East Midlands Special Operations Unit

Job Description

Cyber Protect Officer

Post Number:	XS592
Grade /Scale:	S01 – £29,793 - £31,725
Weekly Hours:	37
Department:	EMSOU RCCU
Status:	Permanent
Responsible To:	Detective Sergeant/Inspector
Responsible for:	N/A
Job Role /Purpose:	To support EMSOU, the five forces it serves, partners and stakeholders in ensuring a consistent approach in delivering cyber security advice in accordance with the PROTECT strand under the Cyber Crime Control Strategy.
Health and Safety:	To comply with the health and safety policy and its associated procedures and co-operate with your manager and the force to protect your health and safety and that of other people. To comply with the relevant risk assessments for your job role and report accidents, incidents and near misses.
Contacts:	Members of the public, officers and police staff employees of UK law enforcement agencies, cross government sector representatives, employees of the criminal justice system members of the business community, partner agencies and other relevant stakeholders.
Equality and Diversity	Actively advance diversity and 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):

- Knowledge of Information Security, Information Technology, Fraud and Cybercrime, with an understanding of the challenges faced working in the cyber and digital environment, including the current and upcoming threats in the Cyber/Digital arena and the benefits of managing these threats effectively.

- Cyber security certifications or equivalent qualification or work experience.
- A proficient IT user with the ability to quickly adapt to new systems and processes.

Work Experience:

- Experience of working within legal frameworks and policy driven environments, with the ability to understand detailed technical procedures, projects and policies.
- Experience of working in partnership with other individuals, organisations and stakeholders to meet common objectives, with an ability to engage and manage relationships with multi-agency partners or similar public or corporate stakeholder dependencies, based on an ethos of mutual respect, equality and diversity.

Personal / Interpersonal Skills, Aptitudes:

- To be able to receive strategic direction and develop that into specific coordinated operational activity.
- Must have strong interpersonal skills supported by a high standard of communication skills, both verbal and written, including an ability to convey technical matters to a technical and non-technical audience as part of panel membership, presenting and exercising.
- Take ownership for resolving problems, demonstrating courage and resilience in dealing with difficult situations and have the ability to work under pressure, prioritising workloads and working to tight timescales within an ever-changing environment.
- Creative and innovative when developing campaigns, initiatives, materials and resources.
- Ability to work with minimal supervision throughout the East Midlands Region and led on initiatives or projects.
- Ability to continually develop knowledge and understanding of cybercrime by effective use of the intelligence and information assets made available to you, attendance at training, conferences and seminars and providing core and competent membership at the relevant panels and forums.

Other:

- A full UK driving licence is considered essential *.

** Reasonable adjustments will be considered under the Equalities Act 2010. IT equipment will be provided and fuel payments will be paid at policy rate. At interview, candidates will be asked to confirm their willingness to undertake this Basic Driving Assessment, which in turn will enable the use of a police authorised vehicle.*

Desirable Criteria

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

Knowledge/ Education (including qualifications):

- Additional academic or industry standard qualifications in cyber security, computer science or computer forensics.
- Knowledge of relevant legislation such as the Computer Misuse Act as well as those offences associated with the commission of serious organised crime.
- Experience/understanding of complex crime investigation and/or victimology.
- Knowledge of the specific threats posed by cyber criminality including the different varieties of malware, network intrusion attacks and threat vectors.

Work Experience:

- Experience of liaison with the media and dealing with marketing and publicity.
- Experience / understanding of neurodiversity.
- Experience of working in support of any discipline under the 4P strands of the Serious and Organised Crime Strategy.

Personal / Interpersonal Skills, Aptitudes:

- Understands the issues around commercial confidentiality and sensitivity.
- Experience in developing material/resources/processes for large scale campaigns.

Special Skills:

- Have prior experiences or qualifications that encompass the psychology of behaviour change.
- Has previously managed performance in a corporate or public sector environment.

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

Core Responsibilities/ Accountabilities

Operational:

Understand the threat picture by using all information and intelligence resources at your disposal. Sit on and contribute to the relevant situational awareness calls, panels, workshops and forums to advance your knowledge and that of others. Address regional priorities taking into account identified threats nationally, regionally and locally.

Promote; nationally derived materials, activities and campaigns from our national lead agencies and support our primary cybercrime and fraud reporting mechanisms.

Identify and build collaborative partnerships with local industry, trade organisations, cyber security experts, education, voluntary sector, law enforcement, public forums and partner agencies to promote, and benefit from Protect messaging to further develop our collective cyber capabilities, reducing the cyber threat we face as a community.

Provide a proactive and reactive (tasked) networked resilience to emerging or current cybercrime risk and threat. To work within an evidenced based, legal and policy driven framework, to mutually agreed communication strategies as part of an established programme in national, regional and local areas.

Work closely with and support local force cyber officers and staff with events and initiatives, build intelligence and identify opportunities to develop cyber resilience across the region. Gather and submit intelligence in line with national intelligence requirements. Share best practice identified with stakeholders minimising the risk of harm and ensuring that future criminal opportunities are minimised and crime is reduced.

Design, develop and present materials / exercise content at host or guest events for the private, law enforcement and public sectors.

Provide government approved, consistent and detailed Protect advice to individuals, public and private sectors, identify vulnerabilities and influence behaviour to increase their resilience to cyber threats and risks.

Conduct reviews of the effectiveness and performance of our local and regional protect activity and submit to management and national leads, providing the necessary comment and interpretation.

Support cybercrime investigations, engage with reporting persons to prevent repeat victimisation.

Support the East Midlands Cyber Resilience Centre, responding to tasking's and requests for assistance.

Management/Leadership:

No prior management experience is required but leadership skills need to be evidenced. The ability to influence, motivate, and enable others in a team is key to delivering our objectives.

Technical:

The post is technical in nature. It requires an understanding of the threat vectors that enable or provide the opportunity to commit cybercrime. This understanding is key to maintain credibility and the ability to influence others with your work.

You will be afforded the relevant paid support, study time, attendance time and materials to obtain the necessary qualifications to discharge your role. Dependant on performance and necessity there are potential opportunities, subject to funding, to support you in obtaining industry recognised qualifications or further education.

Communication:

To establish and maintain professional relationships with partner agencies to enhance communication and dissemination of information.

Prepare planned events and brief reports when completed identifying key learning from them to improve future endeavours.

Ability to absorb technical information and relay it to a non-technical audience.

Deliver cyber security presentations and exercising to public, private, LEA and voluntary organisations within the region. To empower organisations and individuals to protect themselves and increase their resilience to cyber threats.

Deliver general cyber security advice to victims of cybercrime. To prevent repeat victimisation and sign post them to appropriate resources and materials.

General:

Have flexibility regarding work location and hours to suit operational need and be willing to travel within the East Midlands area and occasionally outside this area to attend training, conferences, meetings and any other necessary travel to effectively discharge the role.

Undertake any other duties commensurate with the role and grade as may reasonably be requested by line management.

The post holder will be expected to be deployed as per operational requirements and this could be anywhere in the region including from partner agency locations.

Suitable bandwidth and security awareness to included asset management and GDPR cognisance to facilitate home working where necessary.

Undertake all assignments in a timely manner, being available to work some evenings and weekends, where specific engagements require.

** 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:

Management Vetting (MV)

Security Check (SC)