

JOB DESCRIPTION

Job Title: Cybersecurity & Connectivity Engineer

Reporting To: IT Manager

Working Hours Full-time, 36 hours per week

PayScale SC12

Job Purpose:

This is a newly created post to comply with cyber security to cover all aspects of digital protection of the college perimeter with the necessary hardware and software configured and administered to provide full protection from the dynamically evolving threat space and threat actors. The role's focus is to monitor and analyse threats using latest monitoring tools and techniques and to act proactively to remove the threats.

- As a security analyst you will monitor our systems to detect potential indicators of compromise. You will lead the first stage categorisation and investigation of security alerts generated by analytical tools and capabilities operating across all systems and networks.
- Take a leading role in the administration, customisation, and support of the college's switches, firewall, and wireless technologies.
- Contribute to the maintenance of a designated number of college virtual servers associated with security designated applications
- Assist in the development of staff and students Intranet connectivity and other cloud-based technologies.
- Work with the IT Manager on projects and developments designed to improve the quality, range, and robustness of the ICT-based systems.

Main Duties:

- To be responsible for monitoring cyber security devices operate optimally ensuring an effective response to alerts. Interpreting reports and dashboards analytics using your knowledge of security risks and the latest cyber intelligence,
- Contact support engineers to escalate potential incidents, collating and presenting all necessary information to the IT Manager, to enable an immediate and accurate investigations. You will use malware analysis tools as appropriate to support your recommendations for actions to be taken and decision-making.
- Produce technical policies and procedures to ensure the settings and configurations of security devices and gateways remain intact from external and internal threat actors, software or human initiated.
- Develop and apply theoretical rules to test and deploy across large data sets and will continually review and refine those rules to ensure high quality outputs are maintained and supplied to operational satellite systems and stakeholders.

- Take full technical responsibility, undertaking the administration of a number of designated servers, switching and control devices.
- Maintain connectivity and efficient operations of all of the switch infrastructure, firewall and wireless.
- Customise the college network infrastructure producing and maintaining an accurate schedule of all switches and ports connected to servers.
- Providing 1st /2nd/3rd line support to users over the entire IT estate
- Monitor wired and wireless traffic, AP, wireless controller, and certification server and re-issuing is maintained securely
- Ensure all coms rooms cabling systems are maintained with colour coded cables for easy fault tracing and port schedules displayed for troubleshooting.
- Build up skills using self-development tools or otherwise scripting skills in order to be able to contribute to in the maintenance of cloud-based technologies.
- Assist in supporting MAC technology and its integration with AD.

General

- Undertake any staff development relevant to the needs of the post and collaborative tasks with other providers.
- Comply with Health and Safety Regulations associated with your employment;
- Demonstrate a commitment to promoting and achieving equality and diversity in all areas of college life.
- To carry out any other duties commensurate with the grade and general responsibilities of the post.
- Contribute to Quality Assurance in the College through participation in Performance Review.

The post holder will be expected to be available to work outside of their normal hours from time to time, to support key activities during the academic year. For example, enrolment, roadshows, open evenings, parents' evenings, etc. Advance notice would be given and appropriate time off in lieu would be negotiated.

Terms & Conditions

Full Time (36 hours per week), Monday to Friday.

Annual Leave –25 days per annum plus 2 extra statutory days and Bank Holidays. An average of 7 annual leave days to be taken to cover the College Christmas closure period.

Salary allowance: SC12

Person Specification – Cybersecurity & Connectivity Engineer

*Application form (A), Task (T) or Interview (I)

Criteria for Selection	Essential/ Desirable	Method of assessment*
Qualifications and Training		
Degree in Computer Science, Cybersecurity, or related field	E	A
MCITP Server or Enterprise Administrator	D	A
CompTIA Security+ or equivalent cybersecurity certification	D	A
Experience		
Hands-on experience configuring and managing network switches (HPE, Cisco, Juniper, etc.)	E	A
Experience with firewall technologies (e.g. Palo Alto, Cisco ASA, FortiGate,)	E	A
Experience with mail filtering, MS Defender suite and other monitoring tools	E	A,T,I
Experience in using a wide range of I.T. systems and applications	D	A
PowerShell scripting skills	E	A,T,I
Familiarity with SIEM tools (e.g. Splunk, Sentinel)	E	A,I
Skills, Knowledge, understanding and abilities		
Strong analytical, reasoning and problem-solving skills	E	A,T
Excellent written and verbal communication skills	E	I
Ability to translate technical requirements into user-friendly solutions.	E	A, T
Ability to write and maintain technical documentation	E	A
Excellent time management and planning skills and the ability to work under pressure to balance conflicting demands.	E	A,I
A positive and solutions focussed approach	E	A,I
A collaborative approach, with experience of effectively working with others and supporting a team to achieve success.	E	A,I
Ability to demonstrate a flexible approach to work and changing priorities	E	A,I
Understanding of risk assessment and mitigation	E	A,T
Proactive and self-motivated	E	A, I
Values and Personal qualities		
Commitment to, and advocate for, the vision, mission and strategic priorities of LSC	E	A,T,I
Commitment to and compliance with LSC's safeguarding and health and safety principles	E	A,I
Commitment to respect and value equality and diversity, and an understanding of how this applies to own area of work	E	A,I
Commitment to own continuing personal and professional development	E	A,I