



# Securing Windows Server 2016

Course 20744C

5 Days

Instructor-led, Hands on

## Introduction

This five-day, 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 explains how you can use auditing and the Advanced Threat Analysis feature in Windows Server 2016 to identify security issues. You will also learn how to mitigate malware threats, secure your virtualization platform, and use 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.

This course is for IT professionals who need to securely administer Windows Server 2016 networks. These professionals typically work with networks that are configured as Windows Server domain-based environments, with managed access to the internet and cloud services. Students who seek certification in the 70-744 Securing Windows server exam also will benefit from this course.

## Prerequisites

In addition to professional experience, students who attend this training should already have the following technical knowledge:

- 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.

## Course Objectives

Upon completion of this course, attendees will be able to:

- Secure Windows Server.
- Protect credentials and implement privileged access workstations
- Limit administrator rights with Just Enough Administration
- Manage privileged access

Contact ISInc for more information at 916.920.1700 or by visiting our website at <http://www.isinc.com>

- Mitigate malware and threats
- Analyze activity with advanced auditing and log analytics
- Deploy and configure Advanced Threat Analytics and Microsoft Operations Management Suite
- Configure Guarded Fabric virtual machines (VMs)
- Use the Security Compliance Toolkit (SCT) and containers to improve security
- Plan and protect data
- Optimize and secure file services
- Secure network traffic with firewalls and encryption
- Secure network traffic by using DNSSEC and Message Analyzer

## Course Outline

### Module 1: Attacks, breach detection and Sysinternals tools

This module frames the course so that students are thinking about security in environments where the infrastructure's basis is predominantly Microsoft products. The module begins with teaching students about the "assume breach" philosophy and getting them to understand the different types of attacks that can occur, including attack timelines and vectors. Additionally, it gets students thinking about key resources, how they respond when they detect an incident, and how an organization's direct needs and legislative requirements dictate its security policy

#### Lessons

- Understanding attacks
- Detecting breaches
- Examining activity with the Sysinternals tool

Lab : Basic breach detection and incident response strategies

- Identifying attack types
- Exploring the SysInternals tools

After completing this course, students will be able to:

- Describe the types of attacks that can occur.
- Explain how to detect security breaches.
- Explain how to examine activity by using the Sysinternals suite of tools.

### Module 2: Protecting credentials and privileged access

This module covers user accounts and rights, computer and service accounts, credentials, Privileged Access Workstations, and the Local Administrator Password Solution. In this module, students will learn about configuring user rights and security options, protecting credentials by using Credential Guard, implementing Privileged Access Workstations, and managing and deploying Local Administrator Password Solution to manage local administrator account passwords.

Contact ISInc for more information at 916.920.1700 or by visiting our website at <http://www.isinc.com>

## Lessons

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

Lab : Implementing user rights, security options, and group-managed service accounts

- Configuring user rights and account-security options
- Delegating privileges
- Creating group Managed Service Accounts
- Locating problematic accounts

Lab : Configuring and deploying LAPs

- Installing and configuring local administrator password solution (LAPs)
- Deploying and testing LAPs

After completing this module, students will be able to:

- Configure user rights.
- Implement computer and service accounts.
- Protect credentials.
- Describe how to configure Privileged Access Workstations and jump servers.
- Configure the Local Administrator Password Solution (LAPS).

## **Module 3: Limiting administrator rights with Just Enough Administration**

This module explains how to deploy and configure Just Enough Administration (JEA), which is an administrative technology that allows students to apply role-based access control (RBAC) principles through Windows PowerShell remote sessions.

## Lessons

- Understanding JEA
- Verifying and deploying JEA

Lab : Limiting administrator privileges by using JEA

- Creating a role-capability file
- Creating a session-configuration file
- Creating a JEA endpoint
- Connecting to a JEA endpoint
- Deploying JEA by using Desire State Configuration (DSC)

After completing this module, students will be able to:

Contact ISInc for more information at 916.920.1700 or by visiting our website at <http://www.isinc.com>



- Understand JEA.
- Verify and deploy JEA.

## **Module 4: Privileged Access Management and administrative forests**

This module explains the concepts of Enhanced Security Administrative Environment (ESAE) forests, Microsoft Identity Manager (MIM), and Just In Time (JIT) Administration, or Privileged Access Management (PAM).

### Lessons

- ESAE forests
- Overview of Microsoft Identity Manager
- Overview of JIT administration and PAM

Lab : Limiting administrator privileges by using PAM (Privileged Access Management)

- Layered approach to security
- Configuring trust relationships and shadow principals
- Requesting privileges access
- Managing PAM roles

After completing this module, students will be able to:

- Describe ESAE forests.
- Describe MIM.
- Understand JIT administration and PAM.

## **Module 5: Mitigating malware and threats**

This module explains how to use tools such as Windows Defender, Windows AppLocker, Microsoft Device Guard, Windows Defender Application Guard, and Windows Defender Exploit Guard.

### Lessons

- Configuring and managing Windows Defender
- Restricting software
- Configuring and using the Device Guard feature

Lab : Securing applications by using AppLocker, Windows Defender and Device Guard Rules

- Configuring Windows Defender
- Configuring AppLocker
- Configuring Device Guard

After completing this module, students will be able to:

Contact ISInc for more information at 916.920.1700 or by visiting our website at <http://www.isinc.com>

- Configure and manage Windows Defender.
- Use software restriction policies and AppLocker.
- Configure and use the Device Guard feature.

## **Module 6: Analyzing activity by using advanced auditing and log analytics**

This module provides an overview of auditing, and then goes into detail about how to configure advanced auditing and Windows PowerShell auditing and logging.

### Lessons

- Overview of auditing
- Advanced auditing
- Windows PowerShell auditing and logging

### Lab : Configuring advanced auditing

- Configuring auditing of file-system access
- Auditing domain sign-ins
- Managing advanced audit policy configuration
- Windows PowerShell logging and auditing

After completing this module, students will be able to:

- Describe auditing.
- Understand advanced auditing.
- Configure Windows PowerShell auditing and logging.

## **Module 7: Deploying and configuring Advanced Threat Analytics feature and Operations Management Suite**

This module explains the Microsoft Advanced Threat Analytics tool and the Microsoft Operations Management suite (OMS). It also explains how you can use them to monitor and analyse the security of a Windows Server deployment. You will also learn about Microsoft Azure Security Center, which allows you to manage and monitor the security configuration of workloads both on-premises and in the cloud.

### Lessons

- Deploying and configuring ATA
- Deploying and configuring Microsoft Operations Management Suite
- Deploying and configuring Azure Security Center

### Lab : Deploying ATA and Microsoft Operations Management Suite and Azure Security Center

- Preparing and deploying ATA

Contact ISInc for more information at 916.920.1700 or by visiting our website at <http://www.isinc.com>



- Preparing and deploying Microsoft Operations Management Suite
- Deploying and configuring Azure Security Center

After completing this module, students will be able to:

- Deploy and configure ATA.
- Deploy and configure Microsoft Operations Management Suite.
- Deploy and configure Azure Security Center.

## **Module 8: Secure Virtualization infrastructure**

This module explains how to configure Guarded Fabric virtual machines (VMs), including the requirements for shielded and encryption-supported VMs.

Lessons

- Guarded Fabric
- Shielded and encryption-supported VMs

Lab : Guarded Fabric with administrator-trusted attestation and shielded VMs

- Deploying a guarded fabric VMs
- Deploying a shielded VM

After completing this module, students will be able to:

- Configure the guarded fabric.
- Describe shielded and encryption-supported VMs

## **Module 9: Securing application development and server-workload infrastructure**

This module describes the SCT, which is a free, downloadable set of tools that you can use to create and apply security settings. You will also learn about improving platform security by reducing the size and scope of application and compute resources by containerizing workloads.

Lessons

- Using Security Compliance Manager
- Understanding containers

Lab : Using Security Compliance Manager

- Configuring a security baseline for Windows Server 2016
- Deploying a security baseline for Windows Server 2016

Lab : Deploying and Configuring containers

- Deploying and managing a Windows container

After completing this module, students will be able to:

Contact ISInc for more information at 916.920.1700 or by visiting our website at <http://www.isinc.com>



- Install SCT, and create and deploy security baselines.
- Configure Windows and Hyper-V containers in Windows Server 2016.

## **Module 10: Planning and protecting data**

This module explains how to configure Encrypting File System (EFS) and BitLocker drive encryption to protect data at rest. You will also learn about extending protection into the cloud by using Azure Information Protection.

### Lessons

- Planning and implementing encryption
- Planning and implementing BitLocker
- Protecting data by using Azure Information Protection

### Lab : Protecting data by using encryption and BitLocker

- Encrypting and recovering access to encrypted files
- Using BitLocker to protect data

After completing this module, students will be able to:

- Plan and implement encryption.
- Plan and implement BitLocker.
- Plan and implement Azure Information Protection

## **Module 11: Optimizing and securing file services**

This module explains how to optimize file services by configuring File Server Resource Manager (FSRM) and Distributed File System (DFS). Students also will learn how to manage access to shared files by configuring Dynamic Access Control (DAC).

### Lessons

- File Server Resource Manager
- Implementing classification management and file-management tasks
- Dynamic Access Control

### Lab : Quotas and file screening

- Configuring FSRM quotas
- Configuring file screening and storage reports

### Lab : Implementing Dynamic Access Control

- Preparing for implementing DAC
- Implementing DAC
- Validating and remediating Dynamic Access Control

After completing this module, students will be able to:

Contact ISInc for more information at 916.920.1700 or by visiting our website at <http://www.isinc.com>

- Describe File Server Resource Manager.
- Implement classification and file management tasks.
- Implement Dynamic Access Control.

## **Module 12: Securing network traffic with firewalls and encryption**

This module explains how you can use Windows Firewall as an important part of an organization's protection strategy. It explains the use of Internet Protocol security (IPsec) to encrypt network traffic and to establish security zones on your network. You will also learn about the Datacenter Firewall feature that you can use to help protect your on-premises virtual environments.

### Lessons

- Understanding network-related security threats
- Understanding Windows Firewall with Advanced Security
- Configuring IPsec
- Datacenter Firewall

### Lab : Configuring Windows Firewall with Advanced Security

- Creating and testing inbound rules
- Creating and testing outbound rules
- Creating and testing connections security rules

After completing this module, students will be able to:

- Understand network-related security threats
- Understand Windows Firewall with Advanced Security
- Configure IPsec
- Understand Datacenter Firewall

## **Module 13: Securing network traffic**

This module explores some of the Windows Server 2016 technologies that you can use to help mitigate network-security threats. It explains how you can configure DNSSEC to help protect network traffic, and use Microsoft Message Analyzer to monitor network traffic. The module also describes how to secure Server Message Block (SMB) traffic.

### Lessons

- Configuring advanced DNS settings
- Examining network traffic with Message Analyzer
- Securing and analyzing SMB traffic

### Lab : Securing DNS

- Configuring and testing DNSSEC
- Configuring DNS policies and RRL

Contact ISInc for more information at 916.920.1700 or by visiting our website at <http://www.isinc.com>



Lab : Microsoft Message Analyzer and SMB encryption

- Installing and using Microsoft Message Analyzer
- Configuring and verifying SMB encryption on SMB shares

After completing this module, students will be able to:

- Configure advanced DNS settings.
- Use the Message Analyzer.
- Secure SMB traffic.