Windows Server 2019 - Sécurité - Niveau 1

4 j (28 heures) Ref : WSSN

Public

Toutes les personnes impliquées dans la sécurité du système d'information

Pré-requis

Avoir une expérience en administration Windows Server de minimum 4 ans

Moyens pédagogiques

Formation réalisée en présentiel ou à distance selon la formule retenue
Exposés, cas pratiques, synthèse, assistance post-formation pendant trois mois
Un poste par stagiaire, vidéoprojecteur, support de cours fourni à chaque stagiaire

Modalités de suivi et d'évaluation

Feuille de présence émargée par demi-journée par les stagiaires et le formateur
Exercices de mise en pratique ou quiz de connaissances tout au long de la formation permettant de mesurer la progression des stagiaires
Questionnaire d'évaluation de la satisfaction en fin de stage
Auto-évaluation des acquis de la formation par les stagiaires
Attestation de fin de formation

Objectifs

Concevoir et configurer une infrastructure sécurisée sous Windows Server 2019
Identifier et analyser les risques
Connaître les principales méthodes de sécurisation d'un parc Windows Server

Programme détaillé

LA SECURITE DANS SON ENSEMBLE

Les différents types et niveaux de vulnérabilité
Les différents types de risques
Les impacts de l'approche sécurité dans un système d'information

LA SECURITE DANS UN ENVIRONNEMENT WINDOWS SERVER

Vue d'ensemble des différentes versions de licences Microsoft et leur impact sur la sécurité
Mise en oeuvre de rôles sur Server Core et Server Nano
Description des différentes méthodes d'authentification

SECURISATION DE L'ARCHITECTURE

Vue d'ensemble des différents protocoles liés à la sécurité d'architecture
Configuration et mise en oeuvre de BitLocker au niveau du parc et stratégies de récupération
Mise en place d'EFS (Encrypting File System) et récupérations
Paramétrage du pare-feu avec fonctionnalités avancées
Vue d'ensemble et mise en oeuvre d'IPSec

EXEMPLE DE TRAVAUX PRATIQUES (A TITRE INDICATIF)

Déploiement, dans le cadre d'un scénario typique d'entreprise, d'un parc complet avec Nano (Hyper-V) et Core (principaux rôles, AD, DHCP, IIS...)

EVOLUTION DE WINDOWS SERVER 2019

Découverte des nouveautés en terme de sécurité et d'impacts
Utilisation des outils d'analyse tels que Security Assessment

ACTIONS CORRECTIVES ET APPLICATIONS DES CORRECTIFS

Analyse des différentes actions correctives
Mise en place de ces actions
Configuration d'un serveur de mises à jour
- WSUS (Windows Server Update Services)
- De type "servicing"
Gestion des rapports

EXEMPLES DE TRAVAUX PRATIQUES (A TITRE INDICATIF)

Mise en oeuvre des principales bonnes pratiques de sécurité sur le rôle AD DS (Active Directory Domain Services)
Analyse et mise en oeuvre des stratégies GPO dédiées à la sécurisation de Windows Server
Mise en oeuvre du niveau de sécurité maximal selon le niveau de la ferme Active Directory

SECURISATION D'ACTIVE DIRECTORY (AD)

Principes de bases sur la sécurité AD
- Mise en place et configuration
- AD LDS (Active Directory Lightweight Directory Services)
RODC (Read Only Domain Controller)
Stratégie de mot de passe
Durcissement du service d'identité, gestions des silos

Configuration

- AppLocker

- Device Guard

Problématiques de compatibilité et niveau de sécurité

Audit et logs Active Directory

Analyses des stratégies de sécurité principales

MISE EN PLACE D'UNE PKI (PUBLIC KEY INFRASTRUCTURE)

Introduction aux chiffrements et aux échanges sécurisés

Présentation et déploiement d'une PKI

Configuration et suivi d'une PKI avec AD CS (Active Directory Certificate Services)

Introduction aux services de sécurité annexes