Cyber Security Senior Analyst – Band 8A (Leeds)

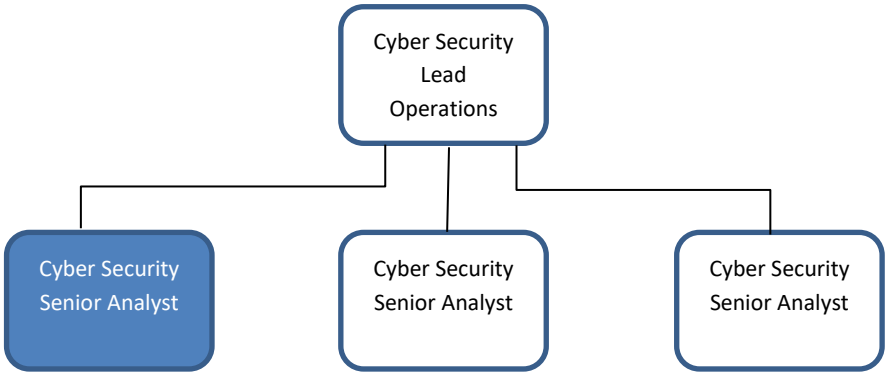
Recruitment role summary and candidate profile

About this role

The Cyber Security Senior Analyst will:

- Keep up to date with the latest security and technology developments, to include: researching and evaluating emerging cyber security threats and ways to manage them.
- Use the Splunk SIEM to monitor for attacks, intrusions and unusual, unauthorized or illegal activity.
- Investigate security alerts and provide incident response.
- Use advanced analytic tools (Windows ATP, Cisco StealthWatch) to determine emerging threat patterns and vulnerabilities.
- Identify potential weaknesses and help organizations improve their security posture.
- Liaise with the Cyber Security Lead Operations in relation to cyber security issues and provide future recommendations.
- Support the Lead Operations plan for disaster recovery in the event of any security breaches.
- Generate reports for technical and non-technical stakeholders.
- Give advice and guidance to NHS organizations on issues such as spam and unwanted or malicious emails, 'phishing' emails and 'pharming' activity.
- Assist with the creation, maintenance and delivery of cyber security awareness training for colleagues and tabletop exercises.

About the team



About NHS Digital

We're the national information and technology partner to the health and social care system. We're using digital technology to transform and improve the NHS and social care. Visit our website to read more about us.

Profession: Cyber Security

Please note, this role profile is an extract taken from the full job description of Cyber Security Senior Analyst

About You

Professional Competencies

- **Information Security Management -** Expert knowledge of the processes, tools and techniques of information security management, ability to deploy and monitor information security systems, as well as detect, resolve and prevent violations of IT security, to protect organizational data.
- **Security Information and Event Management (SIEM) -** Extensive knowledge of concept, procedures and processes of Security Information and Event Management (SIEM); ability to utilize related applications to protect organizational networks from cyber risks.
- **Intrusion Detection and Prevention -** Working knowledge of tools, techniques and processes of intrusion detection and prevention; ability to detect, resolve and prevent intrusion behaviours to protect organizational networks.
- **Modelling Use Case** - Detailed knowledge of the processes and techniques used to identify, clarify, and organize system requirements for users and systems within a business; ability to utilize use case modelling, define and document business requirements and application scenarios during this process.
- **Information Security Operation Centre (ISOC) -** Demonstrable knowledge of modules, processes and technologies of Information Security Operation Centre (ISOC); ability to detect, response and utilize related platform and applications to perform cyber security initiatives.
- **Technical Writing/Documentation** - Working knowledge of the technical language and writing approach, and the ability to write paper-based and on-line technical reference documentation (guidelines, standards, procedures, processes, applications, etc.)

Knowledge, Skills and Qualifications

Essential

- Masters level degree or equivalent level of experience.
- Experience of mentoring and leadership.
- Hold industry qualifications such as SANS, CREST, EC-Council
- Evidence of continuous professional development in the Cyber Security field.
- Excellent written and verbal communication skills.

Desirable

- Knowledge of the NHS.
- Membership of professional body such as SANS, CREST, EC-Council

Values and Behaviours

- **People Focused**: You value and promote positive relationships with colleagues, customers and the public and are responsive to their needs.
- **Trustworthy**: You act with integrity, impartiality and openness and in the best interests of the public.
- **Professional**: You deliver on your commitments by applying the highest levels of expertise, conduct and personal responsibility.
- **Innovative**: You actively embrace change and bring new ideas to deliver excellent services for your customers and better outcomes for the public.

Profession: Cyber Security

Please note, this role profile is an extract taken from the full job description of Cyber Security Senior Analyst

disability confident EMPLOYER

About the Benefits

The Opportunities

- You will be a Tier 3 SME Analyst having worked your way through Tier 1 and 2 roles. A key aspect of the role will be supporting the Cyber Security Lead Operations on upskilling the team's Tier 1 and 2 Analysts through mentoring and training.
- You will be in a team of highly skilled Cyber Security professionals who are all working towards positively improving the Cyber Security posture of NHS organisations while continuously improving their resilience to cyber-attacks and safeguarding their ability to provide services to patients throughout England. The holder of the role will need to have an accurate and analytical mindset.
- You will benefit from a real commitment to your personal and professional development. A twice-yearly Performance Development Review process focuses upon your professional competencies and identifies opportunities for improvement.
- Our staff use the Civil Service-Learning portal which allows access to the best training courses across government.
- You will have the opportunity to work on systems and services of unparalleled scale and complexity.
- You will benefit from a real commitment to your personal and professional development.

The Terms and Conditions

- A competitive salary.
- Flexible working applications considered.
- Family friendly benefits.
- Annual leave starting at 27 days per annum plus statutory bank holidays rising to 33 days with service.
- An excellent contributory pension scheme.

Profession: Cyber Security

Please note, this role profile is an extract taken from the full job description of Cyber Security Senior Analyst

disability confident EMPLOYER