E&M TECHNOLOGIES, INC.
854 Woodmoor Acres Dr.,
Monument, CO, 80132

Job title: Forensics/Malware Analyst
Location: Sierra Vista, AZ/Fort Huachuca, AZ
Security Clearance Required: Top Secret/SCI
This position requires Shift Work

E&M is actively seeking a FORENSICS/MALWARE ANALYST in support of the United States Army Regional Cyber Center-Continental United States.

Responsibilities and Skills:

- Provides and reinforces security and interoperability requirements for all systems and network products and capabilities to ensure confidentiality, integrity, and availability of the information and business processes
- Have a minimum eight (8) years demonstrated/practical hands-on experience performing forensics and malware analysis in a DoD network environment
- Possess exceptional knowledge, experience, and certifications with commercial computer forensic tools including but not limited to: EnCase Forensic, EnCase Enterprise / Cybersecurity, AccessData Forensic Tool Kit (FTK), AccessData Lab, etc.
- Possess exceptional knowledge and experience with commercial binary analysis tools including but not limited to: IDA PRO disassembler, Ollydbg
- Be familiar with analysis tools to include IceSword, Procmon, Analyst Notebook, etc.
- Be proficient and have experience with computer languages including but not limited to: Assembly, C, C++, Perl, Java, Python, etc.
- Strong working knowledge and experience with all Windows OS platforms including but not limited to: Vista, Windows 7, Windows 8, 2K3 Server, 2K8 Server
- Working knowledge and experience with varying flavors of Unix/Linux platforms, and Apple based operating systems
- Possess strong experience with obtaining forensically sound images of, but not limited to, workstations, servers, laptops, flash devices, removable media, cell phones, RAID, virtual systems, etc.
- Be able to reverse-engineer compiled executable code to examine how programs interact with their environment
- Analyze collected media for defensive cyber operations (DCO) value to understand adversary technical capabilities and Tactics, Techniques and Procedures (TTP) methods of employment
- Analyze the attack/exploit capability of malware, document, and catalog findings for future correlation
- Develop necessary procedures or scripts to identify such data

- Work and interact with other DCO professionals, with Law Enforcement and Counter Intelligence personnel, and intelligence professionals as a technical specialist to understand higher-level adversary capability
- Document, update and enhance processes and procedures by producing training materials, standards documents and reports
- As an experienced Forensic Analyst will and can work independently and can work as a positive team member that can organizes work to meet Army customer deadlines

Skills and Experience Requirements:

- 8+ years of recent and relevant hands-on DoD network and systems forensic malware experience with a major Operating System (OS) such as Windows, including but not limited to: Windows 7/8/10, Server 2K3/2K8/2012/2016, and should have a strong working knowledge and additional hands-on experience with Unix/Linux platforms, and Apple based OS's
- Be proficient and have experience with computer languages including but not limited to: Assembly, C, C++, Perl, Java, Python, etc.
- Technical BS degree in engineering/science systems or related software discipline
- IAW AR 25-2, must have current DoDD 8570 IAT Level III certification (CASP CE, CCNP Security, CISA, CISSP (or Associate), GCED, GCIH): GIAC - Certified Forensic Analyst (GCFA) and GIAC Certified Incident Handler (GCIH)
- Must have an active DoD Top Secret/SCI Clearance
- Must be able to follow verbal directions and written policies, SOPs and TTPs to accomplish daily tasks
- Must be able to mentor less knowledgeable personnel and give directions to peers and subordinates as the team, unit or task lead
- Be a positive, self-motivated, and proactive person with the ability to adapt to change and tolerate stressful situations
- Willing to work overtime, holidays, and weekends as necessary
- Must be able to travel up to 20% of the time
- Has recent and relevant AR 25-2 Information Assurance and Management and Army and Joint Technical Architecture (JTA) with regards to network design, implementations and fielding
- Experienced with DoD 8510.01 Risk Management Framework (RMF), the Army AR 25-2 and AR 380-5 security policies as they relate to the overall USARCC-C Systems Administration activities and mission
- Maintains recent technical expertise in all Forensic Malware areas of IT/IP network and computer, servers and software and other assets requiring Forensic support, as required

- Exhibits exceptional ingenuity, creativity, and resourcefulness
- Develops network and systems Forensic concepts that extend knowledge in fields of expertise
- Provides technical leadership and mentorship to junior Forensic Analysts members
- Interacts closely with Army customer representatives on highly advanced technical Malware and other Forensic issues

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**