TITLE: **Security Analyst – Associate or Senior**
Security Operations Center (SOC)

EXPERIENCE: Commensurate with role

EDUCATION: College degree or equivalent work experience

CERTIFICATION: GCIH, GCIA, GNFA or other industry relevant certifications

OVERVIEW: A Security Analyst will have proven their skills in Information Security, Information Systems, Packet Analysis, and Data Loss Prevention.

The Security Analyst provides support for complex computer network exploitation and defense techniques to include deterring, identifying and investigating computer and network intrusions; providing incident response and remediation support; performing comprehensive computer surveillance/monitoring, identifying vulnerabilities; developing secure network designs and protection strategies, and audits of information security infrastructure. The analyst will provide technical support for continuous monitoring and computer exploitation; specifically the identification of target mapping and profiling, network decoy and deception operations in support of computer intrusion defense operations. The Analyst will provide technical support for forensics services to include evidence seizure,. Further, the Analyst will research and maintain proficiency in open source and commercial computer exploitation tools, attack techniques, procedures and trends. [Add detailed information specific to firm/role/industry]

RESPONSIBILITIES:

- Strong hands-on information security skills and experience
- Experience responding to information security incidents
- Understanding of the Incident Response Phases
- Proven capability to consult on large enterprise information security matters
- Must be comfortable acting as a liaison between Information Security, Legal, HR, and Audit teams during security incidents
- Proven experience designing, implementing and managing innovative solutions to complex security and infrastructure environments
- In depth understanding of operating systems, network/system architecture, protocols, and enterprise services, and enterprise architecture design
- Expertise performing packet analysis
- Capability to quickly script and parse data
- Understanding of threats, vulnerabilities, and exploits
- [Appropriate years] experience in Information Security with a track record of successful accomplishments
- Minimum of [Xx] years previous experience working incident management.

- 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 and motivate
- Creative problem solver