Job Title: DevSecOps Cyber Security Engineer (Level 2/3/4)
Job Location: Colorado Springs, Colorado
Security Clearance: SECRET
Clearance Status: Must be Obtainable

Job Summary:

Responsible for designing and implementing a Continuous Integration (CI) / Continuous Delivery (CD) pipeline for an advanced military satellite command and control system used for the Wideband Global SATCOM (WGS) constellation of satellites. The Cyber Security Engineer will support development of "Security as Code" within an Agile framework for the Global SATCOM Configuration Control Element (GSCCE), which is responsible for controlling the payload of all on-orbit WGS satellites while incorporating enhancements necessary to control the newest satellite to the constellation, WGS-11. The candidate will participate as part of the DevSecOps team to architect, design, implement, and maintain the pipeline and deployment environments. The candidate will apply an interdisciplinary, collaborative approach to plan, design, develop, validate, and verify life-cycle balanced information system security solutions.

The ideal candidate for this position will have experience and knowledge implementing cyber security processes, methods, and tools within a DevSecOps environment using a mixture of interdisciplinary skills including those from the software engineering, test engineering, systems engineering, and cyber security engineering domains. The position anticipates a heavy emphasis on modern Static and Dynamic analysis tools such as SonarQube/Coverity, JFrog XRay, Twistlock/Aqua to enable quality gates within a software factory. The position will also benefit from a candidate experienced with the Government's Risk Management Framework (RMF) and the accreditation process for fielding classified systems.

Primary Responsibilities:

- Participate as a member of the DevSecOps team by implementing and maintaining solutions within the CI/CD pipeline across environments (source control, package management, configuration management, infrastructure as code, configuration as code, orchestration, and testing)
- Evaluate customer/operational needs to define and coordinate system security requirements, integrate technical parameters and assure compatibility of all physical, functional and program interfaces throughout the development lifecycle.
- Identify assets and assesses risks, threats, and vulnerabilities of the product assets in accordance with accepted industry, professional, and government standards to ensure security design integrity, availability, confidentiality, and non-repudiation.
- Evaluate and implement remediation recommendations
- Employ system security processes, methods, and tools and assures their consistent application.
- Utilize modern Static and Dynamic analysis tools such as SonarQube/Coverity, JFrog XRay, Twistlock/Aqua to enable quality gates within a software factory

- Builds and maintains a secure software factory using hardened containers in a Kubernetes/OpenShift platform
- Occasional travel required

Required Qualifications:

- Ability to obtain an interim U.S. Government SECRET security clearance (requires US Citizenship)
- Experience working on an Agile development team using a CI/CD pipeline
- Prior work experience in cyber security
- Ability to isolate and resolve complex problems, identify workarounds, and implement and document corrective actions
- Good verbal and written communication skills

Preferred Qualifications:

- Active U.S. Government SECRET security clearance
- Experience with scripting languages a plus (PowerShell, Groovy)
- Experience with Jira, Confluence, Git, Artifactory, SonarQube, XRay, Jenkins, Ansible, OpenShift, Docker, Kubernetes or similar tools will be helpful
- Experience with Virtualization (Vmware, AWS)
- Experience with web service technologies, protocols, and standards (REST, SOAP, JMS, JSON)
- Experience with DOD Security Controls desirable
- Experience implementing RMF (Risk Management Framework) desirable

Educational Requirements:

- *Engineer Level 2*: Bachelor's degree and 3 or more years relevant experience, Master's degree and relevant experience, or 6 or more years relevant military satellite communications experience
- *Engineer Level 3*: Bachelor's degree and 7 or more years relevant experience, Master's degree and 4 or more years relevant experience, or 10 or more years relevant military satellite communications experience
- *Engineer Level 4*: Bachelor's degree and 12 or more years of experience, Master's with 9 or more years of experience

(Degrees must be from an accredited course of study in engineering, computer science, mathematics, or physics)

Ascension Engineering Group is an Equal Opportunity Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, pregnancy, sexual orientation, gender identity, national origin, age, protected veteran status, or disability status.