**Senior Security Analyst – SIEM Engineering – Band 8a**

**Recruitment role summary and candidate profile**

|  |
| --- |
| **Additional narrative about the team / roles**  Cyber Operations’ purpose is to support safe care and build​ public trust by building NHS England’s cyber resilience​ and enabling the wider health system to be cyber resilient, ​supporting Transformation Directorate’s purpose of delivering​ the best care and outcomes for the NHS.    The Cyber Operations sub-directorate consists of 4 operational areas: Cyber Security Operations Unit (CSOU), Cyber Delivery Unit (CDU), Cyber Improvement and Chief Information Security Officer (CISO). This role sits within the CSOU team.    The CSOC, part of the CSOU, function provides centralised monitoring and response across NHSE, and the system. The CSOC consists of Threat Operations​ (ThreatOps), Security Operations​ (SecOps), Incident Management​ & response, Service Operations (ServiceOps) and Development Operations (DevOps).    Consistent, efficient, proportionate security risk management is best achieved by a blend of centralised advice, control and security services blended with individual security responsibility and actions. We support owners of security risk keep their services secure, deliver managed security services to the system, filling the gaps where secure design & operation or other constraints fail to deliver proportionate security across the system.  The Senior Security Analyst SIEM Engineering is responsible for:  Deploying feeds from data sources into the NHS England’s SIEM tool and ensuring compliance with the SIEM’s data modelling, both for newly developed services and for existing services being updated.  Working closely with the Cyber Monitoring teams to manage the SIEM environment, enhance the SIEM capabilities, build alerting rules and conduct tuning activities for new and existing feeds deployed in the SIEM tool. |
| **About You** |
| **Knowledge, Skills and Experience**  **Essential**  **Information Security Management**  Expert knowledge of the processes, tools and techniques of information security management, ability to deploy and monitor information security systems, as well as detect, resolve and prevent violations of IT security, to protect organizational data.  **Information Security Operation Centre (ISOC)**  Demonstrable knowledge of modules, processes and technologies of Information Security Operation Centre (ISOC); ability to detect, response and utilise related platform and applications to perform cyber security initiatives.  **Information Security Technologies**  Demonstrable knowledge of technologies and technology-based solutions dealing with information security issues; ability to apply these in protecting information security across the organisation.  **Intrusion Detection and Prevention**  Working knowledge of tools, techniques and processes of intrusion detection and prevention; ability to detect, resolve and prevent intrusion behaviours to protect organizational networks.  **Mobile Security**  Proven knowledge of the threats, measures and practices of mobile security; ability to reduce mobile risks and protect personal and organizational data and information.  **Information Security Architecture**  Extensive knowledge of the tools and techniques used for creating software, hardware, networking and application infrastructure; ability to meet information security objectives while using these.  **Security Information and Event Management (SIEM)**  Advanced specialist knowledge of concept, procedures and processes of Security Information and Event Management (SIEM); ability to utilize related applications to protect organizational networks from cyber risks.  **Systems Software Infrastructure**  Detailed knowledge of software technology, and the ability to plan global, regional and local software architecture and infrastructure components.  **Systems Programming**  In-depth knowledge of and ability to design, develop and implement operating systems architecture and components.  **Technical Writing/Documentation**  Working knowledge of the technical language and writing approach, and the ability to write paper-based and on-line technical reference documentation (guidelines, standards, procedures, processes, applications, etc.)  **Requirements Analysis**  In-depth knowledge of tools, methods, and techniques of requirement analysis; ability to elicit, analyse and record required business functionality and non-functionality requirements to ensure the success of a system or software development project.  **Big Data Management and Analytics**  Proven knowledge and ability to plan and execute, big data management and analytics.  **Modelling: Use Case**  Detailed knowledge of the processes and techniques used to identify, clarify, and organise system requirements for users and systems within a business; ability to utilise use case modelling, define and document business requirements and application scenarios during this process.  **Innovation**  Working understanding of the value of innovation and ability to develop new ideas and initiatives that improve the performance of the organization.  **Software Product Testing**  Specialist knowledge of and ability to design, plan, and execute testing strategies and tactics to ensure software product quality and adherence to stated requirements.  **Software Product Design/Architecture**  Working knowledge of and experience with activities, tools and techniques for converting market requirements into the software product design.  **Software Integration Engineering**  Demonstrable knowledge of and ability to design, develop and maintain interfaces and linkage to alternative platforms and software packages.  **Qualifications**  **Essential**   * Masters level degree or equivalent level of experience. * Evidence of continuous professional development. * Splunk ES Administrator * Microsoft Azure Architecture and Administration * Scripting Language (e.g. Python) |
|  |