



# Indigenous.Link

Canada's fastest growing Indigenous career portal, Careers.Indigenous.Link is pleased to introduce a new approach to job searching for Indigenous Job Seekers of Canada. Careers.Indigenous.Link brings simplicity, value, and functionality to the world of Canadian online job boards.

Through our partnership with Indigenous.Links Diversity Recruitment Program, we post jobs for Canada's largest corporations and government departments. With our vertical job search engine technology, Indigenous Job Seekers can search thousands of Indigenous-specific jobs in just about every industry, city, province and postal code.

Careers.Indigenous.Link offers the hottest job listings from some of the nation's top employers, and we will continue to add services and enhance functionality ensuring a more effective job search. For example, during a search, job seekers have the ability to roll over any job listing and read a brief description of the position to determine if the job is exactly what they're searching for. This practical feature allows job seekers to only research jobs relevant to their search. By including elements like this, Careers.Indigenous.Link can help reduce the time it takes to find and apply for the best, available jobs.

The team behind Indigenous.Link is dedicated to connecting Indigenous Peoples of Canada with great jobs along with the most time and cost-effective, career-advancing resources. It is our mission to develop and maintain a website where people can go to work!

Contact us to find out more about how to become a Site Sponsor.

Corporate Headquarters:

Toll Free Phone: (866) 225-9067

Toll Free Fax: (877) 825-7564

L9 P23 R4074 HWY 596 - Box 109

Keewatin, ON P0X 1C0

# Job Board Posting



Careers.Indigenous.Link

Date Printed: 2024/07/01

## Lead, Network Security Engineering

<b>Job ID</b>	198839-en_US-7631	
<b>Web Address</b>	<a href="https://careers.indigenous.link/viewjob?jobname=198839-en_US-7631">https://careers.indigenous.link/viewjob?jobname=198839-en_US-7631</a>	
<b>Company</b>	Scotiabank	
<b>Location</b>	Toronto, ON	
<b>Date Posted</b>	From: 2024-06-24	To: 2050-01-01
<b>Job</b>	Type: Full-time	Category: Finance

### Description

Requisition ID: 198839

Join a purpose driven winning team, committed to results, in an inclusive and high-performing culture. We are looking for a dynamic and experienced Lead Network Security Engineer to join our team. As the Lead Network Security Engineer, you will be responsible for providing technical leadership and strategic direction in the design, implementation, and management of network security solutions and platforms. You will play a pivotal role in protecting Scotiabank's network infrastructure from evolving cyber threats and ensuring the confidentiality, integrity, and availability of our systems and data. As a Network Security Engineer under Security Engineering & Deployment, you will be responsible for working with a diverse team, leveraging industry leading technology and processes to engineer, maintain, integrate and automate security tools and infrastructure. Contribute to the overall success of the Network Security Engineering team with a global focus on Network Security supporting the achievement of the Bank's information security objectives of integrity, confidentiality/privacy, availability, and continuity. Is the role right for you

- Based on industry standards and trends, define Network Security vision, strategy and operational policies. Develop and implement network security strategies and procedures to mitigate risks and enhance the overall security posture of the organization.

- Technical ownership of Network Security Engineering initiatives from proposals to designs through to production implementation.
- Participate in the evaluation and vendor selection process for new Network Security technologies by preparing RFPs, bid proposals, contracts, scope of work reports, and other documentation for IT projects and associated efforts.
- Collaborate with cross-functional teams to integrate security best practices into the design and implementation of new network security technologies and initiatives.
- Evaluate network security resiliency and performance to provide statistics reports and enhancement recommendations to executives, stakeholders and department heads.
- Assess emerging threats and vulnerabilities and recommend proactive security measures to safeguard against potential attacks.
- Identify technology and security gaps, develop comprehensive mitigating strategies and contingencies.
- Collaborate with Business and other technology groups to ensure that all initiatives are appropriately assessed and reviewed in terms of risk and security compliance.
- Leadership and technical guidance through security and threat reviews.
- To ensure rapid recovery in the event of a disaster, the Network and Security Architect is required to coordinate the review of policies and procedures to ensure compliance with disaster recovery and contingency plans.
- Conduct regular security assessments and audits to identify gaps in security controls and implement remediation measures as needed.
- Research, review and actively stay informed on newly emerging technologies.
- Serve as a subject matter expert on network security technologies, trends, and industry best practices.

Do you have the skills that will enable you to succeed in this role? Education/Experience

- Bachelor's degree in Computer Science, Information Technology, or related field. Advanced degree or relevant

certifications (e.g., CISSP, CCNP Security, CEH) preferred.

- 5+ years of leadership experience with demonstrated success in implementing continuous improvement and strategic initiatives.

- 8+ years of experience in network security engineering or related role planning, designing and deploying large-scale enterprise or data-center infrastructure/technologies. With in depth knowledge of network security principles, protocols, architectures and technologies.

Professional Certification

- Google/Azure Cloud Security Engineering, CISSP, CCSP

Technical Skills

- In-depth working knowledge of network security principles, protocols, architectures, and technologies is essential. This includes strong working knowledge of industry leading technology providers within the below spaces:

- Next Generation Firewalls (NGFWs)

- Network Access Control (NAC)

- Email Security

- Network Segregation and Microsegmentation

- Content Delivery Network (CDN)

- Zero Trust Security Architecture (ZTA) and Software-Defined Perimeter (SDP)

- Cloud Native Security

- Cloud Secure Web Gateways (SWG)

- Secure Access Service Edge (SASE)

- Familiarity with Google and Azure cloud computing platforms and understanding of cloud security best practices. Ability to implement security controls, monitor cloud environments, and address unique security challenges in the cloud.

- Experience designing and operating secured DDoS resilient infrastructures with WAF, CDNs, SLB, security gateways and content filtering.

- Demonstrated excellence in documenting complex enterprise level systems, processes, and proactively sharing and communicating complex technical information.

- Excellent knowledge of information security standards and best practices.

- Excellent knowledge in overall network security assessment, penetration testing and vulnerability management.

Abilities

- Ability to recommend areas of operational system and process improvements

- Demonstrated excellence in documenting complex enterprise level systems and procedures, and proactively sharing and communicating complex technical and procedural information

- Sound understanding of general business conditions and practices with ability to think strategically with ability to effectively translate business requirements into effective security solutions.

- Strong understanding of regulatory compliance requirements and industry standards related to network security (e.g., ISO 27001, NIST, PCI DSS).

- Proficiency in conducting risk assessments, identifying vulnerabilities, and assessing the potential impact of security threats. Ability to develop risk mitigation strategies and prioritize security measures based on risk levels.

- Ability to interact and effectively communicate technology concepts to senior business managers.

Attributes

- Proactive and results-oriented with good time management skills, and the ability to work well under pressure and focus on multiple priorities concurrently.

- Commitment to staying updated with the latest cybersecurity trends, technologies, and best practices. Ability to adapt to evolving security threats and technological advancements to continuously improve network security posture.

- Excellent communication skills to convey complex technical concepts to non-technical stakeholders. Ability to engage with business leaders, IT teams, and external partners to articulate security risks, requirements, and solutions.

- Excellent organizational, interpersonal and presentation skills.

- Very hands-on person, who embraces new technologies and concepts.

What's in it for you

- Diversity, Equity, Inclusion & Allyship - We strive to create an inclusive culture where every employee is empowered to reach their fullest potential, respected for who they are, and are embraced through bias-free practices and inclusive values across Scotiabank. We embrace diversity and provide opportunities for all employee to learn, grow

& participate through our various Employee Resource Groups (ERGs) that span across diverse gender identities, ethnicity, race, age, ability & veterans.

- Accessibility and Workplace Accommodations - We value the unique skills and experiences each individual brings to the Bank, and are committed to creating and maintaining an inclusive and accessible environment for everyone.

Scotiabank continues to locate, remove and prevent barriers so that we can build a diverse and inclusive environment while meeting accessibility requirements. &#8239;

- Upskilling through online courses, cross-functional development opportunities, and tuition assistance.&#8239;

- Competitive Rewards program including bonus, flexible vacation, personal, sick days and benefits will start on day one.

Location(s): Canada : Ontario : Toronto

Scotiabank is a leading bank in the Americas. Guided by our purpose: "for every future", we help our customers, their families and their communities achieve success through a broad range of advice, products and services, including personal and commercial banking, wealth management and private banking, corporate and investment banking, and capital markets.

At Scotiabank, we value the unique skills and experiences each individual brings to the Bank, and are committed to creating and maintaining an inclusive and accessible environment for everyone. If you require accommodation (including, but not limited to, an accessible interview site, alternate format documents, ASL Interpreter, or Assistive Technology) during the recruitment and selection process, please let our Recruitment team know. If you require technical assistance, please [click here](#). Candidates must apply directly online to be considered for this role. We thank all applicants for their interest in a career at Scotiabank; however, only those candidates who are selected for an interview will be contacted.

For more information, visit [Scotiabank for Lead, Network Security Engineering](#)