Security Analyst (Vancouver, BC)

About Us
Recognized as a leader in innovative energy solutions, Creative Energy designs, builds, owns, and operates sustainable district energy systems across Canada and parts of the US. Our team has a client-focused, community-vested approach to projects that deliver outstanding quality and service while providing tangible value for continued growth.

In addition to owning and operating one of Canada's largest thermal networks in downtown Vancouver, we provide value to developers, landowners, end-users and the broader community through flexible thermal neighbourhood energy systems. Our projects focus on innovation, resiliency, and sustainability, and span across a broad spectrum of technologies including geo-exchange, ocean exchange, cogeneration, microgrids, solar PVs, and sewer heat recovery.

Serving Canadians for over 55 years with a reliability rate of 99.99%, we're developing more than a dozen new low-carbon district energy systems across North America, including the revitalization and decarbonization of our downtown Vancouver steam plant which will be one of North America's largest thermal fuel-switch projects and provide downtown Vancouver with renewable energy infrastructure for decades to come.

The Opportunity:

We are seeking a technology savvy Security Analyst to join our team and play a crucial role in safeguarding information technology and operational technology (IT/OT) infrastructure, as well as ensuring compliance with industry regulations. You possess a deep understanding of cybersecurity principles, risk assessment methodologies, and emerging threats in the utility and critical infrastructure sectors. You will:

- Monitor and analyze security events across the Creative Energy converged IT/OT network to identify potential security incidents and vulnerabilities.
- Conduct regular security assessments and penetration tests to evaluate the effectiveness of existing security controls.
- Collaborate with cross-functional teams to implement security best practices and remediate identified vulnerabilities.
- Develop and maintain security policies, procedures, and documentation to ensure compliance with industry standards and regulations.
- Participate in incident response activities, including investigation, containment, and recovery efforts.
- Stay informed about the latest cybersecurity trends, threats, and technologies, and provide recommendations for enhancing the organization's security posture.
- Assist in the development and delivery of security awareness training programs for employees, to promote a culture of cybersecurity awareness.
- Support audits and regulatory compliance initiatives by providing documentation and evidence of security controls.
- Work closely with internal departments and external vendors to action remediations for identified vulnerabilities of the IT/OT network, applications, and infrastructure.
- Coordinate the resolution of risks identified from penetration testing and vulnerability scanning activities.

- Support implementation, maintenance, and improvement of security tools such as SIEM, EDR/XDR, security Firewalls, Spam and Web filtering, Access control, Mobile security, etc.
- Maintain risk assessments, threat modeling, privacy assessments, and information security reviews on projects and all existing technology and systems.
- Assist in regularly assessing the strength of the organization's IT security governance and current processes, procedures, and technical security controls best practices.
- Propose and implement initiatives to remediate control gaps to reduce enterprise risk.

Qualifications and Experience:

- Possession of, or working towards, relevant cybersecurity certifications such as CISSP or GIAC.
- 4-5 years' experience in technical roles (Network, System Administration, etc.) or a combination of education, training, and experience.
- Minimum of 2-3 years of experience in cybersecurity, preferably in a utility or critical infrastructure environment.

Specialized Skills and Knowledge:

- Strong understanding of IT and OT systems, networks, and protocols.
- Proficient in security tools such as SIEM, IDS/IPS, firewalls, and vulnerability scanners.
- Familiar with industry standards and frameworks such as NIST, CIS Controls, and IEC 62443.
- Excellent analytical and problem-solving skills, with the ability to prioritize and multitask in a fast-paced environment.
- Effective communication skills, with the ability to convey complex technical concepts to non-technical stakeholders.
- Excellent interpersonal skills with the ability to interact with stakeholders and build relationships of trust and committed to providing superior customer service.
- Strong aptitude to take on new challenges and learn innovative technologies.

What we Offer

- Competitive starting salary - $85,000 - $95,000; placement on the range is dependent on your applicable experience, qualifications, skills and knowledge.
- Comprehensive benefits package, including an RRSP matching program.
- Support to maintain your professional credentials.

Interested?
This is an exciting opportunity with a growing firm and innovative leader in District Energy Systems. Please send your application to careers@creative.energy.

We thank all applicants for their interest; however, we will only be contacting selected candidates for follow-up.