ICS Cybersecurity Consultant

Job: Consulting
Job Title: ICS Cybersecurity Consultant
Primary Location: California
Schedule: Part-time
Travel: 25-50% of the Time

About Novesh Ltd.

Novesh provides innovative and state-of-the-art cybersecurity solutions and products to help businesses and organizations in securing their networks and protect their data from cybersecurity breaches. The core mission behind our work is to help companies thrive with a strong IT and OT cybersecurity infrastructure. We offer a thorough assessment of companies' IT and OT/ICS/SCADA/IIoT networks and facilitate their regulatory compliance process via automation. Novesh serves companies and organizations in different industry sectors and verticals.

About the Opportunity

The Industrial Cybersecurity Consultant will be a treasured member of the Novesh's ICS Security consulting team. The Novesh ICS Security Consulting involves in OT/ICS/SCADA cybersecurity consulting practice whose mission is to serve people by improving the safety, security, and reliability of the world's critical infrastructure – improving risk management through resiliency, situational awareness, and preparedness. The Industrial Cybersecurity Consultant will be committed to independently executing significant portions of projects addressing the security of Operational Technology (OT) systems consisting of Industrial Control Systems (ICS), Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLC), Discrete Process Control (DPC) systems, etc.

Industrial Cybersecurity Consultant supports the execution of projects consisting of a variety of assessments (e.g., GAP/Maturity, Vulnerability, Risk, Threat, Firewall, etc.); secure architecture, design, and implementation of OT networks, solution implementation, and operations, respond and recover related services (incident response planning, disaster recovery planning, business continuity planning). The Industrial Cybersecurity Consultant will support cybersecurity programs at client sites across North America utilizing ISA/IEC 62443, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and other key industry best practices and standards.

Job Duties

- Execute the planning, design, development, and implementation of technical controls, procedures, and policies associated with cybersecurity compliance and/or regulatory standards.
- Maintain the highest level of integrity, protecting the confidentiality and security of all clients and project information.
- Identify and diagnose operational issues and implement design alterations to address these issues.

- Conduct vulnerability assessments of OT networks for cybersecurity, risk management, and/or compliance purposes using industry-accepted best practices and approaches to support enterprise business goals and objectives
- Consult with clients on ICS security best practices and provide guidance on cost-effective strategies for implementation of security
- Perform detailed, post-event analysis of unusual events, and direct needed procedure or process changes in response.
- Pursue, obtain, and maintain industry-recognized certifications related to cybersecurity such as ethical hacking, penetration testing, network engineering, Industrial Control System (ICS), Supervisory Control and Data Acquisition (SCADA), risk management, and others, as necessary.
- Resolve technical issues, analyze implications to the client's business, and be able to communicate them with applicable stakeholders within the business.
- Develop policies & procedures for secure process control network design, technical and design recommendations for implementing firewalls, unidirectional gateways, zero trust design, and other network security controls.
- Compiles technical documentation of network traffic as well as firewalls services/solutions, including explanations and diagrams.
- Build and nurture positive working relationships with clients with the intention to exceed client expectations.
- Work collaboratively with other groups and divisions inside of Novesh Ltd.
- All other duties as assigned.

What We Look For

We're interested in intellectually curious people with a genuine passion for cybersecurity. With your broad exposure across Cybersecurity, we will rely on you to speak up with innovative ideas that could make a lasting difference not only to us – but also to the industry as a whole. If you have the confidence in both your presentation and technical abilities to grow into a leading expert here, this is the role for you.

Qualifications

- Bachelor's degree in a technical field, e.g., (Cybersecurity, Industrial Cybersecurity, Industrial Cyber Engineering, Cyber-Physical System Security, Computer Science or Information Systems, Computer Engineering, Electrical Engineering, or another related technical field with appropriate experience.
- Minimum 5 years of industrial cybersecurity experience.
- Additional applicable years of experience may be considered in place of degree requirements.
- Advanced knowledge of security principles and firm knowledge of cybersecurity technologies, as well as industry-recognized certifications.
- Knowledge and experience with ISA/IEC 62443, NIST Cybersecurity Framework (NIST CSF), and ideally NIST SP800-82, and NIST 800-53 required.
- Experience with security engineering principles, various cybersecurity assessment methodologies, security control implementation, and validation, and system life-cycle practices.
- Experience in the capabilities and/or configuration of cybersecurity controls, specifically those relating to firewalls, identity, and access control, zero-trust security, authentication and authorization, anti-virus/anti-malware, patch management, network, and system hardening, SIEM implementation, and/or tuning, and logging.
- Experience working with development teams to determine application requirements.

- Advanced knowledge of control systems utilized by Oil, Gas, and Chemicals; Manufacturing; Utilities (Power and/or Water); Energy; Transportation; etc., is preferred.
- Strong written and oral communication skills.
- Strong analytical and critical thinking skills.
- Ability to operate under pressure and under tight deadlines, to operate onsite within industrial, corporate, and government work settings.
- Demonstrate an understanding of business principles and operational security practices specific to engineering and/or security consulting.
- Knowledge and/or experience with legacy and modern computer networking and telecommunications.
- Experience with physical cabling for network communications and control system input/output.
- Strong technical writing skills
- Ability to develop and maintain strong relationships with clients.
- Ability to present complex technical issues and their impact in an easy-to-understand manner.
- Knowledge and experience with corporate policies and procedures

The Ideal Candidate will also have the following preferred skills:

- Tenacious problem solving
- Result-oriented team player
- Intellectual curiosity
- Dedicated to continuous improvement.
- Consulting background
- Relevant industry certifications such as – CISSP, CISM, CISA, CEH, GICSP, etc.
- Knowledge or experience with – OT asset inventory w/ change detection solutions, Vulnerability Management solutions, Identity and Access Control solutions, Zero Trust Security solutions, OT network & communications monitoring solutions, Security, Orchestration, Automation & Response (SOAR) solutions
- Knowledge of the Purdue model for zones/segmentation
- Certified Ethical Hacker (CET) certification with previous experience performing OT-relevant Pen Testing, Threat Hunting, or similar activities.
- Ability to integrate multiple data sources into a single system.
- Familiarity with code testing frameworks.

If you can demonstrate that you meet the criteria above, please apply via Novesh website, www.novesh.com from the career section or email us your resume and letter of application to jobs@novesh.com.

Equal Employment Opportunity

Novesh is an equal opportunity, affirmative action employer providing equal employment opportunities to applicants and employees without regard to race, color, religion, age, sex, sexual orientation, gender identity/expression, national origin, protected veteran status, disability status, or any other legally protected basis, including arrest and conviction records, in accordance with applicable law. Novesh is committed to providing reasonable accommodation to individuals with disabilities. If you are a qualified individual with a disability and either need assistance applying online or need to request accommodation during the interview process, please email jobs@novesh.com.