E&M TECHNOLOGIES, INC.

854 Woodmoor Acres Dr.,
Monument, CO, 80132

Job title: Computer Network Defense Senior SME
Location: Sierra Vista, AZ
Security Clearance Required: Top Secret/SCI

E&M is actively seeking a COMPUTER NETWORK DEFENSE SENIOR Subject Matter Expert in support of the United States Army Regional Cyber Center-Continental United States.

Responsibilities and Skills:
In this position you may perform a variety of duties as follows

This work will be in support of the U.S. Army Regional Cyber Center (USARCC-C) based in Fort Huachuca, AZ.

- Develop Intrusion Protection System/Intrusion Detection System procedures; correlate and react to security events; perform first- and second-level triage; and forward suspicious activity
- Use a Security Information Management tool to aggregate approximately 13.6 million security events per day from multiple sources. During the life of this contract, other sources may be Active Directory domain controllers and DNS servers
- Perform advanced systems administration for the enterprise sensor mission relative to platform architecture, configuration, lifecycle support, and technology refresh and infusion
- Develop and document disaster recovery procedures for managed CND systems, including IPS/IDS, system baseline tools, host-based systems and agents, server managers, applications, and remote management systems. Store written procedures in the Document Management System database
- Perform daily backups, implement system upgrades, and verify system configurations, accounts, and passwords conform to baseline standards
- Establish and maintain written procedures to set up, track, and document status and location of hardware and software for each baseline of sensors. Store written procedures in the Document Management System database
- Maintain, update, test, and implement signatures and policies for each baseline of sensors; changes must be approved through the established ITIL process
- Build, configure, and assist with implementation of newly fielded sensors that support missions
- Monitor all sensors and agents managed for security event analysis and response. Respond to a detected event and perform triage, ensure proper handling of the associated trouble ticket, and process events according to the CND SOP and appropriate TTPs
- Maintain and update the triage database with current threat data and response methods
- Maintain and update SIM tool software rules for optimal detection of malicious or unauthorized activity. Report system incidents and problems according to CND SOPs and service level agreements

- Validate security event information from the ITSM ticket which includes at a minimum event name, date, time, location, source IP address, destination IP address, source ports, and destination ports. Contact the responsible NEC if additional information is required
- Provide data analysis as tasked by the COR

Certificates Required:

- Global Information Assurance Certification (GIAC) - Information Security Fundamentals or equivalent.
- CND-IS Baseline Certification

Education Required:

- Bachelor's Degree preferred

E&M Technologies offers competitive salaries, medical benefits, and a 401k plan.

To Apply for this Position:
You must have the listed skills and experience in your resume to be selected for an interview. Send your resume to **emtech@eandmtech.com**