DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

Deepwatch Advanced Training

Run an MDR programme at enterprise scale with governance, incident readiness, metrics and continuous improvement.

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/deepwatch/deepwatch-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 Deepwatch course path, you will be able to:

1

Operate MDR day to day

Review investigations, approve response actions and tune detections with your MDR provider.

2

Improve detection coverage

Measure telemetry and ATT&CK coverage and close the gaps that matter most.

3

Govern the MDR programme

Run governance, metrics and incident readiness for a co-managed security operation.

WHAT THE ADVANCED LEVEL ADDS

Programme governance, incident readiness and provider management

Hands-on: Run a ransomware tabletop with MDR. Facilitate a ransomware tabletop that tests escalation, containment approvals and communication, then produce an improvement plan.

WHO SHOULD ATTEND

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

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Measure and improve detection coverage, integrate MDR with your tooling and troubleshoot gaps in telemetry and response.
- 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

Deepwatch 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: MDR concepts, SOC models and onboarding

Included from Foundation

1. Managed security fundamentals: MSSP versus MDR versus in-house SOC, and where Deepwatch fits
2. MDR service model: 24x7 monitoring, detection, investigation, response actions and customer responsibilities
3. SOC fundamentals: tiers, alert lifecycle, triage, escalation paths and service level agreements
4. Security telemetry: endpoint, network, identity, cloud and application log sources and why coverage matters
5. SIEM and EDR basics: how SIEM correlation and endpoint detection and response work together in MDR
6. Onboarding planning: asset inventory, critical systems, contacts, escalation matrix and maintenance windows
7. Log source onboarding: syslog, forwarders, cloud API connectors and verifying data arrives correctly
8. Customer portal basics: viewing investigations, tickets, reports and service health in the Deepwatch platform
9. Alert and investigation basics: severity, true and false positives, evidence and recommended actions
10. Shared responsibility: what the provider handles, what your team must approve and act on
11. Key metrics: mean time to detect, mean time to respond and log source coverage
12. First walkthrough: follow a realistic alert from detection to customer notification and closure

DAY 2 — Essential: Daily operations, investigations and collaboration

Included from Essential

13. Daily workflow: reviewing open investigations, tickets and escalations in the platform portal
14. Investigation review: reading timelines, affected hosts and users, indicators and analyst notes
15. Escalation handling: acknowledging, approving response actions and documenting customer decisions
16. Response actions: host isolation, account disablement, blocking indicators and approval workflows
17. Tuning and suppression: whitelisting known-good activity, maintenance windows and reducing noise
18. Risk-based alerting: how risk scores aggregate related signals by user and asset
19. MITRE ATT&CK in MDR: reading technique mappings and understanding detection coverage
20. Endpoint integration: working with EDR platforms such as CrowdStrike Falcon or Microsoft Defender for Endpoint
21. Identity and cloud signals: Microsoft Entra ID, Okta, AWS CloudTrail and Microsoft 365 audit logs
22. Reports and reviews: weekly and monthly service reports, trend analysis and service review meetings
23. Communication: ticket etiquette, contact roles, after-hours escalation and status updates
24. Team workflow: integrating MDR tickets with ServiceNow or Jira and internal change processes

DAY 3 — Intermediate: Detection coverage, integrations, automation and troubleshooting

Included from Intermediate

25. Coverage assessment: mapping log sources and detections to ATT&CK, finding blind spots and prioritising fixes
26. Security maturity scoring: measuring and improving your security posture with the provider
27. SIEM integration: Splunk Enterprise Security and other SIEM data models, indexes and field normalisation
28. Cloud workload monitoring: AWS, Azure and Google Cloud security services feeding the MDR pipeline
29. Vulnerability management integration: correlating scanner findings with active threats
30. Automation and SOAR: automated enrichment, playbooks and closed-loop response with approval gates

31. Threat intelligence: indicators, adversary context and how intelligence feeds detection
32. Threat hunting: hypothesis-driven hunts, working with the provider on targeted hunts
33. Telemetry troubleshooting: missing logs, parsing errors, timestamp issues and forwarder health
34. Response troubleshooting: failed isolation, stale EDR agents and permission problems
35. Identity threat detection: impossible travel, MFA fatigue, token theft and privilege escalation patterns
36. Security basics for the customer side: least privilege for portal users, MFA and audit of approvals

DAYS 4-5 **Advanced: Programme governance, incident readiness and provider management** — New at this level

37. MDR programme governance: RACI, service levels, contract scope and quarterly business reviews
38. Major incident response: ransomware and business email compromise playbooks, war rooms and handoffs to IR retainers
39. Tabletop exercises: scenario design, decision points and measuring readiness with the MDR team
40. Purple teaming: Atomic Red Team and adversary emulation to validate detections and response
41. Metrics that matter: MTTD, MTTR, escalation accuracy, coverage percentage and executive reporting
42. Compliance support: using MDR evidence for ISO 27001, SOC 2, PCI DSS and India CERT-In reporting duties
43. Multi-entity and global coverage: subsidiaries, regions, data residency and follow-the-sun escalation
44. Integrating MDR with internal SOC: co-managed models, shared tooling and clear ownership
45. Detection engineering partnership: requesting custom detections and testing them safely
46. Provider evaluation and migration: transition planning, data retention and parallel running
47. Continuous improvement: lessons learned, posture roadmap and budget planning
48. Capstone: design a co-managed MDR operating model with metrics, playbooks and a 12-month roadmap

PRACTICE

Hands-on labs

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

FOUNDATION **Prepare an MDR onboarding package**
Build an asset inventory, log source plan and escalation matrix for a fictional company ready for MDR onboarding.

ESSENTIAL **Work a phishing escalation end to end**
Review an escalated phishing investigation, approve the right containment actions and record the decision and follow-up tasks.

INTERMEDIATE **Close a detection coverage gap**
Map current log sources to ATT&CK, identify a missing technique, onboard the needed telemetry and validate the new detection with a safe simulation.

ADVANCED **Run a ransomware tabletop with MDR**
Facilitate a ransomware tabletop that tests escalation, containment approvals and communication, then produce an improvement plan.

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 Deepwatch 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 DEEPWATCH 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/deepwatch/

ENROL OR RESERVE A SEAT
Deepwatch Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com