

Course Outline

2787- Designing Security for Microsoft SQL Server 2005



Duration: 2 days (12 hours)

Learning Objectives:

This course enables database administrators who work with enterprise environments to design security for database systems using Microsoft SQL ServerT 2005. The course emphasizes that students should think about the whole environment, which includes business needs, regulatory requirements, network systems, and database considerations during design. Students will also learn how to monitor security and respond to threats

Target Audience:

This course is intended for current professional database administrators who have three or more years of on-the-job experience administering SQL Server database solutions in an enterprise environment

Prerequisites:

- Have basic knowledge of security protocols and how they work. For example, Windows NT LAN Manager (NTLM) or Kerberos
- Have basic knowledge of public key infrastructure (PKI) systems. For example, how public and private keys work, strengths and weaknesses, and what they are used for
- Have working knowledge of network architectures and technologies. For example, how a firewall works, how IPSec works in a networking context, and common vulnerability points
- Have working knowledge of Active Directory directory service. For example, security models, policies, group policy objects (GPOs), and organizational units (OUs)
- Be able to design a database to third normal form (3NF) and know the tradeoffs when backing out of the fully normalized design (denormalization) and designing for performance and business requirements in addition to being familiar with design models, such as Star and Snowflake schemas
- Have strong monitoring and troubleshooting skills
- Have experience creating Microsoft Office Visio drawings or have equivalent knowledge
- Have strong knowledge of the operating system and platform. That is, how the operating system integrates with the database, what the platform or operating system can do, interaction between the operating system and the database
- Have basic knowledge of application architecture. That is, different methods of implementing security in an application, how applications can be designed in three layers, what applications can do, the interaction between applications and the database, and interactions between the database and the platform or operating system
- Have knowledge about network security tools. For example, sniffer and port scanning. Must understand how they should be used
- Be able to use patch management systems
- Have knowledge of common attack methods. For example, buffer overflow, and replay attacks
- Be familiar with SQL Server 2005 features, tools, and technologies
- Have a Microsoft Certified Technology Specialist: Microsoft SQL Server 2005 credential or equivalent experience

In addition, it is recommended, but not required, that students have completed:

- Course 2778: Writing Queries Using Microsoft SQL Server 2005 Transact-SQL
- Course 2779: Implementing a Microsoft SQL Server 2005 Database
- Course 2780: Maintaining a Microsoft SQL Server 2005 Database

Topics Covered:

- Introduction to Designing SQL Server Security
 - Principles of Database Security
 - Methodology for Designing a SQL Server Security Policy
 - Monitoring SQL Server Security
- Designing a SQL Server Systems Infrastructure Security Policy
 - Integrating with Enterprise Authentication Systems
 - Developing Windows Server-Level Security Policies
 - Developing a Secure Communication Policy
 - Defining SQL Server Security Monitoring Standards
 - Designing a SQL Server Systems Infrastructure Security Policy
 - Developing Microsoft Windows Server-Level Security Policies
 - Developing a Secure Communication Policy
 - Integrating SQL Server Security Within the Active Directory Environment
 - Integrating SQL Server Security With Firewall Configurations
 - Discussing Systems Infrastructure Security Integration
 - Creating an Infrastructure Security Inventory
 - Auditing the SQL Server Logins
 - Auditing the Windows Local Password Policy
 - Auditing SQL Server Service Accounts
 - Monitoring Security at the Enterprise and Server Levels
- Designing Security Policies for Instances and Databases
 - Designing an Instance-Level Security Policy
 - Designing a Database-Level Security Policy
 - Designing an Object-Level Security Policy
 - Defining Security Monitoring Standards for Instances and Databases
 - Designing Security Policies for Instances and Databases
 - Designing an Instance-Level Security Policy
 - Designing a Database-Level Security Policy
 - Designing an Object-Level Security Policy
 - Discussing Database Security Exceptions
 - Validating Security Policies for Instances and Databases
 - Auditing Existing Server Logins
 - Auditing SQL Server Roles Membership
 - Analyzing Existing Object Permissions
 - Monitoring Security at the Instance and Database Level
- Integrating Data Encryption into a Database Security Design
 - Securing Data by Using Encryption and Certificates
 - Designing Data Encryption Policies
 - Determining a Key Storage Method

- Integrating Data Encryption into a Database Security Design
- Selecting a Data Security Method
- Designing a Data Encryption Security Policy
- Selecting a Key Storage Method
- Designing a Security Exceptions Policy
 - Analyzing Business and Regulatory Requirements
 - Determining the Exceptions and their Impact
 - Designing a Security Exceptions policy
 - Identifying Variations from the Security Policy
 - Obtaining Approval of the Security Policy
 - Discussing the Results of Policy Approval Presentations
- Designing a Response Strategy for Threats and Attacks
 - Designing a Response Policy for Virus and Worm Attacks
 - Designing a Response Policy for Denial-of-Service Attacks
 - Designing a Response Policy for Internal and SQL Injection Attacks
 - Designing a Response Strategy for Threats and Attacks
 - Designing a Response Policy for Virus and Worm Attacks
 - Designing a Response Policy for Denial-of-Service Attacks
 - Designing a Response Policy for Internal Attacks
 - Validating a Security Policy