SONNY ENCHILL

Cybersecurity Analyst | SOC Analyst | DevOps & Cloud Engineer | DevSecOps

CONTACT

sonnyenchill@gmail.com
079-0249-7413
United Kingdom
linkedin.com/in/sonnyenchill
Open to Remote / Hybrid / On-site

CYBERSECURITY & SOC

- Security Operations (SOC/SIEM)
- Incident Response & Investigation
- Vulnerability Assessment
- Penetration Testing (Black-box)
- Web App Security (SQLi, XSS)
- Threat Modelling & Risk Mgmt
- Digital Forensics & Log Analysis
- Network Security Monitoring
- MITRE ATT&CK Framework
- ISO 27001 / NIST CSF
- DevSecOps Principles

CLOUD & DEVOPS

- AWS (EC2, VPC, RDS, S3, ALB)
- AWS CloudFront, Auto Scaling, IAM
- Microsoft Azure (VM, VNet, MySQL)
- Terraform (IaC)
- Linux (Ubuntu / CentOS)
- Nginx Web Server
- Git & GitHub (PR Workflow)
- CI/CD Pipelines
- Jira / Scrum / Agile
- Node.js / PM2
- Docker (foundational)
- Agentic DevOps (Claude Code/MCP)

INFRASTRUCTURE & ENTERPRISE

- Microsoft 365 & Azure AD / Intune
- Enterprise Networking & LAN
- Disaster Recovery & BCP
- Identity & Access Management
- VMware Virtualisation
- Windows Server 2008–2022
- MySQL & SQL Server
- IT Governance & Compliance

EDUCATION

MSc Cybersecurity
Robert Gordon University

PROFESSIONAL SUMMARY

Cybersecurity and DevOps professional with a rare dual capability: MSc-level security knowledge combined with hands-on cloud engineering across AWS, Azure, and Terraform. 19+ years of enterprise IT experience in regulated financial services, now specialising in security operations, infrastructure as code, and DevSecOps practices. Currently active as a DevOps Micro-Intern (The CloudAdvisory Oy), deploying production-grade infrastructure across AWS and Azure. Seeking Cybersecurity Analyst, SOC Analyst, or Junior DevOps/Cloud Engineer roles in the UK (Remote/Hybrid/On-site).

PROFESSIONAL EXPERIENCE

DevOps Micro-Intern (Remote)

The CloudAdvisory Oy — DevOps Internship Programme *Jan 2026 – Present*

Production-style internship delivering real DevOps assignments across AWS, Azure, Terraform, Linux, Git, and Agile workflows — every environment treated with production-grade discipline.

- Deployed a full-stack Book Review application in a secure 3-tier AWS architecture: Next.js on EC2 behind a public ALB, Node.js/Express on private EC2 behind an internal ALB, and Amazon RDS MySQL in a private subnet with no direct internet exposure.
- Reproduced the 3-tier architecture on Microsoft Azure: Next.js/Nginx on public VMs, Node.js managed by PM2 on private VMs, and Azure MySQL Flexible Server with HA and read replica — configured through private networking and NSG rules.
- Provisioned complete AWS infrastructure using Terraform (IaC): VPC, subnets, Internet Gateway, Route Tables, Security Groups, EC2, and RDS MySQL — entire stack defined and applied from code.
- Deployed AWS S3 + CloudFront static website via AI-assisted agentic Terraform pipeline (Claude Code) — automating scaffold, validate, plan, apply, and deploy steps.
- Built and validated a Highly Available AWS deployment across two AZs with ALB and Auto Scaling — confirmed zero-downtime recovery by terminating EC2 instances mid-traffic.
- Built CI/CD pipelines with security controls embedded by design: secrets handling, access governance, and automated validation gates — DevSecOps from the start, not as an afterthought.
- Completed full Agile/Scrum sprints in Jira: backlog, Fibonacci estimation, 5-day daily shipping, and full traceability from ticket through Git branch, PR, deployment, and validation.
- Conducted AI-assisted infrastructure security reviews using Claude Code and MCP subagents, auditing Terraform for TLS weaknesses, S3 controls, CloudFront OAC, and HTTPS enforcement — triaging 8 confirmed findings.
- Performed 6-phase operational readiness drills: networking, service health, log analysis, resource monitoring, configuration integrity, and incident simulation/recovery.

Cybersecurity & DevOps Professional Development

Independent Study & Projects *Feb 2024 – Present*

Self-directed upskilling alongside MSc studies across security operations, cloud deployment, and Agile delivery.

- Completed MSc Cybersecurity — Robert Gordon University (Jan 2024 – May 2025): incident response, SIEM, digital forensics, threat modelling, cloud security, web application security, ethical hacking, and risk & compliance.
- Publishes LinkedIn articles on DevOps, cybersecurity, AI governance, and DevSecOps; mentors beginners transitioning into tech.

IT & Facilities Manager

Pensions Alliance Trust Ltd — Financial Services *Jul 2014 – Jan 2024*

Aberdeen, Scotland
Jan 2024 – May 2025

Master's — Information Technology
Sikkim Manipal University Distance Education | 2014–2017

CERTIFICATIONS

CompTIA Security+ (SY0-701)
In Progress — Aug 2026

Agentic AI DevOps — Udemy
Completed 2026

MCSA Windows Server 2012
Microsoft Certified

Microsoft Certified Professional

TOOLS

Security Onion • Kali Linux
Autopsy • Volatility
Wireshark • Burp Suite
Metasploit • MITRE ATT&CK
Terraform • Git • Nginx
Claude Code • MCP
Jira • VMware • Intune
Python (basic) • SQL

Sole owner of enterprise IT, cybersecurity posture, and cloud transformation for a regulated multi-branch financial services organisation (120+ users). Reported directly to the board.

- Spearheaded full Microsoft 365 migration (Exchange Online, SharePoint, Teams, Intune MDM), delivering a 30% productivity uplift and materially strengthening identity and endpoint security.
- Designed, documented, and tested the organisation's Disaster Recovery & BCP, reducing projected recovery time from days to hours and ensuring regulatory compliance.
- Architected and deployed a secure, high-availability data centre achieving 99.9% uptime for 120+ users.
- Implemented layered endpoint protection, network monitoring, and access control policies — materially reducing the attack surface across all branches.
- Migrated on-premises infrastructure to VMware, reducing hardware costs by ~35% and increasing deployment agility.
- Orchestrated organisation-wide remote working rollout (VPN, Intune, M365) during COVID-19 — 98% workforce ready within 72 hours.
- Managed full IT asset lifecycle, vendor relationships, procurement, and IT budget — projects consistently delivered on time and under budget.

IT Infrastructure Officer

StarLife Assurance Company Ltd *Sep 2012 – Jun 2014*

Enterprise infrastructure and LifeMaster insurance platform support across multiple branch offices.

- Designed and implemented network security controls and DR processes across distributed branch offices.
- Executed infrastructure upgrade from Windows Server 2003 to 2008 and modernised SQL Server environments.
- Delivered structured IT training for 50+ staff, improving productivity and reducing support ticket volumes.

Accounts Officer & Stores Manager

StarLife Assurance Company Ltd *Oct 2006 – Oct 2012*

Finance, operations, and IT process improvement across 3+ regional offices — the foundation of the risk awareness applied throughout a technology career.

- Developed a Microsoft Access automation system reducing commission processing time from 72 hours to 12 hours — an 83% efficiency gain.
- Built Excel dashboards tracking utilities, payments, and procurement spend across 3+ offices, improving financial visibility and audit readiness.

KEY DEVOPS PROJECTS — THE CLOUDADVISORY OY

Full-Stack 3-Tier AWS Deployment (Capstone) *Jan–Feb 2026*
Next.js frontend on EC2 behind a public ALB, Node.js/Express API on private EC2 behind an internal ALB, Amazon RDS MySQL in a private subnet. Strict tier isolation via Security Groups, health checks, systemd persistence. Validated: Browser → Public ALB → Web EC2 → Internal ALB → App EC2 → RDS.

3-Tier Architecture on Microsoft Azure *Feb 2026*
Next.js/Nginx on public VMs, Node.js/PM2 on private VMs, Azure MySQL Flexible Server with HA and read replica. Custom VNet, NSGs, private subnets, SSL enforcement. Debugged JSON config errors, Nginx port binding, reverse proxy misconfigurations under real production conditions.

Terraform Infrastructure as Code — AWS Full Stack *Jan–Feb 2026*
Complete AWS stack from code: VPC, subnets, Internet Gateway, Route Tables, Security Groups, EC2, RDS MySQL. Plus S3 + CloudFront static site via agentic Terraform pipeline (scaffold → plan → apply → deploy → CloudFront invalidation).

Highly Available AWS Deployment with Auto Scaling *Jan 2026*
Custom VPC across two AZs, ALB, Auto Scaling Group with Launch Templates. Validated zero-downtime HA by terminating instances mid-traffic and confirming automatic replacement.

AI-Assisted Agentic Infrastructure Security Review *Feb 2026*
Claude Code and MCP subagents auditing Terraform for TLS weaknesses, S3 access controls, CloudFront OAC, HTTPS enforcement, and state management. Triaged 8 confirmed security findings in a structured audit → verify → improve loop.

Agile Sprint — Jira → Git → AWS Deployment *Feb 2026*
Full Agile delivery: Jira backlog, Fibonacci estimation, 5-day daily shipping, burndown chart, and full traceability from ticket through Git branch, PR, deployment, and validation.

GitHub Collaboration — Fork → Branch → Pull Request *Feb 2026*
Real-world open-source contribution workflow: fork, feature branch, atomic commits, upstream sync, and clean Pull Request — full audit trail throughout.

KEY CYBERSECURITY PROJECTS — MSC, ROBERT GORDON UNIVERSITY

Network Intrusion Investigation & SIEM Monitoring *Feb–May 2024*
Security Onion SIEM deployment to investigate simulated ransomware intrusion. IDS packet analysis and log forensics traced infection to a spear-phishing campaign. Professional incident report with remediation recommendations produced.

Web Application Penetration Testing & Hardening *Feb–May 2024*
Black-box assessment exploiting SQL injection, file upload bypass, XSS, and authentication weaknesses on XAMPP. Implemented secure coding fixes and Apache hardening. Tools: Burp Suite, OWASP methodology.

Digital Forensics Investigation — Insider Threat *Feb–May 2024*
Full forensic analysis of disk images, memory captures, and network traffic. Reconstructed attack timeline and produced a professional incident report. Tools: Autopsy, Volatility.

Black-Box Security Assessment (MITRE ATT&CK) *Oct–Dec 2024*
Adversary simulation in Kali Linux lab: reconnaissance, vulnerability discovery, exploitation, post-exploitation. Findings mapped to MITRE ATT&CK TTPs. Executive CISO presentation with risk-based remediation delivered.

Threat Modelling — Enterprise Case Study (Buzzle) *Oct–Dec 2024*
Socio-technical security assessment modelling assets, user personas, data flows, and trust boundaries. Threat modelling and risk analysis produced recommendations to reduce human error and strengthen security posture.

ISO 27001 / NIST Gap Analysis & Risk Assessment *Oct–Dec 2024*
Enterprise risk register, ISO 27001 and NIST CSF gap analysis, and 1-year security improvement programme designed to strengthen cyber hygiene and compliance.

Machine Learning for Spam & Phishing Detection *Oct–Dec 2024*
Supervised ML classification model on a large real-world dataset. Feature engineering, model selection, evaluation metrics. Security and ethical considerations of AI-based detection analysed.

PROFESSIONAL PROFILE

A deliberate career progression from financial operations to enterprise IT to Cybersecurity and DevOps — each stage building on the last. Active LinkedIn contributor on DevOps, cloud architecture, cybersecurity, and AI governance. Mentors beginners transitioning into tech and contributes to structured learning communities focused on disciplined, practical skill development.