ICR The Institute of Cancer Research

Cyber-Security Engineer
Candidate Information

March 2024

The Institute of Cancer Research

About our organisation

We are one of the world's most influential cancer research institutes with an outstanding record of achievement dating back more than 100 years. We are world leaders in identifying cancer genes, discovering cancer drugs and developing precision radiotherapy. Together with our hospital partner The Royal Marsden, we are rated in the top four centres for cancer research and treatment worldwide. As well as being a world-class institute, we are a college of the University of London.

We came second in the league table of university research quality compiled from the Research Excellence Framework (REF 2021). We have charitable status and rely on support from partner organisations, charities, donors and the general public.

We have charitable status and rely on support from partner organisations, charities, donors and the general public.

We have more than 1000 staff and postgraduate students across three sites – in Chelsea and Sutton.

Digital Services

The Digital Services Directorate ensures that everyone at the ICR has access to the technology they need to do their jobs effectively including providing specialist IT support to the ICR's research community.

The Job Role

The Cyber-Security Engineer safeguards our critical data and infrastructure from cyber threats by implementing and maintaining robust security solutions.

Our mission is to make the discoveries that defeat cancer.

Cyber-Security Engineer
Candidate Information

Our values

The ICR has a highly skilled and committed workforce, with a wide variety of roles, each requiring different skills. But whether you work as a researcher, or work as part of our corporate team, your work and behaviour is underpinned by these six values. They are what bring us together as one team - as 'One ICR'.

Pursuing excellence

We aspire to excellence in everything we do, and aim to be leaders in our field.

Acting with Integrity

We promote an open and honest environment that gives credit and acknowledges mistakes, so that our actions stand up to scrutiny.

Valuing all our people

We value the contribution of all our people, help them reach their full potential, and treat everyone with kindness and respect.

Working together

We collaborate with colleagues and partners to bring together different skills, resources and perspectives.

Leading innovation

We do things differently in ways that no one else has done before, and share the expertise and learning we gain.

Making a difference

We all play our part, doing a little bit more, a little bit better, to help improve the lives of people with cancer.

Our values set out how each of us at the ICR, works together to meet our mission – to make the discoveries that defeat cancer. *They summarise our desired behaviours, attitudes and culture – how we value one another and how we take pride in the work we do, to deliver impact for people with cancer and their loved ones."*

Professor Kristian Helin
Chief Executive

Cyber-Security Engineer
Candidate Information

Job description

Department / division:	Digital Services
Pay grade / staff group:	Professional Services 4
Hours / duration:	Full time (35 hours per week), Monday to Friday.
Reports to:	Cyber-Security Manager
Main purpose of the job:	The Cyber-Security Engineer safeguards our critical data and infrastructure from cyber threats by implementing and maintaining robust security solutions.

Objectives

Protect the organization's data, systems, and networks from cyber-attacks: This includes preventing unauthorized access, data breaches, and other malicious activities.
Maintain a secure and compliant IT environment by ensuring the adherence to industry standards and regulations related to cybersecurity.
Proactively identify and mitigate security risks by continuously monitoring for vulnerabilities and implement appropriate controls to minimize threats.

Cyber-Security Engineer
Candidate Information

Duties and Responsibilities

Implement, and manage security controls including firewalls, intrusion detection systems, data encryption, and user access controls.
Respond to security incidents by investigating suspicious activity, contain threats, and recover from breaches.
Implement security policies and procedures and ensure all users are aware of and follow best practices for cybersecurity.
Stay up to date on the latest cyber threats and vulnerabilities.
Collaborate with other departments to raise awareness and promote cybersecurity best practices.

General

All staff must ensure that they familiarise themselves with and adhere to any ICR policies that are relevant to their work and that all personal and sensitive personal data is treated with the utmost confidentiality and in line with the General Data Protection Regulations
Any other duties that are consistent with the nature and grade of the post that may be required.
To work in accordance with the ICR's Values.
To promote a safe, healthy and fair environment for people to work, where bullying and harassment will not be tolerated.
This job description is a reflection of the present position and is subject to review and alteration in detail and emphasis in the light of future changes or development.

Cyber-Security Engineer
Candidate Information

Person specification

Education and Knowledge

A-Levels in Maths & English or equivalent experience in a similar role.	Essential
Industry certifications: Security+, CISSP, CCNA Security, CEH, etc.	Desirable

SFIA Skills

The tables below list the essential SFIA skills, at the relevant level, needed for the position.

Category	Skill	Required Level
Strategy and architecture	Risk management	3
	Information security	3
	Information assurance	3
	Continuity management	3
Development and implementation	Systems design	3
	Programming/software development	2
	Testing	2
Delivery and operation	Capacity management	4
	Application support	3
	Asset management	3
	Change control	3
	Configuration management	3
	Digital forensics	3
	Incident management	3
	IT infrastructure	3
	Network support	3
	Problem management	3
	Release and deployment	3
	Security operations	3
	Vulnerability assessment	3
	Service level management	2
	Systems installation and removal	2
Relationships and engagement	Customer service support	3

Cyber-Security Engineer
Candidate Information

SFIA Supplementary documents

The table below lists the supplementary documents provided. These explain the SFIA framework for those unfamiliar with it, and provide a detailed breakdown of each skill listed above and its importance for the role and how it will be used.

Document	Function
SFIA 8 Summary Chart	Provides a summary chart of the SFIA professional skills and a summary of the generic attributes.
SFIA 8 The framework reference	Provides the full description of the SFIA levels of responsibility, the generic attributes that define the SFIA levels, the behavioural factors, knowledge statements and all the SFIA professional skills.
SFIA 8 skills and responsibilities spreadsheet	Provides the content of the SFIA levels of responsibility, the generic attributes and the professional skills.

These documents can be downloaded here:

SFIA 8 Summary Chart

SFIA 8 Skills and Responsibilities Spreadsheet

SFIA 8 Framework Reference

Cyber-Security Engineer
Candidate Information

Experience

Experience with security tools and technologies, including familiarity with firewalls, intrusion detection/prevention systems (IDS/IPS), vulnerability scanners, security information and event management (SIEM) systems, and endpoint security solutions.	Essential
Firsthand experience in security practices, vulnerability assessments, incident response activities, and security audits.	Essential
Strong understanding of security principles and frameworks: This encompasses knowledge of concepts like risk management, access control, cryptography, and security best practices like those outlined in frameworks like NIST Cybersecurity Framework or CIS Controls.	Essential
Strong understanding of security best practices and frameworks, such as NIST Cybersecurity Framework, CIS Controls, and SOC 2.	Essential
Communication and collaboration skills.	Essential

Cyber-Security Engineer
Candidate Information

Benefits

We offer a fantastic working environment, great opportunities for career development and the chance to make a real difference to defeat cancer. We aim to recruit and develop the best – the most outstanding scientists and clinicians, and the most talented professional and administrative staff.

The annual leave entitlement for full time employees is 28 days per annum on joining. This will increase by a further day after 2 years' and 5 years' service. All staff receive an additional three days at Christmas.

Staff membership to the Universities Superannuation Scheme (USS) is available. The USS is a defined benefit scheme and provides a highly competitive pension scheme with robust benefits. The rate of contributions is determined by USS and details of the costs and benefits of this scheme can be found on their website. If staff are transferring from the NHS, they can opt to remain members of the NHS Pension Scheme.

We offer a range of family friendly benefits such as flexible working, a parents' group, and a maternity mentoring scheme. Other great benefits include interest free loans for discounted season tickets for travel and bicycle purchases, access to the NHS discounts website, a free and confidential Employee Assistance Programme which offers a range of well-being, financial and legal advice services, two staff restaurants, and access to a gym and sporting facilities at our Sutton site.

Further information

You may contact Recruitment for further information by emailing mike.roberts@icr.ac.uk. This job description is a reflection of the current position and is subject to review and alteration in detail and emphasis in the light of future changes or development.