Role: Cyber Security Risk and Vulnerability (RVM) Lead
Area: Business Services
Sub-Area: IT – Security & Operations Technology
Location: Cork/Dublin
Salary: Competitive

Duration: Permanent **Ref:** GNI995

Gas Networks Ireland operates and maintains Ireland's €3bn, 14,725km national gas network, which is considered one of the safest and most modern renewables-ready gas networks in the world.

Almost 725,000 Irish homes and businesses trust Ireland's gas network to provide efficient and reliable energy to meet their heating, cooking, manufacturing and transport needs.

The gas network is the cornerstone of Ireland's energy system, securely supplying more than 30% of Ireland's total energy and over 40% of the country's electricity generation.

Gas Networks Ireland is aiming to deliver a repurposed, resized and fully decarbonised gas network by 2045. Its "Pathway to a Net Zero Carbon Network" envisions transforming the existing gas network into two separate systems carrying 100% renewable gas, one dedicated to biomethane and the other to green hydrogen, with the potential to carry approximately 30% biomethane and 70% green hydrogen, as well as offering significant long term energy export opportunities.

Gas Networks is an organisation with a very strong legacy and a culture founded on pride in our purpose, to keep Irelands energy moving, and commitment to our vision, to be at the heart of Irelands energy future. Our organisational values demonstrate what is important across the organisation including building on our experience across our organisation to build towards our sustainable future, doing what's right for each other and for the people and communities that we serve and finally energised for the change of our future towards a renewable energy landscape. Throughout your career in Gas Networks Ireland, you will be part of an organisation that has a strong commitment to supporting and developing our workforce today and into the future. You will also have an opportunity to get involved in our ambitious iBelong programme ensuring a diverse, equitable and inclusive environment for us all to thrive. Finally, our Time to Talk Mental Health programme and our wellbeing initiatives ensure we provide support across many areas as you work in our organisation.

The Role:

Based in Cork or Dublin and reporting to the Cyber Security Manager, RVM Lead role leads the enterprise-wide Threat and Vulnerability Management (TVM) programme, ensuring proactive identification, assessment, prioritisation, and remediation of cyber risks across IT, OT, and cloud environments. The Risk and Vulnerability Management Lead drives continuous improvement in risk posture through advanced threat hunting, security assessments, cyber threat intelligence integration, attack surface management, insider threat detection, incident response readiness, and robust reporting and metrics. Acting as

the subject matter expert for vulnerability management and cyber resilience, the role collaborates with technical and business stakeholders to safeguard critical assets and enable secure business operations.

Duties and Responsibilities:

1) Threat & Vulnerability Management (TVM)

- Lead the design, implementation, and operation of the TVM programme, covering IT, OT, and cloud environments
- Oversee vulnerability scanning, detection, classification, and assessment using industry-standard tools (e.g., Qualys, Tenable, Rapid7)
- Ensure risk-based prioritisation of vulnerabilities using CVSS, asset criticality, and real-time threat intelligence
- Drive remediation planning and execution, including emergency patching and coordination with system/application owners
- Maintain comprehensive vulnerability reporting, dashboards, and historical trend analysis for stakeholders.
- Lead vendor relationship and performance management for the **TVM managed service**, ensuring quality standards, and integration with internal workflows.

2) Threat Hunting & Security Assessments

- Conduct proactive **threat hunting** across enterprise telemetry (EDR, SIEM, network, cloud) to identify emerging risks and suspicious activity
- Lead and coordinate **security assessments**, including penetration testing, red and blue team exercises, and regulatory reviews
- Integrate findings from threat hunting and assessments into the TVM and incident response processes.

3) Cyber Threat Intelligence (CTI)

- Ingest, analyse, and operationalise **cyber threat intelligence** feeds to contextualise vulnerabilities and inform risk decisions
- Monitor the **global threat landscape** for new vulnerabilities, attack patterns, and threat actor behaviours
- Participate in industry threat intelligence sharing communities (e.g., ISACs) and collaborate with trusted partners.

4) Attack Surface Management

- Map and continuously monitor GNI attack surface, including external exposures, cloud assets, and third-party connections
- Identify and assess changes in the attack surface structure resulting from new deployments, data or information flow integrations, or business initiatives
- Recommend and implement controls to reduce exposure and harden critical assets.

5) Insider Threat Detection

- Develop and maintain insider threat detection capabilities, leveraging behavioural analytics, DLP, and SIEM integrations
- Investigate anomalous activity and coordinate with HR, legal, and compliance teams as required

6) Incident Response Readiness

- Ensure TVM processes are tightly integrated with incident response playbooks and workflows
- Lead vulnerability-driven incident investigations and coordinate rapid containment and remediation actions

- Conduct post-incident reviews and root cause analyses, integrating lessons learned into continuous improvement.

7) Cloud & Third-Party Risk Assessment (TPRA)

- Oversee vulnerability management and risk assessments for cloud platforms (Azure, AWS, GCP) and SaaS applications
- Support third-party risk assessments (lead by Information Security team), ensuring vendors and partners meet enterprise security requirements
- Integrate cloud and third-party risk assessment findings into overall risk posture and reporting.

8) Reporting & Metrics

- Develop and maintain executive dashboards and detailed reports on vulnerability status, remediation progress, risk trends, and security posture
- Track and report key TVM/RVM metrics with overall risk reduction over time
- Present findings and recommendations to senior management, board, and regulatory bodies as required.

9) Mentorship & Collaboration

- Guide junior analysts in advanced threat and vulnerability management practices, while partnering with architects, project teams, and OT stakeholders to ensure robust cyber risk mitigation across IT, OT, and cloud environments.

Knowledge, Skills and Experience:

- Degree in Information Security, IT, or related discipline; advanced degree or certifications (CISSP, CISM, CEH, GIAC) preferred
- 5+ years' experience in cyber risk, vulnerability management, or security operations, with demonstrable leadership in TVM programmes
- Hands-on expertise with vulnerability scanning tools (Qualys, Tenable, Rapid7), SIEM, EDR, and threat intelligence platforms
- Strong understanding of CVSS scoring, exploitability, risk prioritisation, and regulatory frameworks (NIST, ISO, GDPR)
- Capacity to assess risk scenarios, prioritise actions, and propose pragmatic solutions under pressure is essential
- Experience with cloud security, third-party risk assessment, and incident response
- Ability to balance tactical remediation with long-term risk reduction and continuous improvement.
- Excellent communication, stakeholder management, and reporting skills.
- CISSP, CISM, CEH, GIAC (GCIH, GSEC), CompTIA Security+, Azure/AWS/GCP Security Specialist advantageous.

Applications, including current Curriculum Vitae, should be emailed to the following address stating the job title and reference number in the subject line of your email:
recruit@gasnetworks.ie

The closing date for receipt of applications for this vacancy is the 26th November 2025.

Please note that applications submitted after this closing date will not be accepted.

Gas Networks Ireland is an equal opportunities employer

We are committed to providing a diverse and inclusive place of work and have a robust strategy and framework called ibelong to enable this. We are an equal opportunity employer and through our recruitment process we welcome and encourage applications from interested and suitably qualified individuals regardless of gender, age, racial or ethnic origin, membership of the traveller community, religion or beliefs, family or civil status, sexual orientation/gender identity or disability.

GNI will only hold your data for as long as necessary. By providing a CV to GNI you are agreeing for GNI to process this information about you. If you have any question about how GNI processes your data, please see our Privacy Notice. If you have further questions, you can contact us at DataProtection@gasnetworks.ie