Role: Security Analyst (Cyber Security)
Area: Business Services
Sub-Area: IT – Security & Operations Technology
Location: Dublin / Cork
Salary: Competitive

Duration: Permanent **Ref:** GNI993

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, The Security Analyst is a key member of GNI's Security Operations team, responsible for day-to-day security monitoring, incident response, and the administration of security infrastructure across both IT and OT environments. This role combines hands-on technical work with proactive threat detection, vulnerability management, and continuous improvement of security processes. Working closely with internal teams and external partners, the Security Analyst helps ensure

the confidentiality, integrity, and availability of GNI's critical assets, while supporting the business in achieving its strategic objectives.

Duties and Responsibilities:

1) **Security Operations & Infrastructure**

- Oversee the configuration, administration, and ongoing management of firewalls, web proxies, and load balancers to maintain robust perimeter and internal network security.
- Administer and support all IT security hardware and software, including IT and OT firewalls, across on-premises and cloud environments, ensuring optimal functionality and compliance.
- Implement, configure, and administer IT security equipment across GNI sites and data centres, ensuring alignment with security best practices.
- Manage and monitor Intrusion Prevention Systems (IPS), proactively identifying and mitigating potential threats.
- Coordinate and process security-related requests from business units, ensuring prompt and effective resolution in line with organisational policies.
- Liaise with and manage external vendors and service providers to ensure the delivery of high-quality security services.

2) **Security Monitoring, Incident Response & Investigation**

- Actively participate in security incident response activities, including SIEM-generated ticket management and post-incident reviews.
- Lead the investigation, troubleshooting, and resolution of security incidents and service requests, providing clear communication and guidance to stakeholders.
- Develop, update, and maintain comprehensive security documentation, ensuring that all procedures, incidents, and configurations are accurately recorded and accessible.
- Attending critical security matters outside of standard business hours as required, including participation in an on-call rotation.

3) **Threat Intelligence, Vulnerability & Risk Management**

- Conduct cyber threat intelligence activities, including the collection, analysis, and dissemination of threat data to support proactive risk identification and incident response.
- Perform regular threat and vulnerability management scans and remediation, tracking vulnerabilities and supporting risk reduction initiatives.
- Collaborate within a multidisciplinary Infrastructure and Service team, sharing expertise and supporting collective goals to enhance overall security posture.

4) **Strategic Support & Continuous Improvement**

- Provide technical guidance and make strategic recommendations within the IT Infrastructure domain to support business objectives.
- Prioritise and schedule workload based on resources, business priorities, and project timelines.

- Continuously monitor developments in the IT security landscape, applying new insights to strengthen GNI's security framework.
- Demonstrate effective workload prioritisation, scheduling tasks based on available resources, business priorities, and project timelines to maximise efficiency and results.
- Continuously seek opportunities for process improvement and innovation, contributing to the ongoing enhancement of GNI's security posture.

Knowledge, Skills and Experience:

- Bachelor's degree or higher in Information Systems, Computer Science, or a related IT discipline, with a minimum of three years' professional experience in IT Security roles.
- Industry-recognised information security certifications (e.g., CISSP, CISM, CEH, CompTIA Security+) are an advantage.
- In-depth knowledge of firewalls, IDS/IPS, and user authentication mechanisms, including Microsoft Active Directory and Azure Entra ID.
- Strong grasp of TCP/IP protocols, network architectures, and network traffic analysis.
- Hands-on experience with security solutions such as Checkpoint, Palo Alto, F5, and Forcepoint web proxy platforms is an advantage.
- Proficient in cloud security concepts and operations with platforms including Microsoft Azure and Oracle Cloud.
- Demonstrated ability to manage relationships with third-party vendors and service providers.
- Familiarity with security monitoring tools and proactive threat detection and response.
- Experience designing, implementing, and optimising IT technical solutions to enhance security posture.
- Ability to align emerging technologies with business strategy and support core systems in collaboration with partners.
- Excellent written and verbal communication skills, with the ability to interact effectively across technical and non-technical audiences.
- Solid understanding of industry best practices, frameworks, and security toolsets in enterprise environments.
- Proven ability to identify areas for improvement, generate creative solutions, and oversee implementation.
- Self-motivated, analytical, and adept at problem identification, root cause analysis, and delivering actionable recommendations.
- Commitment to continuous professional development and learning.
- Strong drive to set and achieve high performance standards, consistently delivering quality results.
- Experience handling complex and high-pressure situations with a proactive, solutions-oriented approach

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 25th 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