CONCEPT

Database Security: Activity Monitoring, Encryption, Data Masking and Hardening

25 – 29 January 2027
London - Central London four-star



Database Security: Activity Monitoring, Encryption, Data Masking and Hardening

Ref: 901_21156 **Date:** 25 – 29 January 2027 **Location:** London - Central London four-star **Fees:** 25300 SAR

Introduction:

Production databases hold the records attackers want most, yet many estates still run with shared DBA logins, unencrypted backups, full production copies in test and audit settings nobody reviews. This Core Concept course gives DBAs, security analysts and application owners a vendor-neutral approach to database security: least-privilege roles and privileged account control, encryption and key custody, static and dynamic data masking, database activity monitoring, audit trail review, hardening against CIS Benchmarks and vulnerability assessment across on-premises and cloud engines. Participants produce a Database Security Assessment and Hardening Plan for a case database estate.

Course Objectives:

- Inventory a database estate, discover and classify sensitive columns and rate its current security posture against control objectives
- Design least-privilege roles and privileged DBA controls, including vaulted credentials, session recording and break-glass procedures
- Configure encryption at rest and in transit with a key custody and rotation scheme suited to the estate
- Select static masking, dynamic masking or tokenisation to keep production records out of test and analytics environments
- Define database activity monitoring and audit policies and review audit trails for privileged misuse and anomalous access
- Harden, patch and assess database engines against CIS Benchmarks and turn findings into a risk-ranked hardening plan

Target Audience:

- Database administration staff responsible for the configuration, patching and access of production database engines
- Information security analysts who monitor database access, investigate alerts and track remediation
- Application owners accountable for the data their systems hold and for approving access to it
- Infrastructure and cloud operations staff who run managed database services and backup platforms
- IT risk and audit staff who test database controls and assemble evidence for compliance reporting

Course Outline:

Day 1: Database Threat Landscape and Estate Security Baseline

- Database Threat Catalogue: Credential Theft, Excessive Privilege, Injection and Insider Misuse
- Database Estate Inventory: Engines, Instances, Owners and Data Flows
- Sensitive Data Discovery Scans and Classification Labels for Tables and Columns
- Attack Surface Review: Listeners, Network Ports, Linked Servers and Service Accounts
- Current-State Database Security Scorecard Against Control Objectives

Day 2: Authentication, Least-Privilege Roles and Privileged DBA Control

- Authentication Options: Native Accounts, Directory Integration and Multi-Factor Access
- Least-Privilege Role Model: Schema Owners, Application Accounts and Read-Only Analysts
- Privileged Access Vaulting, Session Recording and Break-Glass DBA Accounts
- Division of DBA, Security Administrator and Auditor Rights Inside the Database
- Application Owner Access Recertification and Orphaned Account Clean-Up

Day 3: Encryption, Key Custody and Data Masking

- Transparent Data Encryption for Data Files, Redo Logs and Tablespaces
- TLS for Client Connections and Replication Links with Certificate Validation
- Key Management Basics: Key Hierarchies, Hardware Security Modules, Rotation and Custody
- Static Data Masking for Test Copies: Substitution, Shuffling and Numeric Variance
- Dynamic Masking, Tokenisation and Format-Preserving Encryption for Sensitive Columns

Day 4: Activity Monitoring, Audit Policy, Hardening and Vulnerability Assessment

- Database Activity Monitoring Architectures: Network, Agent, Native Audit and eBPF Sensors
- Audit Policy Design: Privileged Statements, Failed Logins, Schema Changes and Sensitive Reads
- Hardening Against CIS Benchmarks and Patch Cadence for Database Engines
- Database Vulnerability Assessment Scans, SQL Injection Exposure Checks and Finding Triage
- Encrypted Backup Sets, Restore Drills and Cloud Database Shared Responsibility

Day 5: Case Estate Lab: Database Security Assessment and Hardening Plan

- Case Estate Brief: Finance, Healthcare and Retail Databases Across On-Premises and Cloud
- Lab: Audit Trail Review of Privileged Sessions and Anomalous Query Patterns
- Lab: Benchmark Scan Results and Vulnerability Findings Risk Ranking
- Control Evidence Pack for Compliance Reporting to Auditors and Data Owners
- Database Security Assessment and Hardening Plan Presentation and Peer Review

Skills You Will Gain:

- Sensitive Data Discovery
- Database Privilege Design
- Privileged Session Oversight
- Encryption Key Custody
- Test Data Masking
- Database Audit Policy Design
- Secure Configuration Benchmarking
- Database Vulnerability Triage

Why Attend This Course:

- Take back a Database Security Assessment and Hardening Plan built in labs on a multi-engine case estate
- Remove production records from test environments without breaking the applications and reports that depend on them
- Spot the DBA and service account activity that native logs miss and route it to the right reviewer
- Compare database protection practice with DBAs, analysts and application owners from finance, healthcare, retail and public services

Conclusion:

Database security depends on layered controls that are configured, monitored and evidenced, not on a single product. The week moves from the threat catalogue, estate inventory and sensitive data discovery, through authentication, least-privilege roles and privileged DBA control, to encryption, key custody and masking, then activity monitoring, audit policy, benchmark hardening, vulnerability assessment and secure backup. The final day applies these controls to a case estate in the lab and produces a Database Security Assessment and Hardening Plan for each participant.