Durée :	4 jours soit 28 heures	Référence :	IF-WS-SEC

Public visé :

Cette formation s'adresse aux :

- Administrateurs systèmes et réseaux.
- Responsables et techniciens en cybersécurité.
- Ingénieurs et consultants en infrastructures Windows.
- Professionnels de l'IT souhaitant renforcer la sécurité des environnements Windows Server.
- Toute personne en charge de la gestion et de la sécurisation des systèmes Windows et Windows Server en entreprise.

Pré-requis :

Pour assister à cette formation, les participants doivent avoir :

- Une bonne connaissance des environnements Windows (Windows 10, Windows 11).
- Des notions de base sur l'administration des systèmes Windows Server.
- Une compréhension des concepts de réseau (TCP/IP, VPN, DNS, pare-feu).
- Une expérience préalable dans l'administration système et la gestion des droits d'accès est recommandée.

Objectifs pédagogiques :

À l'issue de la formation, les participants seront capables de :

- Comprendre les principes fondamentaux de la sécurité des systèmes Windows et Windows Server.
- Mettre en place et administrer une infrastructure sécurisée avec Windows Server et Active Directory.
- Sécuriser l'authentification et gérer les accès aux ressources de manière avancée.
- Protéger les systèmes, les fichiers et les applications contre les menaces et les vulnérabilités.
- Implémenter des solutions de surveillance et d'audit pour détecter les incidents de sécurité.
- Renforcer la sécurité réseau et gérer les connexions sécurisées.
- Appliquer les bonnes pratiques pour sécuriser les services critiques tels qu'IIS, RDP et Hyper-V.
- Gérer les mises à jour et standardiser les configurations pour garantir la conformité et la sécurité des systèmes.

Compétences acquises à l'issue de la formation :

- Maîtriser les concepts et enjeux de la sécurité des systèmes Windows et Windows Server.
- Implémenter des stratégies de sécurisation des authentifications et de gestion des accès, y compris via Active Directory et les comptes protégés.
- Déployer une infrastructure de clé publique (PKI) et gérer les certificats de sécurité.
- Sécuriser les données, les fichiers et les partages en appliquant les bonnes pratiques de gestion des autorisations et de chiffrement.
- Configurer et administrer les services de sécurité réseau, incluant pare-feu, IPSec et DNS sécurisé.
- Appliquer des politiques de restriction et de contrôle des applications via AppLocker et d'autres solutions.
- Surveiller et auditer les systèmes Windows et Windows Server pour détecter et répondre aux menaces.
- Optimiser et normaliser les configurations système en appliquant des politiques de conformité et en automatisant les déploiements sécurisés.

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure. La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz. L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration. En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Note relative au programme : Les ateliers, démonstrations, travaux pratiques et scénarios présentés dans ce programme sont fournis à titre d'exemples illustratifs et ne sont pas exhaustifs. Afin de garantir une adéquation permanente avec les évolutions

technologiques, le contenu pédagogique ainsi que les environnements de travaux pratiques (TP) sont susceptibles d'être adaptés, ajustés ou mis à jour au cours du temps.

Moyens et supports pédagogiques :

Cadre présentiel

Salles de formation équipées et accessibles aux personnes à mobilité réduite.

- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel

Session dispensée via notre solution iClassRoom s'appuyant sur Microsoft Teams.

- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Modalités d'évaluation et de suivi :

Avant

Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice), qui valide la base de connaissances nécessaires.

Les stagiaires disposent également, depuis leur extranet, d'un **outil d'auto-positionnement** leur permettant d'évaluer leur niveau de maîtrise des compétences visées par la formation. Cette auto-évaluation est réalisée avant le démarrage de la formation à l'aide d'un curseur de positionnement allant du niveau le plus faible au niveau le plus élevé.

Pendant

Après chaque module théorique, un ou plusieurs ateliers pratiques permettent de valider progressivement l'acquisition des connaissances. Un quiz peut accompagner les ateliers pratiques afin de mesurer la compréhension des notions abordées.

Après

À l'issue de la formation, les stagiaires réalisent une nouvelle **auto-évaluation** sur les mêmes compétences que celles évaluées avant la formation. Cette comparaison permet de mesurer leur perception de la progression réalisée et de visualiser les compétences développées au cours de la formation.

Lorsque le programme de formation le prévoit, un examen de certification est organisé conformément aux modalités définies par l'éditeur ou le centre de certification (TOSA, Pearson VUE, ENI, PeopleCert…).

Le formateur réalise également une **évaluation individuelle des compétences** de chaque stagiaire sur l'ensemble des compétences visées par la formation. Pour chacune d'elles, il indique si la compétence est :

- Acquise ;
- En cours d'acquisition ;
- Non acquise.

Lorsque la compétence est évaluée comme **en cours d'acquisition** ou **non acquise**, le formateur formule des observations précisant les difficultés rencontrées ainsi que les actions ou recommandations permettant au stagiaire de poursuivre sa montée en compétences.

Enfin

Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation de formation.

Informations sur l'accessibilité :

Nos formations sont, dans la mesure du possible, conçues pour être accessibles à toutes et à tous. Afin de garantir les meilleures conditions d'accueil et d'apprentissage pour les personnes en situation de handicap, nous vous invitons à contacter notre

référente handicap certifiée :
Céline SOLATGES – 05 61 34 39 80 – csolatges@iform.fr
Nous vous remercions de bien vouloir nous communiquer toute information utile à ce sujet en amont de la formation, afin de mettre en place les adaptations nécessaires et d'assurer un accompagnement optimal.
Pour en savoir plus sur les dispositifs d'accompagnement existants, vous pouvez consulter les sites suivants :

- AGEFIPH
- FIPHFP
- MDPH de votre département

Description / Contenu

Module 1 : Introduction à la sécurité

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

Module 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

Module 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

Module 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

Module 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

Module 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

Module 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

Module 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

Module 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

Module 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

Module 11 : Sécuriser la virtualisation Hyper-V

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

Module 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

Module 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