# Job Description

## Job title: Senior Cyber Security Analyst

**Faculty/Directorate: Digital and Technology** **Job Family: Cyber Security Management**

**Grade: G** **Role profile: TSG1**

**Full time (37 hours per week)** **Permanent** **Date: May 2026**

| | Duties of the role |
|---|---|
| **Overall purpose of the role** | Act as a senior subject matter expert within the information security function in Digital & Technology, responsible for leading the investigation, response, and mitigation of complex security threats across the University.<br><br>The post holder will provide authoritative advice on cyber risk, influence secure design and operational practices, and ensure that security controls are effectively implemented to protect university information systems, services, and data.<br><br>The role will also play a key part in shaping and maturing the University's cyber security capability in line with sector best practice. |

| | |
|---|---|
| **Main duties and responsibilities** | • To be responsible for the design, optimisation, configuration and operation of multiple, technical security solutions. Collaboratively working across internal teams to ensure all security considerations, systems monitoring, and support is in place.<br>• Lead the technical investigation and response to complex cyber incidents, applying advanced analytical techniques and expert judgment, whilst coordinating multi-disciplinary responses from across D&T technical team and external providers.<br>• Contribute to and shape the ongoing development of the University's cyber security strategy, providing expert input to ensure alignment with emerging threats, risk appetite, and sector best practice<br>• To take responsibility for the development of appropriate security solutions that support existing business requirements and those planned to support digital transformation, while maintaining an acceptable level of risk. Ensure that security principles are embedded into all system designs, with risks tracked and reported appropriately.<br>• To define and recommend security improvements and innovative solutions to enhance and expand DMU's cyber security response capabilities and maturity, whilst ensuring clear risk justifications are provided. Support the security team to clearly demonstrate the tangible value these solutions will bring to the university/<br>• To triage, prioritise and lead remediation of security incidents, automated security alerts and reports, highlighting actions required as appropriate and driving forward these to completion. Ensuring these statistics are captured and reported on the appropriate boards.<br>• Proactively identify, assess, and prioritise emerging threats, industry trends, and vendor advisories, translating these into actionable risk insights for the University. Independently initiate and drive mitigation strategies across teams, ensuring risks are effectively reduced and contributing to continuous improvement of the University's security posture<br>• Lead and continuously improve a programme of cyber security awareness and behaviour change, including simulated phishing campaigns, targeted training, and engagement activities. Use metrics and user insights to drive measurable improvements in security behaviours and reduce the University's exposure to cyber risk.<br>• Exercise independent technical and risk-based judgement in complex or ambiguous scenarios, making informed recommendations on risk mitigation, acceptance, or escalation.<br>• Manage the configuration and implementation of proactive system changes, patches and enhancements to ensure all security tools are configured optimally and recoverable in the event of failure. Ensure that all changes are reviewed via CAB and |

| | |
|---|---|
| | **Duties of the role** |

| | |
|---|---|
| | that appropriate stakeholder communications are maintained throughout the change process.<br>• Possess a combination of troubleshooting, technical, and communication skills, as well as the ability to handle a mix of disparate tasks which may include project and self-development work.<br>• Ensure the completion of tasks as allocated by line management and referred to by the D&T Service Desk in accordance with agreed priorities and service levels. Maintain up-to-date records on progress.<br>• Contribute to the development of a culture based on Continual Service Improvement<br>• Act as the primary security liaison for key services or programmes, working with stakeholders across the University to enable effective delivery of services, raising the profile of D&T and ensuring clear, effective communication with internal and external stakeholders.<br>• Ensure compliance with the University's standards for information systems, security and technology in line with the relevant legislation and audit requirements.<br>Supervisory duties:<br>• To mentor and develop new starters and junior team members as required<br>• To monitor service levels in line with agreed key performance indicators taking action to address identified issues, including acting as an escalation point to resolve complex problems<br>• To perform any other duties commensurate with the job grade as reasonably required from time to time.<br>• Act in accordance with DMU Values:<br>o Collaborative – Work together to achieve joint outcomes, understand how your work contributes to DMU, and be aware of your personal impact on others.<br>o Compassionate – Be open, honest, and caring, work on a basis of trust, and hold yourself accountable for your actions.<br>o Creative - Strive for better, challenge bureaucracy, explore digital solutions, and innovate creatively. o Community minded - Embrace alternative views, treat others with respect, and tackle inequalities.<br>• Treat all DMU staff, students, contractors and visitors with dignity and respect. Provide a service that complies with the Equality Act 2010, eliminating unlawful discrimination, advancing equality of opportunity and fostering good relations with particular attention to the protected characteristics of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief (or none), sex and sexual orientation.<br>• All members of staff are responsible for their contribution to improved environmental performance and in reducing greenhouse gas emissions at DMU. It is therefore required that all members of staff are aware of how the Environmental Policy relates to their own role at the University. Staff conduct must reflect the values inherent in the Environmental Policy and where required staff must cooperate with environmental compliance and conformance requirements to help minimise our emissions to air, water and land. |

| | Duties of the role |
|---|---|
| | • The postholder should have a positive attitude towards health and safety, and be aware of and comply with all health and safety policies for the university, as applicable. There will be a requirement to complete all mandatory health and safety training as deemed to be relevant for the position held. The postholder is expected to help maintain a safe working environment for staff, students and visitors by working closely with the local safety coordinator as required. Any accidents or dangerous incidents must be reported promptly through the university's reporting system. |

DE MONTFORT UNIVERSITY LEICESTER

# Person Specification

# Job Description

## Job title: Senior Cyber Security Analyst

**Faculty/Directorate: Digital and Technology** **Job Family: Cyber Security Management**

**Grade: G** **Role profile: TSG1**

**Full time (37 hours per week)** **Permanent** **Date:** May 2026

| Area of responsibility | Requirements | Essential or desirable | | *Method of assessment | | | |
|---|---|---|---|---|---|---|---|
| | | | | A | I | T | D |
| **Qualifications & Training** | Degree in Cyber Security, Computing or equivalent professional experience. | Essential | | X | | | X |
| | ITIL Foundation Certificate | | Desirable | X | | | X |
| | Industry recognised cyber security qualification (e.g. CompTIA Security+, SSCP or equivalent) or substantial professional experience in cyber security. Possession of or demonstrable progression towards more advanced certifications (e.g. CISSP, CISM, GIAC), or equivalent experience .. | Essential | | X | | | X |
| **Previous Work Experience** | Experience of leading investigation and response to complex cyber security incidents | Essential | | X | X | | |
| | Experience of owning and optimising security tooling or controls (e.g. SIEM, EDR, vulnerability management) | Essential | | X | X | | |
| | Experience of working in higher education or across complex organisational boundaries to delivery security outcomes | | Desirable | X | X | | |
| | Exposure to working across multiple IT support teams, facilitating collaboration amongst teams to deliver services. | Essential | | X | X | | |
| | Experience of assessing cyber risk and recommending appropriate mitigation strategies | Essential | | X | X | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Experience of contributing to or supporting security strategy, audit, or compliance activities | Essential | | X | X | | |
| | Experience of delivering IT services to industry best practise | Essential | | X | X | | |
| **Specific Knowledge/Skills /Abilities/ Motivation/ Attitude Required** | Strong knowledge of security technologies including vulnerability management tools, automated penetration testing tools, risk-based access techniques and malware protection methods. | Essential | | X | X | | |
| | Advanced understanding of threat detection, incident response, and security monitoring techniques | Essential | | X | | | |
| | Experience designing or improving security controls based on threat intelligence and incident trends | Essential | | X | X | X | |

| **Area of responsibility** | **Requirements** | **Essential or desirable** | | ***Method of assessment** | | | |
|---|---|---|---|---|---|---|---|
| | | | | **A** | **I** | **T** | **D** |
| | Strong understanding of modern security architectures (cloud, identity, endpoint) | Essential | | X | X | | |
| | Excellent knowledge of IT security frameworks and industry standard certifications (Cyber Essentials, ISO 27001 etc.) | Essential | | X | X | | |
| | An understanding of legislative requirements in relation to information and data management. GDPR | Essential | | X | X | | |
| | Ability to manage supplier relationships and develop partnerships with suppliers. | | Desirable | X | X | | |
| | Ability to follow and author technical procedures | Essential | | X | X | | |
| | Team working and strong organisational skills – whilst having the ability to influence stakeholders and drive adoption of security practices | Essential | | X | X | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | Excellent customer service skills, ensuring a consistently high standard of service | Essential | | X | X | | |
| | Excellent communication skills with the ability to translate complex technical risks into clear, business-focused messages | Essential | | X | X | | |
| | Strong analytical and problem-solving skills | Essential | | X | X | | |
| | Demonstrable ability to proactively improve and enhance the quality of security services and controls | Essential | | X | X | | |
| | Ability to work on own initiative | Essential | | X | X | | |
| | Resilient and able to support and embrace change | Essential | | X | X | | |
| | Able to work flexibly according to the needs of the University, including evenings and weekends | | Desirable | X | X | | |
| **Equality and diversity** | Able to provide a service to a diverse range of people to promote good relations and equality | Essential | | X | X | | |
| **Our Values and Behaviours at DMU** | | | | | | | |
| **We are Collaborative** – | We support each other to achieve joint outcomes | Essential | | | X | | |
| **Area of responsibility** | **Requirements** | **Essential or desirable** | | ***Method of assessment** | | | |
| | | | | **A** | **I** | **T** | **D** |
| we work together to get things done | We understand how our work contributes to DMU<br>We are aware of our personal impact on others | | | | | | |
| **We are honest and Compassionate** | We are open, honest and caring We work on a trust basis<br>We hold ourselves accountable for our actions | Essential | | | X | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **We are innovative and Creative** | We constantly strive for better<br>We challenge bureaucracy and explore digital solutions<br>We are innovative and creative | Essential | | | X | | |
| **We are a community** – we value and champion difference | We embrace alternative views<br>We treat others with respect<br>We tackle inequalities | Essential | | | X | | |

***A = Application Form; I = Interview; T = Test; D = Documentary Evidence**