**INFORMATION SECURITY SYSTEM ENGINEERING LEAD**
Palm Bay, Florida
Compensation: £100,000 - $150,000
Industry: Aerospace / Aviation / Defense
Job Category: Information Technology - Security
**Job Description:**

- Provide Information Security System Engineering support and technical execution of information security activities associated with the authorization of NIST Risk Management Framework (RMF) hardened information systems.
- Support Security Engineering activities, including design, testing, configuration, management and maintenance of information systems.
- Assist Program Security Architect in the development of, and CONOPS for, emerging security technologies and proposals.
- Support compliance certification and vulnerability assessments as required.
- Support the evaluation, qualification, testing and delivery of security architecture improvement, obsolescence replacement and vulnerability response projects.
- Support information assurance data collection and continuous monitoring updates for assigned security architectures.
- Principles of data flows (e.g., TCP/IP, OSI model).

- Cyber security certification experience RMF and NSA Type 1.
- Communications security experience, i.e., COMSEC, TRANSEC.
- Knowledge of cyber offense and defense requirements, design, and implementation.
- Conduct product research of cyber security products and advancements for the purposes of finding alternate, better, and/or quick prototype solutions.
- Ability to translate customer mission goals into technical requirements.
- Explain technical security needs to non-security team members in a manner that facilitates cross-functional design activities.
- Self-motivation, able to work well independently and within inter-disciplinary engineering teams.
- Conduct complex security architecture analysis to evaluate and mitigate risks.
- Identify security risks, threats and vulnerabilities of networks, systems, applications and new technology initiatives (hardware, software, cross-domain solutions, cryptographic devices, firewalls, intrusion detection systems, anti-virus systems and software deployment tools).
- Provide Information Assurance technical leadership to development teams at internal and external gate reviews such as technical baseline reviews and design reviews.
- Perform functional analysis, timeline analysis, detailed trade studies, requirements derivation and allocation, and interface definition studies to translate customer Information Security requirements into hardware and software specifications.
- Responsible for developing security overlays, data flow diagrams, internal requirements, CONOPs and interface control documents from customer / product requirements.

**Basic Qualifications:**

- Bachelor's Degree and minimum 9 years of prior relevant experience. Graduate Degree and a minimum of 7 years of prior related experience
- 3-5 Years of experience in writing and managing RMF body of evidence documents (e.g., System Security Plan (SSP), Security Compliance Traceability Matrix (SCTM), Risk Assessment Report (RAR), Continuous Monitoring (ConMon) Plan, and Security Assessment Plans and Procedures (SAPP).
- 3-5 Years of experience in securing operating systems (Windows, Linux, Cisco IOS, etc.).
- 3-5 Years of experience in securing embedded systems architectures.
- 3-5 Years of experience in DoD 8570.01-M IAT Level 2 certification (e.g. CySA+, GICSP, GSEC, Security+CE, SSCP, or CCNA Security).
- 3-5 Years of experience in DoD 8570.01-M IASAE Level 2 certification (e.g. CASP+ CE or CISSP (or Associate)).
- 3-5 Years of experience with NSA Type 1 Certification efforts.

- 2-3 Years of experience with AT designs and requirements
- 2-3 Years of experience with TEMPEST procedures and testing processes
- 2-3 Years of experience with engineering processes, concepts and information security systems engineering principles (NIST SP 800-160 Vol1).

**Preferred Qualifications:**

- Experience in configuration and use of cyber defense and vulnerability assessment tools such as ACAS and SCC
- Experience in the content development and administration of SEIM/audit reduction tools (e.g., Splunk).
- System testing and evaluation methods and RMF assessment methodology & process.
- Experience with application of STIGs.
- Experience with IBM Rational DOORS for requirements management
- Telecommunications network engineering experience.
- Experience in Cyber Defense technologies.
- Experience with radio communication protocols
- Experience with Model Based Systems Engineering (MBSE) techniques
- Understanding of system vulnerabilities and exploitation.
- Self-motivation, able to work well independently and within inter-disciplinary engineering teams.

- Strong written and oral communication skills.

**COMPENSATION**
Base Salary - $100,000 to $150,000

**CANDIDATE DETAILS**
**7+ to 10 years experience**
Seniority Level - Mid-Senior
Management Experience Required - No
Minimum Education - Bachelor's Degree
Willingness to Travel - Occasionally

**IDEAL CANDIDATE**
Ideal candidate will be in the Central Florida area with an aerospace/aviation and defense background.