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

Programme de formation

Essentiels techniques de la cybersécurité

But de la formation

- Acquérir la connaissance des concepts fondamentaux de la SSI.
- Identifier les besoins en sécurité à tous les niveaux (système, réseau, applications...)
- Comprendre les différents types d'attaques
- Connaitre les mesures de sécurité permettant de les contrer

Objectifs pédagogiques

1. Savoir identifier les points faibles des systèmes d'information
2. Savoir définir les règles de sécurité fondamentales pour sécuriser un SI
3. Comprendre la portée (objectifs, enjeux, impacts, ...) des attaques informatiques

Pré-requis

- Cette formation ne nécessite pas de prérequis particuliers, elle accessible à un large public.

Type de public

- Toute personne souhaitant acquérir la compréhension de la cybersécurité
- Responsable de la sécurité (RSSI) de formation non technique
- Chef de projet et acteur d'un projet sécurité

Cette formation est accessible à un public plus large que la formation "Fondamentaux techniques de la cybersécurité" en permettant aux personnes au profil non informaticien ou non technique d'obtenir une vision opérationnelle de la cybersécurité

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

- Formation non certifiante
- Formation délivrée en partenariat avec HS2

Méthodes pédagogiques

- Cours magistral avec de nombreux exemples pratiques

Durée

14 heures (2 jours).

Programme

Sécurité : concepts fondamentaux

- Concepts de bases
- Gestion du risque : vulnérabilité, menace, impacts métiers
- Dans la peau d'un attaquant
- Principes de base : connaître son SI, moindre privilège, défense en profondeur, prévention et détection

Cryptographie

- Chiffrement
- Hachage
- Signature
- TLS
    - PKI/IGC

Gestion des utilisateurs et des privilèges

- Provisionnement
    - Moindre privilège
- Authentification
- Protection des administrateurs

Sécurité des réseaux

- Principes de base
- Attaques
- Contrôle d'accès
- Filtrage et relayage
- Architecture sécurisée .
    - WiFi

Sécurité des systèmes

- Minimisation et durcissement
- Sauvegarde
- Veille sécurité
- Mise à jour
- Sécurisation active
    - Virtualisation

Sécurité des applications

- Vulnérabilités : le TOP 10 de l'OWASP
- Attaques et défenses
- Stockage des mots de passe
- Processus de développement

Détection et gestion d'incident

- Journalisation
- SOC et CSIRT
- Processus de gestion d'incident