

**NHS NATIONAL SERVICES SCOTLAND**

# JOB DESCRIPTION

|  |  |
| --- | --- |
| **1. JOB DETAILS** | |
|  | |
| Job Holder |  |
| Job Title | Cyber Security Operations Analyst |
| Immediate Senior Officer | Department Manager |
| Division | Digital and Security (DaS) |
| Location | Dundee / Hybrid |
|  | |
| **2. JOB PURPOSE** | |
| You will work as part of a team providing operational support, communication and incident management, to all NHS Scotland health boards to facilitate their cyber security and risk management activities, meeting their strategic, regulatory and compliance requirements, and securing day to day operational objectives and functions.  You will contribute to the design, configuration and operation of multiple cyber security technologies utilised on a national basis in NHS Scotland to detect and respond to security threats.  The security services and technology provided by NSS Digital and Security (DaS) are critical operational components, utilised 24/7 365 days a year. | |
|  | |
| **3. DIMENSIONS** | |
| Security technologies and services provided by NSS DaS are utilised across NHS Scotland including on our national network (SWAN), integrated with national IT systems and locally in each of the health boards.  Examples of the security technology or services include:   * Security Information Event Management (SIEM) systems to identify and track potential threat indicators * Vulnerability management and scanning tools as part of security assessments * Incident handling and communication working with key stakeholders both within NHS Scotland and externally such as CareCERT SOC (NHS England), Local Authorities and NCSC * Microsoft technologies including Office 365, Defender ATP and security dashboards   Security services operate 24/7/365 and health board’s regulatory compliance is intrinsically linked to good security practices utilised to ensure safe and effective services are provided for patients in Scotland.  The security services are comprehensive and fully integrated into the work processes and, therefore need to be supported 24/7/365 by an expert team who have an comprehensive understanding of the security landscape, how technology can be utilised to manage risk and how to respond to support health boards. | |
| **4. ORGANISATION CHART** | |
|  | |
|  | |
| **5. ROLE OF THE DEPARTMENT** | |
| The role of Digital and Security (DaS) Strategic Business Unit (SBU) is to support the NHS Scotland national eHealth agenda through the effective delivery of IM&T products and specialist services that will enable clinical process and efficiency improvements across Scotland. The core remit is focused on the management and delivery of IM&T services focused on the development and enablement of national level business and clinical capabilities. This includes the delivery of IM&T services, systems, data and contracts which enable cross-Board/ boundary integration, workflow, information sharing, cost efficiency realisation and collaboration.  DaS has of the order of 350 staff, approximately 260 based in Edinburgh and 90 based in Glasgow where national level software application products are developed, maintained and supported. DaS is currently involved in over 50 projects and programmes in support of eHealth across NHS Scotland.   * The vision of the organisation is ‘To be valued as a trusted, integral IT services partner’ * The mission of the organisation is ‘To deliver high value national and specialist IT services which maximise health and financial impact’ * The purpose of the organisation is ‘To provide high value shared services, enable national level IM&T capabilities and cross- Board/ boundary collaboration’   The service model is focused on the following key areas:  **> Cyber Security**  Providing national cyber security services to manage information risk and meet regulatory requirements.  **> Architecture & Consulting**  Providing focused IM&T expertise and advice to eHealth and business communities  **> Contract & Vendor Management Services**  Managing 3rd party national level eHealth suppliers end-to-end  **> Programme & Project Management**  Scalable and adaptable delivery of eHealth initiatives at national level.  **> Solutions Design, Development, Integration & Maintenance**  Bespoke systems development, maintenance and support  **> National Solutions Accreditation & Testing**  Assuring inter-operability of the national architecture  **> Solution Stewardship / Service Management**  Managing service delivery assurance for systems after ‘go live  **> Infrastructure Management**  Managing the delivery of customer service, LAN, desktop and other infrastructure services  DaS works in partnership with a wide range of organisations – NSS, NHS Scotland NHS Boards, Hospitals, Primary Care Practitioners, Community Health Partnerships, Local Authorities, Scottish Government Directorates, Other UK eHealth agencies, and major IM&T product and service providers operating in the Scottish public sector.  The role of the business analyst is to support the organisation in delivering solutions to internal and external customers that provide real business benefit. | |
|  | |
| **6. KEY RESULT AREAS** | |
| 1. Operate key national information systems that detect and alert to potential cyber threats across the whole of NHS Scotland on a continual basis. Configure these systems according to your research of malware and other cyber threats to generate alerts for further investigation. 2. Investigate and resolve security alerts that may arise on a 24/7/365 basis and that require specialist technical expertise and an analytical approach. 3. Maintain appropriate and complete documentation at all times, paying close attention to detail in the recording of security alerts and events. Ensure compliance with relevant regulatory / legislative / quality standards e.g. GDPR, NIS, etc. Help NSS and health boards to prepare for regulatory, national and internal audits. 4. Liaise with health board technical teams to understand and troubleshoot complex security information. 5. Research security threats and analyse highly complex security scenarios to develop enhanced detection and response techniques in national information systems to improve cyber security. 6. Deliver security training and share your expertise on new security analysis to the rest of the team and to other staff on occasion to help raise cyber security awareness. 7. Contribute to the design, development, configuration and operation of security tools and technology in the provision of national cyber security services. 8. Provide 24/7 365 days a year security support (as part of a team), advice and guidance to NHS Scotland health boards 9. Support health boards to comply with regulatory requirements including GDPR, NIS and Caldicott guidelines to ensure safety, security and privacy of self, other staff and members of the public. 10. Develop and maintain security response plans, scenarios and scripts utilising appropriate manual and automated processes 11. Maintain a current awareness of developments in information security standards and good practice to ensure continuous professional development. | |
| **7. ASSIGNMENT AND REVIEW OF WORK**  Key objectives will be assigned annually and reviewed by either the NHS CSOC Manager or Information Security Manager on a regular basis via a formal appraisal scheme.  Day to day activities will be guided by standards operating procedures, manuals and established practice for operation of national information security management technologies.  Work may also be generated from:   * Other line managers and Department Heads * Internal or external customers * Cyber security tools and security alerts/advisories * NHS suppliers, partners and support organisations such as NCSC * Self generated based on internal project work and research   The post holder is guided in all work by regulation, policies and standards, including but not limited to “Security of Network and Information Systems Directive” (NIS), NHS Scotland Information Security Policy Framework and General Data Protection Regulation (GDPR) | |
|
|  | |
| **8. COMMUNICATIONS AND WORKING RELATIONSHIPS** | |
| Internal  * Regular informal meetings with the CSOC Manager and other Cyber Security Operations Analysts. * Occasional meetings with representatives of the other elements of NSS such as internal IT * Presentation to internal Information Security Team meetings.  External  * Frequent contact with stakeholders from health boards including technical and security personnel who may be involved in responding to security incidents. * Workshop organisation and facilitation with stakeholders to develop and improve security services provided by DaS * Frequent and sometimes in depth consultation with various external stakeholders including but not limited to product suppliers to resolve vulnerabilities and other security issues, industry and sector advisory bodies such as NCSC and NIS Competent Authority to analyse security event information and external authority bodies such as the Police and ICO for advice or to report or manage incidents. * Contributing to consultation with Scottish Government | |
|  | |
| **9. MOST CHALLENGING PART OF THE JOB** | |
| Developing and maintaining a cutting edge knowledge of a wide range of complex security threats and technologies including many types of malware, operation of cyber threat actors, SIEM good practice, threat detection and how to respond to multiple types of cyber security incident or alert.  Dealing effectively and calmly under pressure with competing demands arising from unforeseen events that require rapid response and resolution.  Urgently and accurately analysing and reporting on complex IT system/operational information to promote the security of NHS Scotland systems and operational requirements 24/7/365. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **10. WORKING ENVIRONMENT AND EFFORT** | | | | | |
| **Physical Effort** | | | | | |
| * Large parts of the working day are spent sitting working at the computer. * Car use/public transportation to attend meetings * Standard computer skills are required. | | | | | |
| Mental Effort | | | | | |
| Intense concentration is frequently required over long periods when working on security problems, to develop and prepare documentation and to prepare project documentation. The post holder will contribute to the review of policies and procedures.  Job requirements can occasionally be unpredictable with a need to prioritise often competing and urgent demands. Due to the nature of the work, in cases of serious incidents where processes in business critical software are stopped, work priorities need to be carefully managed and communicated.  In relation to judgements and analysis, the post holder will make judgements, weighing up all the data and evidence to determine the level of escalation required by a particular security alert. | | | | | |
| **Emotional Effort** | | | | | |
| NHS Scotland is almost totally reliant on the availability of information systems and services. Consequently, when there are security incidents there can be competing demands for assistance simultaneously and from staff in many different locations and departments. Although this is a rare occurrence it can be extremely stressful. | | | | | |
|  | | | | | |
| **11. ENVIRONMENTAL / WORKING CONDITIONS & MACHINERY AND EQUIPMENT** | | | | | |
| Working conditions will include:   * Requirement to travel by car or use public transportation on occasion * Very frequently undertake continuous use VDUs | | | | | |
|  | | | | | |
| **12. QUALIFICATIONS AND/OR EXPERIENCE SPECIFIED FOR THE POST** | | | | | |
| **Qualifications**   * Bachelors Degree OR * Equivalent academic qualifications in information or cyber security   **Qualifications goals/ambitions**  This post may suit someone interested in or working toward qualifications such as:   * Security qualifications or certifications such as CEH, ECIH, CISSP, etc. * Technology certifications such as Microsoft (MCSE or related security modules), Cisco certifications, other suppliers such as Checkpoint, Palo Alto, Fortinet, etc.   **Experience (desirable)**   * Experience working within a Security Operations Centre, or an IT team for a large organisation * Experience delivering, implementing or operating IT infrastructure (networks, servers, desktop, etc.) * Knowledge of the issues, culture and opportunities prevalent in NHS Scotland. * Previous exposure to eHealth, or equivalent, products.   **Other**  Full, clean driving license. | | | | | |
|  | | | | | |
| **13. JOB DESCRIPTION AGREEMENT** | | | | | |
| A separate job description will need to be signed off by each jobholder to whom the job description applies. | | | | | |
| Job Holder’s Signature |  | | Date |  |  |
|  |  | |  |  |  |
| Head of Department |  | |  |  |  |
|  |  | |  |  |  |
| Signature |  | | Date |  |  |
|  |  | |  |  |  |
| Title |  | |  | | |
|  |  | |  |  |  |
| HR Department will check job description format and content and then send the job description to the AfC Team | | | | | |
| HR Representative’s Signature |  | |  | | |
|  |  | |  |  |  |
| Date Job Description Agreed: | |  |  | | |
|  |  | |  |  |  |