JOB DESCRIPTION

Job Title: Regional Cyber Intelligence Development Officer (SEROCU)	**Location:** Whitchurch (Hampshire) moving to near junction 12 of the M4
Job Family: Operational Support	**Role Profile Title:** BB4 Police Staff
Reports To: DS Cyber PURSUE (SEROCU)	**Band level:** 4I
Staff Responsibilities (direct line management of): *Nil*	

a. **OVERALL PURPOSE OF THE ROLE**: Defines the role, put simply, why it exists.

The overall purpose of the role is to: This is an intelligence development role on the specific areas of cybercrime and dark web criminality (Not CSE). The main purpose of the role is;

(a) Identify, collate, research, assess and review information and intelligence on identified individuals and organisations and assist in the preparation and presentation of a variety of intelligence packages and evidential documents for Criminal Proceedings related to cybercrime and dark web criminality.

(b) Develop, evaluate, analyse, report and present in criminal proceedings digital forensic evidence and crypto-currency evidence.

(c) Provide support, assistance and training to other officers and staff within the Region and South East Forces in relation to crypto-currency, cybercrime and dark web tactics, techniques, software available and case studies of investigations.

b. **KEY ACCOUNTABILITY AREAS**: Define the important aspect of the role for which the job holder is responsible for results or outcomes.

The key result areas in the role are as follows:

1. Research and assess intelligence on individuals and organisations linked to serious organised crime. Prepare and present this information in the format required by the relevant customer, e.g. intelligence products, reports, charts and maps for investigative use, summarising clearly, concisely and accurately key research findings. Evaluate the information for its reliability and validity and any consequent impact this may have upon the investigation. Maintain full audit trail for each piece of research to include a good understanding and working knowledge of cyber/dark web & digital forensics software tools and techniques, in order to maximise intelligence and evidential opportunities from a variety of digital devices.

2. Provide analytical function with specialist research using open and closed source techniques such as covert internet investigation to include specialist research and capture of data for intelligence and evidential purposes, from online forums, chat groups, other online social media sites residing in both the internet (open) and dark web (closed) sites. The products produced will be presented in Criminal Proceedings.

3. Develop, evaluate, analyse and produce evidential and intelligence products using specialised software design to investigate crypto-currencies. Identify further lines of investigation or intelligence to support the digital forensic strategies.

4. Identify, secure and seize digital/electronic devices/ sources to assist with investigations as per Best Practice (digital) guidance. Capture, preserve electronic evidence from seized digital media in a laboratory/or on-scene, using bespoke software and hardware, in line with ISO17025 & ISO17020 procedures. Evaluate and a report on the electronic evidence produced using appropriate processes, methodologies and tools to a high standard for Criminal Proceedings.

5. Support live operational activity with real time research and evaluation of information. Manage the data that is provided to the Operations room to ensure that it is up to date and accurate. Deploy with the operational team, during live operations, providing technical support (research and live data acquisitions from a range of digital devices).

6. Monitor and maintain intelligence sources used to deliver other intelligence products. Write and submit applications for telecoms data under RIPA legislation, and manage the resulting product and research content in line with SIO/Investigations telecoms strategy in order to achieve investigative aims.
7. Identify emerging trends within the arenas of organised cyber-crime and where appropriate risk assess the threat. Work closely with intelligence staff, investigators, Digital Forensic Analysts to update and develop intelligence products, and identify intelligence opportunities, links and crossovers between priority and other high risk activity.
8. Support, train and advise other SEROCU investigators, Regional and Force Intelligence Development Officers and Analysts in relation to crypto-currency and dark web investigation to develop the digital skills of other staff in order to improve the organisational response to digital investigations specifically in the area of Cyber Crime and dark web.
9. Recommend further action against those individuals deemed to be linked to cyber-crime and dark web criminality, identifying opportunities for intervention by appropriate resources. The data produced will be actioned by the SEROCU Cyber Pursue, Prevent and Protect and Dark Web units to ensure that the objectives laid out in the National Cyber Security Strategy 2016-2021 are met with the key objectives being to Defend and Deter Cyber Criminality.
10. Participate in cyber-crime and dark web meetings at both Force, Regional and National level. Provide briefings at these as and when required. To ensure that different levels of the organisations are fully informed of the threat, harm and risk of cyber-crime and dark web in the South East. That operational cyber and dark web learning and best practice is shared within the cyber community.

c. **DIMENSIONS**: Include matters as key result areas that make the greatest demands on the role holder, seasonal pressures, items processed, the number of customers and/or level of authority to make financial decisions or commit other resources.

Further Comments:
SEROCU Cyber IDOs – Attend meetings and give presentations as appropriate to the purpose of the role. This will include meetings outside the county or away from police premises, and/or with colleagues from other departments or agencies. - Liaise on a region wide basis with other Forces/departments/agencies (NCA, UKBA, HMRC, Interpol, Europol, Council, DWP etc) in the collection and dissemination of information. - Help improve the quality of Region wide police held data through resolving (or referring to the appropriate person to remedy) data errors identified during the course of research. - Evidence research work as necessary (ANPR, telecoms) and prepare in appropriate format for presentation at court.
Will be working in a fast moving and changing environment. Must be willing to travel and work in other parts of the UK at short notice. Responsible for interrogating all relevant available police databases and external sources. Liaise with police officers and police staff, and partner agencies regionally and nationally to gather and develop intelligence. Requirement to travel regionally, nationally and on occasion internationally to achieve this.

d. **CHARACTERISTICS OF THE ROLE**

Expertise: Concerned with the level of administrative, professional and/or technical expertise (knowledge and skills) needed to perform the role effectively; may be acquired through experience, specialised training, and/or professional or specialist education and training.

The knowledge or skills required in the role are as follows (essential or desirable):	***E/D***
1. Professional experience with broad knowledge and understanding of working within an intelligence environment. With a good knowledge of the intelligence process and cycle, including NIM.	E

2. Proven experience in collating and assessing information and making concise and accurate recommendations based on assessments.	E
3. Excellent communication skills, written and oral, with ability to negotiate and deliver presentations.	E
4. Excellent time management with proven experience of working within a team and also able to work effectively on own initiative.	E
6. Previous experience of working in a security conscious environment with secret and confidential material. Understanding of handling and movement of such documents and able to recognise and deal appropriately with sensitive information.	E
7. Proven high standard of IT skills with accurate keyboard and inputting skills and the ability and commitment to learn new systems in a short time period.**	E
8. Able to demonstrate an understanding of relevant legislation e.g. GDPR, MOPI, CPIA & HRA.	E
9. Must have the capability to travel to different locations across the region and nationally and undertake all assignments in a timely manner. A full UK driving licence is essential. *	E
10. Academic or industry recognised qualification in computing/IT or relevant experience. This can include knowledge and experience of using relevant cyber or digital forensics software and hardware.	D
11. Proven experience of using specific 'blockchain' (cryptocurrency) analytical software (Chainalysis).	D
12. Completed Main Cyber Crime Training course or equivalent.	D
13. Proven experience of using software such as i2, force intelligence systems, ANPR, PNC, PND.	D

Additional Comments;

Training will be provided in the following;

1. CSI Tech Cryptocurrency
2. Specific software training for using Chainalysis for cryptocurrency investigations.
3. Specific software training for using specialist software for intelligence gathering and research of the dark web and cybercrime forums.
4. A range of cyber and dark web training courses provided by National partner QA.

At interview candidates will be asked to confirm their willingness to:
*Undergo Driving Training to enable the use of a police authorised vehicle
**At interview candidates will also be asked to confirm their willingness to train towards achievement of appropriate courses e.g. Covert Internet Investigations.

Role holders will be required to provide fingerprints and DNA for elimination purposes in order to perform the position offered. DNA will be profiled and held on the Contamination Elimination Database (CED) and will be removed 12 months after termination of service. Fingerprints will be held on the Fingerprint Police Elimination Database PEDb and are removed at the termination of service.