Position:

Senior Cybersecurity SEIM Engineer

Terms of Employment:

Full-time position with excellent benefits package

Location: Denver, Colorado

The JW Group, Inc. is seeking an experienced Cybersecurity SEIM Professional to support the daily operations, various systems and tools related to an established Cybersecurity program for a large organization.

Job Responsibilities:

- Designs and implements or makes appropriate changes to the security information event management system deployed.
- Provide daily operations, configuration, and maintenance of the Splunk and Splunk Enterprise Security environments within a medium size implementation.
- Applies advanced security knowledge as well as practices hands on experience with managing installation nuances, onboarding of data, data modeling, and custom Splunk search language writing.
- Provides support in compliance reporting and review of logs in firewalls and other devices.
- Develops threat-modeling use cases leveraging enterprise security data models and notable events.
- Reviews daily logs and assigns severity rating to events being tracked.
- Assist in development and maintenance of Security Operations Center documentation and run books for new and notable events.
- Reviews industry events and on-line tools to stay abreast of ongoing threats in the cybersecurity arena and applies that knowledge to threat modeling and prevention efforts.
- Respond to and attempt to resolve/complete incidents and tickets within a maintenance management tool related to cybersecurity items.
- 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 7 years of experience supporting an IT service organization, of which a minimum of 3 years of experience in a dedicated cybersecurity SEIM role with Splunk experience.
- Experience with threat modeling and Splunk search language
- 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.