Programme de formation

Windows Server 2016 : Assurer la sécurité l'infrastructure

5 jours - 35 heures	Code formation : ADHSYS0607

adhara.fr

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". 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.

Participants

Professionnels IT qui souhaitent administrer Windows Server 2016 avec un maximum de sécurité.

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 d'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.

Pédagogie

La pédagogie est basée sur le principe de la dynamique de groupe avec alternance d'apports théoriques, de phases de réflexion collectives et individuelles, d'exercices, d'études de cas et de mises en situations observées. Formation / Action participative et interactive : les participants sont acteurs de leur formation notamment lors des mises en situation car ils s'appuient sur leurs connaissances, les expériences et mettront en œuvre les nouveaux outils présentés au cours de la session.

Remarques

Certification

Profil de l'intervenant

Consultant-formateur expert. Suivi des compétences techniques et pédagogiques assuré par nos services.

Moyens techniques

Encadrement complet des stagiaires durant la formation. Espace d'accueil, configuration technique des salles et matériel pédagogique dédié pour les formations en centre. Remise d'une documentation pédagogique papier ou numérique à échéance de la formation.

Méthodes d'évaluation des acquis

Un contact téléphonique est systématiquement établi avec le stagiaire ou la personne chargée de son inscription afin de définir le positionnement. Si besoin, un questionnaire est adressé pour valider les prérequis en correspondance et obtenir toute précision nécessaire permettant l'adaptation de l'action. Durant la formation, des exercices individuels et collectifs sont proposés pour évaluer et valider les acquis du stagiaire. La feuille d'émargement signée par demi-journée ainsi que l'évaluation des acquis sont adressées avec la facture.

Programme

Programme de formation

Windows Server 2016 : Assurer la sécurité l'infrastructure

5 jours - 35 heures	Code formation : ADHSYS0607

adhara.fr

ATTAQUES : DÉTECTER LES « BRÈCHES » ET UTILISER LES OUTILS SYSINTERNALS

Comprendre les attaques.
Utiliser les outils Sysinternals pour détecter les « brèches ».
Examiner l'activité avec les outils Sysinternals.

PROTÉGER LES « CREDENTIALS » ET LES ACCÈS PRIVILÉGIÉS

Comprendre les droits utilisateurs.
Comptes d'ordinateurs et de service.
Protéger les « credentials »
Comprendre les stations de travail avec accès privilégiés et les serveurs Jump
Déployer une solution locale de mot de passe administrateur (LAPs)

RESTREINDRE LES DROITS D'ADMINISTRATION AVEC JEA (JUST ENOUGH ADMINISTRATION)

Comprendre JEA
Configurer et déployer JEA

GÉRER LES ACCÈS PRIVILÉGIÉS ET FORÊTS ADMINISTRATIVES

Comprendre les forêts ESAE (Enhanced Security Administrative Environment)
Vue d'ensemble de MIM
Vue d'ensemble de l'administration JIT et PAM

LIMITER LES MALWARES ET LES MENACES

Configurer et gérer Windows Defender
Utiliser les stratégies de restriction des logiciels (SRPs)
Configurer et utiliser Device Guard
Utiliser et déployer le toolkit Enhanced Mitigation Experience (EMET)

ANALYSER LES ACTIVITÉS VIA L'AUDIT AVANCÉ ET LES JOURNAUX D'ANALYSE

Vue d'ensemble de l'audit
Comprendre l'audit avancé
Configurer l'audit et la connexion Windows PowerShell

ANALYSER LES ACTIVITÉS AVEC LA FONCTIONNALITÉ MICROSOFT ADVANCED THREAT ANALYTICS (ATA) ET OPERATIONS MANAGEMENT SUITE (OMS)

Déployer et configurer Advanced Threat Analytics (ATA)
Déployer et configurer Operations Management Suite (OMS)

SÉCURISER L'INFRASTRUCTURE DE VIRTUALISATION

Machines virtuelles protégées
Utiliser Security Compliance Manager (SCM)
Introduction aux Nano servers
Comprendre les conteneurs

Windows Server 2016 : Assurer la sécurité l'infrastructure

5 jours - 35 heures | Code formation : ADHSYS0607

PLANIFIER ET PROTÉGER LES DONNÉES

Planifier et mettre en œuvre le cryptage
Planifier et mettre en œuvre BitLocker

OPTIMISER ET SÉCURISER LES SERVICES DE FICHIERS

Introduction à FSRM
Mettre en œuvre la gestion de la classification et les tâches liées à la gestion de fichiers
Comprendre DAC (Dynamic Access Control)

SÉCURISER LE TRAFIC RÉSEAU AVEC FIREWALL ET CRYPTAGE

Comprendre les menaces de sécurité liées au réseau
Comprendre ce qu'est Windows Firewall avec la sécurité avancée
Configurer IPSec
Firewall Data Center

SÉCURISER LE TRAFIC RÉSEAU

Menaces contre la sécurité du réseau et règles de sécurité pour la connexion
Configurer les paramètres avancés de DNS
Examiner le trafic réseau avec Microsoft Message Analyzer
Sécuriser et analyser le trafic SMB

METTRE À JOUR DE WINDOWS SERVER

Vue d'ensemble de WSUS
Déployer les mises à jour via WSUS