凱風電腦有限公司 |Gallant Computer Company Ltd.
Hotline: 2833 3816
Fax: 2851 6452
Email: info@gallantcomputer.com
Website: www.gallantcomputer.com

(20744A) – Securing Windows Server 2016

OBJECTIVE

This instructor-led course teaches IT professionals how they can enhance the security of the IT infrastructure that they administer. This course begins by emphasizing the importance of assuming that network breaches have occurred already, and then teaches you how to protect administrative credentials and rights to ensure that administrators can perform only the tasks that they need to, when they need to.

This course also details how you can mitigate malware threats, identify security issues by using auditing and the Advanced Threat Analysis feature in Windows Server 2016, secure your virtualization platform, and use new deployment options, such as Nano server and containers to enhance security. The course also explains how you can help protect access to files by using encryption and dynamic access control, and how you can enhance your network's security.

COURSE TOPICS

Module 1: Breach detection and using the Sysinternals tools

- Overview of breach detection
- Using the Sysinternals tools to detect breaches

Module 2: Protecting credentials and privileged access

- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution

Module 3: Limiting administrator rights with Just Enough Administration

- Understanding JEA
- Configuring and deploying JEA

Module 4: Privileged Access Management and administrative forests

- Understanding ESAE forests
- Overview of MIM
- Implementing JIT and Privileged Access Management by using MIM

Module 5: Mitigating malware and threats

- Configuring and managing Windows Defender
- Using software restricting policies (SRPs) and AppLocker
- Configuring and using Device Guard
- Using and deploying the Enhanced Mitigation Experience Toolkit

Module 6: Analysing activity by using advanced auditing and log analytics

- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging

Module 7: Analysing activity with Microsoft Advanced Threat Analytics feature and Operations Management Suite

- Overview of Advanced Threat Analytics
- Understanding OMS

Module 8: Securing your virtualization an infrastructure

- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs

Module 9: Securing application development and server-workload infrastructure

- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers

Module 10: Protecting data with encryption

- Planning and implementing encryption
- Planning and implementing BitLocker

Module 11: Limiting access to file and folders

- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)

Module 12: Using firewalls to control network traffic flow

- Understanding Windows Firewall
- Software-defined distributed firewalls

Module 13: Securing network traffic

- Network-related security threats and connection-security rules
- Configuring advanced DNS settings
- Examining network traffic with Microsoft Message Analyzer
- Securing SMB traffic, and analysing SMB traffic

Module 14: Updating Windows Server

- Overview of WSUS
- Deploying updates by using WSUS

PREREQUISITES

Students should have at least two years of experience in the IT field and should have:

- Completed courses 740, 741, and 742, or the equivalent.
- A solid, practical understanding of networking fundamentals, including TCP/IP, User Datagram Protocol (UDP), and Domain Name System (DNS).
- A solid, practical understanding of Active Directory Domain Services (AD DS) principles.
- A solid, practical understanding of Microsoft Hyper-V virtualization fundamentals.
- An understanding of Windows Server security principles.

TRAINING APPROACH

This course includes lectures, course notes, exercises and hands-on practice.

COURSE DURATION

24 Hours (in 3 days)

Time: 9:00am to 6:00pm

Lunch Time: 1:00pm to 2:00pm

CERTIFICATION COMPLETION

A certificate of completion is provided for all trainees attending the course