Windows Server 2016 - Sécurisation de l'infrastructure

Référence : MS22744
Durée : 5 jours (35h)
Tarif : 2800 €
Date à planifier

Certification : Aucune
Code CPF Unique : Aucun - **Code Certif Info :** Aucun

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel.

Le formateur alterne entre méthode* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en œuvre sont :

- Ordinateurs Mac ou PC, connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

** ratio variable selon le cours suivi*

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

A l'issue de ce stage vous serez capable 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).

Public :

Professionnels IT souhaitant administrer des réseaux sous Windows Server 2016 en toute sécurité, avec un accès aux services Cloud.

Prérequis :

Avoir suivi les cours MS22740 "Windows Server 2016 - Installation, stockage et virtualisation", MS22741 "Windows Server 2016 - Mise en réseau" et MS22742 "Windows Server 2016 - Identité et accès aux données" ou posséder les connaissances équivalentes. Avoir une pratique solide des fondamentaux de la gestion réseau tels que TCP/IP, UDP (User Datagram Protocol), DNS (Domain Name System), Active Directory (AD DS) et d'Hyper-V. Comprendre également les principes de sécurité de Windows Server.

DATADOCKÉ

Les plus de la formation :

Le support de cours est en français.

Cette formation :

- bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.
- est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par ALYF

Programme

- **Attaques, détection de violations et outils Sysinternals**

Présentation des attaques

Détection des violations de la sécurité

Examen de l'activité avec l'outil Sysinternals

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

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

- **Limitation des droits d'administrateur avec JEA**

Présentation d'une administration JEA

Vérification et déploiement d'une administration JEA

- **Gestion de l'accès privilégié et forêts administratives**

Forêts ESAE

Vue d'ensemble de Microsoft Identity Manager

Vue d'ensemble de l'administration JIT et de PAM

- **Réduction des logiciels malveillants et des menaces**

Configuration et gestion de Windows Defender

Restriction des logiciels

Configuration et utilisation de la fonctionnalité Device Guard

Déploiement et utilisation du kit EMET

- **Analyse de l'activité avec audit avancé et Log Analytics**

Vue d'ensemble de l'audit

Audit avancé

Audit et journalisation de Windows PowerShell

- **Déploiement et configuration d'Advanced Threat Analytics et de Microsoft Operations Management Suite (OMS)**

Déploiement et configuration d'ATA

Déploiement et configuration d'OMS

- **Sécuriser l'infrastructure de virtualisation**

Infrastructure protégée

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

- **Sécurisation du développement d'applications et d'une infrastructure workload de serveur**

Utilisation de SCM

Introduction à Nano Server

Présentation des conteneurs

- **Planification et protection des données**

Planification et implémentation du chiffrement

Planification et implémentation de BitLocker

- **Optimisation et sécurisation des services de fichiers**

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

- **Sécurisation du trafic réseau avec des pare-feux et le chiffrement**

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

- **Sécurisation du trafic réseau**

Configuration des paramètres DNS avancés

Examen du trafic réseau avec Message Analyzer

Sécurisation et analyse du trafic SMB

- **Mise à jour de Windows Server**

Vue d'ensemble de WSUS

Déploiement des mises à jour avec WSUS

SUIVI DE L'EXECUTION ET EVALUATION DES RESULTATS

> Feuilles de présence
> Questions orales ou écrites(QCM)
> Mises en situation
> Formulaires d’évaluation de la formation
> Certificat de réalisation de l'action de formation

Dernière mise à jour le 02/02/2022