NARH PHINEHAS TETTEH

LinkedIn
Github
Email: phinehastettehnarh@gmail.com
Mobile: +233 504927804

SUMMARY

Security Engineer experienced in penetration testing, vulnerability management, and security operations. Skilled at identifying exploitable weaknesses in web applications and infrastructure and working with engineering teams to implement practical remediation. Experienced supporting governance and compliance initiatives and strengthening organizational security posture.

EDUCATION

Accra Technical University Accra, Ghana.
Bachelor of Technology in Cyber Security Jan 2022 - Dec 2025
GPA: 4.13

SKILLS SUMMARY

- **Languages:** Python, C#, JavaScript, Go.
- **Libraries:** Pandas, NumPy, sqlite3, logging, os, socket, subprocess, Matplotlib.
- **Security Tools:** Burp Suite, Wireshark, Metasploit, Nmap, Nessus, SAST, DAST.
- **Operations:** SIEM, EDR, XDR, SOC, DevSecOps.
- **Methodologies:** OWASP Top 10, Threat Modeling, CVSS, MITRE ATT&CK.
- **Soft Skills:** Technical Communication, Risk Analysis, Cross-functional Collaboration, Documentation.

WORK EXPERIENCE

APPLICATION SECURITY ENGINEER | ACS Sep 2025 - Current

- Supported ISO 27001:2022 certification efforts through Stage 1 and Stage 2 ISMS audits, drafting internal security policies and adhering to Annex controls to achieve certification.
- Conducted web application penetration testing using Burp Suite and manual techniques, identifying authentication bypass and injection vulnerabilities across production portals.
- Coordinated with DevOps to remediate security incidents and vulnerabilities in staging & production environments.
- Hardened nginx web servers by implementing security headers and managed endpoint protection via Microsoft Intune and M365 Defender application controls.
- Developed vulnerability trackers for centralized reporting and findings management; delivered DMARC configuration training to enhance email security posture.

SECURITY ANALYST | EITBS Oct 2022 - Nov 2024

- Executed vulnerability assessments and penetration testing across 5+ systems and endpoints using Nessus and manual techniques, identifying and driving remediation of 7 critical vulnerabilities to reduce attack surface exposure.
- Administered endpoint protection platforms (Acronis, Symantec) and coordinated security awareness initiatives via KnowBe4, achieving a 47% improvement in phishing resilience metrics across the organization.
- Led technical evaluation for managed SOC provider selection, defining requirements for threat detection and incident response capabilities projected to reduce mean time to respond by 70%.
- Performed application security assessments to support consolidation of 10+ high-resource applications onto centralized infrastructure, ensuring proper resource allocation and reducing server costs by 25%.
- Authored and presented AI risk assessment to senior leadership, initiating a cross-functional task force to evaluate emerging technology threats and adoption strategies.
- Delivered security hardening for 4 endpoints to organizational baseline standards and conducted security awareness training for 20+ employees on threat identification and response protocols.

PROJECTS

Cisco Networking Topology | Link — February 2023

- Architected and deployed five network topologies including enterprise campus (100+ concurrent devices), state agency, and residential environments, implementing defense-in-depth controls.
- Engineered perimeter and internal security controls including firewall rule sets, IPsec VPN tunnels, WPA2/WPA3 encryption, and role-based access controls to enforce least-privilege principles.
- Configured and validated core infrastructure (Cisco 2901 routers, 3560-24PS multilayer switches, 3702i access points) and heterogeneous endpoints, achieving 98% uptime against defined SLAs.

Penetration Testing Projects | Link — October 2024

- Exploited CVE-2011-2523 (vsftpd v2.3.4 backdoor) to achieve remote code execution, documenting attack chain and recommending version upgrade and network segmentation controls.
- Identified and exploited authentication bypass vulnerability in OpenSSH 4.7p1, demonstrating risk of unpatched legacy systems and quantifying exposure impact.
- Produced detailed penetration test reports including proof-of-concept exploits, CVSS scoring, remediation priorities, and compensating controls for stakeholder review.

PROFESSIONAL CERTIFICATES

CompTIA Security+ (CompTIA) — 2026

- Validated core security competencies in threats, vulnerabilities, architecture, implementation, and incident response aligned to industry baseline standards.

Cyber Ops Associate (Cisco) — Feb 2024

- Validated competencies in security monitoring, log analysis, incident triage, and threat intelligence within SOC environments.

AWS Certified Cloud Practitioner (AWS) — Feb 2025

- Demonstrated understanding of AWS shared responsibility model, cloud security controls, and architecture best practices.

Information Technology Infrastructure Library (ITIL) — April 2024

- Applied IT service management principles to align security operations with business continuity and risk management objectives.

CCNA (Cisco) — May 2024

- Certified in network infrastructure security, routing protocols, switching, and network access control implementation.

ISO 27001:2022 Lead Auditor (Mastermind) — Feb 2026

- Qualified to plan, conduct, and lead information security management system audits in accordance with ISO/IEC 27001:2022 auditing guidelines.

TECHNICAL TRAININGS

Certified Red Team Operations Management (CRTOM) — Dec 2025

Led red team operations, aligning adversary emulation with enterprise risk and detection engineering.

Certified Phishing Prevention Specialist (CPPS) — Dec 2025

Designed phishing simulations and mitigation programs to reduce social engineering attack surface.

API Penetration Testing (APIsec University) — May 2026

Assessed REST and GraphQL API security, identifying authentication flaws, BOLA/BFLA, rate-limiting gaps, and injection vectors through structured API-specific testing methodologies.

Data Security (GIZ) — Sep 2025

Implemented data protection controls across classification, encryption, DLP, and compliance domains.

Zscaler Technical Associate (Zscaler) — Jul 2025

Deployed Zero Trust Network Access (ZTNA) and Secure Service Edge (SSE) architectures using Zscaler.

Threat Hunting (Security Blue Team) Apr 2024

Conducted proactive threat hunts using log analysis, ATT&CK mapping, and anomaly detection.

Vulnerability Management (Security Blue Team) Apr 2024

Managed vulnerability lifecycle, prioritizing remediation by CVSS, exploitability, and business impact.

Digital Forensics (Security Blue Team) Mar 2024

Performed forensic investigations, evidence acquisition, timeline analysis, and incident reconstruction.

Penetration Testing (IT Masters) Oct 2023

Executed web, network, and application penetration tests with risk-ranked remediation reporting.

Risk Management (PwC) May 2023

Applied enterprise risk methodologies aligned with ISO 27001 and regulatory requirements.

Machine Learning (Cognizant) Jun 2023

Built supervised and unsupervised models for anomaly detection and predictive analytics.