

Cyber & IT Security Foundation

Durée: 3 Jours Réf de cours: EXCISF

Résumé:

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.

Public visé:

Sont concernés par cette formation et certification les publics suivants : Administrateur réseau, Développeur d'applications, Spécialiste sécurité, Auditeur, Responsable qualité, Directeur opérationnel

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
 - 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
- Comprendre les méthodes de cryptographie
- Contrôler les accès et la gestion des identités
- Expliquer le Cloud et ses vulnérabilités

Pré-requis:

Avoir suivi le cours GKRES1, Les bases du réseau, ou posséder les connaissances équivalentes.

Test et certification

Un voucher sera remis à chaque participant afin qu'il puisse planifier le passage de l'examen en ligne selon les créneaux disponibles à l'issue de la formation.

L'examen dure environ 1 heure. Celui-ci se compose d'un QCM d'environ 40 questions, et les candidats doivent atteindre au moins 65% de bonnes réponses pour obtenir la certification.

Contenu:

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

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

Méthodes pédagogiques :

Support de cours en français accrédité par l'EXIN.

Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur globalknowledge.fr/handicap
- Le Règlement intérieur est disponible sur globalknowledge.fr/reglement