Role: IT Security Analyst
Area: IT Business Operations
Sub-Area: Security
Location: Cork/Dublin

Duration: Fixed term – 2 years **Salary:** Competitive **Ref:** EBS204

Ervia is a commercial semi-state company which provides strategic national gas and water infrastructure and services in Ireland through our regulated businesses, Gas Networks Ireland (GNI) and Irish Water (GNI). Ervia directly employs over 1,600 people who deliver services to 1.6 million customers daily. Our infrastructure supports economic and social development, protects the environment and enhances the health and quality of life of the Irish people. Ervia is currently undergoing an organisational transformation to centralise the IT, HR, Finance and Supply Chain functions through the formation of an Ervia Business Services model. This will create synergies and help create a 'one team' Ervia culture. Ervia's Business Services organisation will define, maintain, and operate end-to-end customer focused IT, HR, Finance, Transaction Services, Business Solutions capabilities and processes in support of the overall Ervia strategic priorities.

Background:

The IT Security Operations area provides IT security support to the business across a wide range of functions including project security management and governance, security project initiation including RFP content, maintenance of existing systems and IT security infrastructure, security enhancements to existing solutions, day-to-day security operations, customer interfaces, security management, IT security standards compliance and quality assurance.

The Role:

Reporting to the Security Operations Manager, the Security SOC/SIEM Analyst has responsibility for supporting the security infrastructure, firewalls, Load Balancers and DMZs, maintaining security tools, recommending new tools, and updating systems. The analyst will be expected to specialise in the SIEM platform and document requirements, procedures, and protocols to ensure that other users have the right resources. The SOC/SIEM Analyst is responsible for the security analysis, incident classification and incident response actions including notification and alerting. Monitors for possible security incidents, using knowledge of attack types and standard protocol behavior to classify incidents, comment, and provide advice on mitigation or remedial actions to the client.

Duties and Responsibilities:

- Monitoring security infrastructure, identifying and reporting Real Time attacks and vulnerabilities on the network.
- Identification of incidents and subsequent analysis and investigation to determine their severity and the response required. Ensure that incidents are correctly reported and documented in accordance with government policy and procedures.
- Responsible for logging of all Security events, patching, monitoring and backing up all Security devices while responding to any potential attacks.
- Responsible for coordinating the effort to remediate security alerts and respond to security related incidents. Provide a Technical Escalation Point during security incidents, establishing the extent of an attack, the business impacts, and advising on how best to contain the incident along with advice on systems hardening and mitigation measures to prevent a reoccurrence.
- Enforce Ervia security policies to protect the environment from potential security breaches.
- Determine security violations and inefficiencies by conducting periodic Infrastructure reviews.
- Performing regular Threat and Vulnerability scans and Penetration testing management.

- Contributing to and maintaining the Group or local IT Security, Risk and Compliance framework that meets regulatory requirements and protects the information and technology assets.
- May be required to identify, extract and document evidence stored on IT systems in order to identify and help prove responsibility for any security incident.
- Identifying trends in monitoring old and new Use Cases, suggest new Use Cases based on industry trends and/or observed monitoring data.
- Other related security activities as directed.
- Assists in selection, installation, and adoption decisions for automated tools that enforce or monitor the compliance with information security policies, procedures, standards, and similar information security requirements.
- Stay informed about the latest developments in the SOC/SIEM information security field, including new products and services. Maintain a keen understanding of evolving threats and vulnerabilities to ensure the security of the network.
- Familiar in IOC of threat indicators
- Keeping up to date on IT security issues and developments.
- To ensure Accountability for all security operations carried out on Information Systems.
- Participate as a technical advisor for a variety of ad-hoc information security projects that will be dictated by current business and technological developments.

Knowledge, Skills and Experience:

- Degree or equivalent in Information Systems or IT discipline with a minimum of 3 years relevant IT and security experience.
- Three years of proven experience in a SOC/SIEM environment and implementation within medium to large organizations.
- Experience in working with at least one SIEM solution
- Deep understanding of cybersecurity threats and enterprise defences
- A thorough understanding of operational security infrastructure controls such as Firewalls, IPS/IDS, Internet proxies PKI Infrastructure, prevention products and methodology as well as various user authentication products
- Experience in managing communications in managed service teams/outsourced teams
- Strong security Knowledge
- Experience in security patch management, security incident and event management.

- Deep understanding of security for Linux/Windows servers, and related TCP/IP protocols. Experience with secure configuration for Linux and Windows servers
- Experience with WLAN security protocols and tools, such as 802.1X, LEAP, PEAP, WPA, and VPN technologies
- Knowledge of Qualys TVM is desirable.
- Strong familiarity with the development and deployment of secure web technologies required
- Strong communication and reporting skills for delivery to both technical and non-technical audience
- This position may require some attendance outside of normal working hours.
- This position may require participation in an On Call Rota
- Demonstrates independent decision-making abilities
- Experience with identifying improvement opportunities, generating ideas and implementing solutions
- Enthusiastic self starter that has excellent analytical skills with the ability to identify and analyse problems, propose potential improvements, and implement these solutions.
- Ability to set up ongoing procedures to collect and review information.
- Proactively identifying new areas of learning and using newly gained knowledge or skills on the job.
- Ability to set own high standards of performance and delivering desired results.

The closing date for receipt of applications for this vacancy is 14th April 2020

Applications, including a current Curriculum Vitae should be emailed to: **recruit@ervia.ie**

Please include the Reference Number for this Role when making an application

Ervia is an equal opportunities employer