Cybersecurity Consultant

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

With rapidly changing cybersecurity threats, clients from all industries look at cybersecurity companies like us for trusted solutions in an increasingly complex environment and risks. As a member of our Cyber Security assessment team, you'll have the opportunity to help clients gain insights into their cybersecurity program and strategy as a whole. You will have access to our robust solutions to advise clients on managing cybersecurity risk, enhancing maturity, and improving efficiency. You will belong to a team of specialists helping our clients with their most complex cybersecurity needs and contributing toward their business resilience.

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.

The opportunity
You will work alongside respected industry professionals, learning about and applying leading practices to better manage cybersecurity people, processes, and technology capabilities. You'll gain insights into the design and operations of cybersecurity programs and strategies in a variety of industries and learn how to design measurable, sustainable programs to keep up with the ever-changing cybersecurity landscape.

Responsibilities
You'll work with a National practice, which often times includes global team members, to assess cybersecurity programs and strategies using our framework, design solutions to remediate gaps or enhance the maturity of specific cybersecurity capabilities, improve cybersecurity measurements and monitoring, and develop sustainable processes. You will gain experience applying risk management principles to a cybersecurity environment and leveraging cybersecurity frameworks/standards like ISO/IEC 27001, NIST CSF, NIST 800-53, IEC-62443 and NIST-800-82, etc. This position will also be focused on providing guidance around security and privacy regulatory and industry standard requirements to our portfolio of clients, conducting security risk assessments, and working with the practice leadership to keep abreast of developments in the information security space from both a strategic and technical perspective.

Key job responsibilities will include:

- Conduct information security assessments using industry-accepted best practices and approaches to support enterprise business goals and objectives
- Evaluate information security risk in the context of the business environment and industry requirements including government agencies/ institutions
- Consult with clients on information security best practices and provide guidance on cost-effective strategies for implementation of security
- Follow standard methodologies and develop new and innovative processes for delivering information security solutions
- Design deliverable content to precisely reflect the engagement contract and client needs
- Work with clients to help them understand where improvements could be made, and propose scenarios and solutions to address these areas of improvement
- Build and nurture positive working relationships with clients with the intention to exceed client expectations
- Ability to travel (50% of the time)

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.

Required Qualifications

- BS in information technology, computer science, or related field preferred
- 3-5 years of experience in information risk management, security governance, program development, regulatory and controls experience
- 2+ years of expertise in strategy roadmap development and policy review, development and procedures
- Hands on experience in the security frameworks and standards such as ISO 27001/2, PCI DSS, NIST 800-53 and the cybersecurity laws and regulations such as HIPAA, FISMA, CMMC, FTC Safeguard and GLBA
- CISSP, CISM, CCSP, CISA, CIPT, CIPM, CRISC or other relevant certification desired
- Solid understanding of the evolving security and privacy controls environment, regulatory landscape and risk management techniques, principles, and practices
- Experience and firm understanding of the development and implementation of information security policies, standards and related procedures
- Ability to provide risk-based recommendations based upon the size and complexity of the client's organization

- Ability to educate clients of the risk implications associated with a particular business decision, and communicate the likelihood and impact of those decisions so clients can fully quantify those risks
- Ability to translate complex technical information across all levels of the organization
- Strong facilitation skills and a clear ability to build strong relationships with business stakeholders at all levels, including executive managers and vendors
- Demonstrated ability to work effectively with a team, delivering high performance and customer satisfaction in a global, matrix-management environment
- Strong business acumen and process-oriented thinking
- Excellent presentation and issue resolution skills
- Verbal and written communication skills for use in preparing formal documentation including deliverables, Statements of Work, proposals, white papers, and case studies
- Ability to interface with C-levels, as well as tactical implementers
- Able to manage projects from inception to successful implementation
- Strong investigative and analysis skills with the ability to handle confidential information
- Understanding of available security tools and technologies

If you can demonstrate that you meet the criteria above, please apply via Novesh website, www.novesh.om 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 an accommodation during the interview process, please email jobs@novesh.com