JOB DESCRIPTION

JOB TITLE:	SOC Engineer	**LOCATION**	Daresbury
DEPARTMENT:	Information Security	**DEADLINE**	TBC

ABOUT ITS

We exist to ensure the UK has the best full fibre networks, to provide the best gigabit capable connectivity and broadband to UK businesses through our growing partner community. This enables opportunity, progress, exploration, creativity, innovation and commerce. Rapidly advancing technology means there's never been a more exciting time; for you, for business, and for the future.

ROLE DESCRIPTION:

We are experiencing a fantastic period of growth, and to support this, we are looking to bring on a skilled Security Operations Engineer to join our organisation. As a Security Operations Engineer, your key responsibility will be to manage and optimise best-in-breed security tools, such as Vulnerability Management Detection and Response (VMDR), Extended Detection and Response (XDR), Security Information and Event Management (SIEM), AI-driven email protection, and Privileged Access Management systems. Your role will focus on ensuring these embedded technologies operate effectively and are continually fine-tuned to meet evolving security and operational needs.

You will play a crucial role in monitoring and maintaining the environment, ensuring adherence to security policies and frameworks while actively contributing to process improvement. Your performance will be measured by your ability to reduce vulnerabilities, enhance operational efficiency, and support key metrics, such as time to remediate and time to mitigate. By leveraging and optimising advanced security tooling, including SIEM systems for enhanced threat detection and incident response, you will directly contribute to the organisation's resilience and success.

Sitting within the Information Security team, the role will involve the following:

KEY RESPONSIBILITIES:

The key accountabilities and responsibilities include but are not limited to:

- Respond promptly to security incidents, conduct thorough investigations, and implement corrective measures.
- Create technical documentation to assist colleagues in root cause analysis, and procedures.
- Responsible for monitoring the ITS technology stack, VMDR, XDR, MSFT Security, AWS Security.
- Manage security tools and software, ensuring they are up to date and effectively protecting the organisations assets.
- Conduct regular system and network security assessments to identify vulnerabilities and mitigate.
- Penetration testing analysis and remediation activities.
- Monitor access control to prevent unauthorised access, data breaches, and cyber-attacks.
- Stay up to date with the threat landscape.
- Partner with other teams, such as Systems, NOC, Network Architecture and Design and system owners, to ensure security is embedded.
- Contribute to building a culture of security awareness.
- Create and improve incident playbooks and runbooks.

JOB DESCRIPTION

ABOUT YOU

You will be and have a demonstrable track record of:

- Passionate about Information and Cuber Security.
- Information Security, Cyber Security or Network Security.
- Experience or demonstrable knowledge in log analysis and PCAP analysis.
- A solid understanding in the approach threat actors take to attacking a network, phishing, port scanning, web application attacks, DDoS, lateral movement.
- Demonstrable knowledge in network fundamentals, for example, OSI Stack, TCP/IP, DNS, HTTP(S).
- Working knowledge of security management frameworks - ISO27001, NIST, TSA
- Experience of implementing and developing key control mechanisms, to improve security posture.
- Experience of reporting on key control mechanisms, e.g. monthly, quarterly or annually.
- Excellent communication skills both verbal and written.
- Self-motivation and drive to meet objectives and targets.
- Analysis, organisation, and planning skills.
- Excellent time management skills.
- Flexibility in your approach to change and challenge.
- MSc Cyber Security, ISC CC, CompTIA SEC +, CySA, Network+.

Note:
All job descriptions outline the key accountabilities and requirements for the role and will form the basis for individual performance assessments/reviews. These are non contractual and are subject to review and amendment from time to time as seen necessary by the organisation.