DevSecOps Lead

Concept Plus is a mission-focused technology solutions provider that transforms IT concepts into impactful solutions for federal agencies. Headquartered in Fairfax, VA, we bring the agility, responsiveness, and customer intimacy of a small business combined with the quality and infrastructure of a larger firm.

Recognized as an award-winning Oracle partner, we have delivered innovative solutions across Defense, Intelligence, Civilian, Health IT, and Tribal sectors. Our highly certified experts build systems that drive efficiency, accelerate modernization, and ensure mission outcomes with certainty.

We offer competitive pay, comprehensive health, dental, and vision insurance, paid life insurance, paid time off, 11 paid holidays, performance bonuses, tuition reimbursement, unlimited training, and the opportunity to thrive in a collaborative, flexible, and innovative environment.

For more information, visit www.conceptplus.com.

About the role

Concept Plus LLC is seeking an experienced DevSecOps Lead to drive the design, implementation, and continuous improvement of secure CI/CD pipelines, automated testing frameworks, and Infrastructure as Code (IaC) practices to provide common services for Oracle eBusiness applications hosted on Oracle Cloud Infrastructure (OCI) platforms. The DevSecOps Lead will embed security, quality, and automation throughout the entire service lifecycle — from development through operations — ensuring that all common services on the Cloud One Oracle Cloud Infrastructure (OCI) platform are delivered with speed, rigor, and compliance. This is a key leadership role requiring a minimum of 5 years of hands-on DevSecOps experience, including demonstrated proficiency with YAML, Ansible, Git, Jenkins or equivalent pipeline tooling (e.g., GitLab CI/CD), Terraform-based IaC, and Kubernetes (K8s) container orchestration, along with experience operating in a DoD or Federal security-controlled environment. An active Secret clearance and DoD 8140/8570 IAT-II or higher certification are required to start.

What you'll do

- Design, implement, and maintain secure CI/CD pipelines using Jenkins, GitLab CI/CD, or comparable enterprise tooling to automate build, test, and deployment workflows for all common services on OCI
- Develop and maintain Infrastructure as Code (IaC) using Ansible, YAML, and Terraform to automate environment provisioning, configuration management, and compliance enforcement across OCI environments
- Architect, deploy, and manage containerized workloads using Kubernetes (K8s) or OCI Container Engine (OKE), including cluster configuration, workload scheduling, secrets management, and runtime security controls
- Integrate SAST, DAST, software composition analysis (SCA), and container image scanning tools into all CI/CD pipelines to enforce security-left practices throughout the development lifecycle

- Establish and maintain a comprehensive automated test framework — including unit, integration, regression, and performance testing — in support of the Government's Test Automation objectives
- Enforce code quality, branching strategies, and version control governance across all development teams using Git (GitHub, GitLab, or equivalent)
- Embed DoD RMF controls and security compliance checks into CI/CD workflows to support continuous ATO and audit readiness
- Collaborate with the Cybersecurity Lead/ISSO to ensure all pipeline artifacts, container images, and deployed services meet required security scanning thresholds and DoD 8140/8570 compliance baselines
- Lead DevSecOps toolchain onboarding, training, and standards adoption across all integrated team members
- Monitor pipeline performance, test coverage metrics, and deployment frequency; report results to the Program Manager and Government stakeholders as part of recurring performance reporting
- Support the Technical Lead in aligning DevSecOps practices with the OCI platform architecture, including OCI DevOps services, OCI Artifact Registry, and OCI Vault
- Develop and maintain automated patching, configuration compliance, and vulnerability remediation workflows to support 24/7/365 operational sustainment requirements
- Contribute to AI/ML integration efforts by implementing automated pipelines for model training, validation, and deployment within the authorized OCI environment
- Support transition-in activities by assessing the incumbent's existing pipeline tooling, identifying gaps, and migrating to the team's DevSecOps toolchain with no disruption to operations

Required Qualifications

- US Citizen
- Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or related technical field
- 5+ years of hands-on DevSecOps, platform engineering, or software delivery engineering experience
- Proficiency with YAML for configuration, pipeline, and IaC definition
- Hands-on experience with Ansible for configuration management and automated provisioning
- Proficiency with Git-based version control (GitHub, GitLab, Bitbucket, or equivalent) and branching/merge strategies
- Hands-on experience designing and maintaining CI/CD pipelines using Jenkins, GitLab CI/CD, or comparable enterprise pipeline tooling
- Demonstrated experience implementing Infrastructure as Code (IaC) using Terraform, including state management, module design, and automated compliance enforcement
- Demonstrated experience deploying and managing containerized applications using Kubernetes (K8s), including cluster administration, Helm charts, namespace management, and workload security

- Experience integrating SAST, DAST, and security scanning tools into automated pipelines (e.g., SonarQube, Fortify, Checkmarx, Twistlock/Prisma Cloud, or equivalent)
- Experience building and maintaining automated test frameworks for web services, APIs, or enterprise applications
- Familiarity with DoD RMF, ATO processes, and embedding security compliance into development and deployment pipelines
- Active DoD Secret clearance required to start; must be maintainable for the duration of the program
- Active DoD 8140/8570 IAT-II or higher certification required at time of hire (qualifying certifications include CompTIA Security+ CE, CompTIA CySA+, GSEC, SSCP, GICSP, CND, or any IAT-III equivalent such as CASP+ CE, CISSP, CISA, CCNP Security, GCED, or GCIH)

Preferred Qualifications

- Active Top Secret (TS) security clearance; candidates holding an active TS clearance will be given strong preference as the program's operational scope and data sensitivity may require TS access
- Experience with FlexDeploy (Flexagon) as a DevOps orchestration and release automation platform, particularly for Oracle-technology deployments including Oracle eBS, Oracle Fusion Middleware, SOA Suite, or WebLogic
- Experience operating within a DISA-managed or Cloud One cloud environment, including familiarity with IL4/IL5 authorization boundaries and FedRAMP controls
- Hands-on experience with OCI DevOps services, OCI Container Engine for Kubernetes (OKE), OCI Artifact Registry, or OCI Vault
- Familiarity with Oracle eBusiness Suite (eBS), Oracle Fusion Middleware, or Oracle database environments and associated patch/deploy automation
- Experience with automated testing tools such as Selenium, Robot Framework, Postman/Newman, JMeter, JUnit, TestNG, or Cucumber
- Experience with security scanning tools specific to Oracle or Java-based environments (e.g., Fortify for Java, OWASP ZAP, or Oracle-specific vulnerability scanning)
- Additional certifications such as Certified Kubernetes Administrator (CKA), HashiCorp Terraform Associate, OCI DevOps certifications, or DoD 8140 CSSP Analyst/Developer designations
- Prior experience supporting AFLCMC, BES Directorate, or a DoD ERP program of record
- Familiarity with Agile/SAFe delivery frameworks and sprint-based DevSecOps execution within Integrated Team Structures

Concept Plus is an Equal Opportunity Employer. As such, we will give your application full consideration without regard to your race, color, religion, sex, age, national origin, disability, veteran status, sexual orientation, gender identity, or any other classification protected by federal, state, or local law.