Windows Server 2016

Assurer la sécurité

Objectifs du cours

Acquérir les connaissances et compétences pour améliorer la sécurité d'une infrastructure IT.

Public cible

Ingénieurs système et réseau.

Prérequis

- Avoir suivi les formations MS20740-Stockage et Virtualisation Windows Server 2016" ; MS20741- Les services réseaux Windows Server 2016" ; MS20742-Gestion des identités avec Windows Server 2016" ou posséder les connaissances et compétences équivalentes
- La compréhension des fondamentaux du réseau tels que TCP/IP, UDP, DNS, des principes de AD DS et des fondamentaux de la virtualisation avec Hyper-V est fondamentale
- Posséder également une bonne compréhension des principes de la sécurité dans Windows Server

Contenu de cours

Détecter des ruptures à l'aide des Sysinternals :

- Généralités
- Les outils Sysinternals

Protéger les informations d'identification et d'accès privilégié :

- 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

Limiter les droits d'administrateur avec JEA (Just Enough Administration) :

- Description
- Implémentation et déploiement

Contenu de cours (suite)

Gérer l'accès privilégié 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

Limiter les malware et les menaces :

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

Analyser l'activité en utilisant la vérification avancée :

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

Analyser l'activité avec la fonctionnalité Microsoft Advanced Threat Analytics (ATA) et Operations Management Suite (OMS) :

- Advanced Threat Analytics
- Présentation de l'OMS

Sécuriser votre infrastructure virtualisée :

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

Assurer le développement d'applications et l'infrastructure de charge du serveur :

- Security Compliance Manager
- Nano Server
- Containers

Protéger les données avec cryptage :

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

Contenu de cours (suite)

Limiter l'accès aux fichiers et aux dossiers :

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

Contrôler les flux réseaux au moyen de pare-feu :

- Le pare-feu Windows
- Pare-feu distribués

Sécuriser le 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

Certification Microsoft Securing Windows Server 2016 :

- Cette formation prépare au passage de la certification Microsoft Securing Windows Server 2016 (70-744)

Durée

5 jours (8h30 – 12h00 et 13h30 – 17h00)

Tarifs

Formation Entreprise : *Sur demande*
Formation Multi-Entreprises : CHF 3'658.- (par pers.)

Remarques

Dans le cas de cours Entreprise, nous pouvons organiser un contenu sur mesure ou à la carte.

Les prix sont mentionnés hors TVA (7,7%) et en CHF (Francs suisses).

Les formations « Multi-Entreprises » ne s'ouvrent qu'à partir de 3 inscriptions.