FORMATION RÉFÉRENT CYBER

High Jack offre une formation intensive qui permettra aux participants de devenir des référents cybersécurité compétents, capables de gérer et de coordonner les initiatives de cybersécurité au sein de leur organisation.

FORMATION PRÉSENTIEL ET DISTANCIEL HYBRIDE ET E-LEARNING

OBJECTIFS

- Sensibilisation et prévention des risques
- Gestion des incidents et réponses aux cyberattaques
- Conformité et réglementation
- Déploiement de solutions et bonnes pratiques
- Pilotage et amélioration continue de la cybersécurité

PROGRAMME

MODULE 1 : INTRODUCTION À LA CYBERSÉCURITÉ ET GESTION DES RISQUES

- Introduction à la cybersécurité : définition, importance, enjeux pour les entreprises.
- Comprendre les concepts de base de la cybersécurité.
- Savoir identifier les risques et les menaces courantes.
- Présentation des menaces courantes : phishing, malware, ransomware, etc.
- Introduction à la gestion des risques en cybersécurité.

MODULE 2 : SENSIBILISATION AUX PRINCIPALES RÉGLEMENTATIONS

- Comprendre les principales réglementations en matière de cybersécurité.
- Connaître les obligations légales et réglementaires des entreprises.
- Introduction à la directive NIS 2 et autres réglementations pertinentes (RGPD, ISO 27001, etc.).

MODULE 3 : CRÉATION ET MISE EN ŒUVRE D'UNE CHARTE INFORMATIQUE

- Concevoir et mettre en œuvre une charte informatique adaptée à l'entreprise.
- Composants essentiels d'une charte informatique.

PROGRAMME

MODULE 4 : TYPES D'ATTAQUES CYBERNÉTIQUES ET MÉTHODES DE DÉFENSE

- Identifier les différents types d'attaques cybernétiques.
- Connaître les méthodes de défense et de prévention des cyberattaques.
- Présentation des types d'attaques : DDoS, social engineering, APT, etc.

MODULE 5 : GESTION DE CRISE CYBER

- Gérer efficacement une crise de cybersécurité.
- Préparer un plan de réponse aux incidents.
- Étapes de la gestion de crise : détection, réponse, récupération, communication.

MODULE 6 : GOUVERNANCE DE LA CYBERSÉCURITÉ

- Comprendre le rôle de la gouvernance dans la gestion de la cybersécurité.
- Apprendre à structurer la gouvernance de la cybersécurité au sein d'une organisation.
- Introduction à la gouvernance en cybersécurité : rôles, responsabilités et processus.
- Définition des politiques de sécurité au niveau de l'entreprise.
- Création d'un comité de sécurité : rôles et missions.

MODULE 7 : ANALYSE DES RISQUES ET GESTION DES VULNÉRABILITÉS

- Savoir identifier, analyser et gérer les risques et vulnérabilités.
- Conduire des audits de sécurité et des tests de pénétration.
- Méthodologies d'analyse de risques : ISO 27005, EBIOS, etc.
- Techniques de gestion des vulnérabilités : identification, classification, priorisation.
- Introduction aux tests de pénétration (pentesting).

MODULE 8 : GESTION DE LA CONTINUITÉ DES ACTIVITÉS ET PLAN DE REPRISE APRÈS SINISTRE

- Comprendre l'importance de la continuité des activités en cas de cyberattaque.
- Mettre en place un plan de reprise après sinistre (PRA) efficace.
- Concepts de continuité des activités (PCA) et de reprise après sinistre (PRA).

ORGANISATION

RESTITUTION ET BILAN DE LA FORMATION + LIVRET BONNES PRATIQUES

- **Évaluation continue** : via des quiz, des études de cas, et des exercices pratiques.
- **Projet final** : les participants créeront un plan de cybersécurité complet pour une organisation fictive, couvrant la gouvernance, la gestion des risques, le PCA/PRA, et une campagne de sensibilisation.
- **Certification** : attestation de formation en tant que référent cybersécurité.

Niveau 2 28 heures	Phase Synch,Async	Module pédagogique
0,5	A	Engagement du tour de table initial
7	A	Mise en situation pratique : sensibilisation aux attaques par malice informatique
0,5	S	Restitution personnalisée de la mise en situation
1,5	S	Module formation : introduction à la cybersécurité
1,5	S	Module formation : la sécurité des réseaux informatiques
0,5	A	Etudes ressources pédagogiques
1	S	Module formation : la sécurité des données
1	S	Module formation : les normes et réglementations du cyberespace
0	S	Module formation : la sécurité informatique par secteur d'activité
0	A	Mises en situation ciblées : deuxième session
0	S	Restitution personnalisée de la deuxième session des mises en situations ciblées
0,5	S	Restitution et bilan de la formation + livret bonnes pratiques Questionnaire à choix multiples permettant de valider les acquis Les points clefs de la formation et leur mise en œuvre opérationnelle

PRÉREQUIS

Personnes formés toutes personnes travaillant dans le monde de l'entreprise ou associatif
Ordinateur connecté à internet avec sortie audio, équipé d'un micro.

COMPÉTENCES ATTESTÉES

1 Introduction à la cybersécurité

Les participants identifieront les principaux enjeux de la cybersécurité ainsi que les acteurs et les motivations des cybercriminels. Ils apprendront à détecter et se protéger des menaces et vulnérabilités. Enfin, ils disposeront d'un recueil de bonnes pratiques en matière de sécurité informatique.

2 La sécurité des réseaux

Ce module enseigne la sécurisation des réseaux, y compris les réseaux locaux et sans fil, ainsi que des réseaux longues distances. Les participants acquerront des compétences pour comprendre la sécurisation et la maintenance des réseaux, leur permettant ainsi d'appréhender les pratiques visant à réduire les vulnérabilités aux cyberattaques.

3 La sécurité des données

Les participants apprendront les principes fondamentaux de la sécurisation des données (préservation de la confidentialité, chiffrement des données). Également, ils étudiront la gestion sécurisée de leurs outils numériques afin de préserver la confidentialité de leurs activités et de leur identité. Enfin, ils développeront leurs compétences en matière de transmission sécurisée des informations à travers les différents dispositifs de messagerie.

4 La sécurité sectorielle

Les participants comprendront les risques relatifs aux infrastructures critiques et industrielles étant interconnectés avec l'informatique de gestion. Ils découvriront comment se protéger des principales attaques sur différents secteurs (santé, bancaire, industriel).

5 Les normes et réglementations

Les participants connaitront les principes de bases des principales normes et réglementations du domaine numérique.
Ils pourront disposer des éléments leur permettant de rester en conformité avec la législation aussi bien dans leurs usages que dans leurs phases de conception de leurs outils métiers

DURÉE DE LA FORMATION

Cette formation se déroule sur une période totale de 14h ou 28h (évaluation comprise).

DÉLAI D'ACCÈS

Jusqu'à 2 mois après signature de la convention de formation. Un test de positionnement avant la formation est effectué sous la forme d'un questionnaire afin de juger le niveau du stagiaire entrant.

MODALITÉS D'EXECUTIONS

À distance via l'outil "Teams" et contenu E-learning via une plateforme LMS.

ACCESSIBILITÉ

La formation est accessible aux personnes en situation de handicap. Nos intervenants adaptent les rythmes, temps de formation et les modalités pédagogiques en fonction des différentes situations de handicap.

Si vous êtes en situation de handicap, contactez notre référent handicap par mail contact@adjan.fr (Thibault JACQUES) afin d'adapter au mieux la formation à vos besoins spécifiques .

MODALITÉS D'ÉVALUATION

- Évaluations formatives : QCM, comptes rendus...
- Évaluations sommatives : QCM, comptes
- rendus...
- Évaluation de satisfaction

MÉTHODES ET SUPPORTS PÉDAGOGIQUES

- Alternance de méthodes expositives, démonstratives et actives.
- Exercices pratiques et études de cas.

Formateur référent : Cyrille ELSEN

TARIFS : 560€/HT

ADJAN
REIMS, NANCY, LIMOGES

Siège social : 74 rue du Docteur Lemoine, 51100 Reims

contact@adjan.fr

03 10 45 40 01