****

Job Description

Senior Cyber Security Analyst (Network Project)

Date last updated/evaluated: June 2025

Author: Vicky Stephenson

School / Department: iSolutions

Faculty / Directorate: Professional Services

Job Family: Management, Specialist and Administrative (MSA)

Grade: Level 5

ERE Pathway (if applicable): Not applicable

Post reporting to: Cyber Security Operations Manager

Post line report(s): Not applicable

Post base location: Hybrid: Campus / Home **:** Office based 1 day a week

Job purpose

Provide specialist cyber security expertise as a key member of the network project team, ensuring the secure design and delivery of the University’s digital network services and defending them against cyber threats. The Analyst will be responsible for implementing and managing robust network security controls, with a focus on Cisco technologies, to protect against evolving threats. In addition to supporting the project, the role will contribute to day-to-day operational security activities, including threat monitoring, policy compliance, and incident response. The post holder will also provide expert advice and guidance on cyber security matters and help to build capability and raise awareness across technical teams within the University.

## Key accountabilities and indicative time allocation:

1. **50%**

Technical and Operational

* Support the day-to-day technical and operational management of cyber and information security within the University under the guidance of the Cyber Security Operations Manager. This includes working within a hybrid Security Operations Centre (SOC) model, assisting with the investigation and resolution of cyber security incidents, and liaising with the University's third-party SOC provider to support effective threat detection, incident response, and continuous monitoring across the University.
* Conduct proactive threat hunting activities to detect advanced threats and anomalous behaviour within the University's network, and provide solutions to inform incident response, vulnerability management, and strategic security decisions.
* Collaborate with third-party providers to scope, coordinate, and review network security assessments, and ensure that findings and recommendations are effectively prioritised, communicated, documented and implemented to improve the University’s security posture.
* Support the network vulnerability management process by identifying, assessing, and prioritising security vulnerabilities, and working with relevant teams and third parties to ensure timely remediation through patching, configuration changes, or other appropriate fixes.
* Design, implement, and support technical security controls to defend University network systems against security threats. These controls include Security Incident and Event Monitoring (SIEM), Cisco Secure Network Analytics (SNA), Software Defined Access (SDA), Cisco Application Centric Infrastructure (ACI), Cisco Identity Services Engine (ISE), Cisco Firepower, DNAC and other such technologies.
* Design, implement and support technical solutions to address specific security challenges across the University, ensuring strong understanding of stakeholder needs and context to influence and ensure the most appropriate solution is delivered and documented.
* Assess security infrastructure, network and systems design to evaluate and identify security risks, threats and vulnerabilities of networks, systems, applications, and new technology initiatives and ensure overall system / network security. Conduct assessments of existing and new software deployments, whilst continuously looking at ways to mature our processes and improve the services.
* Present Security solutions for approval via internal processes such as the Technical Architecture Board (TAG) and Change Advisory Board (CAB).
1. **20%**

Programme Delivery

* Provide technical project leadership for the networking project to implement new functionality, ensuring the design and delivery are secure, resilient, and aligned with best practice cyber security standards.
* Provide technical project leadership for operational cyber security improvement projects and programmes. Ensure that products delivered by the cyber security project are effectively implemented into day to day security management.
* Ensure that the delivery of the digital transformation initiatives is aligned with University Cyber Security strategy, providing technical security operations input as part of the overall governance process.
1. **15%**

Expert Advice

* Subject Matter Expert for Network Security and Cyber Security
* Provide expert advice across the University regarding identification and management of security risks and issues.
* Act as an experienced advisor to staff and external stakeholders on security compliance, in addition to managing and publishing knowledge articles to help educate the wider business.
* Develop the knowledge and capability across the University (including other iSolutions teams) to identify and consider cyber security and information management issues within projects and research, education, and operational business as usual activities.
1. **10%**

Continuous Improvement and Contribution to Strategy

* Conduct assessments of existing and new network equipment and software deployments, whilst continuously looking at ways to mature our processes and improve the services.
* Contribute expert knowledge in the development of Information and Cyber security strategies and business cases.
* Use initiative to propose new and innovative solutions to cyber and information management challenges and make recommendations to the Cyber Security Operations Manager for continual improvement of systems and services.
1. **5%**

Any other duties as allocated by the line manager following consultation with the post holder.

Internal and external relationships:

Working with staff and students across the University to provide advice, solutions and recommendations on cyber and information security matters.

Working with technical staff within iSolutions as well as IT system suppliers, contractors, and consultants.

Work with senior members of iSolutions, Legal Services and the wider University to support the investigation and resolution of security incidents, as well as to provide security advice and guidance.

Operate within a hybrid Security Operations Centre (SOC) model, collaborating with both internal teams and external providers to ensure comprehensive threat monitoring, incident response, and continuous improvement of security operations.

Special requirements:

Occasional travel to other University sites and supplier offices may be required.

Out of hours work may be required to resolve major incidents.

Due to the nature of Information and Cyber Security, the post holder will be expected to always maintain appropriate levels of confidentiality.

# Person Specification – Skills and Competencies

All essential and desirable criteria outlined in this Person Specification will be assessed through a combination of recruitment application and CV, and where applicable numerical or written assessment.

**Knowledge, Experience and Qualifications**

Essential

* Skill level equivalent to achievement of a professional qualification or postgraduate degree in Cyber Security (or other relevant subject), or substantial relevant information/cyber security experience.
* Experience working with Microsoft Azure/M365 (or similar) security technologies, such as:
	+ Microsoft Defender XDR
	+ Microsoft Sentinel
	+ Cisco SNA, SDA, ACI, ISE, Firepower, DNAC
* Experience with software vulnerability detection, assessment, and management.
* Knowledge of security frameworks such as:
	+ NCSC Cyber Essentials
	+ NHS Data Security and Protection Toolkit
	+ IEC/ISO 27000 series
	+ NIST SP-800 series
	+ PCI-DSS
	+ OWASP Top 10
* Knowledge of data protection legislation.
	+ GDPR
	+ Data Protection Act 2018

Desirable

* Relevant professional certification, e.g., CISSP, SSCP, CCSP, Security+, CCNA, CCNP Security
* Experience working with cloud ‘SaaS’ software products and providers.

**Teamwork and Communication**

Essential

* Able to harness the commitment and contribution of other iSolutions team members and others across the University in building security capability.
* Able to provide expert guidance and advice to colleagues across the University to resolve complex problems.
* Able to work effectively as part of a matrix/project team whilst also being able to prioritise and manage own workload.
* Able to collaborate effectively between the Cyber Security Team and the Networking Team to support the implementation of new systems.

**Planning, Organisation and Resource Management**

Essential

* Able to prepare and implement a programme of activity over time to pro-actively monitor security in the University.
* Able to plan and prioritise a range of one’s own standard and nonstandard work activities and effectively meet deadlines.
* Able to plan and manage new projects or significant new activities, ensuring plans complement broader organisational strategy.

**Problem Solving and Initiative**

Essential

* Able to identify broad trends to assess deep-rooted and complex issues.
* Able to take ownership for resolving security issues and deciding appropriate solutions.
* Able to identify and solve complex problems by applying judgement and initiative to tackle some situations in new ways and by developing improved work methods.
* Able to conduct research into new security technologies and present recommendations.
* Pro-active and able to work on own initiative

**Communicating and Influencing**

* Able to work with Senior level stakeholders, advising, influencing, and gaining support for security initiatives.
* Able to deal with sensitive information in a highly confidential manner.
* Able to communicate specialist technical information clearly and confidently to staff and Senior Stakeholders.

# Job Hazard Assessment

A full health clearance is required for this role where any hazards marked “**^**”, using the agreed Occupational Health referral template [available from here](https://sotonac.sharepoint.com/teams/HealthWellbeing/SitePages/Occupational-Health.aspx). Where a full health clearance is required, this will apply to all role holders, including existing members of staff.

## Physical Environment

Working outside **^** Not applicable

Exposure to noise levels >80dbA **^** Not applicable

Working with dust or fumes **^** Not applicable

Working with skin irritants **^** Not applicable

Working with chemicals (industrial or cleaning) **^** Not applicable

Working in a confined space **^** Not applicable

Working at height **^** Not applicable

Working with sewage **^** Not applicable

Contact with cytotoxins **^** Not applicable

Exposure Prone Procedure (EPP) work **^** Not applicable

Contact with clinical specimens or pathology work **^**  Not applicable

Direct patient care or patient contact Not applicable

Exposure to temperature extremes Not applicable

Frequent hand washing Not applicable

Ionising radiation Not applicable

## Psychological and Social Environment

Working shifts **^** Not applicable

Working nights **^** Not applicable

Lone working Constantly >60% Time

Working with children Not applicable

Exposure to persons with challenging behaviourNot applicable

Working with larger groups Not applicable

## Equipment, Tools and Machines

Working with vibrating machinery or tools **^** Not applicable

Driving duties e.g. LGV, PCVs, forklift trucks **^** Not applicable

Food handling Not applicable

Contact with latexNot applicable

## Physical Abilities

Prolonged physical movements or actions e.g. walking **^** Not applicable

Prolonged Standing or Sitting **^** Constantly >60% Time

Moving or handling heavy loads **^** Not applicable

Repetitive pulling or pushing **^** Not applicable

Repetitive climbing (steps, stools, ladders, stairs) **^** Not applicable

Repetitive crouching, kneeling or stooping Not applicable

Repetitive lifting Not applicable

Fine motor grips (e.g. pipetting) Not applicable

Repetitive reaching below shoulder height Not applicable

Repetitive reaching at shoulder height Not applicable

Repetitive reaching above shoulder height Not applicable

# Behaviours

Our [Inclusion and Respectful Behaviour Policy](https://www.southampton.ac.uk/about/governance/regulations-policies/policies/inclusion-respectful-behaviour) describes the expectations of everyone who is a part of our community.

Our **Southampton Behaviours** (below) outline the responsibilities we each have in working collaboratively to achieve our University strategy.

**Personal Leadership**

 - I take personal responsibility for my own actions and an active approach towards my development.

 - I reflect on my own behaviour, actively seek feedback and adapt my behaviour accordingly.

 - I demonstrate pride, passion and enthusiasm for our University community.

 - I demonstrate respect and build trust with an open and honest approach.

**Working Together**

 - I work collaboratively and build productive relationships across our University and beyond.

 - I actively listen to others and communicate clearly and appropriately with everyone.

 - I take an inclusive approach, value the differences that people bring and encourage others to contribute and flourish.

 - I proactively work through challenge and conflict, considering others’ views to achieve positive and productive outcomes.

**Developing Others**

 - I help to create an environment that engages and motivates others.

 - I take time to support and enable people to be the best they can be.

 - I recognise and value others’ achievements, give praise and celebrate their success.

 - I deliver balanced feedback to enable others to improve their contribution.

**Delivering Quality**

 - I identify opportunities and take action to make improvements.

 - I plan and prioritise efficiently and effectively, taking account of people, processes and resources.

 - I am accountable for tackling issues, making difficult decisions and seeing them through to their conclusion.

 - I encourage creativity and innovation in others, to deliver workable solutions.

**Driving Sustainability**

 - I consider the impact on people before taking decisions or actions that may affect them.

 - I embrace, enable and embed change effectively.

 - I regularly take account of external and internal factors, assessing the need for change, and gaining support to move forward.

 - I take time to understand our University strategy and communicate this to others.