ADS — ACADÉMIE DES SAVOIRS — Centre de formation

Formation cybersécurité pour responsable système/réseau en TPE/PME

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

Objectif

Définir la sécurité des réseaux, acquérir la culture sécurité réseaux, et intégrer la sécurité au quotidien dans les réseaux et systèmes.

Pré-requis

Niveau avancé en gestion des systèmes et réseaux.

Participants

Responsable réseaux et systèmes.

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 chef de projet de de« réseaux et systèmes » ou à un responsable informatique les connaissances nécessaires et suffisantes de sécurité pour organiser l'administration des réseaux et des systèmes en sécurité, et améliorer le niveau de maturité cyber de l'entreprise.
Elle vise, en particulier, à bien faire comprendre, son rôle et ses responsabilités dans le domaine de la sécurité,
Elle doit lui permettre d'exprimer les besoins en sécurité et choisir les moyens adaptés à l'activité de son entreprise, de dialoguer avec un expert en cybersécurité, les dirigeants ou les responsables « métier ».

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 leur transformation digitale:
Comprendre les usages privés et professionnels (les réseaux sociaux, WEB, 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 ») dans les services offerts par les systèmes d'information des entreprises et leurs tendances,
Connaître les usages locaux (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
Les essentiels de la cybersécurité :
Comprendre le langage des experts (les définitions, les processus, les actifs essentiels, les évènements redoutés, les risques..)
Définir mon besoin en sécurité,
Mettre en œuvre des processus de cybersécurité quelle que soit la taille de l'entreprise,
Connaître les activités, les domaines, quelques outils
Participer à la résilience numérique de mon entreprise (TPE, PME..)

Module 5
Mise en pratique avec un exemple (actif, critères..)

Module 6
La cybersécurité des réseaux et des systèmes:
Connaître les principes de l'administration des réseaux et systèmes « en sécurité »,
Intégrer la cybersécurité dans la gouvernance du SI,
Analyser le risque cyber,
Participer à la mise en œuvre d'un plan d'amélioration continue de la sécurité

Module 7
La participation de la fonction à la gestion de crise (exercice)

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,
Actions à réaliser en cas de fuite de données,
Utiliser internet en sécurité, pour mes opérations