DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

Secops Advanced Training

Lead and mature a SOC with metrics, purple teaming, crisis management, compliance and AI-assisted operations at enterprise scale.

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	45 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/secops/secops-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 Secops course path, you will be able to:

1

Detect and triage threats

Use SIEM, EDR and network telemetry to detect, triage and escalate security alerts.

2

Respond to incidents effectively

Run the incident response lifecycle with playbooks, forensics basics and SOAR automation.

3

Mature security operations

Improve SOC coverage with detection engineering, threat hunting, purple teaming and metrics.

WHAT THE ADVANCED LEVEL ADDS

SOC maturity, metrics, purple teaming and governance

Hands-on: Run a ransomware crisis simulation. Lead a simulated ransomware incident across detection, containment, recovery and executive communication, then present SOC metrics and improvements.

WHO SHOULD ATTEND

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

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Engineer and test detections, hunt for hidden threats, automate response with SOAR and extend security operations into cloud and DevOps.
- 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

Secops Advanced Training agenda

45 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: SOC concepts, threats, telemetry and frameworks

Included from Foundation

1. Security operations overview: SOC mission, tiers, roles and shift models, in-house vs MSSP and MDR
2. Security fundamentals: CIA triad, defence in depth, least privilege and zero trust principles
3. Threat landscape: ransomware, phishing, credential theft, insider threats and supply-chain attacks
4. Attack frameworks: Lockheed Martin Cyber Kill Chain and MITRE ATT&CK tactics and techniques
5. Telemetry sources: Windows event logs, Sysmon, Linux auditd and syslog, firewall, proxy, DNS and cloud logs
6. Key Windows events: logons, process creation, service installs and account changes
7. Network basics for analysts: TCP/IP, common ports and protocols, packet capture with Wireshark
8. Security tooling map: SIEM, EDR, NDR, IDS/IPS, vulnerability scanners and SOAR
9. SIEM basics: log collection, parsing, correlation rules and alert triage
10. Alert triage: true and false positives, severity, context gathering and escalation
11. Documentation: tickets, case notes and evidence handling for investigations

DAY 2 — Essential: Monitoring, detection, vulnerability and incident handling

Included from Essential

12. Incident response lifecycle: preparation, detection, containment, eradication, recovery and lessons learned; NIST SP 800-61r3 and CSF 2.0
13. Incident handling playbooks: phishing, malware, brute force and account compromise
14. Endpoint detection and response: process trees, isolation, quarantine and live response
15. Network security monitoring: IDS with Suricata or Snort, Zeek logs and NetFlow analysis
16. Phishing analysis: email headers, URLs and attachments, sandbox detonation and user reporting
17. Malware triage basics: hashes, strings, static indicators and VirusTotal-style reputation checks
18. Vulnerability management: scanning, CVSS and EPSS prioritisation, patch coordination and verification
19. Threat intelligence: IOCs, TTPs, STIX and TAXII feeds and enrichment
20. Identity security monitoring: Active Directory and Entra ID sign-in logs, MFA fatigue and impossible travel
21. Correlation rules: writing and tuning SIEM rules to reduce false positives
22. Communication: escalation paths, stakeholder updates and shift handovers

DAY 3 — Intermediate: Detection engineering, threat hunting, SOAR and cloud

Included from Intermediate

23. Detection engineering: detection-as-code, Sigma rules, testing and version control for detections
24. ATT&CK coverage: mapping detections to techniques and finding coverage gaps
25. Adversary emulation: Atomic Red Team tests to validate detections
26. Threat hunting: hypothesis-driven hunts, baselining and hunting with SIEM queries
27. SOAR: playbook design, enrichment, automated containment and case management
28. Digital forensics basics: memory and disk acquisition, timelines and chain of custody
29. Cloud security operations: AWS CloudTrail and GuardDuty, Azure activity logs and Defender, GCP audit logs
30. Container and Kubernetes monitoring: audit logs, runtime detection with Falco

31. DevSecOps integration: feeding pipeline, code and image scan findings into security operations
32. Email and web defences: secure email gateway tuning, DMARC, DKIM and SPF, web proxy controls
33. Troubleshooting telemetry: missing logs, parsing failures, time synchronisation and noisy sources

DAYS 4-5 **Advanced: SOC maturity, metrics, purple teaming and governance** — New at this level

34. SOC design: operating models, staffing, tiering, follow-the-sun coverage and tooling architecture
35. SOC maturity: SOC-CMM assessment and improvement roadmaps
36. Metrics: MTTD, MTTR, alert volume, false positive rate and analyst workload
37. Purple teaming: joint red and blue exercises, findings tracking and detection improvement
38. Major incident and crisis management: ransomware response, legal, PR and executive communication
39. Tabletop exercises: designing and running scenarios for technical teams and executives
40. Compliance and reporting: ISO 27001, SOC 2, PCI DSS, GDPR breach notification and evidence
41. Data strategy: log retention, data lakes, cost control and SIEM migration
42. AI in security operations: AI-assisted triage and investigation, benefits, limits and verification
43. Insider threat and UEBA: behaviour baselines, risk scoring and privacy considerations
44. Third-party and supply-chain incidents: vendor breach handling and coordinated disclosure
45. Capstone: design a SOC improvement plan and run a full incident simulation from detection to lessons learned

PRACTICE

Hands-on labs

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

FOUNDATION

Triage your first SOC alerts

Collect Windows and Linux logs into a SIEM in a lab, generate suspicious activity, then triage the resulting alerts and document each case.

ESSENTIAL

Handle a phishing incident end to end

Investigate a reported phishing email, find affected users in SIEM and EDR, contain the compromise, block indicators and write the incident report.

INTERMEDIATE

Build and validate detections

Write Sigma detections for three ATT&CK techniques, emulate them with Atomic Red Team, tune the rules and automate the response with a SOAR playbook.

ADVANCED

Run a ransomware crisis simulation

Lead a simulated ransomware incident across detection, containment, recovery and executive communication, then present SOC metrics and improvements.

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 Secops 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 SECOPS 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/secops/

ENROL OR RESERVE A SEAT
Secops Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com