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

Cyber Security Specialist (SOC)

Job ID	**247739-en_US-5665**
Web Address	https://careers.indigenous.link/viewjob?jobname=247739-en_US-5665
Company	Rogers
Location	Brampton, ON
Date Posted	From: 2022-01-24 To: 2050-01-01
Job	Type: Full-time Category: Telecommunications

Description

<p>At Rogers, we connect Canadians to a world of possibilities and the memorable moments that matter most in their lives. Every day we wake up with one purpose in mind. To bring loved ones together from across the globe. To connect people to each other and the world around them. To help an entrepreneur realize their dream. A sports fan celebrate a special moment.</p><p> </p><p>Because we believe connections unite us, possibilities fuel us, and moments define us.</p><p> </p><p>As we grow our team, the well-being of our team members remains our top priority. To ensure the health and safety of our team members, including those in the recruitment process, our team members are working from home, and are equipped to do so safely and efficiently.</p><p> </p><p>The Rogers Information and Cyber Security Unit is seeking a highly motivated Cyber Security Specialist to join our Cyber Protection Centre. This role is responsible for maintaining and advancing our existing cybersecurity program through the continual review and development of Rogers's cybersecurity strategy and security incident response procedures. This role is equivalent to a SOC Tier 1 specialist. Reporting to the Sr. Manager, Cyber Incident Response and Intelligence, the incumbent will be tasked with providing support to Rogers’ cyber incident response function, which includes the identification and application of threat intelligence information.</p><p> </p><p>Summary of Essential Job Functions:</p>
Providing first-line response and initial management of any new or developing cybersecurity-related issues including participation in on-call rotation.
Enhanced level triage and assessment of security events to determine the risk to the business.
Utilizing “kill chain” methodologies, effectively determine risk prioritized response, investigate security events, and make clear recommendations on mitigation.
Review and interpret alerts, events, and system alarms using SIEM, other tools, behavioral analytics, and network analysis while providing evolved emergency response services, incident management and analysis.
Respond to service provider network attacks affecting critical network infrastructure and the cloud environments.
Produce detailed incident reports and technical briefs on security incidents and preparing executive risk-based metrics reports based on the MITRE ATT&amp;CK model.
Participate and contribute to post incidents reviews and documentation.
Identify and report on threat intelligence from external &amp; internal resources and use to apply risk based assessments.
Investigation of security events to determine root cause.
Tracking and reporting of events and investigations.
Contribute to security projects, meetings, and ad-hoc requests.
<p>
Required Skills and Experience:</p>
1-3 years + applied technical experience.
Expertise in Kill Chain Methodology &amp; Cyber Threat Intelligence Framework is an asset.
Experience with forensic tools and methodologies is required
Scripting (Powershell, Bash, Perl, Python) knowledge/experience a bonus.
Direct experience with developing security metrics, KRIs and KPIs for leadership team.
Strong knowledge of Clouds, Service provider/ Telecom infrastructure, virtual environments, web applications and APIs
Working knowledge of TCP/IP networking, including routing and common ports/protocols.
Proficiency with large data manipulation tools ie, Excel, DBs, Open Source, and Linux tools
Demonstrated relevant experience as a key member of threat intel, incident response, malware analysis, or similar role.
Strong knowledge of malware families and network attack vectors.
Strong knowledge of Linux, Windows system internals.
Understanding of payment card processing, related fraud, and carding techniques.
Self-motivated individual with a 'will do' attitude and a strong desire for continuous process improvement.
Proven ability to work in a stressful or crisis situation.
Ability to drive things, work well both independently and in a team environment.
Ability to clearly articulate risk &amp; findings to internal clients both verbally and in written form.
Excellent communication, presentation, and relationship skills.
Strong organizational, time management, and multi-tasking skills.
Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM) certification is good to have.
Ability to obtain security clearance (if required).
Undergraduate degree in computer science, engineering, information science, or a related technical discipline.
<p> </p><p> </p><p> </p><p>As a condition of hire, all new employees will be required to provide proof of vaccinations against COVID 19. Any request for an exception under Human Rights legislation must be supported by evidence to be considered by Rogers on a case by case basis.</p><p><p>
Please click here to review conditions that may qualify for medical exemption to the COVID-19 vaccine.</p><p> </p><p> </p><p>Schedule: Full time
Shift: Day
Length of Contract: Not Applicable (Regular Position)
Work Location: 8200 Dixie Road (101), Brampton, ON
Travel Requirements: None
Posting Category/Function: Technology &amp; Information Technology
Requisition ID: 247739

Together, we'll make more possible, and these six shared values guide and define our work:</p>
Our people are at the heart of our success
Our customers come first. They inspire everything we do
We do what’s right, each and every day
We believe in the power of new ideas
We work as one team, with one vision
We give back to our communities and protect our environment
<p> </p><p>What makes us different makes us stronger. Rogers has a strong commitment to

For more information, visit Rogers for Cyber Security Specialist (SOC)