**Position/Job Title: Senior Cyber Threat Intelligence Analyst**

**Ref: POSN108653**

**Location including building: Studland House, Lansdowne Campus and University Wide**

**Faculty/Professional Service: IT Services**

**Group/Section: Information & Cyber Security**

**Normal hours per week: 1 FTE**

**(Some flexibility will be required in order to ensure that key time scales and deadlines are met).**

**Grade: 6**

**Accountable to: Cyber Security Specialist**

**Special conditions:**

**We are committed to providing a safe environment for all students and staff. As this role comes has contact with apprentices, the postholder must be familiar with our Safeguarding Policy and at all times comply with its requirements to safeguard and protect the welfare of young people and vulnerable adults. This includes attendance on relevant mandatory training.**

**Job Purpose**

The Senior Cyber Threat Intelligence Analyst is responsible for cyber security resilience by researching, analysing, and disseminating actionable intelligence on current and emerging cyber threats. This role conducts in-depth assessments of vulnerabilities, coordinates penetration testing activities, and collaborates with various teams to strengthen BU security posture. The Senior Cyber Threat Intelligence Analyst plays a crucial role in providing insights that enhance security controls and prevent potential threats, staying abreast of cyber trends and developments.

In addition to threat intelligence, The Senior Cyber Threat Intelligence Analyst is responsible for supporting the Cyber Security Specialist for carrying out day-to-day security related duties such as monitoring and maintaining security systems, responding to cyber security incidents, identifying and analysing vulnerabilities, as well as reporting threats.

This position is integral and demands a high level of diligence, in-depth analytical skills, the ability to work under pressure, delivering actions and tasks at pace, and adjust to time pressures and quickly changing priorities. A genuine interest in all aspects of cyber security, along with a comprehensive understanding of the tactics, techniques and procedures for defending and mitigating the identified cyber risks, is crucial for success in this role, requiring to continually research and refresh their understanding of new and emerging cyber threats and build an understanding of how such threats might impact BU operations and how they may be countered.

In addition to the outlined responsibilities, the role may be required to take on other duties or realign their work in response to evolving cyber threats, risks, and the organisational response to such threats. This may include participating in incident response drills, conducting security awareness training sessions, analysing vulnerabilities, forensic investigations, coordinating assurance testing, and contributing to the development of cyber security policies and procedures.

**Main Responsibilities**

1. Perform comprehensive vulnerability assessments and play a key role in remediation or mitigation efforts, actively contributing to regular penetration testing initiatives to bolster BU’s cyber security posture.
2. Research and analyse cyber threats, vulnerabilities, and attack techniques, providing actionable intelligence to enhance BU’s security controls and prevent potential threats.
3. Cross-train with colleagues on different security functions to support incident response efforts, vulnerability assessments and maintaining security tooling effectively.
4. Conduct investigations into cyber security incidents and events, collaborating with the Cyber Security team, IT teams and the rest of BU.
5. Analyse and identify appropriate security services (e.g. systems, processes, software) for incident management which provide a coherent range of cyber security capabilities (e.g. identity, authentication, cryptographic services, etc.).
6. Contribute to the development and review of the university's information security strategy and Information Security Management System (ISMS).
7. Monitor and analyse international, national, regional, and local cyber security developments, policies, and solutions.
8. Provide expert advice on cyber security to subject matter experts. This includes, but is not limited to, identifying technical and administrative controls in response to threats to mitigate risks associated with confidentiality, integrity, and availability.
9. Communicate and collaborate with internal and external stakeholders on cyber security.
10. Assist in developing and enhancing cyber security detection and response capabilities.
11. Monitor current, new, and emerging trends in business, technology, and cyber security solutions.
12. Maintain knowledge of university network architecture and applications to understand system exposure and suggest preventative measures.
13. Contribute to reports informing IT leadership and stakeholders on information security questions, issues, and risks.
14. Identify and recommend requirements for security infrastructure monitoring and initial response to incidents.
15. Contribute to timely and effective cyber security management metrics, KPIs, reports, and management information.
16. Develop forensic investigations processes and procedures while identifying relevant policies and systems.
17. Participate in the development and implementation of new security services and toolsets.
18. Collaborate on identifying and developing enhancements for security processes, tools, and services.
19. Adhere to IT services and university policies, processes, and procedures and report any non-compliance.
20. Contribute to embedding information and cyber security review and remediation within IT work.
21. Strive for excellent service in all interactions, fostering trust within the university community.
22. Research and refresh their understanding of new and emerging cyber threats and build an understanding of how such threats might impact BU operations and how they may be countered.

Organisation Chart



IT Services Dimensions

* Over 100 people in IT Services, including established staff, those on fixed term contracts, and contractors.
* Overall ITS budget of approx. £15m per annum
* 40+ projects running at one time
* Supporting 4000+ staff and 20,000+ students
* 4,500 computers
* Over 500 servers
* 1000+ applications

Contacts Internal and external, including level

Internal:

* Colleagues at all levels within the organisation, up to and including members of UET

External:

* Students
* Customers
* HE Sector colleagues
* Suppliers

Challenges

* Delivering excellent service with finite resources
* Ongoing process and service excellence review
* Managing and leading the work of others, where there is no line management responsibility, to achieve service delivery objectives

Information Governance Responsibilities

Data User

1. Comply with the associated data protection, information security, information management and information technology regulations, policies, processes and procedures.

Safeguarding and Regulated Activity

If the role involves engaging in regulated activity relevant to vulnerable groups including children and disabled adults, it is an [offence to apply for](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F2006%2F47%2Fsection%2F7&data=05%7C02%7Ctmutter%40bournemouth.ac.uk%7Cd2f0a9bde0d24e89aba108dcb7b23e47%7Cede29655d09742e4bbb5f38d427fbfb8%7C0%7C0%7C638587223388443008%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=VkNl1hchNFOwhM62d%2Fg5rVsMF5DV%2B%2BFgbfCJ5knFG7g%3D&reserved=0) and perform the role, if a person is barred from engaging in regulated activity. Further information is available in BU’s [Safeguarding Policy](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fintranetsp.bournemouth.ac.uk%2Fpolicy%2FSafeguarding%2520Policy.docx&data=05%7C02%7Ctmutter%40bournemouth.ac.uk%7Cd2f0a9bde0d24e89aba108dcb7b23e47%7Cede29655d09742e4bbb5f38d427fbfb8%7C0%7C0%7C638587223388458920%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=%2FX5vf2e6NPGW52d0qW02kBzvyW%2FavzuW7%2B7R7v0LV%2Bs%3D&reserved=0) and Suitability Statement on the Recruitment and Employment of Ex-offenders.

Additional Information

When on-call, staff must:-

* be expected to be within one hour travel time of the university
* be fit and available for work at all times
* Be available for contact at all times and mindful of areas where mobile reception is poor

NB:

The purpose of the job description is to indicate the general level of responsibility and location of the position. The duties may vary from time to time without changing their general character or level of responsibility.

BU is an equal opportunities employer which values a diverse workforce. The post holder must at all times carry out their responsibilities with due regard to the University’s Dignity, Diversity and Equality Policy Statement.

Our highly skilled and creative workforce is comprised of individuals drawn from a broad cross section of the globe, and who reflect a variety of backgrounds, talents, perspectives and experiences to build our global learning community. Through fused activity, the post holder must have an understanding of and commitment to promoting a global outlook.

All employees have an obligation to be aware of the University’s Sustainability Policy, Climate and Ecological Crisis Action Plan, Travel Plan and associated documents, and to ensure that they carry out their day-to-day activities in an environmentally responsible manner and inspire students to do the same.

December 2024

|  |  |
| --- | --- |
|  | **Person Specification** |

|  |
| --- |
| **Post / Job Title:** Senior Cyber Threat Intelligence Analyst **Post No:** POSN108653  **Faculty / Service:** IT Services **Date:** December 2024 |

|  |  |
| --- | --- |
|  |  |
| **SELECTION CRITERIA** | **E**ssential / **D**esirable |
| Knowledge (including qualifications and experience) |  |
| Knowledge and experience in the administration and maintenance of information security systems | Essential |
| Knowledge of system administration, network, and operating system hardening techniques. | Essential |
| Understanding of computer networking concepts, protocols, and security methodologies. | Essential |
| Knowledge of risk management processes, including assessing and mitigating risks. | Essential |
| Awareness of cyber threats, vulnerabilities, and different classes of attacks. | Essential |
| Knowledge of cryptography, cryptographic key management, and its application in network security. | Essential |
| Understanding of access control mechanisms, network access, and identity management. | Essential |
| Awareness of system and application security threats, including common attack types. | Essential |
| Knowledge and experience in incident responses, categorising and handling methodologies, and timelines for responses. | Essential |
| Familiarity with ethical hacking principles, penetration testing, and application security risks. | Essential |
| Understanding of network attacks, attackers, and organisation-specific threat environments. | Essential |
| Excellent awareness of privacy concepts (e.g. international and industry standards, legal and regulatory constraints, etc.), commensurate with this role | Essential |
| Understanding of IT Service provision in medium to large organisations | Essential |
| Good awareness of IT related legislation and guidelines such as the Computer Misuse Act and Data Protection | Essential |
| Knowledge and experience of working in a production environment and/or development and delivery of enterprise systems. This includes a strong understanding of the secure development lifecycle. | Desirable |
| Knowledge and experience in working with Information Security / Cyber Security related frameworks | Desirable |
| Knowledge of PRINCE2 or other formal project management and ITIL Service Management methodology | Desirable |
| Awareness and understanding of the activities and developments within Higher Education and/or public sector | Desirable |
| Knowledge of emerging technologies relevant to protection of operational infrastructure | Desirable |
| Hold, or have held, technical accreditations, in one or more application focused disciplines. | Desirable |
| **Skills** |  |
| Excellent IT skills, including Microsoft Office suite and Microsoft 365 | Essential |
| Skill in conducting vulnerability scans and recognising vulnerabilities in security systems. | Essential |
| Skill in the use of penetration testing tools and techniques, and network analysis tools to identify vulnerabilities. | Essential |
| Skill in using incident handling methodologies. | Essential |
| Skill of identifying, capturing, containing, and reporting malware. | Essential |
| Skill to develop insights about the context of an organisation’s threat environment | Essential |
| Skill in recognising and categorising types of vulnerabilities and associated attacks. | Essential |
| Excellent interpersonal skills including motivational negotiating, influencing and relationship building (including at a senior level) | Essential |
| Identify, analyse and address problems in order to resolve issues whenever possible in a way that minimises the negative impact on the organisation | Essential |
| Strong analytical skills; ability to evaluate complex issues often with incomplete information | Essential |
| Demonstrable ability to be part of and inspire multi-skilled teams | Essential |
| Demonstrate excellent verbal and written communication skills, across all levels | Essential |
| Demonstrable ability to handle a range of activities to tight and varied timescales | Essential |
| Demonstrable ability to engage and collaborate with staff at a business and technical level | Essential |
| **Attributes** |  |
| Empathetic | Essential |
| Collaborative | Essential |
| Attention to detail | Essential |
| Customer-centric approach | Essential |
| Innovative | Essential |