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:	8 March 2018	**Posting Expires:**	N/A
Mandatory Job Requirements:	Four-year degree in Computer Science or a related technical degree (or a minimum of five years of progressive IT experience.)		

Applications Accepted By:	
Fax or E-mail: michelle.dionne@imcva.com Email Subject Line: Cyber Security Specialist (Mid-Level) *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

The cyber security specialist assigned to this position at the Western Area Power Administration is considered a subject matter expert and primarily provides 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 and/or organization's networked devices utilizing 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 and 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.

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.
- Minimum of two years of experience handling cyber-related incidents.
- Minimum of two years of experience working with Anti-Virus software.
- Minimum of two years of experience with SIEM and/or log aggregation tools.

Preferred Qualifications and Skills:

- CISSP or related certifications preferred (such as SANS, CompTIA Security+, CEH, and others).
- Experience handling cyber-related incidents in a Federal/DOD environment preferred.

Background Information:

Innovative Management Concepts, Inc. (IMC), a Service-Disabled Veteran-Owned Small Business, provides a broad range of 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 solutions and expertise in: IT operations and maintenance, cyber security, systems and network engineering and support services, cloud/hosting services, software engineering and development, website services, software quality assurance and testing (including IV&V), and project management. IMC is certified in International Organization for Standardization (ISO) 9001:2015 Quality Management, ISO 27000:2013 Information Technology Security Management, and ISO 20000:2011 Information Technology Service Management. Find out more about IMC at www.imcva.com.

IMC is an Equal Opportunity Employer