Sr. Principal Cyber Software Engineer

Location	Cincinnati, OH
Work Arrangement	9/80 schedule allows employees who work a nine-hour day Monday through Thursday to take every other Friday off.
Travel	Limited travel may be required – 10%
Clearance	Top Secret

Grit Government Solutions is currently looking for a Sr. Principal Cyber Software Engineer for its customer based out of Cincinnati, OH. We are seeking cleared mid-level Software Engineers who are self-motivated and energetic, with a background in Computer Engineering, Computer Science, or related technical disciplines.

Responsibilities:

- Developing solutions to national security threats with products that may involve kernel development, reverse engineering, or vulnerability research of network and communication systems.
- Kernel Mode (Windows, Linux) programming (C/C++, Assembly)
- Reverse Engineering (x86, x64, MIPS, PPC, or ARM)
- Vulnerability Analysis
- Communications Engineer:
    - Network Programming (C/C++)
    - Network protocols TCP/IP, UDP, HTTP, SSL, etc...
- Infrastructure Engineer

Basic Qualifications:

- Solid software development skills, including familiarity with scripting languages. Knowledge of computer networking, modern software development environments, embedded programming, and software configuration management tools is a plus.
- B.S. degree in Computer Science, Computer Engineering or related field and 8 years of programming experience; or M.S. degree in Computer Science, Computer Engineering or related field and 6 years of programming experience or Ph.D and 4 years of relevant work experience.
- US Citizenship is required
- Active Top Secret clearance is required
- Demonstrated software programming experience in C/C++
- Experience with SDLC (software development life cycle)
- Experience in software development to include any of the following: kernel mode, embedded, command and control, network applications
- Development of lower-level networking protocols such as TCP/IP and UDP
- Understanding of return-oriented programming (ROP) concepts and execution
- Experience with debugging or system analysis tools (e.g., Wireshark, IDAPro, OllyDebug, WinDBG, JTAG debuggers)

Preferred Qualifications:

- Active SCI security clearance

- Experience as Technical Lead leading teams of 2-8 engineers
- Advanced degree in Computer Science, Computer Engineering, or related field
- Experience developing software for multiple operating system environments
- Experience with vulnerability research on one or more operating systems (Android, IOS, Windows, Linux, etc.).
- Familiarity with Assembly Languages (e.g., x86, x64, MIPS, PPC, or ARM)
- Understanding of secure / insecure programming concepts (format string vulnerabilities, heap overflows, etc.)
- Experience with emulation (Renode, QEMU, etc.)
- Experience with reverse engineering compiled binaries using industry-standard tools such as Ghidra or IDA Pro.
- OS Internals experience
- Experience with virtual machine technology
- Ability to develop and implement shell code.
- Familiarity with modern source control platforms (e.g., Git, GitHub, GitLab) and CI/CD workflows using tools such as Jenkins, GitHub Actions, and GitLab CI.
- Experience with the Agile methodology