DEVELOPPER LES BONNES PRATIQUES EN MATIERE DE CYBERSECURITE

Objectifs pédagogiques :

A l'issue de la formation « développer le bonnes pratiques en matière de cybersecurité », les participants doivent être en capacité : de connaître le rôle et missions d'un pilote SSI (Sécurité du Système d'Information), réagir en cas d'incidents, procédures et acteurs à mobiliser, identifier les menaces principales, diffuser les bonnes pratiques, identifier les aides des pouvoirs publics existantes.

Public concerné :

Cette formation s'adresse aux salariés des entreprises adhérentes à AGEFOS PME, et plus spécifiquement aux acteurs en capacité à sécuriser les données de l'organisation : personnel de Direction, d'encadrement, personnel en fonction de la gestion du ou des système d'information.

Prérequis :

Avoir les connaissances de base juridiques et technique sur cybersecurité.

Moyens et méthodes pédagogiques :

Présentation magistrale et pédagogie active centrée sur des échanges prenant en compte les spécificités des participants.

Méthodes d'évaluation :

Bilan de stage écrit en fin de formation rempli par le stagiaire.
Mises en situation (Cas pratiques)

Sanction de la formation :

Attestation de fin de formation

Dates et Lieux :

CCI Formation Perpignan – 8/11/2018

Durée : 1 jour – 7 heures

Horaire : 9H00-12H30 / 14H00-17H30

Prix :

Non adhérent Agefos : 280 € Net / stagiaire

Adhérent Agefos : 266 € Net / stagiaire

Participants : Ouverture confirmée dès lors qu'un minimum de 4 salariés sont inscrits venant de différentes entreprises

CCI OCCITANIE
PYRÉNÉES-MÉDITERRANÉE

Programme :

I. **L'écosystème numérique**
II. **Panorama des menaces**
III. **Reconnaissance des risques**
IV. **Limitation des risques**
V. **Agir et réagir de façon adaptée**

Programme détaillé :

I. **L'écosystème numérique**
Le système d'information et composantes (poste de travail, serveurs, réseau, applications, données)

II. **Panorama des menaces**
Identification des principales attaques, conséquences associées

III. **Reconnaissance des risques**
Audits et valorisation des risques
Les scénarii envisageables
Repérage de l'apparition des anomalies

IV. **Limitation des risques**
Les risques utilisateurs
Messageries, téléchargements
Les périphériques

V. **Agir et réagir de façon adaptée**
L'utilisation des ressources disponibles en prévention et réaction des attaques
La communication en prévention, en cas de dysfonctionnement

Pyrénées Orientales : Perpignan - 04 68 56 62 20 – perpignan@sudformation.cci.fr