EduGroupe
Accompagner pour réussir

Sécurisation des infrastructures Windows

Référence : **SECWIND** Durée : **5 jours (35 heures)** Certification : **Aucune**

Connaissances préalables

- 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 préparée

- Aucune

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 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 et de réflexions

Formateur·rice

- Consultant-Formateur expert Sécurité défensive

Méthodes d'évaluation des acquis

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

Contenu du cours

1. Introduction

-

2. Durcissement système et réseau

- Système : Nécessité du durcissement
- Réseau : Utilité des protocoles obsolètes
- Parefeu et IPsec : Protocoles d'authentification
- Focus : sécuriser votre cloud Microsoft

3. 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

4. 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

5. 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

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.