TITLE: **ICS Security Engineer / Specialist**

EXPERIENCE: Commensurate with role

EDUCATION: College degree or equivalent work experience

CERTIFICATION: GICSP, GRID, GCIH, or other industry relevant certifications

OVERVIEW: An ICS Security Engineer / Specialist will have proven experience protecting industrial control systems (ICS) in critical infrastructure and key resource sectors such as electric power, oil & gas, water, chemical, and critical manufacturing. The ideal candidate will possess an understanding of ICS fundamentals including but not limited to:

- distributed control system (DCS) and supervisory control & data acquisition (SCADA) architecture and the role of common system components;
- understanding of ICS design considerations with emphasis on human safety and the availability/security of operating environment;
- knowledge of IT and OT security best practices and understanding of the differences;
- understanding of protocols common in ICS environments;
- preparation, review, and maintenance of documents, policies, and standards governing the security operations for ICS equipment and networks.

The ICS Security Engineer / Analyst works with control system SMEs and operational staff to design, implement and support the security of ICS networked systems. This role must be familiar with security technologies such as firewall logs, IDS, endpoint security solutions, access control systems, and other related security technologies within ICS environment. Incident response and handling in an ICS environment to include investigating computer and network intrusions; remediation support; performing comprehensive computer surveillance/monitoring, identifying vulnerabilities; developing secure network designs and protection strategies, and audits of information security infrastructure.
[Add detailed information specific to firm/role/industry]

RESPONSIBILITIES:

- Lead maintenance and administration efforts of internal ICS infrastructure (Level 0-2) utilizing strong understanding of ICS environments
- Support current and legacy computer technologies in ICS environment. Operating systems may include Windows 95 through Windows 10 and various Linux operating system such as Red Hat and Ubuntu
- Participate in ICS security incident response through all phases
- Consult on ICS security matters as needed
- Act as a liaison between operations and corporate IT security teams
- Design, implement and manage innovative solutions for complex security and ICS infrastructure environments

REQUIREMENTS:

- In depth understanding of operating systems, network/system architecture, and IT architecture design
- Experience with operational technologies such as Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) software, and Distributed Control Systems (DCS)
- Understanding of IT and OT network communication protocols (including TCP/IP, UDP, DNP3, Modbus, IEC 61850, OPC, OPC UA, and PROFINET) and ability to perform packet analysis
- Understanding of threats, vulnerabilities, and exploits in ICS environments and appropriate mitigation techniques
- [Appropriate years] experience in ICS Security with a track record of successful accomplishments
- Minimum of [Xx] years previous experience working in ICS cyber security or applicable IT security role with willingness to learn uniqueness of ICS cyber-physical systems
- Minimum of [**X**] years previous experience developing and/or deploying mitigation techniques for defending networks.
- Superior organization and follow-up skills
- Excellent verbal and written communication skills
- Effective interpersonal skills
- Demonstrated ability to lead, motivate, and participate as a team player
- Creative problem solver

This position will be filled as an Engineer or Specialist depending on experience and degree held by selected candidate.