Job Title: Security Analyst

Location: Lutterworth, UK
Reports To: Head of IT and CISO
Work Conditions: Monday-Friday, 08:30 to 17:00. Hybrid working, minimum 2 days in the office (some working hours may be remote working from home)

Purpose:

Ensuring the operational security of our current and future IT estate and providing a first line response to security events. Drive ongoing service improvements and security standards across the organisation. Coordinate and maintain processes and documentation for ISO and Cyber Essentials Plus certification. Provide detailed insights, metrics and reports for the CISO, informing the wider security strategy to meet the changing business needs, emerging technologies, and future operational requirements.

Key Responsibilities:

- **Security Operations and Posture** – Managing and improving the organisation's overall security posture, including monitoring security alerts, assessing risks, and coordinating remediation activities, responding to vulnerabilities, threats and vendor security notifications, ensuring a strong and continuously improving security environment and enhancing Microsoft 365 and Defender security scores. Implementing key security technologies.

- **Identity and Access Management** – Manage and secure identity and access controls across Microsoft Entra, Azure, Intune, Jira, AWS, and other SaaS platforms by maintaining Conditional Access, MFA, Privileged Identity Management (PIM), and Identity Protection. Ensure IAM follows best practices, including regular access reviews for privileged, guest, and service accounts.

- **Microsoft Security Stack** – Implement and maintain Microsoft Sentinel and Purview, and configure and tune Defender suite.

- **Vulnerability Management and Penetration Testing** – Manage the vulnerability scanning lifecycle and activities related to the organisation's IT penetration testing programme.

- **Email, Collaboration and Data Protection** – Maintenance of mail / SharePoint / OneDrive / Teams security and sharing controls. Implementing DLP, sensitivity labelling, encryption posture and removable media controls.

- **Security Awareness and Phishing** – Controlling the phishing simulation programme and advising on security awareness training.

- **ISO 27001, Cyber Essentials and Compliance** – Support and maintain ISO 27001, Cyber Essentials and Cyber Essentials Plus standards and certifications, coordinating auditors and responding to security questionnaires.

- **Security Metrics, Insights and Reporting** – producing reports and creating metrics covering all aspects of security.

- **Incident Response** – Define and maintain process, lead incidents and follow up activities.

- **Third Parties and SaaS** – Managing vendor security assessments.

Requirements:

- 4+ years in a security role
- Excellent technical knowledge and experience in Microsoft Entra and Identity, Microsoft Defender Suite, Microsoft Sentinel and Microsoft Purview
- Strong knowledge of management of the vulnerability scanning lifecycle and penetration testing
- Ability to manage compliance with ISO 27001 controls and coordinate Cyber Essentials recertification
- Strong analytical and structured risk-assessment skills across complex, multi-vendor environments
- Excellent security awareness and proactive approach to continuous improvement
- Experience with incident response strategies
- Strong reporting skills
- Excellent communication and documentation skills

Core Competencies:

- Deadline and pressure management
- Planning and organisational skills
- Analytical and creative problem-solving
- Customer-focused communication
- Teamwork, mentoring and relationship building

Desirable Qualifications:

- Degree in Computer Science, Engineering or equivalent experience
- Microsoft certifications
- Full UK driving licence