Umaru Bah

Junior Cybersecurity Analyst

Adresse: Hamburg, Deutschland
Telefon: +49 162 4954393
E-Mail: r11rbq@inf.elte.hu
LinkedIn: linkedin.com/in/bah-umaru-b442a4253
GitHub: github.com/bahh99
Nationalität: Sierra-leonisch
Sprachen: Englisch (fließend), Arabisch, Deutsch

Profil

Cybersecurity-Analyst mit praktischer Erfahrung in SIEM-Monitoring, Log-Analyse und Incident Response. Erfahrung in SOC-Umgebungen (Hack The Box), Bedrohungserkennung und Schwachstellenanalyse. M.Sc. Informatik (Cybersicherheit), Eötvös-Loránd-Universität Budapest. Angestrebte Position: SOC Analyst L1 / Junior Cybersecurity Analyst.

Berufserfahrung

Jan. 2025 – heute
SOC Analyst Training · Hack The Box, *Remote*
- SIEM-basierte Bedrohungserkennung und Log-Analyse in simulierten SOC-Umgebungen
- Untersuchung von Brute-Force-Angriffen (Event ID 4625) mit Splunk und Elastic Stack
- Alert Triage und Incident-Response-Simulationen; Erstellung strukturierter Berichte

Aug. 2023 – Jul. 2025
Studentenbotschafter · Eötvös-Loránd-Universität, *Budapest, Hybrid*
- Beratung internationaler Studierender zu Studienprogrammen und Stipendien
- Organisation von Kulturveranstaltungen, Workshops und Informationswebinaren
- Zusammenarbeit mit Universitätspersonal zur Verbesserung der Unterstützungsangebote

Sep. 2023 – Mai 2024
Sicherheitsforscher · Eötvös-Loránd-Universität, *Budapest*
- Sicherheitsanalyse in Netzwerk- und Cloud-Umgebungen (DSGVO, NIS2)
- Erstellung technischer Berichte zu Schwachstellen und Sicherheitsbefunden
- Zusammenarbeit mit interdisziplinären Teams zu regulatorischen Anforderungen

Jan. 2021 – Dez. 2022
IT-Support-Mitarbeiter · Ahmad Tejan Kabbah Foundation, *Freetown, Sierra Leone*
- IT-Support auf 1./2. Ebene: Hardware-, Software- und Netzwerkprobleme
- Implementierung von IT-Sicherheitsprotokollen; Verwaltung der Website

Jun. 2018 – Dez. 2020
IT-Spezialist (Datenerfassung) · Njala University, *Sierra Leone*
- Konfiguration von Routern und Switches; Diagnose und Wartung von Systemanwendungen

2016 – 2018
Dateneingabe-Mitarbeiter · Wahlkommission Sierra Leone (ECSL), *Sierra Leone*
- Analyse und Überprüfung von Wahlergebnissen; Sicherstellung der Datenintegrität

Ausbildung

Sep. 2022 – Jul. 2025	**M.Sc. Informatik – Cybersicherheit** · Eötvös-Loránd-Universität (ELTE), *Budapest* Abschlussarbeit: Differential Privacy in Secure Federated Averaging Algorithm Schwerpunkte: Netzwerksicherheit, Kryptographie, Cloud-Sicherheit, DSGVO, Anomalieerkennung Zusatz: ENFIELD AI Summer School 2025, Budapest University of Technology (BME)
Mär. 2016 – Apr. 2020	**Bachelor of Science – Business Information Technology** · Njala University, *Sierra Leone* Schwerpunkte: Programmierung, E-Commerce Abschlussarbeit: *Library Management System*

Praktische Projekte

SOC-Erkennung & Log-Analyse	Analyse von Windows Security Event Logs (Event IDs 4625, 4672); Erkennung von Brute-Force-Mustern; Untersuchungsberichte mit KQL-Abfragen. GitHub
SIEM-Labor (ELK)	Aktives Threat Hunting mit Elastic Stack; Identifikation von Anomalien und IoCs im Eigenlabor.
M.Sc.-Forschung	Secure Federated Averaging (SFA)-Framework mit Differential Privacy und Anomalieerkennung (Python). GitHub
CTF-Wettbewerbe	SQL-Injection, Directory Traversal, Authentication Bypass auf Hack The Box und TryHackMe.

Kenntnisse & Fähigkeiten

Security Operations	SIEM (Splunk, Microsoft Sentinel, Elastic Stack), Alert Triage, Incident Response, Log-Analyse
Bedrohungsanalyse	Phishing, Brute-Force-Erkennung, Malware-Verhaltensanalyse, Schwachstellenbewertung
Offensive Security	Penetrationstests, SQL-Injection, XSS, Burp Suite, Metasploit, Hydra, Kali Linux
Systeme & Netzwerke	Windows- & Linux-Administration, TCP/IP, Nmap, Wireshark, VM-Konfiguration
Programmierung	Python, Bash, PowerShell, Git
Büroanwendungen	Microsoft 365 (Excel, PowerPoint, Teams, Word)

Zertifikate & Auszeichnungen

Aug. 2024	**CompTIA PenTest+** – TryHackMe Credential ID: THM-EJGIQUJPYH
Jun. 2024	**Studentenbotschafter-Zertifikat** – Eötvös-Loránd-Universität
2023	**Cybersecurity Essentials** – Cisco Networking Academy
Dez. 2022	**Big Data & Analytics** – Cisco Networking Academy