CHIDUBEM BRANDON ONOCHIE-ONYETENU

Toronto, ON • +1 (437) 655-9305 • chidubemonyetenu@gmail.com

CYBERSECURITY ANALYST | THREAT RESPONSE | RISK & COMPLIANCE

PROFESSIONAL SUMMARY

Cybersecurity professional with more than four years of information technology and security experience, including identifying phishing threats, educating employees on social engineering, and escalating incidents for investigation and containment. ISC2 Certified in Cybersecurity, with hands-on experience in threat monitoring, vulnerability management, and incident response. Applies the National Institute of Standards and Technology Cybersecurity Framework, ISO 27001, and System and Organization Controls 2 to reduce risk, and reduced downtime and security risk exposure by 25% through proactive monitoring and rapid remediation. Works across technical and non-technical teams to turn findings into clear, actionable guidance.

CORE SKILLS

Security Operations & Incident Response: Threat Detection & Monitoring, Security Telemetry & Log Analysis, Incident Investigation & Documentation, Incident Escalation, Root-Cause Remediation, System Hardening

Risk, Vulnerability & Compliance: Risk & Vulnerability Assessments, Gap Analyses, Control Validation, NIST CSF, ISO 27001, SOC 2, CIS Controls, Audit Support & Remediation, Security Policy/SOP Development

Identity & Access Management (IAM): Active Directory, Entra ID (Azure AD), User Provisioning & De-provisioning, Access Reviews, RBAC, MFA, Least-Privilege Enforcement

Network & Endpoint Security: TCP/IP, DNS, DHCP, VPN, Firewalls, Wireless Security, Endpoint Protection/EDR, Antivirus, Patch Management, Windows Server Administration

Governance, Risk & Vendor Management: GRC & Ticketing Tools, Third-Party/Vendor Risk Evaluation, ITSM (Incident, Service Request & Change Management), Jira Service Management, SLA Tracking

Phishing and Social Engineering Defense: Phishing Email and Link Identification, User Security Awareness Education, Threat Escalation, Incident Documentation and Reporting

PROFESSIONAL EXPERIENCE

Cyber Security Analyst | *Topron Consulting* Apr 2024 – Present

- Identified phishing emails and malicious links, educated employees on how to recognize phishing and social engineering attempts, and escalated confirmed threats to the appropriate teams for investigation and containment.
- Conducted risk, business impact, gap, and vulnerability assessments aligned with NIST CSF, ISO 27001, and SOC 2, producing security posture evaluations with identified risks and recommended remediation actions for management review.
- Investigated, triaged, and documented security findings and incidents using GRC and ITSM ticketing tools, supporting incident response, escalation, and knowledge base updates within defined SLAs.
- Provided support to ongoing internal and external IT audits and audit remediation, generating technical recommendations for corrective security controls.
- Assessed security requirements and controls applied throughout systems and application review processes, advising stakeholders on security best practices and control alignment.
- Collaborated with cross-functional IT, network, and business teams to plan, enforce, and implement corrective security controls and technical countermeasures for identified vulnerabilities.

IT & Systems Support Engineer | *Cakasa Maintenance Services* Mar 2021 – Mar 2024

- Monitored enterprise systems, network traffic, and security telemetry for threats, anomalies, and unauthorized activity, supporting early detection and incident containment.
- Performed scheduled vulnerability assessments and tests to uncover flaws, coordinating with technical teams to remediate identified vulnerabilities and maintain security standards.
- Administered endpoint security tools, antivirus software, firewalls, and secure OS baselines to protect systems, networks, and applications across hybrid environments.
- Managed Identity and Access Management (IAM) operations using Active Directory and Entra ID (Azure AD): user provisioning/de-provisioning, access reviews, MFA enrolment, and least-privilege enforcement.
- Diagnosed and resolved network security issues involving VPN access controls, routers, switches, IP routing, and DNS/DHCP configuration.
- Reduced system downtime and security risk exposure by 25% through proactive telemetry monitoring, rapid incident escalation, and root-cause remediation.

EDUCATION

Graduate Diploma – Cybersecurity | Loyalist College, Toronto, ON | 2026
B.Eng. Computer Engineering | Afe Babalola University, Nigeria | 2022

CERTIFICATIONS

ISC2 Certified in Cybersecurity (CC) • Google Cybersecurity Professional Certificate