PROGRAMME DE FORMATION | CYBERSECURITE PARCOURS EXPERT

Réf. : FRM- CYBEXP **Durée : 5 jours, soit 35 heures**

Public visé : Toute personne disposant d'une première expérience en sécurité informatique et souhaitant approfondir ses compétences jusqu'à un niveau expert en cybersécurité.

Prérequis : Avoir suivi au préalable la formation "Cybersécurité : parcours introductif" afin de disposer des bases nécessaires en sécurité numérique.

Objectifs pédagogiques : À l'issue du parcours Expert Cybersécurité, les apprenants seront capables de maîtriser l'analyse avancée des menaces, la sécurisation des infrastructures et la réponse aux incidents complexes. Elle développe les compétences nécessaires pour concevoir, déployer et auditer des dispositifs de sécurité robustes dans des environnements techniques exigeants. Les apprenants sont en mesure d'intervenir sur des architectures critiques et de piloter des stratégies de défense à un niveau expert.

Contenu

1 - 1ère partie (3 jours)

1.1. Initiation à la cybersécurité

- Les enjeux de la sécurité des systèmes d'information : les enjeux, pourquoi les pirates s'intéressent-ils au SI, la nouvelle économie de la cybersécurité
- Les besoins de sécurité, les notions de base et vocabulaire
- Panorama de quelques menaces
- Les différents types de Malwares

Exemples de cas pratiques :
Mise en œuvre d'attaques connues et leurs modes opératoires

1.2. Les bases de la sécurité numérique

- Détection de tentatives d'hameçonnage
- Identification des courriels indésirables ou dangereux
- Navigation sur Internet en toute sécurité
- Maîtrise des données personnelles et des informations de navigation
- Génération de mots de passe robustes
- Protection de la vie privée en ligne
- Gérer son e-réputation
- Chiffrement des données
- Protection de l'ordinateur
- Précautions relatives à la sécurité

Exemples de cas pratiques :
Mise en situation de tentative d'hameçonnage, application des procédures de cybersécurité telle que les mots de passe, la détection phishing et les protections standards.

2 - 2ème partie (2 jours)

2.1. Sécurité des échanges et cryptographie

- Les besoins en cryptographie
- Les crypto-systèmes symétriques et asymétriques
- Les fonctions de hachage
- Les infrastructures à clé publiques PKI
- Les certificats électroniques et les protocoles de validation
- La signature numérique
- Le protocole SSL

Exemples de cas pratiques :
Mise en en œuvre les mécanismes fondamentaux de la cryptographie, depuis les besoins de sécurité jusqu'au hachage. Savoir connaitre les PKI, les certificats électroniques, la signature numérique et le fonctionnement du protocole SSL/TLS..

2.2. La gestion de la cybersécurité au sein d'une organisation

- Intégrer la sécurité au sein d'une organisation et dans les projets : panorama des normes ISO 2700X
- Intégrer la sécurité dans les projets : sécurité dans l'ensemble du cycle de vie d'un projet
- Difficultés liées à la prise en compte de la sécurité : enjeux, implication des acteurs nécessaires, arbitrage de la sécurité selon les différentes sphères
- Métiers liés à la cybersécurité

Exemples de cas pratiques :
Mise en place d'une organisation conforme aux normes ISO 2700X, avec un manuel de bonnes pratiques et une analyse des risques cybersécurité dans le cadre d'un projet.

2.3. Les enjeux et les risques liés à la gestion des données personnelles

- Le concept de vie privée
- Les empreintes laissées par vos données
- Contrôle de l'accès aux données
- Protection du transfert des données sur les réseaux
- Le cadre légal
- Exploration du RGPD

Exemples de cas pratiques :
Recherches d'empreintes sur Internet pour protéger sa vie privée, mise en place d'une RGPD via le cadre légal

Méthode pédagogique

Formation intra-entreprise délivrée en présentiel ou distanciel, personnalisée aux besoins spécifiques des stagiaires, en groupe avec un formateur spécialiste des matières abordées.

Méthodes pédagogiques actives et participatives. Alternance de théorie et de pratique avec application au contexte des participants. Le formateur alterne entre méthode démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Les stagiaires appréhenderont les fondamentaux de la cybersécurité à travers une initiation aux métiers du domaine et une présentation des lois encadrant leurs droits et devoirs. Cette formation leur permettra de comprendre les enjeux de la sécurité informatique grâce à des apports théoriques et à des travaux pratiques encadrés par le formateur. Ils seront également amenés à découvrir les principes du piratage éthique afin de mieux appréhender la protection des données, sous la supervision bienveillante du formateur.

Moyens et supports pédagogiques

La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions.
Variables suivant les formations, les moyens pédagogiques mis en œuvre sont :

- Ordinateurs, connexion internet, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

Dans le cas d'une formation sur site Entreprise, le client s'assure et s'engage à avoir toutes les ressources pédagogiques nécessaires (salle, équipements, accès internet, TV ou Paperboard…) au bon déroulement de l'action de formation conformément aux prérequis indiqués dans le programme de formation

Modalités d'évaluation et de suivi

Le formateur évalue la progression pédagogique des stagiaires tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques… Les participants complètent également un test de positionnement en amont et en aval pour valider les compétences acquises.

L'émargement des stagiaires et du formateur est réalisé chaque demi-journée afin d'assurer le suivi de l'assiduité.

Un questionnaire de satisfaction à chaud et à froid est proposé à l'issue de la formation pour mesurer la perception et l'impact de la formation.

PROGRAMME DE FORMATION | CYBERSECURITE PARCOURS EXPERT

Test de prérequis |

1- Qu'est-ce que le phishing ?

- ☐ Un type de logiciel malveillant qui crypte les fichiers de l'utilisateur
- ☐ Une technique d'attaque visant à obtenir des informations sensibles en se faisant passer pour une entité de confiance
- ☐ Une méthode pour augmenter la sécurité des mots de passe
- ☐ Un protocole de réseau sécurisé pour les transactions en ligne

2- Quel est le rôle principal d'un pare-feu dans un réseau informatique ?

- ☐ Augmenter la vitesse de la connexion Internet
- ☐ Filtrer le trafic entrant et sortant pour protéger le réseau contre les accès non autorisés
- ☐ Stocker des données de manière sécurisée
- ☐ Gérer les emails entrants et sortants

3- Quel est l'objectif principal de réaliser une analyse des risques en matière de cybersécurité ?

- ☐ Détecter les points faibles susceptibles d'être exploités dans les environnements de jeu en ligne
- ☐ Identifier et évaluer les failles de sécurité ainsi que les menaces potentielles afin de mesurer les risques associés aux informations et aux systèmes
- ☐ Justifier une augmentation des ressources financières allouées au département informatique
- ☐ Choisir les prestataires de services Internet offrant les meilleures garanties de sécurité

4- Pourquoi est-il crucial de mettre régulièrement à jour les systèmes et logiciels ?

- ☐ Pour assurer une meilleure interopérabilité avec les plateformes en ligne
- ☐ Pour remédier aux vulnérabilités identifiées et renforcer la défense contre les attaques nouvelles ou émergentes
- ☐ Pour uniquement accroître l'efficience opérationnelle du système
- ☐ Pour répondre spécifiquement aux exigences des applications de communication

5- Pourquoi est-il important de faire des sauvegardes régulières des données ?

- ☐ Pour augmenter la capacité de stockage des serveurs
- ☐ Pour prévenir la perte de données en cas de panne matérielle, de cyberattaque ou de catastrophe naturelle
- ☐ Pour améliorer la performance des applications de base de données
- ☐ Pour réduire le coût des abonnements Internet

6- Qu'est-ce que le chiffrement des données ?

- ☐ Une technique pour compresser les données et économiser de l'espace de stockage
- ☐ Le processus de transformation des données en un format illisible sans la clé de déchiffrement
- ☐ Une méthode pour augmenter la vitesse de transfert des données
- ☐ Un protocole de communication pour les réseaux sociaux

7- Quelle est la première étape à suivre lors de la détection d'une activité suspecte sur un réseau informatique ?

- ☐ Ignorer l'alerte pour éviter de perturber les opérations en cours
- ☐ Informer immédiatement l'équipe de sécurité ou le responsable de la cybersécurité
- ☐ Éteindre tous les ordinateurs pour arrêter l'attaque
- ☐ Envoyer un email à tous les utilisateurs pour les informer de la situation

8- Quelle méthode peut contribuer à sécuriser l'accès à des comptes en ligne en plus du mot de passe ?

- ☐ La navigation en mode incognito
- ☐ L'utilisation d'un gestionnaire de tâches
- ☐ L'authentification à deux facteurs (2FA)
- ☐ Le partage de mots de passe entre utilisateurs

9- Qu'est-ce qu'un VPN (Virtual Private Network) et à quoi sert-il ?

- ☐ Un outil de surveillance en ligne pour les entreprises
- ☐ Une technologie qui permet d'améliorer la qualité graphique des sites web
- ☐ Un réseau privé virtuel permettant de sécuriser les communications sur Internet
- ☐ Un dispositif de stockage pour augmenter l'espace disque des serveurs

10- Qu'est-ce que le guide d'hygiène informatique proposé par l'ANSSI vise à établir ?

- ☐ Un ensemble de pratiques pour la maintenance physique des dispositifs informatiques
- ☐ Un ensemble de stratégies destinées à renforcer la sécurité des infrastructures informatiques et à atténuer les risques d'incidents de sécurité
- ☐ Des instructions pour l'installation et la configuration efficace de solutions antivirus
- ☐ Des conseils pour améliorer l'efficacité des systèmes dédiés au divertissement numérique