East Midlands Special Operations Unit

Job Description

Title – Cloud Security Engineer

Post Number:	XS750
Grade /Scale:	PO40 (£46,674 - £50,109) + £10k market supplement Which is subject to review every 12 months
Weekly Hours:	37 hours
Department:	EMSOU Technical Services
Status:	Permanent
Responsible To:	Technical Services – Senior Solutions Architect
Location Work base:	Vicinity of J27 of the M1
Job Role /Purpose:	At EMSOU, cloud computing allows us to modernise the way we think about data and technology to improve our service to the public and our ability to tackle serious and organised crime. As a Cloud Security SME at EMSOU you will ensure the design, build, and operations hosted in cloud platforms adhere to relevant legislation and security policies. You will advise on information security and cyber risks, working alongside projects or initiatives that may have security implications. You will work at the forefront of a unique cloud-first solution that meets current and changing legislative and cybersecurity policies and priorities within regional policing.
Contacts:	EMSOU colleagues, Senior Police Officers, other member of East Midlands forces, external law enforcement agencies, CPS, partnership agencies, suppliers, industry and academia
Equality and Diversity	Actively advance diversity /equality, work towards eliminating discrimination, harassment and victimisation and foster good relations between all groups of people

Person Specification

Knowledge, Skills & Abilities

Essential Criteria *A clear definition of the necessary criteria.*
Knowledge/ Education (including qualifications): Educated to degree level in Management Information Systems, Computer Science, Information Security or other technical/analytical disciplines, or equivalent experience.

In depth knowledge and understanding of security requirements, best practices, and execution in various cloud implementation scenarios: IaaS, PaaS, SaaS

Applicable cloud certifications with one or more leading cloud providers such as AWS, Microsoft Azure or Google Cloud

Work Experience:

Significant experience in providing security oversight with an understanding of hybrid public/private cloud services, Infrastructure as Code, and DevSecOps toolsets.

Experience with planning and managing project efforts to define, implement, upgrade, enhance, and maintain cloud security systems.

Experience with automation, deployment orchestration, and security configuration management with Terraform, Chef, Puppet, YAML, JSON, PowerShell, BASH, Go, or Python

Experience with hardening CI/CD pipelines, containers, container registries, and code repositories, and use of tools such as Jenkins, Git, Azure DevOps, etc.

Knowledge of threat modelling, static/dynamic/interactive code analysis, fuzzing, software composition analysis, secrets management, and related tools.

Experience with compliance and regulatory security requirements such as NCSC principles.

Experience with designing and implementing network security solutions, including firewalls, intrusion detection, encryption, monitoring, vulnerability scanning, and authentication.

Personal / Interpersonal Skills, Aptitudes:

Excellent communication skills (both written and verbal), conveying technical concepts and guidance at a senior level, to both technical and non-technical audiences.

Ability to work in a multi-disciplinary team, including Business Analysts, Solutions Architects, Data Scientists and subject matter experts, or work alone as required to deliver effective solutions.

** Reasonable adjustments will be considered under the Equalities Act 2010.*

Desirable Criteria

Where available, elements that contribute to improved / immediate performance in the job.

Knowledge/ Education (including qualifications):

Knowledge of Police ICT and relevant Cloud Security Policies.

Work Experience:

Experience with the full software or systems development life cycle, including requirements analysis, design, integration, testing, and implementation

Demonstrate experience with Kubernetes (AKS), Docker, and/or Openshift.

An understanding of operational police work, and relevant legislation to be able to provide security advice proactively in the development of cloud solutions to policing problems.

Experience of developing, implementing and reviewing organisational strategy, processes and procedures in respect of data protection, information security and information management

Personal / Interpersonal Skills, Aptitudes:

Advanced documentation and presentation skills, team player with proven collaboration skills, strategic, critical thinking, and problem-solving skills.

The ability to deal professionally with content of an unpleasant and/or disturbing nature and work to strict procedures and protocols in a confidential environment

Evidence an ability to work independently and manage competing demands with minimal supervision.

** Reasonable adjustments will be considered under the Equalities Act 2010.*

Core Responsibilities/ Accountabilities

Operational:

Provide expertise and design decisions as it relates to relevant cloud security principles, legislation and best practice.

Responsible for ensuring our cloud capabilities meet compliance standards.

Oversee and respond to Cloud incidents and security alerts.

Develop relationships across ROCU entities as they work to move to the cloud

Responsible for the development, assessment and authorisation for cloud infrastructures, including risk assessments, system security plans, IT contingency plans, and incident response plans.

Work with other security teams to define and build to processes necessary to protect cloud infrastructure from common threat vectors including ransomware, OWASP vulnerabilities, and security compliance misconfigurations.

Work closely with various team members to refine and enhance the risk strategy for cloud architecture, ensuring business requirements are met and risk mitigation and management is in place.

Provide security consultation and guidance on new cloud products, features, and technology decisions. Ensuring the security of products with a strategic view of interoperable and flexible cloud solutions.

Work with Information Security Officers, system owners, and other IAM colleagues to address audit and regulatory related issues. Ensuring cloud architectures and processes are accreditable.

Management/Leadership:

Actively engage and foster relationships with security champions on business and cloud teams to understand their needs and promote a DevSecOps culture

Technical:

Create security automation for response and remediation of compliance findings and hardening of cloud infrastructure.

Apply your expertise across all IT Security topics as it relates to the cloud, on-premises, and hybrid enterprise technology and the relationship between the architectures.

Assess Cloud Authentication and Access Management Services in a secure federated environment.

Identify service-level requirements for a cloud service provider (CSP), in line with national and local digital and cloud strategies.

Communication:

Regularly liaise with non-technical customers to understand their requirements, providing advice and guidance, helping to embed cloud-computing techniques within regional investigations.

Administration:

Responsible for monitoring and updating of security policies and procedures including System Security Plans.

Maintain records in accordance with national, local, and departmental policy and procedure.

Complete and implement compliance audits and reporting.

Develop and document processes regarding operation incidents, based on technologies, and tools used in those processes to resolve.

General:

Continuous professional development, learning, and keeping up with changes in cloud technology

** Reasonable adjustments will be considered under the Equalities Act 2010.*

Personal Values /Competencies

The competency and values framework sets out nationally recognised behaviours.

The framework has 6 Competencies – each competency can be split into 3 levels to fit around policing and non policing roles see here : Competency and Values framework

We analyse critically
We are innovative and open-minded
We are emotionally aware
We take ownership
We are collaborative
We deliver, support and inspire

All competencies are underpinned by 4 Values that should underpin everything that we do :

Integrity
Impartiality
Transparency
Public Service

Other

Security Check Levels refer to vetting for the specific levels that relate to this job role:

1) Management Vetting (MV)

2) Security Check (SC)