

Senior DevSecOps Engineer

Location: Remote - United States
Department: Engineering / Platform
Reports to: CTO
Employment: Full-time

About WellBeam

WellBeam is a healthcare interoperability platform connecting health systems, physicians, and post-acute providers. We power clinical orders, secure messaging, and care coordination for health systems, independent medical groups, home health, and hospice agencies.

Our platform integrates with EHRs such as Epic, Cerner, and HCHB using HL7, FHIR, DIRECT, SFTP, eFax, REST APIs, and other enterprise integration methods. Because we move protected health information every day, security, reliability, and compliance are core product requirements.

The Role

We are hiring a Senior DevSecOps Engineer: a hands-on cloud and DevOps engineer who thinks security-first. You will own and improve WellBeam's AWS infrastructure, delivery pipelines, production reliability, and day-to-day security operations, while serving as our internal technical security lead for SOC 2 and HIPAA.

This is a hands-on individual contributor role within our Platform team, reporting to the CTO and partnering with Engineering, Product, Integrations, Customer Delivery, and external security/compliance advisors. You will consolidate responsibilities currently spread across engineers, automate them, and establish how we securely operate production at scale.

What You'll Do

Infrastructure & Delivery

- Own and improve our multi-account AWS environment, including ECS/Fargate, ECR, ELB/Auto Scaling, RDS MySQL (Multi-AZ), S3, SQS, Route 53, KMS, and VPC networking.
- Maintain and expand Infrastructure as Code (CloudFormation today); keep environments reproducible, reviewable, securely separated, and lead tooling changes where they clearly pay off.
- Own and improve CI/CD using Jenkins and GitHub; automate deployment/rollback and embed SAST, dependency/SCA, container scanning, and secrets detection.
- Keep production, staging, QA, and development stable, secure, consistent, resilient, and cost-efficient; continuously evaluate capacity, performance, and cost.
- Support site-to-site VPN and HL7-over-HTTPS connectivity with hospital customers alongside the Integrations team.

Security Operations

- Run vulnerability management end to end: triage and prioritize findings from AWS Inspector, GuardDuty, Security Hub, external scanners, penetration tests, and customer assessments; drive remediation and verification to closure.
- Coordinate third-party penetration tests and own remediation plans and retest evidence.
- Own IAM/least privilege, secrets and key management, encryption standards, vulnerability/patch management, and external security-rating posture.
- Manage endpoint security and device management for our remote workforce; help design and test incident response, lead tabletop exercises, and participate in post-incident reviews.

Reliability & Observability

- Build observability with Datadog and AWS CloudWatch across metrics, centralized logging, tracing, dashboards, and actionable alerting; expand into SIEM/security use cases as needs mature.
- Improve visibility into application health, background processing, integrations, infrastructure performance, and customer-impacting failures; establish meaningful SLIs/SLOs and reduce alert fatigue.
- Strengthen backup, disaster recovery, high availability, and business continuity; define and regularly test RTO/RPO, restore procedures, and backup recovery.
- Join the engineering on-call rotation and make it calmer through automation, better alerting, root-cause analysis, and elimination of recurring failure modes.

Security, Compliance & Program Leadership

- Own technical controls and evidence supporting SOC 2 Type 2 and HIPAA, including change/access management, logging, vulnerability management, backups, encryption, and incident response.
- Own the technical side of our compliance automation platform, keep evidence current year-round, automate evidence collection where practical, and lead technical preparation for the annual SOC 2 Type 2 audit.
- Lead WellBeam's annual HIPAA Security Risk Assessment, maintain the security risk register, and track identified risks through remediation.

- Maintain architecture, PHI data-flow, security-control, and operational runbook documentation so audits and customer security reviews are routine rather than fire drills.
- Act as WellBeam's internal technical security lead: own security policies/procedures and annual reviews, customer security questionnaires, and technical security discussions with hospital IT, security, and procurement teams.
- Run third-party/vendor security reviews; support security-related BAA/vendor records; coordinate security awareness training and phishing education.
- Report security posture, material risks, vulnerabilities, incidents, audit readiness, and security/reliability metrics to the CTO and leadership.

What You'll Bring

- 5+ years in DevOps, SRE, cloud infrastructure, or similar engineering roles, including 2+ years with meaningful security ownership.
- Deep hands-on AWS production experience: ECS or other container orchestration, IAM, VPC networking, RDS, KMS, CloudTrail, GuardDuty, Inspector, and Security Hub.
- Infrastructure as Code experience with CloudFormation, CDK, Terraform, or comparable tooling; strong CI/CD design with security scanning integrated into the development lifecycle.
- Strong cloud/application security fundamentals: IAM and least privilege, network security, TLS/encryption, secrets/key management, vulnerability management, secure SDLC, logging/monitoring, and incident response.
- Hands-on vulnerability management: triaging scanner and pen-test findings, prioritizing real risk, and driving remediation through closure.
- Experience supporting SOC 2 and HIPAA or comparable programs, including audits, technical evidence, risk assessments, policies, and customer security reviews.
- Production monitoring, centralized logging, alerting, and incident response experience; strong troubleshooting across application, networking, cloud, and infrastructure layers.
- Comfortable with Docker, Linux, TLS/DNS/VPN networking fundamentals, and scripting in Bash, Python, JavaScript/Node.js, or similar languages.
- Clear written/verbal communication and ability to work independently, identify gaps, propose pragmatic solutions, and drive them through completion.

Nice to Have

- Healthcare or other regulated-industry experience, including HIPAA, HITRUST, or healthcare security requirements.
- Healthcare interoperability experience with HL7, FHIR, SFTP, REST APIs, site-to-site VPNs, and hospital IT/security teams.
- Datadog experience across APM, log management, infrastructure monitoring, or Cloud SIEM; experience with Vanta, Drata, or similar compliance automation.
- MDM, endpoint security, DLP, or EDR experience for a remote workforce; application security and secure SDLC experience.
- Experience supporting Node.js/JavaScript and React/React Native delivery pipelines.
- AWS Security Specialty, CISSP, Security+, or another relevant cloud/security certification.

Why You'll Love Working at WellBeam

- Competitive salary and equity participation
- Remote work with flexible working hours
- Monthly team dinners (if local to the SF Bay Area) and regular company-wide offsites
- Generous holidays and Paid Time Off
- Health, vision, and dental insurance options
- 401(k)

Compensation Range: \$120,000 - \$170,000

Interested?

Email recruitment@well-beam.com with the role title in the subject line. Please include a brief introduction and your resume.