Securing Windows Server 2016

Duration: 5 Days   Course Code: M20744   Version: A   Delivery Method: Company Event

Overview:

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 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.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

This course is for IT professionals who need to administer Windows Server 2016 networks securely. 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.

Objectives:

- After completing this course, students will be able to:

- Secure Windows Server.

- Secure application development and a server workload infrastructure.

- Manage security baselines.

- Configure and manage just enough and just-in-time (JIT) administration.

- Manage data security.

- Configure Windows Firewall and a software-defined distributed firewall.

- Secure network traffic.

- Secure your virtualization infrastructure.

- Manage malware and threats.

- Configure advanced auditing.

- Manage software updates.

- Manage threats by using Advanced Threat Analytics (ATA) and Microsoft Operations Management Suite (OMS).

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.

Content:

Module 1: Breach detection and using the Sysinternals tools

In this module, students will learn about breach detection, attack types and vectors, cybercrime, and how you can analyse your system's activity by using the Sysinternals tool suite.

Lessons

- Overview of breach detection
- Using the Sysinternals tools to detect breaches
- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution
- 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
- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging
- Overview of Advanced Threat Analytics
- Understanding OMS
- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs
- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Planning and implementing encryption
- Planning and implementing BitLocker
- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)
- Understanding Windows Firewall
- Software-defined distributed firewalls
- 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
- Overview of WSUS
- Deploying updates by using WSUS

Lab: Basic breach detection and incident response strategies

After completing this module, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.
- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

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

This module explains how to use advanced auditing and Windows PowerShell transcripts.

Lab : Configuring EFS and BitLocker

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

After completing this module, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.
- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

Module 11: Limiting access to file and folders

- Identifying attach types
- Using incident-response strategies
- Exploring the Sysinternals tools

After completing this module, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.
- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

Module 2: Protecting credentials and privileged access

This module explains how you can configure user rights and security options, protect credentials by using credential guard,

---

Lessons

- Overview of breach detection
- Using the Sysinternals tools to detect breaches
- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution
- 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
- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging
- Overview of Advanced Threat Analytics
- Understanding OMS
- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs
- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Planning and implementing encryption
- Planning and implementing BitLocker
- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)
- Understanding Windows Firewall
- Software-defined distributed firewalls
- 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
- Overview of WSUS
- Deploying updates by using WSUS

Lab : Configuring encryption and advanced auditing

- Configuring auditing of file-system access
- Auditing domain logons
- Managing the configuration of advanced audit policies
- Windows PowerShell logging and auditing

After completing this module, students will be able to:

- Describe breach detection.

This module explains how to optimize file services by configuring File Server Resource Manager (FSRM) and Distributed File System (DFS). Students will learn how to protect a device's data by using encryption or BitLocker. Students also will learn how to manage access to shared files by configuring Dynamic Access Control (DAC).

Lessons

- Overview of breach detection
- Using the Sysinternals tools to detect breaches
- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution
- 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
- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging
- Overview of Advanced Threat Analytics
- Understanding OMS
- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs
- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Planning and implementing encryption
- Planning and implementing BitLocker
- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)
- Understanding Windows Firewall
- Software-defined distributed firewalls
- 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
- Overview of WSUS
- Deploying updates by using WSUS

Lab : Configuring quotas and file screening

- Configuring FSRM quotas
- Configuring file screening

implement privileged-access workstations, and manage and deploy a local administrator-password solution so that you can manage passwords for local administrator accounts.

Lessons

- Overview of breach detection
- Using the Sysinternals tools to detect breaches
- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution
- 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
- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging
- Overview of Advanced Threat Analytics
- Understanding OMS
- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs
- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Planning and implementing encryption
- Planning and implementing BitLocker
- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)
- Understanding Windows Firewall
- Software-defined distributed firewalls
- 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
- Overview of WSUS
- Deploying updates by using WSUS

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

- Configuring security options
- Configuring restrictred groups
- Delegating privileges
- Creating and managing group managed service accounts (MSAs)
- Configuring the Credential Guard feature

- Describe how to detect a breach by using the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.
- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

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

This module explains the Microsoft Advanced Threat Analytics tool and the Microsoft Operations Management suite (OMS), and details how you can use them to monitor and analyse the security of a Windows Server deployment.

Lab : Implementing DAC

- Preparing DAC
- Implementing DAC

After completing this module, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.
- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

Module 12: Using firewalls to control network traffic flow

- Locating problematic accounts

Lab: Configuring and deploying LAPs

- Installing local administrator password solution (LAPs)
- Configuring LAPs
- Deploying LAPs

After completing this module, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.
- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

Module 3: Limiting administrator rights with Just Enough Administration

Lessons

- Overview of breach detection
- Using the Sysinternals tools to detect breaches
- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution
- 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
- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging
- Overview of Advanced Threat Analytics
- Understanding OMS
- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs
- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Planning and implementing encryption
- Planning and implementing BitLocker
- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)
- Understanding Windows Firewall
- Software-defined distributed firewalls
- 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
- Overview of WSUS
- Deploying updates by using WSUS

Lab : Advanced Threat Analytics and Operations Management Suite

- Using ATA and OMS
- Preparing and deploying ATA
- Preparing and deploying OMS

After completing this module, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.

This module explains the firewalls that are present on Windows Server.

Lessons

- Overview of breach detection
- Using the Sysinternals tools to detect breaches
- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution
- 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
- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging
- Overview of Advanced Threat Analytics
- Understanding OMS
- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs
- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Planning and implementing encryption
- Planning and implementing BitLocker
- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)
- Understanding Windows Firewall
- Software-defined distributed firewalls
- 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
- Overview of WSUS
- Deploying updates by using WSUS

Lab : Windows Firewall with Advanced Security

- Creating and testing inbound rules
- Creating and testing outbound rules

After completing this module, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using

Lessons

- Understanding JEA
- Configuring 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:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.
- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats

- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.
- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

Module 8: Securing your virtualization an infrastructure

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

Lessons

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

- the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.
- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

Module 13: Securing network traffic

This module explains how to secure network traffic and how to use Microsoft Message Analyzer, Server Message Block (SMB) encryption, and Domain Name System Security Extensions (DNSSEC).

Lessons

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

---

and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

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.

Lessons

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

Lab : Limiting administrator privileges by using Privileged Access Management

- Using a layered approach to security
- Exploring MIM
- Configuring a MIM web portal
- Configuring the Privileged Access feature
- Requesting privileged access

After completing this module, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.
- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.

- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution
- 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
- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging
- Overview of Advanced Threat Analytics
- Understanding OMS
- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs
- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Planning and implementing encryption
- Planning and implementing BitLocker
- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)
- Understanding Windows Firewall
- Software-defined distributed firewalls
- 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
- Overview of WSUS
- Deploying updates by using WSUS

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

- Deploying Guarded Fabric VMs with administrator-trusted attestation
- Deploying a shielded VM

After completing this module, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.

breaches
- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution
- 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
- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging
- Overview of Advanced Threat Analytics
- Understanding OMS
- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs
- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Planning and implementing encryption
- Planning and implementing BitLocker
- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)
- Understanding Windows Firewall
- Software-defined distributed firewalls
- 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
- Overview of WSUS
- Deploying updates by using WSUS

Lab : Connection security rules and securing DNS

- Creating and testing connection security rules
- Configuring and testing DNSSEC

Lab : Microsoft Message Analyzer and SMB encryption

- Using Microsoft Message Analyzer
- Configuring and verifying SMB encryption on SMB shares

After completing this module, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.

M20744 A
www.globalknowledge.co.uk
info@globalknowledge.co.uk
01189 123456

- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

Module 5: Mitigating malware and threats

This module explains how to configure the Windows Defender, AppLocker, and Device Guard features.

Lessons

- Overview of breach detection
- Using the Sysinternals tools to detect breaches
- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution
- 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
- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging
- Overview of Advanced Threat Analytics
- Understanding OMS
- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs
- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Planning and implementing encryption
- Planning and implementing BitLocker
- Introduction to FSRM

- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

Module 9: Securing application development and server-workload infrastructure

This module details the Security Compliance Manager, including how you can use it to configure, manage, and deploy baselines. Additionally, students will learn how to deploy and configure Nano Server, Microsoft Hyper-V, and Windows Server Containers.

Lessons

- Overview of breach detection
- Using the Sysinternals tools to detect breaches
- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers

- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.
- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

Module 14: Updating Windows Server

This module explains how to use Windows Server Update Services (WSUS) to deploy updates to Windows Servers and clients

Lessons

- Overview of breach detection
- Using the Sysinternals tools to detect breaches
- Understanding user rights
- Computer and service accounts

- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)
- Understanding Windows Firewall
- Software-defined distributed firewalls
- 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
- Overview of WSUS
- Deploying updates by using WSUS

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

- Configuring Windows Defender
- Configuring AppLocker
- Configuring and deploying Device Guard
- Deploying and using EMET

- Deploying a local administrator-password solution
- 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
- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging
- Overview of Advanced Threat Analytics
- Understanding OMS
- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs
- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Planning and implementing encryption
- Planning and implementing BitLocker
- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)
- Understanding Windows Firewall
- Software-defined distributed firewalls
- 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
- Overview of WSUS
- Deploying updates by using WSUS

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 Nano Server and containers

- Deploying, managing, and securing Nano Server
- Deploying, managing, and securing Windows Server containers
- Deploying, managing, and securing Hyper-V containers

After completing this module, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.

- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution
- 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
- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging
- Overview of Advanced Threat Analytics
- Understanding OMS
- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs
- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Planning and implementing encryption
- Planning and implementing BitLocker
- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)
- Understanding Windows Firewall
- Software-defined distributed firewalls
- 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
- Overview of WSUS
- Deploying updates by using WSUS

Lab : Implementing update management

- Implementing the WSUS server role
- Configuring update settings
- Approving and deploying an update by using WSUS
- Deploying Windows Defender definition updates by using WSUS

After completing this module, students will be able to:

- Describe breach detection.
- Describe how to detect a breach by using the Sysinternals tools.
- understand user rights.
- Describe computer and service accounts.
- Help protect credentials.
- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.

- Understand privileged-access workstations and jump servers.
- Understand how to use a local administrator-password solution.
- Understand JEA.
- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

Module 10: Protecting data with encryption

This module explains how to configure Encrypting File System (EFS) and BitLocker drive encryption to protect data at rest.

Lessons

- Overview of breach detection
- Using the Sysinternals tools to detect breaches
- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access

- Configure and deploy JEA.
- Understand enhanced security administrative environment forests.
- Understand MIM.
- Understand how to implement JIT and Privileged Access Management by using MIM.
- Configure and manage Windows Defender.
- Use Software Restricting Policies and AppLocker.
- Configure and use Device Guard.
- Use and deploy the EMET.
- Understanding auditing.
- Understand advanced auditing.
- Audit and log Windows PowerShell.
- Understand Advanced Threat Analytics.
- Understand OMS.
- Understand Guarded Fabric VMs.
- Understand shielded and encryption-supported VMs.
- Understand Security Compliance Manager.
- Describe Nano Server.
- Understand containers.
- Plan and implement encryption.
- Plan and implement BitLocker.
- Understand FSRM.
- Implement classification management and file-management tasks.
- Understand DAC.
- Describe Windows Firewall.
- Understand software-defined distributed firewalls.
- Understand network-related security threats and connection security rules.
- Configure advanced DNS settings.
- Examine network traffic with Microsoft Message Analyzer.
- Secure SMB traffic, and analyze SMB traffic.
- Understand WSUS.
- Deploy updates with WSUS.

- workstations and jump servers
- Deploying a local administrator-password solution
- 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
- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging
- Overview of Advanced Threat Analytics
- Understanding OMS
- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs
- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers
- Planning and implementing encryption
- Planning and implementing BitLocker
- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)
- Understanding Windows Firewall
- Software-defined distributed firewalls
- 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
- Overview of WSUS
- Deploying updates by using WSUS

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.co.uk

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK