Cybersecurity & IT Infrastructure Specialist

Who We Are:
GrandBridge Energy Inc. is guided by a vision to be a leader in energy transformation and driven by a mission to bridge communities to the energy future. We are proud to provide safe, reliable electricity to over 113,000 customers across the City of Brantford, the City of Cambridge, the Township of North Dumfries, and the County of Brant. Our team of dedicated professionals are committed to helping our communities navigate the transition towards a dynamic and evolving energy landscape. The principles and beliefs that guide our operations are deeply rooted in our values. Join us in our mission to shape the future of energy.

What We Offer:

- Employer Benefits Package (remove if not applicable)
- OMERS Pension Plan (note optional if contract role)
- Training and Educational Reimbursement Programs
- Professional Development & Career Opportunities
- Wellness Resources & Healthy Lifestyle Incentives
- Employee and Family Assistance Program
- Opportunities for Community Involvement
- Recognized as one of Southwestern Ontario's Top Employers for 2025 by MediaCorp Canada Inc., organizers of Canada's Top 100 Employers

What You Will do:

The Cybersecurity & IT Infrastructure Specialist will play a critical role in ensuring the operational excellence and reliability of GrandBridge Energy's datacenter infrastructure and cybersecurity programme. Specifically, you will be responsible for configuring and supporting datacenter infrastructure technologies such as virtualization, networking, backups, disaster recovery, and cybersecurity functions.

This role requires a strong technical leader who embraces standardization of processes and technology and adoption of best practices to drive operational efficiency, scalability, stability and security. A balance of technical expertise, cybersecurity acumen, and collaboration skills will help you succeed as you work closely with IT team members and business stakeholders.

Infrastructure
- Network Administration: Oversee the management and troubleshooting of LAN, WAN, VPN, and Wi-Fi networks, ensuring high availability and security.
- Private and Public Cloud Management: Administer and maintain both on-premises and cloud infrastructure (e.g., VMware, AWS, Azure), including system backups, monitoring, and scaling.
- Participate in the review and evolution of the current and future state of the system infrastructure.
- Participate in the patching/hardening practices of all Infrastructure system components.

Security and Compliance
- Conduct regular security audits, vulnerability assessments, and penetration tests to identify and mitigate risks.
- Manage and maintain security technologies, including Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), Security Information and Event Management (SIEM) platforms, and EndPoint Protection to monitor and prevent threats.

Disaster Recovery and Backup

- Implement and test disaster recovery (DR) protocols to ensure rapid recovery and business continuity.
- Manage daily backups of critical systems, validating integrity and ensuring readiness for restoration.
- Conduct routine testing of backup and DR protocols and simulate recovery scenarios to validate preparedness.

User Support and Documentation
- Provide third-tier technical support to internal users, partners and assist clients with infrastructure-related challenges.
- Create and maintain detailed documentation, including infrastructure configurations, diagrams, policies, and standard operating procedures.
- Train teams on emerging technologies like serverless computing, container orchestration, and SIEM platforms.

Continuous Improvement
- Proactively identify and implement improvements to system performance, security, and reliability.
- Stay updated on emerging technologies, including serverless frameworks, Docker, and AI.
- Evaluate and adopt new tools and processes for enhanced infrastructure automation and proactive response.

What You Will Bring:
- Bachelor's degree or college diploma in Information Technology, Computer Science, Cybersecurity, or a related field
- 5+ years of cybersecurity experience in a senior role supporting a wide range of related technologies
- 5+ years supporting core IT infrastructure services (VMware, Nutanix, Rapid7, Palo Alto, Rubrik)
- Configuring and troubleshooting network equipment, including switches and firewalls (Aruba Networks). Extensive knowledge of IP, WAN, LAN, and VPN technologies
- Experience in conducting internal security audits, vulnerability assessments, and penetration testing would be an asset
- Advanced skill / expertise using security tools and technologies (e.g., SIEM, PAM, EDR, IDS/IPS, firewalls, Email security gateway)
- Enterprise-level expertise with Microsoft Windows technologies, Linux/Unix systems
- Excellent analytical and problem-solving skills
- Strong attention to detail and ability to work under pressure
- Excellent communication and collaboration skills, with the ability to work effectively in cross-functional teams
- Professional security certifications such as CISSP (Certified Information Systems Security Professional) are highly desirable
- Strong interpersonal skills with the ability to work with multiple stakeholder groups and a commitment to fostering a positive and inclusive workplace culture

As a condition of employment, to ensure compliance with company information security standards, successful candidates must complete a background check. This will include an identity verification and criminal background check, both completed by a third party at the expense of the company.

Want to learn more about what makes GrandBridge Energy a great place to work? Ask our people what it's like to work here and here's what they'll tell you https://youtu.be/IYu3yEhhCp0

Apply Now

GrandBridge Energy
39 Glebe Street, P. O. Box 1060
Cambridge, Ontario N1R 5X6
Check us out at https://grandbridgeenergy.com/