DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

DevSecOps Advanced Training

Scale DevSecOps across an organisation with a maturity roadmap, SLSA supply chain controls, compliance evidence and security metrics.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **5 days · Days 1-5**	SELF-PACED VIDEO **1-year LMS access**
BATCH SIZE **Max 10 learners**	NEXT BATCHES **1st of every month · weekends: first Saturday**	CERTIFICATE **Verifiable certificate of completion**

Foundation	Essential	Intermediate	Advanced
1 day · Included	2 days · Included	3 days · Included	5 days · This curriculum

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	50 topics · Foundation to Advanced
Hands-on labs	4 labs
Formats and fees	Live, self-paced, corporate
Trainer and reviews	Rajesh Kumar
Enrolment	Batches, payment, contacts

WHY DEVOPSSCHOOL

- Rated 4.6 on Google
- 1,500+ verifiable certificates issued in the public registry
- Trainer Rajesh Kumar: 20 years in industry
- Small batches: max 10 learners, every session recorded

Course page: www.devopsschool.com/courses/devsecops/devsecops-advance-training.html
Talk to us: WhatsApp +91 99057 40781 · +1 (469) 756-6329 · contact@DevOpsSchool.com · reply within 1 hour

OUTCOMES

What you will achieve

By the end of the DevSecOps course path, you will be able to:

1

Embed security in CI/CD

Add SAST, SCA, secrets, container, IaC and DAST checks to pipelines so every change is tested for security.

2

Secure cloud-native workloads

Protect Kubernetes and cloud deployments with policy as code, runtime detection, managed secrets and signed artifacts.

3

Lead DevSecOps adoption

Use DSOMM, compliance as code and security metrics to plan and measure DevSecOps maturity across teams.

WHAT THE ADVANCED LEVEL ADDS

Maturity, governance and enterprise DevSecOps

Hands-on: Capstone: enterprise DevSecOps pipeline. Design and build a complete DevSecOps pipeline for a microservice with all scan stages, signed artifacts with SLSA provenance, policy gates and a findings dashboard.

WHO SHOULD ATTEND

- Experienced DevSecOps practitioners responsible for quality, security and scale.
- Senior engineers, architects and leads who design and troubleshoot DevSecOps solutions.
- Teams making DevSecOps an organisation-wide standard.

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Secure Kubernetes and cloud workloads with policy as code, runtime detection, signed artifacts and automated compliance checks.
- Basic computer skills and a laptop with a stable internet connection for the live sessions and labs.
- This curriculum includes every earlier level, so it is complete on its own.

AGENDA · FOUNDATION TO ADVANCED

DevSecOps Advanced Training agenda

50 topics. Each level builds on the one before it, so this curriculum lists every earlier level in full. Days are for corporate (day-wise) delivery; live online batches cover the same agenda in max 8-10 hours.

DAY 1 — Foundation: DevSecOps concepts, secure SDLC and core tooling

Included from Foundation

1. Software development foundations: what software development and the SDLC are, SDLC models, Waterfall vs Agile, issues in the traditional way
2. DevOps and CI/CD refresher: what DevOps is, principles, benefits, continuous integration, delivery and deployment, deployment strategies
3. Typical CI/CD toolchain: Git, Bitbucket, Maven, Jenkins, Travis, Docker, Kubernetes, Ansible or Chef, Terraform, InSpec, OWASP ZAP
4. What is DevSecOps: DevSecOps as part of DevOps, OWASP (Open Web Application Security Project), CWE, defect classifications
5. Code analysis basics: static code analysis, dynamic code analysis, secure code review, where each fits in a typical CI/CD pipeline
6. Secure SDLC: activities and security gates across requirements, design, implementation, testing, deployment and maintenance
7. Security in the pipeline: embedding security in CI/CD, DevSecOps challenges with pentesting and vulnerability assessment
8. DevSecOps Maturity Model (DSOMM): maturity levels and tasks, its axes, moving from level 1 to level 4, level-specific practices
9. Software Component Analysis (SCA): SCA solutions, embedding SCA in the pipeline, Black Duck, Sonatype Nexus Lifecycle, JFrog Xray, Snyk
10. SAST: what static application security testing is, pipeline embedding, preventing secrets exposure, Checkmarx, Veracode, Fortify, Coverity
11. DAST: session management and AJAX crawling, SSL misconfiguration testing, baseline scans, scan frequencies, Burp, AppScan, OWASP ZAP
12. Infrastructure as Code: benefits, building blocks, configuration management systems, Ansible modules, tasks, roles and playbooks
13. Compliance as code: handling compliance requirements, using configuration management to achieve compliance, InSpec and OpenSCAP
14. Vulnerability management: managing vulnerabilities across the organization with DefectDojo and RiskSense (now part of Ivanti)

DAY 2 — Essential: Hands-on scanning in the daily team workflow

Included from Essential

15. Git security hygiene: branch protection, signed commits, CODEOWNERS, pre-commit hooks with Gitleaks
16. SAST hands-on: SonarQube quality gates, Semgrep rules on pull requests, triaging and suppressing false positives
17. SCA hands-on: OWASP Dependency-Check, Snyk CLI, Dependabot alerts, fixing vulnerable transitive dependencies
18. Container image scanning: Trivy and Grype, Dockerfile linting with Hadolint, minimal and non-root base images
19. IaC scanning: Checkov and Trivy config for Terraform, CloudFormation and Kubernetes manifests
20. DAST hands-on: OWASP ZAP baseline scan in CI, authenticated scans, reading and acting on ZAP reports
21. Secrets management: HashiCorp Vault basics, Jenkins credentials, limits of Kubernetes Secrets, rotating leaked secrets

22. Threat modelling: STRIDE, data flow diagrams, OWASP Threat Dragon, linking threats to backlog items
23. OWASP Top 10 for developers: injection, broken access control, cryptographic failures and misconfiguration with code-level fixes
24. Security stages in Jenkins: SAST, SCA, image scan and DAST stages, failing builds on severity thresholds
25. Team workflow: security champions, shared responsibility, security acceptance criteria in user stories
26. Findings workflow: importing scan results into DefectDojo, deduplication, owners and remediation SLAs per severity

DAY 3 **Intermediate: Kubernetes, cloud, policy and supply chain security** Included from Intermediate

27. Kubernetes security: Pod Security Standards, RBAC, NetworkPolicies, kube-bench CIS benchmark, admission control
28. Runtime security: Falco rules for container behaviour, alert routing, tuning noisy rules
29. Policy as code: OPA Gatekeeper or Kyverno policies, Conftest for Terraform plans and Dockerfiles
30. Compliance automation: InSpec profiles for CIS benchmarks, OpenSCAP scans, continuous compliance reports
31. Cloud security posture: AWS IAM least privilege, Security Hub, Prowler and ScoutSuite scans, fixing misconfigurations
32. Supply chain security: SBOMs with Syft in CycloneDX or SPDX, cosign image signing, verifying signatures before deploy
33. Dynamic secrets: Vault dynamic database credentials, Kubernetes auth method, External Secrets Operator
34. API security testing: OWASP API Security Top 10, ZAP API scans from OpenAPI definitions, input fuzzing
35. Vulnerability prioritisation: CVSS, EPSS, CISA KEV catalogue, reachability analysis, risk-based remediation
36. Security monitoring: central logs, Kubernetes and cloud audit logs, alerting into a SIEM
37. Hardening CI/CD: least-privilege runners, OIDC federation instead of static cloud keys, protecting build secrets
38. Troubleshooting pipeline security: slow or flaky scans, baselines, handling breaking changes from scanner updates

DAYS 4-5 **Advanced: Maturity, governance and enterprise DevSecOps** **New at this level**

39. DSOMM in practice: assessing current maturity, building a roadmap, comparison with OWASP SAMM, measuring progress
40. Enterprise DevSecOps platform: reusable pipeline libraries, golden paths, central scanner configuration across many repositories
41. SLSA framework: build provenance, isolated builds, in-toto attestations, levels and adoption path
42. Governance and compliance: mapping controls to ISO 27001, SOC 2 and PCI DSS 4.0, evidence collected from pipelines
43. Application security posture management: aggregating SAST, SCA, DAST and cloud findings, risk scoring, executive dashboards
44. Zero trust architecture: identity-aware access, mTLS with a service mesh, workload identity with SPIFFE and SPIRE
45. Security at scale: scanning hundreds of repositories, central rule management, scan scheduling and cost control
46. Incident response: playbooks for leaked secrets and compromised dependencies, container forensics, post-incident reviews
47. Security metrics: mean time to remediate, vulnerability escape rate, security debt, DORA metrics alongside security KPIs

48. Securing AI and LLM workloads: OWASP Top 10 for LLM Applications, prompt injection, model and data supply chain
49. Pentest and red team integration: scoping, feeding pentest findings into the backlog, purple team exercises
50. Capstone: design a secure microservice pipeline with SAST, SCA, IaC and image scanning, signing, DAST and policy gates

PRACTICE

Hands-on labs

You build these yourself during the course, guided by the trainer.

FOUNDATION

Map security tools onto a pipeline

Take a Jenkins pipeline for a Java web application and add a SAST scan, an SCA dependency check and an OWASP ZAP baseline scan, then review the results.

ESSENTIAL

Security-gated Jenkins pipeline

Build a Jenkins pipeline that runs Gitleaks, SonarQube, Dependency-Check, Trivy, Checkov and a ZAP baseline scan, fails on high severity and publishes results to DefectDojo.

INTERMEDIATE

Secure a Kubernetes deployment end to end

Deploy a signed, scanned image to Kubernetes with Kyverno policies, Vault-injected secrets, Falco runtime alerts and an InSpec compliance check.

ADVANCED

Capstone: enterprise DevSecOps pipeline

Design and build a complete DevSecOps pipeline for a microservice with all scan stages, signed artifacts with SLSA provenance, policy gates and a findings dashboard.

HOW YOU CAN LEARN

Formats and fees

The same agenda in three formats. Fees are in Indian rupees as of November 2026; the course page shows them in your currency.

FORMAT	DURATION	WHAT YOU GET	FEE
Live & interactive (online)	Max 8-10 hours	Instructor-led public batch of max 10 learners with demos, labs, Q&A and assignment review. Weekday batches start on the 1st of every month, weekend batches on the first Saturday of every month.	**INR 34,999**
Self-paced video	1-year LMS access	All four DevSecOps levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	5 days for this level	A private batch for your team, on demand. Foundation 1 day, Essential 2, Intermediate 3, Advanced 5 (cumulative). 1:1 training is also available on demand.	**Quote on request**

ASSESSMENT AND CERTIFICATE

Your progress is checked through hands-on labs and assignments at every level. On completion you receive a DevOpsSchool certificate of completion with a unique credential ID that anyone can verify at devopsschool.com/certificates.

INCLUDED WITH EVERY LIVE BATCH

- Every live session is recorded and stays in your LMS for a year.
- Can't attend your batch? Move to next month's batch.
- Free demo class before you pay.
- Free 10-15 minute call with an advisor or the trainer to check the course fits you.

YOUR TRAINER

Learn from Rajesh Kumar

Principal Architect, trainer and mentor in DevOps, SRE, DevSecOps and platform engineering, with 20 years across 8+ software MNCs, including Staff DevOps/SRE Engineer for a leading Japanese mobile-payment platform and Principal DevOps Architect and Manager in Europe.

Profile: www.rajeshkumar.xyz · Videos: youtube.com/@TheDevOpsSchool

20 years in industry	**200+** corporate trainings
10,000+ engineers mentored	**70+** organisations coached

REVIEWS

What learners say

Rated 4.6 on Google · more reviews at devopsschool.com/testimonials and in our video testimonials.

> “Rajesh is very good trainer. Rajesh was able to resolve our queries and question effectively. We really liked the hands-on examples covered during this training program.”
>
> Indrayani, India

> “The training was very useful and interactive. Rajesh helped develop the confidence of all.”
>
> Abhinav Gupta, Pune

START YOUR DEVSECOPS TRAINING

Join the next batch

Weekday batches start on the 1st of every month and weekend batches on the first Saturday of every month, with max 10 learners each. Corporate and 1:1 batches run on demand. We reply within 1 hour.

Pay by UPI, credit and debit cards, net banking or PayPal. Before you pay, read our refund policy. All levels of this course: www.devopsschool.com/courses/devsecops/

ENROL OR RESERVE A SEAT
DevSecOps Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com