# Job Description

| | |
|---|---|
| **Job title** | Cyber Security Analyst |
| **Profession** | Digital, Technology & Data Analytics |
| **Band** | E |
| **Directorate** | CIO (Information Technology) |
| **Accountable to** | IT Security Operations Lead |

**Job Purpose:**

The role helps to support the improvement of organisational resilience by reducing the likelihood and impact of SNG experiencing a serious cyber related incident. The role will be supporting the effective delivery of security operations across the organisation, ensuring compliance with industry regulations and reducing cyber risks through monitoring and maintaining the security of our systems, networks, applications and data.

Working with SNG's external security operations centre (SOC) provider, the role will ensure vulnerabilities are identified and remediated in accordance with timelines agreed with IT security assurance. Monitor security events and alerts using relevant tools and directly liaise with the external SOC to identify potential incidents. Conduct initial triage of security incidents, assessing their severity, impact and urgency and escalate potential security incidents to the Level 2 Cyber Security Analysts or Cyber Security Manager for further investigation and response.

The role will maintain accurate and detailed records of security incidents, actions taken, and outcomes to support incident reporting and analysis; and ensure all activities adhere to the standards and policies created by the IT security assurance team and that standard operating procedures (SOP) are followed meticulously.

**Financial responsibility:** No financial responsibility

**People responsibility:** No direct or indirect reports

**Autonomy:**

Within broad direction set by the IT Security Operations Lead, this role will deliver key accountabilities.

**Key Accountabilities:**

<u>Cyber Security Operations</u>

- Monitor security events and alerts using security information and event management (SIEM) tools and other relevant security technologies to identify potential security incidents.
- Conduct initial triage of security incidents, assessing their severity, impact, and urgency.

- Escalate potential security incidents to the IT Security Operations Lead for further investigation and response.
- Assist with incident response activities, following established procedures and guidelines to ensure prompt and effective incident resolution.
- Perform preliminary analysis of security events and logs to identify indicators of compromise or malicious activity.
- Collaborate with the Cyber Security Analysts and IT Security Assurance Analysts to investigate and analyse security incidents, contributing to the overall incident response efforts.
- Maintain accurate and detailed records of security incidents, actions taken, and outcomes to support incident reporting and analysis.
- Focus on vulnerability remediation across all infrastructure, working closely with the cloud infrastructure team, managed service providers, and wider CIO functions.
- Participate in vulnerability assessment and remediation activities, ensuring that identified vulnerabilities are effectively addressed.
- Collaborate with the cloud infrastructure team, managed service providers, and wider CIO functions to implement security controls and best practices.
- Stay updated with the latest cyber security threats, vulnerabilities, and mitigation techniques through continuous learning and participation in training programs.
- Contribute to the development and enhancement of security monitoring processes and procedures to improve the overall detection and response capabilities.
- Participate in regular security awareness training sessions and contribute to the organisation's security education program to promote a culture of cyber security awareness among employees.
- Monitor & analyse network, system and application logs and other data sources to detect potential security incidents in real-time.
- Quickly & effectively respond to cyber security incidents and breaches, including containing the incident, identifying the root cause and restoring affected systems and data.
- Participate in an on-call rota to provide out-of-hours support for cyber security incidents, ensuring timely response and resolution.
- Identify, assess, prioritise and remediate vulnerabilities in infrastructure, systems and apps and develop & implement effective mitigation strategies.
- Contribute to the development and maintenance of comprehensive incident response plans and procedures, ensuring their alignment with evolving security landscape and regulatory requirements.
- Maintain compliance with relevant laws, regulations and industry standards.

- Provide support to IT security assurance in evaluating the effectiveness of cyber security controls through the use of penetration testing and develop remediation strategies to improve the security posture.
- Engage with cross-functional teams across CIO and other directorates, offering your subject matter expertise in cyber security operations to guide and collaborate on strategic initiatives.

Risks and Incidents

- Participate in an internal security incident response team (SIRT), providing 24/7/365 availability across internal and external functions for all cyber security incidents.
- Support the IT Security Operations Lead in conducting robust forensic investigations, and report on cyber security breaches, providing support to functions such as HR & Communications where necessary.
- Contribute to the management and governance of all operational risks through a process of assessment, recording (via Risk Register), mitigation, and monitoring.
- Support the IT security assurance team to provide regular supplier and vendor reviews that relate to the provision of IT security services.

Projects

- Participate in project work as required.

General

- Role model SNG's values and behaviours, fostering an environment of trust, transparency, inclusion, and employee wellbeing.
- Demonstrate everyone safe and well everywhere, every day by making health and safety a primary consideration in your decision making.
- Participate in learning and development opportunities and activities that develop personal effectiveness and assist in improving performance in the role. Ensure all core and mandatory training is completed and kept up to date.
- Undertake any other duties as may reasonably be required in line with the level of responsibility of the post and to meet the changing needs of the organisation.

**Knowledge and Skills:**

Essential

- Demonstrable experience as a Level 1 Cyber Security Analyst or in a similar role within the cyber security domain.
- Demonstrate an intermediate understanding of cyber security principles, concepts, and industry best practices.
- Strong analytical and problem-solving skills, with the ability to investigate and assess security incidents effectively.
- Security relating to Cloud, Print, EUC, ITSM, Network & Infrastructure services.

- Attention to detail and thrive under pressure in a fast-paced environment, ensuring thorough incident analysis and response.

Desirable

- Professional certifications such as CompTIA Security+, Certified Cyber Security Foundations (CCSF), or Certified Information Systems Security Professional (CISSP) is highly desirable but not mandatory.
- Familiarity with security technologies such as firewalls, intrusion detection systems, and SIEM tools.
- Familiarity with network protocols, firewall configurations, and access control systems.
- Awareness of ISO 27001, NCSC Framework, Cyber Essentials Plus, OWASP.
- Security of Public and Private cloud services and providers.
- Outstanding written and verbal communication skills.
- Ability to deliver change as part of project work.
- Experience of relevant tools (e.g. M365, Cherwell, DevOps) and methodologies (e.g. Agile, TOGAF, ITIL).

*This is an overview of the job and will be periodically reviewed and updated to ensure that the job description fully reflects the responsibilities required of the post holder.*

| Version | Job code | Author | Date created/modified | Effective date |
|---|---|---|---|---|
| 1.0 | 4244 | Graham Mayers | 06/2024 | |
| 2.0 | 4244 | Steven Barber | 08/2024 | |
| 3.0 | 4244 | Steven Barber | 01/2025 | |