesson preparation, practical demonstrations, hands-on exercises, learner engagement, technical troubleshooting, mentoring, feedback, and development of practical cybersecurity skills.

Training evidence reflected in this CV includes ongoing cybersecurity training through AI Info Tech Limited, a fully remote Fushure Consulting training engagement (September–November 2024), and an 8-week hybrid Professional Ethical Hacking (Entry Level) programme with Immonex (4 February–28 March 2025).

CAREER TARGET

Seeking remote and international opportunities in SOC Analysis, Cybersecurity Analysis, Security Operations, Network Security, Vulnerability Assessment, GRC, IT Security, and Cybersecurity Training, with long-term progression toward senior cybersecurity leadership.