400 FORMATIONS
POUR FAIRE LA DIFFÉRENCE

PARCOURS INTRODUCTIF À LA CYBERSÉCURITÉ
CODE STAGE : SECINT

OBJECTIFS

Détenir une vision globale de la cybersécurité et son environnement (enjeux, écosystème...)
Connaître les différents référentiels, normes et outils de la cybersécurité
Appréhender les métiers liés à la cybersécurité
Connaître les obligations juridiques liées à la cybersécurité
Comprendre les principaux risques et menaces ainsi que les mesures de protection
Identifier les bonnes pratiques en matière de sécurité informatique

DURÉE

10 jours

PUBLIC

Toutes personnes souhaitant apprendre les fondamentaux de la sécurité informatique et/ou souhaitant s'orienter vers les métiers de la cybersécurité, notamment les techniciens et administrateurs systèmes et réseaux.

PRÉ-REQUIS

Avoir des connaissances générales dans les systèmes d'information et connaître le guide d'hygiène sécurité de l'ANSSI.

PROGRAMME

Chapitre 1?: Les tendances de la cybercriminalité

Chapitre 2 : Base de la sécurité de l'information

Chapitre 3 : Gestion des cyberattaques

Chapitre 4 : Gestion dcode2utf('8217',0)incidents et riposte face à une cyberattaque

Chapitre 5 : Identifier les acteurs de la lutte contre la cybercriminalité

Chapitre 6 : Les bonnes pratiques

Chapitre 7 : Loi, normes, référentiels, organisme qui régit la cybersécurité

Chapitre 8 : La sécurité offensive et le pentesting

Chapitre 9 : Préparer son test d'intrusion

Chapitre 10 : Collecte d'informations

Chapitre 11 : Énumération de l'infrastructure

Chapitre 12 : Analyse des vulnérabilités

Chapitre 13 : Exploitation

Chapitre 14 : Post-Exploitation

Chapitre 15 : Métiers, support de travail et référentiels

Chapitre 16 : Durcissement des infrastructures Windows

Chapitre 17 : Ouverture à l'investigation numérique avec la collecte de données

Chapitre 18 : Recherche d'artefacts et reporting

Chapitre 19 : État de l'art du management du risque

Chapitre 20 : Créer un programme de gestion des risques

Chapitre 21 : Analyser et estimation des risques

Chapitre 22 : EBIOS

Chapitre 23 : MEHARI

Chapitre 24 : OCTAVE

Chapitre 25 : la méthode Bow-tie

Chapitre 26 : métier de RSSI (responsable de la sécurité des systèmes d'information)

Chapitre 27 : Savoir interpréter les référentiels, normes du marché

Chapitre 28 : NIST Cybersecurity framework

Chapitre 29 : Guide d'hygiène de l'ANSSI

Chapitre 30 : Création d'un tableau de bord

Chapitre 31 : Quid de la gouvernance du DevOps

Chapitre 32 : La sécurité du monde industriel