Northern Ireland Electricity Networks

CYBER SECURITY TECHNICAL ANALYST ROLE SPECIFICATION

BACKGROUND

The NIE Networks Chief Information Office (CIO) team is responsible for the management of IT and Telecoms, including the development of IT Strategy, Data and Cyber Security Management, IT Governance, Application development & support, and the effective management of some specific outsourced services to meet business requirements.

Effective Cyber Security governance is recognised by NIE Networks as a critical part of our business activities. As an Operator of Essential Services and part of the Critical National Infrastructure, NIE Networks needs to continually evolve to combat the increasing number of cyber threats and risks facing the organisation.

NIE Networks is also committed to developing new technological and data sharing solutions which will assist the future distribution and management of electricity. This will involve much greater use of IP connectivity and the Internet of Things (IOT) as we move to a distributed network service model (DNS). This presents a great opportunity to be at the forefront of delivering new systems, services and processes to match the evolving technologies and cyber security solutions.

An exciting opportunity has arisen for a Cyber Security Technical Analyst (CSTA) to assist on all aspects of our technical Cyber Security services and development programmes. The primary focus of the role will be to ensure that cyber security services, processes and policies are compatible with incoming and existing systems and services whilst meeting developing regulations and cyber security standards. This is a challenging role in a fast-developing area where effective cyber security analysis and management are recognised as essential to the business.

Candidates should note that this role is based at our recently refurbished Danesfort office which is situated just off the Stranmillis Road in Belfast. We also offer home working opportunities via our Agile Home Working policy but on a hybrid basis.

THE ROLE

Reporting to the Cyber Security Architect, the Cyber Security Technical Analyst (CSTA) will be a key member of both the Cyber Security and Data Protection team and the wider company (CIO) team. They will help to ensure that the company's cyber security services operate effectively with respect to cyber security and data protection. A key objective of the role is to support effective delivery of cyber security services across the business in line with the agreed risk appetite framework.

The CSTA will also be required to work with key stakeholders and end users to ensure that business requirements are fully reflected in the operational delivery and management of cyber security services.

The principal duties of the post include:

- Assisting with the operational management and monitoring of some specific outsourced cyber security services to ensure they are delivered in a high quality and cost effective manner.
- Assisting stakeholders to ensure that BAU activities such as infrastructure or system upgrades, updates or patches are approved or implemented within agreed timescales and in line with cyber security principles, policies and standards.
- Working with the Cyber Security Architect in the development of the NIE Networks cyber security architecture, providing technical assistance for the development of solutions within that area.
- Supporting the cyber and data team with the implementation of IT projects. Assisting with the co-ordination of cyber security requirements for design, implementation and transition phases of projects.
- Assisting with the development of cyber security documentation such as policies, procedures and standards. Supporting the review process for documentation of existing cyber security architecture, ensuring it is maintained and is accessible to all interested parties.
- Assiting with the due diligence process for cyber and data security suppliers, and providing technical cyber analysis support in product and vendor selection.

- Supporting the investigation, evaluation, selection and documentation of new approaches, methods and technologies, conducting research and providing documented and evaluated technical options to meet requirements.
- Assist with creating relationships and communication channels with key internal and external stakeholders to ensure that all relevant areas of the business are represented in the design of solutions.
- Support detection engineering processes encompassing areas such as threat hunting, threat intelligence analysis and purple teaming techniques. This should include areas such as managed detection & response solutions.
- Providing assistance with cyber threat intelligence analysis from multiple sources such as CISA, NCSC, MISP, Mitre Attack sources and in conjunction with existing suppliers.
- Assisting with the development and implementation of cyber and data awareness training programme, phishing campaigns and simulated red team exercises.

THE INDIVIDUAL

Essential Criteria

- A minimum of 5 years relevant technical cyber security experience.
- Experience of working in delivering technical cyber security analysis and assistance against a set security framework, such as NIS or NIST.
- Previous experience in liaising with business end users.
- Previous IT Project experience.

Desirable Criteria

- Relevant technical cyber security qualifications.

CORE COMPETENCIES

The person appointed must demonstrate the following core competencies:

Communication

Able to communicate information and ideas clearly and articulately both in oral and written form. Uses appropriate language, style and methods depending on audience and the purpose of communication. Able to convey complex information clearly. Anticipates the information that others will need.

Result-Orientedness

The ability to take direct action in order to attain or exceeded objectives.

Organised

Able to achieve results in a quality, timely, and cost-effective way. Sees priorities, plans the efficient use of resources, and monitors progress against objectives. Anticipates crucial stages in projects. Formulates alternative means of achieving objectives. Responds effectively to unforeseen events.

Team Work

Actively participates in team. Encourages co-operation. Aware of the needs of others and responds flexibly. Shares information and supports other team members. Can get things done through others and set realistic objectives. Seeks opportunities to develop others. Prioritises team goals over individual goals.

Customer Orientation

The ability and willingness to find out what the customer wants and needs and to act accordingly, taking the organisations costs and benefits into account.

Flexibility / Adaptability

Has actively sought to learn new things on own initiative. Has responded positively to change and adapted to new situations quickly. Able to take on a diverse range of tasks equally effectively.

ADDITIONAL INFORMATION

Candidates should be able to demonstrate through interview a wide range of specific skills and experience in the following areas:

- Experience of working in cyber security, demonstrating clearly where the work has involved technical cyber security tasks within projects and programmes.
- Ability to understand and demonstrate the importance of effective cyber security analysis in the delivery of a cyber security service.
- A good understanding of Network and Information Systems (NIS) and NCSC security guidance, utility industry standards and the application to enterprise, SCADA and OTN systems and services.
- Ability to understand and work in incident management response with a systematic and logical approach to solving complex problems, providing a high attention to detail.
- Understand the importance of identifying, assessing, threat intelligence and risk assessments.
- Able to assist with the development and delivery of projects for attaining Cyber Security Industry certifications and compliance.
- An understanding of NPSA physical, personnel, procedural and security controls and how to apply them to a CNI.

The nature of the job will change over time in line with the needs of the business. It is a requirement of the jobholder to contribute to the development of the role reflecting these changing requirements.

THE PACKAGE

The remuneration package for this position will be dependent on the successful candidate's skills and experience. The company also offers many other **benefits**. (The QR code will take you to the benefits section of our website).

OUR PEOPLE MATTER

At NIE Networks we realise our employees are at the heart of our success and they are the future of an ever-changing energy industry. With employee wellbeing at the core of our approach, we are continually investing in our people and are committed to helping every individual reach their full potential through both professional and personal development. We believe in nurturing effective teams and high performing leaders to deliver the best possible service for our customers.

DISABILITY

NIE Networks will provide reasonable support to disabled applicants throughout the recruitment process. Applicants who may require special arrangements should identify this clearly within their application form to enable us to make any appropriate adjustments.

DIVERSITY AND INCLUSION

NIE Networks has achieved Silver, Diversity Mark Accrediation and is committed to equality of opportunity and acknowledges the unique contribution that all potential candidates can bring in terms of their education, ethnicity, race, gender, nationality, age, religion, disability, sexual orientation and opinions. Applications are positively welcomed from all backgrounds and appointments are made on merit following a fair, open and transparent selection process.

HOW TO APPLY

Please submit a CV and cover letter together (detailing alignment to the essential criteria) via the NIE Networks recruitment portal www.nienetworks.co.uk/jobs (the best experience of this portal will be through the **Google Chrome** internet browser or click on the QR code)

- Once you are in the careers page select the Cyber Security Technical Analyst role and click on **"Apply Now".**
- You will initially be asked to create a "Candidate Area" by inputting your email address and a secure password – once you select "Create Candidate Area" you can then log in directly using these same details. The address that you register with will be the address that we contact you on.
- Select **"Apply for Vacancy"**
- Once you have created your profile upload both your CV and Cover Letter within your application..
- Please ensure to review your CV before submission as you will not have the opportunity to amend the CV once it has been submitted.
- You will receive an email confirmation once your CV and Cover Letter has been submitted (Please check your junk mail too).
- Late applications will not be accepted

Completed CV's and cover letter must be submitted no later than **11pm on Sunday 8 December 2024**

NIE Networks is committed to the principles of public appointments based on merit with independent assessment, openness and transparency of process.

FOR YOUR INFORMATION

If you would like to view up to date information about NIE Networks please visit our website www.nienetworks.co.uk or scan the QR codes below.

About NIE Networks

About NIE Networks History

Or alternatively check out our social media platforms via the links provided on each graphic below.