Isle of Man Civil Service Job Description	
Date changed:	7/28/26
Job Title:	Security & Networks Analyst Centre (SNAC) Analyst
Grade:	D200 / Pay Band 7
Department:	Cabinet Office
Division:	GTS
Location:	Hybrid Remote / Markwell House
Responsible To:	Security & Networks Analyst Centre (SNAC) Manager

Job Purpose	**Main Duties and Key Accountabilities** The primary purpose of this role is safeguarding the operational integrity and regulatory compliance of the Isle of Man Government (IOMG) by analysing and responding to security threats and vulnerabilities as part of a team of analysts to achieve these purposes. This team will be known as the Security and Networks Analyst Centre (SNAC) The SNAC will serve as the central hub for detecting, analysing, and responding to detected security threats raised via the SIEM tools and security investigations in conjunction with the Security and Networks Team during office hours, ensuring a coordinated defence posture across GTS IT Teams and Infrastructure. This is a technical role that requires a broad knowledge and understanding the organisation and its business needs. Duties will include, but are not limited to: • Initial threat detection, triage alerts and events and assist in response. • Analyse security incidents to assist in determining cause, scope, and impact. • Use of security tools such as SIEM, to monitor, collect and analyse data for patterns, anomalies and risks, and proposals for improvement. • Conduct regular vulnerability scans and escalate identified risks. • Collaborate with IOMG Networks partners and GTS technical operations teams on the security configuration and oversight of IOMG Infrastructure and patch management. • Provide advice on compliance and vulnerabilities. • Contributing to the development of system security policies and standards. • All work will be documented using required standards, methods and tools. It is desirable for the role holder to have an awareness of, or be prepared to gain the necessary understand, of the following. • Knowledge of tools such as Endpoint AV and Malware solutions, Tenable/Nessus, Wireshark. • Knowledge of security standards (e.g., CIS, NIST, ISO/IEC 27001). • Knowledge of firewalls, VPNs, and SIEM platforms • Microsoft Windows Server and desktops • Understanding of local and wide area networks. • Experience with Microsoft Cloud security (Azure, Sentinel, etc) is highly desirable. The post holder will be expected to hold or complete training/gain qualifications for the following or similar; • Microsoft Security, Compliance, and Identity Fundamentals • CompTIA Security+

	The following qualifications are also desirable. • Microsoft Security Operations Analyst Associate • Cisco Cybersecurity Associate Certification • Identity and Access Administrator Associate The post holder shall perform such duties and observe and conform to such reasonable instructions as the Department, or person duly authorised by the Department, may from time to time give.

Main Activities	**Monitoring and detection of security events** • Monitoring networks and systems for patterns, anomalies and suspicious behaviour. • Detecting, triaging and escalating and security risks and incidents. You will ensure that they are conducted in accordance with agreed standards and procedures. • Using management tools and collaborating with other specialists, you will assist with the collection of trend and performance data and statistics to evaluate risks and anomalies. **Reporting** • All work will be documented using required standards, methods and tools. • Documenting insights on the current risks, threats, trends, and providing advice for improvement. • Analyse security incidents to determine root cause, scope, and impact, you will provide advice on preventative measures. **Vulnerability assessments and audit** • Conduct proactive vulnerability scans, you will coordinate and track remediations and validate fixes. • Monitoring the external environment, you maintain a broad understanding and identify emerging technologies, threats and opportunities for improvements. **Tool Management** • Configuring, operating and maintaining tools like SIEM, and SOAR to detect and respond to threats. • Ensure continuous collection of logs from various sources. • Assist with creation and maintenance of automated response workflows and detection events within security platforms to streamline incident response. • Assist with refining and fine-tuning existing security tools to improve efficiency and reduce false positives. • Maintain uptime, performance, and reliability of monitoring tools.

Management of Staff and Resources	The role holder does not have management of Staff or Resources.
Other Information	This post requires a Security Check clearance in accordance with GTS Vetting Policy. All members of the Division are accountable for the responsible handling of Government Information as defined by Government and Divisional policies, procedures and guidelines. Any officer who knows of or suspects a breach of information systems security must

	report the facts immediately to the Information Security Officer. This document is intended to be a guide to the general scope of duties and not a rigid, inflexible specification. The employee shares with the employer the responsibility for suggesting alterations to the scope of duties to improve the work situation. This role description will be reviewed as necessary to reflect the future requirements of the GTS and the Cabinet Office.
Performance Management & Improvement	All Civil Servants have a personal responsibility for performance management, and their own personal development. The role holder will also be expected to contribute fully to performance reviews.
Reporting Framework	The role holder reports to the Security & Networks Analyst Centre (SNAC) Manager, Government Transformation Services.
Management Authority under relevant procedures	The delegation of Management Authority for Officers within GTS has been granted by the Executive Director of GTS and: • is to be exercised in respect of the staff within their individual span of control • is applied with the express agreement of the Executive Director of GTS Disciplinary Procedure • Oral Warning ***D400 and above*** • Written Warning ***D400 and above*** • Final Written Warning ***D600 and above*** • Suspension ***D600 and above*** Capability Procedure • Oral Warning ***D400 and above*** • Written Warning ***D400 and above*** • Final Written Warning ***D600 and above*** • Suspension ***D600 and above*** Grievance Procedure • Stage 1 ***D400 and above*** • Stage 2 ***D500 and above*** • Stage 3 ***D600 and above***
Integrity	All staff of the Cabinet Office are expected to recognise that the everyday business of the Cabinet Office requires the highest level of personal integrity. Each Officer has a personal responsibility to maintain the confidentiality of all Government and client information and ensure the protection of the international reputation of the Isle of Man.
Health & Safety	It is the duty of every employee to take reasonable care for the Health & Safety of themselves, and others including the use of necessary devices and protective clothing and co-operate with management in meeting its responsibilities under the Health & Safety at Work Regulations. Any failure to take such care or any contravention of safety policy or managerial instructions in this area may result in disciplinary action being taken.

Core behavioural skills	**Collaboration & communication**	Able to work alone and with colleagues, understands the need to collaborate with team. Interacts with customers, suppliers and partners and is aware of the need to represent customer needs. Has sufficient oral and written communication skills for effective engagement with colleagues and internal users/customers. Facilitates collaboration between stakeholders who have diverse objectives.
	Creativity & problem solving	Demonstrations analytical thinking and creatively applies innovative thinking in analysing and identifying solutions and making recommendations. Engages and coordinates with subject matter experts to resolve

		complex issues as they relate to customer/organisational requirements. Demonstrations strong analytical thinking and
	Decision making	Uses limited discretion in resolving issues or enquiries. Knows when to seek guidance in unexpected situations.
	Learning & professional development	Develops a wider breadth of knowledge across the industry or business. Takes initiative to advance own skills. Absorbs new information when it is presented systematically and applies it effectively.
	Planning & execution	Plans own work within short time horizons. Demonstrates an organised and rational approach to work. Performs a range of work activities in varied environments. Understands and uses appropriate methods, tools, applications and processes. Is fully aware of and complies with essential organisational security and ethical practices expected of the individual. Has sufficient digital skills for their role. Interacts with and may influence immediate colleagues.

Level of responsibility	**Autonomy Level 2**	Works under routine direction. Uses limited discretion in resolving issues or enquiries. Determines when to seek guidance in unexpected situations. Plans own work within short time horizons.
	Influence Level 2	Interacts with and may influence immediate colleagues. May have some external contact with customers, suppliers and partners. May have more influence in own domain.
	Complexity Level 2	Performs a range of work activities in varied environments. May contribute to routine issue resolution. May apply creative thinking or suggest new ways to approach a task.
	Business Skills Level 2	Understands and uses appropriate methods, tools and applications. Demonstrates a rational and organised approach to work. Has sufficient communication skills for effective dialogue with customers, suppliers and partners. Is able to work in a team.
	Knowledge	Demonstrates application of essential generic knowledge typically found in industry bodies. Absorbs new information when it is presented systematically and applies it effectively. Takes initiative to advance own skills and identify and manage development opportunities in area of responsibility. Achieves required level of training for the role.