Formation Les essentiels de la Cybersécurité

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Cette formation est délivrée en synchrone à distance tout en garantissant l'accès à un environnement d'apprentissage complet! Ce module de formation permet de présenter les bases de la cybersécurité. Il permettra de comprendre les problématiques et les enjeux de la sécurité informatique, d'identifier ses différents acteurs, ainsi que de comprendre son organisation. Il sert d'introduction aux modules avancés en cybersécurité.

Référence	CYBER
Durée	3 jours (21h)
Tarif	2 390 €HT
Repas	60 €HT(en option)

Objectifs

| Expliquer les enjeux de la cybersécurité
| Identifier les principaux types d'attaques et leurs conséquences
| Identifier les risques juridiques autour de la cybersécurité
| Enumérer les méthodes de protection

Public

| personne souhaitant se former aux fondamentaux de la cybersécurité ou souhaitant s'orienter vers les métiers de la cybersécurité.

Prérequis

| avoir des connaissances générales des systèmes d'information et une connaissance du Guide d'hygiène de l'ANSSI et en option avoir suivi le MOOC de l'ANSSI (https://secnumacademie.gouv.fr/).

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 28 au 30 juillet 2025
du 15 au 17 septembre 2025
du 12 au 14 novembre 2025

PARIS

du 15 au 17 septembre 2025
du 12 au 14 novembre 2025

VOIR TOUTES LES DATES

Programme de la formation

Environnement général de la cybersécurité
| La définition de la sécurité
| Les acteurs de la sécurité
| Les composants de la sécurité

Organisation de la cybersécurité
| Les métiers de la cybersécurité
| Le management de la sécurité
| Rôle des Ressources Humaines
| Vérification des antécédents
| Définition des rôles
| Sensibilisation des utilisateurs

Les nouveaux enjeux
| Le phénomène de la cybersécurité aujourd'hui
| Changement de paradigme : la quantité astronomique de données à gérer, l'essor du cloud computing, l'omniprésence des systèmes d'information, etc.
| Menaces, vulnérabilités et risques dans le cyber monde

Les axes majeurs
| La cybersécurité d'un point de vue juridique
| La cybersécurité d'un point de vue organisationnel
| La cybersécurité d'un point de vue technique
| La cybersécurité d'un point de vue humain : l'ingénierie sociale
| La gestion des risques : ?définition du risque, définition de la vulnérabilité, la

menace, l'impact.
| Cycle de vie de gestion de risques : identification, appréciation, traitement, réponse

La cybersécurité d'un point de vue juridique
| Le cadre légal de la cybersécurité
| Les risques juridiques et les solutions
| La cybersécurité du point de vue du droit
| Périmètre et domaines d'application de la loi en matière de cyber sécurité : exemple, le RGPD, la territorialité des données
| Le rôle des autorités de contrôle, le rôle des agences spécialisées (ANSII, Clusif, Cnil, Enisa, etc.)

L'exploitation des vulnérabilités, les différents types d'attaque et les vecteurs de compromission
| Connaître les menaces et les principales attaques du SI
| Les différents profils des attaquants
| Les différentes facettes de la cybersécurité : du codeur au hacker
| Le cyber espionnage
| La cybercriminalité
| Le cyber activisme
| Le cyber terrorisme
| La cyber guerre au service des gouvernements et de l'espionnage
| Les principaux outils utilisés lors des attaques
| Les étapes d'une attaque et savoir comment sont utilisées les vulnérabilités
| Les outils de protection (Antivirus, antispyware, pare-feu, sondes)

Labs
| Lab : Menaces et attaques (LAB 2 - G013)
| Lab : Vulnérabilités Réseau (LAB 3 - G013)
| Lab : Renforcer les services réseau (LAB 8_9701)
| Lab : Détecter les Malwares (LAB 9 - 9701)
| Lab : Surveillance des Systèmes (LAB 12 - 9701)

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.