TITLE: **Security Engineer - Analyst, Associate, or Senior**

EXPERIENCE: Commensurate with role

EDUCATION: College degree or equivalent work experience

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

OVERVIEW: The [Analyst, Associate, or Senior] Security Engineer will focus on security intelligence, anomaly hunting and incident response. The Engineer must leverage intuition, security knowledge and broad of array of tools and advanced security techniques to uncover malicious activity. [Add detailed information specific to firm/role/industry]

RESPONSIBILITIES:

- Experience performing technical analysis involving threat event data and evaluating malicious activity.
- Deep knowledge of TCP/IP and related network protocols: knowledge of standard network protocols like TCP, ARP, ICMP, DHCP, DNS, HTTP, SNMP etc., and accompanying protocol/packet analysis/manipulation tools
- Working/in-depth knowledge of information security protection/detection and authentication systems (firewalls, IDS, IPS, anti-virus, etc.)
- Knowledge of commonly-accepted information security principles and practices, as well as techniques attackers would use to identify vulnerabilities, gain unauthorized access, escalate privileges and access restricted information.
- In-depth knowledge of current operating environments (Microsoft, Linux, & OS X).
- Understanding and application of the follow security tools: [insert relevant TOOLS to role/company]
- Working understanding of database systems, application system development and installation/implementation processes.
- Exceptional analytical and critical thinking, willingness to challenge status quo. Excellent interpersonal skills.
- Advanced written and oral communications, self-motivator. Team player and independent worker, highly adaptive.
- Project management skills.