Job Description

Position Identification			
Position Title	Senior IT Security Analyst		
Position Replaces	IT Security Analyst		
Position Level	Employee	**Position Code**	1396
Pay Group	Group 12	**Date (last revised)**	Jun-25
Supervisor Title	Manager, IT Security and Compliance	**Sup. Position Code**	1626
Additional Requirement	CRC	TMA	
Division	Information Technology	**Flexible Work Arrangement**	Flexible Work

Organizational Description

BC Transit is a provincial crown corporation responsible for the overall planning and delivery for all of the different municipal transportation systems within British Columbia, outside Greater Vancouver.

Our Mission: Delivering transportation services you can rely on

Department Summary

The IT Security & Compliance team plays a critical role in safeguarding BC Transit's information assets. We achieve this through developing & enforcing security policies, security architecture design, real-time security monitoring, security awareness training, and collaboration & communication.

Job Overview

Reporting to the Manager, IT Security and Compliance, the Senior IT Security Analyst is responsible for collaborating with a group of cyber security specialists who are proficient in all elements of technology and cyber security. This role will perform forensic analysis, investigation, and troubleshooting to locate, fix, and report cyber security-related problems. This includes performing threat simulations to identify potential risks and offer remediations, as well as doing risk analysis and analyzing mitigation solutions for cyber security vulnerabilities. Incumbents will also be able to examine and resolve issues with a variety of security platforms, including firewalls, identity management systems, and endpoint detection and response (EDR), etc.

Key Accountabilities and Expectations	
Key Accountability	**Expectation**
Strategy and Planning	• Participate in the planning and design of enterprise security architecture, under the direction of the Manager IS&T, Enterprise Technology and Security Services and in collaboration with other subject matter experts and technical roles within the IS&T department where appropriate • Participate in the creation of enterprise security documents (standards, baselines, guidelines and procedures) • Participate in the planning and design of an enterprise Business Continuity Plan and Disaster Recovery Plan • Maintain and enhance the enterprise's security awareness training program
Acquisition and Deployment	• Maintain up-to-date detailed knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the development of new attacks and threat vectors • Research and support the acquisition of security solutions or enhancements to existing security solutions to improve overall enterprise security • Perform the deployment, integration and initial configuration of all new security solutions and of any enhancements to existing security solutions in accordance with standard best operating procedures generically and the enterprise's security documents specifically
Technology	• Maintain and implement complex technical security controls and processes in support of BC Transit's Information Security Management System • Maintain up-to-date baselines for the secure configuration and operations of all in-place devices • Maintain operational configurations of all in-place security solutions as per the established baselines and operate them accordingly as well as influence and collaborate with other teams • Participate in the design and execution of vulnerability assessments, penetration tests and security audits • Review logs and reports of all in-place devices, Interpret the implications of that activity and devise plans for appropriate resolution • Work with the SOC (Security Operations Center) team to investigate complex flagged events • Configure security measures and software to protect systems and information infrastructure

	• Configure applications that detect and mitigate vulnerabilities (network, OS, web and on-prem applications, etc.) • Support the OS and applications patch management process for compliance • Support internal and external security audits and penetration testing activities • Provide support for end users for all in-place security solutions • Monitoring, review, and handle security related ITSM tickets and escalate as required • Provide security advice across all technology, databases, servers, applications, cloud services, etc. as appropriate
Operational Management	• Ensure the confidentiality, integrity and availability of the data residing on or transmitted to/from/through enterprise workstations, servers and other systems and in databases and other data repositories. • Determines security violations and inefficiencies by conducting periodic audits • Monitor and manage all in-place security solutions for efficient and appropriate operations • Investigate any problematic activity and manage all security related incidents to resolution.
Additional Duties	• Performs related duties in keeping with the purpose and accountabilities of the job

Summary of Qualifications and Job Specific Competencies	

Education	• Post secondary diploma in Information Technology
	• Completion of Two or more of the following certifications is considered an asset:
	  ○ Certified Information Systems Security Professional (CISSP)
	  ○ CompTIA CySA+
	  ○ ISC2 Systems Security Certified Practitioner (SSCP)
	  ○ Certified Ethical Hacker (CEH)
	  ○ ISACA Certified Information Systems Auditor (CISA)
	  ○ CompTIA Security+
	  ○ GIAC Certified Incident Handler (GCIH)

Experience	• Five (5)) years related experience in managing enterprise level information security. • Extensive experience with malware detection and endpoint protection solutions Extensive experience with intrusion detection systems (IDS/IPS) and cybersecurity tools • Extensive experience in enterprise network architecture, design, and support

	• Proven experience in designing enterprise security architecture • Experience in developing and maintaining enterprise security documentation • Experience designing and delivering security awareness training programs for employees • Experience developing and implementing Business Continuity and Disaster Recovery Plans (BCP/DRP) • Hands-on experience with enterprise monitoring and alerting solutions • Strong understanding of networking protocols including IP, TCP/IP, and related technologies • Familiarity with enterprise environments using Windows Server, VMware, Cisco technologies, and network-attached storage (NAS/SAN) • An equivalent combination of education and experience may be considered
Key job-specific competencies	• Solid understanding of network segmentation, VLANs, and enterprise network architecture, with strong knowledge of TCP/IP and related network protocols • Strong knowledge of IT security best practices, frameworks (e.g., NIST, ISO), processes, and tools • Proficiency with Active Directory and Azure AD (Entra ID) configurations, and familiarity with major operating systems including Windows (client/server), Linux, and macOS • Demonstrated ability to prioritize and execute tasks effectively in high-pressure or time-sensitive environments • Strong investigative, analytical, and problem-solving abilities, with a detail-oriented approach • Excellent communication skills—both written and verbal—with the ability to convey technical information to non-technical audiences