Cyber Security Analyst

Information Systems and Change

Overview	
Role Purpose	The Cyber Security Analyst identifies, protects, contains, and recovers from any cyber security threat by remediating and removing vulnerabilities across the system estate. Provide advice and support to the business on any IT security related matter in accordance with the Cyber Security Strategy.
Responsible for	Supporting both the Cyber Security Manager and Senior Cyber Security Analyst for the delivery of all key Cyber security tasks and projects as well as working with trends and analytics to look for unusual behaviours which could be a malicious software or the start of a cyber-attack using the security tools.
Reports to	Cyber Security Manager
Line management	N/A
Tier	7
Expectation Level	Colleague
Role relationships	
Internal	Head of Cyber Security, Cyber Security Manager, Cyber Security Team, Infrastructure and Systems teams, IT Service Delivery team, Data Governance Manager, Data Protection Officer, Information Asset Owners, Directors, Staff
External	Outsourced SOC team, Internal/External Auditors, Third-Party IT Suppliers

Role accountabilities

Your main responsibilities will be to assist the IT Security Manager in:

- Working with our vendors, partners, and internal teams to ensure the confidentiality, integrity and availability of security policies, procedures, and technology
- Respond to cyber security incidents according to the cyber-security incident response policy, provide investigation findings to relevant business units to help improve information security posture
- Work closely with SOC in handling security incidents
- Review and maintain Security baselines and configuration profiles for devices within InTune
- Review, monitor and advise on processes for patch management of endpoints, servers, applications, infrastructure and hardware
- Monitor, maintain and respond to incidents and alerts within the Sentinel and Defender portals
- Assist in identifying weak configuration areas for internet facing systems and cloud infrastructure and applications, performing vulnerability management
- Working with the in-house systems team as well as third party providers to ensure continuous improvement and progress against agreed security practices.

Role accountabilities

- Assist in providing weekly and monthly reporting related to security KPIs, compile, and analyse data for management reporting and metrics
- Assist in building response playbooks against cybersecurity trends
- Review and monitor security policies and processes within the Microsoft 365 suite
- Assist the Head of Cyber Security, IT Architects and Cloud Infrastructure teams in management, and implementation of cybersecurity projects
- Assist Service delivery teams in reviewing security processes, and monitor their process implementation
- Assist with implementation of countermeasures or mitigating controls
- Close working relationship with data governance and protection teams
- Provide information security training and awareness for IT teams and business users
- Monitor information security related news articles to stay up to date on current attacks and trends, and analyse potential impact of new threats and industry threat intelligence and communicate risks to relevant business units
- Work closely with other Housing Associations and cybersecurity teams in sharing knowledge, processes, and collective intelligence to improve own security posture
- Supporting the Senior Cyber Security Analyst, Cyber Security Manager and Head of Cyber Security

The tasks and responsibilities outlined above are not exhaustive; the post holder may undertake other duties as is reasonably required.

To do the job well, we have outlined the knowledge, experience, and skills you need to do the job.

Personal Specification

Professional expertise (know how & experience)

Essential	Desirable
• Proven experience of working in a large and complex customer facing organisation, and enterprise working environment • Experience of undertaking investigations, their resolution and capturing and embedding learning • Production and analysis of performance metrics • Working knowledge of data protection legislation including UK GDPR, principles of information security and governance including NIST 800, NCSC Cyber Essentials and PCI-DSS	

Skills

Essential	Desirable
• Developing and managing relationships across IT and within the business • Strong influencing skills and negotiation skills	

• Good communication skills and ability to build relationships • Ability to explain IT security risks to business stakeholders and be able to relate these to corporate risks • Understanding of threat and vulnerabilities modelling across the IT perimeter. • Being able to explain decisions clearly • Documentation and clear writing skills • Presentation skills to higher management levels within the organisation • Manage simultaneously and conflicting priorities • Experience in Microsoft Sentinel and KQL/threat-hunting • Experience in Microsoft Defender(Servers,Workstations and Mobiles), configuration, deployment, architecture, management, and reporting. • Experience in Microsoft InTune and AutoPilot technologies for deploying security baselines, Antivirus technologies and configuration and compliance profiles • Experience with SIEM/SOAR/MDR platforms and working with managed SOCs • Experience with vulnerability management • Basic understanding of operating under a zero-trust security methodology • Technical experience with Microsoft Identity and Access	

Qualifications and/or professional membership	
Essential	**Desirable**
Good knowledge of Information Security concepts and standards Good knowledge and experience of Microsoft Azure infrastructure and security concepts and tools (Desirable qualifications include Microsoft Security and EndPoint Administration and related qualifications) Knowledge of ITIL Framework	CISSP qualification

NHG Expectations

NHG expectations framework outlines what we expect from our staff at the five different expectation levels we have across the organisation.

This role is a Colleague expectation level and therefore you should refer to the Colleague expectation profile in addition to this role profile.

The full NHG expectations framework is available on our external job site page and intranet, Milo.

You'll be assessed on the knowledge, experience, skills, and expectations criteria at various stages throughout the selection process.