Développez vos talents
Certifiez vos compétences

Windows Server 2019

Windows Server 2019 - Sécurité - Niveau 1

4 jours (28 heures) | ★★★★½ 4,6/5 | WS19-SEC | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Systèmes › Windows Server 2019

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

- Acquérir des connaissances et compétences pour 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.

Niveau requis

Avoir une expérience en administration Windows Server de minimum 4 ans.

Public concerné

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

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Programme

Jour 1

La sécurité 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 sécurité 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

Sécurisation 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 (à 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...)*

Jour 2

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 (à titre indicatif)

- *Mise en place de profils de sécurité pour un ensemble de serveurs et publication par PowerShell DSC*
- *Mise en oeuvre d'une stratégie de mises à jour automatiques et sécurisées*

Jour 3

Sécurisation 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

Exemples de travaux pratiques (à 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*

Jour 4

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