Les essentiels de la cybersécurité

Hard Skills : Bureautique - Informatique -Comptabilité - Gestion

Cybersécurité / RGPD

Référence : 4-IT-CYBA
Durée : 5 jours
Présentiel ou en classe à distance

Tarif Inter : 750 € Prix HT jour / personne
Tarif Intra : 1500 € Prix HT jour / groupe

Mise à jour : 27/11/2023

Durée de validité : du 01/01/2025 au 31/12/2025

Objectifs

- Présentation des cyber-menaces actuelles et sites de référence sur la cybersécurité
- Directives et exigences de conformité
- Cyber rôles nécessaires à la conception de systèmes sûrs
- Cycle des attaques processus de gestion des risques
- Stratégies optimales pour sécuriser le réseau d'entreprise
- Zones de sécurité et solutions standards de protection

Prérequis

Connaissances en réseaux TCP/IP

Public concerné

Professionnels de la sécurité informatique, personnels d'exploitation, administrateurs réseau et consultants en sécurité

Contenu pédagogique

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

Moyens pédagogiques

- Réflexion de groupe et apports théoriques du formateur.
- Travail d'échange avec les apprenants sous forme de réunion – discussion.
- Utilisation de cas concrets issus de l'expérience professionnelle.
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques.
- Alternance entre apports théoriques et exercices pratiques (en moyenne sur 30 à 50% du temps)

Modalités pédagogiques : Présentiel, Distanciel et AFEST

Moyens techniques

En formation présentielle

Accueil des apprenants dans une salle dédiée à la formation et équipée avec :

- Ordinateurs
- Vidéo projecteur ou Écran TV interactif
- Tableau blanc ou Paper-Board

En formation distancielle

A l'aide d'un logiciel comme ® Microsoft Teams ou Zoom, un micro et une caméra pour l'apprenant.

- Suivez une formation en temps réel et entièrement à distance. Lors de la session en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise.
- L'accès à l'environnement d'apprentissage (support de cours, ressources formateur, fichiers d'exercices ...) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
- Les participants recevront une convocation avec le lien de connexion à la session de formation.
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 02 35 12 25 55 ou par email à commercial@xxlformation.com

Modalités d'évaluation

- Positionnement préalable oral ou écrit.
- Feuille de présence signée en demi-journée.
- Evaluation des acquis tout au long de la formation.
- Questionnaire de satisfaction
- Attestation de stage à chaque apprenant
- Evaluation formative tout au long de la formation.
- Evaluation sommative faite par le formateur.

Profil du formateur

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité

Adaptation pédagogique et matérielle

Si vous avez besoin d'adaptation matérielle ou pédagogique, merci de prendre contact avec notre référent Handicap par téléphone au 02 35 12 25 55 ou par email à handicap@xxlformation.com

Modalités et délais d'accès à la formation

Les formations sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.

Nos sessions INTER 2025

Sessions de formation à venir :

- Aucune session à venir pour cette formation.

Nos sessions INTRA 2025

Pour organiser cette formation en intra-entreprise, veuillez nous contacter par mail à commercial@xxlformation.com ou par téléphone au 02 35 12 25 55