

Position: Cyber Security Technician – Senior Level
Clearance Level: DoD Top Secret
Location: Scott AFB, IL

SECURITY CLEARANCE IS REQUIRED.

DO NOT APPLY OF YOU DO NOT HAVE AN ACTIVE TOP SECRET CLEARANCE

The expert who fills this position shall provide cyber security expertise in the execution of the Specialized Engineering for Cyber Optimization, Defense & Evaluation (SE-CODE) contract. The candidate will have a background in complex information and network security systems technology integration efforts.

Duties:

- Will serve as cyber defense network support expert and will implement applicable security best practices; conduct overall vulnerability analysis and provide risk mitigation support.
- Understand, detect and emulate adversary tactics, techniques and procedures.
- Identify and resolve network and application performance issues.
- Perform hardware and software administrator duties, and provide maintenance support to CPTs located at multiple DoD locations.
- Respond to first-line customer requests such as user account issues, configuration issues, regular/scheduled maintenance and other touch maintenance functions.
- Use software and hardware tools to identify and diagnose problems affecting network and mission systems performance. Environments typically include a mixture of platforms: Windows and Linux based operating systems.

Qualifications and Education Requirements:

- Cyber security: experience in vulnerability management and scanning, Host Based Security System (HBSS), intrusion detection/protection systems (IDS/IPS), DNS, wireless technologies, boundary protection solutions (firewalls, web proxies, VPNs, etc.).
- Network Infrastructure: experience in network infrastructure including routers, switches, network management solutions, network access solutions, firewalls, virtualization, and virtual private networks.
- Systems Sustainment: experience in Microsoft and/or Unix-like operating systems, DHCP, group policy, vulnerability management, patch management, and antivirus.
- Understanding of operational and technical requirements of the complex information and network security systems in a military environment – Air Force experience preferred.
- Extensive experience with Commercial off the Shelf (COTS) information and network security systems, technologies, and tools. Not just able to speak the language, but able to perform hands-on hardware and software functions.
- Experience with hardware integration, software development, system testing and configuration management practices.
- Experience with Air Force Cyber Protection Team (CPT) operations preferred.
- Excellent written, verbal, and listening skills and have a demonstrated ability to present complex cyber material in an understandable way to senior DoD and non-DoD officials.

Required Skills:

- TOP SECRET security clearance is required; applicants must already have a fully adjudicated and active clearance.
- 10 years' experience in cyber security, network infrastructure or systems architecture.

- DoD 8570 IAT L3 (CISSP, CISM, etc.)
- Applicant must have technical certifications (MCSE: Data Platform, SANS GWAPT, and RedHat are highly desired)
- Bachelor's Degree in a technical or information/network security field preferred
- Advanced degree in a technical or information/network security field is desirable.
- Due to the nature of this US Government contract, US Citizenship is required.

Atlantic CommTech is an equal opportunity employer and all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, national origin, disability status, protected veteran status or any other characteristic protected by law.