



DevSecOps Engineer

Description: Cassidy Consulting Group is seeking a DevSecOps Engineer. This is a W-2 job opportunity. Please visit our website to learn more about Cassidy Consulting Group – <https://www.cassidyconsulting.us>.

Position Description:

This position is for a DevSecOps Engineer supporting the Army Edge Computing Capability (AECC) project that ALTESS is fielding for the US Army. The AECC solution is a hyperconverged, multitenant hosting environment for hosting Army enterprise and tactical applications. AECC is transitioning to a Kubernetes-based container orchestration platform, which may include Red Hat OpenShift or other Kubernetes distributions, to implement a modernized Software Defined Data Center (SDDC). The DevSecOps Engineer will play a critical role in modernizing applications into a DevSecOps framework, leveraging tools such as GitLab, Terraform, Ansible, and other automation and security tools to streamline development, deployment, and security processes. ALTESS provides value-added common and managed services built on top of the Kubernetes foundation, which hosted Army applications will require. ALTESS is a managed service provider (MSP) and hosting services provider for Army applications. ALTESS is a Product Lead office under Capability Program Executive (CPE) Enterprise Software and Services (CPE ES2).

Position Responsibilities:

- Design, implement, and maintain a DevSecOps framework for modernizing applications hosted in the AECC environment.
- Integrate tools such as GitLab Ultimate, Terraform, and Ansible into CI/CD pipelines to automate application development, deployment, and security processes.
- Develop and enforce security gates within CI/CD pipelines to ensure secure code, container images, and configurations are deployed.
- Collaborate with developers to containerize legacy applications and migrate them into Kubernetes-based environments.
- Integrate static application security testing (SAST), dynamic application security testing (DAST), and container image scanning tools into CI/CD pipelines.
- Use tools such as Trivy, Clair, or Anchore to scan container images for vulnerabilities.
- Implement secrets management solutions (e.g., HashiCorp Vault, Sealed Secrets) to securely manage sensitive data in pipelines and applications.
- Monitor CI/CD pipelines and Kubernetes workloads for performance, security, and compliance using the GitLab CI/CD dashboards.
- Optimize pipeline performance and resource utilization to reduce deployment times and improve scalability.
- Work closely with developers, Kubernetes administrators, and cybersecurity teams to ensure applications meet security and operational requirements.
- Provide training and guidance to development teams on DevSecOps best practices, tools, and workflows.
- Collaborate with internal and external stakeholders to transform high-level technical objectives into comprehensive technical requirements.
- Ensure applications and pipelines comply with frameworks such as DoD RMF, CIS Benchmarks, and NIST 800-53.
- Generate reports on pipeline security, application compliance, and deployment metrics for leadership and stakeholders.

Required Skills:

- Strong expertise in implementing and managing DevSecOps frameworks using tools such as GitLab, Azure DevOps, or Atlassian.
- Proficiency in Infrastructure as Code (IaC) tools, including Terraform and Ansible.

- Experience with containerization and orchestration tools, such as Docker, Kubernetes, and Red Hat OpenShift.

Desired Skills:

- Knowledge of static application security testing (SAST) and dynamic application security testing (DAST) tools (e.g., SonarQube, OWASP ZAP, Burp Suite).
- Familiarity with container image scanning tools (e.g., Trivy, Clair, Anchore).
- Experience with secrets management tools (e.g., HashiCorp Vault, Sealed Secrets).
- Proficiency in scripting languages (e.g., Python, Bash, PowerShell) for automating tasks and workflows.
- Experience with CI/CD pipeline automation and optimization.
- Working knowledge of DoD STIGs, IA Vulnerability Management (IAVM), and Risk Management Framework (RMF) and/or industry hardening best practices and processes.
- Experience with monitoring tools such as Prometheus, Grafana, and GitLab CI/CD dashboards.
- Strong troubleshooting skills for diagnosing issues in CI/CD pipelines and Kubernetes workloads.

Education & Experience: Bachelor's degree or higher in IT-related field (or equivalent experience).

Required Certifications:

- DoD 8570.01-M IAT Level II certification (e.g., Security+ CE).
- Must obtain computing environment certifications (e.g., any GitLab certification, Azure DevOps, Jira, etc.) within 6 months of hire.

Security Clearance: DoD Secret Clearance (must be active or obtainable)

Location: Radford, VA (hybrid/telework onsite as needed)

Cassidy Consulting Group is an Equal Employment Opportunity employer. Cassidy Consulting Group prohibits discrimination against employees and qualified applicants for employment on the basis of race, color, religion, sex (including pregnancy), age, disability, marital status, national origin, veteran status, or any other classification protected by applicable discrimination laws.