



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**

OBJECTIFS



- Comprendre les fondamentaux de la cybersécurité
- Mettre en place une politique de sécurité informatique
- Détecter et réagir face aux incidents de sécurité
- Sécuriser les infrastructures et les outils numériques
- Assurer une veille et une mise en conformité réglementaire

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).

PROGRAMME

Module 9 : formation et sensibilisation continue

- Former les référents à leur rôle de formateurs et sensibilisateurs en cybersécurité.
- Apprendre à concevoir et déployer des campagnes de sensibilisation efficaces.
- Stratégies de formation continue et de sensibilisation en cybersécurité.
- Création de supports pédagogiques : ateliers, webinaires, vidéos.
- Techniques d'animation de sessions de sensibilisation.

Module 10 : veille technologique et mise à jour des connaissances

- Maintenir à jour ses connaissances face à l'évolution rapide des menaces cybernétiques.
- Savoir identifier et intégrer les nouvelles technologies de sécurité.
- Introduction à la veille technologique en cybersécurité.
- Outils et méthodes pour suivre les évolutions technologiques et les nouvelles menaces.

ORGANISATION

Restitution et bilan de la formation + 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 1 70 heures	Phase Synch, Async	Module pédagogique
0,5	A	Engagement du tour de table initial
	A	Mise en situation pratique: sensibilisation aux attaques par malice informatique
0,5	S	Restitution personnalisée de la mise en situation
7	S	Module 1 : Introduction à la cybersécurité et à la gestion des risques
6	S	Module 2 : Sensibilisation aux principales réglementations
7	S	Module 3 : Création et mise en œuvre d'une charte informatique (
10	S	Module 4 : Types d'attaques cybernétiques et méthodes de défense
8	S	Module 5 : Gestion de crise cyber
7	S	Module 6 : Gouvernance de la cybersécurité
7	S	Module 7 : Analyse des risques et gestion des vulnérabilités
7	S	Module 8 : Gestion de la continuité des activités et plan de reprise après sinistre
4	S	Module 9 : Formation et sensibilisation continue
4	S	Module 10 : Veille technologique et mise à jour des connaissances
0,5	S	Restitution et bilan de la formation + bonnes pratiques Questionnaire à choix multiples permettant de valider les acquis Les points clefs de la formation et leur mise en œuvre opérationnelle

PRÉREQUIS

Ordinateur connecté à internet avec sortie audio, équipé d'un micro.

COMPÉTENCES ATTESTÉES

1 Introduction à la cybersécurité et à la gestion des risques

Ce module introduit les concepts fondamentaux de la cybersécurité et met en lumière les principales menaces qui pèsent sur les entreprises. Les participants apprendront à identifier les risques, à comprendre leur impact et à appliquer les bases de la gestion des risques à travers un exercice pratique.

2 Sensibilisation aux principales réglementations

Les participants découvriront les principales réglementations en matière de cybersécurité, telles que la directive NIS2, le RGPD et la norme ISO 27001. À travers des études de cas, ils analyseront les obligations légales des entreprises et travailleront sur l'amélioration d'une charte informatique existante.

3 Création et mise en œuvre d'une charte informatique

Ce module permet d'acquérir les compétences nécessaires pour concevoir une charte informatique adaptée aux besoins de l'entreprise. Les participants identifieront les éléments clés d'une charte efficace et rédigeront leur propre document à travers des ateliers collaboratifs.

4 Types d'attaques cybernétiques et méthodes de défense

Les participants exploreront les différentes cyberattaques, comme le phishing, les attaques DDoS ou l'ingénierie sociale. Ils apprendront les méthodes de protection adaptées et mettront en pratique leurs connaissances à travers une simulation d'attaque et une analyse des réponses aux incidents.

5 Gestion de crise cyber

Ce module enseigne les étapes essentielles pour gérer une crise de cybersécurité, de la détection d'une attaque à la récupération des systèmes. À travers une simulation en groupe, les participants élaboreront un plan de réponse aux incidents et apprendront à coordonner leurs actions face à une menace réelle.

6 Gouvernance de la cybersécurité

Les participants découvriront comment structurer une gouvernance efficace en cybersécurité en définissant des rôles, des responsabilités et des processus adaptés. Ils apprendront à élaborer des politiques de sécurité et à mettre en place un comité de gestion des risques pour leur organisation.

7 Analyse des risques et gestion des vulnérabilités

Ce module aborde les méthodologies d'évaluation des risques et de gestion des vulnérabilités, en s'appuyant sur des standards tels que l'ISO 27005 et EBIOS. Les participants réaliseront un audit de sécurité et apprendront à classer et prioriser les vulnérabilités identifiées.

8 Gestion de la continuité des activités et plan de reprise après sinistre

Les participants découvriront comment structurer une gouvernance efficace en cybersécurité en définissant des rôles, des responsabilités et des processus adaptés. Ils apprendront à élaborer des politiques de sécurité et à mettre en place un comité de gestion des risques pour leur organisation.

9 Formation et sensibilisation continue

Ce module forme les participants à leur rôle de référents en sensibilisation à la cybersécurité. Ils apprendront à concevoir et animer des campagnes de sensibilisation efficaces, en utilisant des supports variés et des méthodes pédagogiques adaptées aux différents publics.

PRÉREQUIS

Ordinateur connecté à internet avec sortie audio, équipé d'un micro.

COMPÉTENCES ATTESTÉES

10 Veille technologique et mise à jour des connaissances

Les participants découvriront comment rester à jour face aux évolutions constantes des menaces et technologies en cybersécurité. Ils apprendront à mettre en place une veille efficace et à exploiter les sources d'information pour adapter les stratégies de protection de leur entreprise.

DURÉE DE LA FORMATION

Cette formation se déroule sur une période totale de 70h (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", E-learning via une plateforme LMS ou en présentiel.

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@high-jack.fr afin d'adapter au mieux la formation à vos besoins spécifiques.

MODALITÉS D'ÉVALUATION

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

MÉTHODES ET SUPPORTS PÉDAGOGIQUES

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

TARIFS : 2800 €/HT

HIGH JACK

REIMS, NANCY, LIMOGES



Siège social : 74 rue du Docteur Lemoine, 51100 Reims



contact@high-jack.fr



03 10 45 40 01