

Brook Belihu Duessa

Cybersecurity & Cloud Engineering | M.Sc. Cyber Security
brookbdt@gmail.com | [+49 152 2595 1262](tel:+4915225951262) | Cottbus, Germany
[linkedin.com/in/brookbelihu](https://www.linkedin.com/in/brookbelihu) | github.com/brookbdt | www.brookduessa.dev

PROFILE

Software engineer with 5+ years building cloud-native platforms (AWS), now pursuing an M.Sc. in Cyber Security at BTU Cottbus. Building hands-on detection engineering, cloud security, and AI-assisted triage portfolio projects. Seeking a Werkstudent role in cybersecurity, cloud security, or DevSecOps. Available up to 20 hrs/week; eligible for student employment under German residence law.

TECHNICAL SKILLS

Security	Wazuh SIEM, Sysmon, auditd, MITRE ATT&CK, GuardDuty, CloudTrail, Detection Engineering
Cloud / IaC	AWS (Lambda, S3, IAM, SNS, CloudFormation, CDK), Terraform, Docker, CI/CD
Languages	Python, TypeScript / Node.js, Bash, SQL
Platforms	Linux (Ubuntu), Windows, Git, PostgreSQL, REST / GraphQL APIs

SECURITY PROJECTS

SOC Homelab Detection Lab [GitHub](#)

- Deployed Wazuh SIEM via Docker with Windows (Sysmon) and Ubuntu (auditd) endpoints on Apple Silicon
- Simulated brute-force, reconnaissance, and persistence attacks mapped to MITRE ATT&CK
- Wrote custom detection rules with tuning for false-positive reduction
- Produced incident response reports with IOCs, timelines, and remediation steps

Cloud-Native AI Security Triage Pipeline [GitHub](#)

- Provisioned AWS security infrastructure (CloudTrail, GuardDuty, S3, IAM, SNS) using Terraform with least-privilege IAM design
- Built 7-stage Python pipeline: ingest → normalize → enrich (MITRE ATT&CK) → cluster → deterministic risk score → AI triage (Claude API) → report
- Deterministic-first design: LLM receives only structured incident clusters, never raw JSON
- Generates analyst-ready Markdown incident reports with risk reasoning, investigation steps, and response actions
- Implemented pytest test suite covering all pipeline stages

PROFESSIONAL EXPERIENCE

Pulse ERP — Systems Architect Aug 2024 – Jan 2026

- Built multi-tenant AI-native ERP on AWS (Aurora, Lambda, AppSync, S3, CloudFront); designed secure REST/GraphQL APIs.
- Integrated AWS Bedrock (Claude) for intelligent analytics; led small cross-functional engineering team.

Kelal Tech — Software Engineer Aug 2019 – Aug 2024

- Delivered full-lifecycle software projects (logistics, edtech, e-commerce) using Node.js, Flutter, PostgreSQL.

EDUCATION

M.Sc. Cyber Security — BTU Cottbus-Senftenberg Oct 2025 – Present

B.Sc. Software Engineering — Addis Ababa Science & Technology University GPA 3.49 (1.7 German Scale)

LANGUAGES

English (Fluent) | German (A2 – actively improving) | Amharic (Native)