Position Description: System Engineer - Cyber Security

Job Location: Manassas, VA.

System Engineer - Cyber Security - Job Description:

Designs, develops, and implements security controls to preserve the confidentiality, integrity and availability of information systems. Provides security engineering expertise to develop security documentation packages consistent with federal requirements, specifically the DOD 8500 series, NIST SP 800-53 and ICD 503. Performs certification and accreditation activities with government authorities and certification agents to obtain official Authorization to Operate (ATO) or Interim Authorization to Test on Enterprise and Platform IT (PIT) systems. Candidate must be U.S. citizen able to obtain a DoD Secret level security clearance.

Other tasks may include:

- Evaluating requirements, selecting/implementing security controls, reviewing installation procedures.
- Identify technological and functional risks inherent in system functionality, system exposure, and data sensitivity to determine the required security controls.
- Tailoring and configuring security controls for specific product use, security assessment plan preparation, test procedure preparation, test execution and reporting.
- Performing security vulnerability assessments using Assured Compliance Assessment Solution (ACAS), and performing SCAP security assessment/configuration.
- Provides support as the technical interface with customers, vendors, suppliers, and internal organization for related issues. Identify issues and recommend solutions.
- Conducting verification and validation of test procedures and script changes.

System Engineer - Cyber Security Required Skills:

1. Extensive experience assessing and implementing security controls for customer enterprise information systems.
2. Experience with TCP/IP and Network domain knowledge.
3. Experience with Linux file systems, kernel design, and device-level driver integration.
4. Familiarity with using Bash/Shell to produce hardening scripts and workable knowledge of using utilities such as SCAP and ACAS to identify system vulnerabilities.
5. Familiarity with DISA STIGS and the ability harden applications (e.g., OS, web server, database, etc.) in accordance with the recommended STIG guidance.
6. Ability to effectively communicate with the Certification and Accreditation (C&A) authorities regarding security requirements and their implementation method.

Highly Desirable Skills for System Engineer - Cyber Security:

1. Experience working in an Agile/Sprint release planning environment including depth of understanding of providing impact analysis on testing as Sprint and releases are introduced to the integration environment.
2. Existing certifications (e.g., Security+, CEH, Network+, etc) and CISSP certification.
3. Understanding of full system exposure and system wide activity – Integration testing across systems usage flow checks how one program integrates/impacts other components of the system.

Additional Requirements for System Engineer - Cyber Security:

1. Bachelor’s degree in related discipline, or three to five years equivalent professional experience.
2. Proactive/self-starter. Task driven with ability to work independently.
3. Team player that takes ownership and develops relationships that fosters team success.

Contract Term: Full-Time Employee, 40 hours/week**.**

Start Date: Negotiable

Rate: Negotiable

“All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin."