WINDOWS SERVER 2016

Sécuriser l'infrastructure avec Windows Server 2016

5 jours (35h00) | WS004 | Num form : form-23 | Perfectionnement / Avancé

INFORMATIQUE / INFRASTRUCTURE / WINDOWS SERVER 2016

À l'issue de ce stage vous serez capable de :

- configurer les machines virtuelles (VM) Guarded Fabric ;
- utilisez la boîte à outils de conformité à la sécurité (SCT) et les conteneurs pour améliorer la sécurité ;
- planifier et protéger des données utilisateurs ;
- optimiser et sécuriser les services de fichiers ;
- sécuriser le trafic réseau avec des règles du pare-feu et la cryptographie ;
- sécuriser le trafic réseau en utilisant le DNSSEC et l'analyseur de messages ;
- maitriser tous les aspects techniques liés à la sécurisation de Windows Serveur 2016.
- protéger des comptes utilisateurs ;
- mettre en place des postes de travail à accès privilégiés ;
- encadrer les droits des administrateurs avec Just Enough Administration ;
- comprendre et gérer des accès privilégiés dans le temps ;

Niveau requis :

- maîtriser les fondamentaux de Microsoft Hyper-V ;
- connaitre les principes de sécurisation d’un serveur Windows.
- avoir une bonne maîtrise des fondamentaux réseaux (TCP/IP, DNS, UDP) ;
- avoir une bonne connaissance du fonctionnement d'Active Directory Domain Services ;

Public concerné :

- Professionnels IT qui souhaitent administrer Windows Server 2016.
-
-

Programme :

Gérer la sécurité de Windows server 2016 par la détection des « brèches » et utilisation des outils Sysinternals

Vue d'ensemble de la détection des « brèches »
Utiliser les outils Sysinternals pour détecter les « brèches »

Gérer la sécurité de Windows server 2016 par la 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
Mettre en œuvre JIT et la gestion des accès privilégiés via MIM

Limitation des malware et des menaces sous Windows Server 2016

Configurer et gérer Windows Defender
Utiliser les stratégies de restriction des logiciels (SRPs) et AppLocker
Configurer et utiliser Device Guard
Utiliser et déployer le toolkit Enhanced Mitigation Experience (EMET)

Analyse des activités via l'audit avancé

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)

Vue d'ensemble de Advanced Threat Analytics (ATA)
Comprendre Operations Management Suite (OMS)

Sécurisation du développement d'applications et de l'infrastructure serveur

Utiliser Security Compliance Manager
Introduction aux Nano servers
Comprendre les conteneurs

Protection des données avec le cryptage

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

Limitation de l'accès aux fichiers et aux dossiers

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)

Utilisation des firewalls pour contrôler le trafic

Comprendre ce qu'est Windows Firewall
Fireawalls software-defined distribués

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 2016

Vue d'ensemble de WSUS
Déployer des mises à jour via WSUS