Job Description: Ethical Hacker

Salary: £49,700 - £64,500

Any offer made above the base grade will be made up with a non-pensionable specialist pay allowance based on capability.

Contract type: Permanent

Grade: Grade 7

Hours: 37 per week (excluding lunch)

Business area: CO - Chief Digital and Information Office (CDIO) - Security Pillar - G7 Ethical Hacker

Working pattern: flexible working, full-time, part-time, job share

Location: London, Manchester, Bristol, Glasgow, York, Birmingham, Norwich, Newcastle

Number of posts: 1

Who we are

The Cabinet Office supports the Prime Minister and ensures the effective running of government. It is also the corporate headquarters for government, in partnership with HM Treasury, and takes the lead in certain critical policy areas.

We are the Cabinet Office's cyber security team, and our mission is to secure the department (including it's arms length bodies such as the Government Digital Service) against cyber threats. We protect our nationwide internal IT infrastructure, and high-profile citizen-facing digital services such as GOV.UK, Notify, and Register to Vote.

Find out more about the work Cabinet Office and GDS get involved in at the GDS blog, Inside GOV.UK blog and Technology in Government blog.

What you'll do

The Ethical Hacking team delivers penetration testing and red teaming capabilities for the Cabinet Office and GDS, and is responsible for simulating offensive cyber tools and techniques to identify and drive security improvements.

As a member of this team, you'll work with others to build and deliver these core capabilities. The platforms you'll help secure include our nationwide internal IT infrastructure and high-profile citizen-facing digital services such as GOV.UK and Register to Vote.

As an Ethical Hacker, you will:

- deliver web application and infrastructure penetration tests

- deliver endpoint build reviews, AWS/Azure reviews, infrastructure as code reviews (e.g. Terraform), and secure code reviews
- work alongside Security Analysts on “purple team” exercises to improve threat detection and incident response capabilities
- build and improve the processes and training within the Ethical Hacking team
- implement automated and continuous penetration testing pipelines
- schedule and scope penetration tests for the team, working directly with the developers and product managers
- contribute to the development of cyber security tooling and solutions to improve the efficiency and effectiveness of the team
- help us to continually improve and automate reporting processes and data collection

Who you are

It’s essential that you have:

- experience delivering security testing of web based services, cloud services and underlying infrastructure, looking for sophisticated attack vectors and recommending mitigations
- recognised certifications (e.g., CRT, OSCP) in the field of penetration testing
- good analytical skills to understand the implications of security threats
- good verbal and written communication skills to ensure business and technical risks as clearly communicated
- experience using penetration testing tools such as BurpSuite, Nmap and Metasploit
- experience developing and/or reviewing source code
- experience reviewing cloud infrastructure configurations and infrastructure as code

It is also desirable that you have:

- experience working within a software development team and environments with frequent change
- experience of working with PCI environments
- experience of working in an Agile environment as part of a multidisciplinary team

Civil Service Competencies

In the Civil Service we use our Competency Framework to outline expected behaviours and we will use these as part of our wider assessment during the interview process.

For this role, the following competencies are the most relevant:

- changing and improving
- communicating and influencing
- making effective decisions
- delivering at pace