Sécurité Windows

Référence : **SECSW** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Connaissances en administration Windows. • Connaissances en réseau. • Connaissances en système virtualisé.

PROFIL DES STAGIAIRES

• Administrateurs. • Consultants. • Ingénieurs/Techniciens.

OBJECTIFS

• Définir une politique de sécurité robuste (définir les besoins des clients , identifier les points de sensibilités , choisir une politique efficace). • Évaluer sa configuration. • Mettre en place une politique de sécurité efficace (connaître les dangers de configurations Windows , comprendre les processus de sécurité mis en place par l'OS , créer une infrastructure , déployer des GPO efficaces).

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

JOUR 1

Présentation du système Windows

Protection du BIOS/UEFI

Protection du système

- Active Directory
- Stratégie de groupe
- Mises à jour
- Journaux d'événements Windows
- La suite d'outils Sysinternals
- PowerShell
- La base SAM et le stockage des mots de passe
- Les méthodes d'authentification sous Windows
- Chiffrement du disque avec Bitlocker

JOUR 2

Protection Utilisateurs

- Gestion des droits
- SmartScreen
- Applocker
- UAC
- Déploiement de certificat
- Stratégie de groupe essentielles

Protection de la mémoire sous Windows

- DEP
- ASLR
- Stack canary
- SEHOP

JOUR 3

Protection des services

- Déployer une autorité de certification
- Infrastructure à clé publique
- Durcissement du service LDAP
- Durcissement du service SMB
- Durcissement du service Microsoft SQL
- Durcissement du service Bureau à distance
- Durcissement du service DNS
- Durcissement du service IIS