Job Title:	Senior Enterprise Security Architect		
Job Opening Id:	44054	**# Required:**	2
Business Unit:	Corporate Services	**Division:**	I.T. Solutions
Location:	Headquarters Campbell West	**Standard Hours:**	35.00 / week
Full/Part Time:	Full-Time	**Regular/Temporary**:	Regular
Salary Grade:	7	**Salary Range:**	$115,940 - $ 136,400
Post Date:	2025-12-16	**Close Date:**	2026-01-18

About Us

Serving a diverse urban and rural population of more than 475,000, Niagara Region is focused on building a strong and prosperous Niagara. Working collaboratively with 12 local area municipalities and numerous community partners, the Region delivers a range of high-quality programs and services to support and advance the well-being of individuals, families and communities within its boundaries. Nestled between the great lakes of Erie and Ontario, the Niagara peninsula features some of Canada's most fertile agricultural land, the majesty of Niagara Falls and communities that are rich in both history and recreational and cultural opportunities. Niagara boasts dynamic modern cities, Canada's most developed wine industry, a temperate climate, extraordinary theatre, and some of Ontario's most breathtaking countryside. An international destination with easy access to its binational U.S. neighbour New York State, Niagara attracts over 14 million visitors annually, as well as a steady stream of new residents and businesses.

At Niagara Region, we value diversity - in background and experience. We are proud to be an equal opportunity employer. We aspire to hire and grow a workforce reflective of the diverse community we serve. By doing so, we can deliver better programs and services across Niagara.

We welcome all applicants! For more information about diversity, equity, and inclusion at Niagara Region, *Diversity, Equity and Inclusion - Niagara Region, Ontario* or email related questions to diversity@niagararegion.ca. To send input on reducing barriers in the current hiring process, please email myhr@niagararegion.ca

For the Region's full employee equity statement, Working at Niagara Region - Niagara Region, Ontario.

Don't have every qualification? You may be hesitant to apply if you do not have every qualification listed in the posting. While specific qualifications are important for certain roles, we invite individuals from diverse

backgrounds and varying levels of experience and education to apply. Our recruiters will evaluate your suitability for the role.
Please note that for unionized roles, we must follow collective agreement requirements. However, we encourage all interested candidates to submit their applications. We believe success in a role can extend beyond meeting every single requirement

Job Summary

Reporting to the IT Security Manager, the Senior Enterprise Security Architect is responsible for leading the technical design, strategy, and overall insight related to the planning and implementation and validation of new or updated enterprise security environments and services. This role is responsible for leading the logistical development and integration of network and security policies and systems across the IT department, as well as ensuring strategic alignment of enterprise IT standards, practices, and policies. This position will also assess, design, develop, and implement various security, network, threat, vulnerability and incident response disciplines, shared services solutions, and will also be the primary subject matter expert for security related requests.

Important Notices:

- *This position currently falls within our hybrid model, allowing the employee to typically work a minimum of 50% of your time at your regular work location and the other 50% of time at home.*

Education

- Bachelor’s degree in information technology, Computer Science or related discipline
- Post-Secondary courses in any of the following: computer forensics and security, cloud architecture and security is preferred.
- One or more cyber security certifications (CISSP, CISM, CEH, CCSP, CSSLP, OSCP,) is preferred
- One or more architecture certifications (Azure Solutions Architect, Azure Cyber Security Architect, SABSA, TOGAF, CISSP-ISSAP) is preferred
- Microsoft Azure Network Engineer, Azure Security Engineer Associate is considered an asset
- PMP certification is considered an asset
- An equivalent combination of education and experience may be considered.

Knowledge

- 10 years’ experience in Information Systems and Technology in a medium-to-large-sized data center and network security and design environment focused on:
- Microsoft products, such as Entra, Active Directory, Windows Operating Systems, , Office Productivity Suites, Security Product Suites,
- Network appliances and technologies i.e. CISCO, Aruba,VPN, Load Balancing, NAC Security appliances and technologies i.e. NextGen Firewalls (NGFW), Web Application Firewall (WAF), , PAM, Vulnerability Management tools, Exposure Management solutions, and Web Application Scanning tools
- Threat Management technologies i.e. Cortex XDR, Microsoft XDR, SIEM solutions (e.g. Azure Sentinel, Splunk), external threat monitoring tools, and SOAR/AI technologies
- 5 years of experience in disaster recovery planning and incident response planning.
- In-depth knowledge of data center environments and security related tools and technologies, security best practices and policies, and IT compliance and regulations.
- 5 years of project leadership or management experience is preferred.
- In-depth knowledge of Security Operation Centers (SOC).
- Experience with PCI-DSS compliance.

- Experience in monitoring the threat landscape, mapping potential applicable threats, and ethical hacking methodologies, including threat hunting methods
- Experience with application security, and programming/scripting skills using Python, PowerShell, and other programming languages
- Experience in vulnerability assessment of end points, switches, routers, gateways, servers, storage, storage area networks, firewalls, applications, web services, cloud services, etc.
- Experience with Azure Cloud technologies, and cloud security products (CASB, SASE, SSE) including email security
- Maintain currency of knowledge on current and emerging security trends, including but not limited to cloud-based services, IoT, etc.
- Understanding of IT information, process, system, technology architectures and models
- Good oral, written, interpersonal and organizational skills
- Strong analytical, reasoning and problem-solving skills

Responsibilities

IT Security Strategy and Design (25% of time)

- Designs, implements, and provides on-going support of enterprise-wide infrastructure architecture(s) and data/ security systems integrations.
- Provides security related planning and technical direction and consultation for data center and disaster recovery sites, including: wide area network, server infrastructure, storage, backup, disaster recovery .
- Evaluate, identify, document, and assess process functions, security weaknesses, vulnerabilities and controls.
- Coordinates and leads the development of business case proposals for IT Security initiatives in conjunction with input by other IT peers and departments.
- Provides key concepts and expertise towards the development of long-term security strategies to ensure the confidentiality, integrity, and availability of the overall enterprise IT infrastructure .
- Acts as technical lead and participates in committees and work groups across areas and departments to address specific projects and issues.
- Provides IT Security architectural expertise, advice, direction, and assistance to the IT team.

Disaster Recovery, Business Continuity and Incident Response – Design and Problem Solving (20% of time)

- Ensures the availability of all critical corporate infrastructure technologies and highly sensitive data such as Financial Systems, Microsoft Messaging, mobile device management services and all externally public facing systems hosted at and for the Region.
- Collaborates in the architectural design and implementation of complex enterprise disaster recovery plans in accordance with established recovery time objectives and recovery point objectives.
- Identifies vulnerable areas within the Region's critical infrastructure functionalities and provide/execute on those recommendations.
- Recommends and implements disaster avoidance and business impact reduction strategies.
- Directs and coordinates staff and other departmental key staff for testing of disaster recovery and incident response playbook strategies.
- Develops and leads the implementation of an incident reporting system as it relates to the network and system security infrastructure.

Security Network and Administration – Design and Strategy (10% of time)

- Champions network design and administration tasks for the primary and secondary disaster recover sites, and develops the guiding principles and framework which establishes network and integration standards, continuous improvement methods, and security models
- Designs network solutions for the Niagara Region or external invested parties, ensuring the integrity, security, and safeguarding of data is completed by applying a complex set of disciplines in the process. Incorporates and uses the base foundation of the CIA (availability, integrity, and confidentiality) model to mitigate data leakage risks, or exposure of Niagara Region's network and server systems internally or externally
- Designs and implementation of security tools with data, performance and availability in mind to minimize traffic bottlenecks, and to ensure appropriate sizing .
- Leads the research on emerging products, services, protocols, and standards in support of contingency planning and development efforts and recommends technologies that will increase cost effectiveness, systems flexibility, integrate seamlessly into the enterprise environment.

Security and Administration – Design, Implementation and Operation (30% of time)

- Defines security frameworks for existing and new systems which include developing, implementing, maintaining policies, standards, guidelines, and procedures.
- Establishes, and implements a breach management policy and response plan. Deals with issues that are abstract in nature, and not easily identifiable. Able to disseminate changing data on the fly, in order to thwart any given attack method utilized. Identifies and assembles ad-hoc mitigation plans when required.
- Designs and defines methods to ensure encryption standards are formulated and standardized in order to safeguard data integrity and confidentiality.
- Monitors security logs from technical security controls for intrusion detection.
- Determines and implement log aggregation and analysis strategies for distributed system and network security devices.
- Actively recommends changes to establish methods and procedures, suggests alternative solutions and new methods to improve quality and increase productivity.
- Works with IT team to design, co-ordinate, and direct activities to implement and maintain a network security infrastructure including wired and wireless systems and handheld mobiles, against internal and external intrusion threats.
- Implements security services (firewalling, EDR – endpoint detection/response), identities and accesses management products (PAM), anti-virus, anti-spam, trusted time sources, content management, file integrity tools, audit and IDS products, and encryption tools.
- Performs Cyber Threat and Vulnerability management tasks in accordance with established programs and directed by the IT Security Manager
- Conducts regular review of Indicators of Attack (IoAs) and Indicators of Compromise (IoCs) derived from all available sources (e.g., SIEM, NGFW, Logs from Systems and Security Tools) to assess the real and material threats and vulnerabilities
- Performs ethical hacking activities at the direction of management, as well as perform programming, and related scripting duties
- Tunes the SIEM, and all security related tools to recognize real and actionable threats from security information and events collected
- Creates playbooks to automate the response for actionable threats and link them to risk objects
- Optimizes the collection, processing, and analysing parameters to improve the efficiency of the SIEM, XDR, and security technologies

- Creates and evolve new/existing rules in security tools to accommodate new and evolving threats
- Performs proactive threat hunting in a systemic and iterative manner throughout the environment to detect and isolate threats
- Performs threat-based risk assessments on systems and services and effectiveness of controls
- Assesses discovered/identified threats, obtained through subscribed feeds and recommend appropriate actions to reduce exposure and ensuring risks remains within the tolerance levels
- Reviews, develop and report on appropriate metrics for the Threat/Vulnerability Management solutions, performance, exception and compliance and ensure continuous improvements of such metrics
- Develops and document guidelines, processes and procedures for review and approval and implement approved procedures to secure IT environment
- Liaises between departments to develop and implement approved security standards and guidelines
- Maintains broad awareness of threat and vulnerability trends including changes to legislations and regulatory frameworks
- Raises awareness of good security practices to all levels of the organization and perform security awareness and learning duties as directed
- Advises on security practices for all IT projects as required

Policy and Guiding Principles Development (15% of time)

- Develops policies (i.e. Incident Response, Data Encryption policies), including the research, analysis, consultation and synthesis of information to produce the recommendations.
- Enforces data center security guidelines, processes, policies and change controls to promote the stability, efficiency, and effectiveness of regional infrastructure.
- Informs and mentors other staff members on their responsibilities concerning IT business policies and procedures, and accompanying emergency response documentation.
- Ensures effective corporate and regional policies and standards are followed, in co-ordinance with current network internal/external controls.
- Contributes to the creation and sustainment of technology frameworks (e.g. regional/corporate architectures, methodologies, tools, techniques and standards).
- Assist and provide input into policies and processes around data security and business continuity, with a focus on best practices and techniques.

Perform other related duties and responsibilities as assigned or required.

Special Requirements

- In accordance with the Corporate Criminal Record Check Policy, the position requires the incumbent to undergo a Criminal Records Check and submit a Canadian Police Clearance Certificate.
- Must maintain ability to travel in a timely manner to other offices, work locations or sites as authorized by the Corporation for business reasons.
- May be required to support emergency operations under the incident management structure, at the direction of the Emergency Operations Centre Director
- Regional staff strive to enable the strategic priorities of council and the organization through the completion of their work. Staff carry out their work by demonstrating the corporate values.

How to Apply

Regional staff strive to enable the strategic priorities of council and the organization through the completion of their work. Staff carry out their work by demonstrating the corporate values. To view the full job description, requirements and apply on our Careers Site, visit our Careers page - Job Opening **#44054** (https://www.niagararegion.ca/government/hr/careers/)

Uncover the wonder of the Niagara Region and join a team dedicated to meeting tomorrow's challenges, today!

Let us know why you would be an excellent team member by submitting your online application no later than **January 18, 2026,** before midnight by visiting our 'Careers' page at www.niagararegion.ca. We thank all candidates for their interest however, only those candidates selected for an interview will be contacted.