**Chinedu David Ikechukwu**

**SOC Analyst | Penetration Tester**

Email: chinedudavid.ng@gmail.com

Phone: +234 9072100854

GitHub: <https://github.com/chinedudavid-ng>

LinkedIn: [www.linkedin.com/in/chinedu-david-272134254](http://www.linkedin.com/in/chinedu-david-272134254)

Portfolio: <https://chinedudavid-ng.github.io/Portfolio/>

**PROFESSIONAL SUMMARY**

Dedicated SOC Analyst and Penetration Tester with hands-on experience in cybersecurity, threat detection, and vulnerability assessment. Skilled in leveraging cutting-edge tools and methodologies to identify, analyze, and mitigate security risks. Proven expertise in Splunk, SIEM solutions, and offensive security practices, complemented by strong problem-solving and communication skills. Passionate about safeguarding systems, networks, and data.

**KEY SKILLS**

- Penetration Testing: Vulnerability Assessment, Exploitation, Post-Exploitation, Reporting

- SOC Operations: Threat Monitoring, Incident Response

- SIEM Tools: Splunk,

- Scripting & Automation: Python

- Cybersecurity Tools: Metasploit, Burp Suite, Wireshark, Nessus, Nmap, Kali Linux

- Frameworks & Standards: MITRE ATT&CK, OWASP Top 10

- Compliance: GDPR, HIPAA

**PROFESSIONAL EXPERIENCE**

**Cybersecurity Intern**

Coscharis Medical - Lagos, Nigeria | 2024- 2025

- Performed initial vulnerability scans and assessments on medical equipment and corporate networks.

- Assisted in configuring Splunk dashboards for monitoring security events.

- Documented and analyzed cybersecurity policies to ensure regulatory compliance.

- Provided support during incident response by collecting and analyzing evidence.

**SOC Analyst (Hands-on Training)**

Hack The Box - Sherlock & Challenge Labs | Jan 2024– Present]

- Conducted incident investigations and threat hunting using Sherlock challenges on Hack The Box.

- Analyzed security logs, network traffic, and system artifacts to detect malicious activity.

- Utilized Splunk, Wireshark for log analysis and forensic investigations.

- Identified and reported Indicators of Compromise (IoCs), recommending remediation actions.

**EDUCATION**

BSc. in Computer Science with Statistics

University of Nigeria Nsukka- Enugu, Nigeria. | 2021 - 2025

**CERTIFICATIONS**

- Opswat: Introduction to critical infrastructure

- Udemy: Python programming language

**PROJECTS & ACHIEVEMENTS**

- Investigated cybersecurity incidents using Hack The Box Sherlock challenges, analyzing logs and identifying threats in a SOC environment, leveraging Splunk and security tools to detect anomalies..

- Web Application Penetration Testing: Identified and mitigated critical vulnerabilities (e.g., SQL Injection in client applications using Burp Suite and SQL Map

- Automation Scripts: Designed Python scripts to automate log parsing, saving [specific time or percentage] of analyst hours.

- Medical Device Security Assessment: Conducted a security review of IoT-connected medical devices, uncovering Unpatched Vulnerability and Configuration.

**TECHNICAL TOOLS**

- SIEM: Splunk

- Pentesting Tools: Metasploit, Burp Suite, Wireshark, Nessus, Nmap etc

- Programming Languages: Python(Scripting)

- Version Control: Git, GitHub

**REFERENCES**

Available upon request.