NON-CONTRACT ROLE DESCRIPTION

JD5798

ROLE TITLE:	Senior Technical Analyst, Security Operations	**ROLE DESCRIPTION NO.:**	5798
DEPARTMENT:	Information Management/Information Technology	**HEABC REFERENCE NO.:**	18721829
REPORTING TO:	Manager, IM/IT Security	**HSCIS CODE:**	05050
CLASSIFICATION:	NCEM/Range 7	**JOB CODE:**	91789

ROLE SUMMARY

In accordance with the Vision, Purpose, and Values, and strategic direction of the Vancouver Island Health Authority (Island Health) patient and staff safety is a priority and a responsibility shared by everyone; as such, the requirement to continuously improve quality and safety is inherent in all aspects of this position.

Reporting to the Manager IM/IT Security, the Senior Technical Analyst (STA), IM/IT Security works as a senior technical resource primarily supporting the delivery of operational security tools and technologies for Island Health.

The STA provides the senior technical skills required and is responsible for the daily management, integration, technical delivery, and support of Island Health s Security Incident and Event Management solution, Web Security Gateway, Intrusion Prevention, Vulnerability Management and Forensic investigation tools. The STA provides guidance and direction to members of the security operations team, represent security operations with respect to initiatives and projects within Island Health and IM/IT, as well as act as the senior resource responsible for the analysis, development, implementation, and maintenance of security operations systems and any related layered products, utilities and hardware.

This effort includes ongoing response to Service Desk incidents and problems as well as strict adherence to Island Health s ITIL-based Change Management policies and processes. This role will be expected to have the skills necessary to manage and maintain the operational environment of our security operations infrastructure and will also be a key resource on behalf new initiatives such as planning and implementing upgrades to existing technologies as well as challenging new projects and technologies.

DUTIES AND RESPONSIBILITIES:

1. Works with the IM/IT Security team, as well as the Manager, IM/IT Security to develop the vision, architecture, and roadmap for the security operations tools and technologies.

2. Directs, leads, and supports the installation, configuration, and ongoing operations of the security operations infrastructure and technologies.

3. Assist the Manager, Technical Services and Manager, IM/IT Security with technical decision-making processes, writing RFPs and developing briefing notes for Executive, yearly budget planning, as well as participate in HR recruitment and hiring processes, as it relates to the security operations team.

4. Functions, with minimal supervision, as the senior resource within the security operations team by providing leadership to team members as well as day-to-day administration and support of a complex, integrated suite of security operations tools and technologies.

5. Establish and execute incident response methods, tools and processes which provide the organization value by reducing risk.

6. Identify, triage and prioritize security events, incidents, and vulnerabilities based on organizational risk.

7. Conducts problem identification and issue resolution of the supported technologies following industry best practices and leveraging Island Health's IM/IT incident and change management procedures and processes.

8. Develops, prepares, and maintains technical documentation specific to Island Health's implementation of any Security Operations technologies.

9. Monitors and reports on the performance and service delivery of the Security Operations infrastructure by implementing appropriate monitoring and reporting tools and processes.

10. Develops, implements, and monitors Island Health's and IMIT's compliance to standards, strategies, and business plans to ensure availability and security as it relates to Security Operations services.

11. Performs other related duties as assigned.

QUALIFICATIONS:

Education, Training And Experience

A level of education, training and experience equivalent to graduation from a recognized degree or diploma program in Computer Science, with five (5) years' recent related experience (such as administering security technologies including but not limited to Advanced Malware detection, FirePower IPS, Cisco WSA, Tenable Vulnerability Scanner, Sentinel & LogRhythm SIEMs and Forensics tools)

Skills And Abilities

- A broad, senior level of technical knowledge in relation to information systems, networking and technical architecture.
- Active CISSP, SANS GIAC, and/or industry recognized computer forensics certification strongly preferred.
    - Ability to communicate effectively both verbally and in writing.
    - Ability to deal with others effectively.
    - Physical ability to carry out the duties of the position.
    - Ability to write programs in a variety of programming languages.
    - Ability to organize work.
    - Ability to operate related equipment.