WorkshopPLUS – Data AI: SQL Security Essentials

WorkshopPLUS

Duration: 3 Day [Remote / Onsite]
Difficulty Level: 300 - Advanced

Description

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

Objectives

- Understand SQL Server Authentication Authorization process.
- Understand Windows Firewall with Advanced Security, Extended Protection for Authentication and network considerations for SQL Server.
- Learn how to audit SQL Server.
- Understand how to Prevent SQL Injection Attack.
- Understand the concepts of certificates, encryption and cryptography.
- Gain experience on securing and exploring the tools to audit, trace, and identify possible security breaches.
- Understand PowerShell Desired State Configuration.

Outcomes

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

Methodology

Learn by example - Learn with presentations, demonstrations and group discussion.

Requirements

Participants

- Database Administrators
- Data Engineers
- Business Analysts

Skill Requirements - Recommended

- Basic concepts and knowledge of SQL Server
- fundamentals of Security concepts

Delivery Requirements

- Computer with Windows 10 or later, audio equipment, internet access.
- Modern browser and at least 1-Mbps bandwidth per participant.
- Microsoft/Windows Live ID to connect to the virtual environment.
- Microsoft Teams for remote delivery.

Microsoft

Delivery Outline

The scope of this engagement will be agreed based on your specific needs. Final agenda will be determined in the scoping call.

Delivery Details

Platform and Network Security

- Securing the Operating System
- Network Security with Firewall and Advanced Features
- Network Security with Extended Protection
- Service Accounts and Local Rights Assignments
- Networking and Connectivity Considerations
- Kerberos Authentication

SQL Server Security Model

- SQL Security Overview
- Authentication and Authorization
- SQL Server Logins and Users
- SQL Server Roles and Credentials
- SQL Server Permissions and Schemas
- Metadata Visibility and Execution Contexts
- Contained Databases

Data Encryption and Security

- Managing Certificates and Keys
- Data Encryption including Backup Encryption, Transparent Data Encryption (TDE) and Always Encrypted
- Encrypted Connections
- Row-Level Security
- Dynamic Data Masking

SQL Server Logging, Auditing, and Vulnerability Assessment

- SQL Server Trace and Auditing Mechanisms
- Introduction to SQL Server Audit
- Ledger for SQL Server

Surface Area Configuration

- Surface Area Configuration After SQL Server Installation
- Policy-Based Management
- PowerShell Desired State Configuration
- Extending Security from the Cloud

Threats and Countermeasures

- Operating System Logging Mechanisms
- SQL Server Logging Mechanisms
- Central and Other Logs in SQL Server
- SQL and Code Injection Attacks
- Anti-Forensics Attack Scenario

For more information: Contact your Microsoft Representative for more details.