Job Description

A Post Details:

Job Title: Cyber Security Specialist	**Grade:** B003
Department: Technology	**Division:** A
Reports to: Cyber Security Manager	**Contract Type:** Permanent
Level of Vetting: Security Check	**Numbers in Post:** 4
Welsh language required: No	

B Purpose of the Post:

To implement security technology and programs that protect the enterprise against unauthorised access to organisation, customer or partner data. Responsible for monitoring and evaluating new information security technologies and sharing knowledge with operations.

Responsible for providing specialist cyber security advice for projects and programmes, carrying out threat analysis, blocking security threats, and educating end users.

C Dimensions of the Post:

Financial – Direct or Non-Direct

None

Staff Responsibilities – Direct or Non-Direct

None

Any Other Statistical Data

None

D Principal Accountabilities:

Skills Framework for the Information Age v8

Required level priority: 🟩 Normal 🟦 High

Strategy and architecture									
Security and privacy		0	1	2	3	4	5	6	7
Information security						🟩			
Vulnerability research	New						🟩		
Threat intelligence	New					🟩			
Delivery and operation									
Security services		0	1	2	3	4	5	6	7

Security operations					□			▨
Vulnerability assessment New		▨				□	▨	▨

Strategy and architecture

Security and privacy

Information security - 4: Enable

- Provides guidance on the application and operation of elementary physical, procedural and technical security controls.
- Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems.
- Identifies risks that arise from potential technical solution architectures.
- Designs alternate solutions or countermeasures and ensures they mitigate identified risks.
- Investigates suspected attacks and supports security incident management.

Vulnerability research - 5: Ensure, advise

- Plans and manages vulnerability research activities.
- Maintains a strong external network in the area of vulnerability research.
- Gathers information on new and emerging threats and vulnerabilities.
- Assesses and documents the impacts and threats to the organisation.
- Creates reports and shares knowledge and insights with stakeholders.
- Providing expert advice and guidance to support the adoption of tools and techniques for vulnerability research.
- Contributes to the development of organisational policies, standards, and guidelines for vulnerability research and assessment.

Threat intelligence - 4: Enable

- Collates and analyses information for threat intelligence requirements from a variety of sources.
- Contributes to reviewing, ranking and categorising qualitative threat intelligence information.
- Creates threat intelligence reports.
- Evaluates the value, usefulness and impact of sources of threat intelligence sources.

Delivery and operation

Security services

Security operations - 4: Enable

- Maintains operational security processes and checks that all requests for support are dealt with according to agreed procedures.
- Provides advice on defining access rights and the application and operation of elementary physical, procedural and technical security controls.
- Investigates security breaches in accordance with established procedures and recommends required actions.
- Provides support and checks that corrective actions are implemented.

Vulnerability assessment - 5: Ensure, advise

- Plans and manages vulnerability assessment activities within the organisation.
- Evaluates and selects, reviews vulnerability assessment tools and techniques.
- Provides expert advice and guidance to support the adoption of agreed approaches.
- Obtains and acts on vulnerability information and conducts security risk assessments, business

impact analysis and accreditation on complex information systems.

E Decision Making:

Level 4 - By making decisions which influence the success of projects and team objectives, this level of decision making will pro-actively support delivery of projects/workstreams and subsequently have an impact on achieving organisational objectives.

F Contact with Others:

Internal

- Manage stakeholders; raise any gaps in existing/new security solutions and make recommendations of how to be secure by design to minimize business risk.
- Working closely with Information Management / Information Security and the Cyber Security Unit.
- Act as a bridge between technical teams on security matters.

External

- Working with external partners, counterparts in Home Office Forces as well as the NCSC

G Essential Criteria:

Qualifications and Training:

- Industry certification such as CISSP, CCSP, Azure Security, Architecture, Security+, Togaf, SABSA
- Educated to degree level in a specific IT or engineering discipline or equivalent experience
- Industry certification such as CISSP, CCSP, Azure Security, Architecture, Security+, Togaf, SABSA

Experience:

- An extensive background working in IT Security based roles, having relevant industry experience and/or qualifications (e.g. CASP, CISSP).
- Experience with multi-vendor firewalls, configuration of multi-layer security solutions and management of SIEM solutions.
- Experience with cyber security concepts, such as threat detections, incidents response, penetration testing (external / internal), malware and DDoS mitigation.

Business and Technical Skills:

BTP Skills Framework

Business

Communication - Expert: Extensive experience and diverse application

- Inspires trust and openness by being reliable, discreet and respecting confidentiality.
- Adapts influencing tactics to the motives and style of others (e.g. logical appeal, emotional appeal, etc.).
- Identifies and directs gathering the most critical information to inform development of opinions and insights.
- Delivers written and oral communications that engages audience participants and has impact.
- Analyses others' perspectives and needs and develops influence strategies and

communications that create mutual benefits.
- Presents complex and difficult messages skilfully, using a variety of media and methods.
- Advises on team members' writing and speaking skills.

Influencing Others - Expert: Extensive experience and diverse application

- Evaluates and focuses on business opportunities likely to be of considerable strategic or long-term value.
- Adapts communication messages, methods and influence strategies to the person or audience.
- Adapts influencing tactics to the motives and style of others (logical appeal, emotional appeal, etc.).
- Utilises positive or negative influence strategies appropriately to garner support for key initiatives.
- Expands reach of influence by motivating others to focus on shared goals and a common purpose.
- Uses knowledge of personalities and team dynamics to effectively solve problems and facilitate decision making.

Problem Solving - Expert: Extensive experience and diverse application

- Advises on root cause analysis principles to resolve key problems.
- Coaches team members in problem solving methods and practices.
- Transforms problems into opportunities for organisational learning.
- Establishes and leads teams to solve complex problems.
- Collaborates across groups to maximise effectiveness of problem solving approaches.

Technical Specialisms

Cloud Platform

Microsoft Azure - Working: Hands-on experience and application.

- Supports migration tasks of data and applications for the cloud.
- Assists with setting up the organisation's Azure environment; configuring virtual machines, storage and networking.
- Monitors the Azure environment for issues and troubleshoots problems that arise. Sets up alerts and dashboards to track performance metrics and identify potential issues.
- Works with Azure's cloud migration tools, services and containerisation technologies.
- Tests migration processes and works with tools which automate the testing and deployment of code changes.

Cloud Migration - Working: Hands-on experience and application.

- Supports migration tasks of data and applications for the cloud.
- Assists with implementing DevOps practices to streamline migration processes and deploy applications.
- Troubleshoots and resolves common migration problems and recommends actions for prevention.
- Works with cloud migration tools and services and containerisation technologies.
- Tests migration processes and works with tools which automate the testing and deployment of code changes.

Knowledge:

- Good knowledge of emerging security technologies and their applicability to the Force
- Good knowledge of information security protocols including device and network encryption services.
- Good knowledge of relevant security frameworks (NIST, CIS, ISO) and integrating such frameworks into their functional work.

Desirable Criteria:

- Certified Ethical Hacker (CEH) qualification
- CompTIA Security+ qualification
- Project Management experience/qualifications

H Additional Information:

Participation in an on-call rota to provide out-of-hours triage, diagnostics, and remedial work in their specialist field plus, plus attendance on site if deemed necessary for operational reasons.

For Panel to complete only:

Line Manager Approval: James Morley
Panel Approval: BTP Reward Team
Date: 2024-01-17

Email the Job Evaluation submission form together with supporting documentation (organisational charts, job descriptions) to People & Culture Policy & Reward inbox.
PolicyandReward@btp.police.uk

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