DevOpsSchool

Course curriculum · November 2026

LEVEL 03 OF 04 · INTERMEDIATE

# Black Duck Intermediate Training

Integrate Black Duck into CI/CD and developer tools, automate with REST APIs and administer users and access.

| | | |
|---|---|---|
| LIVE ONLINE<br>**Max 8-10 hours** | CORPORATE (DAY-WISE)<br>**3 days · Days 1-3** | SELF-PACED VIDEO<br>**1-year LMS access** |
| BATCH SIZE<br>**Max 10 learners** | NEXT BATCHES<br>**1st of every month · weekends: first Saturday** | CERTIFICATE<br>**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 | 32 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/blackduck/black-duck-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 Black Duck course path, you will be able to:

1

### Identify open source risk

Scan applications with Black Duck to find components, vulnerabilities and license obligations.

2

### Remediate and enforce policy

Triage findings, apply policies and gate CI/CD pipelines on security and license rules.

3

### Govern the software supply chain

Run Black Duck at scale and deliver SBOMs, audits and compliance reporting.

WHAT THE INTERMEDIATE LEVEL ADDS

### CI/CD integration, automation and administration

**Hands-on:** Policy gate in CI/CD. Add Black Duck Detect to a pipeline that fails on critical policy violations, sends alerts to Jira and reports via the REST API.

WHO SHOULD ATTEND

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

BEFORE YOU START

- The Essential level, or equivalent hands-on experience.
- You can already: Triage BOM components, vulnerabilities and licenses, define policies and produce SBOM and notices reports.
- 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

# Black Duck Intermediate Training agenda

32 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: Open source risk, SCA concepts and first scan

Included from Foundation

1. Open source risk: security vulnerabilities, license compliance and operational risk in dependencies
2. Software composition analysis: how SCA identifies components, versions and known vulnerabilities
3. Software bill of materials: what an SBOM is and the SPDX and CycloneDX formats
4. Black Duck SCA overview: KnowledgeBase, Black Duck Security Advisories and supported ecosystems
5. Architecture: Black Duck server, PostgreSQL database, job runners and the Detect scanning client
6. Deployment options: hosted service versus self-managed installs on Docker or Kubernetes
7. UI tour: dashboard, projects, versions, Bill of Materials and component details
8. Scan types: package manager detectors, signature scanning, binary scanning and snippet matching
9. Black Duck Detect: running the Detect script, required properties and API tokens
10. First scan: scanning a Maven or npm project and reviewing the resulting BOM

## DAY 2 — Essential: BOM review, vulnerabilities, licenses and policies

Included from Essential

11. Projects and versions: naming, phases, distribution settings and project ownership
12. BOM review: components, origins, match types and confirming or ignoring components
13. Vulnerability management: CVE versus BDSA records, CVSS scores and exploitability
14. Remediation workflow: remediation statuses, upgrade guidance and comments
15. License management: license families, license terms, obligations and conflicts
16. Policy management: policy rules for severity, license, component age and usage
17. Component adjustments: manual additions, version overrides and usage settings
18. Detect configuration: properties files, environment variables, excluded directories and detector options
19. Snippet and string search scanning: when to enable and how to review results
20. Reports: SBOM export in SPDX or CycloneDX, notices reports and vulnerability reports
21. Notifications: subscribing to project changes and new vulnerabilities

## DAY 3 — Intermediate: CI/CD integration, automation and administration

**New at this level**

22. Scanning modes: rapid scans versus full intelligent scans and when to use each
23. Jenkins integration: Detect in pipelines, credentials and failing builds on policy violations
24. GitHub Actions, GitLab CI and Azure DevOps: running Detect and publishing results
25. Container scanning: Docker image inspection and layer-aware results
26. Developer feedback: Code Sight IDE plugin for early findings
27. Black Duck Alert: routing notifications to Jira, Slack, Microsoft Teams and email
28. REST API: authentication, project and BOM endpoints and automating reports
29. User administration: users, groups, roles and project-level access
30. Authentication: SAML single sign-on and LDAP integration

31. Troubleshooting Detect: logs, diagnostic mode, detector failures and network issues
32. Scan hygiene: duplicate scans, code locations and cleaning up stale scans

PRACTICE

## Hands-on labs

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

FOUNDATION

**Scan your first project**

Generate an API token, run Black Duck Detect against an open source Java or Node.js project and review its BOM and risks.

ESSENTIAL

**Triage and report a project**

Define vulnerability and license policies, triage a scanned project's BOM, remediate key findings and export an SBOM and notices file.

INTERMEDIATE

**Policy gate in CI/CD**

Add Black Duck Detect to a pipeline that fails on critical policy violations, sends alerts to Jira and reports via the REST API.

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 Black Duck 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 BLACK DUCK 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/blackduck/

ENROL OR RESERVE A SEAT
**Black Duck Intermediate Training**

WHATSAPP · INDIA
**+91 99057 40781**

WHATSAPP · USA
**+1 (469) 756-6329**

EMAIL
**contact@DevOpsSchool.com**

**Next step after this level: Black Duck Advanced Training** - Run Black Duck at enterprise scale and build a governed open source and software supply chain program around it.