DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

# Container Security Advanced Training

Design defense in depth for multi-tenant container platforms with sandboxed runtimes, workload identity, compliance and governance.

| | | |
|---|---|---|
| LIVE ONLINE<br>**Max 8-10 hours** | CORPORATE (DAY-WISE)<br>**5 days · Days 1-5** | SELF-PACED VIDEO<br>**1-year LMS access** |
| BATCH SIZE<br>**Max 10 learners** | NEXT BATCHES<br>**1st of every month · weekends: first Saturday** | CERTIFICATE<br>**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 | 40 topics · Foundation to Advanced |
| Hands-on labs | 4 labs |
| Formats and fees | Live, 1:1, 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/container/container-security-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 Container Security course path, you will be able to:

1

### Build secure images

Produce minimal, scanned, signed images with SBOMs and safe Dockerfiles.

2

### Protect running workloads

Apply pod security, admission policies, RBAC and runtime detection in Kubernetes.

3

### Govern container security

Design defense in depth and compliance evidence for multi-tenant container platforms.

WHAT THE ADVANCED LEVEL ADDS

### Sandboxing, zero trust, compliance and scale

**Hands-on:** Hardened platform capstone. Design a multi-tenant cluster with sandboxed runtimes, signed-image enforcement, workload identity and a compliance evidence pack.

WHO SHOULD ATTEND

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

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Enforce policies at admission, detect runtime threats, lock down cluster access and secrets, and investigate container incidents.
- 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

# Container Security Advanced Training agenda

40 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: Container threats, isolation and image scanning

Included from Foundation

1. Container threat model: image, registry, runtime, orchestrator, host and supply chain risks
2. Isolation primitives: namespaces, cgroups, capabilities, seccomp, AppArmor and SELinux
3. Image anatomy: layers, base images, tags versus digests
4. Common weaknesses: outdated packages, secrets in images, running as root and privileged mode
5. Image scanning: Trivy and Grype, CVE severity and fixed versions
6. Dockerfile security: minimal base images, non-root USER, COPY versus ADD and .dockerignore
7. Registry security: private registries, access control and immutable tags
8. Docker daemon security: socket exposure and rootless mode
9. Benchmarks: CIS Docker Benchmark and docker-bench-security
10. First hardening pass: scan, fix and rescan an application image

## DAY 2 — Essential: Minimal images, SBOMs, signing and pod security

Included from Essential

11. Minimal images: distroless, Wolfi-based images, scratch and multi-stage builds
12. SBOM generation: Syft with CycloneDX and SPDX formats
13. Vulnerability management: triage, VEX statements, risk acceptance and rebuild cadence
14. Build secrets: BuildKit secret mounts and keeping secrets out of layers
15. Image signing: Sigstore cosign and keyless signing
16. CI scanning: failing builds on severity thresholds and linting Dockerfiles with hadolint
17. Runtime flags: read-only root filesystem, dropped capabilities, no-new-privileges and resource limits
18. Kubernetes basics: securityContext and Pod Security Standards (restricted profile)
19. Network segmentation: Kubernetes NetworkPolicies with default deny
20. Registry gates: allowing only scanned images into protected registries

## DAY 3 — Intermediate: Admission policy, runtime detection and RBAC

Included from Intermediate

21. Admission control: Kyverno and OPA Gatekeeper policies
22. Runtime detection: Falco rules, alerts and response actions
23. Kubernetes RBAC: least-privilege service accounts and permission audits
24. Secrets management: encryption at rest, External Secrets Operator and HashiCorp Vault
25. Cluster benchmarks: kube-bench and cluster scanning with Trivy or Kubescape
26. Kernel hardening: user namespaces, rootless containers, seccomp RuntimeDefault and AppArmor profiles
27. Supply chain frameworks: SLSA levels, provenance attestations and in-toto
28. Signature enforcement: Kyverno verifyImages and Sigstore policy-controller
29. Audit and logging: Kubernetes audit logs and shipping container logs to a SIEM
30. Incident investigation: analysing a compromised container and capturing forensic data

DAYS 4-5 **Advanced: Sandboxing, zero trust, compliance and scale** — New at this level

31. Sandboxed runtimes: gVisor, Kata Containers and RuntimeClass
32. eBPF security: Cilium network policies and Tetragon runtime enforcement
33. Workload identity and mTLS: SPIFFE and SPIRE with service mesh zero trust
34. Multi-tenant isolation: namespaces, quotas, dedicated node pools and virtual clusters
35. Compliance mapping: NIST SP 800-190, PCI DSS and SOC 2 evidence for containers
36. Security at scale: central policy management, exception workflow and metrics
37. CNAPP overview: unifying posture, workload and pipeline security
38. Managed Kubernetes hardening: EKS, AKS and GKE security features
39. Adversary emulation: container escape scenarios and detection validation
40. Capstone: hardened multi-tenant container platform

PRACTICE

## Hands-on labs

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

FOUNDATION

**Harden and scan a first image**

Scan an application image with Trivy, rewrite its Dockerfile to run as non-root on a smaller base and show the drop in vulnerabilities.

ESSENTIAL

**Secure an image pipeline**

Build a CI pipeline that produces a distroless image with an SBOM, scans and signs it, and deploys it with a restricted pod profile.

INTERMEDIATE

**Enforce and detect in a cluster**

Apply Kyverno policies that require signed, non-root images, deploy Falco and investigate a simulated container compromise.

ADVANCED

**Hardened platform capstone**

Design a multi-tenant cluster with sandboxed runtimes, signed-image enforcement, workload identity and a compliance evidence pack.

HOW YOU CAN LEARN

## Formats and fees

The same agenda in four 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** |
| **1:1 live training (online)** | Max 8-10 hours, one-to-one | The same agenda, taught one-to-one by the trainer. Starts immediately, without waiting for the next batch; sessions planned around your working hours, at your pace. | **INR 99,999** |
| **Self-paced video** | 1-year LMS access | All four Container Security 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). | **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 CONTAINER SECURITY 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. 1:1 training can start immediately; corporate 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/container/

ENROL OR RESERVE A SEAT
**Container Security Advanced Training**

WHATSAPP · INDIA
**+91 99057 40781**

WHATSAPP · USA
**+1 (469) 756-6329**

EMAIL
**contact@DevOpsSchool.com**