Senior Analyst (Cyber Security) 25000089

The University

At Durham University we are proud of our people. A globally outstanding centre of educational excellence, a collegiate community of extraordinary people, a unique and historic setting – Durham is a university like no other. Across the University we have a huge variety of roles and career opportunities, which together make us a large and successful community, which is a key hub of activity within our region and nationally. Whether you are at the very start, middle or end of your career, there is a role for you. We believe everyone has their own unique skills to offer. We would be thrilled if you would consider joining our thriving University. Further information about the University can be found here

The Role and the Department

The Computing and Information Services (CIS) has an annual operational budget in excess of £12m, multi-million pound programmes of change within year, and approximately 185 staff. The Senior Leadership Team report directly to the Chief Information Officer (CIO) with the following portfolios: Strategy and Change; Technical Services (TS); Information Services (IS), and Cyber Security. CIS work with departments across the university to provide academic, teaching and administrative services that underpin the day-to-day activities of the whole organisation. Details of the Digital Strategy and ongoing work can be found at Digital Strategy - Durham University

CIS is a friendly, but demanding department, where much is expected and can be achieved by competent, self-motivated individuals who are demonstrable in their teamwork ability. The department works in a hybrid capacity depending on the job role and individual personal requirements.

As part of the Security team, the post holder will:

- Work with colleagues and external partners to detect and respond to cyber security alerts, incidents and reports (who and what affected, what is the risk, next steps).

- Perform security investigations and take responsibility for carrying out more specialist security incident resolution.

- Operate, improve and take ownership of security tools, securing University networks, systems, users and assets from malicious activity.

- Implement and monitor protocols, procedures, processes and regulations.
- Interpret, curate, design and present artefacts, information, data, equipment and resources including anti malware, encryption, Network Access Control, web & email filtering, Security Information Event Monitoring and authentication capabilities.

- Engage with internal and external networks, exchanging knowledge and information to provide input into the planning and development of future projects and services.

- Assist in managing security risk and issue logs.

- Share security best practice, principles and standards within in the team and externally.

- Contribute to the preparation and maintenance of user security documentation (web pages, FAQs, guides)
- Sharing knowledge and experience with the rest of the team, including more junior members.

Working Hours:

35 Hour Week

The University is piloting hybrid working and is flexible to remote working for this role. Flexibility to cover 8am-6pm and work out of hours may be required on occasion.

Further information about the role and the responsibilities is at the bottom of this job description.

Working at Durham

A competitive salary is only one part of the many fantastic benefits you will receive if you join the University: you will also receive access to the following fantastic benefits:

• 27 Days annual leave per year in addition to 8 public holidays and 4 customary days per year – a total of 39 days per year. The University closes between Christmas and New Year
• No matter how you travel to work, we have you covered. We have parking across campus, a cycle to work scheme which helps you to buy a bike and discount with local bus and train companies.
• Lots of support for health and wellbeing including discounted membership for our state of the art sport and gym facilities and access to a 24-7 Employee Assistance Programme.
• On site nursery is available and access to holiday camps for children aged 5-16 throughout the year.
• Family friendly policies, including maternity and adoption leave, which are among the most generous in the higher education sector (and likely above and beyond many employers).
• There is a genuine commitment to developing our colleagues professionally and personally. There is a comprehensive range of development courses, apprenticeships and access to qualifications and routes to develop your career in the University. All staff have dedicated annual time to concentrate on their personal development opportunities.
• The opportunity to take part in staff volunteering activities to make a difference in the local community
• Discounts are available via our benefits portal including; money off at supermarkets, high street retailers, IT products such as Apple, the cinema and days out at various attractions.
• We offer generous pension schemes.

Durham University is committed to equality, diversity and inclusion

Our collective aim is to create an open and inclusive environment where everyone can reach their full potential and we believe our staff should reflect the diversity of the global community in which we work.

As a University equality, diversity, and inclusion (EDI) are a key part of the University's Strategy and a central part of everything we do. We also live by our values and our Staff Code of Conduct. At Durham we actively work towards providing an environment where our

staff and students can study, work and live in a community which is supportive and inclusive. It's important to us that all of our colleagues are aligned to both our values and commitment to EDI.

We welcome and encourage applications from members of groups who are under-represented in our work force including people with disabilities, women and black, Asian and minority ethnic communities. If you have taken time out of your career, and you feel it relevant, let us know about it in your application. If you are a candidate with a disability, we are committed to ensuring fair treatment throughout the recruitment process. We will make adjustments to support the interview process wherever it is reasonable to do so and, where successful, reasonable adjustments will be made to support people within their role.

What you need to demonstrate when you apply/Person Specification

When you apply it is important that you let us know what skills/experience you have from a similar role and/or what skills/experience you have which would make you right for this role. Further information about the role and responsibilities is at the end of this job description. Where a criteria has an asterisk* next to it, it may be given additional weighting when your application is considered.

Your application should cover the following criteria:

Qualifications/Experience

1. Five GCSE's at least Grade C or level four (or equivalent) including English Language and Mathematics or a Post-16 qualification or equivalent experience.
2. Have been awarded a higher education qualification at bachelor's level and possess a minimum 2:2 classification by a recognised university or other recognised higher education institution.
3. Knowledge and expertise in security technologies such as anti-malware, encryption, SIEM, web & email filtering, firewall and authentication.
4. Experience of providing advice and guidance to a range of customers and colleagues.
5. Proven experience performing risk assessments and recommending mitigating controls, preferably in the information security space.
6. Experience of implementing policies and procedures.

Skills/Abilities/Knowledge
7. Broad IT knowledge of systems, networks, applications, web, hardware and scripting.
8. Demonstrable knowledge of the wider security threat landscape and issues.
9. Good spoken and written communication skills including the ability to develop effective working relationships, both internally and externally.
10. Strong digital competence across a range of digital devices and apps.
11. Ability to solve problems and decide on and plan appropriate solutions.
12. Committed to continuing professional development.
13. Ability to work collaboratively with other team members to ensure the delivery of high-quality services.
14. Ability to participate in networks to share and discuss good practice and exchange information.

Desirable Criteria

1. Professional craftsperson/practitioner with knowledge and expertise in IT service provision.

2. Relevant industry and professional recognition and certification of achievement of skills and knowledge.
3. Evidence of continuing professional development.
4. Regulatory, local and national professional knowledge and experience of compliance.
5. Experience of contributing to the delivery of IT provision.
6. Ability to provide support for IT projects
7. Ability to effectively network and exchange advice and information for development purposes.
8. High levels of self-motivation, initiative and ability to promote and demonstrate a flexible 'can do' attitude.
9. Experience of implementing policy and procedures.

How to apply

To progress to the assessment stage, candidates must evidence each of the essential criteria required for the role in the person specification above. Where there are desirable criteria we would also urge you to provide any relevant evidence. Please don't forget to check if there is any weighted criteria (see above).

While some criteria will be considered at the shortlisting stage, other criteria may be considered later in the assessment process, such as questions at interview.

Submitting your application

We prefer to receive applications online. We will update you about your application at various points during the process, via automated emails from our e-recruitment system. Please check your spam/junk folder periodically to ensure you receive all emails

What you are required to submit:

• A CV
• A covering letter or statement which shows examples of how you meet all of the criteria within the Person Specification

Contact details

If you would like to have a chat or ask any questions about the role, we would be happy to speak to you. neil.lough@durham.ac.uk / gary.foster@durham.ac.uk

Typical Role Requirements

Service Delivery

• Show a commitment to equality, diversity and inclusion and the University's values.
• Ensure that the University's procedures and values are always reflected in all aspects of the service and adapt ways of working where this is not evident.
• Provide specialist advice and make decisions to resolve problems relating to the services you are responsible for.
• Deliver infrastructure services and projects in collaboration with other across the University.

- Manage and monitor the use of systems, applications and resources.

- Perform proactive and reactive IT security monitoring and investigate and report incidents.

- Provide the best possible service to the University by reviewing and making suggestions to improve security services.
- Resolve incidents that require relevant expertise.

- Demonstrate ability to use a range of security technologies.
- Take responsibility for carrying out more specialist security risk assessments and incident resolution.
- Assist in managing security risk and issue logs and the development of plans to manage these as appropriate.
- Create repeatable solutions and processes (test scripts, checklists, etc.).
- Track security risks including unpatched systems, clients and applications, escalating to management where necessary.
- Contribute to the preparation and maintenance of user security documentation (web pages, FAQs, guides).

Planning and Organising
- Plan and organise own workload with or without involvement with project work streams.

- Plan, manage and deliver assigned projects and activities in accordance with agreed objectives.

- Supervise service users and stakeholders undertaking activities, events, project work and exhibitions.

- Take responsibility for day-to-day decision making within own area of responsibility for operational aspects of service delivery, translating external requirements into practical application and advice.

- Seek feedback to ensure that the service is being adapted to meet customer expectations.
- Manage budgets and expenditure including buying (and returning) goods and services.

Communication/Liaison

- Develop and improve services by taking part in meetings, working groups and committees.

- Relationship building, network participation internally and externally to build and update knowledge and skills.

- Engage with external peers and specialists to exchange knowledge and information

- Explain and demonstrate to others how to carry out tasks and use a range of tools

- Liaise with key stakeholders and client representatives across the University to inform and offer advice about key security activities.
- Champion security best practice, principles and standards.

- Create good working relationships, including internal and external networks which allow you to increase your knowledge and skills, while swapping information with peers.
- Any other reasonable duties.

Useful links
If you would like further information you may find the following will help

Please note that in submitting your application Durham University will be processing your data. We would ask you to consider the relevant University Privacy Statement <u>Privacy Notices - Durham University</u> which provides information on the collation, storing and use of data.