Prérequis

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

Public concerné

Toute personne impliquée dans la sécurité du système d'information.

Durée de la Formation :4 Jours (28heures)

Prix de la Formation : 2560 euros TTC

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Concevoir et configurer une infrastructure sécurisée sous Windows Server 2019, Windows Server 2022 et Windows Server 2025
- Identifier et analyser les risques
- Lister les principales méthodes de sécurisation d'un parc Windows Server
- Respecter les bonnes pratiques.

Programme de votre formation

1.

FORMATION

Contextualisation du projet de formation et prise en compte des besoins de chacun

- Positionnement initial de l'apprenant par rapport aux objectifs
- Définition des priorités et des objectifs personnels de l'apprenant
- Vidéos de mise en situation
- Accès au Chat interactif myM2i pour interagir avec les membres de son groupe

2.

FORMATION

Programme

Jour 1 - Matin

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
- Protection de l'information et de l'identité
- Mettre en oeuvre une stratégie de sécurité dans le cadre d'un SSI

La sécurité dans un environnement Windows Server

- Vue d'ensemble des différentes versions de licences Microsoft et leurs impacts sur la sécurité
- Mise en oeuvre de rôles sur Server Core et Server Nano
- Notions de Secured-core Server
- Description des différentes méthodes d'authentification

Jour 1 - Après-midi

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 du chiffrement personnel
- Mise en oeuvre de la protection de l'information
- Paramétrage du pare-feu avec fonctionnalités avancées
- Vue d'ensemble et mise en oeuvre d'IPsec
- Durcissement de l'ensemble des flux de l'infrastucture
- Notions de durcissement des principaux services
  - DHCP
  - DNS
  - SMB

Jour 2 - Matin

Evolution de Windows Server 2019 / 2022 / 2025

- Découverte des nouveautés en termes de sécurité et d'impacts

Jour 2 - Après-midi

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 des services de mises à jour et d'une politique associée
- Gestion des rapports
- Notions de durcissements de PowerShell

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 - Matin

Sécurisation d'Active Directory (AD)

- Principes de bases sur la sécurité AD
- Principes JIT (Just In Time) et JEA (Just Enough Administration)
- Vue d'ensemble des approches Red Forest, Bastion et RAMP
- Mise en place et configuration
  - AD LDS (Active Directory Lightweight Directory Services), RODC
- Stratégie de mot de passe
- Durcissement du service d'identité, gestions des silos
- Authentification / autorisations
- Problématiques de compatibilité et niveau de sécurité
- Audit et logs Active Directory
- Analyses des stratégies de sécurité principales
- Gestion des protocoles
- Intégration des bonnes pratiques (GMSA...)

Jour 3 - Après-midi

Sécurisation des systèmes

- Configuration et mise en oeuvre
  - AppLocker, Application Guard
  - System Guard, Device Guard, VSB, KDMA, SMB3...
- Mises en oeuvre des nouveautés dédiées au durcissement
- Introduction aux outils Microsoft Defender

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 (Group Policy Object) 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 - Matin

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 Azure

Introduction à Microsoft Defender 365

Tour d'horizon et intégration des bonnes pratiques et guides de référence

Jour 4 - Après-midi

Surveiller et auditer l'activité

- Vue d'ensemble de l'auditing
- Configuration de l'audit avancé
- Gestion des logs et des audits d'un parc
- Auditing des stratégies et des accès

Vue d'ensemble des nouveautés sécurité dans Windows Server 2019 / 2022 / 2025

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains 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

En cas de formation intra sur site externe à Maftechnologies , le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

Modalités d’évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Accessibilité de la formation

Maftechnologies s'engage pour faciliter l'accessibilité de ses formations. Toutes nos formations sont accessibles aux personnes en situation de handicap : les détails de l'accueil des personnes sont consultables sur la page Accueil PSH.

Modalités et délais d'accès à la formation

Les formations Maftechnologies sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation.