Job Description - Cyber Security Engineer

Salary: PO1, Pt 27 – 30 £31,346 - £33,782

Hours of work: 37 hrs per week, 52 weeks a year
Mon to Thurs 8am – 4pm and Fri 8am – 3.30pm

Line of Responsibility: Trust IT Manager

Role Description

Main duties & responsibilities:

- Provide, install, manage and oversight of the internally delivered Security Monitoring system
- Coordinating the appropriate response to the identified alerts
- See opportunities for continuous improvement in security operations
- Demonstrate a detailed understanding of Cyber security
- Demonstrate an understanding of Vulnerability management and cyber security frameworks
- Host quarterly presentations to committees on risks detected and corrected
- Network analysis experience with Network sensors
- Experience of managing modern Anti-Virus solutions (Sophos)
- Knowledge of and use of industry standard threat Intelligence sources
- Training will be provided via a full set of UDEMY courses

Key tasks:

- Monitoring all security logs in Office 365, Azure, Network Devices, Anti Virus etc
- Act on alerts by reconfiguring and setting up extra defences
- Keep up to date on latest DfE and NCSC advice
- Knowledge on standards such as ISO27001 (Information Security Management), PCI DSS, Cyber Essentials, GDPR, NIST and SANS Top 20.
- Experience conducting Cybersecurity investigations into network and application activity
- Complete regular PEN testing and security hole detections
- Maintain and track all Infrastructure Security
- Ensure students cannot access areas of the schools they shouldn't like CCTV systems, Staff Shares, Servers etc.
- Install, configure and maintain Ping Castle
- Implement tools and processes to contain attacks

You will be required to support the IT team as and when necessary.

Personal Specification:

Technical skill requirements –

- computer networking fundamentals
- modern threats and vulnerabilities
- attack methodologies
- Understanding of Windows/Linux/Unix operating systems
- Understanding of operating system and software vulnerabilities and exploitation techniques
- Experience demonstrating core security and infrastructure technologies during investigations such as firewall logs, network security tools, malware detonation devices, proxies, or IDS/IPS
- Provide support for to IT team to ensure the delivery of best practices and standards
- Scripting languages Python, Bash, Powershell, WMI

Qualifications -

- GCSE's (A-C Maths, English and IT) or equivalent
- Relevant experience of three years minimum
- One or more of the following (or equivalent) is desirable but not essential:
  - Microsoft MCP in Server 2016, 2019
  - Microsoft MCP in Windows 10
  - Any other certifications in line with the technical skill requirements
- Further training can be given during employment should it be required

Personal skill requirements –

- Able to share information and communicate effectively
- Excellent communicator
- Able to problem-solve
- Able to work under own initiative
- Good team player
- Willingness and adaptability in tackling the variety of tasks arising in a school environment
- Experience of risk management and assessment

Conditions of Employment

The above responsibilities are subject to the general duties and responsibilities contained in the written statement of conditions of employment (the Contract of Employment).

The postholder is required:

to support and encourage the school's ethos and its objectives, policies and procedures as agreed by the governing body.

to uphold the school's policy in respect of child protection matters.

is subject to all relevant statutory and institutional requirements.

to perform any other reasonable tasks after consultation.

This job description allocates duties and responsibilities but does not direct the particular amount of time to be spent on carrying them out and no part of it may be so constructed.

This job description is not necessarily a comprehensive definition of the post. It will be reviewed at least once a year and it may be subject to modification at any time after consultation with the postholder.

All staff participate in the school's performance management scheme.