Windows Server 2016 - Mise en œuvre de la sécurité

Référence : 19003-170424-1-WIN
Durée : 5 jours soit 35 heures

Filière : Systèmes

Population visée :
Ouvrier – Employé – Employé qualifié – Cadre – Cadre supérieur

Public concerné :
Toute personne souhaitant implémenter et administrer Windows Server 2016 en réseau de façon sécurisée.
Administrateurs travaillant dans des environnements de domaine Windows Server 2016 ayant accès à internet et aux services de cloud.
Professionnels souhaitant préparer la certification Microsoft 70-744.

PRÉ-REQUIS

- Expérience de la virtualisation avec Hyper-V.
- Expérience avancée sur Active Directory.
- Expérience avancée des réseaux.
- Avoir suivi les autres formations Windows Server 2016.

OBJECTIFS PEDAGOGIQUES

A l'issue de cette formation, l'apprenant sera capable de :

- Sécuriser un Windows Server 2016.
- Gérer la sécurité des données.
- Sécuriser le trafic réseau.
- Sécuriser une infrastructure virtualisée.
- Gérer les menaces et logiciels malveillants.
- Configurer de l'audit avancé.
- Gérer les mises à jour de Windows Server 2016.
- Gérer des lignes de référence en matière de sécurité.

OBJECTIFS OPERATIONNELS ET CONTENU DE LA FORMATION

Attaques, détection d'intrusions et les outils Sysinternals

- Comprendre les attaques
- Détecter les failles de sécurité
- Surveiller l'activité avec les outils S ysinternals

Protection de l'authentification et gestion des accès privilégiés

- Comprendre les droits utilisateurs
- Les comptes d'ordinateurs et les comptes de services
- Protéger l'authentification
- Stations de travail à accès privilégiés et serveurs de renvoi
- Local Administrator Password Solution (LAPS)

Limiter les droits administrateurs avec JEA (Just Enough Administration)

- Comprendre JEA
- Valider et déployer JEA

La gestion des accès privilégiés et des forêts administratives

- Les forêts à environnement de sécurité renforcée (ESAE)
- Vue d'ensemble du gestionnaire d'identité Microsoft
- Vue d'ensemble de l'administration juste à temps (JIT) et de PAM (Privileged Access Management)

Atténuer le risque des logiciels malveillants et des menaces

- Configurer et gérer Windows Defender
- Restreindre les logiciels
- Configurer et utiliser les fonctionnalités Device Guard
- Déployer et utiliser la trousse à outils EMET (Enhanced Mitigation Experience Toolkit)

Analyser l'activité avec les outils d'audit avancés et l'analyse des logs

- Vue d'ensemble de l'audit
- Audit avancé
- Audit et Logs avec Windows PowerShell

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

- Déployer et configurer ATA
- Déployer et configurer OMS

Sécuriser une infrastructure virtualisée

- Guarded Fabric
- Machine virtuelles chiffrées et blindées

Sécuriser le développement d'applications et les charges de travail des serveurs d'infrastructure

- Utiliser SCM (Security Compliance Manager)
- Introduction aux serveurs Nanos
- Comprendre les conteneurs

Gérer et protéger les données

- Implémenter et gérer le chiffrement
- Implémenter et gérer BitLocker

Optimiser les serveurs de fichiers

- Le gestionnaire de ressources de serveur de fichier
- Implémenter la classification et les tâches de gestion de fichiers
- Le contrôle d'accès dynamique

Contrôler les flux de trafic réseau avec les pare-feu

- Appréhender les fonctionnalités de sécurité avancées du pare-feu Windows
- Pare-feu de Datacenter

Sécuriser le trafic réseau

- Menaces relatives à la sécurité des réseaux et règles de connexion sécurisées
- Configurer les paramètres avancés du DNS
- Analyser le trafic réseau avec Microsoft Message Analyser
- Sécuriser et analyser le trafic SMB

Mettre à jour Windows Server

- Vue d'ensemble de WSUS (Windows Server Update Services)
- Déployer des mises à jour avec WSUS

Méthodes et moyens :

- Explications théoriques suivies de pratiques guidées puis mises en autonomie
- 1 vidéoprojecteur par salle
- Stage en mode « In Class » : 2 téléviseurs et 1 caméra HD par salle.
- 1 ordinateur par stagiaire

Méthodes d'évaluation des acquis :

- Exercices de synthèse et d'évaluation
- Evaluation de fin de stage

Support stagiaire :

- Support papier ou électronique (dématérialisé)
- Les exercices d'accompagnement peuvent être récupérés sur clef USB