Sécuriser Windows Server 2016

Durée: 5 Jours **Réf de cours: M20744** **Version: C**

Résumé:

Cette formation permet aux participants d'acquérir les connaissances et compétences pour améliorer la sécurité d'une infrastructure IT.
Ce cours commence par souligner l'importance de supposer que les brèches réseau ont déjà eu lieu, puis vous enseigne comment 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.
Ce cours explique en outre 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. Le cours explique 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.

Public visé:

La formation s'adresse aux professionnels IT qui souhaitent administrer Windows Server 2016.

Objectifs pédagogiques:

- Sécuriser Windows Server
- Protéger les informations d'identification et mettre en oeuvre les accès privilégiés
- Limiter les droits des administrateurs avec Just Enough
- Gérer les accès privilégiés
- Gérer les malware et les menaces
- Analyser les activités avec l'audit avancé et l'analyse des journaux
- Gérer les menaces via ATA (Advanced Threat Analytics) et OMS (Operations Management Suite)
- Configurer les machines virtuelles Guarded Fabric (VMs)
- Utiliser SCT (Security Compliance Toolkit) et les conteneurs pour améliorer la sécruité
- Planifier et protéger les données
- Optimiser et securiser les services de fichiers
- Sécuriser le trafic réseau avec les firewalls et le cryptage
- Sécuriser le trafic réseau avec DNSSEC et Message Analyzer

Pré-requis:

Avoir suivi les cours M20740, M20741 et M20742 ou posséder des connaissances 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:

Attaques, détection des « brèches » et utilisation des outils Sysinternals

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

Protection des « credentials » et des 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

Gestion des accès privilégiés et des forêts administratives

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

Limitation des malware et des 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)

Analyse des 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

Analyse des 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)

Sécurisation de l'infrastructure de virtualisation

- Guarded Fabric
- Machines virtuelles protégées

Sécurisation de l'infrastructure de virtualisation

- Utiliser Security Compliance Manager
- Introduction aux Nano servers
- Comprendre les conteneurs

Planification et protection des données

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

Optimisation et sécurisation des 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)

Sécurisation du 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

Sécurisation du 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 Windows Server

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

Méthodes pédagogiques :

Pour profiter pleinement du support électronique dès le 1er jour, nous invitons les participants à se munir d'un PC ou d'une tablette, qu'ils pourront connecter en WiFi dans nos locaux de Rueil, Lyon ou Lille.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

•Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.