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

Security Assessment Analyst

Job ID	**18-968-08-073-2945**
Web Address	https://careers.indigenous.link/viewjob?jobname=18-968-08-073-2945
Company	CSIS
Location	Ottawa, Ontario
Date Posted	From: 2019-02-22 To: 2050-01-01

Description

Closing Date 2019-08-07
Reference Number 18-968-08-073
Job Category Experienced
Who Can Apply Canadian Citizens

Location Ottawa, Ontario
Salary Range $78,800 - $95,870
$69,350 - $84,360
Status Indeterminate (permanent)
Language Requirement Bilingual Non Imperative (BBB/BBB)

Job Summary

Implement and administer IT security policies and procedures; Ensure the integrity, confidentiality, and availability of critical data resources and automated system components; Administer and configure the Enterprise Management suite of tools; Manage IT vulnerability management services by analyzing, prioritizing, and conducting vulnerability assessments and penetration testing; Provide regular and on-going security assessments of IT systems and networks, including the maintenance of its policies and procedures; Develop and maintain Security Configuration Benchmarks (SCB) or Security Technical Implementation Guides (STIGS) used in applications, databases, systems, and networks; Work with clients to ensure compliance to security policies and IT security hardening frameworks; and Assist the Security Operations Center (SOC) to address detected security concerns and escalations.

Education

- Undergraduate degree and three (3) years of relevant experience
- Technologist diploma or Professional technologist equivalency designation and four (4) years of relevant experience
- Fields of study: Computer science, electrical, electronics, network security, telecommunications, or engineering
The educational program must be from an accredited learning institution recognized in Canada. Note: Any higher level of education could be recognized as experience.

Experience

Candidates who do not fully possess the experience required may be considered for this position as an underfill.
- Experience in IT security including investigating security incidents and implementing associated corrective action

- A minimum of one (1) year of Vulnerability Management Services performing vulnerability assessments and/or penetration testing.
- Recent and significant experience in penetration testing using products such as, but not limited to Kali/Backtrack, Metasploit, NExpose, Nikto, SQLmap, and Veil-Framwork, and the customization of its scripts, exploits, and payloads.
- Recent experience implementing and customizing technical security controls in recognized hardening frameworks such as, but not limited to CIS - Security Configuration Benchmarks and/or NIST - Security Technical Implementation Guides.
- Recent and significant experience in running Vulnerability Management assessments using various tools and following industry standard practices.
- Recent experience analyzing, designing, and/or implementing security controls in business applications and infrastructure systems in both Linux and Windows environments.
- Experience in network security skills such as packet, vulnerability and exploit analysis.
Recent experience is defined as experience acquired within the last four (4) years. Significant experience is defined as the depth and breadth of experience that would normally be acquired by a person in a position where the performance of these duties constitutes his or her main functions over a period of two (2) years.   Assets: - Information Security Certifications including:
- Offensive Security Certified Professional/ Certified Expert (OSCP/OSCE; OffSec)
- Global Information Assurance Certified Penetration Tester (GPEN; GIAC)

- Certified Penetration Testing Consultant/Engineer (CPTC/CPTE; EC-Council)

- Certified Penetration Tester/Certified Expert Penetration Tester (CPT/CEPT; IACRB)
Foundational understanding of:
- NIST 800-115
- ISECOM - Open Source Security Testing Methodology Manual
- Bypassing System ASLR & NX/DEP (such as Return Oriented Programming / Code Reuse)
- Heap Spraying (such as Management, Feng Shui & Heaplib) and Browser User-After-Free Conditions
- EMET Protection (such as LoadLibrary, MemProt, Caller, SimExecFlow, StackPivot)
- Code Poly/Metamorphism, Caves, Splitting, Packing, Obfuscation and/or Encryption

- OWASP References and SQL Vulnerabilities
Experience with:
- Assembly Language (x86/64), C, Python, Ruby, and/or SQL Language(s)
- GCC & MinGW Compilers
- Virtualization Technologies

Competencies

- Behavioral Flexibility
- Initiative
- Problem Solving
- Analytical Skills
- Collaboration

Conditions of Employment
 Not applicable

Notes

- A written examination will be administered for the screening of candidates. The exam will be used to assess candidates' technical skills as it relates to the position.
- For bilingual non-imperative positions, offers will be conditional upon meeting the linguistic requirements within two (2) years of appointment.
- This position is designated CS; therefore, the employee may be eligible for a terminable allowance of 7% of the annual salary (4% at the underfill level).
- Some relocation expenses may be reimbursed.

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 Security Assessment Analyst