CB

CloudBridge DevOps Consulting

DevSecOps — Security Engineering Program

Integrate security into every phase of the SDLC. SAST, DAST, container security, secrets management, compliance-as-code — build secure pipelines from day one.

Duration	Mode	Fee	Placement
10 Weeks	Live Online + Offline (Hyd)	Rs 80,000 (one-time)	100% Assurance

Designed for: Australia | United States | Canada | Singapore | Germany | India (Offline)

Target Audience: Onsite Professionals | Domain Change Professionals | IT Engineers

Tools & Technologies Covered:

SonarQube | Trivy | Snyk | OWASP ZAP | HashiCorp Vault | Checkov | OPA | Kyverno | Falco | GitLeaks | Cosign | Semgrep | Docker Bench | AWS Security Hub

Contact Us

Phone: +91 7993 822600 | WhatsApp: wa.me/917993822600

Address: 506, Manjeera Majestic Homes, Kukatpally, Hyderabad, Telangana 500072

Detailed Curriculum

Module 1 DevSecOps Fundamentals & Shift-Left Security

Topics

- DevSecOps principles and culture
- Shift-left security: Embedding security early in SDLC
- Security as Code: Automation-first approach
- Threat modeling: STRIDE, DREAD, attack trees
- Security champions program in DevOps teams
- Compliance frameworks: SOC 2, ISO 27001, PCI-DSS, HIPAA
- Risk assessment and vulnerability management lifecycle
- OWASP Top 10 web application vulnerabilities

Hands-on Practice

- Conduct threat modeling exercise
- Create security requirements for a sample app
- Map OWASP Top 10 to real-world vulnerabilities
- Design a DevSecOps pipeline architecture

Module 2 SAST — Static Application Security Testing

Topics

- SonarQube: Architecture, quality profiles, quality gates
- SonarQube installation and configuration
- Code quality metrics: Bugs, vulnerabilities, code smells, debt
- Custom quality gates and thresholds
- SonarQube integration with CI/CD pipelines
- Semgrep: Pattern-based static analysis
- CodeQL: GitHub Advanced Security
- IDE integration: SonarLint for developers

Hands-on Practice

- Deploy SonarQube on Docker/Kubernetes
- Configure quality profiles and gates
- Integrate SonarQube with Jenkins/GitHub Actions
- Fix real vulnerabilities found by SAST
- Set up quality gate as CI pipeline blocker

Module 3 Container Security & Image Scanning

Topics

- Container threat landscape and attack vectors
- Trivy: Comprehensive vulnerability scanner
- Snyk Container: Image and dependency scanning
- Docker Bench Security: CIS benchmark compliance
- Image hardening: Distroless, scratch, minimal base images
- Container runtime security: Falco, AppArmor, Seccomp
- Registry security: Signing, scanning policies, admission control
- Kubernetes Pod Security Standards and Policies

Hands-on Practice

- Scan container images with Trivy
- Integrate Snyk in CI/CD pipeline
- Harden Docker images following CIS benchmarks
- Configure Kubernetes Pod Security Standards
- Set up admission controllers for image scanning

Detailed Curriculum (continued)

Module 4 — DAST — Dynamic Application Security Testing

Topics

- DAST concepts: Black-box testing, fuzzing, crawling
- OWASP ZAP: Architecture, spider, active scan, passive scan
- ZAP automation in CI/CD pipelines
- Burp Suite essentials for security testing
- API security testing: REST, GraphQL
- IAST: Interactive Application Security Testing overview
- Penetration testing workflow and reporting

Hands-on Practice

- Run OWASP ZAP scan on test application
- Automate ZAP scanning in CI pipeline
- Perform API security testing
- Generate and analyze security reports

Module 5 — Secrets Management & Encryption

Topics

- HashiCorp Vault: Architecture, secrets engines, auth methods
- Vault deployment: Dev, HA, auto-unseal
- Dynamic secrets for databases and cloud providers
- PKI and certificate management with Vault
- Kubernetes secrets: External Secrets Operator, Sealed Secrets
- AWS Secrets Manager, Azure Key Vault, GCP Secret Manager
- Git secrets detection: GitLeaks, TruffleHog, detect-secrets
- Encryption at rest and in transit best practices

Hands-on Practice

- Deploy HashiCorp Vault on Kubernetes
- Configure dynamic database secrets
- Integrate Vault with Kubernetes workloads
- Set up pre-commit hooks for secret detection
- Implement External Secrets Operator

Module 6 — Infrastructure Security & Compliance-as-Code

Topics

- Infrastructure scanning: Checkov, tfsec, Terrascan
- Cloud security posture management (CSPM)
- Policy-as-code: Open Policy Agent (OPA), Rego
- Kubernetes policy enforcement: Kyverno, Gatekeeper
- Network security: Zero Trust architecture
- Service mesh security with Istio
- Compliance-as-code: InSpec, Chef Compliance
- Security monitoring and SIEM integration

Hands-on Practice

- Scan Terraform code with Checkov
- Write OPA policies for Kubernetes
- Configure Kyverno policies on cluster
- Implement network policies for Zero Trust
- Create compliance audit automation

Detailed Curriculum (continued)

Module 7 — Security in CI/CD Pipelines

Topics

- Secure pipeline architecture and design patterns
- Dependency scanning: OWASP Dependency-Check, Snyk SCA
- Software Bill of Materials (SBOM) generation
- Signed commits and artifact signing (Sigstore, Cosign)
- Supply chain security: SLSA framework
- Security gates: Blocking deployments on vulnerabilities
- Automated remediation and fix suggestions
- Security dashboards and reporting

Hands-on Practice

- Build complete DevSecOps pipeline
- Integrate all security tools in CI/CD
- Configure security gates with fail criteria
- Generate and verify SBOM
- Sign container images with Cosign

Capstone Project

Every student completes a **full end-to-end production deployment project** — from application inception through CI/CD pipeline creation, security scanning, infrastructure provisioning, container orchestration, monitoring setup, and production release. This is NOT a demo — this is a real production-grade deployment.

- Complete application code to multi-cloud production deployment
- Automated CI/CD pipeline with security gates and quality checks
- Infrastructure as Code with Terraform modules
- Kubernetes deployment with Helm charts and ArgoCD GitOps
- Full monitoring, alerting, and incident response setup
- Cost optimization and automated scheduling
- Complete documentation and architecture diagrams

Batch Schedule & Enrollment

Next Batch: **27th February 2026**

Country	Schedule	Timing
Australia	MON-FRI (12 Weeks)	6:30 PM - 8:30 PM AEST
US / Canada	MON-FRI (12 Weeks)	8:00 PM - 10:00 PM EST
Singapore	MON-FRI (12 Weeks)	7:00 PM - 9:00 PM SGT
Germany	MON-FRI (12 Weeks)	7:00 PM - 9:00 PM CET
India (Offline)	MON-FRI (12 Weeks)	10:00 AM - 1:00 PM IST

Course Fee: Rs 80,000 (One-time Single Payment)

This is 100% real-time production-based training, not pre-recorded theory.

100% Placement Assurance | Lifetime Access to Recordings | Dedicated Mentor

Enroll Now:

Phone / WhatsApp: **+91 7993 822600**

Address: 506, Manjeera Majestic Homes, Kukatpally Housing Board Colony, Hyderabad, Telangana 500072

Facebook: facebook.com/profile.php?id=61588159723801

Instagram: instagram.com/anumulasetty.1

YouTube: youtube.com/channel/UCeEKRXyy3Zzn3QC5kVen84A