Job Description

Job Title:	**Cyber Security Specialist**		
Location:	Lakewood, CO	**Travel Required:**	Minimal
Level/Salary Range:	Open based on Experience	**Position Type:**	Full-Time
Date Posted:	5 February 2018	**Posting Expires:**	N/A
Mandatory Job Requirements:	Four-year degree in Computer Science or a related technical degree (or a minimum of 5 years of progressive IT experience.)		

Applications Accepted By:

Fax or E-mail: michelle.dionne@imcva.com Email Subject Line: Cyber Security Specialist *Preferred method of receiving applications is email*	**Mail:** Michelle Dionne, Corporate Recruiter Innovative Management Concepts, Inc. 21400 Ridgetop Circle, Suite 210 Dulles, VA 20166

Job Description

This position, considered as a subject matter expert, will provide monitoring and traffic analysis of organizational computer network data flow. A strong comprehension of malware, emerging threats and calculating risk is a critical component to the capabilities of a cyber security Specialist.

Responsibilities:

- Configuring and maintaining black and white lists on the Web Proxy environment (Blue Coat) as well as monitoring user traffic.
- Configuring devices to be monitored and customizing monitoring capabilities of Network Monitoring Tool (Solarwinds).
- Configuring scan zones and conducting various internal and external scans of the organization's networked devices by means of the Vulnerability management tool (Security Center).
- Conduct internal network scanning using of organization's networked devices using the vulnerability management tool (Core Impact).
- Conduct analysis of files/organization's networked devices using Encase Forensic software.
- Configuring policies, maintaining up to date rule sets and monitoring intrusion events alerted on by the ID/PS (Sourcefire).
- Configuring log sources and rule sets, maintaining system software and monitoring SIEM (QRadar) offenses.
- Creating reports on suspicious/malicious traffic and alerting the respective Regional Cyber Security Officer in a timely manner.
- Review reports and advisories for indicators and process accordingly.
- Working with a nationally distributed team.
- Collaborating with team members as well as other internal/external customers, business partners, management, and vendors.
- Lead small to medium size projects as directed by management.
- Deliver appropriate and accurate metrics to management.
- Other duties as assigned.

Required Qualifications and Skills:

- Four-year degree in Computer Science or a related technical degree (or a minimum of 5 years of progressive IT experience).
- Demonstrated hands-on experience in Cyber Security monitoring and assessment (TCP/UDP traffic analysis using tools like WireShark, TCPDump, etc.) and analyzing traffic flows and other activities to identify malicious activity or for troubleshooting purposes and escalate as needed.
- Ability to research and develop testing tools, techniques, and process improvements in support of security posture of the organization.
- In-depth understanding of networking concepts and infrastructure designs, including routing, firewall functionality, host and network intrusion detection systems, encryption, load balancing, and other network equipment and protocols.
- Excellent communication skills, analytical ability, strong judgment and leadership skills, and the ability to work effectively with clients and IT management and staffs, both technical and non-technical.
- Dedicated and self-driven desire to research current information in the security landscape.
- Ability to work on weekends, after-hours and on-call as necessary, especially during security incidents and emergencies.
- Two or more years of experience handling cyber-related incidents.
- Two or more years of experience handling cyber-related incidents working with anti-virus software.
- Two or more years of experience handling cyber-related incidents with SIEM and/or log aggregation tools.

Desired/Preferred Qualifications and Skills:

- CISSP or related certifications preferred (SANS, Security +, CEH, and others).
- Two or more years of experience handling cyber-related incidents (in a Federal/DOD environment preferred).

Innovative Management Concepts, Inc. (IMC), a Service-Disabled Veteran-Owned Small Business, provides systems engineering and information technology services to government and commercial clients. As a Service-Disabled Veteran-Owned Small Business, IMC places a special emphasis on recruiting and hiring veterans. Since its founding in 1989, IMC has offered expertise in: software development, verification, and validation; technology and project forecasting; continuous feedback and organizational communications; training systems; IT architectures; and website development, maintenance, and help desk support. Find out more about IMC at www.imcva.com.

IMC is an Equal Opportunity Employer

Reviewed By:	IMC HR	Date:	5 February 2018
Approved By:	IMC HR	Date:	5 February 2018