Windows Server 2016 : Assurer la sécurité

Référence : **MS20744** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 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.

PROFIL DES STAGIAIRES

• Professionnels IT qui souhaitent administrer Windows Server 2016.

OBJECTIFS

• Acquérir les connaissances et compétences pour améliorer la sécurité d'une infrastructure IT. • Apprendre à protéger les informations d'identification et les droits administratifs afin de s'assurer que les administrateurs ne peuvent exécuter que les tâches dont ils ont besoin, lorsqu'ils en ont besoin. • Comprendre comment vous pouvez atténuer les menaces de logiciels malveillants, identifier les problèmes de sécurité en utilisant l'audit et la fonctionnalité Advanced Threat Analysis dans Windows Server 2016, sécuriser votre plate-forme de virtualisation et utiliser de nouvelles options de déploiement, comme les Nano servers et les conteneurs. • Comprendre également comment vous pouvez contribuer à protéger l'accès aux fichiers en utilisant le cryptage et le contrôle d'accès dynamique et comment améliorer la sécurité de votre réseau.

CERTIFICATION PREPAREE

- Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Windows Server 2016

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

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 privilégies et les serveurs Jump

- Déployer une solution locale de mot de passe administrateur (LAPs)

Restreindre les droits administrateur avec JEA (Just Enough Administration)

- Comprendre JEA
- Configurer et déployer JEA

Gérer les accès privilégiés et les 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 malware 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

- Guarded Fabric
- Machines virtuelles protégées
- Utiliser Security Compliance Manager
- Introduction aux Nano servers
- Comprendre les conteneurs

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