Romy Peter

Dublin, Ireland | +353 85 225 8824 | romysvn.p@gmail.com
romy2k.com | linkedin.com/in/romy-peter | github.com/rsvptr
Work authorisation: Stamp 1 (Critical Skills Employment Permit)

Summary

Cybersecurity graduate at Iarnród Éireann (Irish Rail), working across security operations, incident response, business continuity and GRC for a national critical-infrastructure operator. MEng in Cyber Security, First Class Honours; CompTIA A+ and INE eJPT certified. Takes stalled or undefined problems through to documented, audit-ready outcomes.

Experience

Cybersecurity Graduate
Oct 2025 - Present

Iarnród Éireann (Irish Rail) — *Dublin, Ireland*

Cybersecurity graduate on a rotational programme (security operations, business continuity, governance, risk & compliance, and operational technology security) for a national railway operator and critical-infrastructure provider.

- Triaged the central cyber mailbox and handled phishing and account-compromise cases using Microsoft Defender (analysis, containment, IOC extraction).
- Scribed and authored SitReps, executive summaries and post-incident reports for major-incident bridges and cyber crisis exercises, including ENISA/NCSC Cyber Europe 2026.
- Owned high-volume access-review queues in ServiceNow (170+ USB/removable-media reviews, plus external and overseas reviews from Active Directory), enforcing least privilege.
- Ran proactive threat hunting and OSINT investigations into public-domain data exposure (including a CVSS 6.5 finding), and supported penetration-test coordination and vulnerability research.
- Assessed Microsoft 365 Copilot data-exposure risk ahead of rollout and set out Microsoft Purview (DLP, sensitivity labels) and Entra ID access-review controls.
- Authored security policy, incident-response playbooks (NIST 800-61r2, NIS2, GDPR) and GDPR DPIAs, including an evidence-based external-access policy.
- Developed and maintained BIAs and BCPs across ICT (RTO/RPO/MTD/MBCO), coordinated disaster-recovery tests and tabletop exercises end to end, and helped formalise the DR-testing process.
- Led the procurement and onboarding of an out-of-band Google Workspace business-continuity platform end to end (a five-figure investment), and built bulk-SMS alerting and process automation.

IT & Security Support
Jul 2023 - Jun 2024

Freelance — *Muscat, Oman*

- Built a small business's online presence end to end: domain, a multi-page website and hosting, business email, and basic protection (web application firewall and third-party DDoS protection) on a hardened security baseline.
- Refurbished and set up end-user computers, imaging machines over network boot, installing and updating operating systems and software, and tuning older hardware for reliability.
- Hardened small-office networks by updating router firmware, setting strong credentials, applying QoS, turning off insecure features such as WPS, and monitoring connected devices.
- Applied security basics across client systems: patching, system hardening, least-privilege account separation, monitoring for unauthorised access, and simple data backup and redundancy.
- Diagnosed and resolved hardware, software and network issues for clients, minimising downtime and keeping day-to-day operations running.

Education

University of Limerick
Sep 2024 - Aug 2025

Master of Engineering in Cyber Security, First Class Honours (1.1) — *Limerick, Ireland*

Indian Institute of Information Technology, Sri City
Aug 2019 - Jun 2023

Bachelor of Technology in Computer Science & Engineering, GPA 8.04/10 — *Andhra Pradesh, India*

Technical Skills

Security operations: incident response, phishing analysis, threat hunting, OSINT, SIEM, vulnerability management, penetration-test coordination; Microsoft 365 Defender, ServiceNow, Qualys, SOCRadar, UpGuard

Identity & access management: Microsoft Entra ID, Active Directory, MFA and Conditional Access, LAPS, access reviews, least privilege

Cloud & data security: Microsoft 365, Google Workspace, cloud security, Microsoft Purview (DLP, sensitivity labels, data classification), DNS and email security (SPF/DKIM/DMARC/MX)

Governance, risk & compliance: security policy development, risk assessment, GDPR and DPIA (Article 35), third-party risk management, ITIL; NIST CSF 2.0, NIST SP 800-61r2, ISO/IEC 27001, ISO 22301, NIS2, CER, MITRE ATT&CK, CIS Controls, NCSC/CSIRT reporting, ENISA exercise framework

Business continuity & resilience: business impact analysis, business continuity planning, disaster-recovery testing, recovery metrics (MTD/MBCO/RTO/RPO), crisis communications

Security engineering & AI: Python, network security, IDS/IPS, cryptography, application security, AI security, security awareness training, prompt engineering and adversarial testing; Claude Code, LLMs

Automation, documentation & collaboration: technical writing, stakeholder management, Microsoft Power Automate, Power Apps, SharePoint, Microsoft 365 Copilot, Jira, Confluence, Excel, Visio, Lucidchart, PlantUML

Certifications

CompTIA A+ | *Issued Nov 2024 · Expires Nov 2027* — Credential ID KV2Q8RCYYFREQP3E

INE eJPT (Junior Penetration Tester) | *Issued Nov 2023 · Expires Nov 2026* — Credential ID 88259711

In progress: CompTIA Network+ and Security+

Projects

RailSecure

Next.js, React, TypeScript, Claude API, NVD CVE API — *railsecure.vercel.app*

- Rail-focused cyber-readiness platform combining phishing training, incident drills, playbook generation, compliance Q&A, a live CVE feed and awareness content in a single workspace.
- Built on schema-constrained AI workflows rather than a free-form chatbot, with server-side prompt-injection guardrails and rate limiting.

Firewall Logging & Automated Incident Response

MEng thesis · Python, TensorFlow, Scapy, nftables — *github.com/rsvptr/firewall-logging-incident-response*

- Automated network-defence system pairing a hybrid IDS (rule-based detection plus a CNN for flow anomalies) with a playbook-driven response engine that auto-contains threats through nftables blocking or honeypot redirection.
- MITRE-mapped playbooks, real-time dashboard and integrated LLM assistant; validated in a four-VM lab, handling thousands of attack events at sub-second to low-second detection and containment.

CrypticComm

Next.js, React, TypeScript, Web Crypto API — *crypticcomm.vercel.app*

- Browser-based RSA workspace covering key generation, OAEP encryption, RSA-PSS signing, an AES-GCM encrypted wallet and WebRTC peer chat, all local via the Web Crypto API; backed by 34 crypto unit tests.

Earlier ML/NLP projects

Python, scikit-learn, NLTK, Streamlit

- **FactGuard**: fake-news classifier that judges writing style rather than topic, 0.97 accuracy on unseen articles (factguard.streamlit.app).
- **Deb8**: clickbait-headline detector trained on around 52,000 headlines, 0.93 accuracy (deb-eight.streamlit.app).

Volunteering

UL Global Student Ambassador | *University of Limerick* — **Sep 2024 - May 2025**

Created content for UL Global's social channels across two semesters (blogs, photos, videos and graphics), and represented UL at webinars, orientations and campus visits with event coverage and videography. Answered prospective and current international students' questions by email and social media, sharing first-hand experience to help them settle in. Contributed volunteer hours toward the UL President's Volunteer Award and received a Certificate of Completion and a programme reference from UL Global.

Interests

Photography, Audiophile Equipment, Graphic Design, Video Production, Classic Cinema, Retro Gaming