

## Cloud Security Engineer (AWS)

Department:	<b>Health Informatics</b>
Salary:	£59,675 - £69,164
Hours of work:	Full time or 0.8FTE. Flexible working hours/ options compatible with the role can be discussed.
Base:	Cambridge. We offer flexible working arrangements. Our staff combine on-site and remote working, enabling us to come together when it matters most and promote a healthy work-life balance.
Reports to:	Principal Bioinformatic Infrastructure Engineer
Closing date for applications:	Wednesday 10 July 2024, 08:30am
Date of Interview:	Monday 22 July 2024, in person (Cambridge)

### About Health Innovation East

Health Innovation East helps the best innovations in health and care reach the people, places and problems where they bring most benefit.

We are a team of clinicians, data scientists, life sciences industry experts and skilled programme leaders passionate about helping the best innovations in health and care reach the people, places and problems where they bring most benefit. Whether working with global companies, pioneering start-ups, leading universities or regional health providers, we never lose sight of the patients and communities we serve.

As the regional innovation arm of the NHS our collective skill set is valued by the NHS and industry to implement the advances being made across health and care.

<https://healthinnovationeast.co.uk/>

### Our values and commitment to equity, diversity and inclusion

Health Innovation East is fully committed to being an inclusive employer, affording equity of opportunity and welcoming applicants from broad and diverse backgrounds.

Staff at Health Innovation East have come together to co-produce our values and expected behaviours. Our values focus on providing trusted expertise, being inclusive, kind and collaborative in all our working relationships and implementing innovations that truly matter to our communities and partners.

### What are we looking for?

We are looking for colleagues who share not only our values but also our enthusiasm and commitment to making a difference for our communities. We are united by being

dynamic, curious, creative and adaptable. We appreciate the value of evidence, enjoy trying new and different approaches to solving problems, and are comfortable with ambiguity, often-changing plans and unanticipated challenges.

## **Job summary and purpose**

As a Cloud Security Engineer, you will work closely with the wider Health Informatics function to design and implement secure environments for health data research on AWS. You will work within a multidisciplinary Agile team focusing on implementing DevSecOps throughout the development lifecycle of projects. This will include automating security monitoring and reporting (secret scanning, application/container scanning etc.) and introducing or enhancing security practices (e.g. vulnerability management and threat modelling) to new and existing projects. This role is charged with actively seeking out, designing, prioritising, implementing and improving the security posture of all layers of the stack on an ongoing basis. Additionally, maintenance and improvement of security scanning and automation pipelines to ensure tooling can be consumed by the wider team as part of ongoing development activities. The post holder will act as both a subject matter expert and hands-on engineer in cloud security, increasing cyber security awareness within the team by sharing knowledge on threats and vulnerabilities, identifying and implementing proportionate security controls.

A significant portion of this role will be supporting the [East of England Secure Data Environment](#) (SDE). Part of an interoperable NHS Research Secure Data Environment network, giving approved researchers secure access to de-identified NHS healthcare data, for approved projects.

## **KEY RESPONSIBILITIES**

- Work as an integral member of the cloud platform team to plan, prioritise recommend and implement security requirements as part of the secure software development lifecycle (SSDLC).
- Recommending and implementing security best practices for cloud platforms and automating compliance with cloud security baselines (e.g. CIS Benchmarks).
- Implementation of automated security tooling (e.g. within a Continuous Integration (CI) pipeline) to validate security requirements and identify potential issues.
- Reviewing the outputs from security tools and security practices. You will filter and prioritise these into security stories that can be understood and actioned by the delivery teams.
- Verifying the implementation of security principles, architectural patterns, and requirements.
- Driving the adoption of cyber security practices (e.g. vulnerability management, threat modelling etc.) within Agile delivery teams.
- Supporting wider cloud platform design and development activities.

## **Corporate and personal responsibilities**

- Promote equal opportunities and affirm that staff, colleagues, patients, and others who encounter Health Innovation East are afforded equality of access, experience and outcomes.
- Observe Health Innovation East’s equity, diversity and inclusion pledges in every aspect of your work, avoiding any behaviour which discriminates against colleagues, potential employees, patients, or partners on any grounds.
- Uphold and promote the organisation’s values.
- Work flexibly and collaboratively with others to achieve the organisation’s goals and support its values.
- Support the organisation in creating an environment that values risk management and promotes the highest standards of health and safety for Health Innovation East’s employees, supported by policies and procedures as appropriate.
- Ensure up to date knowledge is maintained and comply with current data protection laws and company data protection and confidentiality policies and procedures.
- Ensure that we only operate within our remit of not offering clinical advice.
- Adhere to all company policies and procedures and any applicable legislation.

### Person specification

<b>Competence</b>	<b>Essential requirements</b>	<b>Desirable requirements</b>
Qualifications and training	AWS Cloud Practitioner certification (or higher)	Industry recognised qualification in Cyber Security
Knowledge	Awareness of modern cryptography and its application for encryption in-transit, encryption at-rest, hashing and digital signatures	
Skills	<p>Excellent spoken and written communication</p> <p>Able to convey security issues to technical and non-technical people.</p> <p>Confident working in a collaborative team.</p> <p>Comfortable prioritising and managing workload</p> <p>Experience working with agile software development methodologies (e.g. Scrum or Kanban).</p>	<p>AWS Security Specialty Certification.</p> <p>Awareness of security practices such as threat modelling and penetration testing.</p> <p>Awareness of integrating application security tools (e.g. static analysis, dynamic analysis etc.) into the SSDLC.</p> <p>Participation in the cyber security community (e.g. OWASP, HackTheBox, CTFs etc.).</p>

Experience	<p>Demonstrable experience git tooling, branching, tagging and release methods.</p> <p>Demonstrable experience of production grade Python and Linux shell scripting.</p> <p>Demonstrable experience of Infrastructure as Code development (Terraform, Ansible, ideally python-CDK).</p> <p>Experience of AWS Cloud platform and AWS security best practices and use of AWS CLI &amp; SDKs.</p> <p>Evidence of direct experience working with web application security defence toolkits (e.g. OWASP Top 10).</p> <p>Experience of vulnerability management and application security testing</p>	
------------	--	--

**Right to work in the UK: Applicants must be able to provide evidence of their right to work in the UK at the point of interview.**

The role holder will sometimes be required to be flexible with their hours of work for the team to collectively meet certain deadlines.

Occasional travel both within the region and nationally is required.

### **Personal development responsibilities**

- Understanding and awareness of own personal development needs
- Maintenance of a compliant professional portfolio where required.

### **Key relationships**

*Internal* - all Health Innovation East employees will be expected to form key relationships within the organisation relevant to the role.

*External* - in addition, the successful appointee will need to develop and build relationships with external colleagues as relevant to the role. These may include, but are not limited to, relationships with colleagues within partner organisations such as:

- Industry partners including SMEs and large corporates within the health arena.
- Academic partners in Higher Education Institutes and Tech Transfer Offices.
- Funding/investment organisations.
- Applied Research Collaboration (ARC) East of England colleagues.
- NHS Trusts and NHS Foundation Trusts.
- Local Government.

- Integrated Care System and Integrated Care Boards.
- Third Sector Organisations.
- Patient Advisory Groups/Services.

## **Benefits of working at Health Innovation East**

As part of the benefits package, Health Innovation East's employees are entitled to 27 days of annual leave plus bank holidays (pro rata for less than whole-time equivalent) and are offered a company pension (employer contribution up to 10% of annual salary), life insurance (on completion of a probationary period) as well as a cycle to work scheme. In addition, all employees have unlimited access to the company's well-being programme which is externally provided and fully confidential. Team members on secondment will remain on their employer's terms and conditions.

## **How to apply**

To apply please submit your CV and a covering letter by 08:30am on Wednesday 10 July 2024 to [recruitment@healthinnovationeast.co.uk](mailto:recruitment@healthinnovationeast.co.uk) specifying your motivation for applying and how you meet our person specification. For an informal discussion, please contact [healthinformatics@healthinnovationeast.co.uk](mailto:healthinformatics@healthinnovationeast.co.uk).

*This job description is intended as an outline of the general areas of activity and will be amended in the light of the changing needs of the organisation. This document was developed by Health Innovation East's EDI group and approved by the senior management team on 18/10/2023.*