ANSHIO RENIN

Dublin, Ireland | anshiorenin2001@gmail.com | +353 89 980 4804 | LinkedIn | GitHub | Portfolio

PROFILE

MSc Cybersecurity graduate and CompTIA Security+ certified analyst based in Dublin, focused on security operations and detection engineering. I operate a Wazuh SIEM and XDR lab where I triage alerts, investigate root cause and respond end to end, and I authored a detection the platform was missing for LSASS credential dumping, validated across 22 alerts and mapped to MITRE ATT&CK T1003.001. I hunt proactively across SIEM data with SQL, validate coverage with Atomic Red Team, and I have built a distributed IoT intrusion-detection system for my dissertation, run SAST and DAST assessments, and automated cloud deployments with Terraform, Ansible and GitHub Actions. I work across Azure, Microsoft 365 and Entra ID, know NIST CSF and ISO 27001, and script in Python and PowerShell. Open to roles anywhere in Ireland and happy to relocate. Eligible to work in Ireland under Stamp 1G graduate permission, no employment permit or sponsorship required, available immediately.

SKILLS

- **Security Operations:** SIEM Monitoring, Wazuh (SIEM/XDR), Sysmon, Alert Triage, Threat Detection, Detection Engineering, Threat Hunting, Incident Response, MITRE ATT&CK, Log Analysis and Correlation
- **Detection Engineering:** Detection authoring and tuning, false positive reduction, alerting thresholds, IDS/IPS rule writing, MITRE ATT&CK coverage mapping, Atomic Red Team validation, SQL threat hunting
- **Network Security:** TCP/IP, DNS, DHCP, HTTP/S, VLANs, Firewalls, VPN and IPSec, Wireshark, SNORT IDS/IPS, Network Monitoring
- **Microsoft and Endpoint:** Microsoft 365, Microsoft Entra ID (Azure AD), Conditional Access, Microsoft Defender for Endpoint, EDR/XDR concepts, Active Directory, Group Policy, Windows 10/11, Windows Server
- **Vulnerability and AppSec:** Vulnerability Assessment, risk-based prioritisation and remediation, SAST (SonarQube, Semgrep), DAST (OWASP ZAP, Burp Suite), OWASP Top 10, CVE/CWE Triage
- **Cloud:** Azure Security Concepts, AWS (EC2, IAM), Terraform, Docker, GitHub Actions CI/CD, Zero Trust, Least Privilege, CIS Hardening
- **Governance and Risk:** ISO 27001, NIST CSF, NIS2, CIS Controls, GDPR Awareness, Risk Assessment and Risk Registers, Control Testing, Audit Support, Policy Documentation
- **Programming:** Python, PowerShell, Bash, SQL, C, REST APIs, Local LLM integration (Ollama), Prompt-injection Hardening

WORK EXPERIENCE

Cybersecurity Intern | Prodigy InfoTech | Remote | Apr 2026 - May 2026

- Built five Python security tools covering network packet analysis, cryptography utilities and password strength assessment.
- Applied log and network traffic analysis to practical technical tasks and automated repeatable security workflows in Python.
- Documented each tool clearly so other team members could run and extend the work.

Supervisor | Centra | Dublin, Ireland | Sep 2024 - Present

- Act as manager in the store manager's absence: run daily operations, oversee and delegate to staff, and own decisions during trading.
- Deliver front-line customer service in a high-volume environment, resolving queries and escalating issues appropriately.
- Manage stock ordering and supplier coordination, and complete weekly cash reconciliation and till counts to a strict accuracy standard.
- Work rotating shifts including evenings and weekends, maintaining service quality under time pressure.

PROJECTS

- **AI-Assisted SOC Detection Lab** *(Wazuh, Sysmon, Python, SQL, Ollama)*: Built a Wazuh SIEM monitoring lab on Linux, analysed and hunted across 241 security events in SQL, and authored a custom detection rule that closed a coverage gap, validated across 22 alerts and mapped to MITRE ATT&CK T1003.001. Integrated a local LLM for automated indicator enrichment and triage.
- **Network Intrusion Detection System (SNORT)** *(SNORT, Linux, IDS)*: Deployed and configured SNORT IDS with 8 custom rules for port scanning, brute force, SQL injection and DNS abuse. Analysed and triaged the resulting alerts to resolution, tuning rules with detection filters to reduce false positives, and produced prioritised written incident reports.
- **DCIS Mesh: Distributed IoT Threat Detection (MSc Dissertation)** *(Python, MQTT, Raspberry Pi, ESP32)*: Designed, built and tested a distributed detection system across Windows, Raspberry Pi and ESP32 nodes. Tested against 450+ attack instances across 40+ distinct attack types, achieving 88 to 100% detection depending on node density.
- **Automated Secure Cloud Deployment** *(AWS, Docker, Ansible, GitHub Actions)*: Automated an AWS deployment with Terraform, Ansible and GitHub Actions, keeping the SSH key in encrypted GitHub Secrets rather than in the repository and validating the build through a CI pipeline on every commit; documented an honest hardening backlog for the parts not yet production-ready.
- **Application Security Assessment (SAST/DAST)** *(Snyk, SonarQube, Semgrep, OWASP ZAP)*: Performed structured static and dynamic testing on vulnerable web applications: identified 16 high-severity issues on OWASP WebGoat (10 via Snyk dependency scanning, 6 via OWASP ZAP), and separately reviewed MoinMaster and Hackazon with SonarQube and Semgrep, producing prioritised remediation for non-specialist stakeholders.

EDUCATION

- MSc in Cybersecurity, Dublin Business School, Dublin, Ireland | Second Class Honours Grade 1 (2:1) | 2024 - 2025. Specialisation: Distributed Systems Security and Threat Detection.
- BE in Electronics and Communication Engineering, KSR Institute of Engineering and Technology, India | 8.76/10 CGPA, First Class | 2019 - 2023.

CERTIFICATIONS AND TRAINING

- CompTIA Security+ (SY0-701) - Certified, July 2026.
- Google Cybersecurity Professional Certificate. | TryHackMe Cyber Security 101 Path.
- Job Simulations (Forage): Deloitte Cyber, Mastercard Cybersecurity, TCS Cybersecurity - breach response, phishing analysis and IAM access-control scenarios.
- Work Authorisation: Stamp 1G graduate permission. Full-time work rights in Ireland, no employment permit or sponsorship required. Available immediately.