



ORGANISME DE FORMATION AUX TECHNOLOGIES ET METIERS DE L'INFORMATIQUE

Formation Cyber & IT Security Foundation

N° ACTIVITÉ : 11 92 18558 92

TÉLÉPHONE : 01 85 77 07 07

E-MAIL : inscription@hubformation.com

Cette formation Cyber & IT Security Foundation permet aux participants d'acquérir les compétences et connaissances nécessaires pour comprendre et maîtriser tous les aspects techniques de la sécurité de l'information. Elle constitue la base de toute autre formation spécialisée en sécurité informatique. Celle-ci prépare à l'obtention de la certification EXIN. Un voucher sera remis à chaque participant; il devra programmer le passage de son examen ultérieurement.

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

Objectifs

- | Expliquer le fonctionnement d'un réseau local, identifier les types de serveurs et les différents systèmes d'exploitation
- | Identifier les vulnérabilités des systèmes
- | Sécuriser le poste de travail et les serveurs
- | Expliquer le concept du développement d'application et de la nécessité d'en sécuriser les différentes étapes
- | Expliquer les modèles de SGBD et leurs fonctionnalités
- | Sécuriser les applications et les bases de données
- | Identifier les méthodes de cryptographie
- | Contrôler les accès et la gestion des identités
- | Expliquer le Cloud et ses vulnérabilités

Public

| Administrateur réseau, Développeur d'applications, Spécialiste sécurité, Auditeur, Responsable qualité, Directeur opérationnel

Prérequis

| Avoir suivi le cours HF-RES1, Les bases du réseau, ou posséder les connaissances équivalentes.

Programme de la formation

Fonctionnement d'un réseau local

- | Caractéristiques d'un réseau
- | Les modèles OSI et TCP/IP
- | Commutation et Routage
- | Les équipements
- | Applications, protocoles et services
- | Les organismes

Les systèmes

- | Présentation des systèmes (ordinateurs et serveurs)
- | Rappels des différents composants, Types de serveurs
- | Rappel des principaux systèmes d'exploitation
- | (Systèmes Windows, Unix et Linux. Présentation des annuaires LDAP et des OS mobiles
- | Identification des principales vulnérabilités des systèmes
- | Sécurisation des postes de travail et des serveurs

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 2 au 4 juin 2025

du 12 au 14 novembre 2025

PARIS

du 2 au 4 juin 2025

du 12 au 14 novembre 2025

[VOIR TOUTES LES DATES](#)

Applications et bases de données

- | Description des concepts du développement d'applications
- | Prise en compte de la sécurité pendant au cours du développement
- | Rappels du principe des bases de données
- | Description des différents modèles de SGBD et de leurs fonctionnalités
- | Description des problèmes de sécurité liés au développement des applications et des bases de données
- | Sécurisation des applications et des bases de données

Cryptographie

- | Présentation de la cryptographie
- | Chiffrement symétrique et asymétrique
- | Méthodes de hachage, signature numérique
- | Infrastructures à clés publiques (PKI) et certificats numériques
- | Sécurisation des communications avec SSL et IPSec

Contrôle d'accès et gestion des identités

- | Identification et authentification
- | Biométrie, certificats, token
- | Gestion des mots de passe
- | Authentification forte (two-factor authentication)
- | SSO (Single Sign-on)
- | Principes d'autorisation
- | Gestion des autorisations (ACM, DAC, MAC, RBAC, ABAC)

Le Cloud Computing

- | Caractéristiques du Cloud Computing
- | Modèles de déploiement (public cloud, private cloud et hybrid cloud)
- | Les différents types (SaaS, PaaS, IaaS, SECaaS, IDaaS)
- | Identifier les risques liés au Cloud Computing

L'exploitation des vulnérabilités

- | Identifier les différents types d'attaques
- | Identifier les acteurs de la cyber criminalité
- | Connaître les outils des attaquants
- | Identifier les étapes permettant d'exploiter des vulnérabilités

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.