Formation Sécurité Windows Server 2016 – Assurer la sécurité de l'infrastructure

Code : WS11 **Durée** : 5 jours **Classe** : Présentiel / à distance

Public

- Ingénieurs système et réseau opérant dans des environnements Windows complexes, comportant notamment des accès Cloud et Internet

Prérequis

- Connaissances Windows Server et Active Directory
- Bases en réseau (TCP/IP, DNS, DHCP)
- Notions de virtualisation Hyper-V
- Expérience en administration système

Objectifs

- Sécuriser les systèmes Windows Server
- Protéger les accès et identifiants privilégiés
- Configurer le pare-feu et les politiques de sécurité
- Mettre en place des solutions de détection et d'audit

Programme détaillé

1- Détection des intrusions avec les outils Sysinternals

- Généralités
- Les outils Sysinternals

2- Protection des identifiants et des accès privilégiés

- Droits utilisateur
- Comptes d'ordinateur et comptes de service
- Protection des identifiants
- Stations dédiées et serveurs intermédiaires
- Déploiement d'une solution de gestion des mots de passe d'administrateur local

3- Limitation des droits d'administration et principe du privilège minimal

- Description
- Implémentation et déploiement

4- Gestion des accès privilégiés et forêts administratives Le concept de forêt administrative

- Introduction à Microsoft Identity Manager
- Administration "Just In Time" et gestion des accès privilégiés avec Microsoft Identity Manager

5- Atténuation des risques liés aux logiciels malveillants

- 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

6- Méthodes d'analyse et d'audit avancées pour la surveillance

- Introduction : l'audit système
- Stratégies d'audit avancées
- Audit et enregistrement des sessions PowerShell

7- Analyse de l'activité avec Microsoft Advanced Threat Analytics

- Advanced Threat Analytics
- Présentation de OMS

Formation Sécurité Windows Server 2016 – Assurer la sécurité de l'infrastructure

Code : WS11 **Durée** : 5 jours **Classe** : Présentiel / à distance

8- Curisation de l'infrastructure de virtualisation
- Infrastructures protégées (Guarded Fabric)
- Machines virtuelles chiffrées (encryption-supported) et blindées (shielded)

9- Sécurisation de l'infrastructure de développement applicatif
- Security Compliance Manager
- Nano Server
- Containers

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

11- Limitation des accès aux fichiers
- File Server Resource Manager (FSRM)
- Automatisation de la gestion et de la classification des fichiers
- Contrôle d'accès dynamique (Dynamic Access Control)

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

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

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