Formation Cybersecurity Foundations

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

Cette formation permet aux participants d'avoir une vue globale des défis que présente la conception d'un système sécurisé. Au moyen d'exposés et de labs, les tendances des menaces actuelles sur l'Internet et leur impact sur la sécurité de l'organisation sont exposés. L'exploitation des failles et les remèdes existants y sont traités également.

Référence	CYB-SEC
Durée	5 jours (35h)
Tarif	3 390 €HT
Repas	100 €HT(en option)

Objectifs

| Identifier les cyber-menaces actuelles et les sites de référence sur la Cybersécurité
| Expliquer les directives et exigences de conformité
| Décrire les Cyber rôles nécessaires à la conception de systèmes sûrs
| Expliquer le cycle des attaques
| Discuter du processus de gestion des risques
| Définir les stratégies optimales pour sécuriser le réseau d'entreprise
| Mettre en oeuvre les zones de sécurité et les solutions standards de protection

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 22 au 26 septembre 2025
du 8 au 12 décembre 2025

VOIR TOUTES LES DATES

Public

| professionnels de la sécurité informatique, personnels d'exploitation, administrateurs réseau et consultants en sécurité.

Prérequis

| Connaissances en réseaux TCP/IP

Programme de la formation

Le champ de bataille
| La croissance d'Internet dans le monde entier
| Principes et objectifs de sécurité
| Terminologie des menaces et de l'exposition
| Documents et procédures de gestion des risques

Structure de l'Internet et TCP/IP
| Normes de conformité juridique
| Internet Leadership IANA
| Modèle TCP/IP

Évaluation de la vulnérabilité et outils
| Vulnérabilités et exploits
| Outils d'évaluation de la vulnérabilité
| Techniques d'attaques avancées, outils et préventions

Sensibilisation à la cyber sécurité
| Ingénierie sociale : Objectifs de l'ingénierie sociale, cibles, attaque, hameçonnage
| Sensibilisation à la cyber sécurité : Politiques et procédures

Cyber-attaques : Footprinting et scannage
| Footprinting
| Identification du réseau cible et sa portée
| Techniques de scannage de port

Cyberattaques : Effraction
| Attaque des mots de passe, escalade des privilèges
| Authentification et décodage du mot de passe

Cyberattaques : Porte dérobée et cheval de Troie (Backdoor and Trojans)
| Logiciels malveillants, Cheval de Troie, Backdoor et contre-mesures
| Communications secrètes
| Logiciel anti-espion
| Pratiques de lutte contre les logiciels malveillants

Évaluation et gestion des risques cybernétiques
| Actifs protégés : CIA Triad
| Processus de détermination de la menace
| Catégories de vulnérabilités
| Actifs de l'entreprise vs risques

Gestion des politiques de sécurité
| Politique de sécurité
| Références de politiques

Sécurisation des serveurs et des hôtes
| Types d'hôtes
| Directives de configuration générale et correctifs de sécurité
| Renforcement des serveurs et périphériques réseau
| Renforcement de l'accès sans fil et sécurité des VLAN

Sécurisation des communications
| Application de la cryptographie au modèle OSI
| Tunnels et sécurisation des services

Authentification et solutions de chiffrement
| Authentification par mot de passe de systèmes de chiffrage
| Fonctions de hachage
| Avantages cryptographiques de Kerberos
| Composants PKI du chiffrement à clef symétrique, du chiffrement asymétrique, des signatures numériques

Pare-feu et dispositifs de pointe
| Intégration de la sécurité générale
| Prévention et détection d'intrusion et défense en profondeur
| Journalisation

Analyse criminalistique
| Gestion des incidents
| Réaction à l'incident de sécurité

Reprise et continuité d'activité
| Types de catastrophes et Plan de reprise d'activité (PRA)
| Haute disponibilité
| Documentation de collecte de données
| Plan de Reprise d'Activité et Plan de Continuité d'Activité

Cyber-révolution
| Cyberforces, Cyberterrorisme et Cybersécurité : crime, guerre ou campagne de peur ?

LABS
| Lab1: Installation du lab
| Lab 2 : Comprendre TCP/IP
| Lab 3 : Evaluation de la vulnérabilité
| Lab 4 : Sensibilisation à la cybersécurité
| Lab 5 : Scannage
| Lab 6 : Cyber-attaques et mots de passe
| Lab 7 : Cyber-attaques et portes dérobées
| Lab 8 : Évaluation des risques
| Lab 9 : Stratégies de sécurité
| Lab 10 : Sécurité hôte

| Lab 11 : Communications secrètes
| Lab 12 : Authentification et cryptographie
| Lab 13 : Snort IDS
| Lab 14 : Analyse criminalistique
| Lab 15 : Plan de continuité des affaires

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.