

DevSecOps Engineer

Job Description:

- Manage static and dynamic application security testing for vulnerabilities and embed security tools in Jenkins pipeline.
- Automation/Build such as Jenkins, Docker, Chef or Puppet
- Designing and implementing container (Docker) solutions on Kubernetes or OpenShift
- Design and implementation of Continuous Integration, Continuous Deployment, Continuous Delivery and DevOps Operations for Agile projects, working with technologies and platforms including UNIX/Linux, Java, Git, Jenkins, OpenStack, Ansible, Chef, Puppet, Kubernetes and Docker
- Converting the agile process to the DevSecOps Framework.
- Modify and develop new CI/CD pipelines to support a wide variety of software languages and software product teams.
- Automated processes to support continuous software deployments.
- Linux Administration (Installation, Configuration, Tuning and Upgrades of Linux)

EDUCATIONS:

- Bachelor's degree in Computer Science, Computer Engineering, Information Technology or IT related field.
- Experience in application security, secure software development, vulnerability management, encryption key management and solution design/configuration of security tools

EXPERIENCES:

- CISSP, GIAC, and/or related certifications preferred
- Knowledge and experience in network security, application security, vulnerability management, encryption key management and/or solution design/configuration of security tools.
- Familiar with public cloud eg. GCP, AWS or Azure
- Familiar with DevOps technology and platform; Kubernetes, Terraform, Ansible, Jenkins, Git
- Good command of written and spoken English.
- Good interpersonal skills – able to communicate effectively with various levels (from end-users to executives).
- Logical & systematic approach to problem solving