IT Security Analyst (Security Operations Centre)

Job Ref: REQ240918

As part of the University's ongoing commitment to redeployment, please note that this vacancy may be withdrawn at any stage of the recruitment process if a suitable redeployee is identified.

We are looking for an IT Security Analyst whose primary focus will be SOC operations. This hands-on role will be responsible for supporting key day-to-day operations in our new Security/Networks Operations Centre initiative. This role is varied to support your continuous development and will include security/networks alert investigations, vulnerability scanning and reporting, undertaking support tasks and engaging with third parties.

As a member of IT Services, you can expect:

- support in developing your career, allowing you to progress towards your goals in a friendly environment;
- mentoring and development opportunities including exposure to a wide breadth of technologies;
- to work closely with all of our partners from across the University to support digital transformation and deliver outstanding levels of service that are recognised as the best in the country by our students in the National Student Survey;
- a supportive dynamic working policy with flexible home/hybrid working where possible - This role will typically require working on campus in Loughborough for approximately two days per week.
- a superb 440-acre green site in the heart of Leicestershire with first-rate facilities, plenty of open space, gardens, and sports areas;
- a great salary and benefits package, generous holiday allowance and pension scheme.

Job Description

Job Grade: Technical Services Grade 5

Job Purpose

The role holder will be responsible for supporting the department in identifying, mitigating, responding and reporting on cyber security threats, as part of the IT Security Team. As a member of this team, the role holder will significantly contribute to the IT security of all University staff, students, fellows and contractors, co-ordinating the response to IT security incidents and improving the defence of the University's IT infrastructure and information assets.

Job Duties

- To perform regular monitoring of University security systems to identify virus and malware infections, compromised systems and user accounts and unusual network activity.

- To perform "threat hunting" across the University network, "deep-dive" trend analysis, thematic research and undertaking different aspects of IT security investigations.

- To actively defend the network with technologies such as next generation firewalls, vulnerability scanning, penetration testing, network traffic analysis, event log analysis, anti-malware, and access control technologies.

- To maintain a high level of awareness of the IT security threat landscape, and how it impacts the business.

- To perform vulnerability scanning of systems, identifying security threats and vulnerabilities, and taking ownership of issues until resolution.

- To ensure that security technologies and practices are operating in accordance with Loughborough University's policies and standards to mitigate risk and ensure compliance.

- To generate general trend data based on a range of agreed IT security metrics.

- To alert on internal non-compliance with the University's policies, standards, and procedures.

- To liaise with IT technical teams and business teams in a clear and professional manner to define effective security controls, practices and processes and advise on implementation.

- To participate in projects to introduce and update IT systems and services and to roll out these services to users.

- To develop and continuously improve documentation, procedures, and controls.

- Be familiar with relevant University policies and procedures (EDI, acceptable use, data protection, freedom of information, information governance etc) and advise colleagues and end users accordingly.

IT Services Special Conditions:

This post involves configuration, development, or management of infrastructure for corporate IT systems or carrying out other work that requires privileged access to applications and data. Therefore, applicants must provide details of referees including their current line manager covering the three years prior to their application to a post at the University.

Many staff carry mobile phones which allow them to be notified by various systems at all reasonable hours of the week. When monitoring, diagnosis and configuration of services needs to be done outside normal working hours, it can sometimes be appropriate for the work to be carried out remotely at home when convenient.

Attendance on site outside normal working hours is occasionally necessary, for example during major system changes and maintenance. Such out-of-hours working as is necessary is scheduled in negotiation with the group of staff with relevant skills and takes account of the personal commitments and wishes of colleagues.

For purposes of system management, IT Services staff often have enhanced access to data, files and computer systems and must at all times respect the privacy of information to which they have enhanced access. The only exception to this will be investigations authorised by IT Services Director or their nominee.

Points To Note

The purpose of this job description is to indicate the general level of duties and responsibility of the post. The detailed duties may vary from time to time without changing the general character or level of responsibility entailed.

Special Conditions

All staff have a statutory responsibility to take reasonable care of themselves, others and the environment and to prevent harm by their acts or omissions. All staff are therefore required to adhere to the University's Health, Safety and Environmental Policy & Procedures.

All staff should hold a duty and commitment to observing the University's Equality & Diversity policy and procedures at all times. Duties must be carried out in accordance with relevant Equality & Diversity legislation and University policies/procedures.

Successful completion of probation will be dependent on attendance at the University's mandatory courses which include Respecting Diversity and, where appropriate, Recruitment and Selection.

Organisational Responsibility

Reports to the IT Security Team Manager but may receive strategic direction from colleagues in the IT Security and Networks and Smart Campus teams.

Person Specification

Your application will be reviewed against the essential and desirable criteria listed below. Applicants are strongly advised to explicitly state and evidence how they meet each of the essential (and desirable) criteria in their application. Stages of assessment are as follows:

1 – Application
2 – Test/Assessment Centre/Presentation
3 – Interview

Essential Criteria

Area	Criteria	Stage
Experience	Experience of providing technical IT support in a managed desktop and server environment.	1, 3
	Experience of supporting aspects of IT Security at a first- or second-line level including: Phishing, MFA, Anti-Virus, etc.	1, 2, 3
	Experience of working both individually and effectively as part of a wider team.	3
	Displays a responsible attitude to following procedures, keeping records, and caring for equipment and other assets.	1, 3
Skills and abilities	Has good inter-personal skills. Is well organised and practical, with a logical, analytical approach to problem solving. Pays careful, close attention to detail.	1, 3
	Knowledge of essential networking concepts, such as TCP/IP, subnets, ports, and services as applied to IT security.	1, 2, 3
	Knowledge of IT security issues and vulnerabilities (e.g. Phishing, social engineering, MiTM attacks, DDoS etc).	1, 2, 3
	Analytical skills with the ability to interpret data across large multiple datasets.	2
	Awareness of SIEM technologies.	1, 2, 3
	Awareness of vulnerability scanning technologies.	1, 3
	Has good oral communication skills and takes an analytical approach to problem solving.	1, 3
	Excellent written skills to write technical procedures, reports, system specifications, documentation etc.	1
	Excellent time management.	3
	Ability to schedule your own workload and prioritise your work.	1, 3
Training	A willingness to undertake further training and to learn and adopt new procedures as and when required.	1, 3
Qualifications	Must be educated to “A” level or equivalent.	1
Other	Ability to undertake various other tasks on an occasional basis at the request of more senior staff in the department, and to a level commensurate with training, knowledge, grade, and skills.	1, 3
	To promote and engage with the principals in the University Equity, Diversity & Inclusion Core Plan, and associated initiatives.	3

Desirable Criteria

Area	Criteria	Stage
Experience	Knowledge of Windows, Linux and/or OSX system administration and security hardening.	1, 3
	Experience of working in Higher Education.	1
Skills and abilities	Ability to write scripts or code to perform analysis and/or aid automation.	1, 3
Qualifications	Educated to degree level in a relevant area such as computing or have relevant IT professional qualifications and/or experience.	1
Other	Familiarity with relevant University IT-related procedures and policies (acceptable use, data protection, information governance etc.) and advises colleagues and end-user accordingly.	1, 3

Conditions of Service

The position is FULL TIME and OPEN-ENDED/. Salary will be on Technical Service 5, £28,879 to £33,882 per annum, at a starting salary to be confirmed on offer of appointment.
The appointment will be subject to the University's Terms and Conditions of Employment for STAFF GRADES 1-5/, details of which can be found here.

The University is committed to enabling staff to maintain a healthy work-home balance and has a number of family-friendly policies which can be found here.

The University offers a wide range of employee benefits which can be found here.

We also offer an on-campus nursery with subsidised places, subsidised places at local holiday clubs and a childcare voucher scheme (further details are available at: http://www.lboro.ac.uk/services/hr/a-z/childcare-information---page.html

In addition, the University is supportive, wherever possible, of flexible working arrangements.
We also strive to create a culture that supports equality and celebrates diversity throughout the campus. The University holds a Bronze Athena SWAN award which recognises the importance of support for women at all stages of their academic career. For further information on Athena SWAN see http://www.lboro.ac.uk/services/hr/athena-swan/

Applications

The closing date for receipt of applications is **as per the advert.**.