happy to
talk flexible
working

1 Advertisement

Post Title: Junior Cyber Security Analyst
School/department: ITS
Hours: full time considered up to a maximum of 1 FTE
Requests for flexible working options will be considered (subject to business need).
Contract: fixed term until May 2024.
Reference: 20390
Salary: starting at £22,630 to £23,662 per annum, pro rata if part time current salary scales can be found here
Placed on: 3rd May 2023
Closing date: 23rd May 2023 Applications must be received by midnight of the closing date.
Expected Interview date: To be confirmed
Expected start date: As soon as possible

The University of Sussex is a leading academic institution nestled in the beautiful South Downs, on the outskirts of Brighton. With staff and students from over 100 countries, we are a diverse and innovative environment, and one of the highest performing universities in the world. We are also a major local employer, with a revenue of over £320m per year and over 3,000 employees.

Led by an award-winning Chief Digital Transformation Officer and inspirational leadership team, we are now embarking on an ambitious programme of transformational change. Over the coming years, this digital transition will be an ever-developing programme supported by senior stakeholders both financially and strategically. Put simply, whilst we are already a highly successful organisation and business, the University will be a very different world in years to come and achieve levels of performance and digital delivery as yet unseen in the sector. All of this is underpinned by major construction and estate renewal, an exciting programme of work to add thousands of accommodation spaces, and a network replacement project to install the latest digital infrastructure as part of the journey towards a fully data-enabled organisation.

We are moving to an agile world and need to take the organisation on the same journey; to be sector leading and to deliver a model of digital delivery fit for the coming years. As this programme gains momentum, we need more people to join us as we unpick our challenges and legacy systems and move towards meeting our potential.

The Junior Cyber Security Analyst works within the Cyber Security team ensuring that the services and systems that underpin the University activities form a digitally safe environment and deliver a seamless environment and experience for all our students and staff. The role supports the University’s Cyber Security ‘business as usual’ activities and the improvement programme by assisting with actively identifying and addressing security threats and mitigating risks and working to ensure compliance to standards and certifications such as Cyber Essentials Plus. The role involves collaboration with colleagues, University stakeholders, 3rd Parties and project teams to support the delivery of strategic objectives.

To be successful in the role you will be able to demonstrate an interest for IT and in particular basic knowledge of Cyber Security systems and controls, including end point security, vulnerability management, web content filtering, intrusion prevention, SIEM, email security, data loss prevention, NAC, IAM, cloud security and firewalls. An interest in cyber threat landscape including emerging threats, risks and vulnerabilities aligned with mitigation strategies used to defend and protect information will also be of particular interest.

You will have well-developed interpersonal skills with the ability to quickly build rapport to effectively contribute to team working as well as effective oral and written communications skills to work with colleagues and customers providing information and responding to questions and queries, with the ability to relay technical issues to a non-technical audience in an engaging and informative manner.
This role will have a structured support network that will allow you to grow your experience and enhance your current skillset and therefore we are seeking an individual that has a willingness to learn from others and is happy to take direction in your day to day work.

You will receive full training on a number of our IT systems used by the University's main ITS department. You will gain general experience of working in a professional services environment, including the day to day running of a team and the use of our systems. All University of Sussex staff have access to professional development opportunities in areas such as equalities, IT, wellbeing, and cultural awareness.

Not only do we offer flexible and remote working, a vibrant atmosphere, use of our incredible facilities, benefits, and an amazing pension; but we are offering the opportunity to be part of a transformation that will see us set the benchmark for a model of digital delivery in the HE sector.

For further information please contact Michelle Richardson at michelle.richardson@sussex.ac.uk

For full details and how to apply see our vacancies page

The University of Sussex values the diversity of its staff and students and we welcome applicants from all backgrounds.

IT Services delivers a wide range of digital services to users across our Campus and beyond.
Our Chief Digital Transformation Officer, Jason Oliver, is now tasked with shaping the strategic initiatives and strategies that will secure a successful and sustainable future for the institution, where digital technology and mobile platforms will increasingly transcend physical and geographical boundaries providing opportunities for the transformation of our students' and staff lives.
Prior to joining Sussex he undertook similar advancements at the Science Museum Group and the Royal Opera House, where he built sector-leading teams and delivered a large-scale transformation agendas resulting in step-changes in organisational culture.

IT Services is organised into four main teams, delivering services through an evolving agile service management and delivery model**:**
The Digital Engagement team are primary changes agents working to transform our business processes and systems, to nurture the relationships between IT Services and its stakeholders, and helping us to understand and develop the ambitions for our use of digital technologies in education, research, student services and university administration.
The Strategy and Architecture team ensure our strategies, technologies, security and standards support our digital aspirations whilst planning the replacement, upgrades and improvements to our technologies and systems, ensuring that they are aligned and prioritised around the University's

strategic plans and objectives.
The Infrastructure team work to define, modernise and automate our underlying platforms and network ensuring that they are optimised to meet the needs of the diverse communities across the University, to continue our journey to the cloud and to advance our approaches to ubiquitous connectivity across our campus.
The Operations team work across the research, teaching, professional services and student groups to manage our product areas, develop and integrate our platforms and applications, and support our communities to ensure outstanding service provision across the operational activity of IT Services.

3. Job Description

Job Title:	Junior Cyber Security Analyst
Grade:	3
School/Division:	IT Services
Location:	Shawcross, University of Sussex
Responsible to:	Cyber Security and Compliance Analyst
Direct reports:	n/a
Key contacts:	Cyber Security Manager Assistant Director, Strategy and Architecture ITS Operations ITS Networks and Infrastructure Sussex Projects

Role description:

The Junior Cyber Security Analyst works within the Cyber Security team ensuring that the services and systems that underpin the University activities form a digitally safe environment and deliver a seamless environment and experience for all our students and staff. The role supports the University's Cyber Security 'business as usual' activities and the improvement programme by assisting with actively identifying and addressing security threats and mitigating risks and working to ensure compliance to standards and certifications such as Cyber Essentials Plus. The role involves collaboration with colleagues, University stakeholders, 3rd Parties and project teams to support the delivery of strategic objectives.

PRINCIPAL ACCOUNTABILITIES

- Working alongside the Cyber Security and Compliance Analyst to assist in identifying and monitoring threats and risks to University systems, helping to identify options and recommending solutions, liaising closely with relevant operational teams and ensuring plans for remediation are followed in a timely way.

- Assisting the Cyber Security and Compliance Analyst with carrying out the day-to-day tasks around handling security events and incidents, checking security systems are operating correctly and carrying out investigations and reviews.
- Supporting the Cyber Security programme to achieve Cyber Essentials Plus certification and ensure that the University remains in compliance with these and other security certifications and standards, including PCI-DSS.
- Supporting the Cyber Security and Compliance Analyst in conducting audits and risk assessments that support the University's digital strategy.
- Supporting the Cyber Security and Compliance Analyst and wider Sussex project function with the assessment and implementation of operational tools related to Cyber Security.
- Assisting the Cyber Security and Compliance Analyst with providing robust and insightful data on agreed performance indicators with the aim of establishing best practice around the use and interpretation of analytics to drive activity.
- Providing information, advice, and guidance to ensure people, data and systems remain safe.
- Supporting colleagues in accessing and interpreting information provided.

KEY RESPONSIBILITIES

Identification and Monitoring of Cyber Security Threats

- Assisting with monitoring the SIEM platform and utilising other tools and sources to identify any potential or actual cyber security threats.
- Conducting vulnerability and penetration testing activities including recording of findings and ensuring findings are remediated in accordance with agreed time frames and priorities.
- Reviewing security events and incidents as they are raised and assessing the most appropriate way for them to be addressed, working with colleagues to ensure timely resolution.
- Updating records of security incidents and resolutions, capturing root causes in order that issues can be identified and recommendations made for continuous improvements.
- Contributing to the development of management information reporting which provides data on the achievement of identified key performance indicators.
- Compile and present appropriate standard reports for key stakeholders, including narratives to clarify meaning and aid decision making which take into account the needs of the stakeholder group and presents material in the most appropriate way.

Supporting achieving and maintaining certifications

- Supporting the Cyber Security and wider project team and others to identify and carry out activities necessary to achieve Cyber Essentials Plus certification.
- Working with colleagues in Finance, and other business areas, to help to complete and assure continued compliance with Payment Card Industry Data Security Standard (PCI-DSS).
- Following agreed strategy, work with colleagues to achieve any other cyber security related standards.
- Under guidance, carrying out periodic reviews and assessments to ensure continued compliance with any achieved security standards.

Providing advice and guidance

- Working with the University Data Protection team and users to address data protection-related concerns, providing advice and support as required.
- Providing advice in the most accessible and user-friendly way about digital security, supporting the safety of people, data and systems.
- Working collaboratively with colleagues, being actively involved in meetings, training sessions, sharing information and contributing to the development of processes.

- To stay up to date with current developments in cyber security data analysis and be aware of best practice in tools, techniques and trends.
- Support colleagues in accessing and interpreting information provided.
- To carry out any other duties that are within the employee's skills and abilities whenever reasonably instructed.

Dimensions

- This role does not have any budget responsibility.
- This role does not have any line management responsibility.
- This role does not have any responsibilities for equipment or premises.

- Support achievement of the Division’s/Unit’s/School’s compliance with all applicable statutory and regulatory compliance obligations, including (but not limited to): UKVI, Health & Safety, the Prevent Duty, data protection, Competition and Markets Authority requirements and equal opportunities, as appropriate to the grade and role. Additionally, to promote good practice in relation to university policy, procedure, and guidance in relation to those compliance matters in respect of students, staff and other relevant parties.

This Job Description sets out current responsibilities of the post that may vary from time to time without changing the general character of the post or level of responsibility entailed.

UNIVERSITY OF SUSSEX

PERSON

SPECIFICATION

1. An interest and enthusiasm for IT and Cyber Security

2. Studying to degree level or equivalent work experience in technology roles

3. Effective planning and organisational skills to organise own workload and priorities

4. Analytical skills with the ability to interpret data

5. Recognise and work in ways that support strategic plans

6. Identify opportunities and share ideas and best practice with others

7. Well-developed interpersonal skills with the ability to quickly build rapport to effectively contribute to team working

8. Effective oral and written communications skills to work with colleagues and customers providing information and responding to questions and queries, with the ability to relay technical issues to a non-technical audience in an engaging and informative manner

9. Demonstrate a flexible approach to teamwork, together with a willingness to learn from others and able to seek and take direction when using initiative and problem solving

10. Able to organise and manage own workload

11. Ability to maintain confidentiality and keep information/data secure

ESSENTIAL ROLE-SPECIFIC CRITERIA

1. Basic knowledge of cyber security systems and controls, including end point security, vulnerability management, web content filtering, intrusion prevention, SIEM, email security, data loss prevention, NAC, IAM, cloud security and firewalls

2. General IT knowledge systems and their relationship with data

3. Some knowledge of cyber threat landscape including emerging threats, risks and vulnerabilities aligned with mitigation strategies used to defend and protect information

4. Basic understanding of risk management

DESIRABLE CRITERIA

1. Some experience of cyber security tools, information security technologies and best practice processes

2. Basic knowledge of UK Data Protection legislation and other information security legislation and best practice

3. Basic knowledge of cyber security standards, including Cyber Essentials, PCI-DSS and ISO27000 family