Gideon Opukeme

Aberdeen, Scotland, UK | opukemegideon@gmail.com | GitHub | LinkedIn | Portfolio

PROFESSIONAL SUMMARY

Security engineer focused on detection engineering, AI security, and adversarial testing. Builds Sigma rules mapped to MITRE ATT&CK, engineers LLM proxies tested against 62 adversarial cases, and develops open-source threat detection tooling. Junior Security Engineer at Handi Digital Solutions while completing an MSc in Cyber Security at the University of Aberdeen.

EXPERIENCE

Junior Security Engineer Jul 2026 – Present

Handi Digital Solutions (tryhandi.com) Lagos, Nigeria

- First security hire at an early-stage service marketplace. Implementing application security controls—input validation, API authentication, data encryption—across iOS, Android, and web platforms handling user PII and payment data.
- Conducting code reviews and vulnerability assessments across the TypeScript/Node.js backend and React Native mobile applications, prioritising and driving remediation of security findings with the engineering team.

IT Support Aug 2025 – Aug 2026

Hendrique Consultants Limited Abuja, Nigeria

- Provided day-to-day IT support for a consulting firm: troubleshooting hardware and software faults, managing user access and system file organisation, and coordinating meetings. Streamlined routine IT workflows, improving staff productivity.

SECURITY PROJECTS

Detection Engineering Lab github.com/Gideon145/detection-engineering-lab

Sigma · MITRE ATT&CK · Elastic Stack · Incident Response

- Developed 10 Sigma detection rules covering 12 MITRE ATT&CK techniques across execution, credential access, lateral movement, and persistence for Windows and Active Directory environments.
- Wrote a complete incident response report tracing a full attack chain—credential phishing → BloodHound reconnaissance → Kerberoasting → PsExec lateral movement → LSASS dump → domain controller compromise—with root cause analysis and post-incident detection improvements. Reduced false positives from 94 alerts/day to 3 through context-aware filter tuning.

LLM Prompt Injection Firewall github.com/Gideon145/llm-prompt-firewall

Python · FastAPI · OWASP LLM Top 10 · AI Red-Teaming

- Built an HTTP proxy that intercepts LLM API requests in real time, blocking prompt injection, jailbreak, and data extraction attacks before they reach the model. Detection pipeline uses 30+ signatures across 9 attack categories, 7 heuristic analysers (entropy, encoding ratio, instruction deviation, delimiter density), and an evasion-resistant normalisation layer.
- Achieved 100% detection rate with zero false positives across 62 adversarial test cases and 8 benign prompts. Paired the firewall with InjectionForge, a genetic algorithm fuzzer that discovered 7 novel LLM guardrail bypass techniques including zero-width injection, Unicode homoglyph substitution, and leet-speak encoding.

Open-Source Detection Research

YARA · Snort/Suricata · Sigma · Malware Analysis

- Built a Mirai detection toolkit: 5 YARA rules targeting ARM, MIPS, and x86 binaries, 4 Snort/Suricata network signatures for C2 beaconing and DDoS patterns, a 12-bot C2 traffic simulator, and an IoT credential scanner covering 62 Mirai default credentials. Also authored Mirai C2 heartbeat and telnet brute-force detection rules in Sigma format. github.com/Gideon145/mirai-detector

EDUCATION

MSc Cyber Security, University of Aberdeen In Progress

BSc Computer Science, Western Delta University 2018 – 2022 · 2.1

Cybersecurity Certificate, University of Maryland 2025

CERTIFICATIONS & AWARDS

Google Cybersecurity Certificate (2025) | Fortinet Certified Fundamentals + NSE 3 (2026) | Cisco Intro to Cybersecurity (2025)

Award: OKX Build X Season 2 — 3rd Place, X Layer Arena — Parry Protocol, autonomous DeFi protection agent

TECHNICAL SKILLS

Detection & SIEM: Elastic Stack, Sigma, YARA, Snort/Suricata, MITRE ATT&CK | **Languages:** Python, TypeScript, SQL, Solidity

Security Domains: Threat Detection, Incident Response, AI/LLM Security, Malware Analysis | **Platforms & Tools:** Docker, FastAPI, Linux (Kali/Ubuntu), Git