|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A | **Post Details** | | | |
|  | Job Title: IT Cyber Security Analyst |  | Function: | Engineering, IT and Major Contracts |
|  | Location:  Four More London |  | Unique Post Number: |  |
|  | Reports To: IT Cyber Security Manager |  | Grade: MG1 |  |
| B | **Purpose of the Job**  The Cyber Security Analyst role deals with the daily operational cyber security incidents, working closely with the Service teams to mitigate and resolve issues. It also acts as a primary contact point for the Security Operations Centre the organisation is partnered with, and will work with their analysts to understand and resolve alerts.  The analyst role also manages the security systems and services deployed to protect the organisations perimeter and internal systems, including the vulnerability management platform, ensuring that the security posture of the organisation is protected, whilst protecting operational requirements of the organisation  The role will also undertake security investigations, and assist with data search requirements.  The Cyber Analyst role will work with other organisations within Go-Ahead Group, as well as working with Suppliers to ensure potential threats and known vulnerabilities are understood and remedial actions are worked up and deployed in a timely manner. | | | |
|  |  | | | |
| C | **Principal Accountabilities** | | | |
| C1  C2  C3  C4  C5  C6  C7  C8  C9 | Daily security incident investigation and resolution  Ongoing management of security systems and services  Point of contact for the SOC analysts to engage when security alerts are generated.  Generate reports for security incidents  Work with the Cyber Security Manager and other IT teams to achieve and maintain the security requirements to meet compliance with NIS and ISO 9001/27001 trajectory, and other requirements adopted by the organisation  Work with the organisation’s directorates and project teams to incorporate Security by Design in new and existing services  Work with the Infrastructure Manager and Service Manager in defining security baselines for systems and infrastructure  Participate in an on-call escalation rota, covering nights and weekends, including bank holidays to support the service team on security issues  Undertake any other activity that is commensurate with the role, as requested by management | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| D | **Safety Responsibilities** | | | | |
| D1 | This post is required to undertake SAFETY CRITICAL WORK | Yes |  | No | **🗸** |
| D2 | This is a KEY SAFETY POST or nominated deputy | Yes |  | No | **🗸** |
| D3 | The holder of this post is identified as a KEY SAFETY MANAGER | Yes |  | No | **🗸** |
| D4 | The job requires competence in PERSONAL TRACK SAFETY | Yes |  | No | **🗸** |
| D5 | This job has SPECIFIC SAFETY RESPONSIBILITIES (if Yes see section D6 below) | Yes |  | No | **🗸** |
|  |  | | | | |
| D6 | The post holder has the following specific safety responsibilities: | | | | |
|  | Carrying out Planned General Inspections of the following locations:   * None | | | | |
|  | Acting as Fire Precautions Manager for the following locations:   * None | | | | |
|  | Safety Interface with the following external parties:   * None | | | | |
|  | Investigation of accidents occurring at the following locations or as requested by Safety & Environment:   * None | | | | |
| E | **Decision making Authority** | | | | |
| E1 | As appropriate to ensure resolution of security incidents | | | | |
| F | **Most Challenging and/or Difficult parts of the role** | | | | |
| F1 | Ensuring incidents are managed and resolved whilst protecting the operational state of the organisation | | | | |

|  |  |
| --- | --- |
| G | **Person Specification** |
|  | Southeastern aims to recruit people not just for jobs but for long term careers. We want good quality, talented people with the right attitude who will stay with us.For these reasons we look for evidence of Southeastern values and behaviours in all potential staff and our existing staff looking for promotion along with the particular experience/knowledge, skills and behaviours relevant to the position applied for. These areWe care passionately about our people and passengers  * + we put ourselves in our passengers’ shoes to do what’s right for them   + we support our colleagues to be, feel and do their best   + we love the places we serve and do our bit for our communities and environment  We aim to be the best  * + we move with pace, we’re agile and learn from everything   + we relentlessly strive to be the best   + we are professionals with personalities  We make the difference together  * + we are answerable to each other and our passengers   + we trust each other and do what we say we will   + we are stronger together than we are as individuals   We also have identified behaviours required to be successful in leading Southeastern.    The Leading Southeastern framework details **how** we should be behaving in order to drive up performance to deliver **85 by 18**.  All shortlisted candidates seeking promotion will be assessed against this framework.  The job demands the following blend of experience/knowledge, skills and behaviours (all are essential , unless otherwise shown and will be assessed by application and/ or interview/assessment) : |
| G1 | Experience, Knowledge & Qualifications (including any specific safety training requirements) 2 Years experience working in a Cyber security role  Extensive experience of Microsoft products  Experience of working in red/blue team scenarios  CompTIA Security+ (or equivalent)  Certified Ethical Hacker |
| G2 | Skills (including any specific safety critical competencies) Driven individual with a ‘CAN DO’ attitude that engenders confidence, respect and support.  Passion, enthusiasm and expertise.  Good written and verbal communication skills  Quality and transparency  Good prioritising skills and the ability to meet targets |
| G3 | Behaviours Honesty  Integrity  Reliable |
| G4 | **Other** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| H | **Dimensions of role** | | | | |
| H1 | Financial – | |  | | |
| H2 | Financial – Other: | |  | | |
| H3 | Staff Responsibilities – Direct: | |  | | |
| H4 | Staff Responsibilities – Other: | |  | | |
| H5 | Any Other Statistical Data: | |  | | |
| I | **Acknowledgement** | | | | |
| I1 | Prepared By: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Date: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| I2 | Approved By (Head of Department): | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Date: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **J** | **Job Description Briefing** | | | | | |
|  | The post holder has been briefed on and understands the requirements of this Job Description and other related documents: | | | | | |
|  | Name of post holder: |  | Signature: |  | Date: |  |
|  | Name of briefing manager: |  | Signature: |  | Date: |  |
| **K** | **Nominated Deputy for Safety requirements** | | | | | |
|  | If this is a KEY SAFETY POST (D2 in Safety Details above is YES) at least one nominated deputy must be identified. The Job Holder must ensure that the Nominated Deputy(ies) receives a copy of, and is briefed on this Job Description. If there are more nominated deputies, they should sign further copies of this Job Description. | | | | | |
|  | The nominated deputy has been briefed on and understands the requirements of this Job Description and other related documents: | | | | | |
|  | Name of nominated deputy: |  | Signature: |  | Date: |  |
|  | Name of briefing manager: |  | Signature: |  | Date: |  |