DevOpsSchool

Course curriculum · November 2026

LEVEL 03 OF 04 · INTERMEDIATE

Neuvector Intermediate Training

Enforce runtime protection and admission control, detect and respond to threats in real time and integrate NeuVector with CI and SIEM.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **3 days · Days 1-3**	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 · This curriculum	5 days · Next step

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	31 topics · Foundation to Intermediate
Hands-on labs	3 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/neuvector/neuvector-intermediate-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 Neuvector course path, you will be able to:

1

Secure the container lifecycle

Scan images, registries and running workloads and act on vulnerabilities before and after deployment.

2

Enforce runtime protection

Apply segmentation, process and file controls and admission rules that stop real attacks.

3

Operate container security at scale

Run NeuVector across clusters with policy as code, integrations and audit-ready reporting.

WHAT THE INTERMEDIATE LEVEL ADDS

Runtime protection, admission control and integrations

Hands-on: Detect, block and respond. Simulate a container compromise, detect it in real time, quarantine the pod and block vulnerable images through admission control.

WHO SHOULD ATTEND

- Regular Neuvector users who want to automate, integrate and manage it at a deeper level.
- Specialists who support Neuvector for colleagues or customers.
- Leads preparing Neuvector for wider use across projects.

BEFORE YOU START

- The Essential level, or equivalent hands-on experience.
- You can already: Scan images and running workloads for vulnerabilities and use NeuVector's firewall to segment application traffic safely.
- 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 INTERMEDIATE

Neuvector Intermediate Training agenda

31 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 security basics, architecture and installation

Included from Foundation

1. Introduction to NeuVector: open-source full lifecycle container security platform and its key features
2. Container security basics: image, registry, orchestrator, host and runtime risks in container deployments
3. How NeuVector addresses these risks: discovery, vulnerability management, network and runtime protection
4. Architecture: controller, enforcer, manager, scanner and updater components
5. Deployment options: Kubernetes, Rancher, OpenShift and supported container runtimes
6. Installation and configuration: deploying NeuVector with the Helm chart and checking pods
7. Accessing the manager console: first login, admin password change and licence-free open-source use
8. Discovery mode: how NeuVector learns applications, connections and processes automatically
9. Network activity view: visualising pods, services and connections
10. First policy look: learned groups and rules for a demo application

DAY 2 — Essential: Vulnerability scanning, segmentation and policy modes

Included from Essential

11. Vulnerability scanning: scanning running containers, nodes and the platform for CVEs
12. Registry scanning: connecting Docker Hub, Harbor, ECR, ACR or GCR registries and scheduling scans
13. Reading scan results: severity, fix availability, layers and vulnerability profiles for accepted risks
14. Network segmentation and firewall: Layer 7 network rules between groups and services
15. Policy modes: discover, monitor and protect and moving applications through them safely
16. Groups: learned groups, custom groups by labels or namespaces and group-based rules
17. Process and file access profiles: learned process baselines and file monitoring rules
18. Compliance checks: CIS benchmarks for Docker, Kubernetes and hosts
19. Notifications: events, incidents and violations views in the console
20. Users and roles: built-in roles, namespace-scoped users and LDAP or SAML login

DAY 3 — Intermediate: Runtime protection, admission control and integrations

New at this level

21. Runtime protection: configuring runtime protection policies for processes, files and network
22. Real-time threat detection: detecting exploits, reverse shells, tunnelling and suspicious processes
23. Threat response: response rules, quarantine of containers and webhook actions
24. Admission control: rules that block images with critical CVEs, root users or unapproved registries
25. Shift-left scanning: NeuVector scanner in CI with Jenkins, GitHub Actions or GitLab CI
26. DLP and WAF sensors: detecting sensitive data and attack patterns in application traffic
27. Integration with other security tools: syslog to SIEM systems, firewalls and intrusion detection
28. REST API and CLI: automating queries, exports and configuration
29. Security policy as code: exporting rules as NvSecurityRule CRDs and applying them with kubectl
30. Upgrades and backups: Helm upgrades and backing up controller configuration

31. Troubleshooting: enforcer status, missing connections, false positives and log collection

PRACTICE

Hands-on labs

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

FOUNDATION

Install NeuVector and discover workloads

Install NeuVector with Helm, deploy a multi-tier demo app and review the learned groups, connections and processes.

ESSENTIAL

Scan and segment an application

Scan a registry and the running app, then move the app from discover to protect mode with tuned network and process rules.

INTERMEDIATE

Detect, block and respond

Simulate a container compromise, detect it in real time, quarantine the pod and block vulnerable images through admission control.

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 Neuvector levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	3 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 NEUVECTOR 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/neuvector/

ENROL OR RESERVE A SEAT
Neuvector Intermediate Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com

Next step after this level: Neuvector Advanced Training - Operate NeuVector across many clusters with federation, GitOps policy, zero trust segmentation and audit-ready compliance reporting.