



E&M TECHNOLOGIES, INC.

854 Woodmoor Acres Dr.,
Monument, CO, 80132

Job title: ITIL Senior SME

Location: Sierra Vista, AZ

Security Clearance Required: Top Secret/SCI

E&M is actively seeking an ITIL SENIOR Subject Matter Expert in support of the United States Army Regional Cyber Center-Continental United States.

Responsibilities and Skills:

The Senior ITIL Subject Matter Specialist will examine malicious software/capabilities to identify the nature of the threat; Reverse-engineer the compiled executable code to examine how the program interacts with its environment. Analyze collected media for DCO value to understand adversary technical capabilities and Tactics, Techniques and Procedures methods of employment. United States Citizenship and an active TS/SCI DoD Security Clearance is required to be considered for this position.

- Analyze the attack/exploit capability of the software, document, and catalog findings for future correlation
- Provide all pertinent finding to personnel responsible for the development of signatures capable of detecting the analyzed malware as it propagates on infected systems
- Works and interacts with other DCO professionals internal and intelligence professionals as a technical specialist to understand higher-level adversary capability
- Collect, preserve and transfer forensic evidence of unauthorized access to a military/partner network, device or information systems
- Analyze forensically sound images to identify suspicious/malicious files, all intrusion related artifacts, and entry points/attack vectors
- Document, update and enhance processes and procedures by producing training materials, standards documents and reports
- Perform filter queries of network flow data and analyze results for anomalies and malicious indicators
- Analyze the origins, pathways, and methodologies of malicious cyber activities to attribute, model and predict future intrusions
- Provide mitigation techniques to deny further exploitation by the adversary; synchronize and integrate intelligence activities to detect, analyze, and recommend mitigation of cyber threats and vulnerabilities
- Provide recommendations for appropriate response and actions to the activity to identify vulnerabilities, correct faults, and defeat or defend against threat activity
- Other support duties as needed/directed

Skills and Experience Requirements:



E&M TECHNOLOGIES, INC.

854 Woodmoor Acres Dr.,
Monument, CO, 80132

- Must be able to get forensically sound images to identify suspicious/ malicious files, all intrusion related artifacts, and entry points / attack vectors
- 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
- Must have working knowledge and experience with varying flavors of Unix/Linux platforms, and Apple based operating systems
- Will have familiarization with additional analysis tools including but not limited to IceSword, Procmon, Analyst Notebook, etc
- Must be proficient and have experience with computer languages including but not limited to: Assembly, C, C++, Perl, Java, Python, etc
- Have exceptional knowledge and experience with commercial binary analysis tools
- Perform technical analysis of computer network intrusion events and malicious activity in support of cyber intelligence efforts
- Have exceptional knowledge, experience, and certifications with commercial computer forensic tools including but not limited to: EnCase Forensic, EnCase Enterprise / Cybersecurity, AccessData Forensic Tool Kit, AccessData Lab, etc
- Have strong working knowledge and experience with all Windows OS platforms including but not limited to: Vista, Windows 7, Windows 8, 2K3 Server, 2K8 Server, etc

Certificates Required:

- 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