Red Helix
Always evolving. Always there.

JOB DESCRIPTION

Job title:	**Cyber Security Analyst**
Location:	**Aylesbury, Bucks**
Reporting/Responsible to:	**Operations Manager/COO**
Direct Reports:	**N**

JOB ROLE

Role context and purpose:
The Cyber Security Analyst is responsible for protecting our clients' computer systems and information from security risks in line with the services they have purchased. Responsibility includes proactively identifying problems and developing recommendations and plans to protect information from threats such as unauthorised access, data theft or file damage and data loss due to malware or other suspicious activity in the clients' networks.

The Cyber Security Analyst will develop and maintain subject matter expertise in the services that Red Helix sell, with a deep understanding of the technology underpinning these, and able to undertake work on behalf of our clients using this expertise. They will work closely with the appropriate contacts within both technology partners and clients to establish Red Helix credibility and experience in delivering this. They will be a strong advocate for the products and services Red Helix delivers to ensure we give our clients a great experience of our services.

Key Responsibilities:

- Keep up-to-date with the latest security and technology developments
- Research/evaluate emerging cyber security threats and ways to manage them
- Investigate security alerts and provide incident response aligned with clients' services
- Monitor identity and access management, including monitoring for abuse of permissions by authorised system users
- Liaise with stakeholders in relation to cyber security issues and provide future recommendations
- Plan for disaster recovery and create contingency plans in the event of any security breaches
- Using our selected tools and technology, monitor for attacks, intrusions and unusual, unauthorised, or illegal activity across our clients
- Test and evaluate security products as part of the product lifecycle process
- Use advanced analytic tools to determine emerging threat patterns and vulnerabilities and provide recommendations
- Innovate by contributing new ways to detect, hunt and prevent threats for both the company and clients
- Engage in 'ethical hacking', for example, simulating security breaches
- Identify potential weaknesses, recommendations and implement measures
- Generate reports for both technical and non-technical staff and stakeholders
- Maintain an information security risk register and assist with internal and external audits relating to information security
- Monitor and respond to 'phishing' emails and 'pharming' activity
- Assist with the creation, maintenance, and delivery of cyber security awareness training for colleagues

Additional Responsibilities:

- Travel to client sites may be a necessary part of this role
- Flexibility is required of all job holders to adjust responsibilities as required from time to time by their Line Manager/Divisional Director
- The content and reporting lines detailed in this job description may be reviewed and changed from time to time to reflect organisational requirements
- This list is not exhaustive but provides an indicator of likely tasks and responsibilities

PERSON SPECIFICATION: *Profile of ideal job holder, what is necessary to enable the job to be performed to the required standard*

Education and Qualifications *GCSE, A level, degree, professional quals*	Essential • Degree level or equivalent in IT, Computer Science or similar discipline or certification.
	Desirable • Technical certification in any discipline would be helpful
Experience	Essential • Understanding of networking technology including fibre networks, data centre networks, operator networks, and Software Defined Networks • Cyber security service trends and compliance requirements in enterprise organisations • Minimum 3 years' experience in a support role in a client facing commercial organisation • Core cyber security products including SIEM, Zero Trust and NDR/XDR products • Core network routing and switching products
Competencies and Skills	Essential • Passionate about delivering a great client experience • Excellent standard of written and spoken English • A solid understanding of technology and services • An enthusiastic, driven, committed and flexible approach to work • Natural initiative and pro-activeness to their method of working • Keen to learn and continue to build on knowledge and experience • Be open to new ideas and have a positive outlook • Must be a team player but also able to work on own initiative with minimum supervision • High degree of accuracy and attention to detail • Ability to work well to deadlines and under pressure • Ability to think logically • Good problem-solving skills

Knowledge	Essential • Knowledge of cyber security requirements and services • Knowledge of network performance and optimisation and services
	Desirable • Understanding of cyber security risks and identifying potentially malicious activity through an enquiring mind • Understanding of Service Provider environments • Knowledge of UK information security laws and standards and specifically ICO rules and regulations