



Position Title: Cyber Security Analyst

Position Status: Full-Time Regular

Department: Corporate Services

Employee Group: Teamsters Local 31

Location: 4515 Central Boulevard, Burnaby

Salary Range/ Wage Rate: PG T29 \$4,054.93 - \$4,794.43 bi-weekly

Our Corporate Services Department is seeking a Cyber Security Analyst who will play a key role in protecting the organization from evolving cyber threats and strengthening our overall security capabilities. The ideal candidate will bring cybersecurity experience in areas such as threat detection, incident response, security operations, and risk management.

You are an experienced cyber security professional with strong technical expertise in security architecture, network and cloud security, threat and risk assessment, vulnerability management, and incident response. You are a strategic and analytical thinker who can identify emerging risks, navigate complex security challenges, and develop practical solutions. A collaborative and trusted advisor, you communicate complex technical concepts clearly, build strong relationships with technical and non-technical stakeholders, and bring a proactive, solutions-focused approach to protecting our organization.

This role:

- Participates in the development of enterprise wide security architectures and in the development of cyber security standards; performs baseline assessments on cyber security; provides cyber security consultation; conducts cyber security risk assessments and enterprise wide health checks; researches cyber security threats and responds to real or suspected cyber security incidents; maintains the enterprise cyber security risk register; and performs cyber security forensic activities as required.
- Conducts cyber security investigations and activities related to the response protocols; develops and implements the annual cyber security awareness campaigns; provides the cyber security awareness presentations, associated materials, and online training.
- Conducts ongoing compliance assessments; manages and maintains security related rules; conducts vulnerability scanning and penetration testing for all network and/or internet connected systems; and develops and implements risk mitigation plans.

- Acts as key team member for the development, coordination, and implementation of large or complex cyber security related to hardening, certification and accreditation of new and existing IT systems, cloud adoption strategy and security; and manages and oversees the work of third-party consultants.
- Responds to emergency or trouble calls during working and after hours; investigates and assesses security incidents, data breaches, or emergency changes related to mitigating security risks; and arranges for corrective action where possible.
- Provides advice, assistance and training to staff on technical matters; and may oversee and direct the work of subordinates engaged in skilled technical work.
- Performs related work as required.

To be successful, you have:

- University degree in computer science, engineering or other relevant discipline, considerable related experience, including network security management; or an equivalent combination of training and experience.
- Thorough knowledge of security architecture and cyber security standards.
- Thorough knowledge of network security practices and techniques including antivirus, IPS, and firewalls configuration and maintenance.
- Thorough knowledge of email, web, cloud security, identity and access management.
- Thorough knowledge of wired and wireless network access control and of industrial controls security.
- Considerable knowledge of data protection policies, procedures and products.
- Considerable knowledge of vulnerability scanning and penetration testing.
- Considerable knowledge of security threat and risk assessment and threat modeling.
- Considerable knowledge of security event and incident management.
- Considerable knowledge of the functions of departments served and their requirements as applied to the work performed.
- Sound knowledge of mobile security and mobile device management.
- Sound knowledge of PCI compliance and micro segmentation.
- Ability to establish and maintain effective working relationships with a variety of internal and external contacts and to provide advice, information and assistance to same.
- Ability to communicate effectively both orally and in writing.
- Ability to think analytically and problem solve.
- Ability to develop presentations and training material and present and train others on relevant information.
- Ability to work well in a team environment.
- Driver's Licence for the Province of British Columbia.

Our Vision:

Metro Vancouver embraces collaboration and innovation in providing sustainable regional services that contribute to a livable and resilient region and a healthy natural environment for current and future generations.

Metro Vancouver employees proudly serve the region and demonstrate the behaviours and attributes of six leadership competencies: Accountability, Adaptability, Building and Nurturing Relationships, Communication, Continuous Learning, and Strategic Thinking and Action.

At Metro Vancouver, we are committed to cultivating a diverse, safe, equitable, and inclusive work environment for all. We strive to attract and retain a talented, diverse workforce that is reflective of the region we serve. If an accommodation is required during the recruitment and selection process, please contact careers@metrovancover.org for support. Learn more about our commitments to diversity, equity, and inclusion [here](#).

Please follow this link <https://metrovancover.org/about-us/careers> to our Careers page where you can submit your application by October 19, 2026.