LEBENSLAUF
KENNEDY AIKOHI

Geburtsdatum 08. März 1987 in Lagos

Adresse Eickenscheidter Fuhr 74,
45139 Essen
Nordrhein-Westfalen
Deutschland

Telefon +49 163 3353 612

E-Mail aikohikennedy@gmail.com

LinkedIn linkedin.com/in/aikohikennedy

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

PROFIL

Cybersecurity Analyst mit praktischer Erfahrung im Security Operations Center, SIEM Monitoring und Incident Response. Erfahrung in der Überwachung von Unternehmensumgebungen mit mehr als 500 Endpunkten sowie in der Optimierung von Detection Regeln zur Reduktion von False Positives. Analytisch strukturiert mit besonderem Fokus auf Threat Detection, Log Analyse und die kontinuierliche Verbesserung von Sicherheitsprozessen.
Ergänzend eigenständige Entwicklung mehrerer sicherheitsorientierter Softwareprojekte, darunter eine MITRE ATT&CK basierte Threat Intelligence Plattform, ein Hash basiertes Digital Defense Dashboard zur sicheren Dokumentenanalyse sowie Tools im Bereich macOS Forensik und Speicheranalyse. Schwerpunkt auf Blue Team Operations, Incident Response und Detection Engineering.

BERUFSERFAHRUNG

12/2025 – Heute

Technischer Trainer, freiberuflich

The Knowledge Academy, internationale Einsätze

- Durchführung internationaler IT Security Schulungen, darunter eine viertägige CompTIA Security+ Schulung auf einer US Airbase in Kaiserslautern, eine viertägige Network Segment Routing Schulung in Italien sowie ein eintägiges Adobe Experience Manager Training in Dänemark
- Konzeption und Entwicklung praxisnaher Lab Szenarien sowie strukturierter Schulungsunterlagen zur praxisorientierten Wissensvermittlung
- Vermittlung komplexer technischer Inhalte an internationale Fachkräfte mit unterschiedlichen technischen Hintergründen

05/2025 – voraussichtlich 04/2026

Intensiv Integrationskurs Deutsch, B1 abgeschlossen

DÜS Eckert Spracheninstitut

- Vollzeit Sprach und Integrationsprogramm mit erfolgreichem Abschluss B1 inklusive Leben in Deutschland
- Kontinuierliche fachliche Weiterentwicklung im Bereich Cybersecurity parallel zum Sprachkurs
- Eigenständige Skill Enhancement Projekte in Threat Detection, Log Analyse und Incident Response

10/2024 – 01/2025

Cybersecurity Analyst Intern

DuskBeacon, Remote USA

- Monitoring von mehr als 500 Unternehmensendpunkten mit Splunk und IBM QRadar
- Analyse und Priorisierung von über 150 Security Alerts pro Woche
- Reduktion von False Positives um 30 Prozent durch Optimierung von SIEM Regeln
- Zuordnung von Detection Mechanismen zu MITRE ATT&CK
- Technische Dokumentation gemäß ISO 27001 orientierten Prozessen

03/2024 – 09/2024	**SOC Analyst, Praktikum** **Clarusway GmbH, Deutschland** • Verbesserung der SIEM Erkennungsgenauigkeit um 35 Prozent • Durchführung von Schwachstellenanalysen mit Nessus und OpenVAS • Analyse von Malware Vorfällen • Erstellung strukturierter Security Berichte
06/2022 – 02/2024	**Produktionsmitarbeiter / Produktionshelfer, Überbrückungstätigkeit** persona service AG & Co KG sowie PerSe Partner Velbert GmbH, Deutschland • Tätigkeit im Produktionsumfeld während der beruflichen Integration in Deutschland • Maschinenbedienung, Montagearbeiten und Qualitätskontrollen
10/2021 – 05/2022	**Relocation nach Deutschland und Familienzeit** • Administrative Unterstützung im familiengeführten Einzelhandelsunternehmen • Organisation der Relocation nach Deutschland • Vorbereitung auf Integration und berufliche Neuorientierung
02/2020 – 09/2021	**IT Support Specialist, freiberuflich** **Ikhuoria Consult LLC, Remote** • Verwaltung von mehr als 5000 Endpunkten über MDM Plattformen • Umsetzung von Sicherheitsrichtlinien wie Verschlüsselung und Zugriffskontrolle • Bearbeitung sicherheitsrelevanter Vorfälle • Durchführung von Phishing Simulationen und Awareness Schulungen
03/2015 – 10/2019	**Remote Property Manager (freiberuflich)** Global Realtors Network, Lagos (Remote) • Eigenständiges Management von Immobilienverkäufen und -vermietungen; Abschluss von über 50 Verträgen jährlich durch fundierte Marktanalysen.

TECHNISCHE FÄHIGKEITEN

Security Operations, Detection und Blue Teaming	Splunk | IBM QRadar | Elastic Stack | Wazuh | CrowdStrike | SentinelOne | MITRE ATT&CK | ISO 27001 | NIST CSF
Forensik und Schwachstellenmanagement	Wireshark, Volatility, Autopsy, Zeek, CyberChef, Nessus, OpenVAS
Red Team Tools und Adversary Simulation	Nmap, Metasploit, Burp Suite, Cobalt Strike, Python, PowerShell, Bash

AUSBILDUNG

Apr 2009 – Sept 2012	**Bachelor of Science in Chemie** Ambrose Alli University | Ekpoma, Nigeria |
Apr 2013 – Sept 2014	**Studium der Informatik** Kharkiv National University of Radio-Electronics | Kharkiv, Ukraine

ZERTIFIZIERUNGEN

CompTIA Security+

Clarusway Cybersecurity Analyst Professional Certificate

Cisco Endpoint Security & Ethical Hacking

IBM Security Operations Center

SPRACHEN & KERNKOMPETENZEN

Sprachen	Deutsch: Mittelstufe Englisch: Verhandlungssicher Russisch: Fließend
Kernkompetenzen	Praktische Bedrohungsanalyse | Effektive Kommunikation | Alert-Triage & Priorisierung | Teamarbeit | Technische Dokumentation | Awareness-Training | Stressresistenz | Geschäftsorientierte Sicherheit