# Charles Kwarteng

Oberhausen, Germany | kwartcharles@gmail.com | +4917624267157 | www.linkedin.com/in/ckwarteng

## PROFESSIONAL PROFILE

IT Security and Operations Professional with an M.Sc. in Data Science focusing in IT Security Strategy, and over three years of hands-on experience across security operations, ISMS governance, infrastructure monitoring, and cross-functional stakeholder management. Maintained 99.99% system availability and 95% SLA-based incident closure without escalation across 24/7 national government infrastructure; administered IAM governance for over 200 users via Microsoft Entra ID. Ranked top 3% globally on TryHackMe and currently certified in CompTIA CySA+, Security+, BTL1, and ISC2 CC.

## CORE SKILLS

- ISMS development and management (ISO 27001:2022)
- SIEM Security Operations: Splunk, ELK Stack, Microsoft Sentinel
- Threat detection, alert triage and MITRE ATT&CK mapping
- GDPR, NIS2, DORA and regulatory compliance
- Incident response and digital forensics (DFIR)
- Network management: LAN/WAN, VPN, SD-WAN, VoIP
- Microsoft 365, Azure and Entra ID administration
- Endpoint management: Windows 10/11, Intune, MDM, patching
- Risk management: risk register, KPI dashboards, reporting
- Network monitoring: Nagios, SolarWinds, Cacti, PingInfoView
- Scripting and automation: Python, PowerShell, SQL
- Frameworks: NIST CSF, MITRE ATT&CK, Zero Trust, GDPR

## PROFESSIONAL EXPERIENCE

### Blue Team Security Researcher | TryHackMe, Freelance, Remote

*March 2025 – Present*

- Ranked top 3% globally on TryHackMe, completing intensive hands-on labs in SIEM operations (Splunk, ELK), MITRE ATT&CK-mapped threat detection, digital forensics (Autopsy, FTK Imager), network traffic analysis (Wireshark/PCAP), and IOC enrichment with MISP and TheHive.

### Data Analyst and IT Support Specialist | Danquah Institute, Ghana

*February 2022 – February 2023*

- Designed and maintained IT security documentation, incident procedures, and audit-ready governance records in SharePoint, reducing downtime by 25% through structured incident handling and continuous process improvement.
- Administered Active Directory user accounts (15+ users), access permissions, and backup processes, strengthening identity governance and access control across the organisation.
- Automated KPI reporting and compliance monitoring workflows using Excel (Power Query), SQL, and Python, delivering 90% operational visibility through dashboards for senior management.
- Managed hardware and software procurement end-to-end: vendor evaluation, quotation comparison, endpoint configuration, and asset lifecycle tracking.

### Network Operations Engineer (NOC) | National Information Technology Agency (NITA), Ghana

*September 2020 – January 2022*

- Supervised continuous 24/7 operations across Tier III critical national infrastructure spanning WAN/LAN/WLAN/SD-WAN/VoIP environments, sustaining 99.99% service availability for government-connected systems serving multiple public institutions simultaneously, and performing real-time fault diagnosis and performance analysis to resolve outages and degradation before SLA thresholds were breached.
- Triaged and prioritised Tier 1/2 security and operational alerts using Nagios, SolarWinds, Cacti, and PingInfoView, resolving incidents by impact and urgency in strict SLA alignment and achieving 95% ticket closure within defined response windows through accurate escalation and full documentation.

- Configured and managed firewalls, routers, and switches, applying and enforcing secure baseline configurations that protected operational integrity, reduced the attack surface, and maintained compliance with security standards across core and client network environments.
- Partnered with the SOC team to monitor live threat alerts, correlate security events, and enforce network-level controls, providing government and public-sector clients with real-time visibility into the threat landscape and supporting active containment strategies.
- Administered Microsoft Entra ID (Azure AD) for over 200 users, managing provisioning, group policy, compliance settings, and audit readiness to maintain the organisation's identity security posture and reduce unauthorised access risk.
- Implemented and tested redundancy, failover, and disaster-recovery strategies that strengthened business continuity and eliminated single points of failure across critical systems, ensuring sustained resilience for national-level infrastructure.
- Produced incident reports, outage documentation, post-incident reviews, and management KPI dashboards in Jira, feeding the institutional knowledge base, driving root-cause analysis of recurring fault patterns, and supporting continuous operational improvement.

**IT Support Intern** | Metro TV, Ghana

*April 2019 – September 2019*

- Delivered first-line IT support for hardware, software, and network issues across departments, setting up and maintaining desktops, laptops, printers, and broadcast IT equipment for over 35 users while keeping systems patched, backed up, and antivirus-protected.
- Improved IT asset-tracking accuracy by 40% by tightening documentation and inventory practices, resolving support tickets promptly and establishing consistent lifecycle management processes across all hardware categories.
- Led a team of interns to plan and deliver a full structured cabling upgrade, improving secure data transfer efficiency by 90% and producing complete infrastructure documentation for the IT team.
- Supported the Master Control Room across 50+ live productions, monitoring on-air signals and switching live feeds, commercials, and recorded content to maintain seamless transmission; set up and dismantled studio and field production equipment and assisted post-production editing, earning recognition from senior engineers for composure and reliability under high-pressure broadcast conditions.

## EDUCATION

**M.Sc. Data Science (Focus: IT Security Strategy)** | University of Europe for Applied Sciences, Potsdam, Germany

*March 2023 – February 2025*

*Thesis: Proposed Robust Cybersecurity Framework Leveraging GDPR and Zero Trust Architecture; a multi-jurisdictional governance framework applicable to NIS2, DORA, and ISO 27001 compliance*

**B.Sc. Computer Engineering** | Ghana Technology University College, Accra, Ghana

*January 2017 – August 2020*

## CERTIFICATIONS

- CompTIA Cybersecurity Analyst (CySA+)
- CompTIA Security+ (CE)
- ISO 27001:2022, Information Security Management Systems (ISMS) – Course Completed
- Blue Team Level 1 (BTL1)
- ISC2 Certified in Cybersecurity (CC)
- Microsoft 365 Certified: Fundamentals (MS-900)

## LANGUAGES

English: Native. | Akan (Twi): Native | German: B1 Certified, B2 in progress