Senior Malware Analyst—Cybersecurity

Location: Maryland
Part Time/Full Time: Full Time
Exempt/Non-Exempt: Non-Exempt
Travel: Minimal/local

Key Role

Join the dynamic, high-performance and growing TREADA Cyber Security Solutions team in Central Maryland. Work as part of a high-performance, highly technical cybersecurity team to deliver significant value to an important Federal client while growing cybersecurity skills, leadership skills and other skills as part of the technical staff of Treada Technology Group. Join this fast paced team and make an Impact—be part of a perpetually innovative TREADA CYIC—CYber Innovation Center.

Job Description

- Employs engineering techniques and processes to analyze software to identify vulnerabilities
- Re-creates programs to rebuild something similar to it, exploits its weaknesses, or strengthens its defenses
- Develops design specifications by inspection and analysis to offset various malware and to protect and defend US FEDERAL AGENCY infrastructure
- Develops, researches, and maintains proficiency in tools, techniques, countermeasures, and trends in computer and network vulnerabilities, data hiding, and encryption
- Conducts vulnerability assessments/penetration tests of information systems
- Ensures software standards are met; designs, develops, documents, tests, and debugs applications software and systems that contain logical and mathematical solutions
- Performs in-depth detailed research of software and methodologies to build defensive and offensive technical capabilities for US FEDERAL AGENCY
- Possesses senior-level experience as a Malware Analyst with a background in cutting-edge cyberspace technologies
- Often and without source code or documentation, performs system analysis, reverse engineering, and static, dynamic, and best-practice malware analytics methodologies and analysis on Windows, Android, or UNIX-based platforms
- Coordinates effort to develop and analyze cyberspace operations, DCO, Computer Network Exploitation (CNE), and OCO solutions
- Creates malware detection topologies
- Possesses comprehensive knowledge of programming skills especially including C/C++ and Assembly language, Windows internal C/C++ and either UNIX/Linux or mobile (Android) platform, malware and things related to malware research and analysis, reverse engineering, vulnerability analysis, exploit development, and related disciplines

Qualifications

- TS/SCI Clearance with Full Scope Polygraph
- Minimum 10 years of experience as a Malware Analyst
- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- A minimum of DOD 8140/DOD 8570 IAM Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.
- Must be excellent team player and must be highly motivated, goal-driven, and results-oriented
- Must be self-disciplined, and possess positive, "get things done" attitude