TORYS

SECURITY ANALYST

Torys is a highly respected international business law firm with offices in Toronto, New York, Calgary, Montréal and Halifax. We work together to offer seamless cross-border services to our clients all over the world.

As a Torys employee, you will enjoy both an exciting, fast-paced work environment and a supportive, collegial and team-based culture. Our positions are best suited to individuals who take pride and ownership in their work and demonstrate exceptional client service in everything they do. At Torys, we take pride in our ability to attract and retain individuals who excel in their respective fields. We do this by providing stimulating work and learning and development opportunities, as well as a competitive compensation and benefits package.

POSITION OVERVIEW

Reporting to the Sr. Manager, Information Security, the Security Analyst is responsible for maintaining the daily operations of the firm's computer systems, servers and network connections by ensuring complete integrity and reliability of information residing in firm databases, workstations, servers and other systems.

KEY ACCOUNTABILITIES

Daily Operations:

- Monitors connection security for local and wide area networks, wireless networks, firm web sites, intranets/portals, and email communications. Ensures the security of data transferred internally and externally.
- Maintains and monitors the firm's security systems and their associated software or tokens, including firewalls, VPNs, IDSs, authentication and cryptography systems, and anti-virus systems for unusual or suspicious activity. Administers user logon and password management procedures.
- Interprets network activity and potential incidents and implements plans for remediation wherever necessary.
- Ensures that the appropriate patches, hot fixes, and service packs are installed on firm-managed systems and software in a timely manner.
- Monitors and reviews 3rd party penetration testing of all systems in order to identify system vulnerabilities and apply remediation as necessary.
- Keeps current with emerging security alerts and issues. Advises management, team and users as appropriate.
- Assists in developing and testing of incident response plans and participates in activities relating to contingency planning, business continuity management and IT disaster recovery.
- Researches and provides input on the firm's information security governance.
- Participates and assists in investigations and forensics for information security events and incidents.
- Participates in projects and initiatives as required. Provides 24/7 on-call security and systems support.

Vendor Engagement:

- Works with vendors as required to resolve complex issues, or implement system upgrades/testing.

Team Support:

- Provides hands-on support, guidance, and training to stakeholders as they interface with various systems and technology in the course of performing their roles; investigates and resolves any issues.

Continuous Improvement:

- Provides input and makes recommendations on continuous improvements in process, awareness, knowledge and capability within information services in the area of security.

ATTRIBUTES & EXPERIENCE

- A diploma/degree in technology with 5+ years of experience in an Information Technology role and 2+ years in an Information Security position.
- CISSP or related IT security certification would be an asset.
- Broad hands-on knowledge of network and information security components, including firewalls, intrusion detection systems, anti-virus/anti-malware/anti-exploit software, data loss prevention, data encryption, event log aggregators, access control methodologies, cryptographic systems and other industry-standard techniques and practices.
- Experience with Check Point, FireEye, and RSA ACE Server is preferred.
- Strong knowledge of Internet Protocol (IP) and Microsoft Active Directory Services is required.
- Experience with investigation of security events and ability to identify if an incident has occurred.
- Familiarity with penetration, vulnerability testing toolkits and the “black hat” industry of ethical hackers.
- Familiarity with security and privacy legislation as it applies to information and network security.
- Basic knowledge of information security frameworks (NIST, ISO 27001, CoBIT, PCI, SOX).
- Excellent communication skills (verbal and written) with the ability to present information security ideas and best practices in user friendly language and interact with individuals at all levels within the firm with tact and diplomacy.
- Exceptional client service combined with the ability to manage multiple client needs at the same time.
- Strong interpersonal skills with the ability to work well both independently and collaboratively within a team environment.
- A pro-active, self-starter with good organizational skills and exceptional attention to detail.
- Sound judgment including the ability to deal with confidential information with utmost discretion.
- Ability to prioritize remediation of vulnerabilities and assess potential impact to business.
- Strong research, analytical and problem-solving abilities.
- Flexibility to work after hours.

HOW TO APPLY:

Please address your resume and cover letter, stating your salary expectations to Firm Admin Recruiting (firmadminrecruiting@torys.com).

We thank all applicants for their interest in Torys LLP; however only candidates selected for an interview will be contacted.

At Torys we are committed to diversity in the recruitment, retention and advancement of our people. We believe that diversity of backgrounds, experiences and perspectives enhances the quality of our work and enriches our lives. We are committed to fostering an inclusive and accessible work environment. Accommodations are available for applicants with disabilities. If you require accommodation at any time during the recruitment process, please contact Ruby Dhindsa, Manager, Human Resources.