Database Development with a Security-First Mentality

Data Grillen 2026



Late summer 2025...



Be aware of what you share

Introduction



Danny de Haan

Solutions Engineer

redgate

CIS Center for Internet Security®

thatinfradba.com | thatinfradba@pm.me | /dannydh | /ThatInfraDba



Session Objectives

- Security First Development
- Design Secure Databases
- Continuous Monitoring



The Stakes

- Data breaches are costly
- Compliance Requirements
- Security as a business enabler



Common Pitfalls

- Security as an afterthought
- Over-privileged accounts
- Weak authentication
- Lack of monitoring & auditing



Agenda

- Mindset vs. Mentality
- Principles of secure development
- Core Security Features
- Continuous Monitoring & Risk Mitigation
- Security as a lifestyle



Mindset vs Mentality



Mindset vs. Mentality in Security

- **Mindset** → “we patch because we must”
- **Mentality** → “we design securely because it’s who we are”
- Why it matters: **Security isn’t just a checklist** → it’s a discipline that must be lived, not just followed.



Principles of Secure Development



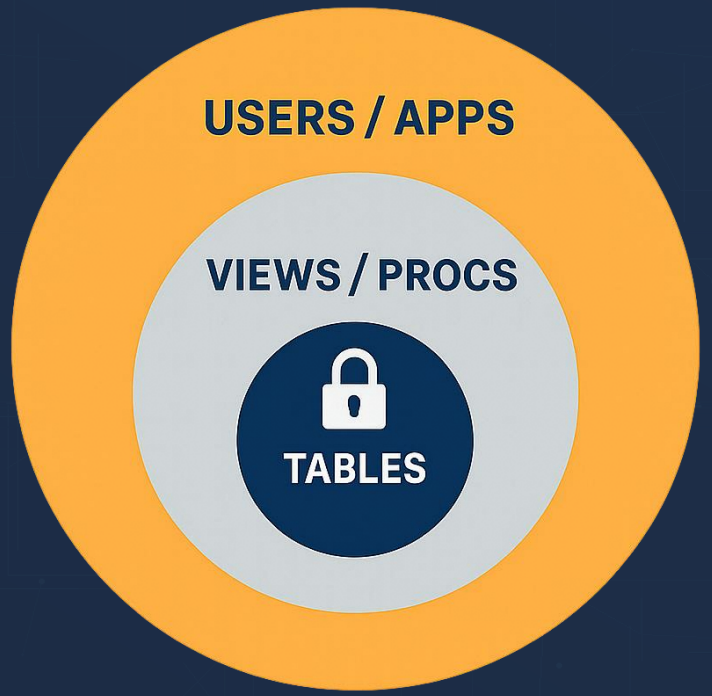
Security in the blueprint

- Would you build a house and add locks later?
- Or design it with doors, locks, and alarms from the start?
- Security must be part of the blueprint, not an afterthought.



Foundations of Secure Data Architecture

- Least privilege
- Defense in Depth
- Separation of Concerns



The Core Data Layer

- Tables hold the raw data - the “vault”
- Direct access = broad exposure risk
- Sensitive columns (e.g., passwords, PII) must be protected
- Restrict direct table access to DBAs (and trusted services) only



Controlled Windows into our Data

- Views expose only what’s needed
- Hide sensitive columns (e.g. mask SSNs, exclude password hashes)
- Apply row-level security (filter by user context)
- Simplify queries for consumers while enforcing rules



Gatekeepers of Logic

- Stored procedures encapsulate business logic
- Enforce parameterization
- Centralize validation and auditing
- Prevent ad-hoc queries by end users



Core Security Features



SQL Server Security Features

- Authentication
- Authorization
- Encryption
- Row-Level Security
- Data Masking
- Auditing



SQL Server Security Features

- Authentication
  - Windows vs SQL Logins vs Managed Indentity*
  - Multi-factor authentication*
  - Contained users

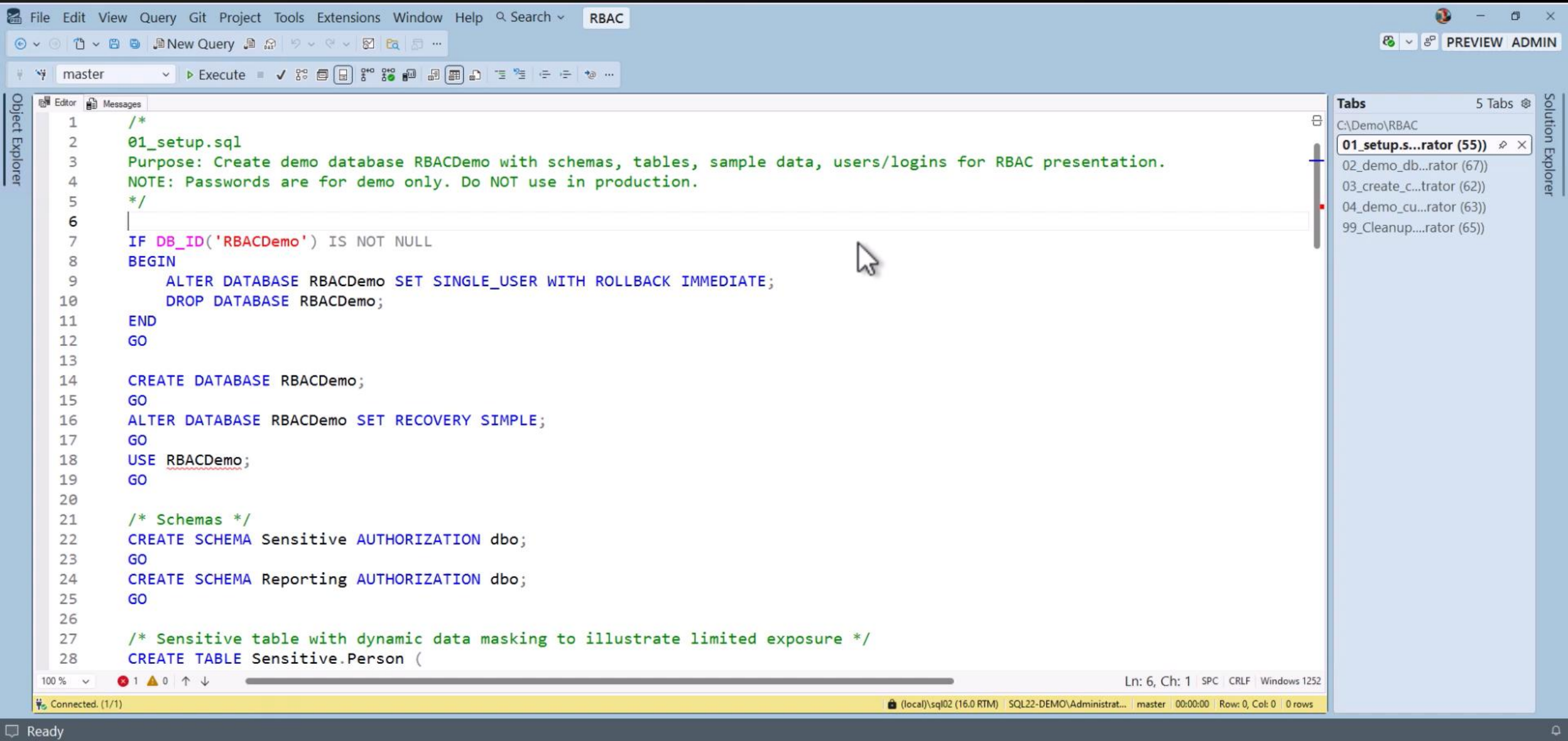
* Requires Azure Arc



SQL Server Security Features

- Authentication
- Authorization
  - Role-based access control
  - Custom roles
  - Avoid direct user permissions




File Edit View Query Git Project Tools Extensions Window Help Search RBAC
New Query
PREVIEW ADMIN
master
Execute
Editor
Messages
Object Explorer
Solution Explorer
Tabs
5 Tabs
C:\Demo\RBAC
01_setup.s...rator (55))
02_demo_db...rator (67))
03_create_c...trator (62))
04_demo_cu...rator (63))
99_Cleanup....rator (65))
/*
01_setup.sql
Purpose: Create demo database RBACDemo with schemas, tables, sample data, users/logins for RBAC presentation.
NOTE: Passwords are for demo only. Do NOT use in production.
*/
IF DB_ID('RBACDemo') IS NOT NULL
BEGIN
ALTER DATABASE RBACDemo SET SINGLE_USER WITH ROLLBACK IMMEDIATE;
DROP DATABASE RBACDemo;
END
GO
CREATE DATABASE RBACDemo;
GO
ALTER DATABASE RBACDemo SET RECOVERY SIMPLE;
GO
USE RBACDemo;
GO
/* Schemas */
CREATE SCHEMA Sensitive AUTHORIZATION dbo;
GO
CREATE SCHEMA Reporting AUTHORIZATION dbo;
GO
/* Sensitive table with dynamic data masking to illustrate limited exposure */
CREATE TABLE Sensitive.Person (
100 %
Ln: 6, Ch: 1
SPC
CRLF
Windows 1252
Connected. (1/1)
(local)\sql02 (16.0 RTM)
SQL22-DEMO\Administrat...
master
00:00:00
Row: 0, Col: 0
0 rows
Ready

SQL Server Security Features

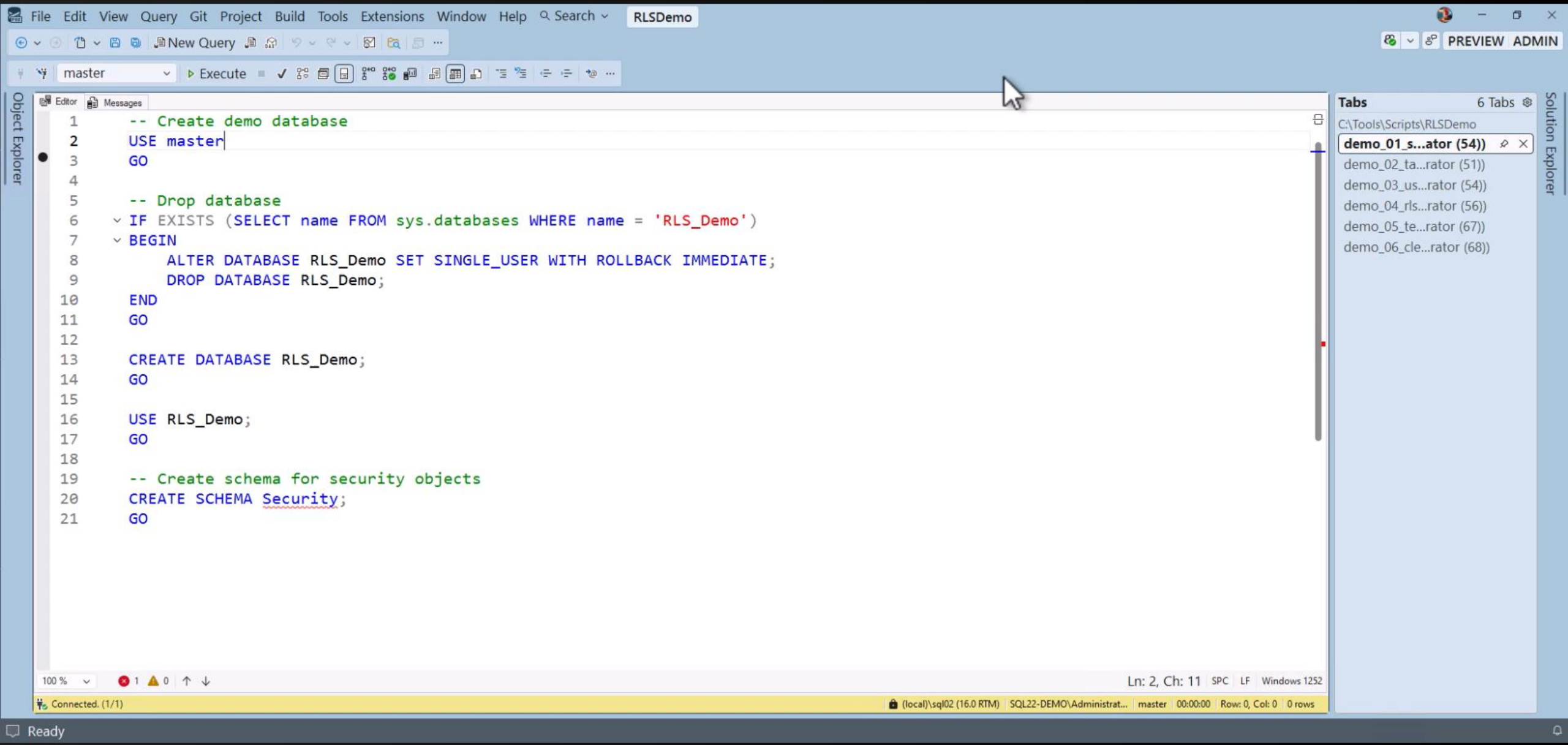
- Authentication
- Authorization
- Encryption
  - Transparent Data Encryption (TDE)
  - Always Encrypted
  - Column-level encryption



SQL Server Security Features

- Authentication
- Authorization
- Encryption
- Row-Level Security
  - Fine-grained access
  - Predicate functions




File Edit View Query Git Project Build Tools Extensions Window Help Search RLSDemo
New Query
PREVIEW ADMIN
master
Execute
Editor
Messages
1 -- Create demo database
2 USE master
3 GO
4
5 -- Drop database
6 IF EXISTS (SELECT name FROM sys.databases WHERE name = 'RLS_Demo')
7 BEGIN
8 ALTER DATABASE RLS_Demo SET SINGLE_USER WITH ROLLBACK IMMEDIATE;
9 DROP DATABASE RLS_Demo;
10 END
11 GO
12
13 CREATE DATABASE RLS_Demo;
14 GO
15
16 USE RLS_Demo;
17 GO
18
19 -- Create schema for security objects
20 CREATE SCHEMA Security;
21 GO
Tabs
6 Tabs
C:\Tools\Scripts\RLSDemo
demo_01_s...ator (54))
demo_02_ta...rator (51))
demo_03_us...rator (54))
demo_04_rls...rator (56))
demo_05_te...rator (67))
demo_06_cle...rator (68))
Object Explorer
Solution Explorer
100 %
Ln: 2, Ch: 11
SPC
LF
Windows 1252
Connected. (1/1)
(local)\sql02 (16.0 RTM)
SQL22-DEMO\Administrat...
master
00:00:00
Row: 0, Col: 0
0 rows
Ready

SQL Server Security Features

- Authentication
- Authorization
- Encryption
- Row-Level Security
- Data Masking
  - Protect sensitive fields
  - Masked vs unmasked views



SQL Server Security Features

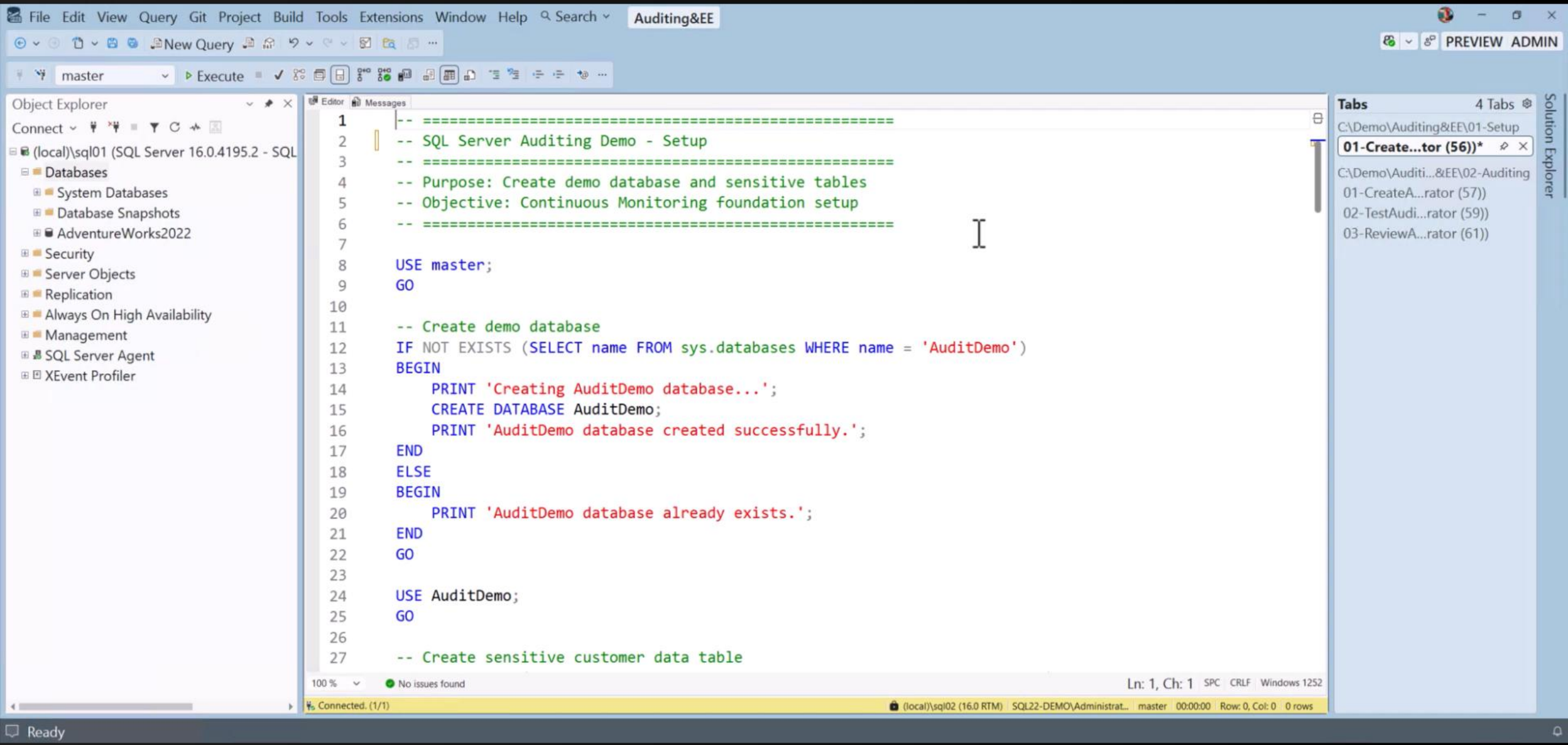
- Authentication
- Authorization
- Encryption
- Row-Level Security
- Data Masking
- Auditing



SQL Server Security Features

- Authentication
- Authorization
- Encryption
- Row-Level Security
- Data Masking
- Auditing
  - SQL Server Audit
  - Extended Events
  - Centralized log collection




File Edit View Query Git Project Build Tools Extensions Window Help Search
Auditing&EE
New Query
PREVIEW ADMIN
master
Execute
Object Explorer
Connect
(local)\sql01 (SQL Server 16.0.4195.2 - SQL
Databases
System Databases
Database Snapshots
AdventureWorks2022
Security
Server Objects
Replication
Always On High Availability
Management
SQL Server Agent
XEvent Profiler
Editor
Messages
1 -- ==========
2 -- SQL Server Auditing Demo - Setup
3 -- ==========
4 -- Purpose: Create demo database and sensitive tables
5 -- Objective: Continuous Monitoring foundation setup
6 -- ==========
7
8 USE master;
9 GO
10
11 -- Create demo database
12 IF NOT EXISTS (SELECT name FROM sys.databases WHERE name = 'AuditDemo')
13 BEGIN
14 PRINT 'Creating AuditDemo database...';
15 CREATE DATABASE AuditDemo;
16 PRINT 'AuditDemo database created successfully.';
17 END
18 ELSE
19 BEGIN
20 PRINT 'AuditDemo database already exists.';
21 END
22 GO
23
24 USE AuditDemo;
25 GO
26
27 -- Create sensitive customer data table
100 %
No issues found
Ln: 1, Ch: 1
SPC
CRLF
Windows 1252
Connected. (1/1)
(local)\sql02 (16.0 RTM)
SQL22-DEMO\Administrat...
master
00:00:00
Row: 0, Col: 0
0 rows
Tabs
4 Tabs
C:\Demo\Auditing&EE\01-Setup
01-Create...tor (56))*
C:\Demo\Auditi...&EE\02-Auditing
01-CreateA...rator (57))
02-TestAudi...rator (59))
03-ReviewA...rator (61))
Solution Explorer
Ready

Continuous Monitoring & Risk Mitigation



Continuous Monitoring & Risk Mitigation

- Alerts & Dashboards
- SIEM integration
- Incident Response



Regular Security Assessments

- SQL Vulnerability Assessment → Built-in scanner in SSMS & Azure; baseline misconfigurations
- Microsoft Defender for SQL → Threat detection, anomalous access alerts
- CIS Benchmarks → Industry baseline for SQL Server hardening
- Penetration testing → External validation, at least annually
- Permission audits → Review role membership & orphaned users quarterly



Security as Fire Prevention

- Firefighting = reacting once the blaze has started
- Prevention = sprinklers, alarms, safe wiring built in
- Security must be prevention, not just emergency response



DevSecOps

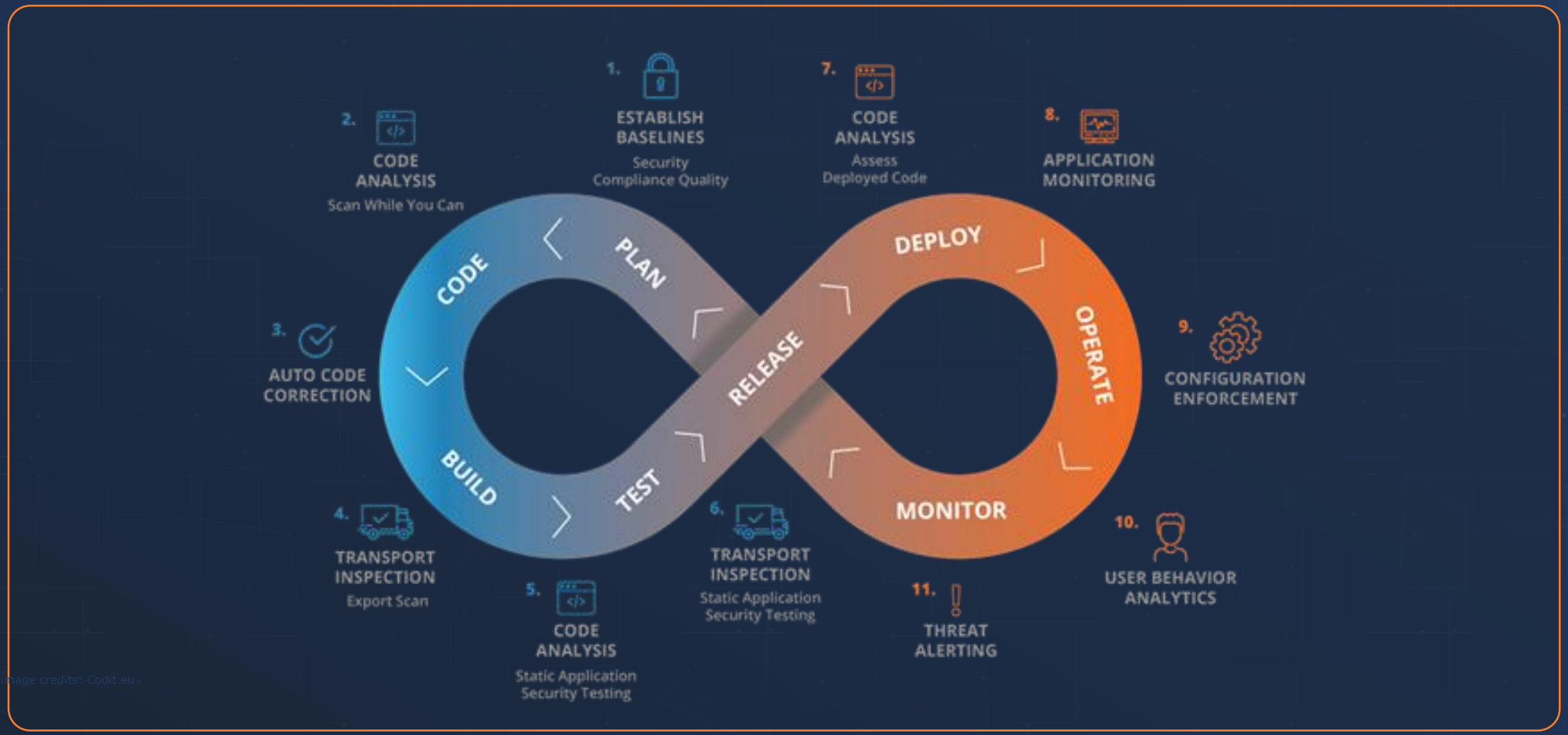


Image credits: Codit.eu

DevSecOps for Databases

- Source control everything → Schema, permissions, static data (state-based or migration-based)
- Secret scanning → Block connection strings & credentials at PR time
- Static analysis → T-SQL linting, SQL injection patterns, missing schema binding
- Deployment gates → Require review for permission changes; drift detection on prod
- Shift left → Run vulnerability assessment in CI, not after release



Key Takeaways

- Build security in from the start
- Use your DBMS’ built-in features
- Monitor Continuously
- Stay Compliant




Q&A

Thank you very much

Session



Danny de Haan

Event

thatinfradba.com | thatinfradba@pm.me | /dannydh