ABOUT US

Pathway Communications is a leading Canadian Managed IT and Cybersecurity Services Provider with a rich history of success since 1995. Our team of over 150 technical staff, which works out of four offices, delivers cutting-edge IT management and cybersecurity services to businesses across Canada and the USA. Our services include IT infrastructure and application management, 24/7 cybersecurity and SOC, data centre services, private and public cloud solutions, secure connectivity, telephony and expert consulting. Our commitment to excellence is reinforced by the critical certifications we have. These include, amongst others, SOC, ISO 27000, PCI DSS and Uptime Institute Tier III Certifications for our data centre.

THE POSITION

We are seeking an experienced Cybersecurity Manager to lead cybersecurity service delivery and ensure that our clients receive the highest standards of safety and protection. This pivotal role includes management of our 24/7 Security Operations Centre (SOC), strategic customer liaison and engagement, sales engineering, contributions to pricing and new service development.

KEY RESPONSIBILITIES

- ***Leadership of the SOC*****:** Direct and manage the 24/7 SOC and its team of skilled technical staff. Oversee security operations including continuous security monitoring, incident response and remediation and the use of threat intelligence to ensure timely detection and mitigation of cyber threats, risks and vulnerabilities.
- ***Security architecture*****:** Oversee the design and implementation of secure client IT architecture and systems. Develop, implement, and refine proactive security tactics and methods to counter emerging threats.
- ***Risk management:*** Develop and maintain a comprehensive cyber risk management framework that aligns with industry standards (e.g., NIST, ISO 27001) and incorporates the unique requirements of clients. Continuously identify, assess, and mitigate client cyber risk exposure; implement and maintain robust risk management practices.
- ***Customer engagement*****:** Serve as the primary cybersecurity contact with clients. Provide expert advice and support to clients on cybersecurity matters and ensure a high level of customer satisfaction with company cybersecurity solutions. Build and maintain strong client relationships.
- ***Technical sales engineering support*****:** Collaborate with the sales team to provide cybersecurity expertise during the sales process. Assist in developing proposals, pricing strategies, and client presentations. Play a pivotal role in the technical evaluation and design stage of the sales process, acting as a consultant to both clients and the sales team.
- ***Cybersecurity strategy*****:** Contribute to strategic planning and development of the company's cybersecurity services. Stay abreast of the regulatory environment and emerging cybersecurity trends, threats and technologies to ensure that our services remain at the forefront of the industry.
- ***Compliance and governance:*** Ensure compliance with relevant cyber security regulations and standards (e.g., GDPR, PIPEDA, MFIPPA, PCI-DSS). Conduct regular vulnerability assessments, penetration tests, and compliance audits for clients. Develop and enforce policies and procedures related to information security and privacy.

- ***Vendor management:*** Manage relationships with cybersecurity vendors and service providers. Ensure the quality and effectiveness of vendor products and services.
- ***Continuous improvement*****:** Promote a culture of innovation; identify and implement state-of-the-art security tools and techniques which will adapt to changes in the cyber threat landscape and technological advancements; provide continuous staff training and skill improvement.

REQUIRED QUALIFICATIONS AND SKILLS.

- *Experience*: 12 to 15 years in Information Technology management out of which 7 years should consist of hands-on experience in cybersecurity, in a leadership role, preferably managing a SOC.
- *Education*: Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or related field. Master's degree preferred.
- *Certifications*: CISSP, CISM, CEH, or equivalent; relevant vendor certifications.
- *Technical expertise*: Strong knowledge of operating systems, networks, virtualised server environments and storage. Proficiency in the hands-on use of cybersecurity tools and technologies, including but not limited to SIEMs, SOARs, firewalls, IDS &IPS, EDR, cloud and mobile security, vulnerability and penetration testing, zero trust systems, threat intelligence platforms and desktop exercises. Experience with forensics tools desirable.
- *Communication skills*: Interpersonal, communication and presentation skills to effectively engage and build trust with clients and team members.
- *Employee* management: Leadership, management and mentorship of technical staff.

JOIN US

At Pathway Communications, you'll have the opportunity to work and expand your career and skills as part of the leadership team in a dynamic, innovative environment where your contributions are valued. If you're passionate about cybersecurity and looking for a challenging yet rewarding role we'd love to hear from you.

Pathway is committed to creating a diverse environment and is proud to be an equal opportunity employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, gender, gender identity or expression, sexual orientation, national origin, genetics, disability, age, or veteran status. Furthermore, Pathway is committed to providing accommodations for people with disabilities in accordance with provincial legislation. Please let us know if you require a reasonable accommodation during the application or interview process.

OTHERS

- Candidates must be willing to undergo a technical exam.
- All applications must be submitted through this job posting. For any concerns or queries, kindly email **recruitment@pathcom.com**