**JOB DESCRIPTION**

**Job:** **Information Security Engineer / Analyst**

**Location: Midlands Based**

**Reports to: Head of IT**

**Salary: £50k to £55k**

**Contract term:** FTE

**Travel Required:** National travel required in line with business requirements

**MAIN PURPOSE OF ROLE**

The **Information Security Engineer/Analyst** is responsible for supporting and enhancing our organization's cybersecurity posture through securing enterprise applications, data and infrastructure by identifying, assessing, and mitigating security risks. This is a hands-on role requiring experience in application and data security, vulnerability assessments, security administration, and threat monitoring and response.

You’ll work cross-functionally supporting colleagues from across the business and the wider IT team to ensure security requirements are met and service delivered.

**KEY ACTIVITIES**

**Application Security**

* Perform security reviews of application architecture, source code, and third-party integrations.
* Collaborate with development teams to implement secure coding practices and conduct secure SDLC assessments.
* Use tooling to Identify application vulnerabilities and support remediation efforts.

**Security Administration**

* Manage and configure security tools and systems (e.g., firewalls, SIEM, IDS/IPS, endpoint protection, etc.).
* Monitor security policies, standards, and best practices.
* Review and monitor user access and identity management controls across systems.

**Penetration Testing & Vulnerability Assessments**

* Conduct internal and external penetration tests to evaluate system security.
* Perform regular vulnerability scans using tools like Nessus, Qualys, or OpenVAS.
* Analyse scan results, prioritize risks, and coordinate with stakeholders for remediation.

**Threat Monitoring & Incident Response**

* Monitor networks, systems, and applications for potential threats and unusual activity.
* Respond to security incidents, investigate breaches, and lead root cause analyses.
* Maintain incident response procedures and participate in tabletop exercises.

**Security Posture Enhancement**

* Recommend technical and procedural improvements to strengthen security defences.
* Stay current with emerging security threats, vulnerabilities, and compliance requirements.
* Conduct security awareness training and collaborate across departments to promote a security-first culture.
* Liaise with stakeholders to understand requirements, provide updates, and ensure project alignment with business objectives.
* Implement monitoring and alerting systems to ensure the health and performance of all systems.
* Ensure all systems and processes comply with security best practices and industry standards.
* Troubleshoot and resolve issues related to security breaches.
* Provide monthly Information Security reporting.
* Maintain comprehensive documentation of systems, processes, and procedures.

**KEY SKILLS**

* Demonstrable experience of Information and Cyber Security practices like NIST, Cyber Essentials +, ISO27001.
* Familiarity with regulatory compliance and auditing standards.
* Ability to identify, assess and mitigate security risks.
* Knowledge of penetration testing and vulnerability scanning tools like Nessus and Qualys.
* Proficiency in applying security tooling including firewalls, VPN’s, Network Traffic Analysis.
* Knowledge of network protocols TCP/IP, HTTP, DNS, SSH
* Familiarity with network segmentation
* Experience with endpoint protection software EDR, Anti-Virus, DLP and securing mobile, tablet, laptop, desktop devices.
* Familiar with Zero Trust security models
* Proficient in using SIEM tools
* Experience with log analysis and incident detection.
* Familiarity with securing cloud-native applications, containers and microservices.
* Incident detection, containment and mitigation through post-incident investigations and root cause analysis.
* Data encryption and Data Loss Prevention.
* Identity Access Management deployment Azure AD, MFA, SSO, RBAC
* Security auditing and monitoring.
* Experience in deploying security solutions across business projects.
* Excellent analytical and problem-solving abilities.
* Strong communication skills and stakeholder management.

**EDUCATION & EXPERIENCE**

* Bachelor's degree in Computer Science, Information Security, or related field (or equivalent experience).
* 3–5+ years of experience in cybersecurity or information security engineering/analysis.
* Strong knowledge of MITRE ATT&CK, NIST, ISO 27001, and other frameworks.
* Experience with security tools.
* Familiarity with scripting languages (Python, Bash, PowerShell) is a plus.
* Relevant certifications (e.g., CEH, OSCP, CISSP, Security+, GSEC) preferred.

**MEASURES OF SUCCESS**

* Time, cost, quality measures of deliverables to support successful outcomes.
* Business stakeholder feedback.
* Prevention of successful cyber-attacks and breaches.
* Achieving and maintaining external security standards.
* Completion of regular vulnerability assessments of existing and new solutions.
* Customer satisfaction survey results.
* Positive contribution to resolving team issues and aid other team members as required.
* Accurate and up-to-date reporting.
* Ownership of technical documentation for DevOps

**GENERAL**

* Operate with pace, purpose and professionalism
* Demonstrate the company REACH values are at the centre of all you do
* Undertake training and development deemed necessary for the pursuance of the post
* Comply with all company policies & procedures
* Attention to detail, ability to follow instructions and take ownership of workload.

**ORGANISATIONAL**

* Ensuring compliance with safeguarding procedures, throughout all work within the Company, keeping the manager informed of work in progress and inform the manager immediately of any child protection matter or serious complaint.
* To fulfil Health & Safety responsibilities.
* To work within the provisions of the Data Protection Act, observing strict confidentiality in relation to all aspects of work undertaken.
* Undertake training and development deemed necessary for the pursuance of the post
* Comply with key company policies including;
  + Equal Opportunities Policy and Procedure in all employment practices
  + No smoking policy
  + IT Acceptable usage, Information Security and Data Protection policies
* Travel to Compass Community offices and locations may be required as part of the role
* The nature of the business means that tasks and responsibilities are sometimes unpredictable. Employees are therefore expected to work flexibly when the occasion arises where tasks, which are not specifically covered in the job description, need to be undertaken.