Email: info@smartfuture.tn Téléphone : (+216) 70 100 500

Sécurisation Windows Server 2016

2021

5 jours

+ 20 ANNÉES d'expériences à votre service

Smartfuture

FORMATION

Windows®

Smartfuture
Business Education Training solutions

www.smartfuture.tn

in/ smartfuture.officiel

Adresse : 47 Av. Mouaouia IBN ABI SOFIANE, El MENZAH VI, 2091 ARIANA, TUNISIE

Sécurisation Windows Server 2016

COURSE SF22744

Durée:

5 jours

Langue

Francais

Formations dirigées par un instructeur

Objectif

Ce cours de cinq jours animé par un instructeur apprend aux professionnels des technologies de l'information à améliorer la sécurité de l'infrastructure informatique dont ils assurent l'administration. Il commence par mettre en avant l'importance de supposer que des violations du réseau ont déjà eu lieu, puis montre comment protéger les informations d'identification et les droits d'administration pour veiller à ce que les administrateurs puissent effectuer uniquement les tâches qu'ils doivent effectuer, quand ils doivent les effectuer.

Profil population cible

Ce cours convient aux professionnels des technologies de l'information qui doivent administrer les réseaux Windows Server 2016 en garantissant leur sécurité. Ces professionnels travaillent généralement avec des réseaux configurés comme des environnements Windows Server basés sur un domaine avec un accès géré à Internet et aux services Internet.Ce cours est également utile aux stagiaires qui recherchent une certification avec l'examen 70-744 Sécurisation Windows Server.

Examen de certification

Préparation pour examen : 70-744

PROGRAMME

Prérequis :

Les stagiaires doivent avoir au moins deux ans d'expérience dans le domaine des technologies de l'information et avoir:
Suivi les cours 740, 741 et 742, ou équivalent.
Une connaissance solide et pratique des bases de la gestion réseau, notamment TCP/IP, le protocole UDP et DNS (Domain Name System).
Une connaissance solide et pratique des principes AD DS (Active Directory Domain Services).
Une connaissance solide et pratique des bases de la virtualisation Microsoft Hyper-V.
Une connaissance des principes de sécurité Windows Server.

Plan du cours

Module 1

Attaques, détection de violations et outils Sysinternals

Dans ce module, les stagiaires vont découvrir la détection de violations, les types d'attaques et les vecteurs, la cybercriminalité et comment analyser l'activité du système en utilisant la suite d'outils Sysinternals.

Leçons

- Identification des types d'attaques
- Exploration des outils Sysinternals
- À la fin de ce cours, les stagiaires seront à même de:
- Décrire la détection de violations
- Décrire comment détecter une violation en utilisant les outils Sysinternals

PROGRAME

Module 2

Protection des informations d'identification et de l'accès privilégié

Ce module explique comment configurer les droits d'utilisateur et les options de sécurité, protéger les informations d'identification à l'aide de Credential Guard, implémenter des stations de travail à accès privilégié, puis gérer et déployer une solution de mots de passe des administrateurs locaux pour pouvoir gérer les mots de passe des comptes des administrateurs locaux.

Leçons

- Comprendre les droits d'utilisateur
- Décrire les comptes d'ordinateur et de service
- Contribuer à la protection des informations d'identification
- Comprendre les stations de travail à accès privilégié et les serveurs de rebond
- Comprendre comment utiliser une solution de mots de passe d'administrateurs locaux

Module 3

Limitation des droits d'administrateur avec JEA

Ce module explique comment déployer et configurer une administration JEA (Just Enough Administration).

Leçons

- Création d'un fichier de fonctionnalité de rôle
- Création d'un fichier de configuration de session
- Création d'un point de terminaison JEA
- Connexion et test d'un point de terminaison JEA
- Déploiement d'une configuration JEA sur un autre ordinateur

PROGRAMME

Module 4

Gestion de l'accès privilégié et forêts administratives

Ce module explique les concepts suivants : forêts ESAE (Enhanced Security Administrative Environment), MIM (Microsoft Identity Manager), administration JIT (Just In Time) ou Privileged Access Management.

Leçons

- Comprendre les forêts ESAE
- Comprendre MIM
- Comprendre l'administration JIT et PAM

Module 5

Réduction des logiciels malveillants et des menaces

Ce module explique comment configurer les fonctionnalités Windows Defender, AppLocker et Device Guard.

Leçons

- Configurer et gérer Windows Defender
- Limiter les logiciels
- Configurer et utiliser la fonctionnalité Device Guard
- Utiliser et déployer le kit EMET

PROGRAME

Module 6

Analyse de l'activité avec audit avancé et analytique des journaux

Ce module explique comment utiliser un audit avancé et des transcriptions Windows PowerShell.

Leçons

- Configuration de l'audit de l'accès au système de fichiers
- Audit des connexions au domaine
- Gestion de la configuration d'une stratégie d'audit avancé
- Journalisation et audit de Windows PowerShell

Module 7

Déploiement et configuration d'Advanced Threat Analytics et de Microsoft Operations Management Suite

Ce module décrit l'outil Microsoft Advanced Threat Analytics et Microsoft Operations Management suite (OMS), puis explique en détail comment les utiliser pour surveiller et analyser la sécurité d'un déploiement Windows Server.

Leçons

- Préparation et déploiement d'ATA
- Préparation et déploiement de Microsoft Operations Management Suite
- À la fin de ce module, les stagiaires seront à même de:
- Déployer et configurer ATA
- Déployer et configurer Microsoft Operations Management Suite

PROGRAMME

Module 8

Sécuriser l'infrastructure de virtualisation

Ce module explique comment configurer des machines virtuelles d'infrastructure protégée et décrit notamment la configuration requise des machines virtuelles dotées d'une protection maximale et qui prennent en charge le chiffrement.

Leçons

- Déploiement d'une infrastructure protégée avec attestation approuvée par l'administrateur
- Déploiement d'une machine virtuelle dotée d'une protection maximale
- Comprendre les machines virtuelles d'infrastructure protégée
- Comprendre les machines virtuelles dotées d'une protection maximale avec prise en charge du chiffrement

Module 9

Sécurisation du développement d'applications et d'une infrastructure de charge utile de serveur

Ce module décrit Security Compliance Manager, notamment comment l'utiliser pour configurer, gérer et déployer des bases de référence. De plus, les stagiaires apprendront à déployer et à configurer Nano Server, Microsoft Hyper-V et les conteneurs Windows Server.

Leçons

- Comprendre SCM
- Décrire Nano Server
- Comprendre les conteneurs.

PROGRAMME

Module 10

Planification et protection des données

Ce module explique comment configurer le système de fichiers EFS (Encrypting File System) et le chiffrement de lecteur BitLocker pour protéger les données au repos.

Leçons

- Chiffrement et récupération de l'accès aux fichiers chiffrés
- Utilisation de BitLocker pour protéger les données
- À la fin de ce module, les stagiaires seront à même de:
- Planifier et implémenter le chiffrement
- Planifier et implémenter BitLocker

Module 11

Optimisation et sécurisation des services de fichiers

Ce module explique comment optimiser les services de fichiers en configurant les Outils de gestion de ressources pour serveur de fichiers (FSRM) et le système de fichiers DFS. Les stagiaires apprendront à protéger les données d'un appareil en utilisant le chiffrement ou BitLocker. Ils apprendront aussi à gérer l'accès aux fichiers partagés en configurant le Contrôle d'accès dynamique (DAC).

Leçons

- Comprendre la gestion de ressources pour serveur de fichiers
- Implémenter les tâches de gestion de classification et de gestion de fichiers
- Comprendre le Contrôle d'accès dynamique

PROGRAMME

Module 12

Sécurisation du trafic réseau avec des pare-feu et le chiffrement

Ce module décrit les pare-feu présents dans Windows Server.

Leçons

- Comprendre les menaces de sécurité associées au réseau
- Comprendre le Pare-feu Windows avec fonctions avancées de sécurité
- Configurer IPsec Comprendre le pare-feu de centre de données

Module 13

Sécurisation du trafic réseau

Ce module explique comment sécuriser le trafic réseau et utiliser Microsoft Message Analyzer, le chiffrement SMB (Server Message Block) et les extensions de sécurité DNS (DNSSEC).

Leçons

- Installation et utilisation de Message Analyzer
- Configuration et vérification du chiffrement SMB sur les partages SMB
- Configurer les paramètres DNS avancés
- Examiner le trafic réseau avec Message Analyzer
- Sécuriser le trafic SMB et l'analyser

PROGRAMME

Module 14

Mise à jour de Windows Server

Ce module explique comment utiliser WSUS (Windows Server Update Services) pour déployer des mises à jour sur les serveurs et clients Windows.

Leçons

- Implémentation du rôle serveur WSUS
- Configuration des paramètres de mise à jour
- Approbation et déploiement d'une mise à jour à l'aide de WSUS
- Comprendre WSUS
- Déployer des mises à jour avec WSUS

PROGRAME

Smartfuture

Make it
happen...

« we do it with quality »

/smartfuture.officiel