Votre partenaire formation depuis 20 ans

Windows Server 2016 – Assurer la sécurité de l'infrastructure

Référence **MS20744**
Durée **5 jours**
Prix **2725€ / HT**

Certification **non**
Eligible au CPF

Nos prochains cours

Le 18/02/2019, Le 13/05/2019, Le 08/07/2019, Le 07/10/2019, Le 02/12/2019

Modalité pédagogique

Cours dispensé en mode présentiel avec une alternance d'apports théoriques et méthodologiques, et de mises en situations pratiques

Objectifs :

- Être en mesure d'assurer la sécurité des systèmes Windows Server
- Comprendre comment assurer la sécurité des infrastructures de développement et de production
- Apprendre à configurer et mettre en oeuvre l'administration « Just In Time »

- Disposer des connaissances nécessaires pour assurer la sécurité des données
- Savoir configurer le pare-feu Windows et les pare-feu distribués
- Être capable de sécuriser le trafic réseau et de parer les attaques
- Apprendre à sécuriser l'infrastructure de virtualisation
- Prendre en compte les menaces liées aux logiciels malfaisants

Pré-requis

- Avoir suivi les formations « Installation de Windows Server 2016, gestion du stockage et de la virtualisation », « Les services réseaux Windows Server 2016 et « Gestion des identités avec Windows Server 2016 » ou connaissances équivalentes
- Posséder une solide expérience sur les réseaux (TCP/IP, UDP, DNS…), les principes AD DS, la virtualisation Hyper-V et la sécurité Windows Server

Programme

DÉTECTION DES INTRUSIONS AVEC LES OUTILS SYSINTERNALS

- Généralités
- Les outils Sysinternals

PROTECTION DES IDENTIFIANTS ET DES ACCÈS PRIVILÉGIÉS

- Droits utilisateur
- Comptes d'ordinateur et comptes de service
- Protection des identifiants

- Stations dédiées et serveurs intermédiaires
- Déploiement d'une solution de gestion des mots de passe d'administrateur local

LIMITATION DES DROITS D'ADMINISTRATION ET PRINCIPE DU PRIVILÈGE MINIMAL

- Description
- Implémentation et déploiement

GESTION DES ACCÈS PRIVILÉGIÉS ET FORÊTS ADMINISTRATIVES

- Le concept de forêt administrative
- Introduction à Microsoft Identity Manager
- Administration « Just In Time » et gestion des accès privilégiés avec Microsoft Identity Manager

ATTÉNUATION DES RISQUES LIÉS AUX LOGICIELS MALFAISANTS

- Configuration et gestion de Microsoft Defender
- Stratégies de restrictions logicielles et AppLocker
- Configuration et utilisation de Device Guard
- Utilisation et déploiement de Enhanced Mitigation Experience Toolkit

MÉTHODES D'ANALYSE ET D'AUDIT AVANCÉES POUR LA SURVEILLANCE DE L'ACTIVITÉ

- Introduction : l'audit système
- Stratégies d'audit avancées
- Audit et enregistrement des sessions PowerShell

ANALYSE DE L'ACTIVITÉ AVEC MICROSOFT ADVANCED THREAT ANALYTICS ET OPERATIONS MANAGEMENT SUITE

- Advanced Threat Analytics
- Présentation de OMS

SÉCURISATION DE L'INFRASTRUCTURE DE VIRTUALISATION

- Infrastructures protégées (Guarded Fabric)
- Machines virtuelles chiffrées (encryption-supported) et blindées (shielded)

SÉCURISATION DE L'INFRASTRUCTURE DE DÉVELOPPEMENT APPLICATIF ET DE PRODUCTION

- Security Compliance Manager
- Nano Server
- Containers

PROTECTION DES DONNÉES PAR CHIFFREMENT

- Planification et implémentation du chiffrement EFS (Encrypting File System)
- Planification et implémentation de BitLocker

LIMITATION DES ACCÈS AUX FICHIERS

- File Server Resource Manager (FSRM)
- Automatisation de la gestion et de la classification des fichiers
- Contrôle d'accès dynamique (Dynamic Access Control)

LIMITATION DES FLUX RÉSEAUX AU MOYEN DE PARE-FEU

- Le pare-feu Windows
- Pare-feu distribués

SÉCURISATION DU TRAFIC RÉSEAU

- Menaces liées au réseau et règles de sécurisation des connexions
- Paramétrage avancé de DNS
- Analyse du trafic réseau avec Microsoft Message Analyzer
- Sécurisation et analyse du trafic SMB

MISE À JOUR DE WINDOWS SERVER

- Présentation de WSUS
- Déploiement des mises à jour avec WSUS