ICS/OT Cybersecurity Consultant

Job Title:
Industrial Control Systems (ICS) and Operational Technologies (OT) Cybersecurity Consultant

Job Summary:
Our company is seeking an experienced Industrial Control Systems (ICS) and Operational Technologies (OT) Cybersecurity Consultant to join our team. The successful candidate will be responsible for providing cybersecurity services and solutions to clients in the industrial and operational technology sectors.

Key Responsibilities:
- Conducting cybersecurity risk assessments and vulnerability assessments of ICS/OT environments to identify potential threats and vulnerabilities
- Developing and implementing cybersecurity strategies and plans to address identified risks and vulnerabilities
- Performing security assessments of ICS/OT systems and networks
- Conducting incident response, forensics and disaster recovery (business continuity) exercises and investigations for ICS/OT environments
- Providing guidance and recommendations to clients on common/best practices for securing their ICS/OT environments
- Participating in the development and delivery of ICS/OT cybersecurity training and awareness programs for clients
- Staying current with industry developments and emerging threats to ICS/OT environments, and keeping clients informed of these developments

Qualifications:
- Minimum of 5 years of experience in ICS/OT cybersecurity consulting or related field
- Strong knowledge of ICS/OT environments and associated cybersecurity risks and vulnerabilities
- Experience with conducting cybersecurity risk assessments and vulnerability assessments of ICS/OT environments
- Familiarity with relevant standards and frameworks such as NIST Cybersecurity Framework, ISA/IEC 62443, and NERC CIP
- Experience with conducting security assessments and penetration testing of ICS/OT systems and networks
- Strong problem-solving skills and ability to work independently and as part of a team
- Excellent communication and interpersonal skills, including the ability to communicate technical information to non-technical stakeholders
- Relevant cybersecurity certifications such as GIAC Global Industrial Cybersecurity Professional (GICSP), Certified SCADA Security Architect (CSSA), or similar certifications are preferred

This is a contract (1099) position that may require some travel to client sites. The successful candidate will have the opportunity to work with a team of highly skilled cybersecurity professionals and gain experience in a dynamic and challenging field.