

Job Title	Senior Specialist Cyber Architecture
Division	Office of the Chief Information Security Officer
Reports To	Manager Strategy & Architecture
Salary Range	\$110,947.20 to \$130,353.60
Work Location	55 John Street, Toronto
Job Type	Permanent Full Time
Shift Information	Monday to Friday, 35 hours work week

JOB SUMMARY:

To support the execution of the Chief Information Security Officer's (CISO) mandate, cyber vision and strategy, providing technical and business advice, support and services to all City divisions, agencies and corporations.

To define, develop and support cyber programs and initiatives, engaging with teams across the organization to build alignment on key projects and develop execution roadmaps.

To provide subject matter expertise, strategic advice, senior level guidance and operational support for Cyber Architecture area within the Cyber Diplomacy & Governance section.

MAJOR RESPONSIBILITIES:

- Leads the development, deployment and management of the City's cyber architecture of applications, programs and initiatives.
- Works with clients to design, build, implement and integrate complex and sustainable cyber capabilities.
- Architects security solutions and frameworks, using cloud-based technologies where feasible.
- Develops, implements and maintains security standards and procedures, including application and infrastructure hardening guides and best practices for key infrastructure.
- Participates in the information security governance process.
- Conducts cyber risk assessments of planned initiatives/projects across the organization and produces reports articulating potential risks.
- Reviews and implements management's action plans for cyber-related risk assessments

QUALIFICATIONS/CERTIFICATIONS:

- Post-secondary degree in Technology or a related discipline.
- Over 6 years experience in Cyber Architecture.
- In-depth knowledge of architectural design and implementation methodologies including software, network and infrastructure.
- Excellent understanding of data centre technologies including network, compute, storage, virtualization, containers and enterprise application stacks.

- Excellent understanding of the cyber-kill chain model and associated technologies, and detection/mitigation techniques such as firewalls, traffic scrubbing, signature-based detection and 0-day detection.
- Expertise in performing threat modeling exercise and security control design analysis
- Proficient in building and maintaining documented target security architectures, roadmaps, blueprints, patterns, and standards
- Extensive experience with common information security management frameworks, such as International Standards Organization (ISO) 27001, National Institute of Standards and Technology (NIST) cybersecurity framework and other leading edge security frameworks.
- Preferred Certifications (any two in the list): CISSP, TOGAF, SABSA, AWS/Azure Certifications.

SKILLS:

- Ability to work in transformative programs.
- Ability to lead efficient communication between all project stakeholders, including internal teams and clients
- Ability to achieve business objectives through influencing and effectively working with key stakeholders.
- Excellent written & verbal communication skills (comfortable & confident communicating at all levels including business partners, leadership and vendors).
- Excellent problem-solving skills with capability to identify solutions to unusual and complex problems.
- Keen attention to detail and strong organizational skills.
- Highly organized, proactive, self-motivated team player who takes initiative and is able to work independently.
- Ability to work in a fast-paced environment managing multiple priorities with proven time management skills.
- Strong analytical skills and ability to prioritise and multitask.
- Ability to prioritize and effectively manage competing priorities and projects.
- Ability to manage multiple initiatives while adhering to strict deadlines.
- Able to work extremely well under pressure while maintaining a high level of professionalism
- Self-motivated person with desire to go above and beyond tasks
- Transferable skills, like communication and decision-making, are equally important.
- Being able to think on your feet and show good judgment are especially valuable in this field. "Security pros should always be ready to react to cyber-related incidents quickly.

ADDITIONAL COMMENTS/INFORMATION:

A normal work week is 35 hours, however, unforeseen situation may require extended hours of work with little or no prior notice. In case of a cyber incident or breach, rotation shift, continuous extended hours may be required with little or no prior notice.

*Subject to a police check, background check, psychological assessment and/or any other checks on a regular basis as the Office of the CISO handles highly sensitive and confidential information.

EQUITY, DIVERSITY AND INCLUSION

The City is an equal opportunity employer, dedicated to creating a workplace culture of inclusiveness that reflects the diverse residents that we serve. Learn more about the City's commitment to employment equity.

ACCOMODATION

The City of Toronto is committed to creating an accessible and inclusive organization. We are committed to providing barrier-free and accessible employment practices in compliance with the Accessibility for Ontarians with Disabilities Act (AODA). Should you require Code-protected accommodation through any stage of the recruitment process, please make them known when contacted and we will work with you to meet your needs. Disability-related accommodation during the application process is available upon request. Learn more about the City's Hiring Policies and Accommodation Process.