University of Nottingham
UK | CHINA | MALAYSIA

Role profile

Job title	Cyber Security Analyst	Job family and level	Administrative, Professional and Managerial Level 4
School/ Department	Digital & Technology Services (DTS)	Location	Jubilee Campus

Purpose of Role

The Cyber Security Analyst is responsible for monitoring all computer systems connected to the university network to identify known vulnerabilities, potential weaknesses, security breaches, unusual activity and unauthorised or illegal activity.

You will assume responsibility for supporting the university's endpoint detection and response (EDR) platforms, security incident and event management (SIEM) and cloud protection platforms to identifying and remediate user account or system compromises. You will use vulnerability management tools detected security weaknesses and assisting with the installation and testing of software and security updates. You will also assist in the production of information security best practice and work closely with the service management team to ensure consistent reporting and feedback of security related incidents and problems.

	Main Responsibilities (Primary accountabilities and responsibilities expected to fulfil the role)	% time per year
1	**Monitor all computer systems connected to the university network:** • Identify compromised systems or accounts, unauthorised and irregular activity • Analyse security breaches and other cybersecurity incidents to identify the root cause and recommend any action required to prevent reoccurrence • Support the Vulnerability Management process through continual vulnerability analysis, threat hunting and anomaly detection • Implement and maintain vulnerability management systems across assets on-premises and in the cloud • Perform regular security audits and assessments to ensure university systems comply with the information security policy • Deploy and maintain endpoint detection and prevention tools across the university estate • Ensure accurate documentation, recording and reporting to ensure quality information provision (e.g. Service Management tools, security reports, risk register, monthly reports) • Maintain security solutions to enable consistent function	60%

	• Support of a range of operating systems and applications across the university	
2	**Analyse and champion security solutions across the University:** • Verifying the security of third-party vendors and collaborating with them to meet University security requirements • Implement security improvements by assessing current trends, threats, legal and regulatory requirements • Provide detailed information and documentation to first line support teams to ensure effective and efficient troubleshooting activity • Involvement in security incident activities with other groups within Digital & Technology Services and the wider University, working with JISC Computer Security Incident Response Team, third party supplier, and security services as required • Collaborate with other Digital & Technology Services staff, departmental system administrators and end users to provide advice on secure work practices and security of networks servers, workstations and data • Conducts risk and vulnerability assessments of business applications and computer systems against current threats and recommend appropriate action to management	20%
3	**Platform Ownership** • Perform the role of Platform owner for one or more platforms/technology	10%
4	**Other** • Promote secure computing practices through seminars and published documents • Research security enhancements and make recommendations • Stay up-to-date on information technology trends, security standards and emerging threats • Assist other team/group members provide technical support for other platforms when required • Participation in the out of hours on-call service, to protect the university's computing services in the event of security incidents	10%

Person Specification

	Essential	Desirable
Skills	• Ability to enhance Windows and Linux system security through continual vulnerability assessment and providing advice on required system hardening or secure configuration • Ability to detect, assess, and appropriately, response to cybersecurity threats • Able to use utilise security tools (such as Microsoft Defender 365) to detect, investigate, and respond to potential account compromises and suspicious activity • Good understanding of Endpoint Detection and Response (EDR), Anti-Virus and Anti-Malware solutions and the mechanisms required to prevent and respond to malware or ransomware incident • Excellent analytical/problem solving skills • Good all-round knowledge of infrastructure and security technologies including Zero Trust Architecture principles. • Ability to work in a team, to deadlines and under pressure and to work effectively with minimal support, for example, outside working hours • Ability to communicate effectively within a large organisation and to build a network of contacts • Ability to maintain an up-to-date awareness of current IT legislation and best practice in relation to Information Security • Ability to prioritise and schedule workloads in the face of conflicting demands • Ability to rapidly assimilate and deploy detailed technical knowledge in specialist areas • Willingness to travel from site to site within Nottingham and the UK. • Excellent customer/supplier facing skills; Confident presenter, with influencing and negotiation skills • Willingness to take responsibility for Platform and Services in a global context	• Knowledge of Apple based solutions • Digital forensics, including log file analysis in support of incidents and capturing disk images to support investigations • Familiarity with the Cyber Kill Chain and/or MITRE ATT&CK for incident and control classification
Knowledge and experience	• Experience administering Windows/Linux systems to achieve secure configuration, with	• Knowledge of the HE environment

	appropriate security hardening and patch management • Demonstrated experience supporting and delivering security focused projects • Strong experience administering a range of desktop and server operating systems • Awareness of current IT legislation, regulatory compliance framework (e.g GDPR, NCSC CAF) and best practice in relation to Information Security and ability to apply in practice • Involvement working with and managing 3rd party suppliers • Experience administering Endpoint Detection and Response (EDR), Anti-virus and anti-malware software solutions and/or responding to malware outbreaks • Experienced in conducting vulnerability assessments, analysing identified risks, and effectively communicating mitigation strategies to technical and non-technical stakeholders • Familiar with user account and directory services administration, supporting secure access and identity management • Familiar with networking services and able to specify connectivity requirements and diagnose connectivity problems • Experience of working within a structured IT Service Delivery Framework (Change Management) • Experience in collecting and analysing operational data to assess and enhance the performance of cybersecurity measures	• Experience of administering and configuring SIEM solutions • Practical experience of designing and implementing solutions for a large, distributed organisation • Experience of providing support in Incident Response and Priority security incidents • Experience in forensic analysis to support investigations • Experience in reviewing and assessing the effectiveness of firewalls • Knowledge of penetration testing tools and toolkits • Experience of delivering IT services complex and large-scale environment • Experience of using Service Desk tools and applications within an ITIL environment
Qualifications, certification and training (relevant to role)	▪ Degree or equivalent in IT-related subject or equivalent relevant experience	▪ Industry relevant and recognised IT security certification

Expectations and Behaviours

The University has developed a clear set of core expectations and behaviours that our people should be demonstrating in their work, and as ambassadors of the University's strategy, vision and values. The following are essential to the role:

Valuing people	Is always equitable and fair and works with integrity. Proactively looks for ways to develop the team and is comfortable providing clarity by explaining the rationale behind decisions.
Taking ownership	Is highly self-aware, looking for ways to improve, both taking on board and offering constructive feedback. Inspires others to take accountability for their own areas.
Forward thinking	Driven to question the status quo and explore new ideas, supporting the team to "lead the way" in terms of know-how and learning.
Professional pride	Sets the bar high with quality systems and control measures in place. Demands high standards of others identifying and addressing any gaps to enhance the overall performance.
Always inclusive	Ensures accessibility to the wider community, actively encouraging inclusion and seeking to involve others. Ensures others always consider the wider context when sharing information making full use of networks and connections.

Key Relationships with others