

Course Name:	Windows 2008 and Windows 7 Security
Duration:	2 Day
Medium of Instruction:	Cantonese (with terminology & handout in English)
Award of Certificate:	Certificate of Attendance

Nature and Objectives:

Windows 7 and 2008 server are a complete change on Windows architecture, operation scheme, user account management, event logs management, etc. It is a completely different OS. Microsoft adopts industry best practices and implements these practices in the Microsoft Windows 7 and 2008 server. System kernels, user account control, system management modules and many other security features have been changed. The aim of this course to equip the participants with knowledge in deploying secure Windows 7 and 2008 server environment. In addition to concept, case studies, intensive hands-on workshop will be arranged through out the training to make participants to grasp the essential knowledge of deploying secure Windows environment.

Who Should Attend:

System and network administrators/ engineers / Analysts, Technical Engineers/ Managers, Data Security Officers, Information Security Analysts / Managers, IT Auditors and Managers, Network Manager, Security Consultants, and System Integrators. Participants are expected to have hands-on experience in administering Windows2008 and Windows 7.

Course Outline:

Microsoft OS Security Concepts

- New Windows internal design
- Security Design Concept of new Windows
- New features in Microsoft Windows 7 & 2008
- Security Features in Windows 7 & 2008

Identification, Authentication, Authorization and Access Control

- Secure Authentication Module
- Login Authentication and Authorization
- NTLM, NT GINA, Kerberos
- Credential Manager

File Systems

- File Systems Security
- Access Control setting in new File System
- Encrypted File Systems Security
- User Access Control
- Bit Locker Security
- File Virtualization

System Configuration

- Active Directory
- Bootup process
- Registry Security Setting
- Security for Domains Controllers and Servers

Group Security Policies

- Windows Policy Enforcement
- Microsoft Network Access Protection and Quarantine Control Network
- Windows Integrity Control

- Security Template Settings
- Security Configuration and Analysis Snap-in Template
- Group Policies

Network Configuration & Network Services

- Windows Networking design
- Remote Access Facilities
- IP Security, VPN
- DNS and DHCP Security
- IIS 7 Security

Patches

- Patch management system for Windows
- WSUS and other patch management systems

Backup and Restore

- System Backup Configuration
- System Restoration Configuration
- Automated System Recovery Configuration

Audit Logging

- Event log facilities & setting
- Event log review procedures

Other Windows Features

- Windows firewall with advanced security
- Internet Explorer 8 Security
- Parental Control in Windows
- Software Restriction Policies
- Secure Code Signing
- Windows PowerShell