

JOB DESCRIPTION

Title of Position	Information Security Analyst
Department	SOC – Managed Security Services (MSS)
Immediate Supervisor	Director, Information Security Service (MSS)
Location	Montreal

The role of the information security analyst is to analyze alerts generated by intrusion detection systems, which are deployed on client networks worldwide. When necessary, the analyst will be required to counter attacks by intervening in a manner that is in accordance with the intervention process established with clients. The analyst is also responsible for producing analysis reports on a monthly basis for clients and ensuring the optimum performance of client networks from an information security's perspective.

Responsibilities

- Using specialized tools, review alerts generated by intrusion detection systems as well as logs produced by multiple types of systems.
- Open and track incidents based on suspicious alerts and/or logs in accordance with the intervention protocol of each client.
- Track vulnerabilities found on the infrastructure of clients using our vulnerabilities detection systems, and assist with the identification and recommendation of solutions related to the scheduling of the scans.
- Monitor the networks of clients using our remote monitoring and intrusion detection infrastructure, ensure the availability of said infrastructure and recommend solutions that would improve the security posture of the clients.
- Produce the required monthly reports.
- Answer and respond to calls for support.
- Contribute to the evaluation of our intrusion detection systems in the pre-production environment in order to identify and report anomalies and/or to suggest improvements to the remote monitoring solution.
- Other duties related to the position or according to emerging business needs.

Qualifications

- University Degree in IT or College degree with 2 years of relevant IT experience
- Sound technical knowledge related to network security
- Proficiency in communication protocols found on modern networks (ICMP, IP, UDP, TCP, ARP, HTTP, HTTPS/SSL, SNMP, POP, etc.)
- Deep knowledge of operating systems such as Windows and Linux (RHEL, CentOS)
- Familiarity with tools and techniques related to intrusion detection and incident management
- Certifications in security are considered to be an asset.

Skills and Experience

- Client-focused approach with excellent communication skills, in both English and French, verbally and in writing (Spanish is an asset)
- Absolute integrity and focus on security at all times
- Strong analysis, organizational and documentation skills
- Ability to effectively communicate business concepts in a multicultural context
- Capacity to provide solid recommendations for continuous improvements in the area of security processes
- Sense of urgency, resourcefulness and initiative
- Flexibility and adaptability to change
- Availability for working in a team-oriented environment during work shifts, 24/7/365

We offer

- Thorough in-house, expert training on cutting-edge technology
- State-of-the-art IT equipment
- Friendly and dynamic work environment in new and modern office
- Employee Referral Bonus
- Group insurance plan
- Team spirit and dedication to service excellence
- Sense of belonging to a global, brand-name organization