Securing Data on Microsoft SQL Server 2014

Institution: **Phone:** +

Instructor: **E-mail:**

Hours: 12

Intro

Security is a process of keeping necessary level of risk in acceptable boundaries. That means, security is a continual process and not a final state. Organization or institution can't consider itself "secured" after last security check. That process needs to be continual. Security require: people, knowledge and resources and it based on the constant following security trends.

Description:

Target Audience This course is intended for Database Developers, Security Professionals, Database Administrators, and other people that need to secure database servers

Goals:

The goal of this two-day instructor-led course is to provide students with the database and SQL server security knowledge and skills necessary to secure data on Microsoft SQL Server 2014.

Prerequired:

Students should have a working knowledge of the following:

- Microsoft SQL Server 2008/2014/2014

Minimum PCs requirement: Intel Core i5, 8GB RAM, 500 GB HDD.

PCs has to have the following software preinstalled: Windows with SQL Server 2014

Type of exam:

1- Practical exam for evaluation of security skills

Pregled kursa:

Module	Decription
Module 1: Security and Privacy Concepts in SQL Server	This module provides the background knowledge of security and privacy concepts in SQL server. Lessons presented in this module will provide an overview of SQL Server 2014 security and privacy. You will also learn the basics of auditing/monitoring users and how to use the built-in SQL Server tools.
Module 2: Security During and After Installation	This module describes the security steps during and after installing SQL Server 2014. Lessons presented in this module will detail the security and service accounts during the installation. You will learn about the SQL Server Configuration Manager and working with Windows Firewall. You will also understand the password issues and policies for consumers of SQL resources.
Module 3: Authentication and Authorization	This module describes how to the authentication and authorization process in SQL Server works. Lessons presented in this module will detail how to authenticate and authorize users to access and use SQL data. You will also learn about server-side and database security.
Module 4: Protecting Data	This module describes how to protect your data in SQL Server 2014. Lessons presented in this module will detail how cryptography works and the crypto features in SQL Server 2014. You will learn about security keys and how they various methods of data encryption used, such as TDE, Symmetric and Asymmetric encryption. You will also learn the difference between hashing and encryption
Module 5: Auditing on SQL Server	This module describes the auditing process and how to use the various methods. Lessons presented in this module will detail the classic auditing methods, such as using triggers. You will learn how to configure SQL Server auditing and how to access the audit logs. You will also learn about database forensics and collecting digital evidence.
Module 6: SQL Server Security Threats and Countermeasures	This module describes the security threats and the countermeasures used to protect your data and database server. Lessons presented in this module will detail the weak points inside and outside of SQL Server 2014. You will also learn how to identify specific threats, such as data transfer sniffing and SQL code injection and how to prevent them with the appropriate countermeasures