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 connaitre 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

- Maitriser 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
- Maitriser les enjeux de la cybersécurité
- Concevoir des mots de passe sécurisés et les gérer au quotidien
- Connaitre 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...)
- Connaitre 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 maitriser 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 maitrise 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 connaitre 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

- Connaitre 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
- 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

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

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

- 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 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

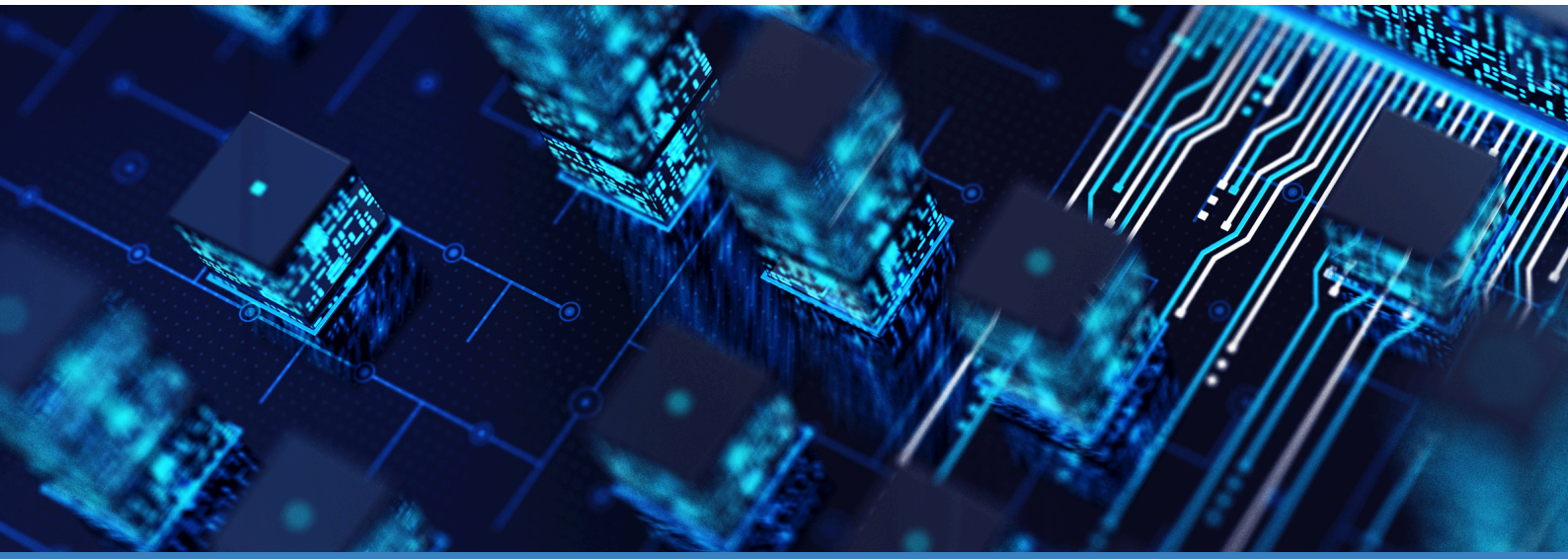
MÉTHODES ET SUPPORTS PÉDAGOGIQUES

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

TARIFS 28H : 1120€/HT

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

High-jack.fr © 2024 : tous droits réservés. Reproduction interdite sans autorisation.
DETOXIO, et SERENICITY CONTROL sont des marques déposées par SERENICITY.