Job Description

Job descriptions should be no more than four pages when complete.

Where you are amending an existing job description you must make the changes using Track Changes.

Once you have decided what role you require within your team / department structure, you need to articulate this into a job description. This needs to be a specific description of the role, including the responsibilities that the job-holder will carry out as well as what qualifications and skills they will require to fulfil the role. Please note: job description should not be based on an individual but on the role the business requires.

Job descriptions must be accurate and created before the recruitment process.

A Post Details

Job Title: Senior Cyber Security Engineer	Grade: B004
Department: Technology	Division: A
Reports to: Head of Cyber Security	Contract Type: Select Contract Type
Level of Vetting:**Management Vetting**	Numbers in Post: 3

B Purpose of the Post

The Senior Cyber Security Engineer is responsible for ensuring the confidentiality, integrity and availability of the Forces IT estate. Working within the Cyber Security team and reporting to the Head of Cyber Security, the postholder will play a critical role in protecting BTP's infrastructure, systems and data from malicious cyber threats. They will also act as the subject matter expert as we transform to new technologies and working practices, developing BTP's cyber offering and leading on the creation and implementation of the core NIST cyber security pillars: (Identify, Protect, Detect, Respond & Recover).

The role will deliver operational cyber security analysis and response, support to other teams within Technology, assist project teams via provision of security requirements, design and implementation validation.

The postholder will also offer specialist advice and guidance to stakeholders as well as upskilling team members and assist in maturing the existing cyber security function.

BTP operate a flexible working policy, including the ability to work from home. The role will be based at our Force Head Quarters (FHQ) in Camden and will require at least 2 days in the office.

Travel to sites may be required and flexibility in working hours to manage/resolve high priority incidents.

C Dimensions of the Post

Financial – Direct or Non-Direct Direct: No Direct Financial Responsibility. Non-direct: No Staff Responsibilities – Direct or Non-Direct Direct: None. Any Other Statistical Data: The role will involve being on call and part of an on-call rotation for the provision of support services during outage, compromise or incident response / recovery

D Principal Accountabilities

- Support the Head of Cyber Security and Technology department by being the senior security technical specialist, and support effective governance, architecture and policing processes, through effective policy, education and regular awareness communication to the Force.
- Ensure the 5 NIST core pillars (Identify, Protect, Detect, Respond Recover) of our Cyber Security strategy are embedded, matured and aligned to BTP's agreed risk position
- Ownership of the Security Infrastructure with hands-on technical design, implementation and management of core security platforms, and jointly leading on cyber security related projects with the Cyber Security & Compliance Manager
- Be the product owner for security solutions, ensuring they are implemented effectively in conjunction with Technology Infrastructure, Networks, End User Computing (EUC) teams and relevant 3rd parties
- Lead in the analysis, mitigation and resolution of security incidents and threats
- Define and coordinate cyber incident response testing to assess capabilities and breach preparedness
- Perform internal threat hunting to detect historic or active malicious/unauthorised activity
- Perform reviews of operational processes to ensure policies are effectively implemented and followed
- Support the delivery of new projects, ensuring that they are risk assessed, security controls are identified and implemented successfully to protect the confidentiality, integrity and availability (CIA) before going live, and that solutions meet the relevant information and cyber security principles set by BTP
- Perform threat modelling and impact assessments to scope and pre-empt risk whilst offering solutions in the form of playbooks and disaster recovery plans where required
- Identify security design gaps in existing and proposed architectures and recommend changes or enhancements
- Provide security inputs into technical working groups
- Identify and implement opportunities for innovation and continuous improvement in the delivery of appropriate cyber security solutions
- Act as the trusted security advisor and champion a security-first approach across Technology operational and project teams within BTP

E Decision Making

- Incident management priorities related to Cyber Security
- Proactive Cyber Security health-checks and infrastructure/services security monitoring
- Access management controls and best practices in place to manage the access of BTP
- employees
- Specific recommendations affecting Cyber Security projects (SOC, SIEM, Accreditations,
- Threat Intelligence)
- Key input to the Change Authority Board (CAB) and associated Cyber Security planned
- works.
- Develop and implement a strong risk management regime, ensuring Cyber Security
- Controls are adequately applied to all relevant infrastructure and services

F Contact with Others

Internal:

- Contact with domains across the Technology function (Infrastructure, Applications, Service
- Desk)
- Engagement with management across the Technology organisation
- Engagement with wider BTP functions including Digital Policing, Information Management, CCTV, SSU,

CCU

G Essential Criteria

- Excellent all-round technical understanding and demonstrable problem-solving capability
- Strong demonstrable hands-on experience implementing cyber security solutions
- Experience in at least three of; End User Device Security, Server and Network Security, Cloud Infrastructure Security, Application Development Security
- Extensive experience of Microsoft Windows platforms, including SQL Server and Azure cloud platform
- Strong Identity management experience
- Good understanding of application and information security policies, principles, and controls
- Collaborative approach to identifying and implementing improvements
- Flexibility to operate in a small team and communicate with a wide range of stakeholders
- Excellent written and oral communication skills in English

Qualifications and Training:

- Educated to degree level or equivalent experience
- Industry certification such as CISSP, CCSP, Azure Security, Architecture, Security+, Togaf, SABSA
- Experience and understanding of ISO27001/ISO27002 and GDPR

Experience:

- Strong experience in one or more of the following areas: cloud security (security controls, assessments, privacy and regulatory risks, security frameworks), Security Operations, Infrastructure Security, Application Security and DevSecOps
- Experience of managing security in Microsoft Azure, Azure AD, MS O365, cloud, networking, monitoring and use of MS Sentinel and Defender
- Experience of Identity Access Management systems e.g. SailPoint
- Significant hands-on experience in Cyber Security disciplines including access management, incident management and engineering of security platforms (IDS/IPS, SIEM, EDR solutions, PKI, vulnerability management, Microsoft Security toolsets etc.
- Extensive implementation experience of a wide range of security products such as access audit tools, IDS, IPS, DLP, End Point security, encryption, DDOS protection, etc.
- Strong knowledge of cyber threats, penetration testing, and vulnerability assessments
- Extensive understanding of networks, encryption, security policy and access controls
- Hands-on experience of selecting, deploying and maintaining a variety of security solutions
- Experience of supervising and supporting third party cyber security providers
- Demonstrable experience driving new processes and best practices across teams

Skills:

- Strong analytical, reasoning, and organisational skills are essential
- Strong verbal and written communications skills are essential
- Ability to prioritise and handle multiple tasks simultaneously
- Ability to work in collaboration with colleagues across technology around incident and problem management

- Excellent communication and collaboration skills to influence and support a diverse community
- Proven track record of cyber technical security experience and to be seen as a subject matter expert for BTP
- Ability to demonstrate an exceptional analytical skill set and knowledge of current and evolving Cyber threats

Knowledge:

- Knowledge and experience of security and risk management methodologies, frameworks and standards, such the NIST Cyber Security Framework (CSF), ISO27001, ISO31000, ITIL, OWASP, and the MITRE Att&ck framework
- Knowledge of threat modelling methodologies, e.g., STRIDE, DREAD etc.
- Strong knowledge and ability to understand technology across multiple domains with broad technical landscape awareness, especially Microsoft Azure, Office 365 and Dynamics with additional technologies such as Sentinel an advantage
- Knowledge in Security Architecture (On-Prem and Cloud)
- Experience with Cloud infrastructure (Azure)
- Significant industry knowledge of cyber and information security standards and best practices
- Working knowledge of host hardening techniques including Windows/UNIX/Linux
- Detailed understanding of tools and techniques used by ethical hackers including vulnerability testing tools and methodologies

Desirable criteria:

- In depth security architectural design review skills and the ability to discuss the merits and trade-offs of using any particular design approach and technologies
- Experience working with or in a Computer Security Incident Response Team (CSIRT)
- Experience with security testing tools, development of threat assessments and security testing methodologies is desirable
- Experience working with security controls in cloud services e.g. Azure, Office 365, etc. and XaaS providers
- Knowledge and experience of the Microsoft Azure Cloud Adoption Framework

H Additional Information

- Flexible to travel across the UK as required
- On call requirement within the role supporting the function

For Panel to complete only:

Line Manager Approval: (this is only signed off when the line manager has approved the final version)

Panel Approval: (this will only be signed off once the job has gone through the Job Evaluation Panel)

Date: Click or tap to enter a date.

Email the Job Evaluation submission form together with supporting documentation (organisational charts, job descriptions) to **People & Culture Policy & Reward inbox**

You will be advised of a panel date following receipt of the submission