University of Nottingham
UK | CHINA | MALAYSIA

Role profile

Job title	Senior Cyber Security Analyst	Job family and level	Administrative, Professional and Managerial Level 5
School/ Department	Digital & Technology Services	Location	Kings Meadow Campus

Purpose of Role

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

You will take the lead on supporting the university's centrally managed anti-virus solution, assisting with the installation and testing of software and security updates, endpoint performance monitoring, tracking, analysis, optimisation, and usage reporting. 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. You will be experienced at tackling complex security issues and will serve as a point of escalation and coach/ mentor for less experienced staff members. You will have experience in identification of appropriate information security controls, their implementation and operation.

	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, 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 • Support of a range of operating systems and applications across the university	50%

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 • Implements 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 such as DTS Support teams, Enterprise Operations, the police and JANET Computer Security Incident Response Team • Support automatic distribution systems for installing, securing and updating of a range of operating systems and application software • Provide expertise to other DTS staff, departmental system administrators and end users to advise on how to work securely and best secure networks servers, workstations and data • Assesses the effectiveness of firewalls, Gateways, IDS (Intruder Detection Systems) and IPS (Intruder Prevention Systems) to improve network/system resilience • Conducts risk and vulnerability assessments of business applications and computer systems against current threats and recommends appropriate action to management.	20%
3	**Platform Ownership** • Assume the role of Platform owner for one or more platforms	15%
4	**Other** • Promote secure computing practices through seminars and published documents • Research security enhancements and suggest, lead and implement recommendations • Maintain current knowledge of up-to-date information technology trends, security standards and emerging threats • Mentor and support other team/group members and 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 • Provide support and mentoring to other less experienced team members	15%

Person Specification

	Essential	Desirable
Skills	• Excellent knowledge of a range of desktop and Server Operating Systems, in particular Windows and Linux / Unix and aspects of security hardening, administration, patch management, installation and support • Strong, proven understanding of Anti-Virus and Anti-Spyware solutions and the mechanisms required to prevent and respond to virus outbreaks • Proven expertise with networking services and able to specify connectivity requirements and diagnose connectivity problems • Excellent analytical/problem solving skills • Good all round knowledge of infrastructure and security technologies • Ability to work in a team, to deadlines and under pressure and also 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 • Acute awareness of current IT legislation and best practice in relation to Information Security and ability to apply in practice • Proven ability to prioritise and schedule workloads in the face of conflicting demands • The ability to rapidly assimilate and deploy detailed technical knowledge in specialist areas • Excellent customer/supplier facing skills; Confident presenter, with influencing and negotiation skills ▪ Able to assume responsibility for Platform and Services in a global context	• Knowledge of Apple based desktop solutions • Understanding of enterprise email systems (eg Exim, Office 365) • 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	• Track record of leading large scale security focused projects • Proven experience administering a range of desktop and server operating systems • Involvement working with and managing external suppliers	• Knowledge of the HE environment • Experience of administering and configuring SIEM solutions

	• Experience of supporting automated solutions for enterprise-wide Anti-virus and security patch distribution • Experience in undertaking vulnerability assessments and communicating identified risks and required mitigations. • Familiarity with username and directory administration • Familiar with networking services and able to specify connectivity requirements and diagnose connectivity problems • Strong experience in the support, maintenance and configuration of the relevant infrastructure technologies • Significant experience of working within a structured IT Service Delivery Framework (Change Management) • Significant experience of delivering IT services in a complex and large-scale environment ▪ Experience of using Service Desk tools and applications within an ITIL environment ▪ Experience in gathering operational evidence on the performance of cyber security	• 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 • Review and assess the effectiveness of firewalls • Experience with any of the following technologies: Active Directory, Splunk, Carbon Black, Cisco Umbrella. Azure Security Center; Qualys vulnerability management; Office 365 Administration and/or Security • Knowledge of penetration testing tools and toolkits
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

Athena SWAN Silver Award

The University of Nottingham is focused on embedding equality, diversity and inclusion in all that we do. As part of this, we welcome a diverse population to join our work force and therefore encourage applicants from all communities, particularly those with protected characteristics under the Equality Act 2010.

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.

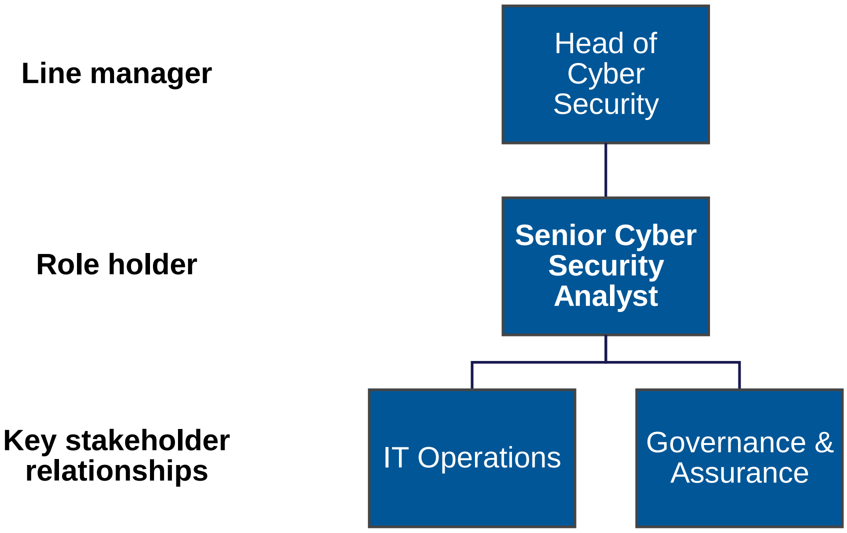
Taking ownership Is highly self-aware, looking for ways to improve, both taking on board and offering constructive feedback. Inspires others to take accountability for their own areas.

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


Line manager
Head of Cyber Security
Role holder
Senior Cyber Security Analyst
Key stakeholder relationships
IT Operations
Governance & Assurance