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

Programme de formation

Fondamentaux techniques de la cybersécurité

But de la formation

- Être en mesure dans tous les domaines techniques de la sécurité (système, réseau, applications, cryptographie...) de :
  - Maîtriser le vocabulaire et les concepts principaux du domaine
  - Connaître différentes techniques d'attaque
  - Choisir et appliquer les bonnes mesures de sécurité

Pré-requis

- Bonnes connaissances en informatique

Type de public

- Administrateurs système ou réseau,
- Architectes,
- Développeurs,
- Personnel débutant ou souhaitant acquérir de bonnes bases techniques en SSI.

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 HS2
- Formation délivrée en partenariat avec HS2

Méthodes pédagogiques

- Cours magistral illustré par des travaux pratiques réguliers

Durée

40 heures (6 jours).

Programme

Module 1 : SSI - principes de bases

- Pourquoi la SSI ?
- Notion de risque
- Les règles de base
- Contrôle d'accès
    - AAA
    - Gestion des utilisateurs
    - Authentification
    - Gestion des privilèges

Module 2 : Cryptographie

- Concepts fondamentaux
- Fonctions de base
    - Chiffrement
    - Hachage
    - Signature
- Protocoles
    - TLS
    - IPSec
    - SSH
- PKI / IGC

Module 3 : Réseau

- Modèles théoriques : OSI, TCP/IP
- Attaques classiques
    - Découverte de ports
    - Man-in-the-Middle
- Contrôle d'accès réseau
- Segmentation
    - Qu'est qu'une bonne architecture ?
    - Comment segmenter son réseau
    - VLAN
    - Parefeu
    - Proxy
- Réseaux sans fil
- Sécuriser le Cloud

Module 4 : Applications

- Architecture n-tiers
- Protocoles
- Authentification et sessions
- Top 10 de l'OWASP
- Buffer Overflow
- Processus de développement

Module 5 : Windows

- Installation
- Bitlocker
- Mesures Windows 10 :
    - Device Guard
    - Application Guard
    - Exploit Guard
- Gestion des administrateurs
- Éviter le Pass-The-Hash

Module 6 : Linux

- Système de fichiers
- Minimisation
- Comptes utilisateurs
- Authentification
- SELinux
- AppArmor
- SSH
- Netfilter
- Journalisation

Module 7 : Gestion d'incidents

- SOC et CSIRT
- Gestion d'incidents
- La base : sauvegarde et journalisation
- Analyse inforensique