

Formation "Intégrer la cybersécurité dans les projets informatiques"

| | | |
|-------------------------------|---|-------------------|
| PROGRAMME DE FORMATION | DURÉE : 1 jour (7 heures) – en centre de formation ou en entreprise. | Présentiel |
|-------------------------------|---|-------------------|

Objectif

Exprimer un objectif et un besoin en cybersécurité, et s'assurer de leur prise en compte dans les projets informatiques.

Pré-requis

Niveau avancé en informatique/développement.

Participants

Chefs de projets informatiques.

Validation

L'évaluation du cours se fera à travers des exercices : des phases de quizz et de questions/réponses.

Modalités

Nos formateurs utilisent les méthodes andragogiques suivantes : la démonstration, l'étude de cas, le projet, le questionnement de groupe et le quizz.

Infos complémentaires

Délai d'accès :
Entre 15 et 45 jours. Formation accessible aux personnes en situation de handicap.
Plus d'informations au 0692 22 55 83.

Débouchés :
Cette formation permet une montée en compétences mais ne permet pas de se former à un métier.

Passerelles :
Aucune passerelle disponible.

Programme synthétique

Objectifs spécifiques

Cette formation a pour objectif de donner à un chef de projet les clés pour que la cybersécurité soit prise en compte efficacement dans tout le cycle de vie d'un projet informatique. Elle vise, en particulier, à bien faire comprendre, son rôle et ses responsabilités dans le domaine de la sécurité des projets. Elle doit lui permettre d'exprimer les besoins en objectifs de sécurité, de dialoguer avec un expert en cybersécurité, et de contrôler l'implémentation des mesures mises en place, tout au long de la durée de vie du projet.

Module 1

Les cyberattaques locales récentes,
Témoignages de victimes de cyberattaques
Un site pour se tenir informé de l'actualité cyber

Module 2

L'environnement numérique des entreprises, et la numérisation de la fonction « logistique » et de la chaîne d'approvisionnement :
Comprendre la révolution numérique à travers une brève histoire , et son impact sur les pratiques des entreprises, et sur le métier de chef de projet
Comprendre les usages privés et professionnels (les réseaux sociaux,, le « Darkweb»..) et leur impact sur le fonctionnement de l'entreprise,
Comprendre les apports des technologies (Cloud, 5G, Big Data, IOT, Intelligence Artificielle , la « blockchain ») et les services qu'elles offrent pour améliorer le fonctionnement des entreprises, et leur performance,
Les tendances,
L'état de l'art local (à La Réunion)

Module 3

Panorama des menaces
Définir Les sources de risques, les effets recherchés d'une attaque par type (sabotage, espionnage, atteinte à l'image, cybercriminalité, cyberguerre..)
Qualifier les attaquants, et les menaces qu'ils peuvent faire peser sur les entreprises,
Connaître les principales menaces

Module 4

Exercice sur les mesures envisagées pour anticiper et contrer les attaques

Module 5

Les essentiels de la cybersécurité
Connaître le « jargon » des experts en cybersécurité (les définitions, les processus, les référentiels, la cyberrésilience..)
Connaître les activités, les domaines, des outils de développement,

Module 6

Mise en pratique avec manipulation des concepts de cybersécurité

Module 7

La cybersécurité des projets:
Les grandes étapes de l'intégration de la sécurité dans les projets et selon leur type, de la conception au retrait de service,
La sécurité des données dans les projets
L'analyse du risque cyber dans les projets
Le maintien en condition de sécurité des projets

Module 8

Les bonnes pratiques de cybersécurité au quotidien
Connaître les principaux vecteurs pour les attaquants (le hameçonnage, les supports amovibles, et mots de passe..),
Sécuriser mes informations,
Réagir en cas de fuite de données,
Utiliser internet en sécurité, pour mes opérations