



HIGHJACK

CYBERSÉCURITÉ

FORMATION CYBERSÉCURITÉ NIVEAU 1

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

Parcours pédagogique

Pour appréhender efficacement les principales thématiques de la cybersécurité et de la protection de l'information, il faut connaître les bases du fonctionnement de l'écosystème numérique tels que les systèmes et les réseaux informatiques.

La formation s'articule donc en différents modules théoriques et aussi de mises en situations pratiques proposant aux apprenants d'acquérir progressivement les bases technologiques nécessaires pour ensuite appréhender sereinement les aspects pratiques de la cybersécurité afin de savoir comment :

- Assurer la continuité opérationnelle des activités
- Conserver l'avantage concurrentiel
- Rester en conformité avec la législation

Objectifs pédagogiques

- Maîtriser les bases du fonctionnement des réseaux informatiques pour mieux se protéger des attaques
- Comprendre les techniques opérationnelles de protection des flux véhiculés sur les réseaux informatiques
- Maîtriser les enjeux de la cybersécurité
- Concevoir des mots de passe sécurisés et les gérer au quotidien
- Connaître les principaux moyens de protection des données et assurer la confidentialité des affaires
- Savoir détecter les attaques réseau et interpréter les événements détectés par une sonde réseau (DETOXIO)
- Se prévenir des attaques par malice informatique (phishing, liens sites internet frauduleux, etc...)
- Connaître les principales normes et réglementations du domaine numérique

Évaluation des atteintes des objectifs

Un questionnaire à choix multiples est présenté pour chaque objectif pédagogique.

Mises en pratique

- **Savoir comprendre et interpréter les flux réseaux**

Afin de comprendre et de pouvoir ensuite maîtriser les flux présents sur le réseau informatique de l'entreprise, la formation inclut une phase d'installation d'une sonde réseau (DETOXIO) qui sera positionnée en coupure de l'accès internet de l'entreprise. Cette sonde permet de visualiser l'ensemble des flux entrants et sortants du système d'information afin d'en détecter les flux toxiques et d'établir une cartographie des équipements présents sur le réseau de l'entreprise. C'est avec ce type de sonde qu'il est possible de déterminer la légitimité des flux véhiculés sur le réseau et des équipements y étant connectés. La maîtrise des flux réseaux est un point fondamental pour comprendre les cyberattaques.

- **Savoir se protéger des technologies d'extraction ou d'interception des informations**

Présentation de matériels spécifiques permettant aux apprenants de comprendre les techniques d'interception de données de leurs smartphones ou de compromission de leurs ordinateurs au travers de clefs ou de câbles USB actifs.

- **Savoir déjouer les attaques par malice informatique.**

Réalisation de mises en situation via des techniques de phishing en plusieurs étapes afin de démontrer aux apprenants la nécessité du maintien de la vigilance face aux éléments reçus via les messageries ou directement via les sollicitations des systèmes. Les mises en situation sont dans un premier temps, identiques aux attaques courantes sur internet, puis dans un deuxième temps, pour les formations de 28h, les simulations d'attaques sont spécifiquement contextualisées pour l'organisation afin que les apprenants puissent connaître les techniques employées par les cybercriminels ciblant leur entreprise

- **Savoir interpréter la criticité des vulnérabilités découvertes lors des tests de recherches de vulnérabilités.**

Réalisation par l'équipe High Jack d'un Pentest Flash© permettant de mettre en évidence les vulnérabilités éventuelles du système d'information et élaboration d'un rapport de test avec une proposition de plan de remédiation. Cette mise en situation permet aux apprenants de comprendre le niveau de robustesse de leur système d'information et de pouvoir prendre les décisions nécessaires afin de réduire la surface d'exposition au risque.

PROGRAMME

Module 1 : introduction à la cybersécurité

- Comprendre les enjeux de la cybersécurité.
- Les acteurs et les motivations des cyberattaques
- Connaître 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 reconnaître 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

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
- Connaître les mécanismes permettant de chiffrer et de signer les courriers électroniques
- Savoir utiliser les moyens de transmissions des informations en environnement sécurisé

PROGRAMME

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

- Connaître 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)
- Connaître 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 1 14 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 cyberspace
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

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 étudieront 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 connaîtront 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@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.



HIGHJACK

CYBERSÉCURITÉ

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

Parcours pédagogique

Pour appréhender efficacement les principales thématiques de la cybersécurité et de la protection de l'information, il faut connaître les bases du fonctionnement de l'écosystème numérique tels que les systèmes et les réseaux informatiques.

La formation s'articule donc en différents modules théoriques et aussi de mises en situations pratiques proposant aux apprenants d'acquérir progressivement les bases technologiques nécessaires pour ensuite appréhender sereinement les aspects pratiques de la cybersécurité afin de savoir comment :

- Assurer la continuité opérationnelle des activités
- Conserver l'avantage concurrentiel
- Rester en conformité avec la législation

Objectifs pédagogiques

- Maîtriser les bases du fonctionnement des réseaux informatiques pour mieux se protéger des attaques
- Comprendre les techniques opérationnelles de protection des flux véhiculés sur les réseaux informatiques
- Maîtriser les enjeux de la cybersécurité
- Concevoir des mots de passe sécurisés et les gérer au quotidien
- Connaître les principaux moyens de protection des données et assurer la confidentialité des affaires
- Savoir détecter les attaques réseau et interpréter les événements détectés par une sonde réseau (DETOXIO)
- Se prévenir des attaques par malice informatique (phishing, liens sites internet frauduleux, etc...)
- Connaître les principales normes et réglementations du domaine numérique

Évaluation des atteintes des objectifs

Un questionnaire à choix multiples est présenté pour chaque objectif pédagogique.

Mises en pratique

- **Savoir comprendre et interpréter les flux réseaux**

Afin de comprendre et de pouvoir ensuite maîtriser les flux présents sur le réseau informatique de l'entreprise, la formation inclut une phase d'installation d'une sonde réseau (DETOXIO) qui sera positionnée en coupure de l'accès internet de l'entreprise. Cette sonde permet de visualiser l'ensemble des flux entrants et sortants du système d'information afin d'en détecter les flux toxiques et d'établir une cartographie des équipements présents sur le réseau de l'entreprise. C'est avec ce type de sonde qu'il est possible de déterminer la légitimité des flux véhiculés sur le réseau et des équipements y étant connectés. La maîtrise des flux réseaux est un point fondamental pour comprendre les cyberattaques.

- **Savoir se protéger des technologies d'extraction ou d'interception des informations**

Présentation de matériels spécifiques permettant aux apprenants de comprendre les techniques d'interception de données de leurs smartphones ou de compromission de leurs ordinateurs au travers de clefs ou de câbles USB actifs.

- **Savoir déjouer les attaques par malice informatique.**

Réalisation de mises en situation via des techniques de phishing en plusieurs étapes afin de démontrer aux apprenants la nécessité du maintien de la vigilance face aux éléments reçus via les messageries ou directement via les sollicitations des systèmes. Les mises en situation sont dans un premier temps, identiques aux attaques courantes sur internet, puis dans un deuxième temps, pour les formations de 28h, les simulations d'attaques sont spécifiquement contextualisées pour l'organisation afin que les apprenants puissent connaître les techniques employées par les cybercriminels ciblant leur entreprise

- **Savoir interpréter la criticité des vulnérabilités découvertes lors des tests de recherches de vulnérabilités.**

Réalisation par l'équipe High Jack d'un Pentest Flash© permettant de mettre en évidence les vulnérabilités éventuelles du système d'information et élaboration d'un rapport de test avec une proposition de plan de remédiation. Cette mise en situation permet aux apprenants de comprendre le niveau de robustesse de leur système d'information et de pouvoir prendre les décisions nécessaires afin de réduire la surface d'exposition au risque.

Moyens pédagogiques spécifiques

- Mise à disposition d'un équipement permettant de faire des analyses des flux réalisés sur le réseau de l'entreprise
- Utilisation d'outils spécifiques permettant d'effectuer des mises en situations afin d'apprendre à déjouer les attaques par malice informatique
- Réalisation d'un PENTEST FLASH© avec production d'un rapport d'analyse et de plan d'action pour effectuer les remédiations nécessaires
- Utilisation de matériel (Câbles, clefs USB, etc) permettant d'appréhender des techniques de compromissions simples sur les moyens de communication (ordinateurs et smartphones)

Phases d'apprentissage

- **Phases d'apprentissage synchrone** : les modules de formation sont dispensés en visio conférence et/ou en présentiel suivant un planning prédéfini.
- **Phases d'apprentissage asynchrones** :
 - Enseignement individuel au moyen de support pédagogiques digitaux et de ressources documentaires
 - Chaque apprenant peut acquérir les connaissances à son rythme et n'est pas contraint par un rythme de groupe
 - En complément, une plateforme de ressources pédagogiques en ligne est mise à disposition des apprenants pendant les différentes phases de la formation

Engagement du tour de table initial

- Échanger sur les pratiques et l'expérience formative de chacun
- Confronter les retours d'expériences
- Confronter les attentes de chacun

Mises en situation pratique

- Connaître les principales attaques par malice informatique
- Savoir détecter les courriers électroniques à caractère frauduleux et les sollicitations douteuses telles que l'arnaque au dirigeant, au faux support technique, etc
- Comprendre les techniques utilisées pendant les mises en situations et identifier les points d'amélioration à travailler pour limiter la surface d'exposition du risque lié aux attaques par malice informatique
- Savoir détecter les messages et autres types de sollicitations à caractère frauduleux qui ont été spécifiquement créés pour duper les utilisateurs et les inciter à transmettre des informations sensibles
- Restitution personnalisée pour chaque mise en situation pratique ciblées

PROGRAMME

Module 1 : introduction à la cybersécurité

- Comprendre les enjeux de la cybersécurité.
- Les acteurs et les motivations des cyberattaques
- Connaître 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 reconnaître 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

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
- Connaître les mécanismes permettant de chiffrer et de signer les courriers électroniques
- Savoir utiliser les moyens de transmissions des informations en environnement sécurisé

PROGRAMME

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

- Connaître 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)
- Connaître 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 cyberspace
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 étudieront 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 connaîtront 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@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.



FORMATION RÉFÉRENT CYBER

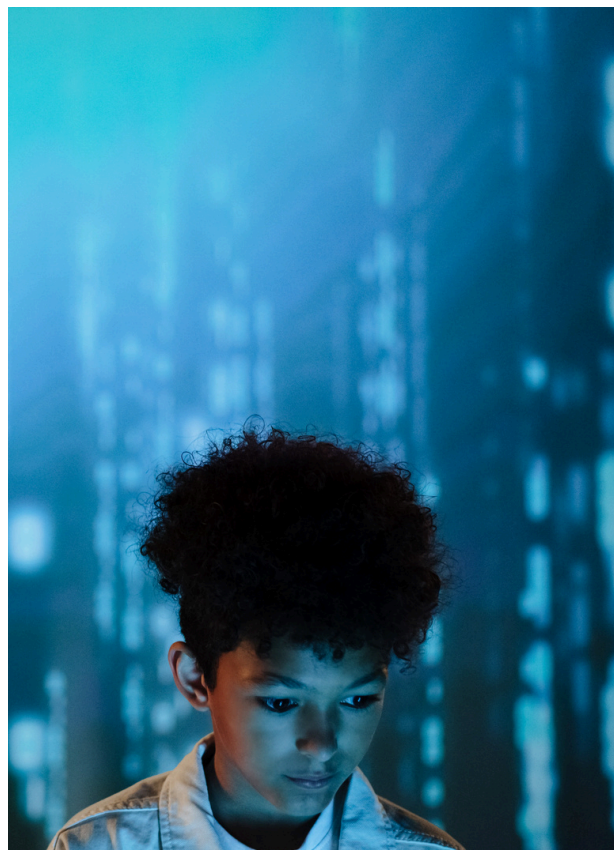
High Jack offre une formation intensive qui permettra aux participants de devenir des référents cybersécurité compétents, capables de gérer et de coordonner les initiatives de cybersécurité au sein de leur organisation.

FORMATION PRÉSENTIEL
ET DISTANCIEL

DEVENEZ RÉFÉRENT CYBER POUR VOTRE ENTREPRISE

Le rôle du Référent Cyber (RC) consiste à accompagner la Direction dans l'organisation et la gestion de la sécurité informatique, afin de garantir la continuité des activités, préserver la compétitivité de l'entreprise et assurer le respect des réglementations en vigueur dans le domaine numérique.

Le RC connaît l'entreprise, son organisation, ses besoins et ses contraintes. Il occupe donc une position centrale dans l'organisation de la relation entre l'entreprise et ses prestataires informatiques, en agissant de manière complémentaire à leurs actions.



Véritable relais de confiance, il permet à la direction de s'appuyer sur un collaborateur compétent pour piloter efficacement un enjeu stratégique qu'est la cybersécurité des moyens numériques de l'entreprise.

Le RC ne se substitue pas aux prestataires déjà engagés par l'entreprise, mais en assure la coordination afin d'optimiser la cohérence et l'efficacité des interventions.

Cette coordination est essentielle, car les prestataires et fournisseurs ne maîtrisent pas toujours l'ensemble des spécificités et mécanismes internes de l'entreprise, pourtant déterminants pour la réussite de leurs missions.

Dans ce contexte, le rôle du RC prend toute sa dimension, devenant un atout stratégique et un partenaire de confiance pour l'entreprise. Il constitue un véritable soutien pour la direction, en la libérant des préoccupations techniques afin qu'elle puisse se concentrer pleinement sur la création de valeur.

DEVENEZ RÉFÉRENT CYBER POUR VOTRE ENTREPRISE

Caractéristiques

- Formation opérationnelle en cybersécurité adaptée aux TPE et PME.
- Modules pratiques : gouvernance, gestion de crise, continuité d'activité, protection des données, relations avec les prestataires IT.
- Accessible à toute personne de confiance dans l'entreprise, il n'est pas nécessaire d'être un expert informatique.
- Durée 70H réparties en 10 modules combinant théorie, et mises en situations pratiques directement utilisables par l'entreprise
- Livrables fournis : fiches pratiques, modèles de PSSI, PCA, PRI, chartes informatiques, etc.

Avantages

- Permet de structurer la cybersécurité sans dépendre uniquement des prestataires informatiques.
- Crée un pont entre la direction et les prestataires techniques.
- Favorise une meilleure maîtrise des risques numériques internes et externes.
- Met en place une démarche continue de protection des activités de l'entreprise.
- Contribue à la conformité réglementaire (ex : RGPD, LPM, NIS2).
- Exclusivement dispensée en distanciel, elle permet aux collaborateurs de rester au sein de l'entreprise sans pénaliser leurs activités quotidiennes.

Bénéfices

- Gain en sérénité pour la direction : le référent cyber devient un interlocuteur de confiance en interne.
- Moins de pertes de temps et d'argent liés à des incidents informatiques évitables.
- Valorisation de l'entreprise auprès des partenaires, clients et assureurs.
- Meilleure capacité de réaction face aux cyberattaques, pannes ou incidents.
- Permet à la direction de se concentrer sur son cœur de métier, en confiant la veille et la coordination cybersécurité à une personne formée et de confiance.

OBJECTIFS DE LA FORMATION



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

Les participants apprennent à comprendre les notions fondamentales de la cybersécurité et à appliquer les bases de la gestion des risques à travers un exercice pratique.

2 Sensibilisation aux principales réglementations

Les participants sont capables de comprendre les obligations légales (directive NIS2, RGPD, ISO 27001) et de les analyser dans le cadre d'une charte informatique existante.

3 Création et mise en œuvre d'une charte informatique

Les participants apprennent à analyser les besoins de l'entreprise et à concevoir une charte informatique personnalisée, en mobilisant des ateliers collaboratifs.

4 Types d'attaques cybernétiques et méthodes de défense

Ils explorent les différents types de cyberattaques, appliquent des méthodes de défense et évaluent l'efficacité de leur réponse via des simulations.

5 Gestion de crise cyber

Les participants comprennent les étapes d'une gestion de crise, élaborent un plan de réponse et analysent des scénarios d'incidents en groupe.

6 Gouvernance de la cybersécurité

Ils identifient les rôles, responsabilités et processus d'une gouvernance efficace et créent des politiques de sécurité ainsi qu'un comité de gestion des risques.

7 Analyse des risques et gestion des vulnérabilités

À partir des standards ISO 27005 ou EBIOS, les participants réalisent un audit de sécurité et évaluent les vulnérabilités pour les classer et les prioriser.

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

Ils comprennent les principes de continuité d'activité et créent des politiques adaptées pour assurer la résilience des systèmes en cas de crise.

9 Formation et sensibilisation continue

Les participants appliquent des techniques d'animation de sensibilisation et créent des supports pédagogiques adaptés à différents publics.

10 Veille technologique et mise à jour des connaissances

Ils apprennent à comprendre les enjeux d'une veille efficace, à évaluer les sources d'information pertinentes et à créer une stratégie de veille adaptée à leur organisation.

PRÉREQUIS

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

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.

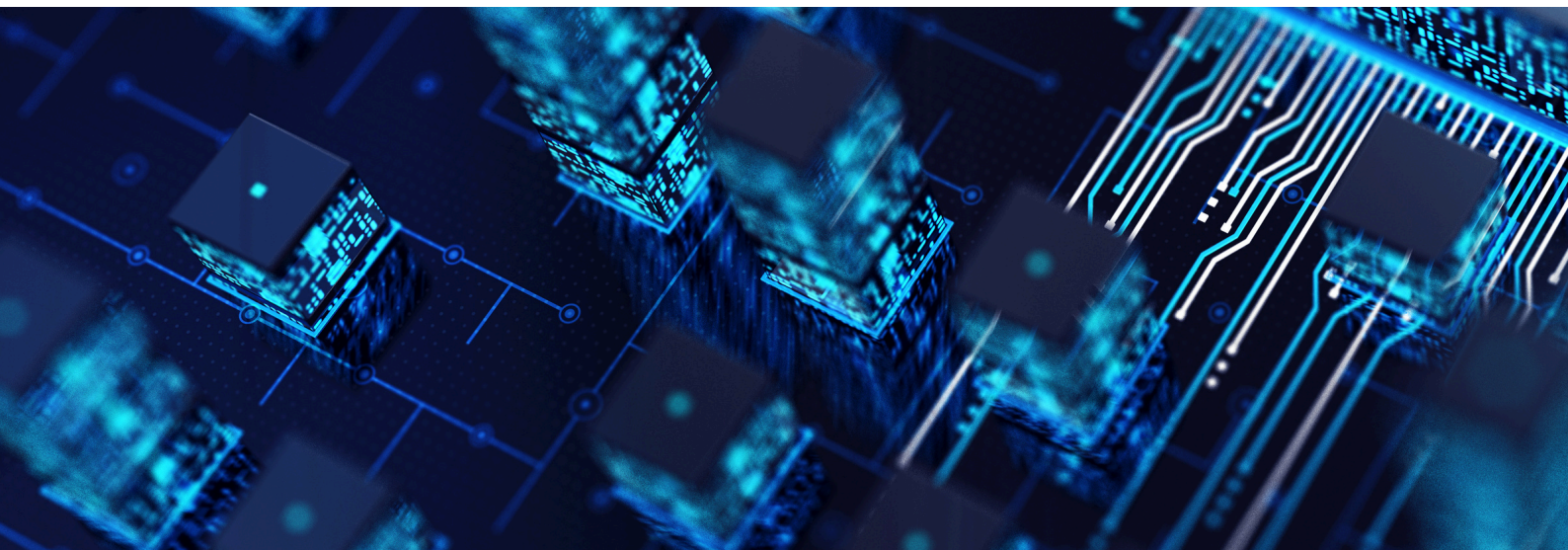
FORMATEUR

- Cyrille ELSEN : DSI et directeur des programmes de formation

TARIF PAR STAGIAIRE: 2 800 €HT
TARIF DE GROUPE SUR DEMANDE

HIGH JACK

REIMS, NANCY, LIMOGES



Siège social : 74 rue du Docteur Lemoine, 51100 Reims



contact@high-jack.fr



03 10 45 40 01