Programme de la formation

Sécuriser Windows Server 2016

Détection des intrusions avec les outils Sysinternals

- Généralités
- Les outils Sysinternals

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

Limitation des droits d'administration et principe du privilège minimal

- Description
- Implémentation et déploiement

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

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

Méthodes d'analyse et d'audit avancées pour la surveillance de l'activité

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

Analyse de l'activité avec Microsoft Advanced Threat Analytics et Operations Management Suite

- Advanced Threat Analytics
- Présentation de OMS

Sécurisation De L'infrastructure De Virtualisation

- Infrastructures protégées (Guarded Fabric)
- Machines virtuelles chiffrées (encryption-supported) et blindées (shielded)

Sécurisation de L'infrastructure de Développement applicatif et de production

- Security Compliance Manager
- Nano Server
- Containers

Protection des données par chiffrement

- Planification et implémentation du chiffrement EFS (Encrypting File System)
- Planification et implémentation de BitLocker

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)

Limitation des flux réseaux au moyen de pare-feu

- Le pare-feu Windows
- Pare-feu distribués

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

Mise à jour de Windows server

- Présentation de WSUS
- Déploiement des mises à jour avec WSUS