E&M TECHNOLOGIES, INC.

E&M Technologies
4465 Northpark Drive, Suite 304
Colorado Springs, CO 80907

POSITION: Blue Team Cyber Defense Engineer
Work Location: Ft Belvoir, VA
Required Clearance: Top Secret/SCI

E&M Technologies, Inc. is currently seeking a **Blue Team Cyber Defense Engineer** to support a Federal government client.

Technical Task Order (TTO): Provide Tactics, Techniques, and Procedures (TTP), Tools, and Software Development, Integration and Test (SDIT) services for the IT enterprise systems engineering lifecycle of 1st IO CMD Networks and Mission Information Systems (MIS), including those networks/MIS designated for 1st IO CMD operations, mission deployments, training exercises and system development computing environments (CE). The work performed under this TTO enables the INSCOM/1st IO CMD the ability to deliver outstanding technical support and world-class technical delivery to several Brigade and Battalion-level Stakeholder Mission Networks, MIS, CEs, Mission Equipment and Engagement Platforms.

Responsibilities:

- Assess Mission Assurance in support of IO Assessments (Blue Team Operations)
- Provide certified and experienced vulnerability assessment analysts to conduct off-site system vulnerability, network architecture, policy and procedural, application, and system integrity reviews.
- Provide certified and experienced vulnerability assessment analysts to conduct threat-based emulation and cyber red teaming against Army and DOD networks.
- Assist with Development and Maintenance of CNSE Assessment Methodology, Tools, and Techniques
- Perform protocol and input fuzzing in order to find vulnerabilities.
- Perform analysis of disassembled code when source code is unavailable.
- Develop exploits based on identified vulnerabilities.
- Recommend fixes and mitigation for identified vulnerabilities.
- Provide expertise of network security testing, server hardening, vulnerability scanning tools and penetration testing techniques.
- Create/maintain adversary emulation toolsets/development.
- Contribute to technical and executive summaries of Blue Team missions.
- Document tools, techniques, processes, and procedures

Required Education/Experience:

- Bachelor's Degree (minimum) in the Area of Cybersecurity /or Computer Science from an Accreditation Board of Engineering and Technology (ABET) accredited college/university program, or four (4) years of equivalent software development and architecture practical experience supporting the IC, the DoD, Federal Community or Commercial Industry
- DoD 8140 (formerly DoD 8570) Certifications – Minimum IAT- Level III at the time of hire (e.g., Certified Information Systems Security Professional (CISSP), CompTIA Advanced Security Practitioner (CASP), CISCO Certified Network Professional-Security (CCNP-Security), ISACA Certified Information Security Auditor (CISA), GIAC Certified Enterprise Defender (GCED), or GIAC Certified Incident Handler (GCIH))
- Candidate must also possess at the time of hiring a CSSP Auditor certification (e.g., Certified Ethical Hacker (CEH), CompTIA Cyber Security Auditor +(CySA+), ISACA Certified Information Security Auditor (CISA), GIAC Systems and Network or Auditor (GSNA))
- Cyber Defense Engineer Practical Experience – At least four (4) years minimum of practical, hands-on experience and in-depth knowledge in the following technical areas
  - Network/MIS Hardware (HW) and System Configuration of Firewalls, Servers, Layer 2/3 Switches, Routers
  - NESSUS – Vulnerability Scanner for Information Assurance Vulnerability Management (IAVM)
  - Network Architecture Fundamentals and Core Network Device/Appliance Functions (e.g., Servers, Routers, Switches, Firewalls, VMs)
  - Practical working experience and knowledge of System, Security, Activity Audit Logs and/or Tier Security Information and Event Management (SIEM)
  - Practical Penetration Testing Experience w/ Metasploit, Wireshark, BurpSuite, Nmap and SQLmap.
  - Familiarity with Ports and Protocols Summary (PPS) and/or Port Security
  - Working knowledge of conventional and advanced information technologies used in either Commercial Industry, or; the United States Federal Government (USG), Department of Defense (DoD), and/or the Intelligence Community (IC)
- Experience with performing moderate to expert-level Technical Writing and performing technical reviews.
- Production of HW, Systems and Security Engineering Deliverables through the use of Microsoft VISIO – including technical documentation, white papers, artifacts and engineering work products (EWPs – e.g., Enterprise and System Architecture Documents such as Rack and Wiring Diagrams, Network Topologies)

- Offensive Security Certified Professional (OSCP), GIAC Global Industrial Security Professional (GISCP), GIAC Response and Industrial Defense (GRID) or GIAC Wireless Penetration Testing and Ethical Hacking (GAWN) is a plus.

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

To Apply for this Position:
You must have the Required Qualifications in your resume to be selected as a candidate.

Send your resume to emtech@eandmtech.com

All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, marital status, national origin, age, veteran status, disability, or any other protected class. U.S. Citizenship is required for most positions.