G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Programme de formation

Sécurisation des infrastructures Windows

But de la formation

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

Pré-requis

- Formation "Fondamentaux techniques de la cybersécurité"
- (ou) Expérience d'administration d'infrastructure Windows
- (ou) Solides bases en sécurité des systèmes d'information

Type de public

- Administrateurs
- Architectes
- Experts en sécurité
- Responsables sécurité

Moyens pédagogiques

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Sanction de la formation

- A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification par HS2.
- Formation délivrée en partenariat avec HS2

Méthodes pédagogiques

- Cours magistral illustré par des travaux pratiques réguliers

Durée

40 heures (6 jours).

Programme

Introduction
Module 1 : 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

Module 2 : Administration sécurisée

- Qu'est-ce qu'un administrateur
- Administration sécurisée : pourquoi ?
  - TTP : Techniques, Tactiques et Procédures
  - Compromettre un Active Directory
    - Compromission initiale
    - Mouvement latéral : Pass-the-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

Module 3 : 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

Module 4 : 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
- Examen