Windows Server 2016-2019-2022-2025 - Sécuriser une infrastructure Windows

Présentiel ou en classe à distance

4 jours (28 h)

Prix inter : 2.890,00 € HT
Forfait intra : 6.890,00 € HT

Réf.: MS504



A qui s'adresse cette formation ?

- RSSI, administrateurs Windows, architectes d'infrastructure et de système, ingénieurs systèmes

- Avoir de bonnes connaissances des systèmes Windows et de PowerShell
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

Pendant

1 - Introduction à la sécurité

- État des vulnérabilités et mauvaises pratiques
- Les risques
- Principaux types et vecteurs d'attaques

2 - Mettre en place une infrastructure de clé publique (PKI)

- Vue d'ensemble d'une PKI
- Déployer et configurer une PKI (autorité de certification, CRL, répondeur en ligne, ...)
- Définir et gérer les modèles de certificats
- Gérer, surveiller et révoquer les certificats
- Audit et surveillance d'une PKI

Déployer une PKI avec deux niveaux d'autorités de certification et un répondeur en ligne

Créer et utiliser des modèles de certificats

3 - Sécuriser les authentifications et Active Directory

- Vues d’ensemble des méthodes d’authentification
- Bonnes pratiques d'administration
- Réorganisation de la structure Active Directory et bastions
- Mettre en oeuvre des hôtes d’administration sécurisés
- Durcissement des authentifications (bloquer les protocoles à risque, NTLM et la négociation d’authentification…)
- Amélioration de la sécurité des mots de passe ordinateurs et sécurisation des changements de mot de passe des comptes locaux (Windows Server 2025)
- Compte krbtgt
- Groupe Protected Users
- Administration par couche (tier), stratégies et silos d’authentification
- Usage et configuration des RODC
- Autorisations et délégations dans l’annuaire
- Comptes de service gérés et de groupe – MSA et GMSA
- Comptes de service gérés délégué – DMSA (Windows Server 2025)
- Stratégies de mots de passe
- Gestion de l’accès privilégié
- Mettre en oeuvre Microsoft et Windows LAPS pour les mots de passe Administrateurs locaux, points d’attention liés à LAPS et améliorations liées à Windows Server 2025 et Windows 11 24H2
- Les stratégies de groupe pour la sécurité des systèmes et stratégies de sécurité
- Bonnes et mauvaises pratiques liées aux stratégies de groupe
- Administration sécurisée avec PowerShell JEA
- Auditer et surveiller les authentifications, les tickets Kerberos et Active Directory

  Configurer un bastion

  Configurer des silos de stratégie d’authentification

  Déléguer l’administration

  Créer et utiliser des comptes de services MSA, GMSA et DMSA

  Créer des stratégies de mot de passe affinés

  Configurer et utiliser Windows LAPS

4 - Sécuriser les services réseau et les connexions

- Sécuriser les serveurs DNS
- Mettre en oeuvre DNSSec
- Définir des stratégies DNS
- Désactiver NetBIOS par DHCP ou par GPO
- Configurer le pare-feu
- Mettre en oeuvre IPSec

  Configurer DNSSec

  Désactiver NetBIOS

5 - Sécuriser les serveurs de fichiers et les données

- Rappels sur les autorisations NTFS
- Rappels sur le gestionnaire de ressources du serveur de fichiers (FSRM) et filtrages
- Inexploité mais précieux contrôle d’accès dynamique
- Présentation d’ADRMS
- Sécuriser le trafic SMB
- Limitation des tentatives de connexions NTLM avec mauvais mot de passe (Windows Server 2025)
- Bloquer les authentifications NTLM des clients (Windows Server 2025 et Windows 11 24H2)
- Utiliser le chiffrement EFS, avantages, inconvénients et récupération
- Mettre en oeuvre BitLocker et options avancées (déverrouillage réseau, …), de la nécessité de chiffrer aussi les serveurs
- Gérer la récupération BitLocker

  Configurer des autorisations NTFS et associer des stratégies d’accès central

  Chiffrer avec BitLocker un serveur et les points d’attention liés

6 - Sécuriser les serveurs IIS

- Déplacer les dossiers de site sur une partition dédiée
- Configurer les authentifications et authentifications basées sur un serveur RADIUS
- Définir des restrictions IP dynamiques des requêtes
- Restreindre les requêtes autorisées sur le serveur

- Configurer ou forcer HTTPS
- Choisir la réécriture des requêtes HTTP en HTTPS et HSTS, avantages et inconvénients
- Isoler les sites avec un pool d'application dédié
- Limiter les accès anonymes au pool d'application
- Sécurisation NTFS des dossiers physiques des sites

Configurer les liaisons HTTPS et forcer SSL

Configurer les authentifications et protéger les authentifications anonymes

7 - Sécuriser les services de bureau à distance et le protocole RDP

- Méthodes pour sécuriser les services de bureau à distance : les mauvaises solutions
- Méthodes pour sécuriser les services de bureau à distance
- Authentification multi-facteurs pour les services de bureau à distance
- Points clés pour sécuriser les services de bureau à distance
- Sécuriser le protocole RDP
- Configurer un accès via une passerelle ou un VPN
- Mettre en oeuvre une authentification multi-facteurs

8 - Mettre à jour les systèmes

- Configurer un serveur WSUS
- Paramétrages avancés et sécurisation
- Rapports WSUS et limites
- Gérer les mises à jour applicatives non Microsoft

9 - Normaliser les systèmes

- Installer et gérer un serveur en installation minimale
- Mettre en oeuvre la sécurité basée sur la virtualisation (Credential Guard, Device Guard)
- Utiliser PowerShell DSC pour unifier les configurations et sécuriser les systèmes
- Exploiter le Security Compliance Toolkit et ses lignes de base
- Appliquer des lignes de base avec OSConfig
- Audit et surveillance générale des systèmes

Configurer la sécurité basée sur la virtualisation

Exploiter le Security Compliance Toolkit

10 - Restreindre les applications autorisées

- Restrictions logicielles ou AppLocker ?
- Mettre en oeuvre AppLocker et les restrictions logicielles
- Exploiter des stratégies d’intégrité de code avec PowerShell
- Surveiller les applications

Mettre en oeuvre AppLocker

Configurer et activer des stratégies d’intégrité de code

11 - Sécuriser la virtualisation Hyper-V

- Sécuriser Hyper-V
- Notion d’hôtes gardés (Guarded Fabric)
- Présentation des machines virtuelles blindées (Shielded VM)

12 - Introduction à Microsoft Defender XDR

- Présentation de Microsoft Defender XDR
- Implémenter et gérer Microsoft Defender XDR
- Utiliser les recommandations de sécurité fournies par Microsoft Defender XDR

13 - Surveiller et auditer les systèmes

- Configurer les audits selon les types de serveurs
- Configurer les journaux et leur archivage, durée de conservation
- Centraliser les journaux, solution Microsoft ou tierce
- Mise en oeuvre de la solution Microsoft
- Analyser les accès
- Les événements à prioriser

Les objectifs de la formation

- Définir les risques et les vulnérabilités
- Implémenter et configurer une PKI
- Sécuriser Active Directory et les authentifications
- Sécuriser les services réseaux et les connexions
- Sécuriser les données
- Durcir les serveurs IIS
- Sécuriser les connexions RDP
- Implémenter et configurer WSUS
- Normaliser les systèmes pour mieux les connaître et mieux les gérer
- Implémenter des restrictions logicielles
- Sécuriser Hyper-V et les machines virtuelles
- Surveiller et auditer les systèmes

Evaluation

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques.
Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Une pédagogie efficace : l'alternance d'exposés théoriques et de mises en application immédiates à travers de nombreux travaux pratiques.
- Les conseils et bonnes pratiques pour assurer la sécurité du système d'exploitation serveur de Microsoft.
- Les retours d'expérience de formateurs spécialistes de la sécurité des systèmes Windows.
- 84% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Evaluation

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques.
Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Dates et villes 2027 - Référence MS504

Dernières places disponibles Session garantie

A distance

du 25 janv. au 28 janv.	du 30 août au 2 sept.
du 18 mai au 21 mai	du 15 nov. au 18 nov.

Paris

du 25 janv. au 28 janv.	du 30 août au 2 sept.
du 18 mai au 21 mai	du 15 nov. au 18 nov.