DAVID SIAW-DARFOUR

+233 54 714 1961 | dvdsiaw@gmail.com
LinkedIn: linkedin.com/in/david-darfour

Cybersecurity Analyst | Security Operations | Threat Monitoring | Vulnerability Management

PROFESSIONAL SUMMARY

Certified cybersecurity professional with hands-on expertise in vulnerability management, penetration testing, incident detection and response, and endpoint security across enterprise networks. Proficient in reviewing, analysing, and investigating security events, performing incident triage, conducting vulnerability assessments, and managing identity and access security using industry-leading tools such as Wazuh, Snort, OpenVAS, Nessus, Kali Linux, and Microsoft Security solutions. Well-versed in nationally recognized certifications including eJPT, CEH, CompTIA Security+, Network+, Cloud+, A+, and ISC² Cybersecurity credentials. Strong analytical and problem-solving skills, focused on building cyber-resilient organizations by enhancing threat visibility, deploying preventive controls, and ensuring robust security governance.

CORE TECHNICAL COMPETENCIES

- Security Operations & Monitoring

SIEM Monitoring (Wazuh), Security Event Analysis, Incident Triage & Threat Detection, Windows Event Log Analysis

- Vulnerability Management

OpenVAS Vulnerability Scanning, Nessus Security Assessments, CVSS Risk Scoring & Prioritization and Security Misconfiguration Detection

- Penetration Testing & Ethical Hacking

Kali Linux, Nmap Network Reconnaissance, Metasploit Framework, Web Application Security Testing

- Identity & Access Security

Active Directory Administration, Microsoft Entra ID, Identity Lifecycle Management, Privileged Access Controls

- Cloud & Endpoint Security

Microsoft 365 Security Administration, Microsoft Intune Endpoint Management, Multi-Factor Authentication (MFA) & Endpoint Compliance Monitoring

- Networking & Infrastructure Security

TCP/IP Networking, Routing & Switching, Firewall Fundamentals and Network Segmentation & Defense.

PROFESSIONAL EXPERIENCE

Improtech – Accra, Ghana
Cybersecurity Instructor (Security+ & CySA+) **October 2024-Present**

- Delivered structured training on threat detection, vulnerability management, and incident response aligned with CompTIA Security+ and CySA+ objectives.
- Designed and facilitated hands-on labs simulating brute-force attacks, log analysis, and SIEM-based alert investigation to strengthen practical defensive skills.
- Guided students in interpreting vulnerability assessment reports and applying remediation strategies based on risk severity.
- Introduced log correlation techniques using real-world attack scenarios to enhance analytical and incident triage capabilities.

Provided mentorship and technical guidance to learners, improving their readiness for cybersecurity certifications and entry-level SOC roles.

Sylversys Consulting Ltd – Accra, Ghana
Help Desk / IT Security Intern **May 2025-November 2025**

- Supported centralized management of endpoints by configuring and deploying endpoints for the company using Microsoft Intune for strong compliance to device security.
- Administered identity provisioning for the users and role-based access controls for users using Active Directory and Microsoft Entra ID, thus contributing to security governance of identity.
- Supported resolving incidents related to failed authentication attempts and access denial incidents, able to investigate cases and expedite their resolution, while minimizing impact on operations through timely response.
- Ensured compliance with Microsoft 365 security policies, I supported the enforcement of security policies (MFA implementation, User Access Reviews and Permissions Audits) and helped in supporting audit trails.
- Identified suspicious activity in the system logs and authentication events was accomplished through the analysis of system logs and authentication events, while escalating potential threats as they were identified.
- Provided technical support to users in regard to security issues, while ensuring compliance with internal security standards and all compliance requirements.

Key Achievements

- Founded the standardization of the deployment and configuration methods for managed devices, thereby increasing the overall security posture of the endpoints.
- Delivered secure access controls for identity management and better authentication protocols thus enhancing the strength of identity management with industry best practices in identity management.

2nd Generation IT Institute – Accra, Ghana **November 2023-July 2025**
Network Instructor

- Delivered training on routing and switching concepts, VLAN implementation, subnetting, and LAN/WAN architecture.
- Supervised practical labs involving Cisco IOS configuration, including Access Control Lists (ACLs) and network segmentation techniques.
- Integrated packet analysis using Wireshark to help students understand network traffic behaviour and identify anomalies.
- Guided students in troubleshooting network issues and applying best practices for secure network design.

Key Achievements

- Improved students' practical networking skills through hands-on lab sessions and real-world configuration scenarios.
- Strengthened foundational knowledge in network security concepts aligned with industry standards.

Eistec Technologies – Accra, Ghana
Cybersecurity Intern **August 2024 – January 2025**

- Performed vulnerability assessments of WordPress-based environments to find security misconfigurations and risk of exposure.
- Performed vulnerability scanning of networks/software configurations using OpenVAS/Nessus, reviewing results and categorizing remediation tasks according to severity level.
- Documented security vulnerabilities/recommendations for remediation to assist with improving how well systems are hardened.
- Assisted in evaluating Web application security posture in order to decrease vulnerable surface area and improve ability to mitigate common type attacks.
- Assisted with documenting and reporting on vulnerability assessment results ensuring that risk information was communicated accurately to technical teams.

Key Achievements

- Strengthened the security posture of client web applications by identifying critical vulnerabilities and recommending actionable remediation steps.
- Improved efficiency of vulnerability management processes through structured documentation and clear risk communication to technical teams.
- Contributed to enhanced awareness of web application security risks among internal stakeholders and clients.
- Supported successful mitigation of high-risk vulnerabilities, reducing potential exposure and aligning with industry best practices.

Palm University College – Accra, Ghana **FEBRUARY 2023 – OCTOBER 2023**
ASSISTANT LECTURER

- Delivered undergraduate lectures on IT concepts, computing fundamentals, and foundational cybersecurity principles.
- Maintained and optimized the university's WordPress site, enhancing digital presence and user experience.
- Provided academic leadership and mentorship within the IT department, supporting student development and curriculum delivery.
- Integrated practical labs and applied learning exercises to reinforce theoretical concepts and improve technical competency.

Key Achievements

- Boosted student engagement and comprehension through hands-on, practical-based teaching methods.
- Enhanced students' preparedness for IT and cybersecurity career pathways through mentorship and applied learning initiatives.
- Improved the university's digital footprint via optimized WordPress site management.

WAS Institute – Accra, Ghana **SEPTEMBER 2021 – OCTOBER 2022**
CCNA Trainer (Part-Time)

- Delivered training in Cisco CCNA curriculum, focusing on routing, switching, and LAN/WAN design.
- Guided students through Cisco IOS labs and practical configuration exercises.
- Prepared students for CCNA certification exams with real-world lab practice.

Key Achievements

- Strengthened students' practical networking and configuration skills through lab-driven instruction.
- Improved CCNA exam readiness with structured hands-on exercises and mentorship.

NIIT Openlabs – Accra, Ghana **SEPTEMBER 2021 – OCTOBER 2022**
Network Instructor

- Delivered training on computer hardware troubleshooting, networking fundamentals, and operating systems.
- Designed and facilitated hands-on labs focused on IP addressing, LAN setup, and network troubleshooting.
- Guided students in diagnosing hardware and connectivity issues using structured troubleshooting methodologies.
- Introduced foundational cybersecurity concepts within networking and system administration topics.

Key Achievements

- Improved student competency in troubleshooting and networking through practical, lab-driven instruction.
- Established structured learning approaches that strengthened foundational IT and support skills.

National Banking College – Accra, Ghana **September 2020 – September 2021**
National Service Personnel

- Performed data entry and maintained accuracy in institutional reporting.
- Supervised library operations, supporting both physical and digital resources.
- Applied Microsoft Office Suite for documentation and information management.

Key Achievements

- Maintained high accuracy in data management and reporting processes.
- Supported smooth library operations for students and staff, improving access to resources.

CYBERSECURITY LABS & PROJECT EXPERIENCE

Wazuh SIEM Deployment & Threat Monitoring

- Implemented centralized SIEM system (Wazuh) with Windows Event Logs and other systems to gather and analyze security incidents from multiple sources.
- Configured log correlation rules to detect brute-force attacks, unauthorized entries, and abnormal authentication patterns.
- Reviewed Windows Event Logs and system alerts for potential indicators of compromise and suspicious user activity.
- Enhanced visibility into current threats with centralized monitoring and alert management.

Snort Intrusion Detection System (IDS) Implementation

- Built a Snort IDS in a simulated lab to validate malicious traffic detection.
- Created custom Snort IDS rules to detect reconnaissance and port scanning, as well as other suspicious network activity.
- Completed packet analysis to validate detection accuracy and enhance intrusion detection capabilities.

Penetration Testing Lab

- Used Nmap for network reconnaissance and enumeration to identify exposed services and other attack surfaces to secure those areas of vulnerability.
- Simulated controlled attacks on web applications in laboratory settings to better understand potential exploitation techniques and their associated weaknesses.
- Conducted privilege escalation testing on systems for post enumeration analysis of scenarios in which those systems may become compromised.

Vulnerability Assessment Project

- Conducted comprehensive vulnerability scanning using OpenVAS and Nessus across simulated environments.
- Analysed security reports and prioritized remediation based on CVSS risk ratings.
- Recommended security hardening controls to mitigate identified vulnerabilities and strengthen system defense.

PORTFOLIO

SOC & Cybersecurity Projects: https://github.com/BlackRain12/SOC-Portfolio

- Showcases hands-on labs, SIEM deployments, IDS configurations, vulnerability assessments, and penetration testing projects.
- Demonstrates applied security operations, threat monitoring, and incident response skills.

CERTIFICATIONS

- eLearn Security Junior Penetration Tester (eJPT)
- Certified Ethical Hacker (CEH)
- CompTIA Security+
- CompTIA Network+
- CompTIA Cloud+
- CompTIA A+
- ISC² Certified in Cybersecurity (CC)

EDUCATION

- **Master of Science (MSc), Information Technology**

Accra Institute of Technology — 2025

- **Bachelor of Science (BSc), Information Technology** — 2019

Ghana Technology University College

REFERENCE: Available upon request.