ADS — ACADÉMIE DES SAVOIRS — Centre de formation

Formation cybersécurité pour les Responsables des achats

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

Objectif

Contribuer à la cybersécurité de mon entreprise pour les responsables des achats (Rôle et responsabilité dans le domaine).

Pré-requis

Compréhension de l'informatique de base.

Participants

Responsables des achats.

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
La sécurité numérique des entreprises passe une bonne perception par les managers, des enjeux dans ce domaine, des impacts potentiels d'une attaque sur leur activité, des responsabilités qui leur incombent au sein de l'entreprise.
Cette formation ne demande aucun prérequis technique. Les technologies présentées doivent permettre à un non-expert de mieux comprendre leur performance, et les menaces que leur emploi induit.
La fonction « achat »
Elle vise à :
Faire percevoir les enjeux de cybersécurité pour la fonction achat et appréhender l'impact sur l'activité.
Sécuriser simplement l'activité en prenant en considération les risques spécifiques
Connaître la gestion des données sensibles,
Mettre en œuvre les bonnes pratiques.

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 transformation digitale des achats,
Comprendre la révolution numérique, le rôle des géants de la tech, les usages (WEB, Darkweb, réseaux sociaux..), les tendances, et les usages locaux (à La Réunion), les entreprises de Services numériques, les plates-formes « tech »
Comprendre Les apports concrets des technologies (WEB, Cloud, 5G, Big Data, IA IOT. « smart environment »), et leur impact.

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 brièvement les attaquants, et les menaces qu'ils peuvent faire peser sur les entreprises
Connaître les principales menaces (et les autres) sur les données et les processus des achats

Module 4
Les essentiels de la cybersécurité
Connaître mes actifs essentiels d'un système d'information
Définir Les critères de sécurité (les exemples pour les ressources humaines
Mettre en œuvre (impérativement) des processus quelle que soit la taille de l'entreprise,
Connaître les activités, les domaines, quelques outils
Différencier cybersécurité et cyber résilience

Module 5
Mise en pratique de manipulation des concepts (actifs, critères, risques..)

Module 6
Les « acheteurs », acteurs de la sécurité des prestations des entreprises
Intégrer la sécurité dans la dématérialisation des processus d'achats (e-achat..)
Contrôler la maturité numérique d'un prestataire ou fournisseur
Intégrer les clauses de sécurité dans les contrats (plan d'assurance 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, réagir en cas de fuite de données ,
Utiliser internet en sécurité