Information Security Analyst

Department: Chief Operating Office

Division: Modernisation and Digital

Reports to: Network Security Manager

JE Reference: COO1035

Grade: 7 **JE Date:** 21/9/2021

Job purpose

Pro-actively undertake the installation, maintenance, development and support of the organisation's cyber security technical capabillites, including security infrastructure components, cloud and data protection technologies, logging and monitoring, threat intelligence and vulnerability management solutions ensuring that all systems operate and function with a focus on customer-based delivery.

Job specific outcomes

- Assist in the maintenance of cyber security systems and platforms deployed across the environment end to end including any service deployment activities, routine upgrades and associated upgrade planning.

- Support the provision of IT administrative and other operational duties on the security solutions deployed across the environment, helping to maximise the ability of the organisation to identify, detect, respond and recover from a range of cyber attacks.

- Collaborate and work with various parties (both internal and external to the organisation) in the event of a cyber attack, to bring about an effective and timely response whilst helping to limit any operational impacts.

- Support various colleagues throughout the organisation with any investigation, remediation and/or improvement activities subsequent to a cyber incident/attack.

- Participate in the delivery of support to the Security Information and Event Management (SIEM) platform provided to the organisation by a third party supplier and contribute to the ongoing continuous improvement of the service/platform on behalf of the organisation

- Participate in the delivery of support to the Vulnerability Management platform provided to the organisation by a third party supplier and contribute to the ongoing continuous improvement of the service/platform on behalf of the organisation

- Participate in the delivery of support to the End-Point Detection & Response (EDR) platform provided to the organisation by a third party supplier and contribute to the ongoing continuous improvement of the service/platform on behalf of the organisation.

- Participate in the delivery of support to the Network Threat Intelligence platform provided to the organisation by a third party supplier and contribute to the ongoing continuous improvement of the service/platform on behalf of the organisation.

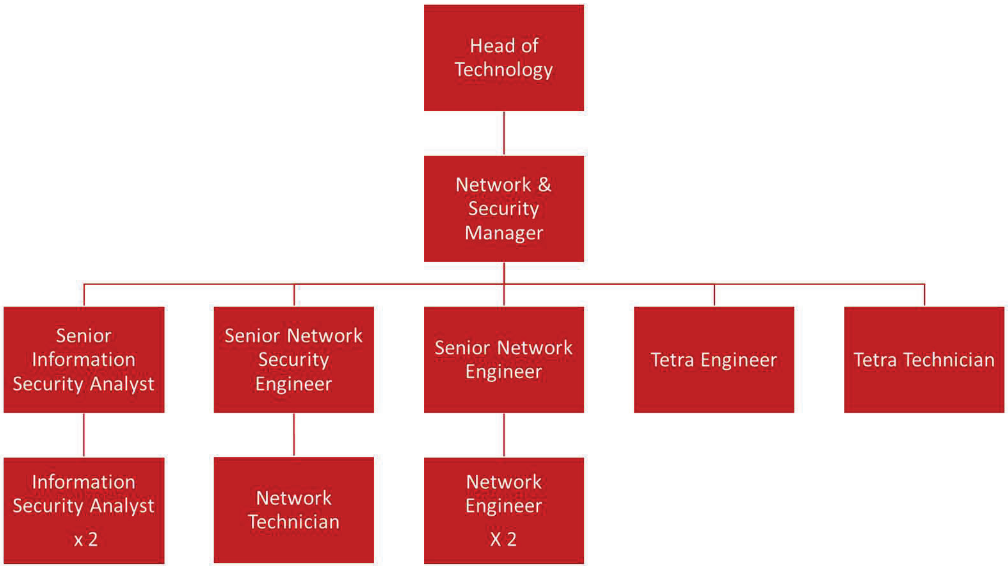
- Assist with the management of changes to the security systems and/or operational platforms, infrastructure etc. mentioned above to ensure that any impacts e.g. an increase/decrease in operational workload/demand, changes to monitoring procesess and/or incident response actvities etc. are handled appropriately.

- Support and assist in the monitoring of cyber incidents, requests for technical security services and relevant project work as instructed, following agreed processes and in line with the relevant response/resolution targets, to ensure that appropriate service levels are being maintained.

Statutory responsibilities

Active engagement, participation, and compliance with other statutory responsibilities applicable to the role, as amended from time to time

Organisation Chart


Head of Technology
Network & Security Manager
Senior Information Security Analyst
Senior Network Security Engineer
Senior Network Engineer
Tetra Engineer
Tetra Technician
Information Security Analyst x 2
Network Technician
Network Engineer X 2

Person Specification

Specific to the role

ATTRIBUTES	ESSENTIAL	DESIRABLE
Qualifications *Please state the level of education and professional qualifications and / or specific occupational training required.*	Educated to at least A-level standard in Information Technology or other relevant subject or demonstrate such a level of equivalent qualifications and experience	Industry recognised professional qualifications such as CISSP, Comp TIA CySA+, CCSP, ECIH, CEH etc. are highly desirable Additional qualifications held in relevant infrastructure, network, cloud and endpoint technologies would also be a distinct advantage e.g. MCSE, VCP, CCNA etc.
Knowledge *This relates to the level and breadth of practical knowledge **required** to do the job (e.g. the understanding of a defined system, practice, method or procedure).*	This is an entry-level role, but a high degree of interest and enthusiasm in the field of cyber security and security operations will be required in order to be successful	
Technical / Work-based Skills *This relates to the skills specific to the job, e.g. language fluency, vehicle license etc.*	Ability to understand and acquire knowledge in IT infrastructure, networks, application development and cloud computing, with a strong interest in the challenges associated with legacy systems, as well as current and emerging technologies/market trends An entry level appreciation of what it is that a Security Operating Centre does and why it would be important to the organisation in terms of mitigating the risks associated with a cyber attack A desire to learn more about developing security threats across the industry, in order to help the organisation identify and understand potential security issues that might arise	
General Skills/Attributes *This relates to more general characteristics required to do the job*	Good customer service focus, with an ability to build rapport quickly. Able to establish effective and trustful working relationships with colleagues and customers alike.	

effectively, e.g. effective written communication skills, ability to delegate, motivation or commitment etc.	Good communication skills, both written and verbal. Ability to communicate effectively with managers, peers and other colleagues/customers throughout government. Team player that works with and communicates well within and across technical teams, actively prompting respect for colleagues, sharing of skills and information and building trust amongst teams. Excellent time management skills, especially working under pressure within tight deadlines. Good organisational skills and be able to schedule their work under conflicting demands. Capable of applying strong analytical skills to their Role. Good change management skills.	
Experience *This is the proven record of experience and achievement in a field, profession or specialism.* *This could include a minimum period of experience in a defined area of work if required by an external body (for example a period of post-qualification experience).*	Whilst this is an entry level role, it would be anticipated that some background/experience working in an IT support team for a public or private sector organisation would be required.	Experience in a similar role providing support to a Security Operations Centre in a large, complex organisation.

Core Accountabilities, Attributes and Behaviour Indicators

Appointees to this role will be required to adhere to and perform their duties in line with the standards identified in the States of Jersey tier 5 core accountabilities attributes and behaviour indicators.

The standards relevant to this tier, identified in the Government of Jersey core accountabilities, attributes, and behaviour indicators, are to be attached in a separate document.