DevOpsSchool

Course curriculum · November 2026

LEVEL 02 OF 04 · ESSENTIAL

# Database Security Essential Training

Configure authentication, least-privilege roles, encryption and native auditing on SQL Server and MongoDB for everyday operations.

| | | |
|---|---|---|
| LIVE ONLINE<br>**Max 8-10 hours** | CORPORATE (DAY-WISE)<br>**2 days · Days 1-2** | 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 · This curriculum | 3 days · Next step | 5 days · Later |

## INSIDE THIS CURRICULUM


| | |
|---|---|
| What you will achieve | Outcomes and level focus |
| Who should attend | Audience and prerequisites |
| Agenda | 24 topics · Foundation to Essential |
| Hands-on labs | 2 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/databases/database-security-essential-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 Database Security course path, you will be able to:

1

### Harden SQL and NoSQL

Apply CIS-aligned hardening, encryption and least-privilege access to SQL Server and MongoDB.

2

### Audit every sensitive action

Configure native database auditing and stream it to a SIEM with alerts for risky activity.

3

### Prove compliance with evidence

Map database controls to GDPR, PCI DSS and DPDP requirements and produce audit-ready evidence.

WHAT THE ESSENTIAL LEVEL ADDS

### Authentication, encryption, auditing and access control

**Hands-on:** Lock down and audit both engines. Enable TLS, least-privilege roles, masking and native auditing on SQL Server and MongoDB, then prove each control by querying the audit logs.

WHO SHOULD ATTEND

- Learners who know the basics of Database Security and want to use it confidently every day.
- Professionals taking over Database Security work on a live project.
- Teams agreeing on a common way of working with Database Security.

BEFORE YOU START

- The Foundation level, or equivalent hands-on experience.
- You can already: Explain how SQL and NoSQL databases work, where they are attacked and which controls protect them in SQL Server and MongoDB.
- 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 ESSENTIAL

# Database Security Essential Training agenda

24 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: Database fundamentals, threats and engine architecture

Included from Foundation

1. Database fundamentals: data models, tables and documents, transactions, ACID and the role of databases in business systems
2. DBMS and RDBMS: schemas, primary and foreign keys, SQL, normalisation and how relational engines enforce integrity
3. NoSQL databases: document, key-value, wide-column and graph models; BASE versus ACID trade-offs
4. Common threats and challenges: SQL and NoSQL injection, excessive privileges, weak credentials, unpatched engines, exposed ports
5. Database security issues: data breaches, insider misuse, ransomware, stolen backups and misconfigured cloud databases
6. Database administrator role: security duties, separation of duties, change control and least privilege for DBAs
7. Controls and policies: preventive, detective and corrective controls; access, password, retention and backup policies
8. MS SQL Server architecture: instances, system databases, protocol layer, relational engine, storage engine and SQLOS
9. SQL Server security model: logins versus users, server and database roles, schemas, Windows and SQL authentication
10. MongoDB architecture: mongod, BSON documents and collections, replica sets, sharding with mongos and config servers
11. MongoDB security model: SCRAM authentication, role-based access control, built-in roles, bindIp and default exposure risks
12. Lab environment: SQL Server 2022 and MongoDB Community in Docker, connecting with sqlcmd, SSMS and mongosh

## DAY 2 — Essential: Authentication, encryption, auditing and access control

**New at this level**

13. Authentication hardening: password policy (CHECK_POLICY), contained users, Microsoft Entra ID logins, MongoDB SCRAM-SHA-256
14. Authorization: GRANT, DENY and REVOKE, least-privilege role design, MongoDB custom roles and privilege actions
15. Auditing in SQL database: SQL Server Audit, server and database audit specifications, targets, reading sys.fn_get_audit_file
16. Auditing in NoSQL database: MongoDB auditing in Enterprise and Atlas, audit filters, Percona Server for MongoDB audit log
17. Encryption in transit: TLS certificates for SQL Server and MongoDB, forcing encrypted connections, verifying cipher suites
18. Encryption at rest: SQL Server TDE and backup encryption, MongoDB encrypted storage engine with KMIP key management
19. Column and field protection: Always Encrypted, Dynamic Data Masking, MongoDB client-side field level and Queryable Encryption
20. Row-level security: SQL Server security predicates, MongoDB views and field restrictions for multi-tenant data

21. Secure configuration: surface area reduction, disabling xp_cmdshell and CLR, MongoDB security.authorization enabled
22. Injection defence: parameterised queries, stored procedures, ORMs, MongoDB operator injection ($where, $ne) and input validation
23. Backup security: encrypted backups, access-controlled backup storage, retention rules and regular restore tests
24. Team workflow: access requests, periodic privilege reviews, change tickets and a documented security baseline

PRACTICE

## Hands-on labs

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

FOUNDATION

**Map the attack surface of two databases**

Install SQL Server and MongoDB in containers, create logins and users, and document every open port, default account and privilege you find.

ESSENTIAL

**Lock down and audit both engines**

Enable TLS, least-privilege roles, masking and native auditing on SQL Server and MongoDB, then prove each control by querying the audit logs.

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 Database Security levels, plus 20+ more courses and 50+ tools, at your own pace. | **INR 833/month** billed yearly at INR 9,996 |
| **Corporate (day-wise)** | 2 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 DATABASE SECURITY 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/databases/

**ENROL OR RESERVE A SEAT**
**Database Security Essential Training**

**WHATSAPP · INDIA**
**+91 99057 40781**

**WHATSAPP · USA**
**+1 (469) 756-6329**

**EMAIL**
**contact@DevOpsSchool.com**

**Next step after this level: Database Security Intermediate Training** - Harden SQL Server and MongoDB against CIS Benchmarks, automate compliance scans and stream database activity into a SIEM.