Position:

Senior Information Systems Security Professional

Terms of Employment:

Full-time position with excellent benefits package

Location: Denver, Colorado

The JW Group, Inc. is seeking an experienced Senior Information Systems Security Professional to support an established Cybersecurity program for a large organization. The successful candidate will provide support for the development / refinement of long term strategy and policies as well as implementing established procedures and processes supporting the Cybersecurity program.

Job Responsibilities:

- Perform senior lead role within Cybersecurity program.
- Provide architecting and engineering security solutions support and be responsible for operating information security systems and infrastructure.
- Security solutions includes firewalls, web filtering, file integrity monitoring, vulnerability scanning and configuration management, log collection, event correlation, VPNs and other safeguards.
- Performs technical investigations, incident response and root cause analysis.
- Implements and enforces Information Security policies and standards and conducts security awareness training, phishing campaigns and more.
- Interacts with third parties including auditors that evaluate PCI DSS compliance, IT general and financial controls.
- Provides reporting capability and metrics around the Cybersecurity program.
- Applies advanced security knowledge as well as practices hands on experience with managing security solutions.
- Provides support in compliance reporting.
- Reviews industry events and on-line tools to stay abreast of ongoing threats and countermeasures.
- Assist with overall program level strategy and future capabilities planning.
- Inspire trust and build strong, productive relationships with technical teams, vendors and working partners by being transparent and candid, following through on commitments, and getting ahead of challenges that may impede delivery
- Demonstrate outstanding verbal and written communication skills to leadership audiences and technical developers, with the ability to simplify highly technical or complex problems to express requirements to non-technical business partners and clients
- Other duties as assigned

Job Requirements and Minimum Qualifications:

- **Essential**: Bachelor's degree in computer science, business, or a related field. Technical certifications. Experience maintaining and supporting Splunk and Security Operations Center environments, policies, and procedures. Ability to communicate clearly and effectively, both orally and in writing, at all levels within and outside the organization.
- **Desirable**: Experience in Service Now application and monitoring/managing service requests and incidents. Certificates in cybersecurity.
- Minimum of 10 years of experience supporting an IT service organization, of which a minimum of

3 years of experience in a dedicated cybersecurity role with Security Operations Center experience at a senior level.

- Advanced experience with threat modeling, designing and deploying counter and control measures, monitoring and providing status and compliance reports to C-level management.
- Required Competencies:
    - Customer Focus
    - Communication Skills
    - Time Management
    - Ethics (Values, Honesty, Integrity)
    - Action Oriented
    - Functional, Technical Skills
    - Negotiating
    - Managing & measuring work
    - Drive for Results
    - Decision Quality
    - Process Management
    - Directing Others/Informing
    - Planning

Employment is contingent upon the candidate being able to clear a security background check required for airport badging within thirty (30) days of offer.

All candidates must be legally eligible to reside and work in the U.S. without company sponsorship.