DevOpsSchool

Course curriculum · November 2026

LEVEL 03 OF 04 · INTERMEDIATE

Qualys Intermediate Training

Extend Qualys to policy compliance, web apps, cloud and containers, and automate it through the API, ITSM, SIEM and CI/CD.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **3 days · Days 1-3**	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 · This curriculum	5 days · Next step

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	35 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/qualys/qualys-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 Qualys course path, you will be able to:

1

Find and prioritise vulnerabilities

Discover assets and detect vulnerabilities with Qualys scanners and Cloud Agents, ranked by TruRisk.

2

Drive measurable remediation

Turn findings into tickets, patches, reports and dashboards that owners act on.

3

Run enterprise risk programmes

Govern, automate and report a risk-based vulnerability and compliance programme on Qualys.

WHAT THE INTERMEDIATE LEVEL ADDS

Compliance, WAS, cloud, containers, API and integrations

Hands-on: Automate scanning in a pipeline. Scan a container image and a web application from a CI pipeline, push findings to Jira or ServiceNow via the API, and evaluate a CIS policy.

WHO SHOULD ATTEND

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

BEFORE YOU START

- The Essential level, or equivalent hands-on experience.
- You can already: Run authenticated, scheduled VMDR scans, prioritise with TruRisk and threat intelligence, and drive remediation with reports and tickets.
- 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

Qualys Intermediate Training agenda

35 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: Vulnerability management basics and Qualys setup

Included from Foundation

1. Vulnerability management fundamentals: assets, vulnerabilities, CVE, CVSS, exploitability and the VM lifecycle
2. Qualys platform overview: SaaS architecture, platform regions, apps and the unified user interface
3. Data collection options: Cloud Agent, virtual, physical and cloud scanner appliances, passive sensors and connectors
4. Accounts and access: users, roles, business units, scopes and two-factor authentication
5. Asset inventory: adding IPs and domains, CyberSecurity Asset Management and Global AssetView
6. Asset tagging: static and dynamic tags, tag rules and organising assets with tags
7. Virtual scanner appliance: deploying on VMware, Hyper-V or cloud, personalisation code and network requirements
8. Cloud Agents: activation keys, installing Windows, Linux and macOS agents, configuration profiles
9. Qualys KnowledgeBase: QIDs, severity levels, CVE mapping and vendor references
10. First vulnerability scan: option profiles, launching a scan, scan status and reading results
11. Qualys Query Language basics: searching assets and vulnerabilities with QQL

DAY 2 — Essential: VMDR scanning, prioritisation, reporting and remediation

Included from Essential

12. VMDR workflow: discover, assess, prioritise and remediate in one continuous lifecycle
13. Authenticated scanning: authentication records for Windows, Unix and databases, and vault integration
14. Option profiles in depth: port scanning, vulnerability detection settings, performance and bandwidth
15. Scan scheduling: recurring scans, scan windows, blackout periods and scanner selection
16. Asset groups and networks: organising IP ranges, overlapping networks and scan targets
17. Prioritisation with TruRisk: Qualys Detection Score, Asset Criticality Score and TruRisk scores
18. Threat intelligence: real-time threat indicators, exploitability, CISA KEV and ransomware associations
19. Reporting: scan, scorecard and remediation reports, formats and scheduled distribution
20. Dashboards: unified dashboards, QQL-driven widgets and trend tracking
21. Remediation workflow: remediation policies, ticket assignment and verification rescans
22. Patch Management basics: patch detection, patch jobs and correlating patches with vulnerabilities
23. False positives and exceptions: ignoring vulnerabilities, risk acceptance and documenting decisions

DAY 3 — Intermediate: Compliance, WAS, cloud, containers, API and integrations

New at this level

24. Policy Compliance: compliance policies, CIS benchmarks, DISA STIGs and control evaluation
25. Compliance scanning and reporting: posture evaluation, exceptions and policy reports
26. Web Application Scanning: adding web apps, crawl settings, authentication and OWASP Top 10 detections
27. TotalCloud CSPM: connecting AWS, Azure and Google Cloud accounts, misconfiguration checks and remediation
28. Container Security: sensors, registry and CI image scanning and runtime visibility
29. File Integrity Monitoring: monitoring profiles, change events and compliance use cases
30. Endpoint Detection and Response: Multi-Vector EDR overview, threat hunting and response actions

31. Qualys API: authentication, VM and asset APIs, pagination, rate limits and scripting with Python
32. Integrations: ServiceNow, Jira, Splunk and Microsoft Sentinel for ticketing and SIEM workflows
33. CI/CD integration: scanning images and infrastructure code in Jenkins, GitHub Actions or Azure DevOps
34. Agent administration: configuration profiles, agent updates, performance settings and on-demand scans
35. Troubleshooting: authentication failures, scanner connectivity, agent health and missing detections

PRACTICE

Hands-on labs

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

FOUNDATION

Run your first Qualys scan

Deploy a virtual scanner and a Cloud Agent, tag a group of lab hosts, run an unauthenticated scan and review the detected QIDs.

ESSENTIAL

Build a prioritised remediation plan

Run authenticated scans on Windows and Linux hosts, rank findings by TruRisk and KEV, and produce remediation reports and tickets for owners.

INTERMEDIATE

Automate scanning in a pipeline

Scan a container image and a web application from a CI pipeline, push findings to Jira or ServiceNow via the API, and evaluate a CIS policy.

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 Qualys 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 QUALYS 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/qualys/

ENROL OR RESERVE A SEAT
Qualys Intermediate Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com

Next step after this level: Qualys Advanced Training - Run an enterprise risk-based vulnerability programme on Qualys with scaled scanning, governance, automation and executive reporting.