FORMATION CYBERSÉCURITÉ NIVEAU 2

High Jack forme les participants aux principaux concepts, pratiques et outils de la cybersécurité pour renforcer la sécurité numérique des entreprises et protéger les données sensibles.

FORMATION PRÉSENTIEL ET DISTANTIEL

OBJECTIFS

- Se protéger des attaques
- Concevoir des mots de passe sécurisés et les gérer
- Se prévenir du phishing
- Comprendre le fonctionnement des systèmes et des réseaux
- Savoir protéger ses informations

PROGRAMME

Module 1 : introduction à la cybersécurité

- Comprendre les enjeux de la cybersécurité.
- Les acteurs et les motivations des cyberattaques
- Connaitre les principaux types d'attaques, les menaces et vulnérabilités
- Comprendre et savoir appliquer les meilleures pratiques en matière de sécurité informatique

Module 2 : la sécurité des réseaux

- Comprendre le fonctionnement des différents types de réseaux informatiques
- Savoir reconnaitre les différents types d'adressages des réseaux
- Comprendre le fonctionnement des principaux protocoles
- Appréhender les principales techniques de sécurisation des réseaux locaux (LAN) et sans fil (Wi-Fi)
- Comprendre le fonctionnement des principaux équipements de protection des réseaux
- Savoir déjouer les attaques par déni de service

Etudes ressources pédagogique

- Pouvoir acquérir de manière autonome une culture générale dans le domaine de la cybersécurité
- Obtenir un panorama de ressources d'information sur des thématiques cyber en relation avec l'actualité

PROGRAMME

Module 3 : la sécurité des données

- Comprendre les principes fondamentaux de la sécurisation des informations et savoir protéger ses données
- Comprendre les mécanismes de chiffrement des informations et savoir chiffrer ses données sensibles
- Cryptographie : comprendre les différences entre les chiffrements symétriques et asymétriques
- Connaitre les mécanismes permettant de chiffrer et de signer les courriers électroniques
- Savoir utiliser les moyens de transmissions des informations en environnement sécurisé

Module 4 : la sécurité sectorielle

- Comprendre les spécificités sectorielles de la cybersécurité.
- Appréhender les techniques d'attaques au travers d'exemples concrets en surface de vente, en milieu industriel, en zone tertiaire, etc.

Module 5 : les normes et réglementations

- Connaitre les objectifs des principales normes et réglementations du domaine numérique
- Comprendre les enjeux des normes ISO 27001 pour le management de la sécurité informatique
- Appréhender les principes fondamentaux de la gestion des risques au travers de la norme ISO 27005
- Acquérir les principes réglementaires liés à la gestion des données à caractère personnel
- Comprendre les enjeux législatifs des principaux articles du code pénal
- Découvrir les principes fondamentaux des réglementations sectorielles (DORA, NIS 2, LPM, etc)
- Connaitre les risques liés aux lois extraterritoriales

ORGANISATION

Restitution et bilan de la formation + livret bonnes pratiques

- Obtenir un retour d'expérience sur les acquis de la formation
- Etablir un référentiel des bonnes pratiques immédiatement applicables en milieu professionnel ou privé
- Questionnaire à choix multiples permettant de vérifier les acquis

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
2	S	Module formation : introduction à la cybersécurité
2	S	Module formation : la sécurité des réseaux informatiques
2	A	Etudes ressources pédagogiques
2	S	Module formation : la sécurité des données
2	S	Module formation : les normes et réglementations du cyberespace
2	S	Module formation : la sécurité informatique par secteur d'activité
7	A	Mises en situation ciblées : deuxième session
0,5	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

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 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", E-learning via une plateforme LMS ou 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

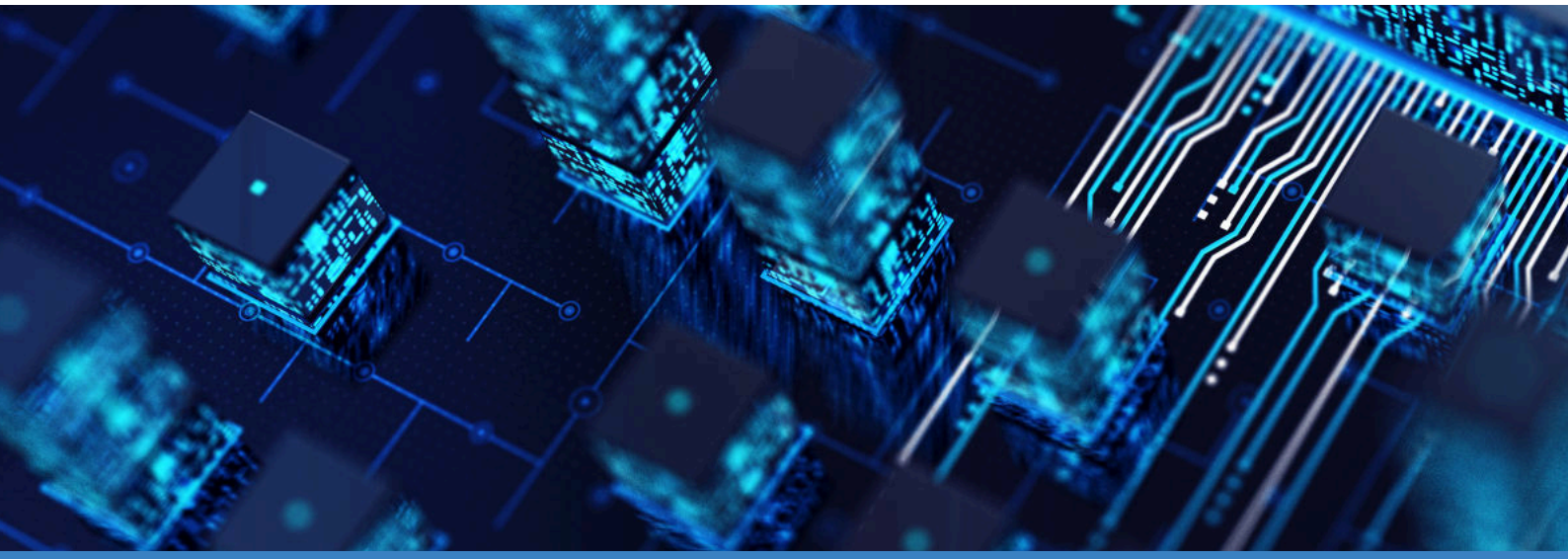
- Évaluations formatives : QCM, comptes rendus...
- Évaluations sommatives : QCM, comptes rendus...
- Évaluation de satisfaction

MÉTHODES ET SUPPORTS PÉDAGOGIQUES

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

HIGH JACK

REIMS, NANCY, LIMOGES



HIGHJACK
CYBER-SÉCURITÉ

Siège social : 74 rue du Docteur Lemoine, 51100 Reims

contact@high-jack.fr

03 10 45 40 01

VERSION 3 - JANVIER 2025