Amos AKOGBE

aakogbe@andrew.cmu.edu | amosakogbe@gmail.com
(+250) 796897683 | (+229) 0194409664
https://www.linkedin.com/in/amos-akogbe-744954234/ | https://bit.ly/cyberintel4

SUMMARY

Certified Cybersecurity Analyst with hands-on experience in SOC operations, incident response, penetration testing and technical documentation, proficient in developing Incident Response Playbooks, tracking security metrics (SLA/KPI), and creating awareness materials for diverse audiences, translating complex technical findings into clear, business focused insights to support decision-making and strengthen organizational resilience is my premiere goal seeking an internship as a Security Engineer or a Threat Intelligence Analyst.

EDUCATIONAL BACKGROUND

Master of Science in Information Technology **August 2025 – May 2027**
Carnegie Mellon University, Africa
Concentration: Cybersecurity, Cyber Threat Intelligence and DFIR

Bachelor of Information Technology Security **September 2021 – November 2024**
University of Abomey-Calavi, Abomey-Calavi, Benin
GPA: 3.7/4
Concentration: Information Technology, Cybersecurity and Information Security

PROFESSIONAL EXPERIENCE

Cybersecurity Compliance Apprenticeship **March 2025 – June 2025**
Cyber Research Link, Washington, USA (Remote)

- Produced a keynote presentation on Threat Intelligence and its importance in the present cybersecurity landscape.
- Produced TED Talks study papers on cybersecurity and AI & the role of cybersecurity in avoiding cyberattacks.
- Completed a vulnerability assessment for a simulated firm using OpenVAS for vulnerability identification and Microsoft Sentinel for Threat analysis.

Pentester Intern **February 2025 – June 2025**
Bodah Logistics, Abomey-Calavi, Benin

- Assessed the website and the internal API of Bodah Logistics security with the correction of 4 critical vulnerabilities.
- Implemented the incident response of Bodah Logistics during the cyberattack that targeted Bodah Logistics and one of its employees achieving full recovery to normal activities in two days.
- Produced the security policy and the annual security strategy of Bodah Logistics for 2025 completing the full process including assets inventory, security controls assessment and risk management.

Blue Team Program Graduate **January 2025 – April 2025**
Blacks in Cybersecurity, Baltimore, USA (Remote Traineeship)

- Investigated and resolved more than 12 security incident cases on KC7 Cyber game platforms, analyzing security events and using KQL to retrieve data and logs.
- Wrote down three full reports of my investigation and track down all the data for the Management report.
- Used Virus Total and other blue team tools to analyze suspicious files and programs, ensuring users' security.

Cybersecurity Analyst Intern **August 2024 – October 2024**
CodeAlpha, Lucknow, Uttar Pradesh, India (Remote)

- Produced an awareness campaign document on phishing attacks, providing secure habits to avoid phishing.
- Designed a Python network sniffing tool for advanced network monitoring using Scapy and tcpdump.
- Designed a secure file exchange application using Python and the RSA encryption algorithm.

Information Security Analyst Intern **April 2024 – August 2024**
EMES Sarl, Cotonou, Benin

- Performed Backend development with JavaScript and Node.js to develop microservices for a business platform.
- Used Continuous development and integration (CI-CD) with Docker and Cloud infrastructures, including Microsoft Azure.
- Implemented three microservices and their deployment on the company's server.
- Realized IT Security based projects like the setup of OpenVAS, a vulnerability assessment tool in a Kathara network to detect and analyze vulnerabilities.

PROJECTS

Cloud Security Incident Response **October 2025**

- Identified the vulnerable assets and the related misconfiguration concerned using the Security Command Center.
- Responded to the incident by deleting vulnerable assets and applying secure policies on the Firewall and Cloud Storage bucket.
- Wrote a full documentation of the Incident for the incident playbook.

Virtual Security Lab for Attack analysis **April 2025 – August 2025**

- Built a Security Lab to implement vulnerable scenarios using Kathara with full infrastructure and code replicable and accessible in open source on GitHub.
- Analyzed the techniques and tactics used by the potential attacker using MITRE ATT&CK and the Cyber Kill Chain.
- Completed a full security assessment report with recommendations for proactive monitoring and enforced security.

Secure File Transfer App **August 2024**

- Built a secure app to easily, safely, and quickly transfer large numbers of files in a network.
- Used Python, Scapy library, tcpdump, and applied the RSA encryption algorithm to ensure confidentiality.

Windows server monitoring using Splunk SIEM **March 2024**

- Set up and created an Active Directory domain to manage client machines.
- Configured the Splunk server and its utilities for a client machine.
- Built a virtual workstation composed of a Kali Linux machine, a Windows server and an Ubuntu server.

SKILLS

- Programming Languages: Python, Bash, KQL, JavaScript, HTML, CSS, C++, C and PowerShell
- Frameworks and Tools: Node.js, Git, Splunk, Metasploit, Nmap, OSINT Framework, Microsoft Office
- Soft Skills: Bilingual: French (Fluent); English (C1); Curious, Dedicated and Experience working on a collaborative team

INTERESTS & ACHIEVEMENTS

- Translated threat intelligence into actionable defense strategies, directly improving the organizational security posture and supporting advanced threat hunting efforts.
- Google IT Support Professional, Google Cybersecurity and Google Cloud Cybersecurity certificates
- Ethical Hacking, Linux Fundamentals, Networking Fundamentals certificates
- Microsoft Azure Fundamentals AZ-900 certificate.
- 45th place at PicoCTF 2024 in Africa
- Preparing the Cyberwarfare Labs CRTA and Certified Associate Penetration Tester (Hackviser) certifications
- Blacks in Cybersecurity Blue Team Program graduate, completing 12 real-world security investigations with reports.