Microtel
Training institute

SÉCURISATION WINDOWS SERVER 2016

CURSUS:
MICROSOFT

CODE DE LA FORMATION:
MS-SYS-22744

ÉDITEUR OU CONSTRUCTEUR:
MICROSOFT

DURÉE:
5 JOURS

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.
Ce cours explique en détail comment réduire les menaces de logiciels malveillants, identifier les problèmes de sécurité avec un audit et la fonctionnalité Advanced Threat Analysis de Windows Server 2016, sécuriser votre plateforme de virtualisation et utiliser les nouvelles options de déploiement, comme Nano Server et les conteneurs, pour améliorer la sécurité. Il explique aussi comment protéger l'accès aux fichiers en utilisant le chiffrement et le contrôle d'accès dynamique, puis comment améliorer la sécurité de votre réseau.

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.

PUBLIC:

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.

OBJECTIFS:

À la fin de ce cours, les stagiaires seront à même de :

- Sécuriser Windows Server
- Sécuriser le développement d'applications et une infrastructure de charge utile de serveur
- Gérer les bases de référence de la sécurité
- Configurer et gérer une administration JEA et JIT

- Gérer la sécurité des données
- Configurer le Pare-feu Windows et un pare-feu distribué défini par le logiciel
- Sécuriser le trafic réseau
- Sécuriser votre infrastructure de virtualisation
- Gérer les logiciels malveillants et les menaces
- Configurer un audit avancé
- Gérer les mises à jour logicielles
- Gérer les menaces avec ATA (Advanced Threat Analytics) et Microsoft Operations Management Suite (OMS)

CONTENU:

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

- Présentation des attaques
- Détection des violations de la sécurité
- Examen de l'activité avec l'outil Sysinternals

Atelier : Détection de violations de base et stratégies de réponse aux incidents

- 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.

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

- Présentation des droits d'utilisateur
- Comptes d'ordinateur et de service
- Protection des informations d'identification
- Stations de travail à accès privilégié et serveurs de rebond
- Solution de mots de passe des administrateur locaux

Atelier : Implémentation des droits d'utilisateur, des options de sécurité et des comptes de service administr

- Configuration des options de sécurité
- Configuration des groupes restreints
- Délégation de privilèges
- Création et gestion de comptes de service administrés de groupe
- Configuration de la fonctionnalité Credential Guard
- Localisation des comptes problématiques

Atelier : Configuration et déploiement des mots de passe d'administrateurs locaux

- Installation et configuration des mots de passe d'administrateurs locaux
- Déploiement et test des mots de passe d'administrateurs locaux

À la fin de ce module, les stagiaires seront à même de :

- 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

- Présentation d'une administration JEA
- Vérification et déploiement d'une administration JEA

Atelier : Limitation des privilèges administrateur avec JEA

- 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

À la fin de ce module, les stagiaires seront à même de :

Comprendre l'administration JEA

Vérifier et déployer une administration JEA

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

- Forêts ESAE
- Vue d'ensemble de Microsoft Identity Manager
- Vue d'ensemble de l'administration JIT et de PAM

Atelier : Limitation des privilèges administrateur avec PAM

- Approche hiérarchisée de la sécurité
- Configuration de relations d'approbation et de principaux fantômes
- Demande d'un accès privilégié
- Gestion des rôles PAM

À la fin de ce module, les stagiaires seront à même de :

- 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

- Configuration et gestion de Windows Defender
- Restriction des logiciels
- Configuration et utilisation de la fonctionnalité Device Guard
- Déploiement et utilisation du kit EMET

Atelier : Sécurisation des applications avec AppLocker, Windows Defender, Device Guard Rules et EMET

- Configuration de Windows Defender
- Configuration d'AppLocker
- Configuration de Device Guard
- Déploiement et utilisation du kit EMET

À la fin de ce module, les stagiaires seront à même de :

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

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

- Vue d'ensemble de l'audit
- Audit avancé
- Audit et journalisation de Windows PowerShell

Atelier : Configuration d'un audit avancé

- 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

À la fin de ce module, les stagiaires seront à même de :

- Comprendre l'audit
- Comprendre l'audit avancé
- Auditer et journaliser 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

- Déploiement et configuration d'ATA
- Déploiement et configuration de Microsoft Operations Management Suite

Atelier : Déploiement d'ATA et de Microsoft Operations Management Suite

- 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

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

- Infrastructure protégée
- Machines virtuelles dotées d'une protection maximale avec prise en charge du chiffrement

Atelier : Infrastructure protégée avec attestation approuvée par l'administrateur et machines virtuelles dotée

- Déploiement d'une infrastructure protégée avec attestation approuvée par l'administrateur
- Déploiement d'une machine virtuelle dotée d'une protection maximale

À la fin de ce module, les stagiaires seront à même de :

- 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

- Utilisation de SCM
- Introduction à Nano Server
- Présentation des conteneurs

Atelier : Utilisation de SCM

- Configuration d'une base de référence de la sécurité pour Windows Server 2016
- Déploiement d'une base de référence de la sécurité pour Windows Server 2016

Atelier : Déploiement et configuration de Nano Server

- Déploiement, gestion et sécurisation de Nano Server
- Déploiement, gestion et sécurisation des conteneurs Windows

À la fin de ce module, les stagiaires seront à même de :

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

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

- Planification et implémentation du chiffrement
- Planification et implémentation de BitLocker

Atelier : Protection des données avec le chiffrement et BitLocker

- 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

- Outils de gestion de ressources pour serveur de fichiers
- Implémentation des tâches de gestion de classification et de gestion de fichiers
- Contrôle d'accès dynamique

Atelier : Quotas et filtrage de fichiers

- Configuration des quotas Gestion de ressources pour serveur de fichiers
- Configuration du filtrage de fichiers et des rapports de stockage

Atelier : Implémentation du Contrôle d'accès dynamique

- Préparation à l'implémentation du Contrôle d'accès dynamique
- Implémentation du Contrôle d'accès dynamique
- Validation et correction du Contrôle d'accès dynamique

À la fin de ce module, les stagiaires seront à même de :

- 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

Module 12: Sécurisation du trafic réseau avec des pare-feu et le chiffrement

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

Leçons

- Présentation des menaces de sécurité associées au réseau
- Présentation du Pare-feu Windows avec fonctions avancées de sécurité
- Configuration d'IPsec
- Pare-feu de centre de données

Atelier : Configuration du Pare-feu Windows avec fonctions avancées de sécurité

- Création et test de règles entrantes
- Création et test de règles sortantes
- Création et test de règles de sécurité de connexion

À la fin de ce module, les stagiaires seront à même de :

- 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

- Configuration des paramètres DNS avancés
- Examen du trafic réseau avec Message Analyzer
- Sécurisation et analyse du trafic SMB

Atelier : Sécurisation de DNS

- Configuration et test de DNSSEC
- Configuration de stratégies DNS et de RRL

Atelier : Microsoft Message Analyzer et chiffrement SMB

- Installation et utilisation de Message Analyzer
- Configuration et vérification du chiffrement SMB sur les partages SMB

À la fin de ce module, les stagiaires seront à même de :

- Configurer les paramètres DNS avancés
- Examiner le trafic réseau avec Message Analyzer
- Sécuriser le trafic SMB et l'analyser

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

- Vue d'ensemble de WSUS
- Déploiement des mises à jour avec WSUS

Atelier : Implémentation d'une gestion de mises à jour

- 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

CERTIFICATION:

Ce cours prépare au passage de l'examen de certification 70-744 Sécurisation Windows Server.