



CCRI Analyst - Blue Team

Job Description

- Perform security assessments/blue team assessments for all systems, to include hardware, software, and other IT technologies, as requested.
- Evaluate systems using DoD IA security controls, based on DoD IA 8500.01/2, NIST SP 800-53 Rev 4, and CNSSI 1253, as well as other DoD security control categorization and control processes.
- Review routine and ad hoc system vulnerability and STIG compliance scans and identify weaknesses. Conduct root-cause analysis and remediation activities as needed.
- Support the review and approval of Firewall & Domain Naming Standards (DNS) requests. Support includes but not limited to performing a security analysis/assessment of requested changes; provide a brief statement within the request identifying security issues or risks implementing the change would impose on the enterprise network and approve/disapprove requests based off of risk and DISA/DoD policy.
- Monitor risk-related information by using existing USCG Information Security tools/utilities, analytical methodologies, and security best practices.

Required Qualifications

- Active Secret clearance
- CompTIA Security + or CEH certification

Additional Qualifications

- 3-5 Years ISSE, System Administration, or Network Administration experience is considered a plus.
- Experience with Command Cyber Operations Readiness Inspections (CCRIs) and/or other technical Cyber compliance inspections.
- Experience with Defense Information Systems Agency (DISA) STIG Toolset & SCAP.
- Technical understanding and use of Security Technical Implementation Guides (STIGs).
- Working experience of the DoD Information Assurance Vulnerability Management (IAVM) and DHS Information System Vulnerability Management (ISVM) Programs.
- Strong oral and written communication skills.
- Ability to solve complex problems utilizing creative thinking skills.
- Ability to critically analyze and understand systems and communicate system requirements to the customer and senior leadership.
- CISSP is considered a plus.

First Information Technology Services, Inc. is an Equal Opportunity Employer and prohibits discrimination and harassment of any kind. FITS is committed to the principle of equal employment opportunity for all employees and to providing employees with a work environment free of discrimination and harassment. All employment decisions at FITS are based on business needs, job requirements, and individual qualifications, without regard to race, color, ethnicity, religion or belief, sex, sexual orientation, gender identity and/or expression, national origin, family or parental status, disability, military or veteran status, or any other status protected by the laws or regulations in the locations where we operate. FITS will not tolerate discrimination or harassment based on any of these characteristics. FITS encourages applicants of all ages.