DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

Twistlock Advanced Training

Run Twistlock or Prisma Cloud Compute across many clusters and clouds with strong governance, automation and audit-ready reporting.

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	47 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/twistlock/twistlock-and-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 Twistlock course path, you will be able to:

1

Secure the container lifecycle

Scan images, registries and hosts and enforce vulnerability and compliance rules from build to deploy.

2

Protect running workloads

Use runtime defense, firewalls, WAAS and admission control to stop attacks on containers and hosts.

3

Govern at enterprise scale

Operate Console and Defenders across clusters with policy as code, reporting and SIEM integration.

WHAT THE ADVANCED LEVEL ADDS

Scale, multi-cluster governance and operational excellence

Hands-on: Capstone: container security programme rollout. Design a multi-cluster deployment with collections per team, policy as code, CI gates, runtime rules and a compliance report for audit.

WHO SHOULD ATTEND

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

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Protect running workloads with runtime models, firewalls and admission control, and investigate incidents in the Console.
- 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

Twistlock Advanced Training agenda

47 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 concepts, Console and Defenders

Included from Foundation

1. Container security risks: vulnerable images, misconfiguration, exposed secrets and runtime attacks
2. Twistlock history: acquisition by Palo Alto Networks and today's Prisma Cloud Compute capabilities
3. Architecture: Console, Defenders, Intelligence Stream and how data flows between them
4. Defender types: container, host, serverless and app-embedded Defenders and where each fits
5. Editions: self-hosted Compute Edition versus the SaaS Compute module
6. Installing the Console: Linux host or Kubernetes deployment, licensing and first login
7. Deploying Defenders: twistcli generated manifests, DaemonSets and single-host install scripts
8. Console tour: Monitor, Defend and Manage sections, radar view and dashboards
9. First vulnerability scan: scanning deployed images and reading CVE, severity and fix status
10. First compliance check: CIS Docker benchmark results for a host and its containers
11. Users and roles: local users, built-in roles and access to the Console

DAY 2 — Essential: Vulnerability, compliance and registry scanning

Included from Essential

12. Vulnerability rules: severity thresholds, grace periods, alert versus block actions and scopes with collections
13. Registry scanning: Docker Hub, Amazon ECR, Azure Container Registry, Google Artifact Registry and Harbor
14. Host scanning: package vulnerabilities, installed applications and host compliance
15. Compliance policies: CIS Docker and Kubernetes benchmarks, custom checks and trusted images
16. Secrets and malware: detecting embedded secrets and malware in images
17. CI scanning with twistcli: twistcli images scan, pass and fail thresholds and output formats
18. Jenkins and pipeline plugins: integrating scans into Jenkins, GitHub Actions and GitLab CI
19. Risk prioritisation: risk factors such as exploit available, internet exposure and package in use
20. Vulnerability explorer: tracking top CVEs across images, hosts and functions
21. Remediation workflow: base image updates, package fixes and rescans
22. Alerts: email, Slack, Jira, webhook and SIEM integrations for findings
23. Collections: grouping resources by team, namespace or cluster for scoped rules and views

DAY 3 — Intermediate: Runtime defense, firewalls and access control

Included from Intermediate

24. Runtime defense: learning mode, automatic models and process, network and file system rules
25. Custom runtime rules: allow and deny lists, prevent versus alert and custom rule language
26. Incident Explorer: incident types, audits and investigating suspicious behaviour
27. Forensics: container and host forensic data and preserving evidence
28. Cloud Native Network Firewall: microsegmentation between containers, apps and hosts
29. WAAS: web application and API security rules, OWASP Top 10 protections and API discovery
30. Admission control: Open Policy Agent rules to block risky Kubernetes deployments

31. Trusted images: allowing only images from approved registries and base layers
32. Serverless protection: function scanning and runtime protection for AWS Lambda
33. Authentication: LDAP, SAML and OIDC single sign-on and custom roles
34. API automation: Compute API for scans, reports and policy changes
35. Troubleshooting: Defender connectivity, upgrade order and log collection

DAYS 4-5 **Advanced: Scale, multi-cluster governance and operational excellence** **New at this level**

36. Scale architecture: Console sizing, Defender fleets across many clusters and network requirements
37. Projects and tenants: multi-Console projects for business units and isolated teams
38. High availability and backup: Console backups, restore and disaster recovery planning
39. Upgrades: Console and Defender upgrade sequencing and version compatibility
40. Policy as code: managing rules through the API, version control and automated promotion
41. Compliance reporting: PCI DSS, HIPAA, NIST and CIS mapped reports and audit evidence
42. SIEM and SOAR: Splunk, Cortex XSOAR and syslog pipelines with alert tuning
43. Hardening the platform: certificate management, least-privilege roles and Console access controls
44. Noise reduction: tuning vulnerability exceptions, runtime false positives and alert routing
45. Migration: moving from the self-hosted Console to the SaaS module or between clusters
46. Metrics and governance: vulnerability SLAs, exception reviews and security KPIs for leadership
47. Capstone: an end-to-end container security programme from pipeline scan to runtime response

PRACTICE

Hands-on labs

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

FOUNDATION **Install Console and scan workloads**
Install the Console on a Kubernetes cluster, deploy Defenders as a DaemonSet and review the first vulnerability and compliance findings.

ESSENTIAL **Block vulnerable images in CI**
Add a twistcli scan to a pipeline with a high-severity threshold, connect a container registry for scanning and send findings to Slack.

INTERMEDIATE **Detect and block a runtime attack**
Let a runtime model learn a demo web application, simulate a cryptominer and reverse shell, block them with runtime rules and investigate the incident.

ADVANCED **Capstone: container security programme rollout**
Design a multi-cluster deployment with collections per team, policy as code, CI gates, runtime rules and a compliance report for audit.

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 Twistlock 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 TWISTLOCK 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/twistlock/

ENROL OR RESERVE A SEAT
Twistlock Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com