Peter Abiya

Cybersecurity Engineer | Detection Engineering | AI Security

abiyapeter01@gmail.com +2348103930730 Asaba, Delta State Nigerian
linkedin.com/in/peter-abiya

Profile

Cybersecurity Engineer with hands-on experience in security operations, vulnerability assessment, security engineering, and web security. Skilled in Wazuh SIEM, Linux, networking, and web technologies, with experience supporting security monitoring, incident response, and security assessments. Passionate about vulnerability research, detection engineering, and building automated security solutions to improve organizational security posture.

Professional Experience

2026
Remote

EXPADOXLAB, *Security Engineering Intern*

- Designed and implemented a comprehensive **STRIDE threat model** for **SecOpsAI**, identifying 14 threats across six categories with **MITRE ATT&CK** mappings, ownership assignments, and mitigation tracking before development began, following **Security by Design** principles. Led the security architecture by producing context diagrams, trust-boundary data flow diagrams, Architecture Decision Records (ADRs), and a MITRE ATT&CK Navigator layer.
- Contributed as a **DevOps Engineer** on **SecOpsAI**, establishing the project structure, configuring the Docker Compose stack (Kafka, PostgreSQL, MLflow, Grafana, Prometheus), securing environment variable management, and supporting the shared development workflow across four engineering teams.
- Built the **SOAR automation layer** for **ShieldFlow**, developing automated playbooks for secret exposure, critical CVEs with live NVD enrichment, and OWASP DAST findings, alongside a secure webhook server with Bearer token authentication and SHA-256-based alert deduplication.
- Engineered **FireOps**, a centralized threat visibility platform using **Wazuh SIEM**, **Suricata IDS**, **AWS CloudTrail**, Docker, and **Tailscale VPN**, enabling real-time detection of SSH brute-force attacks, privilege escalation, and network reconnaissance with automated email alerting. Also remediated credential exposure by replacing hardcoded secrets with secure environment variable management.
- Contributed to **adversarial AI security** by hardening an **XGBoost** intrusion detection model trained on the **CICIDS2017** dataset using **IBM Adversarial Robustness Toolbox (ART)**, evaluating model resilience through pre- and post-hardening performance analysis.

2026
Remote

BINCOM DEVELOPMENT CENTER, *Cybersecurity Intern*

- Participate in hands-on cybersecurity training focused on real-world security operations and governance practices
- Assist with vulnerability assessments, risk analysis, and security control evaluations
- Contribute to security documentation aligned with ISO 27001 and information security management practices
- Support incident response simulations and threat analysis exercises
- Collaborate with engineering and product teams to understand secure development practices

2024 Sep – 2025
Nigeria

SEcybersafe, *Technical Writer*

- Create clear and concise technical content on cybersecurity and online safety.
- Collaborate with experts to simplify technical information for a broader audience.
- Research and document emerging cyber threats, online scams, and security best practices.
- Assist in developing educational materials to promote cybersecurity awareness.

2023 – 2024

Hagital Consulting Ltd., *Cybersecurity Analyst Intern*

2022 **ST. BARTHOLOMEW'S COMPUTER INSTITUTE, BENIN,**
Branch Manager and Computer Operator

- Oversaw branch operations, ensuring efficiency in daily administrative and inventory-related activities.
- Managed and maintained inventory records, ensuring proper documentation of office supplies.
- Trained students in computer operations, including Microsoft Office Suite (Word, Excel, PowerPoint) and office software applications.
- Provided guidance and supervision to trainees, ensuring they developed strong computer literacy and data management skills.
- Maintained accurate records of incoming and outgoing items using MS Excel.
- Assisted in administrative tasks and ensured smooth office workflow.

2020 **DELTA STATE INNOVATION HUB, ASABA,** *Web Developer & Instructor*

Education

2018 **B.SC. PHARMACOLOGY,** *DELTA STATE UNIVERSITY ABRAKA, NIGERIA*

Projects

1. Threat Visibility & Security Monitoring Platform (FireOps Systems)

- SIEM deployment
- Detection engineering
- Cloud log monitoring
- IDS integration
- MITRE ATT&CK
- Incident response
- Alerting
- Threat detection

2. ShieldFlow – AppSec Pipeline & SOAR Automation Platform

- Security automation
- SOAR
- Vulnerability management
- DevSecOps
- Security orchestration

3. WannaCry Malware Behavior Analysis

- Malware analysis
- IOC development
- Threat intelligence
- Forensics

4. IoT Firmware Security Analysis

- Reverse engineering
- Vulnerability assessment
- Security research

5. Project Ghostwire

- Threat emulation
- Detection
- Network forensics
- Defensive engineering

6. Threat Visibility & Security Monitoring Platform, *FireOps Systems*
Deployed enterprise-grade Wazuh SIEM on Docker, connected six team endpoints via Tailscale VPN, integrated Suricata IDS and AWS CloudTrail. Simulated and detected SSH brute force (T1110), privilege escalation (T1548), and network reconnaissance (T1046). Built custom detection rules mapped to MITRE ATT&CK and configured automated email alerting via Gmail SMTP relay through Postfix.
Wazuh, Suricata, Elasticsearch, Kibana, Docker, Tailscale, AWS CloudTrail, Python, Postfix

Technical Skills

Security Operations & Monitoring (Security Operations Center (SOC) | Security Monitoring | Threat Detection | Event Correlation | Log Analysis | Alert Investigation | Incident Triage | MITRE ATT&CK Mapping)
Threat Detection & Incident Response (Incident Response | Threat Hunting | IOC Identification | Attack Simulation | Security Event Investigation | Network Forensics | Malware Analysis | Root Cause Analysis)
Vulnerability Management & Security Assessment (Vulnerability Assessment | Security Control Evaluation | Risk Assessment | Web Application Security Testing | OWASP Top 10 | Access Control Analysis | Threat Modeling | Security Architecture Review)
Cloud Security (AWS IAM | AWS CloudTrail | Cloud Log Monitoring | Identity & Access Management | Least Privilege Principles)
Networking & Infrastructure (TCP/IP | DNS | HTTP/HTTPS | VPN Technologies | Network Security Monitoring | Firewall Concepts | IDS/IPS Technologies)
Operating Systems (Windows | Linux (Ubuntu, Kali Linux))
Security Tools (Wazuh SIEM | Suricata IDS | Wireshark | Procmon | Regshot | Binwalk | Firmwalker | John the Ripper | Checksec | Nmap | Hydra | Burp Suite | OWASP ZAP | Trivy | Semgrep | Gitleaks)
Scripting & Automation (Python | GitHub Actions | Security Automation | SOAR Concepts | Docker)
Compliance & Governance (ISO/IEC 27001 | ISO 22301 | ISO 31000 | ISMS | NDPR Awareness | Security Documentation | Technical Reporting)

Certificates

Foundations of Cybersecurity: Coursera

ISO-31000:2018 (RISK MANAGEMENT) FOUNDATION: Standards & Best Practice

ISO/IEC 27001: 2022 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) FOUNDATION: Standards & Best Practice

ISO/IEC 27032:2023 GUIDELINES FOR CYBERSECURITY FOUNDATION: Standards & Best Practice

ISO 9001:2015 QUALITY MANAGEMENT SYSTEM (QMS) FOUNDATION: Standards & Best Practice

ISO 22301:2019 BUSINESS CONTINUITY MANAGEMENT SYSTEMS (BCMS) FOUNDATION: Standards & Best Practice

CERTIFICATE IN CYBERSECURITY: Hagital Consulting

English For IT 1: Cisco Networking Academy

English For IT 2: Cisco Networking Academy

Introduction to Prompt Engineering for Generative AI: LinkedIn Learning

Build Your Generative AI Productivity Skills with Microsoft and LinkedIn: LinkedIn Learning

Generative AI Skills for Creative Content: Opportunities, Issues, and Ethics: LinkedIn Learning

Excel with Copilot: AI-Driven Data Analysis: LinkedIn Learning

Copilot in PowerPoint: From Prompt to Presentation: Project Management Institute

AI Productivity Hacks to Reimagine Your Workday and Career: Project Management Institute

Declaration

References available upon request.