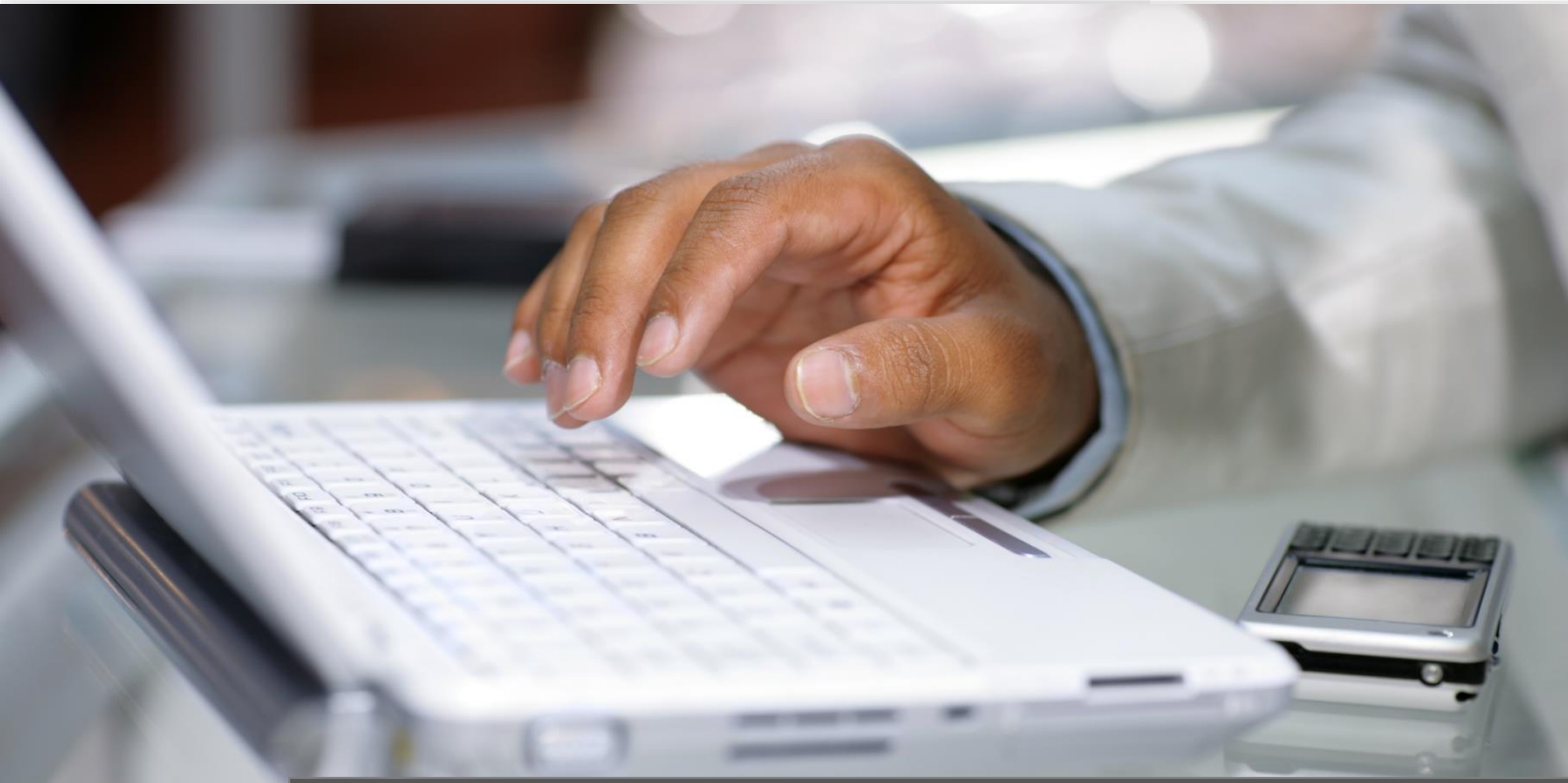
Securing Windows Server 2016

Online-Training | Examen 744



Ausbildungsinhalte

ITKservice

Securing Windows Server 2016

Mit dem Bestehen des Wahlexamens 744 erlangen Sie als MCSA 2012, MCSA 2016, *MCSA Cloud Platform* oder *MCSA Linux on Azure* den Titel *Microsoft Certified Solutions Expert (MCSE) Cloud Platform and Infrastructure*.

Ausbildungspfad | Microsoft Certified Solutions Expert (MCSE) Cloud Platform and Infrastructure

Die Zertifizierung zum Microsoft Certified Solutions Expert (MCSE): Cloud Platform and Infrastructure bestätigt, dass Sie über die erforderlichen Fähigkeiten verfügen, ein hocheffizientes und modernes Rechenzentrum zu betreiben. Dafür besitzen Sie Fachkenntnisse in den Bereichen Cloud-Technologie Identitätsmanagement, Systemmanagement, Virtualisierung, Speicher und Netzwerken.

	Online-Training	Dauer	Examen
	Securing Windows Server 2016	18 UE	744

Das Seminar beinhaltet die Verbesserung der Sicherheit von IT-Infrastrukturen, angefangen mit der Bedeutung der Erkenntnis, dass Netzwerkverstöße bereits stattgefunden haben, bis zu den Schutzmöglichkeiten für administrative Rechte, um sicherzustellen, dass Administratoren nur die Aufgaben durchführen können, zu denen sie berechtigt sind.

	Unterrichtseinheit	UE 01	744

Securing Windows Server 2016
- ✓ Allgemeine Vorstellung des Kurses und der Inhalte
- ✓ Einführung: Was ist generell IT Security?
- ✓ Vorstellung der Module
- ✓ Hinweise zur Prüfung
- ✓ Klärung erster grundlegender Begriffe

Securing Windows Server 2016
- ✓ Was versteht man unter Angriffen?
- ✓ Wichtigkeit der Dokumentation eines Systems
- ✓ Mögliche Gefahren
- ✓ Kurzer Abriss über sysinternaltools

	Unterrichtseinheit	UE 02	744

Angriffe, Entdecken von Sicherheitslücken und Verwendung der Sysinternals-Tools
- ✓ Was sind Angriffe?
- ✓ Unterscheidung: Angriffe auf ein einzelnes System, Angriffe auf Anwendungen, Angriffe auf die Infrastruktur
- ✓ Sich über Angriffe bewusstwerden
- ✓ Erkennen potentielle Gefahren für ein System
- ✓ Grundvoraussetzung der Dokumentation
- ✓ Angriffe auf physische oder virtuelle Systeme
- ✓ Unternehmensbewusstsein für Angriffe: Sicherheit geht alle an

Angriffe, Entdecken von Sicherheitslücken und Verwendung der Sysinternals-Tools
- ✓ Ziele der Angreifer
- ✓ Verschiedene Verfahren bei Angriffen
- ✓ Malware, Viren, Trojaner, Phishing, Social Engineering
- ✓ Bewertung von Informationen
- ✓ Compliance in Anwendungen
- ✓ Verantwortlichkeiten beim Thema Sicherheit
- ✓ Was sind Sicherheitslücken und wodurch entstehen sie?
- ✓ Was macht ein Sicherheitskonzept aus?

Unterrichtseinheit	UE 03	744

Systeme vor Angriffen schützen und Angriffe erkennen

- ✓ Was ist die "Attack timeline"?
- ✓ Wie bereitet sich ein Angreifer auf mögliche Angriffe vor?
- ✓ Gefahr des Social Engineering
- ✓ Persistent Threats
- ✓ Einsatzzweck von Intrusion Detection Systems
- ✓ Grenzen von IDS
- ✓ Schützenswerte Ressourcen

Systeme vor Angriffen schützen und Angriffe erkennen

- ✓ Response Strategies
- ✓ Was ist Compliance und wie tragen sie zum Schutz von Informationen bei?
- ✓ Sicherheitslücken/Einbrüche erkennen
- ✓ EventLogs
- ✓ Scheduled tasks
- ✓ Benutzer und Gruppen
- ✓ Die sysinternal tools

Unterrichtseinheit	UE 04	744

Systeme vor Angriffen schützen und Angriffe erkennen

- ✓ Einführung in PowerShell
- ✓ Notwendigkeit der PowerShell
- ✓ PowerShell auf Windows Server 2016
- ✓ PowerShell Versionen
- ✓ Cmdlets
- ✓ Einbinden von Modulen
- ✓ Das ActiveDirectory Modul

Systeme vor Angriffen schützen und Angriffe erkennen

- ✓ Select-Object
- ✓ Subshells
- ✓ Übergabe an andere Cmdlets
- ✓ Property und ExpandProperty
- ✓ Get-Help
- ✓ Formatierte Ausgabe

Unterrichtseinheit	UE 05	744

- ✓ Benutzer und Privilegien
- ✓ additive und subtraktive Systeme
- ✓ Principle of least privilege
- ✓ Benutzerrechte per GPO
- ✓ Account-security options
- ✓ Kennworteinstellungen
- ✓ Vergleich on Premise/azure
- ✓ Account policy settings
- ✓ Delegation von Rechten
- ✓ Computer und ServiceAccounts
- ✓ Built-in accounts
- ✓ Credentials

Unterrichtseinheit	UE 06	744

- ✓ Privileged Access Management und administrative Forests Zusammenfassung
- ✓ Optimierung und Absicherung von Dateisystemen
- ✓ File Server Ressource Manager
- ✓ Funktionalitäten Quota und File Screening
- ✓ Was ist Klassifizierung von Dateien?
- ✓ Problematik Dateiendungen
- ✓ Einführung in Dynamic Access Control und Kontext zu Claims
- ✓ Claims und Identities
- ✓ Verwaltung über Domaingrenzen hinweg

Unterrichtseinheit	UE 07	744

Absichern von Anwendungsumgebungen

- ✓ Problem: Reichweite und Eingriffe von Anwendungen ins Betriebssystem
- ✓ Gefahren unsicherer Anwendungen: übergreifende Prozesse, erhöhte Rechte, Verlust von Daten etc.
- ✓ Ziel: Absichern der Anwendungsumgebung
- ✓ Das Security Compliance Toolkit

Absichern von Anwendungsumgebungen

- ✓ Verfügbare Tools im SCT
- ✓ Baselines für Windows Server 2016
- ✓ Was sind Container?
- ✓ Entwicklung von Applications nach Apps
- ✓ Besonderheiten von Apps
- ✓ Apps und Container

Unterrichtseinheit	UE 08	744

- ✓ AppV und Med-V als Clientvirtualisierung von Anwendungen
- ✓ Abgrenzung der beiden Verfahren
- ✓ Kernel und User Modes bei Containern
- ✓ Wie arbeiten Windows Container?
- ✓ Wie arbeiten Hyper V Container?
- ✓ Abgrenzung Windows Container und Hyper V Container?
- ✓ Was ist docker?
- ✓ Beschreibung der Vorgehensweise bei docker
- ✓ Szenarien für den Einsatz von Containern
- ✓ Anbindung an Azure

Unterrichtseinheit	UE 09	744

Data Encryption

- ✓ Abgrenzung Absicherung von Anwendung/Anwendungsdaten
- ✓ Wo können Anwendungsdaten vorkommen?
- ✓ Besonderheit: temporäre Dateien durch Download oder Work Folders
- ✓ EFS als Lösung auf File-Ebene
- ✓ Wie arbeitet EFS?
- ✓ Transparentes Verfahren

Data Encryption

- ✓ EFS und Dateisysteme
- ✓ EFS und Zertifikate
- ✓ Problem bei self signing certificates
- ✓ Recovery Agents bei EFS
- ✓ TroubleShooting bei EFS
- ✓ EFS Gültigkeitsbereiche
- ✓ Alternativen bei beweglichen Daten

Unterrichtseinheit	UE 10	744

- ✓ Mitigating Malware & Threads
- ✓ Was ist Malware?
- ✓ Welche Arten von Malware gibt es?
- ✓ Sensibilisierung der Benutzer
- ✓ Der Windows Defender
- ✓ Das Defender Security Center
- ✓ Zusammenarbeit mit anderen Produkten
- ✓ Defender Antivirus
- ✓ Windows Defender Application Guard
- ✓ Defender Smart Screen
- ✓ Besonderheiten bei Exploits

Unterrichtseinheit	UE 11	744

- ✓ Gefahren durch Software
  - ✓ Zu hohe Rechte
  - ✓ Eingriffe in OS-Prozesse
  - ✓ Eingriffe in andere Prozesse
- ✓ Software einschränken
- ✓ Software Restriction Policies
- ✓ AppLocker
- ✓ AppLocker Rules
- ✓ Das Defender Device Guard Feature
- ✓ Device Guard Policies
- ✓ Code integrity File Rules
- ✓ CFG

Unterrichtseinheit	UE 12	744

- ✓ Analyzing activity with advanced auditing and log analytics
- ✓ Overview of auditing
- ✓ Audit Policies
- ✓ Audit settings on files and folders
- ✓ Considerations for audit settings
- ✓ Events in the security log
- ✓ Advanced auditing
- ✓ Advanced policy configuration
- ✓ Expression-based audit policies
- ✓ Event log forwarding
- ✓ Audit collection services

Unterrichtseinheit	UE 13	744

- ✓ Audit Policies
- ✓ Audit Policies für Dateien und Ordner
- ✓ Events im security log
- ✓ Advanced audit policy configuration
- ✓ Verschiedene Policy Settings im Detail
- ✓ Auditing und Logging via PowerShell
- ✓ Vorstellung einiger PowerShell Cmdlets zur Verwaltung der Ereignisanzeige
- ✓ PowerShell Transaction Logging
- ✓ PowerShell Module Logging
- ✓ PowerShell ScriptBlock Logging

Unterrichtseinheit	UE 14	744

Bereitstellung und Konfiguration von Microsoft Advanced Threat Analytics (ATA) und Operations Management Suite (OMS)

- ✓ Advanced Persistent Threats
- ✓ Intrusion Detection vs. Intrusion Prevention
- ✓ ATA für OnPremise Systeme
- ✓ ATA Installationskomponenten
- ✓ Einbruchserkennung durch Signaturen
- ✓ Einbruchserkennung durch Training

Bereitstellung und Konfiguration von Microsoft Advanced Threat Analytics (ATA) und Operations Management Suite (OMS)

- ✓ Training durch Benutzerverhalten
- ✓ Funktionsweise von ATA
- ✓ Installationsvorrausetzungen für ATA
- ✓ Installation von ATA
- ✓ Abgrenzung zur Operations Management Suite für hybride Systeme

Unterrichtseinheit	UE 15	744

- ✓ Einbruchserkennung durch Training
- ✓ Training durch Benutzerverhalten
- ✓ Funktionsweise von ATA
- ✓ Installationsvorrausetzungen für ATA
- ✓ Installation von ATA
- ✓ Abgrenzung zur Operations Management Suite für hybride Systeme
- ✓ Azure Backup Komponenten
- ✓ Security and Compliance
- ✓ Visualisierungen und Big Data Analysen
- ✓ Azure Security Center
- ✓ Abgrenzung zur Microsoft Operations Managenent Suite Security policies Just in Time VM Access

Unterrichtseinheit	UE 16	744

- ✓ Network related security threats
- ✓ Common network related security threats
- ✓ DDos Attacken
- ✓ Malware
- ✓ Viren, Würmer, Trojanische Pferde
- ✓ Spyware und adware
- ✓ Man in the middle
- ✓ Gefahr von Bot-Netzwerken
- ✓ Interesse am Gewinnen von User-Daten und User-Verhalten
- ✓ Problematik neuerer Komponenten im Netzwerk
- ✓ Problematik des BYOD
- ✓ Problematik der Entdeckung
- ✓ Der Faktor Mensch bzw. der Faktor Anwender

Unterrichtseinheit	UE 17	744

- ✓ Firewall Types
- ✓ Application-layer gateway
- ✓ Circuit-level gateway
- ✓ Packet filter
- ✓ Stateful multilayer inspection
- ✓ Well-known ports
- ✓ Windows Firewall with Advanced Security
- ✓ Network location profiles
- ✓ Windows Firewall properties
- ✓ Windows Firewall with Advanced Security rules
- ✓ Inbound Rules
- ✓ Outbound Rules
- ✓ Additional configuration options
- ✓ Deploying firewall rules

Unterrichtseinheit	UE 18	744

- ✓ Securing network traffic
- ✓ Configuring advanced DNS settings
- ✓ DNS Security
- ✓ DNSSec
- ✓ NRPT
- ✓ DNS Policies
- ✓ RRL
- ✓ DANE

Weitere wichtige Informationen

Optimale Prüfungsvorbereitung

Für die optimale Vorbereitung auf das Microsoft-Examen, empfehlen wir die IT-Prüfungsvorbereitungs-Plattform CertBase, die Sie unter www.CertBase.de aufrufen können. In diesem Portal werden Fragen bereitgestellt, die den Original Microsoft Prüfungen gleichen und mit deren Hilfe Sie Ihre Chancen auf ein erfolgreiches Bestehen der gewünschten Prüfung deutlich steigern.

Microsoft Test- und Demoumgebungen

Unter der Adresse www.mycontoso.de finden Sie eine Auswahl an Werkzeugen zur Demonstration aktueller Microsoft-Produkte und Services. Diese vorkonfigurierten Demoumgebungen aus der Microsoft Demonstration Plattform eignen sich auch sehr gut für administrative Übungszwecke.

Sie haben Fragen oder Anregungen?

Falls Sie Fragen, Wünsche oder Anregungen zu dieser oder zu anderen Ausbildungen haben, stehen wir Ihnen montags bis donnerstags in der Zeit von 08:00 – 17:00 Uhr und freitags von 08:00 – 13:00 Uhr sehr gerne zur Verfügung.

Sie erreichen uns unter:

Telefon: 09526 95 000 60
E-Mail: info@ITKservice.NET

Ihre Ansprechpartner für das ITKwebcollege.ADMIN

Christoph Holzheid
Anne Hirschlein
Sylvia Sonntag
Thomas Wölfel

Copyrights und Vertragsbedingungen

Kontaktdaten | Impressum

ITKservice GmbH & Co. KG
Fuchsstädter Weg 2
97491 Aidhausen

Telefon: 09526 95 000 60
Telefax: 09526 95 000 63

www: ITKservice.NET
E-Mail: info@ITKservice.NET

Sitz der Gesellschaft: Aidhausen | Amtsgericht Bamberg, HRA 11009, Ust-Id: DE 262 344 410 | Vertreten durch: Thomas Wölfel (GF).
Bildnachweise: Alle in diesem Dokument dargestellten Bilder wurden von der ITKservice GmbH & Co. KG bei ccvision.de lizensiert.

Redaktion: ITKservice GmbH & Co. KG