DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

Falco Advanced Training

Operate Falco at enterprise scale with a detection engineering lifecycle, automated response and compliance-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	48 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/falco/falco-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 Falco course path, you will be able to:

1

Detect runtime threats

Detect suspicious behaviour in hosts, containers and Kubernetes in real time with Falco.

2

Engineer reliable detections

Write, test and tune Falco rules with low false positives and clear ownership.

3

Respond and scale securely

Route, automate and govern Falco alerts across multiple clusters and security tools.

WHAT THE ADVANCED LEVEL ADDS

Detection engineering, scale, governance and incident response

Hands-on: Build a detection-as-code pipeline. Create a Git repository of custom rules tested in CI with event-generator, publish them as an OCI artifact and roll them out to two clusters.

WHO SHOULD ATTEND

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

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Run Falco across Kubernetes clusters with Helm, enrich alerts with metadata, add cloud plugins and troubleshoot detection gaps.
- 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

Falco Advanced Training agenda

48 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: Runtime security concepts, drivers and installation

Included from Foundation

1. Runtime security basics: why scanning is not enough, detecting threats while containers and hosts are running
2. What Falco is: CNCF graduated runtime security project, system call monitoring and rule-based detection
3. Falco architecture: kernel event collection, libscap and libsinsp, rules engine and output channels
4. Event sources: system calls, plus plugins for Kubernetes audit logs, AWS CloudTrail and other sources
5. Drivers: modern eBPF probe, legacy eBPF probe and kernel module, and how to choose for your kernel
6. Installation on Linux: packages (deb, rpm), systemd services per driver and falcoctl driver setup
7. Running in a container: the falcosecurity/falco image, privileges and host mounts
8. Configuration file: falco.yaml, rules_files, outputs, priority threshold and json_output
9. Default rules: falco_rules.yaml, rule maturity levels and what ships enabled
10. Reading alerts: priority, rule name, output fields such as proc.name, user.name and container.id
11. Common detections: shell in a container, sensitive file read (/etc/shadow), unexpected outbound connection
12. First example: trigger a terminal shell in a container and capture the alert

DAY 2 — Essential: Writing rules, macros, lists and alert outputs

Included from Essential

13. Rule syntax: rule, desc, condition, output, priority, tags and enabled fields
14. Conditions and fields: evt.type, proc.cmdline, fd.name, container.image.repository and operators
15. Macros and lists: reusing conditions, overriding default macros and maintaining lists
16. Exceptions: structured exceptions with fields and values to reduce false positives
17. Rule overrides: append and replace with override, custom rules files and load order
18. Rule testing: the event-generator tool, dry runs and validating rules files with falco -V
19. Output channels: stdout, file, syslog, program and http outputs, and json formatting
20. Falcosidekick: forwarding alerts to Slack, Teams, Elasticsearch, Loki, webhooks and more
21. Falcosidekick UI: browsing, filtering and counting events
22. falcoctl: installing and updating rules and plugins as OCI artifacts, artifact follow
23. MITRE ATT&CK tags: mapping rules to tactics and techniques for triage
24. Team workflow: storing custom rules in Git, peer review and promoting rules between environments

DAY 3 — Intermediate: Kubernetes deployment, plugins, metadata and troubleshooting

Included from Intermediate

25. Kubernetes deployment: falcosecurity Helm chart, DaemonSet, driver selection and values.yaml settings
26. Kubernetes metadata: container runtime integration, pod, namespace and label fields in alerts
27. Kubernetes audit logs: k8saudit plugin, webhook backend and detecting risky API activity
28. Cloud plugins: CloudTrail plugin for AWS activity, plus Okta and GitHub plugins overview
29. Falco Talon: automated response actions such as labelling, terminating or isolating pods
30. Metrics: Falco metrics, Prometheus endpoint and dashboards for event drops and rule hits

31. Performance basics: syscall selection, base_syscalls, buffer sizes and dropped event alerts
32. Kubernetes-specific detections: privileged pods, hostPath mounts, service account token access, kubectl exec
33. Integrations with SIEM: shipping alerts to Elasticsearch, Splunk or Microsoft Sentinel
34. Troubleshooting: driver load failures, unsupported kernels, missing fields and no-alert situations
35. Upgrading Falco: version compatibility of rules, plugins and drivers
36. Security of Falco itself: least privilege, protecting configuration and alert channel integrity

DAYS 4-5 **Advanced: Detection engineering, scale, governance and incident response** **New at this level**

37. Detection engineering lifecycle: threat modelling, rule design, testing, deployment and retirement
38. Detection as code: CI pipelines that lint, test and package rules as OCI artifacts with falcoctl
39. Multi-cluster operations: central alert aggregation, fleet configuration and consistent rule versions
40. Scale and performance: high-throughput nodes, adaptive syscalls, CPU overhead measurement and drop analysis
41. Writing plugins: plugin SDK concepts for new event sources and field extraction
42. Incident response with Falco: alert triage, forensic context, capture files and response playbooks
43. Advanced response automation: Falco Talon rules, Argo Workflows or serverless functions for remediation
44. Compliance mapping: Falco rules for PCI DSS, NIST 800-53 and CIS controls evidence
45. Defence in depth: Falco with admission control (Kyverno or Gatekeeper), image scanning and network policy
46. Runtime threats in the cloud native stack: container escapes, cryptomining, reverse shells and lateral movement
47. Governance: rule ownership, alert SLAs, false positive budgets and periodic rule reviews
48. Capstone: design and run a multi-cluster Falco programme with CI-tested rules, SIEM integration and auto response

PRACTICE

Hands-on labs

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

FOUNDATION **Catch your first runtime threat**

Install Falco with the modern eBPF driver, run suspicious commands inside a container and trace each resulting alert back to its rule.

ESSENTIAL **Write and tune a custom rule**

Write a rule that detects a crypto-miner style process, add a macro and exception for a known tool, and send alerts to Slack through Falcosidekick.

INTERMEDIATE **Protect a Kubernetes cluster with Falco**

Deploy Falco with Helm and the k8saudit plugin, detect a kubectl exec and a privileged pod, and trigger an automated Falco Talon response.

ADVANCED **Build a detection-as-code pipeline**

Create a Git repository of custom rules tested in CI with event-generator, publish them as an OCI artifact and roll them out to two clusters.

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 Falco 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 FALCO 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/falco/

ENROL OR RESERVE A SEAT
Falco Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com