skillsoft global knowledge™

SECURING WINDOWS SERVER 2016

Course Code: 821530

Discover how you can enhance your network's security.

In this course, you will learn how to enhance the security of the IT infrastructure that you 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 the precise tasks they need at any time, 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.

What You'll Learn

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

Who Needs to Attend

IT professionals who need to administer Windows Server 2016 networks securely and work with networks that are configured as Windows Server domain-based environments with managed access to the Internet and cloud services.

Prerequisites

At least two years of experience in the IT field as well as:

- 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

SECURING WINDOWS SERVER 2016

Course Code: 821530

CLASSROOM LIVE	$2,995 USD	5 Day

Classroom Live Outline

1. Attacks, Breach Detection, and Sysinternals Tools
    - Understanding attacks
    - Detecting security breaches
    - Examining activity with the Sysinternals tools
2. Protecting Credentials and Privileged Access
    - Understanding User Rights
    - Computer and Service Accounts
    - Protecting Credentials
    - Privileged Access Workstations and jump servers
    - Local administrator password solution
3. Limiting Administrator Rights with Just Enough Administration (JEA)
    - Understanding JEA
    - Verifying and Deploying JEA
4. Privileged Access Management and Administrative Forest
    - ESAE forests
    - Overview of Microsoft Identity Manager (MIM)
    - Overview of JIT administration and PAM
5. Mitigating Malware and Threats
    - Configuring and Managing Windows Defender
    - Restricting software
    - Configuring and Using Device Guard
6. Analyzing Activity with Advanced Auditing and Log Analytics
    - Overview of Auditing
    - Advanced Auditing
    - Windows PowerShell Auditing and Logging
7. Deploying and Configuring Advanced Threat Analytics (ATA) and Operations Management Suite (OMS)
    - Deploying and configuring ATA
    - Deploying and configuring Microsoft Operations Management Suite

    - Deploying and configuring Azure Security Center
8. Secure Virtualization Infrastructure
    - Guarded Fabric
    - Shielded and Encryption-Supported VMs
9. Securing Application Development and Server-Workload Infrastructure
    - Using Security Compliance Manager
    - Understanding Containers
10. Planning and Protecting Data
    - Planning and Implementing Encryption
    - Planning and Implementing BitLocker
    - Protecting data by using Azure Information Protection
11. Optimizing and Securing File Services
    - Introduction to FSRM
    - Implementing Classification and File-Management Tasks
    - Access Control (DAC)
12. Securing Network Traffic with Firewalls and Encryption
    - Understand network-related security threats
    - Understanding Windows Firewall with Advanced Security
    - Configuring IPsec
    - Datacenter Firewall
13. Securing Network Traffic
    - Configuring Advanced DNS Settings
    - Examining Network Traffic with Microsoft Message Analyzer
    - Securing Server Analyzing SMB Traffic

Classroom Live Labs

- Lab 1: Basic Breach Detection and Incident Response Strategies
- Lab 2: Implementing User Rights, Security Options, and Group-Managed Service Accounts
- Lab 3: Configuring and Deploying LAPs
- Lab 4: Limiting Administrator Privileges with JEA
- Lab 5: Limiting Administrator Privileges with Privileged Access Management
- Lab 6: Securing Applications by with Windows Defeder, AppLocker, , Device Guard Rules.
- Lab 7: Configuring Advanced Auditing
- Lab 8: Deploying Advanced Threat Analytics and Operations Management Suite and Azure Security Center
- Lab 9: Guarded Fabric with Administrator-Trusted Attestation and Shielded VMs
- Lab 10: Using Security Compliance Manager
- Lab 11: Deploying and Configuring Containers
- Lab 12: Protecting Data by Using Encryption and BitLocker
- Lab 13: Quotas and File Screening
- Lab 14: Implementing DAC

- Lab 15: Configuring Windows Firewall with Advanced Security
- Lab 16Securing DNS
- Lab 17: Microsoft Message Analyzer and SMB Encryption

SECURING WINDOWS SERVER 2016

Course Code: 821530

VIRTUAL CLASSROOM LIVE	$2,995 USD	5 Day

Virtual Classroom Live Outline

1. Attacks, Breach Detection, and Sysinternals Tools
    - Understanding attacks
    - Detecting security breaches
    - Examining activity with the Sysinternals tools
2. Protecting Credentials and Privileged Access
    - Understanding User Rights
    - Computer and Service Accounts
    - Protecting Credentials
    - Privileged Access Workstations and jump servers
    - Local administrator password solution
3. Limiting Administrator Rights with Just Enough Administration (JEA)
    - Understanding JEA
    - Verifying and Deploying JEA
4. Privileged Access Management and Administrative Forest
    - ESAE forests
    - Overview of Microsoft Identity Manager (MIM)
    - Overview of JIT administration and PAM
5. Mitigating Malware and Threats
    - Configuring and Managing Windows Defender
    - Restricting software
    - Configuring and Using Device Guard
6. Analyzing Activity with Advanced Auditing and Log Analytics
    - Overview of Auditing
    - Advanced Auditing
    - Windows PowerShell Auditing and Logging
7. Deploying and Configuring Advanced Threat Analytics (ATA) and Operations Management Suite (OMS)
    - Deploying and configuring ATA
    - Deploying and configuring Microsoft Operations Management Suite

    - Deploying and configuring Azure Security Center
8. Secure Virtualization Infrastructure
    - Guarded Fabric
    - Shielded and Encryption-Supported VMs
9. Securing Application Development and Server-Workload Infrastructure
    - Using Security Compliance Manager
    - Understanding Containers
10. Planning and Protecting Data
    - Planning and Implementing Encryption
    - Planning and Implementing BitLocker
    - Protecting data by using Azure Information Protection
11. Optimizing and Securing File Services
    - Introduction to FSRM
    - Implementing Classification and File-Management Tasks
    - Access Control (DAC)
12. Securing Network Traffic with Firewalls and Encryption
    - Understand network-related security threats
    - Understanding Windows Firewall with Advanced Security
    - Configuring IPsec
    - Datacenter Firewall
13. Securing Network Traffic
    - Configuring Advanced DNS Settings
    - Examining Network Traffic with Microsoft Message Analyzer
    - Securing Server Analyzing SMB Traffic

Virtual Classroom Live Labs

- Lab 1: Basic Breach Detection and Incident Response Strategies
- Lab 2: Implementing User Rights, Security Options, and Group-Managed Service Accounts
- Lab 3: Configuring and Deploying LAPs
- Lab 4: Limiting Administrator Privileges with JEA
- Lab 5: Limiting Administrator Privileges with Privileged Access Management
- Lab 6: Securing Applications by with Windows Defeder, AppLocker, , Device Guard Rules.
- Lab 7: Configuring Advanced Auditing
- Lab 8: Deploying Advanced Threat Analytics and Operations Management Suite and Azure Security Center
- Lab 9: Guarded Fabric with Administrator-Trusted Attestation and Shielded VMs
- Lab 10: Using Security Compliance Manager
- Lab 11: Deploying and Configuring Containers
- Lab 12: Protecting Data by Using Encryption and BitLocker
- Lab 13: Quotas and File Screening
- Lab 14: Implementing DAC

- Lab 15: Configuring Windows Firewall with Advanced Security
- Lab 16Securing DNS
- Lab 17: Microsoft Message Analyzer and SMB Encryption

Sep 15 - 19, 2025 | 8:30 AM - 4:30 PM EDT

SECURING WINDOWS SERVER 2016

Course Code: 821530

PRIVATE GROUP TRAINING	5 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/5/2025 9:13:31 PM