Cyber Security Operations Engineer

**Department:** Directorate of Technology Estates and Facilities

**Hours of work:** Full Time | 37 hours per week

**Contract type:** Open

**Salary:** Grade 6 | £34,308 - £42,155 per year
Introduction

The Directorate of Technology, Estates and Facilities [DTEF] is responsible for ‘providing outstanding work, study, research facilities, and facilities to enhance the student experience, on campus and online’.

The role will be part of the cyber security team within IT Services. Cyber Security is a key priority at the University of York. Through investment from the University Executive Board the Cyber Security Team must maintain an updated position in order to continue to meet the ever changing landscape of Information Security.

We believe in developing our own people and investing in the future, and this role within Security Operations requires experience of cyber security but with the scope to develop skills in one or more specialist areas, and in which a high degree of trust will be placed. Security is a rapidly growing and evolving industry, and we see this as a great role for someone wanting to explore a career in it.

Main purpose of the role

The Cyber Security Operations Engineer will report to the Cyber Security Operation Manager and will be a team member for the support and operation of the Cyber Security toolset, working closely within the Security Operations Team, ITS and key suppliers for day to day operations.

The Cyber Security tooling includes:

- Security Information and Event Management with Managed SOC
- Managed Detection and Response and Antimalware solutions
- Vulnerability scanning and detection
- Firewalls, IDS and VPNs
- Security credential store

Key responsibilities

(Role holders will be required to undertake some or all of the duties below)

1. Role Specific Responsibilities

Cyber Security Team

- As Security Operations Engineer you provide operational support on the toolset, guidance and support to other cyber security team members within the team and other operational ITS and University colleagues for onboarding and use of tooling.
- As Security Operations Engineer you will be hands-on with the security tooling; conducting daily checks, assessing information and alerts, liaising with ITS colleagues to provide cyber security response and guidance on assessed alerts.

Technical Security

- As part of the Security Operations Team you will ensure security tooling is documented, maintained, deployed in line with requirements and administration of the tooling is inline with our specifications and standards.
- As the technical user within the Security Operations Team, support the Cyber Security Operations Manager in the technical use of the security toolset and cross team collaboration within IT Services and other University technical teams.
You will triage and respond to issues raised with the security operations team.

Policy & Process

- As Security Operations Engineer, applying your experience and cyber security knowledge to proactively monitor security of University IT services and have appropriate identify vulnerabilities, issues or incidents, and to take action to initiate responses and ensure issues are resolved.
- You will support the Head of Cyber Security in identifying gaps, non-compliances or improvements in policy.
- Ensure that Security Operations services are documented and presented to ensure that ITS and non-ITS technical teams know the processes for engagement and the requirements to support tooling in their environments.

Incident Management

- Communicate specific alerts to IT colleagues and other technical support staff across the University with timely updates on new vulnerabilities identified.
- You will be required to determine sources and assess threat analysis data in support of cyber security alerts and future use cases that may be important for the University to understand.

Strategy

- As required you will contribute to or lead the development of requirements, liaison with specific suppliers or the implementation of new services, this includes liaising with and gathering requirements from across ITS.

Security Community

- Attend ITS Security Group as required to present reports and developments; highlighting performance data, issues and actions that need to be discussed across ITS.

Suppliers

- You will be interacting, receiving alerts from and assisting with upskilling the Managed Security Operations Centre service. You will be assigned specific issues or projects to collaborate across IT Services.

2. University of York Responsibilities for Grade 6

Service and Operational Delivery

- Oversee a responsive and proactive support service to ensure service expectations are met.
- Collect and analyse stakeholder feedback to help define needs and requirements and the design and planning of services.
- Contribute to operational leadership teams and decision making to shape the nature and level of support services.
- Implement changes to the design and development of a service.
- Accountable for delivery of a service within a defined area or defined responsibilities.
- Make effective use of digital solutions to carry out operational activity and implement efficiency improvements.
- Depending on the role, may be required to act as operational line manager - setting, monitoring and overseeing the work of the team on a day to day basis.
Continuous Improvement

- Analyse service and operational delivery data and provide reports, making recommendations for improvement as appropriate.
- Ensure the review and improvement of systems and procedures in line with University frameworks.
- Review internal and external practice to identify opportunities for future improvements or efficiencies.
- Apply expertise to identify, understand and propose resolutions for issues or problems.
- Proactively identify opportunities for building personal knowledge and skills, and ensure training and development needs of the team are met.
- Deliver knowledge sharing on specialist defined processes across the broader team.

Specialist Contribution

- Provide advice to stakeholders in relation to complex policy, procedures and regulations.
- Provide specific technical advice to ensure compliance with legislation, statutory duties, etc.
- Provide specialist expertise and support with complexity of data and information sources, providing interpretation and analysis.
- Carry out in-depth, complex investigations or searches; interrogate the information and data to identify trends and patterns.
- Deliver training, teaching and/or development delivery for stakeholders.

Collaboration and Communication

- Establish, maintain and develop productive and ongoing relationships with University stakeholders to create ideas for tactical service or operational delivery development.
- Build relationships and networks internally and externally to build and update knowledge and skills.
- Use a range of digital media and tools to communicate with a diverse range of key stakeholders.
- Act as a supportive and encouraging member of a team. For roles at this level with supervisory responsibilities, demonstrate compassion and give advice on commonly occurring wellbeing issues.

Governance and Oversight

- Oversee activity to ensure all processes and transactions are delivered in line with regulatory and professional service and policy standards.
- Provide advice and training to stakeholders regarding compliance and regulations relating to the area of responsibility.
- Contribute to the creation or development of policy and procedures to take account of internal and external changes.
- Ensure activities and documents comply with internal University and external regulation, policy and procedures.

Planning and Organisation

- Plan, organise and prioritise the work of self and team members on a regular basis, taking into account operational needs and changing circumstances over the short to mid term.
- Contribute to longer term strategic/planning of the team’s work.
- Lead the delivery of projects to facilitate service operational change or play a role in University-wide projects.
The above list of duties is not exhaustive and is subject to change. The post holder may be required to undertake others duties within the scope and grading of the post.
## Person specification

<table>
<thead>
<tr>
<th>Role Specific</th>
<th>Essential / Desirable</th>
</tr>
</thead>
<tbody>
<tr>
<td>A working understanding of cyber security, secure working practices, technical controls and emerging threats</td>
<td>Essential</td>
</tr>
<tr>
<td>Ability to develop and deliver technical training and support to users of varying ability</td>
<td>Essential</td>
</tr>
<tr>
<td>Familiarity with the legislation governing data processing (GDPR, DPA, PECR)</td>
<td>Essential</td>
</tr>
<tr>
<td>Experience in leading or supporting technology based change activities</td>
<td>Essential</td>
</tr>
</tbody>
</table>

### University of York Person Specification for Grade 6

#### Qualifications:

Level 3 qualification. (Qualifications at this level include A levels. Please view the full list). We also welcome applicants with equivalent non-uk qualifications or equivalent professional experience.  

#### Skills - demonstrates the ability to:

- Lead projects | Essential
- Gather, analyse, interpret and report complex data/information | Essential
- Use digital technologies including Google applications and/or Microsoft Office | Essential
- Communicate effectively in verbal and written formats, including the use of a variety of digital tools | Essential

#### Behaviours:

- Works collaboratively with others | Essential
- Delivers a quality service | Essential
| Develops self and others                      | Essential |
| Actively champions respect, inclusivity, equality and diversity | Essential |
| Identifies and implements continuous improvement | Essential |