

NHS NATIONAL SERVICES SCOTLAND

# JOB DESCRIPTION

|  |  |
| --- | --- |
| 1. JOB DETAILS | |
| Job Title | **Senior Security Operations Analyst** |
| Immediate Senior Officer/ Line Manager | Head of Information and Cyber Security |
| Department | Cyber Security Team |
| SBU | Digital and Security |
| Location | Flexible |
| CAJE Reference | NPITG294 |
|  | |
| **2. JOB PURPOSE** | |
| The Senior Security Operations Analyst will run security operations for NSS and NHS Scotland health boards to ensure the ongoing security of networks, information systems and other products and services. This will include utilising security tools to monitor the network, identify potential threats, providing advice and recommendations and to mitigate risk, information security design and assurance advice and supporting the overall business to implement security good practice. | |
|  | |
| **3. DIMENSIONS** | |
| This is a national role providing security services that impact all NHS Scotland health boards. The primary activity of the role will be using cyber security technology to detect, analyse and respond to network, data or other events that may indicate an actual or attempted cyber security breach, attack or other incident. Further the post holder will need to engage with health board technical contacts to further investigate and resolve their cases, deliver corresponding training, formulate improvement plans and support projects to build secure designs that integrate with national solutions.  The Senior Security Operations Analyst will operate on a day to day basis within the Cyber Security Operations Centre (CSOC) budget and does not have a delegated budget. However, the post holder will contribute to the drawing up of the national NHS Scotland cyber security budget and will design business cases for security initiatives and technology solutions such as for SIEM, endpoint protection or vulnerability management solutions. Project budgets tend to range between £10k for something simple such as a cloud based external security scanner, up to £1m for a national project such as endpoint protection solution for all NHS Scotland health boards.  The Senior Security Operations Analyst reports to the Head of Information & Cyber Security and does not have any direct line management responsibilities themselves.  The Senior Security Operations Analyst is responsible for the delivery of core specialist information security training both within NSS and for health boards. This will include delivering training on CSOC platforms and incident handling. The audience of training will be IT operations, security practitioners and any other health board staff involved in the management of security platforms or handling security incidents. The Senior Security Operations Analyst will need to both generate new content and adapt existing content to deliver effective training for technology us in NHS Scotland context. | |
| **4. ORGANISATION CHART** | |
|  | |
|  | |
|  | |
| **5. ROLE OF THE DEPARTMENT** | |
| The Cyber Security Team provides national information security services across the whole of NHS Scotland in four key result areas:   * **Security policy and compliance**: Delivering national security policy and standards, and helping health boards to implement these to meet regulatory requirements * **Cyber Security Operations Centre (CSOC)**: Identifying and mitigating cyber threats continually and real-time. Providing advanced cyber security services on a national basis “once for Scotland” * **Security advisory services**: Security design and assurance of NHSS applications and IT projects to ensure security of NHS Scotland data and manage risk * **Managing national infrastructure**: SWAN cyber security including assurance of service design, managing supplier, handling incidents and supporting members   The Cyber Security Team sits within the Digital and Security (DaS) business unit.  DaS supports the NHS Scotland national eHealth agenda through the effective delivery of IM&T products and services across Scotland.  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. | |
|  | |
| **6. KEY RESULT AREAS** | |
| 1. Provision of cyber security subject matter expert national support and services through the NHS Scotland Cyber Security Operations Centre (CSOC). This is a national service operated by NSS to provide security operations capability to all health boards and national infrastructure including SWAN and national information systems 2. Operating advanced cyber security tools and technology to detect, identify and action cyber security threats to NHS Scotland networks and information systems. Analysing threats to capture and understand details and formulate corresponding action steps and recommendations to help health boards to mitigate and counteract threats 3. Provision of security management consultancy to NHS Scotland health boards. This would include security requirements definitions, costed proposals, planning and tracking for projects (up to £1m per project) as required. The advice and project work to plan and implement security improvements stems from the post holder’s analysis of information security events. The improvements will span DaS, all of NSS or all of NHS Scotland in the case of national initiatives, and may cover several years for national rollouts. 4. Managing security incidents, working under stressful conditions and in the heat of the moment to decide appropriate steps needed to reduce the impact of an incident in progress 5. Developing business cases and progressing procurements for information security technology solutions (for example SIEM, endpoint protection, vulnerability management solutions) – project budgets likely to range between £10k for a cloud based security service such as an external security scanner, up to £1m for a national endpoint protection solution 6. Ensure appropriate security standards and techniques are developed and followed within NSS and NHS Scotland, supporting the NHS Scotland Information Security Policy Framework (ISPF) and helping health boards to maintain regulatory compliance 7. Designing and implementing national cyber security improvement initiatives, either for NSS or impacting all of NHS Scotland, for example to implement end point/EDR infrastructure along with associated procurement of technology 8. Preparing and delivering security training to NSS and other health board staff on the use of new security technology, interpretation and response to security alerts and associated intelligence & data, and the handling of incidents 9. Maintaining and developing knowledge of the latest cyber security technology, standards & good practice, ensuring appropriate advances can be incorporated into NSS and eHealth products to ensure we are combating the current cyber risks 10. As the department develops the post holder may need to work under “on call” circumstances to be contactable in the case of an incident out of hours 11. Promoting the vision, capabilities and potential of DaS by understanding the business needs of health boards, IT teams and other stakeholders and demonstrating how DaS can help. 12. Plan and organise a number of complex security analysis activities including multi-platform investigation and prioritisation of threats and incidents for resolution and creating medium and long term improvement programs to help NHS Scotland improve security practice 13. Establishing and carrying out research projects to understand a particular threat such as a new type of malware/exploitation technique and recommend appropriate new practices, standards, configurations, etc. to enable NHS Scotland to mitigate the risk 14. The Senior Security Operations Analyst is responsible for the operation of multiple CSOC information systems covering the whole of NHS Scotland, this is a major job responsibility. In particular the post holder will operate the Security Information and Event Management (SIEM) solution monitoring network traffic and threat indicators across all national information systems and health boards, and operating the Advanced Threat Protection (ATP) infrastructure and carrying out advanced threat hunting to monitor NHS Scotland services. | |
|  | |
| **7. ASSIGNMENT AND REVIEW OF WORK** | |
| On a day to day basis the expected results are defined but the post holder decides how they are best achieved and is guided by principles and broad occupational policies or regulations – including the Security of Network and Information Systems (NIS) regulation, NHS Scotland Security Policy Framework (ISPF), industry standards such as ISO27001 and technical standards and guidance relating to the specific technologies.  Guidance will be provided by peers or external reference points, including the CSOC Manager and health board contacts, partner contacts in NHS Digital or National Cyber Security Centre (NCSC) and expert contacts in supplier organisations.  The post holder will work within the goals of the Cyber Security Team which are all generated from the strategic and regulatory context:   * Scotland's Digital Health and Care Strategy – the digital strategy covering all of NHS Scotland * NSS Strategy – our top level strategy to national infrastructure services and solutions which are integral to the delivery of health and care services in Scotland Work is allocated by manager/self generated. * Key regulation and policy – in particular the Security of Network and Information System (NIS) regulation and corresponding NHS Scotland Information Security Policy Framework   On a day to day basis the Information Security Analyst will carry out incident investigations, follow evidence and carrying out research, drawing conclusions and making recommendations and engaging with peers and stakeholders both internally and in external organisations as needed. The post holder will create deliverables; write reports and reference strategic context to determine appropriate outputs.  Work will be carried out primarily through technical analysis but will also require personal contact with a full range of other personnel (including technology specialists, project owners and end users), formal and informal meetings, producing written reports, problem solving, analysis and investigation.  The role requires accessing and understanding information feeds, correlating data events, digging into the underlying detail and bringing this all together to draw accurate and meaningful conclusions will form the core of activity on many days. Additionally, the post holder will then need to be able to make recommendations to address potential security concerns, and confirm based on further analysis if changes have been successful. | |
|
|  | |
| **8. COMMUNICATIONS AND WORKING RELATIONSHIPS** | |
| **Communication and relationship skills**  The post holder will provide and receive highly complex information on a day to day basis.  The post holder will need to distil and communicate complex technical and security information where the post holder will be an expert but the recipients of information will have mixed levels of technical capability and understanding.  Most communication will be internal to the Cyber Security team. The post holder will also regularly need to communicate with technical personnel within NSS and other health boards during an investigation and to resolve security alerts and manage incidents.  The post holder will also need to communicate with external partners and the wider security community such as with NHS Digital to share information and work collaboratively; engaging with suppliers to highlight and resolve vulnerabilities; and engaging with security authorities and partners regarding security policy. | |
|  | |

|  |
| --- |
| **9. MOST CHALLENGING PART OF THE JOB** |
| * The prolonged levels of concentration required to complete technical analysis such as during a normal security analysis which is the daily pattern of work. This will involve complex manipulation of multiple data sets, investigating IT systems in real time looking for possibly subtle details in a vast amount of data, and identifying and confirming correlations to make meaningful conclusions * Communicating complex information to varied audiences - The post holder will need to distil and communicate complex technical and security information where the post holder will be an expert but the recipients of information will have mixed levels of technical capability and understanding. * Working under stressful conditions during a cyber incident – Occasionally there will be a need for intense concentration, such as during a security incident which can be a particularly stressful situation. For example if there is a significant service outage or a major loss of data, the post holder may need to work with staff in the affected organisations to assist in the incident investigation and response – these can be stressful times for all involved and ability to remain calm and work positively under this pressure will be valuable. * Maintaining skills and expertise and keeping up with the fast moving world of security threats, technology and good practice |
|  |
| **10. SYSTEMS** |
| **Cyber security systems**  The post holder will work with Cyber security systems that are core daily activity, including but not limited to:   * ATP and Microsoft 365 security portal – as a primary tool to identify and investigate alerts on a daily basis, and to create advanced hunting rules to generate new alerts based on research and analysis * Endpoint, inventory and patching – such as Ivanti Endpoint Security (IES) and Xtraction to monitor vulnerabilities and deliver a national dashboard and reports * Vulnerability scanners & pen testing tools – such as Tenable, PenTera etc. to monitor NHS Scotland estate for externally facing vulnerabilities, to carry out security assessments of NHS Scotland websites and complete pen testing for Internet facing services such as VPN or APIs * Forensic analysis systems – standalone and purpose built systems to image compromised systems and take RAM dumps, gather logs and protect forensic information for further investigation * NCSC Active Cyber Defence (ACD) systems – such as WebCheck, MailCheck or CNR systems to monitor   **Business and office systems**  Standard office productivity and automation systems, including:   * NSS business systems: flexi-time, expenses, meeting room and HR/appraisal systems – which the post holder will use to manage their time, benefits, payroll and other office working data * Standard office productivity and collaboration tools such as MS Office, Teams, Visio and ServiceNow which the post holder will use to carry out their day to day activites, write documents, manage tasks and interact with other staff |
|  |

|  |
| --- |
| **11. WORKING ENVIRONMENT AND EFFORT** |
| The working environment will be almost entirely office or home based with minimal physical effort.  A combination of sitting, standing and walking with little requirement for physical effort. There may be a requirement to exert light physical effort for short periods. Majority of work is computer based, the post holder should be comfortable working at a computer over an extended period.  The post holder will frequently be required to concentrate for prolonged periods, such as during a cyber risk assessment which is an example of a typical daily pattern of work. Occasionally there will be a need for intense concentration, such as during a security incident which can be a particularly stressful situation.  NSS supports flexible working and the post holder will have good flexibility around working hours, however, sometimes working long hours may be required, such as to meet a deadline during the development of a major IT project milestone such as project gates.  There can be occasional exposure to distressing or emotional circumstances, for example during a major cyber security incident, or when working toward major deadlines or deliverables for national projects. Particularly if there is a significant outage of service or a major loss of data, the post holder may need to work with technical specialists in the affected organisations to assist in the incident investigation and response – these can be stressful times for all involved and ability to remain calm and work positively under this pressure will be essential. |
|  |
| **12. ENVIRONMENTAL / WORKING CONDITIONS & MACHINERY AND EQUIPMENT** |
| There is a requirement to use Visual Display Unit equipment more or less continuously on most days.  The working environment will be almost entirely office based, and will mostly involve working at a computer. There will likely be no need to operate machinery. May need to go into server rooms or under desks on occasion to access network cabling.  The post holder will likely need to travel off site on occasion and this may sometimes be needed during poor weather.  There is no need to handle dangerous substances or equipment and no prolonged exposure to unpleasant environmental conditions. |
|  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **13. QUALIFICATIONS AND/OR EXPERIENCE** | | | | |
| The post holder will utilise specialist knowledge across a range of cyber security procedures and practices, underpinned by theoretical knowledge of IT and security (networks, servers, endpoints, access control, security events, etc.) or relevant practical experience such as handling incidents or investigating breaches.  The post holder will hold a Technical degree in computer science degree or similar (or equivalent).  The post holder will additionally hold one of the following qualifications;   * CSOC technology qualifications – qualifications or material experience in CSOC technology such as Microsoft Sentinel, Splunk or other SIEM certifications, Microsoft security certifications (ATP, Azure, etc.), CEH, Incident Handler, etc. * Information security qualifications – qualifications or material experience in information or cyber security such as information security manager, information security officer, CISSP, CISM, ISO27001 implementer or auditor, etc. * Technical qualifications – certification in various core IT infrastructure technology such as Cisco, Microsoft, Amazon, Checkpoint, Juniper, Palo Alto, Fortinet, etc.   The following baseline skills and experience are essential:   * IT experience – experience working in IT discipline such as software development, network administration, solution architecture or design or IT support * Advanced standard computer skills – the post holder will be an advanced computer user familiar with all basic aspects of utilising multiple applications simultaneously, moving data around, fast typing and advanced use of standard Office applications * Driving license as may need to be able to travel to remote areas in Scotland to assist a health board on site as part of an incident investigation   The post holder will utilise specialist knowledge across multiple cyber security technologies (such as SIEM, security administration/group policy, firewalls, endpoint protection, anti-malware, vulnerability management, etc.), procedures and practices (such as incident handling, breach investigation, alert analysis, etc.), and will need to apply a theoretical knowledge of security, networks and information technology to correctly analyse and interpret data and identify trends.  Previous experience in configuring, operating or administering networks and enterprise IT infrastructure will assist in the creation of relevant, concise and targeted recommendations to mitigate threats. | | | | |
|  | | | | |
| **14. JOB DESCRIPTION AGREEMENT** | | | | |
| A separate job description will need to be signed off by each post holder to whom the job description applies. | | | | |
| Post holder Signature: |  | Date: |  |  |
|  |  |  |  |  |
| Post holder Print: |  |  |  |  |
|  |  |  |  |  |
| Manager Signature: |  | Date: |  |  |
|  |  |  |  |  |
| Manager Print: |  |  | | |
|  |  |  |  |  |
| Manager Title: |  |  | | |
|  |  |  |  |  |
|  |  |  |  |  |