Position:
Senior Cyber Security Analyst

Terms of Employment:
Full-time position with excellent benefits package including health insurance (medical, dental, vision), life insurance and 401k

Location:
Denver, Colorado

Position Overview:
The JW Group, Inc. is seeking an experienced Senior Cyber Security Analyst to support a cybersecurity program for a large organization. The successful candidate will serve as a senior resource within a Security Operations Center which is entrusted to protect digital information and system assets and managing security solutions that will protect security systems and related infrastructure of the organization. This includes web filtering, file integrity monitoring, vulnerability scanning and configuration management, log collection, event correlation, VPNs, and other safeguards.

The Information Security team is also responsible for performing technical investigations, incident response and root cause analysis. Furthermore, the team is charged with implementing and enforcing Information Security policies and standards and conduct security awareness training, phishing campaigns for staff members. The position also requires interaction with third parties including auditors that evaluate our PCI DSS compliance, IT general- and financial controls.

The position is not an entry-level position and prior fulltime Information Security or SOC experience is required. Interaction with Technologies team members and business stakeholders is frequent and superior customer service skills are required. Furthermore, the ability to work independently as well as within groups is very desirable as is sensitivity to accuracy, timeliness, and professionalism in all areas of support activity is imperative. Denver International Airport is a fast-paced and dynamic environment that offers many opportunities and rewards.

Roles and Responsibilities:
The successful candidate will be required to:

- Interact with fellow technology team members and business stakeholders.
- Analyze system and network data from sources such enterprise security information and event monitoring (SIEM), data feeds of alerts and logs from firewalls, routers, and other network devices or hosts, network IPS/IDS systems, other host and network-based signature and heuristics-based systems, AAA systems, and other information sources. This serves to ensure the safety of digital assets and to protect systems from intentional or inadvertent access, prevent security violations, system intrusions, data breaches, and system destruction.
- Perform Information Security Incident Response and investigation activities and maintains logs to record and report incidents.
- Prepare reports on an as needed basis for compliance, change management, systems monitoring, and intrusion analysis.
- Assist in the development and implementation of new security alerting criteria based on new or existing data in the SIEM environment.
- Create formal documentation and diagrams for systems administration, operations, and maintenance

- Assist with the management of Information Security's service ticket queue. Perform service ticket resolution or escalation in a timely fashion while meeting SLA response time.
- Work as a key member of the Cybersecuity Incident Response Team during significant security incidents.

Desired Skillsets:

- Incident response skills and experience, including but not limited to: network and host data analysis, systems forensics, root cause analysis, IR lifecycle activities, etc.
- Enterprise logging including syslog-ng, event correlation, Splunk, ArcSight, Qradar, etc.
- A thorough understanding of TCP/IP principles, vLANs, routing, the OSI model.
- Experience in network security monitoring/scanning tools such as Nmap, Rapid7, Nessus, eEye Retina, etc.
- Network IDS/IPS systems such as SNORT, SourceFire, TippingPoint, CheckPoint, PAN, etc.
- Proxy technology including systems such as ScanSafe, WSA, BlueCoat, Imperva, Apache Modsec, squid.
- Enterprise AV systems such as McAfee EPO, Symantec, Cylance, PAN Traps, and other host AV and IPS systems.
- Endpoint Detection and Response (EDR) tools such as CrowdStrike FalconHost, McAfee Active Response, Carbon Black, etc.
- Python, PERL, or other scripting and automation skills
- In-depth understand of ports, protocols, and network traffic analysis as it relates to network security.
- Understanding of formal processes for change and release management including Change Requests, Standard Operating Procedures, etc.
- Familiarity with standard industry frameworks such as ITIL, PCI-DSS, NIST, etc.
- Experience in utilizing open-source tools to fulfill a variety of business and information security related needs.

Recommended Qualifications:

EDUCATION:

Bachelor's Degree in Computer Science or a related technical discipline, or the equivalent combination of education, technical training, or work experience.

EXPERIENCE:

- 4+ years of IT experience with minimum of 2 years working in a SOC or responding to information security alerts.

CERTIFICATIONS:

- Any relevant industry certifications such as Security+, CISSP, CCNA, SSCP, CEH, SANS (ex. GSEC, GCIH, GCFW, GCIA), CISA, CISM, etc.

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

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