



Masterclass:

SQL Server Security

Duration: 5 days

Live Virtual Class

CQURE

Warsaw New York Dubai Zug

info@cquire.pl

www.cquire.pl

www.cquireacademy.com





CQURE has been providing cybersecurity services and trainings since it was set up in Warsaw in 2008. Throughout the years, our services have reached a wide range of clients around the world, which allowed us to open new offices in New York (2013), Dubai (2014), and Zug (2016).

CQURE Academy focuses on cybersecurity training program consisting of over 40 high-quality technical workshops and seminars and providing certification to specialists. Additionally, in October 2016 CQURE has successfully launched online and subscription-based training.


CQURE Experts speak at international events and engage in multiple cybersecurity projects – they bring their knowledge and experience to trainings. CQURE Academy also involves R&D – that is why CQURE Team is recognizable in the cybersecurity field.



SQL Server Security

In this workshop, you will explore, learn, and practice essential tasks to implement a highly secure SQL Server environment. We'll begin by identifying security challenges in database servers and analyzing the most common attack vectors. You'll get hands-on experience by simulating real-world threats on default SQL Server installations to better understand vulnerabilities and mitigation techniques. In short, we will break our systems to learn how to protect them effectively!

About the course

 This training is essential for database administrators, IT professionals, and security specialists responsible for securing SQL Server environments. Delivered by experienced database security experts with years of practical knowledge and successful projects, this course offers an in-depth, hands-on experience with SQL Server 2022 and 2025.

Throughout the five-day workshop, we will explore every layer of SQL Server security, from understanding core security principles to implementing advanced protection mechanisms such as encryption, role-based access control, and auditing. We will examine system and network security implications on database servers, cover the latest security features, and discuss how to integrate SQL Server with Azure security solutions like Azure Defender and Sentinel.

Our practical, scenario-based exercises will allow you to test security configurations, simulate attacks, and implement countermeasures, giving you the confidence to secure your SQL Server infrastructure effectively. Additionally, we will get into monitoring and compliance auditing to ensure regulatory alignment with standards like GDPR and PCI-DSS.

At the end of the training, you will have a solid understanding of SQL Server security, the ability to identify and mitigate threats, and the knowledge to configure robust defenses.

Duration: 5 days (35 hours)

Running hours: 9AM - 4PM (CET)



Loads of Knowledge

The course is an intense workshop! During these 5 days we recommend a good cup of coffee – this course is really intense and in order not to miss a thing you MUST stay awake!



Exercises

This workshop is based on practical knowledge from tons of successful projects, many years of real-world experience, and no mercy for misconfigurations or insecure solutions! All exercises are based on SQL Server 2022 and 2025. Remember that the hybrid identity lab environment will stay online for an extra three weeks so you may practice even more after the training is completed!



Certification

What is wonderful about our certification is that it is **lifetime valid** with **no renewal fees** – the technology changes, but fundamentals and attitude remain mostly the same. Our Virtual Certificates, which entitle you to collect **CPE Points**, are issued via Accredible.



Target Audience

Database administrators, infrastructure architects, security professionals, system engineers, advanced database developer, IT professionals, security consultants and other people responsible for implementing databases security.

CQURE
ACADEMY

Agenda

Module 1: Overview of SQL Server Security (SQL Server 2022 & 2025)

- a) New security features in SQL Server 2022 and 2025, including enhanced encryption and cloud integration.
- b) SQL Server architecture and how it impacts security.
- c) Integration with Azure SQL Database, Azure Defender, and Azure Active Directory for improved security in hybrid environments.

Module 2: Common Threats & Best Practices for Data Protection

- a) Identifying common SQL Server vulnerabilities (SQL injection, unauthorized access, misconfigurations).
- b) Best practices for protecting SQL Server, including encryption, secure authentication, and role-based access control.

Module 3: Setting Up SQL Server Environment

- a) Installation of SQL Server 2022, ensuring secure configuration.
- b) Configuring firewalls and ports for secure SQL Server access.
- c) Testing connectivity using different protocols (TCP/IP, Named Pipes) and validating network security.

Module 4: Securing the Operating System & Network

- a) Hardening Windows Server to protect SQL Server from external threats.
- b) Configuring secure file-sharing, system permissions, and Windows Defender.
- c) Setting up firewall rules and encrypted communications to prevent unauthorized access.

Module 5: User Account and Role Management

- a) Creating and managing SQL Server logins, using Windows Authentication vs. SQL Authentication.
- b) Integrating Azure Active Directory Authentication for centralized identity management.
- c) Role-based security and assigning permissions based on job functions to implement the Principle of Least Privilege.

Module 6: Managing Permissions and Data Access

- a) Implementing row-level security to restrict data access based on user context.
- b) Using Dynamic Data Masking to obfuscate sensitive information from unauthorized users.
- c) Configuring Custom Permissions and testing access controls with different user roles.

Module 7: Data Encryption in SQL Server

- a) Always Encrypted for encrypting sensitive data both at rest and in transit.
- b) Transparent Database Encryption (TDE) for protecting entire databases and backups.
- c) Column-Level Encryption and implementing Dynamic Data Masking to secure sensitive columns.
- d) Best practices for End-to-End Encryption to secure data throughout its lifecycle.

Module 8: Backup Security

- a) Best practices for securing backup files, including encryption and managing backup certificates.
- b) Creating encrypted backups and testing backup and restore procedures to ensure data security.

Module 9: Auditing SQL Server Access and Data Usage

- a) Configuring SQL Server Auditing to log access attempts, data changes, and administrative actions.
- b) Using Extended Events to monitor SQL Server activities and detect unusual or suspicious behavior.
- c) Implementing auditing for compliance with regulations like GDPR, PCI-DSS, and HIPAA.

Module 10: Security Monitoring Tools

- a) Integrating Azure Defender for SQL Server to monitor vulnerabilities and threats in SQL Server environments.
- b) Using Azure Sentinel for advanced threat detection and security information management (SIEM).

- c) Setting up monitoring alerts and integrating SQL Server logs with SIEM systems for real-time threat analysis.

Module 11: Securing SQL Server Services

- a) Securing SQL Server Agent, Analysis Services (SSAS), and Reporting Services (SSRS) by controlling access to these services and jobs.
- b) Implementing policies to ensure that only authorized users have access to critical SQL Server services and data.
- c) Securing Azure SQL Database by configuring firewall settings, virtual networks, and managing secure access through Private Endpoints.

Module 12: Protecting SQL Server Instances from External Attacks

- a) Techniques to prevent SQL injection and other common attacks by using parameterized queries and stored procedures.
- b) Securing SQL Server against Denial of Service (DoS) attacks by configuring server resources and network isolation.
- c) Ensuring secure communication by using SSL/TLS for data in transit and encryption for communication channels between clients and SQL Server instances.

Module 13: Simulating Attacks and Testing Responses

- a) Simulating real-world attacks, such as SQL injection, unauthorized access attempts, and Denial of Service attacks.
- b) Testing SQL Server defenses against these simulated attacks to evaluate security configurations and response mechanisms.
- c) Reviewing SQL Server's ability to log attacks and respond appropriately to minimize damage.

Module 14: Managing Certificates

- a) Configuring SSL/TLS certificates for encrypted connections between SQL Server and clients.
- b) Managing certificates for backup encryption and securing data exchanges.
- c) Ensuring the integrity of certificates used for authentication and encryption across the SQL Server infrastructure.

