**Senior Program Manager, Security Operations Center - Contract**

**Job Details:**

**Requisition Number: 2015\_051**

**Title:** Senior Program Manager, Security Operations

**City:** Bellevue, WA

**Type:** Contract 18 months (with possible extension)

**# of Positions:** 2

**About This Position:**

The Senior Program Manager Security Operations Center has strong expertise in Managed Security Service Provider (MSSP), network security monitoring and incident response. The SOC Manager will be open minded, bring fresh ideas to the outsourced (MSSP) SOC team and be ready to protect, defend and respond to information security related events. Also, the SOC Manager, will lead key MSSP program elements including the following areas Predictive monitoring, Threat and Vulnerability Management, Threat Hunting and Cyber Security Risk Assessments. The SOC Manager will be responsible for security awareness and enforcement. This will be accomplished by pulling together information from a variety of systems; and normalizing and correlating the information. The SOC provides real-time (or near real-time) detection and reaction services for information security incidents within the company. Decision making is one of the most important traits.

**Primary Responsibilities:**

* Perform in-depth network security analysis and work with the SOC analyst team conducting incident response, event analysis and threat intelligence for the corporate enterprise
* Provide both strategic analysis and near real-time auditing, analyzing, investigating, reporting, remediation, coordinating and tracking of security-related activities for the corporate enterprise
* Analyze data and prepare reports that document vulnerabilities from network based attacks and recommends actions to prevent, repair or mitigate these vulnerabilities
* Provide technical mentoring to other team members
* Establish and create standard operating procedures for a variety of computer network defense (CND) related tasks/positions within the team
* Provide technical expertise on post event network security logs and trend analysis
* Review security events that are detrimental to the overall security posture; analyze and detect sophisticated and nuanced attacks and discern false positives and provide results to management
* Perform correlation of events from a variety of network, enterprise and host collection sensors
* Coordinate and liaise with other departments within the company and external auditors with information regarding intrusion events, security incidents, and other threat indications and warnings information
* Demonstrate both technical acumen and critical thinking abilities
* Experience with trouble ticketing and change management tools
* Coordination and escalation of issues to the Incident Response team
* Provide detection and response to security events and incidents within **CUSTOMER** Network
* Web application vulnerability scanning
* Security log management and monitoring
* Intrusion detections and prevention systems operations
* Maintaining information security metrics

**Required Skills:**

* Strong knowledge of leading MSSP program
* Security log management
* Strong analytical, documentation, and communication skills
* Strong understanding of IDS & IPS technologies
* Strong understanding of Windows event log analysis
* Experience with enterprise information security data management tools such as ArcSight, Splunk; etc.
* Understanding of network traffic analysis
* 8+ years of applicable experience and a minimum of 5 years of supervisory experience
* Must possess planning, organizational, and motivational skills, able to write clearly and succinctly in technical and non-technical formats.
* Ability to speak both extemporaneously and in formal settings.
* Experience in root cause analysis, industry benchmarking, survey evaluation and data interpretation is required.
* Have the ability to apply logic and reason to solve complex problems.
* Able to infuse innovation and creativity to strategic plans.
* Possess knowledge in the area of emergency/disaster management, physical security, critical incident stress management, risk management and business resiliency
* Familiar with emergency procedure protocols and regulatory interfaces.
* Experience in leading a team.
* Strong analytical, critical thinking and problem solving skills.
* Ability to establish and maintain cross-functional and positive working relationships.
* Proven ability to influence key business partners.
* Ability to build strategic vision and drive organizational change.
* Strong organization and planning skill with the ability to work in and define ambiguity/gray areas.
* Advanced computer skills and proficiency.
* Strong inter-personal and networking skills with a strong ability to work in a team environment.
* Ability to work under stressful and tight deadlines as well as the ability to manage in a fast paced environment.
* Above average computer hardware and software knowledge.
* Excellent verbal and communication skills.
* Ability to multi-ask, discerns patterns in details.
* Think through problems for logical solutions, and remain calm and professional under stress.
* Strong decision making ability during both crisis and non-crisis situations.
* Able to work with highly confidential information.
* Must be able to speak clearly,· give direction, and provide guidance to employees and security staff during emergencies.
* Able to work and communicate effectively with all levels of leadership.

**Required Experience:**

* Bachelor’s degree in computer science + or a related discipline
* Five to ten years of experience in the security field highly desirable.
* CISSP, CISM, GIAC certifications highly desirable

For further information or consideration, please contact a Groundwork Tech recruiter at the following address [jobs@groundworktech.com](mailto:jobs@groundworktech.com).

.