Référent Cybersécurité

Durée	**4 jours**	**Référence Formation**	**4-IT-RECY**

Objectifs

Identifier et analyser des problèmes de cybersécurité dans une perspective d'intelligence et de sécurité économique
Connaître les obligations et responsabilités juridiques de la cybersécurité
Identifier et comprendre les menaces liées à l'utilisation de l'informatique et des réseaux internet, réseaux privés d'entreprises ou réseaux publics
Mettre en œuvre les démarches de sécurité inhérentes aux besoins fonctionnels
Savoir présenter les précautions techniques et juridiques à mettre en place pour faire face aux attaques éventuelles

Participants

Tout public

Pré-requis

Aucun prérequis

Moyens pédagogiques

Accueil des stagiaires dans une salle dédiée à la formation équipée d'un vidéo projecteur, tableau blanc et paperboard ainsi qu'un ordinateur par participant pour les formations informatiques.
Positionnement préalable oral ou écrit sous forme de tests d'évaluation, feuille de présence signée en demi-journée, évaluation des acquis tout au long de la formation.
En fin de stage : QCM, exercices pratiques ou mises en situation professionnelle, questionnaire de satisfaction, attestation de stage, support de cours remis à chaque participant.
Formateur expert dans son domaine d'intervention
Apports théoriques et exercices pratiques du formateur
Utilisation de cas concrets issus de l'expérience professionnelle des participants
Réflexion de groupe et travail d'échanges avec les participants
Pour les formations à distance : Classe virtuelle organisée principalement avec l'outil ZOOM. Assistance technique et pédagogique : envoi des coordonnées du formateur par mail avant le début de la formation pour accompagner le bénéficiaire dans le déroulement de son parcours à distance.

PROGRAMME

Cybersécurité : notions de bases, enjeux et droit commun
- Définitions
- Intelligence économique, sécurité économique globale
- Cybersécurité

L'hygiène informatique pour les utilisateurs
- La nouvelle économie de la cybercriminalité

- Panorama des menaces selon une typologie
- Les vulnérabilités (exemples, détermination, veille)
- Focus sur l'ingénierie sociale

Gestion et organisation de la cybersécurité
- Présentation du principe de défense en profondeur
- Identification et évaluation des actifs et des objectifs de sécurité

Protection de l'innovation et cybersécurité
- Responsabilités
- Préservation de la preuve
- L'offre assurantielle

Administration sécurisée du système d'information (SI) interne d'une entreprise
- La prévention
- Le traitement des cyberattaques et la réponse judiciaire
- Rôle et missions des acteurs étatiques chargés du traitement technique et judiciaire des attaques cybers

La cybersécurité des entreprises ayant externalisé tout ou partie de leur SI
- Connaître le système d'information et ses utilisateurs
- Identifier le patrimoine informationnel de son ordinateur (brevets, recettes, codes, source, algorithmes…)
- Maîtriser le réseau de partage de documents (en interne ou sur internet)
- Mettre à niveau les logiciels
- Authentifier l'utilisateur
- Nomadisme-Problématiques liées au BYOD (Bring your Own Devices)

Sécurité des sites internet gérés en interne
- Présentation des publications/recommandations
- Guides de l'ANSSI
- Recommandations de la CNIL
- Recommandations de la police et de la gendarmerie
- Club de la sécurité de l'information Français, Club des experts de la sécurité de l'information et du numérique (CLUSIF/CESIN), etc.
- Observatoires zonaux de la Sécurité des systèmes d'information (SSI)
- Les CERTs (Computer Emergency Response Team)