Salary: Up to 75,000 depending on skills and experience
Contract type: 2-year fixed term appointment
Grade: MoJ Band Ac
Number of open roles: 1
Location: London
Hours: 37 hours/week (42 hours incl. lunch)
Working pattern: flexible working, full time, part time
Closing date for applications: rolling campaign, please apply asap
Interviews: ongoing
Interview location: 102 Petty France, London SW1H

Introduction

These are exciting times at MOJ Digital and Technology. We have a clear vision - to develop a digitally-enabled justice system that works more simply for users - and we're looking for talented people to help us achieve it. We're making things better by building adaptable, effective services and making systems that are simple to use for staff and citizens. It can be challenging but it's also important and rewarding.

As well as doing great work, we're creating a place that's great to do work in. We offer tip-top kit, brilliant training opportunities and support from expert colleagues. On top of that, you'll find flexible working, an inclusive culture and a place where your opinion is valued.

The team

The Head of SecOps role is critical to the protection of the Ministry of Justice's technology systems and services, and the vital information they contain and process.

Our team provide excellent operational security support to all of the technology operational zones across the Ministry of Justice (an operational zone being a self-contained service area such as our Digital platforms, or enterprise technology in a particular agency). Our aim is to provide constant vigilance against attacks, respond when they do occur, and continuously seek out ways to improve the security of our systems.

You'll oversee all security monitoring across our estate, undertaking incident analysis in conjunction with operational teams and their suppliers. Your team will also support operational zones / live service teams in cyber security incident management, providing expert cyber security input, analysis, forensic support, and liaison with other organisations (such as the National Cyber Security Centre) and security researchers, etc.

You'll enable your team to build out new capabilities and leverage advanced threat data sources through building a threat hunting capability and determining how threat intelligence should both be used but also shared.

Working with cyber security risk advisors, you'll ensure that senior decision makers are kept abreast of the latest cyber security threats to the MoJ and its systems and people, and understand where our real weaknesses are. You'll also work closely with our cyber security consultants to devise effective operational security mechanisms as new systems are deployed, ensuring they can be kept secure through-life.

Your team will also be entrusted with some of our most sensitive work - specifically the control of IT investigations into insider misuse of our systems.

Our team is based in different locations around the UK..

You'll

- Lead a team of security analysts and security operation specialists as they defend the MoJ's digital and technology solutions against security threats.
- Work closely with operational zone teams, and service suppliers, ensure threats and vulnerabilities are remediated effectively, and acting as incident command for security matters.
- Communicate of team findings to stakeholders in a clear and actionable fashion, focussing on real-world impact and with pragmatic options for resolution.
- Monitor Security across all of the department's technology estate to seek out areas of weakness, potential problems, and active threats.
- Develop and implement our security monitoring strategy, enabling us to more effectively monitoring on-prem and cloud-based services, across a variety of technologies and systems; working with architects and project managers in these programs to define security monitoring capabilities and product managing the security monitoring capability.
- Set up and operationalising a threat hunting capability to proactively understand the tools, techniques and practices of threat actors and discover any indication of malicious activity across the department's technology estates.
- Contribute to threat sharing groups and programmes across government and industry.
- Ensure IT investigations are performed effectively, lawfully, and appropriately, using the skills of the whole cyber security team as required. Communicate findings appropriately and effectively, and working with outside agencies (such as law enforcement) when necessary.
- Develop and implement tools and techniques, using practices such as SecDevOps, to automate as much of the team's work as possible, providing continuous assurance that systems are protected against common problems, and enabling your team to focus on more MoJ-specific threats.
- Develop and mentor team members to improve their skills and capabilities, along with wider knowledge transfer to other security and non-security teams to help build a culture of cyber security across the Ministry of Justice.

You'll have

- Strong knowledge of security monitoring approaches, techniques and widely-used products. Experience of developing and implementing cyber security monitoring strategies, leading a team of security analysts as they use monitoring and other investigative techniques to seek out security threats, and improve an organisation's security posture.
- Experience of running and developing a team of technical specialists, ideally in the field of security operations. You will be familiar with coaching, mentoring, and supporting people at different stages of their career, managing a portfolio of work - much of it urgent - and providing effective delegation and leadership to a team.
- Experience of IT investigations, e-Discovery tasks, digital forensics, etc. Knowledge of appropriate processes and procedures required to effectively collect, interrogate and preserve information from a wide range of enterprise IT sources.
- Experience with threat and vulnerability management, and other security operations processes and techniques (such as identity management, cryptography, patch

management etc). Good knowledge of threat to widely used digital and technology systems, including on-prem and cloud-based solutions.
- Enabling and informing risk based decisions - Works with risk advisors to advise and give feedback. Advise on risk impact. Propose realistic and pragmatic mitigations that address these problems, and work with the product / project team to implement these effectively into their work.

Desirable:

- Understanding security implications of transformation - Can interpret and apply understanding of policy and process, business architecture, and legal and political implications in order to assist the development of technical solutions or controls.
- Research and development experience, building and automating common security operation team processes and activities.
- Knowledge of security architecture, in particular for modern digital services, including how they are developed and operated at scale.

In the Civil Service, we use Success Profiles, a flexible framework, to assess candidates against a range of elements using a variety of selection methods, therefore giving you the opportunity to demonstrate the various elements required to be successful in the role.

At the interview we will be assessing your technical/specialist skills and experience, testing your ability through relevant assessments and asking you questions to around the behaviours we require to be successful in this role. The **behaviours** we assess are:

- Leadership
- Communicating and influencing
- Making effective decisions
- Delivering at pace
- Managing a quality service
- Working together
- Developing self and others
- Seeing the big picture
- Changing and improving
- Managing a quality service

Throughout the process we will assess your technical specialist skills and experience on the above requirements.

We are an equal opportunity employer and value diversity at our company. We do not discriminate on the basis of race, religion, colour, national origin, gender, sexual orientation, age, marital status or disability status.

Selection process details

Candidates must submit:

- a current and relevant CV;
- a Cover letter (1 page max) setting out why you are interested in the role and how you meet the essential skills and experience required.

The job advert lists the essential, specialist skills and experience as well as key Civil Service competencies required for the role.

At the CV review/sift stage we will use the technical/specialist skills and experience to determine your suitability for the role. At the interview we ask you questions based on the specialist/technical skills and experience as well as behaviours outlined.

At the Interview we will ask open-ended questions to which they are seeking answers/evidence of essential, previous skills, experience and behaviours in order to guide their hiring decision.
Note: due to the volume of applications we receive we are unable to provide feedback after the CV review (sift) stage.

Salary and working arrangements

If successful, the salary we offer you will be within the advertised range and will depend on the skills and experience you demonstrate at the interview. Therefore in your cover letter it would be helpful to the hiring teams if you can indicate your salary expectations and if possible your notice period.

Benefits:

- Flexible working options - working from home or remotely, working part-time, job sharing, or working compressed hours, we have people doing it and are happy to discuss further
- Lots of training and development opportunities
- A civil service pension with an average employer contribution of 22%
- 25 days annual leave (plus bank holidays), and an extra day off for the Queen's birthday.
- Great maternity, adoption, and shared parental leave, with up to 26 weeks leave at full pay, 13 weeks with partial pay, and 13 weeks further leave. And maternity support/paternity leave at full pay for 2 weeks, too!
- Bike loans and secure bike parking (subject to availability and location)
- Season ticket loans, childcare vouchers, and eye-care vouchers.

Things you need to know

Security and Immigration checks

Successful candidates must pass a disclosure and barring security check.
Successful candidates must meet the security requirements before they can be appointed. The level of security needed is security check.

Candidates will be subject to UK immigration requirements as well as Civil Service nationality rules. If you're applying for a role requiring security clearance please be aware that foreign or dual nationality is not an automatic bar. However certain posts may have restrictions which could affect those who do not have sole British nationality or who have personal connections with certain countries outside the UK.

Nationality requirements

Open to UK, Commonwealth and European Economic Area (EEA) and certain non EEA nationals. Further information on whether you are able to apply is available here.

Eligibility
Candidates in their probationary period are not eligible to apply for vacancies within this department.

Working for the Civil Service

The Civil Service Code sets out the standards of behaviour expected of civil servants.
We recruit by merit on the basis of fair and open competition, as outlined in the Civil Service Commission's recruitment principles.

The Civil Service embraces diversity and promotes equality of opportunity. There is a guaranteed interview scheme (GIS) for candidates with disabilities who meet the minimum selection criteria.

Contact point for applicants- for further information regarding this role please contact MoJ D&T Recruitment.

Further information

All Civil Servants will adhere to the 'Civil Service code', which outlines the Civil Service's core values, and the standards of behaviour expected of all civil servants in upholding these values.

Note for current Civil Servants: If successful, the salary offered would normally be determined by applying the MoJ salary progression rules. If the appointment is on level transfer your substantive salary (excluding any allowances) will remain unchanged, unless it exceeds the maximum stated within the MoJ pay band, and unless your current salary is below the relevant MoJ grade minimum. If the appointment is on temporary or substantive promotion the salary will be increased by the appropriate promotion percentage or moved to the minimum of the relevant MoJ grade minimum, whichever is the greater.

Note for non Civil servant applicants: This post is open to UK Nationals, Commonwealth Citizens, EEA Nationals of other member states and certain non-EEA family members. There must be no employment restrictions or time limit on your permitted stay in the UK. You should normally have been resident in the United Kingdom for at least 3 years and in some cases 5 or even 10 years preceding your application due to the requirement to have a checkable history for security vetting purposes. If you answer 'No' to the questions regarding nationality then it is unlikely your application will be pursued. If you are unsure as to your eligibility on any of these points, please contact the recruitment team for clarification or advice.