WINDOWS SERVER 2016 : ASSURER LA SÉCURITÉ

CODE STAGE : MS20744

OBJECTIFS

code2utf('8211',0) Être en mesure dcode2utf('8217',0)assurer la sécurité des systèmes Windows Server
code2utf('8211',0) Comprendre comment assurer la sécurité des infrastructures de développement et de production
code2utf('8211',0) Apprendre à configurer et mettre en oeuvre lcode2utf('8217',0)administration code2utf('8220',0)Just In Timecode2utf('8221',0)
code2utf('8211',0) Disposer des connaissances nécessaires pour assurer la sécurité des données

DURÉE

5 jours

PUBLIC

code2utf('8211',0) Ingénieurs système et réseau

PRÉ-REQUIS

code2utf('8211',0) Avoir suivi les formations MS20740-Stockage et Virtualisation Windows Server 2016code2utf('8243',0) ; MS20741- Les services réseaux Windows Server 2016code2utf('8243',0) ; MS20742- Gestion des identités avec Windows Server 2016code2utf('8243',0) ou posséder les connaissances et compétences équivalentes
code2utf('8211',0) Posséder une solide expérience sur les réseaux (TCP/IP, UDP, DNScode2utf('8230',0)), les principes AD DS, la virtualisation Hyper-V et la sécurité Windows Server

PROGRAMME

Module 1 : Détection des intrusions avec les outils sysinternals
Généralités
Les outils Sysinternals

Module 2 : Protection des identifiants et des accès privilégiés
Droits utilisateur
Comptes dcode2utf('8217',0)ordinateur et comptes de service
Protection des identifiants

Stations dédiées et serveurs intermédiaires
Déploiement dcode2utf('8217',0)une solution de gestion des mots de passe dcode2utf('8217',0)administrateur local

Module 3 : Limitation des droits dcode2utf('8217',0)administration et principe du privilège minimal
Description
Implémentation et déploiement

Module 4 : Gestion des accès privilégiés et forêts administratives
Le concept de forêt administrative
Introduction à Microsoft Identity Manager
Administration code2utf('8220',0)Just In Timecode2utf('8221',0) et gestion des accès privilégiés avec Microsoft Identity Manager

Module 5 : Atténuation des risques liés aux logiciels malfaisants
Configuration et gestion de Microsoft Defender
Stratégies de restrictions logicielles et AppLocker
Configuration et utilisation de Device Guard
Utilisation et déploiement de Enhanced Mitigation Experience Toolkit

Module 6 : Méthodes dcode2utf('8217',0)analyse et dcode2utf('8217',0)audit avancées pour la surveillance de lcode2utf('8217',0)activité
Introduction : lcode2utf('8217',0)audit système
Stratégies dcode2utf('8217',0)audit avancées
Audit et enregistrement des sessions PowerShell

Module 7 : Analyse de lcode2utf('8217',0)activité avec Microsoft Advanced Threat Analytics et Operations Management suite
Advanced Threat Analytics
Présentation de OMS

Module 8 : Sécurisation de lcode2utf('8217',0)infrastructure de virtualisation
Infrastructures protégées (Guarded Fabric)
Machines virtuelles chiffrées (encryption-supported) et blindées (shielded)

Module 9 : Sécurisation de lcode2utf('8217',0)infrastructure de développement applicatif et de production

Security Compliance Manager
Nano Server
Containers

Module 10 : Protection des données par chiffrement
Planification et implémentation du chiffrement EFS (Encrypting File System)
Planification et implémentation de BitLocker

Module 11 : Limitation des accès aux fichiers
File Server Resource Manager (FSRM)
Automatisation de la gestion et de la classification des fichiers
Contrôle dcode2utf('8217',0)accès dynamique (Dynamic Access Control)

Module 12 : Limitation des flux réseaux au moyen de pare-feu
Le pare-feu Windows
Pare-feu distribués

Module 13 : Sécurisation du 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

Module 14 : Mise à jour de Windows Server
Présentation de WSUS
Déploiement des mises à jour avec WSUS