

CANDIDATE SPECIFICATION



JOB TITLE	IT Security Engineer	
REPORTING TO	Group IT Manager	
DEPARTMENT/SUB DEPARTMENT	IT	
LOCATION	Southend-On-Sea	
OVERALL PURPOSE		
To design, implement, and maintain robust security solutions that protect the organisation’s digital assets, infrastructure, and data. The IT Security Engineer plays a critical role in proactively identifying vulnerabilities, automating security processes, and ensuring compliance with relevant industry standards, enabling the business to operate securely and efficiently in a dynamic threat landscape		
PRINCIPLE ACCOUNTABILITIES		
<ul style="list-style-type: none"> Analyse logs from SIEM platforms and network devices to detect threats and vulnerabilities, Collaborate with infrastructure, support and business systems teams to ensure security is integrated across all systems, Act as the escalation point for the IT Support Team on security-related issues, Lead investigations into cybersecurity incidents and compile detailed reports for stakeholders, Conduct malware analysis and digital forensics to support incident response, Maintain accurate and detailed documentation of security configurations, audits, and compliance activities, Identify and remediate system vulnerabilities through proactive assessments, Monitor endpoint activity to detect anomalies and ensure system integrity, Provide expert advice to incident response teams and other departments on cyber threats, Review and update records based on findings from scheduled vulnerability scans, Evaluate and triage security alerts, applying containment and mitigation strategies, Participate in incident response exercises to enhance incident readiness and response, Recommend improvements to security practices in line with evolving regulations and business needs, Enforce IT security policies, procedures, and operational standards, Perform routine checks on systems and equipment, taking preventive action to avoid larger issues, Accurately differentiate between genuine threats and false positives, Provide support for out-of-hours tasks, including handling escalated issues and responding to system downtime, security incidents and / or major incidents, where reasonable, Abide by specific internally established control systems and authorities, to lead by personal example and encourage all employees to conduct their activities in accordance with all applicable laws and the Company’s Standards, Policies and Procedures, To travel to such places (both in and outside the UK) and in such manner as may be reasonably required, To carry out any other tasks where reasonable and relevant, when required. <p>This is not an exhaustive list.</p>		
QUALIFICATIONS	ESSENTIAL	DESIRABLE
Bachelor's degree in Computer Science, Information Technology, Cyber Security, or a related field.	✓	
Cyber certifications such as CISM, CISA, CEH, or CompTIA Security+		✓
IT certifications such as CompTIA A+, Network+		✓

CANDIDATE SPECIFICATION



EXPERIENCE/ SKILLS	ESSENTIAL	DESIRABLE
Extensive experience in cybersecurity	✓	
Strong knowledge of security protocols, cryptography, and security technologies	✓	
Proven experience with security tools such as firewalls, EDR/XDR software, SIEM and intrusion detection systems.	✓	
Experience within a NOC/SOC environment.	✓	
Understanding of regulatory frameworks and industry standards (e.g., NIS, NIST, ISO 27001, GDPR).		✓
Experience in scripting or programming languages including PowerShell for automating security tasks.		✓
Ability and enthusiastic approach to pick up new technologies and learn them	✓	
Ability to work independently while collaborating in a team environment	✓	
Ability to work under pressure and to deadlines	✓	
PERSONAL SKILLS	ESSENTIAL	DESIRABLE
Team Player	✓	
Strong Work 'Can-do Ethic'	✓	
Exceptional at building relationships	✓	
Excellent Customer Service skills	✓	
Strong attention to detail and time management	✓	
Exceptional Planning and Organisation skills	✓	
High awareness of Productivity and Quality	✓	
Excellent Communication skills	✓	
Flexibility	✓	
Takes Responsibility for actions	✓	
Learn, Apply and Improve	✓	