DevSecOps Engineer

Security | SMB | Enterprise

[Company Name] is hiring a DevSecOps Engineer to embed security throughout our software development lifecycle. You will build automated security scanning into CI/CD pipelines, define infrastructure security policies as code, and partner with engineering teams to remediate vulnerabilities before they reach production. This role bridges development, operations, and security to create a culture where shipping fast and shipping securely are the same thing.

Key Responsibilities

- Integrate static analysis (SAST), dynamic analysis (DAST), and software composition analysis (SCA) into CI/CD pipelines
- Design and enforce infrastructure security policies using policy-as-code frameworks
- Build automated vulnerability scanning and container image scanning workflows
- Collaborate with development teams to triage and remediate security findings
- Manage secrets management solutions and enforce rotation policies
- Conduct threat modeling sessions for new features and architecture changes
- Maintain compliance automation for standards such as SOC 2, ISO 27001, or HIPAA

Required Skills & Experience

- 3+ years of experience in DevOps, SRE, or security engineering roles
- Hands-on experience integrating security tools into CI/CD pipelines (GitHub Actions, GitLab CI, Jenkins)
- Proficiency with container security scanning tools (Trivy, Snyk Container, or Aqua)
- Experience with infrastructure-as-code security (Terraform Sentinel, Checkov, or tfsec)
- Knowledge of OWASP Top 10 vulnerabilities and common remediation strategies
- Familiarity with secrets management tools (HashiCorp Vault, AWS Secrets Manager)
- Strong scripting skills in Python, Bash, or Go
- Understanding of cloud security fundamentals in AWS, Azure, or GCP

Nice-to-Have

- Experience with policy-as-code frameworks such as Open Policy Agent (OPA) or Kyverno
- Familiarity with SBOM generation and supply chain security tooling
- Knowledge of compliance frameworks (SOC 2 Type II, ISO 27001, FedRAMP)
- Experience with runtime security monitoring tools (Falco, Sysdig)
- Relevant certifications (CISSP, CEH, AWS Security Specialty, or CKS)

Tech Stack

Snyk | Trivy | HashiCorp Vault | Terraform | GitHub Actions | Open Policy Agent | Docker | Kubernetes | SonarQube

What We Offer

- Competitive salary and equity package
- Flexible remote or hybrid work arrangement
- Health, dental, and vision insurance
- Annual learning and development budget
- Generous PTO policy

Interview Process

1. Recruiter phone screen (30 min) — role fit and logistics
2. Technical phone screen (45 min) — security fundamentals and CI/CD concepts
3. Hands-on exercise — review a CI/CD pipeline configuration and identify security gaps
4. On-site or virtual loop (3 hours) — threat modeling scenario, architecture discussion, and team fit
5. Offer and reference checks