

CV

KENNEDY AIKOHI

📅 Birthday 8th March 1987 in Lagos

📍 Address Eickenscheidter Fuhr 74
45139 Essen
North Rhine-Westphalia
Germany.

📞 Phone +49 163 3353 612

✉ Email aikohikennedy@gmail.com

🌐 LinkedIn linkedin.com/in/aikohikennedy

🌐 Github https://github.com/kennedy-aikohi



PROFILE

Cybersecurity Analyst with hands-on experience across **SOC operations, DFIR, threat hunting, malware analysis, reverse engineering, adversary tradecraft, and web application and network security**. Skilled in cutting through alert noise, maintaining composure during incidents, and clearly communicating technical findings to both technical teams and executive leadership. Experienced in network traffic analysis using Wireshark to identify malicious activity, protocol abuse, and lateral movement. Delivered **CompTIA Security+** instruction to military personnel at a **U.S. Air Base in Kaiserslautern, Germany**, strengthening understanding of threat identification, risk mitigation, web and network defense, and security governance. Actively maintains hands-on skills and ranks among top global performers on **Security BlueTeam Labs, Hack The Box, and TryHackMe**.

KEY ACHIEVEMENTS

- CompTIA Security+ Instructor**
 - Delivered **4-day CompTIA Security+ certification training** at a **U.S. Air Base in Kaiserslautern, Germany**, instructing **military and civilian personnel** and translating complex cybersecurity concepts into clear, practical guidance (**December 2025**)
- Top Global Performance in Security Competitions**
 - Ranked **1st globally** in the **Security Blue Team Frostbyte (2025)**
 - Placed **24th out of 11,342 participants** in the **HackTheBox Holmes CTF (2025)**

PROFESSIONAL EXPERIENCE

Oct 2024 – Jan 2025

DuskBeacon | Virginia, USA (Remote)

Cybersecurity Analyst Intern

- Monitored **500+ enterprise endpoints** using **SIEM tools (Splunk, QRadar)**, triaging **150+ weekly alerts** and escalating only confirmed security incidents
- Reduced **false positives by 30%** through systematic **correlation rule tuning** and **SOC playbook optimization**, improving analyst efficiency and trust in reporting
- Collaborated with cross-functional teams to map detections to the **MITRE ATT&CK framework** and **ISO/IEC 27001** controls, producing clear documentation that simplified **compliance and audit reporting**

Mar 2024 – Sep 2024

Clarusway GmbH | Wolfenbüttel, Germany

Security Operations Center (SOC) Analyst

- **Improved SIEM detection accuracy by 35%** through methodical **rule refinement and dashboard optimization**, reducing unnecessary alerts while maintaining comprehensive threat coverage
- **Conducted vulnerability assessments** across multiple hosts using **Nessus** and **OpenVAS**, prioritizing remediation based on **business risk** rather than severity scores.
- **Performed phishing simulations** and **malware analysis** exercises, documenting findings in accessible language for **security awareness training** and **executive briefings**

IT Support Specialist

- **Managed security compliance** for 5,000+ enterprise endpoints via **MDM platform**, enforcing **policies, device encryption**, and **access controls** while providing technical support across a distributed workforce
- **Responded to security incidents** including compromised accounts, malware alerts, and lost/stolen devices, performing **remote wipes, credential resets**, and escalating genuine threats
- **Delivered cybersecurity awareness training** to end users, translating technical security concepts into practical guidance on **phishing prevention, password security**, and safe computing practices

TECHNICAL CAPABILITIES

SIEM & Monitoring

Splunk | IBM QRadar | Elastic Stack | Wazuh | CrowdStrike Falcon | SentinelOne

Security Analysis

Volatility | Autopsy | FTK Imager | Wireshark | Zeek | Arkime | CyberChef

Vulnerability Management

Nessus | OpenVAS | Burp Suite | Nmap | Metasploit | Cobalt Strike

Infrastructure

Windows Server | Linux (Ubuntu, Kali, CentOS) | Active Directory | VMware | Hyper-V

Frameworks

MITRE ATT&CK | NIST CSF | ISO/IEC 27001

Scripting

Python | PowerShell | Bash

Ticketing

TheHive | Jira

EDUCATION

Apr 2009 – Sept 2012

Bachelor of Science in Chemistry

Ambrose Alli University | Ekpoma, Nigeria |

Apr 2013 – Sept 2014

Computer Science Studies

Kharkiv National University of Radio-Electronics | Kharkiv, Ukraine

CERTIFICATIONS

CompTIA Security+

Clarusway Cybersecurity Analyst Professional Certificate

Cisco Endpoint Security & Ethical Hacking

IBM Security Operations Center

Chemistry (University Transcript)

LANGUAGES & CORE STRENGTHS

Languages

German: Intermediate (B1)

English: Professional Proficiency (C2)

Russian: Fluent

Core Strengths

Practical Threat Analysis | Effective Communication | Alert Triage & Prioritization | Team Collaboration | Technical Documentation | Security Awareness Training | Calm Under Pressure | Business-Focused Security