Cybersecurity Analyst

Job ID #: In-TAC-010-16
Sector: IT
Job Type: Full time
Location: Vancouver, BC
Number of Openings: 1
Salary: DOE (Depending on Experience)
Closing Date: Ongoing until filled

The company is one of the largest software companies headquartered in downtown Vancouver. Their office is located near the waterfront where they have great views and close proximity to public transit, shops and restaurants. They have designed a new office to provide a bright and inspiring work environment with a variety of custom-built spaces so they can collaborate, communicate, and concentrate. They celebrate their wins in large common areas where they hold hackathons, end of quarter celebrations, and monthly socials. The company believes in a good work / life balance which is reflected in their annual employee retreat where it's all about friends and family.

The Cyber Security Analyst is responsible for providing in-depth analysis of malicious activities that could be or have been carried out within customer's environments, as well as a detailed breakdown of the associated risk factors and mitigation techniques available.

The company offers the opportunity to apply theoretical knowledge to explore solutions to real-life technical problems. You will work with a dynamic, fast-paced team that plays a key role in building security products and services that help the customers identify and reduce security incidents. You will have access to domain experts, software developers and the user experience teams. The company strives to create an environment that is both productive and fun.

Responsibilities

- Insider threat hunting using a variety of tools and methods including the mining of large customer datasets.
- Forensic analysis of devices running Windows, Linux, Mac, and Android.
- Producing forensic reports and presentations with both high-level and detailed findings, along with recommendations for mitigation.
- Providing cyber-security knowledge and advice to clients as well as internally to our leadership.
- Collaborating with product team to grow and evolve the company's security offerings.
- Maintaining awareness of trends in IT security technology and regulatory requirements.

Qualifications

- Minimum of five years of IT/SW experience with at least three years of security forensic analysis experience. Related post-secondary education is an asset.
- Experience in Host Forensics analysis
- Experience with scripting and programming
- Experience in Malware and Malicious code analysis, including reverse engineering analysis
- Knowledge and understanding of common Intrusion Analysis models
- Strong knowledge of networking protocols.
- Strong troubleshooting, reasoning and problem solving skills.

Desirable:

- Experience with network analysis and sensors is a plus
- Experience with forensic tools such as Encase, Bit9/Carbon Black, RSA Netwitness, CrowdStrike and similar

- In-depth knowledge and significant experience in one or more of: Security Information Event Management (SIEM), Web Content Filtering, Internet Policy Enforcement, Network Access Control (NAC), Public Key Infrastructure (PKI) solutions.
- Experience with digital evidence handling and chain of custody
- Experience with malicious code behavioral analysis
- Understanding of steganography and encryption
- Security certifications such as: CISSP, CISM, CFCE

How to Apply:

Eligibility to apply for the job: Pre-arrival immigrants to Canada with valid passport from China, Hong Kong, Macau, or Taiwan

For Pre-Arrival clients already registered with In-TAC Pre-Arrival Services, please email your resume to your Counsellor, including "**Job ID # In-TAC-010-16**" in subject line. To access *free* pre-arrival services, please click here to register as our client.