

NWODU ROBERT

IT SECURITY ANALYST | CYBERSECURITY & SOC OPERATIONS | DFIR

Nigeria (Remote) | +234 803 345 7468 | Chimuanyanwodu200@gmail.com
[linkedin.com/in/robertchimuanwodu](https://www.linkedin.com/in/robertchimuanwodu) | github.com/Robertnile | robertnile.github.io

PROFESSIONAL SUMMARY

Junior SOC Analyst with hands-on experience in threat detection, SIEM log monitoring, and incident response across a remote traineeship and five self-directed detection engineering lab cases. Proficient in **Splunk, Zeek, Velociraptor**, and **REMnux** — all work mapped to MITRE ATT&CK and documented on GitHub.

SELECTED SECURITY PROJECTS

Full case-study write-ups and live demos at robertnile.github.io · All source repositories at github.com/Robertnile

- **CASE-005:** AgentTesla JS Dropper Analysis — static/dynamic malware analysis on REMnux, MITRE mapped (T1027, T1047, T1547)
- **CASE-004:** DNS & HTTPS C2 Detection — six behavioral SPL detections across Zeek and Splunk for dnscat2 and Meterpreter
- **CASE-001:** Splunk SIEM Lab — 3-VM environment, four attack chains simulated, detected, and mapped to MITRE ATT&CK

TECHNICAL SKILLS

SIEM & Log Monitoring: Splunk Enterprise, Splunk Universal Forwarder, SPL Query Authoring, Zeek (conn/dns/http/ssl logs), Windows Event Logs, Syslog

Threat Detection & IR: Velociraptor, VQL Artifact Engineering, IOC Extraction, Incident Triage, PICERL IR Playbooks, Behavior-based Detection

Malware & Network Analysis: REMnux, Wireshark, Hybrid Analysis, VirusTotal, DNS/HTTPS C2 Detection, Dropper Deobfuscation

Vulnerability & SecOps: Nmap, Metasploit, GoPhish, Phishing Forensics (SPF/DKIM/DMARC), Kali Linux, Linux/Windows Admin

OS & Virtualisation: Linux (Ubuntu, Kali, REMnux), Windows 11, VirtualBox, multi-VM network configuration

Security Concepts: DNS tunneling, WMI-based evasion, behavioral vs. signature detection, brute force/privilege escalation detection

Scripting: Bash (lab automation), VQL (Velociraptor custom artifacts)

TECHNICAL PROJECTS & THREAT DETECTION LABS

CASE-005 — AgentTesla JavaScript Dropper Analysis

Jul 2026 – Present

github.com/Robertnile/case-005-agenttesla-js-dropper

- **Static analysis** of a 65,573-line obfuscated JS dropper on REMnux — identified junk switch/case obfuscation (T1027, T1497) designed to exhaust sandbox timeouts and evade AV.
- **Extracted and decoded** a Base64-encoded C2 URL disguised as a PNG image using grep and base64 — bypassed proxy content inspection (T1036, T1105).
- **Traced full WMI execution chain:** PowerShell assembled in memory → stored in environment variable → WMI spawns hidden process (ShowWindow=0) — mapped T1047, T1564.003, T1059.001.
- **Identified persistence** via Startup folder self-copy and LOLBin abuse (caspol.exe) — T1547.001, T1016.
- **Submitted to Hybrid Analysis and VirusTotal** — Threat Score 100/100, 31/60 engines flagged; dynamic analysis revealed a second payload URL missed during static analysis.

CASE-004 — Tunneling in Plain Sight: DNS & HTTPS C2 Detection

Jun 2026 – Present

github.com/Robertnile/Tunneling-in-Plain-Sight-Detecting-DNS-C2-with-Zeek-and-Splunk

- **Simulated DNS tunneling (dnscat2) and HTTPS C2 (Meterpreter)** — achieved root shell over both channels with no direct TCP/UDP.
- **Built six behavioral SPL detections** across both protocols — same methodology caught both C2 channels despite different tools, ports, and log sources.
- **Discovered and documented a critical Zeek/Splunk props.conf parsing bug** (FIELD_HEADER_REGEX) affecting all Zeek sourcetypes — now a required fix referenced in subsequent cases.

CASE-003 — Phishing Attack Simulation & Detection

Apr 2026 – Present

github.com/Robertnile/phishing-simulation-lab

- **Deployed full-stack phishing lab** (4 VMs: Kali, Ubuntu Server, Windows 11, Splunk) replicating real SOC attacker-vs-defender workflow using GoPhish and MailHog.
- **Wrote SPL detection queries and built a Phishing Attack Analysis dashboard** — mapped T1566.002, T1056.003, T1071.001; performed email header forensics (SPF/DKIM/DMARC).

CASE-002 — Velociraptor Threat Hunting & DFIR Lab

Mar 2026 – Present

github.com/Robertnile/velociraptor-threat-hunting-lab

- **Deployed Velociraptor across Windows 11 and Ubuntu 24.04** — simulated 11 real-world attack techniques including credential dumping, lateral movement, and C2 communication.
- **Authored custom VQL artifacts** for each technique — demonstrating detection engineering capability beyond default built-in queries.

CASE-001 — Splunk SIEM Lab: Metasploitable3 Attack Detection

Feb 2026 – Present

github.com/Robertnile/splunk-metasploitable-lab

- **Built 3-VM SIEM environment** (Splunk, Kali, Metasploitable3) with real-time auth.log/syslog ingestion and Zeek for network-level visibility.
- **Simulated four attack chains** — Nmap recon (T1046), SSH brute force (T1110.001), reverse shell C2 (T1571), privilege escalation (T1136.001) — wrote SPL detections and real-time alerts for all four.
- **Authored four IR playbooks (PB-001–004)** following PICERL framework; built a Linux Account and Privilege Monitoring dashboard.

WORK EXPERIENCE

SOC Analyst Trainee | Luke Tech Limited — Canada (Remote)

Oct 2025 – Present

- Monitored security telemetry and performed alert triage to support threat detection and response readiness across remote SOC operations.
- Investigated suspicious endpoint activity and validated network IOCs against known threat indicators for escalation decisions.
- Documented investigation findings and escalated confirmed security events using structured incident response protocols.

IT Support Technician | Edulinks Business Ventures — Nigeria

Feb 2023 – May 2025

- Managed system administration, hardware/software troubleshooting, and user identity management for organizational network users.
- Maintained network security standards, system patches, and firewall rules to support operational continuity.

CERTIFICATIONS & TRAINING

CompTIA Security+ | In Progress — Target: October 2026

ISC2 Certified in Cybersecurity (CC) | In Progress — Target: November 2026

TryHackMe SOC Level 1 Learning Path | In Progress

PORTFOLIO

Full case-study write-ups and live project demos at robertnile.github.io. All source repositories at github.com/Robertnile — each includes full documentation, MITRE ATT&CK mapping, detection queries, and remediation guidance.