

KENNEDY AIKOHI

APPLICATION FOR THE POSITION OF CYBERSECURITY ANALYST / SOC ANALYST



CONTACT DETAILS:

Eickenscheidter Fuhr 74
45139 Essen
North Rhine-Westphalia
Germany
Phone: +49 163 3353 612
Email: aikohikennedy@gmail.com
LinkedIn: linkedin.com/in/aikohikennedy
Website: <https://kennedy-aikohi.com/>

ATTACHMENTS:

- CV
- Certificates

CV KENNEDY AIKOHI

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

Highly motivated and certified Cybersecurity Analyst (CompTIA CySA+ / Security+) and 1st Place Winner of the Security Blue Team FrostByte Global Challenge (2025), outperforming an international field in practical threat hunting, defensive operations, and live incident response. Offers over 5 years of blended experience across security infrastructure monitoring, SIEM/EDR alert triage, email header tracking, and advanced technical training. A resilient, bilingual professional (Fluent English, B1 German) fully aligned for US time zones (EST/CST) and prepared to bring elite analytical rigor to a fast-paced 24/7 SOC environment.

TECHNICAL SKILLS & CERTIFICATIONS

Certifications:	CompTIA CySA+ CompTIA Security+ Security Analytics Professional
Vulnerability Assessment:	OpenVAS Burp Suite Zed Attack Proxy (ZAP) Nmap
Endpoint & Detection:	CrowdStrike Falcon SentinelOne
Security Analysis & Forensics:	Wireshark Volatility Autopsy FTK Imager Zeek CyberChef
Scripting & Automation:	Python PowerShell Bash Rust
Ticketing & Case Management:	TheHive Jira
Email & Messaging Security:	Phishing Triage Email Header Analysis Social Engineering Defense

CORE COMPETENCIES

Security alert triage, incident classification, and log-based threat detection
Phishing analysis, email header triage, and sandbox malware investigation
Incident documentation, technical report writing, and escalation workflows
MFA deployment, user access controls, and endpoint security configuration
Technical communication and collaborative teamwork in fast-paced SOC environments

PROFESSIONAL EXPERIENCE

12/2025 - 05/2026

The Knowledge Academy

IT Security Trainer (Independent Contractor) | Europe (Onsite)

- Delivered hands-on cybersecurity training and intensive exam preparation across Europe, notably instructing active-duty military personnel at U.S. Air Base Kaiserslautern on threat vectors and malware mechanics.
- Deconstructed complex network architectures and defenses into actionable workflows for diverse technical groups, while maintaining elite threat communication and documentation standards.

10/2024 – 01/2025

Cybersecurity Analyst, Project-Based

DuskBeacon | Remote (USA)

- Executed alert triage and incident classification utilizing enterprise SIEM and EDR platforms including IBM QRadar and CrowdStrike.
- Investigated suspicious process activity to isolate threat indicators, documenting all findings systematically to streamline escalation workflows.

03/2024 – 09/2024

Junior SOC Analyst

Clarusway GmbH | Germany

- Conducted infrastructure vulnerability assessments and analyzed phishing or malware samples, executing deep-dive log reviews to author structured technical reports.
- Applied enterprise SOC workflows and investigation protocols to handle alert lifecycles, optimizing triage efficiency to substantially decrease mean time to respond (MTTR).

03/2022 – 03/2024

Logistics Operations & Professional Upskilling Phase

Lennestadt, Germany

- Handled inventory management, operational workflows, and team coordination within a fast-paced German logistics facility to secure family stabilization following relocation from Ukraine.
- Dedicated concurrent hours to rigorous technical upskilling, mastering German IT market frameworks and completing advanced cybersecurity certification pathways.

02/2020 – 09/2021

IT Support Specialist, Freelance

Ikhuria Consult LLC | Remote (UAE)

- Hardened endpoints and enforced data encryption via Microsoft Intune MDM to securely deploy a surging remote workforce.
- Provided remote IT support and user guidance to eliminate home-network vulnerabilities and operational risks.

05/2015 - 09/2017

IT Infrastructure & Security Consultant (Senior Trainer)

Globaltech World Professionals Limited (globaltechsworld.net) | Remote

- Managed Windows Server deployments and optimized network architecture for corporate and public clients.
- Taught email header analysis and social engineering defense to prepare organizations to detect and mitigate Business Email Compromise (BEC).

TECHNICAL PROJECTS (GITHUB)

JIGSAW & LogRaptorX:

Engineered an automated DFIR triage application mapped to MITRE ATT&CK for rapid forensic evidence processing, and developed custom Windows log parsing utilities.

EZ Sentinel Workbench:

Created a simple GUI wrapper for selected forensic tools to support hands-on analysis of Windows artifacts such as Prefetch and Registry data.

YARA Detection Lab:

Built basic YARA rules to practice signature-based detection and understand common malware patterns.

EDUCATION

2009 – 2012

B.Sc. Chemistry

Ambrose Alli University, Nigeria

2013 – 2014

Computer Science Studies

Kharkiv National University of Radio Electronics, Ukraine

LANGUAGES

English:

Fluent (C2)

German:

Intermediate (B1)

Russian:

Advanced (C1)