Data AI: SQL Security Essentials

WorkshopPLUS

Duration: 3 days

Focus Area: Security and Compliance

Difficulty: 300-Advanced

Overview

This course will provide attendees with the deep knowledge of hardening and securing SQL Server using different built-in features and techniques. It also covers audit strategy according to business needs, certificates to protect data, Policy Based Management, hardening Windows and SQL Server and forensic techniques to identify attacks and act upon consequence.
This workshop is targeted at Architect, Database Admins and Security Admins.

Objectives

After completing this training, students will be able to:

- Understand SQL Server Authentication
- Learn how to audit SQL Server
- Understand the requirements before and after SQL Server installation
- Learn SQL Server Vulnerability Assessment
- Understand how to Prevent SQL Injection Attack
- Understand the concepts of certificates, encryption and cryptography.
- Gain experience on securing and exploring the tools available to audit, trace and identify possible security breaches.

Key Takeaways

Course Material

- Gain a deeper understanding of monitoring data access across all SQL Servers, hardening SQL Server on premises and cloud.

Hands-on Labs

- Most of the concepts covered above will be supported by hands-on labs and demos.
- Attendees have access to resources and labs for up to 6 months after workshop completion.

Agenda

Day 1

- SQL Security Basics
- SQL Audit

Day 2

- Data Encryption
- Policy based management
- Host Security

Day 3

- SQL Hardening
- SQL Server Security Forensics
- SQL Server Security on Linux [Optional]

Plan for three full days. Early departure on any day is not recommended

Course Details

Module 1: SQL Security Basics

- SQL Security Overview
- SQL Server Logins and Users
- SQL Server Roles and Credentials
- SQL Server Authentication
- SQL Server Authorization and Schemas

Module 2: SQL Audit

- Working with SQL Server Trace
- Working with Extended Events
- Introduction to SQL Server Audit
- SQL Server Audit Events Discovery
- Using PowerShell for Auditing SQL Server

Module 3: Data Encryption

- Managing Certificates
- Key Management and Data Encryption
- Always Encrypted
- Row-Level Security
- Dynamic Data Masking

Module 4: Policy based management

- Policy Based Management Architecture
- Policy Based Management Implementation
- Policy Based Management Monitoring and Alerting
- Policy Based Management Monitoring with PowerShell
- Enterprise Policy Management (EPM) Framework

Module 5: Host Security

- Securing the Operating System (OS)
- Network Security with Firewall and Advanced Features
- Network Security with Extended Protection
- Service Accounts
- Kerberos Authentication

Module 6: SQL Hardening

- Considerations before SQL Server Installation
- Network Considerations after SQL Server installation
- Connectivity Considerations after SQL Server Installation
- Connectivity Considerations after SQL Server Installation
- Surface Area Configuration after SQL Server Installation
- Introduction to SQL Server Vulnerability Assessment
- How to Prevent SQL Injection Attack

Module 7: SQL Server Security Forensics

- Operating System Logging Mechanisms
- SQL Server Logging Mechanisms
- Central and Other Logs in SQL Server
- Anti-Forensics
  Attack Scenarios

Module 8: SQL Server Security on Linux (Optional)

- SQL Server Security Features on Linux
- SQL Server on Linux Security Limitations

Recommended Qualifications

Before attending this workshop, it is highly recommended that you meet the following criteria:

- Understanding of the fundamentals of SQL Server
- Understanding of the fundamentals of Security concepts

Hardware Requirements

- An Intel Core-i5-based PC
- USB port
- Microsoft/Windows Live ID to connect to the virtual environment
- 4 GB RAM
- 128 GB HDD
- Windows 7 SP1 or later
- Office 2013 Professional Plus
- Internet access with at least 1 Mbps bandwidth per student.

For more information

Contact your Microsoft Account Representative for further details.

This data sheet is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY