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: 2024/04/20

Network exploitation analyst

Job ID	**21-968-08-049-6982**	
Web Address		
https://careers.indigenous.link/viewjob?jobname=21-968-08-049-6982		
Company	CSIS	
Location	Ottawa, Ontario	
Date Posted	From: 2021-03-25	To: 2050-01-01
Job	Type: Full-time	Category: Public Administration

Description

Closing Date 2021-06-23
Reference Number 21-968-08-049

Job Category Subject Matter Expert
Who Can Apply Canadian Citizens

Location Ottawa, Ontario
Salary Range $84,050 - $102,250
$95,350 - $116,060
Status Indeterminate (permanent)
Language Requirement Various

Job Summary

As a Network Exploitation Analyst at CSIS you will be part of a team of energetic professionals in the area of operational investigations. Your day will be filled with the excitement and challenges that you would expect as a Technical Analyst within Canada's spy agency. Your role within our agency will offer you the chance to become part of a dedicated team that investigates cyber threats to the security of Canada, such as cyber-espionage, cyber-foreign-influenced-activities, and cyber-terrorism. Your day-to-day functions will include conducting technical analysis of Adversary Computer Network Exploitation artifacts using forensics and other methodologies. You will also be involved in the development, design, implementation, and maintenance of creative systems and tools which support cyber national security investigative activities.

A career as a Network Exploitation Analyst within CSIS will provide you with the opportunity to play a key role in keeping Canadians Cyber safe by investigating and countering cyber-attacks impacting Canada o/r Canadian interests.

Network Exploitation Analyst:

- Conduct technical analysis of technical artifacts using reverse engineering and forensics.

- Design, architect and implement systems to support cyber investigative activities.
- Assist in developing and maintaining malware information sharing platforms.
- Prepare technical assessments and operational reports.
- Maintain infrastructure onsite or cloud based.

Senior Network Exploitation Analyst:

- Lead, mentor and case manage cyber investigations.
- Provide specialized advise on cyber investigations.
- Responsible for assessing, interpreting and attributing cyber activity investigated by the Service to direct the cyber investigations.
- Oversee the creation of cyber threat intelligence related to the Service's cyber investigations.
- Lead the analysis of cyber investigations including malware analysis, hard drive forensics, and network traffic forensics, related to foreign CNE operations.

Education

Network Exploitation Analyst:

- Undergraduate degree in Computer Science or Engineering and four (4) years of recent experience\\
- Technologist diploma and five (5) years of recent experience
- Professional technologist equivalency designation and five (5) years of recent experience

Senior Network Exploitation Analyst:

- Undergraduate degree in Computer Science or Engineering and seven (7) years of recent experience
- Technologist diploma and eight (8) years of recent experience
- Professional technologist equivalency designation and eight (8) years of recent experience

The educational program must be from an accredited learning institution recognized in Canada. If you have completed a program outside of Canada, you will be required to obtain proof of a Canadian equivalency at your expense from an accredited learning institution recognized in Canada. Note: Any higher level of education could be recognized as experience.

Experience

Network Exploitation Analyst: Candidates must demonstrate experience in all four of the subjects listed below. The number of years of experience must be acquired and demonstrated for each subject. In addition, experience must have been gained within the last 6 years.

- Experience in scripting / automating processing (e.g. Python, PHP, shell) or software development (C/C++)
- Experience in IT Security appliances (e.g. VPN, Firewall, IDS, etc.)
- Experience with network communication protocols (e.g. DNS, TCP, etc.)
- Experience with IT Infrastructure (LAN/WAN, networking)

Assets:

- Experience with threat intelligence platforms such as MISP or similar
- Experience in malware signature development (e.g. regex, yara)
- Experience in malware analysis, network penetration testing, vulnerability research, or software exploit development

- Experience in providing briefings and/or presentations

Senior Network Exploitation Analyst:

Requirement 1: Candidate must demonstrate experience in one (1) of the three (3) subjects listed below. The number of years of experience must be acquired and demonstrated. In addition, experience must have been gained within the last ten (10) years.

- Experience in malware analysis (static or dynamic)
- Experience in malware signature development (e.g. regex, yara)
- Experience in computer forensics (disk, memory, mobile) or network forensics (PCAP, DNS, TCP)

Requirement 2: Candidate must demonstrate experience in two (2) of the eight (8) subjects listed below**. The number of years of experience must be acquired and demonstrated for each subject. In addition, experience must have been gained within the last ten (10) years.

- Experience in malware analysis (static or dynamic)
- Experience in malware signature development (e.g. regex, yara)
- Experience in computer forensics (disk, memory, mobile) or network forensics (PCAP, DNS, TCP)
- Experience in cyber threat analysis, or the production of cyber threat intelligence
- Experience in scripting (e.g. Python, PHP, Shell) or software development (C/C++)
- Experience IT Infrastructure (LAN/WAN, networking)
- Experience in IT Security appliances (e.g. VPN, Firewall, IDS, etc.)
- Experience with network communication protocols (e.g. DNS, TCP, etc.)

**Candidate may not select the same experience twice and must have a total of three (3) different experiences (one experience from Requirement 1 and two experiences from Requirement 2).

Assets:

- Experience in providing briefings and/or presentations
- Experience with threat intelligence platforms such as MISP or similar
- Experience in scripting/automating the processing of large volumes of data
- Experience in data science and implementing machine learning models/algorithms
- Experience with techniques used by computer hackers to penetrate computer networks and related technologies

Competencies

- Analytical skills,
- Innovation
- Problem Solving
- Ability to learn
- Rigour
- Communication

Conditions of Employment

Not Applicable

Notes

The majority of work in our organization must be done in the office and cannot be performed at

home. A written exam will be administered to successful applicants . If you are successful at the exam, you will be invited to an interview. The exam will serve to evaluate analytical skills and technical knowledge related to the required experience. Successful candidates may be eligible to a retention allowance.

Reference Links

Security Requirements
 Candidates must be eligible to receive an Enhanced Top Secret security clearance. The process involves a security interview, a polygraph, and a background investigation that includes credit and financial verifications. The use of illegal drugs is a criminal offense. Drug use is an important factor considered in your reliability and suitability assessment during the selection process. Therefore it is important not to use any illegal drugs from the time you submit your application.

Others
 We thank all applicants for their interest in CSIS. However, only those who are selected for further consideration will be contacted.

For more information, visit CSIS for Network exploitation analyst