Formation Windows Server 2019/2022 - Sécurité

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Référence	M504
Durée	3 jours (21h)
Tarif	2 620 €HT

Objectifs

| 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
| 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

Public

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

Prérequis

| Avoir de bonnes connaissances des systèmes Windows et de PowerShell

Pogramme de la formation

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

3 - Sécuriser les authentifications et Active Directory
| Vues d'ensemble des méthodes d'authentification
| Réorganisation de la structure Active Directory et bonnes pratiques d'administration
| Mettre en oeuvre des hôtes d'administration sécurisés
| Durcissement des authentifications (bloquer les protocoles à risques et la négociation d'authentification, ...), stratégies et silos d'authentification
| Usage et configuration des RODC
| Autorisations et délégations dans l'annuaire
| Stratégies de mots de passe
| Gestion de l'accès privilégié
| Mettre en oeuvre LAPS pour les mots de passe
| Administrateurs locaux et points d'attention liés à LAPS
| Les stratégies de groupe pour la sécurité des systèmes et stratégies de sécurité

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 10 au 12 juin 2024
du 9 au 11 septembre 2024

PARIS
du 10 au 12 juin 2024
du 9 au 11 septembre 2024

AIX-EN-PROVENCE
du 10 au 12 juin 2024
du 12 au 14 novembre 2024

BORDEAUX
du 9 au 11 septembre 2024

LILLE
du 9 au 11 septembre 2024
du 12 au 14 novembre 2024

LYON
du 10 au 12 juin 2024
du 12 au 14 novembre 2024

NANTES
du 10 au 12 juin 2024
du 12 au 14 novembre 2024

RENNES
du 10 au 12 juin 2024
du 12 au 14 novembre 2024

ROUEN
du 10 au 12 juin 2024

VOIR TOUTES LES DATES

| 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

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

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
| 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

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

7 - 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

8 - 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
| Audit et surveillance générale des systèmes

9 - 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

10 - Sécuriser la virtualisation Hyper-V
| Sécuriser Hyper-V
| Sécuriser l'infrastructure virtuelle avec des hôtes gardés (Guarded Fabric)
| Mettre en oeuvre des machines virtuelles blindées (Shielded VM)

11 - Introduction à Microsoft Defender Advanced Threat Protection
| Présentation de Microsoft Defender ATP
| Implémenter et gérer Microsoft Defender ATP
| Utiliser les recommandations de sécurité fournies par Microsoft Defender ATP

12 - 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

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

| Mise en oeuvre de la solution Microsoft
| Analyser les accès
| Les événements à prioriser

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.