STEPHEN ODUNZE

Cybersecurity Analyst | SOC Operations | Vulnerability Management | Cyber Risk & Compliance

CISA | CompTIA Security+ | ISO 27001 Lead Auditor | CCNA | DevNet Associate | CC (ISC2) | ITIL

ISACA | ISC2 | BCS – The Chartered Institute for IT

Portfolio: https://stephenodunze.online/ | **GitHub**: https://github.com/Herculis411 | **LinkedIn**: https://www.linkedin.com/in/stephen-odunze411/

PROFESSIONAL SUMMARY

A Cybersecurity Analyst with over 14 years of IT experience and a focused track record in SOC operations, security incident response, vulnerability management, and cyber risk assessment. I hold a Master's degree in Cyber Security (Robert Gordon University) and active certifications including CISA, CompTIA Security+, and ISO 27001 Lead Auditor. Proven ability to monitor, triage, and investigate security alerts using Microsoft Sentinel, Splunk, and Microsoft Defender for Endpoint; map detections to MITRE ATT&CK; and produce clear governance reports for executive and board-level stakeholders. Experienced in collaborating with SOC teams, IT departments, and cross-functional groups in complex, process-driven organisations. Familiar with Cyber Essentials Plus, NCSC guidance, ISO 27001, NIST CSF, and CIS Controls. Committed to continual professional development and maintaining awareness of emerging threats and sector guidance from trusted sources including NCSC and Jisc.

CORE SKILLS & TECHNOLOGIES

Security Operations & Incident Response: Microsoft Sentinel, Splunk, Microsoft Defender for Endpoint, SIEM/SOAR, alert triage, MITRE ATT&CK mapping, containment and remediation

Vulnerability Management: Nessus, Qualys, OpenVAS, CVSS scoring, risk-based prioritisation, remediation tracking, patch management

Endpoint & Identity Protection: Microsoft Defender for Endpoint, EDR, Azure AD/Entra, MFA, Conditional Access, PAM-aligned practices, CIS Benchmarks

Network Security: Firewalls (Cisco Firepower, Fortinet, Juniper SRX), IDS/IPS (Snort, Suricata), VPNs, network segmentation, Wireshark, Nmap

Cyber Risk & Compliance: ISO 27001/27005, NIST CSF, NIST 800-30/800-53, NCSC CAF, Cyber Essentials / Cyber Essentials Plus, CIS Controls, PCI DSS

Cloud Security: AWS (IAM, VPC, CloudWatch), Azure (Entra, Sentinel, Defender), cloud misconfiguration assessment, logging and monitoring

Governance, Audit & Reporting: ITGC testing, Risk & Control Matrix, SoA, ServiceNow GRC, Power BI dashboards, executive and board reporting, assurance workshops

DevSecOps & Automation: Terraform, Kubernetes (EKS), CI/CD (GitHub Actions, ArgoCD), Docker, secrets management, infrastructure security auditing

Stakeholder Engagement: Tabletop exercises, security awareness, cross-functional collaboration, translating technical risk for non-technical audiences

CAREER HISTORY

DevSecOps Engineer (Internship) | **The CloudAdvisory Oy** | Oct 2025 – Present

- Provisioned and managed AWS infrastructure using Terraform, including VPCs, EKS, ECR, RDS, and IAM, with remote state management via S3 and DynamoDB.
- Implemented CI/CD and GitOps pipelines using GitHub Actions, ArgoCD, and Docker to automate secure infrastructure and application deployments.
- Designed observability solutions using Prometheus, Grafana, Fluent Bit, and CloudWatch for centralised logging, metrics, and distributed tracing.
- Supported DevSecOps security practices through infrastructure auditing, secrets management, and AI-assisted automation workflows.
- Collaborated in Agile Scrum sprints using Jira and GitHub feature branches to deliver production-ready, security-hardened infrastructure changes.

Cybersecurity Analyst | **University of Aberdeen** | Apr 2025 – Oct 2025

- Monitored and investigated security alerts, collaborating with SOC analysts and IT teams to triage, contain, and remediate potential threats in line with defined SOPs.

- Conducted vulnerability assessments across infrastructure, web applications, and systems using enterprise scanning tools; prioritised findings by exploitability, business impact, and CVSS score.
- Led quarterly tabletop exercises (TTX) with IT, research, and management teams, testing incident response readiness and improving communication flows; phishing and ransomware simulations improved staff response rates by 35%.
- Produced periodic governance dashboards and risk reports for executive and board-level stakeholders, supporting assurance and audit requirements.
- Performed ITGC testing covering identity and access management, patch management, and system operations; managed compliance evidence for internal and external audits.
- Collaborated with departments to design mitigation strategies for control deficiencies and supported remediation tracking through to closure.

Key Achievement: Contributed to a standardised Risk & Control Matrix (RCM) template subsequently adopted across multiple teams, improving audit consistency and evidence quality.

Cybersecurity Analyst | **CyBlack** | May 2024 – Mar 2025

- Analysed security logs, vulnerability scan outputs, and system configurations to identify weaknesses; mapped alerts to MITRE ATT&CK techniques to enhance correlation rules and detection coverage.
- Conducted control effectiveness testing, reviewed audit evidence, and created remediation roadmaps aligned to ISO 27001 and NIST CSF controls.
- Maintained and updated key ISMS documents including Statement of Applicability (SoA) and Risk Treatment Plan, ensuring traceability between risks and applied controls.
- Integrated compliance tracking into ServiceNow GRC, providing real-time visibility of risk and control performance to governance stakeholders.
- Collaborated with cross-functional teams to strengthen incident response controls and change management processes.

Key Achievement: Supported ISO 27001 recertification and Cyber Essentials Plus audit with zero major findings by improving evidence quality, coverage, and audit readiness procedures.

Network Security Analyst | **MTN Communication PLC** | Jan 2022 – Feb 2023

- Conducted network security audits using Nmap, OpenVAS, and Wireshark to identify misconfigurations, unpatched services, and open ports; coordinated remediation with infrastructure teams.
- Utilised Microsoft Defender for Endpoint and Microsoft Sentinel to triage security alerts, manage incident workflows, and develop containment plans guided by MITRE ATT&CK.
- Enhanced SIEM detection logic in Splunk and Sentinel by developing custom correlation rules and KQL queries, reducing mean-time-to-response (MTTR) by 30%.
- Collaborated with IT audit teams to verify compliance against CIS Controls and internal governance frameworks; conducted vulnerability and patch management assessments.

Network Engineer | **Huawei Technologies** | Nov 2011 – Dec 2021

- Led the design and secure deployment of network infrastructure (2G/3G/4G/5G) across multiple sites; configured VLANs, enforced firewall rules, and deployed IDS/IPS systems.
- Served as primary escalation point for security incidents; conducted real-time analysis and coordinated with response teams using Huawei threat intelligence to contain and remediate threats.
- Monitored and maintained network systems using Wireshark and Zabbix; applied patches and enforced hardening standards aligned to CIS Benchmarks.
- Implemented a preventative maintenance programme using SolarWinds, reducing unplanned network outages by 25% and improving field operational efficiency.

PROJECTS

- Performed OWASP Top 10 web application security testing using Burp Suite and OWASP ZAP; documented findings and produced remediation guidance.
- Conducted enterprise vulnerability scanning and risk prioritisation using Nessus and OpenVAS across simulated production environments.

- Completed AWS cloud security assessments, identifying and remediating IAM misconfigurations and over-permissive security groups.
- Implemented Linux server hardening and database security improvements aligned to CIS Benchmark controls.

EDUCATION, CERTIFICATIONS & PROFESSIONAL AFFILIATIONS

Education

- MSc Cyber Security – Robert Gordon University, Aberdeen (2024)
- BEng Electronics and Computer Engineering – Nnamdi Azikiwe University (2009)

Certifications

- ISO/IEC 27001:2022 Lead Auditor – Mastermind (Dec 2025)
- Certified Information Systems Auditor (CISA) – ISACA (Jun 2025)
- CompTIA Security+ ce (Jul 2023)
- Certified in Cybersecurity (CC) – ISC2 (Aug 2023)
- DevNet Associate – Cisco (Apr 2024)
- CCNA: Enterprise Networking, Security and Automation – Cisco (Jan 2024)
- JNCIA-Cloud – Juniper Networks (May 2019)
- ITIL v3 Foundation – Axelos (May 2018)
- AWS Going Cloud Native (May 2020)
- AZ-500: Microsoft Azure Security Engineer Associate (In View)

Professional Affiliations

- Member, ISACA (Jan 2025) | Member, ISC2 (Jul 2023) | Member, BCS – The Chartered Institute for IT (Mar 2021)