Sécurisation des infrastructures Windows

Référence : **SECWIND** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 1-Expérience d'administration d'infrastructure Windows. • 2-Solides bases en sécurité des systèmes d'information.

PROFIL DES STAGIAIRES

• 1-Administrateurs. • 2-Architectes. • 3-Experts en sécurité. • 4-Responsables sécurité.

OBJECTIFS

• Durcir un serveur Windows. • Administrer de façon sécurisée. • Sécuriser vos postes de travail. • Auditer votre infrastructure.

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

Introduction

Durcissement système et réseau

- Système : Nécessité du durcissement ; Minimisation ; Gestion des services ; Journalisation
- Réseau : Utilité des protocoles obsolètes ; Cloisonnement réseau
- Parefeu et IPsec : Protocoles d'authentification ; Autres points d'attention ; Desired State Configuration
- Focus : sécuriser votre cloud Microsoft

Administration sécurisée

- Qu'est-ce qu'un administrateur
- Administration sécurisée : pourquoi ?
- TTP : Techniques, Tactiques et
- Procédures
- Compromettre un Active Directory
- Compromission initiale
- Mouvement latéral : Passthe-hash…
- Élévation de privilèges
- Vulnérabilités classiques
- Bonnes pratiques
- Utilisateurs et groupes locaux
- Délégation
- Powershell et le JEA
- Active Directory et les GPO
- Administration sécurisée
- Forêt « bastion »
- Administration en strates
- Silos d'authentification
- Environnement d'administration
- Focus : Golden Ticket et krbtgt

Sécurité du poste de travail

- Windows 10 et le VBS
- Secure Boot
- Device Guard
- Application Guard
- Exploit Guard
- Credential Guard

- Bitlocker
- Chiffrement de disque
- Autres fonctionnalités
- Isolation réseau
- Mise à jour

Auditer son infrastructure

- Différents types d'audits
- Points à auditer
- SCM
- Pingcastle
- Recherche de chemins d'attaque
- BloodHound et AD-Control-Path
- Les extracteurs
- Graphes d'attaques
- Simulation et remédiation