CYBERSECURITE – LES FONDAMENTAUX

FORMATION

PRÉSENTATION

La Cybersécurité, aussi appelée « sécurité du numérique », est une discipline qui définit un modèle holistique de sécurité pour répondre aux menaces visant l'informatique de gestion, industrielle ou les objets connectés.
La Cybersécurité couvre la sécurité opérationnelle, la gouvernance et à la veille technologique tout en comprenant des aspects juridiques. Ce module de fondamentaux destiné à éveiller et former tous les participants de l'entreprise à ces enjeux est truffé d'exercices pratiques pour que les participants reviennent de formation également des savoir-faire techniques

PUBLIC

Toute personne dans l'entreprise amenée à manipuler un ordinateur ou tout objet connecté

Minimum : 4 participants **Maximum : 10 participants**

PRÉREQUIS

Aucun prérequis n'est demandé pour cette formation de fondamentaux

OBJECTIFS

- Connaître et comprendre les enjeux de la sécurité du SI pour s'impliquer
- Pouvoir anticiper les risques par la connaissance des points de vulnérabilité
- Comprendre les éléments à sécuriser et acquérir une vision globale des menaces digitales
- Connaître les bonnes pratiques en Cybersécurité
- Être capable de réaliser des actions simples de prévention en Cybersécurité
- Obtenir une vision globale des référentiels normatifs du domaine de la Cybersécurité, leurs avantages et leurs périmètres d'application
- Comprendre les extensions et évolutions des métiers liés à la Cybersécurité
- Comprendre le cycle et la réflexion d'un attaquant
- Bénéficier d'un retour opérationnel des spécialistes du terrain et avoir ainsi un premier aperçu de la réalité du travail à venir

DURÉE, DATES ET LIEUX

- 3 jours soit 21 heures
- Intra-entreprise : nous déployons cette formation sur devis, en distanciel ou présentiel partout en France
- Nos formations sont accessibles à tous. Pour toute situation de handicap, merci de nous contacter par téléphone au 01 43 67 32 52 ou par e-mail à l'adresse contact@fctsolutions.com

MODALITÉS PÉDAGOGIQUES ET D'ÉVALUATION

- Cette formation est disponible en mode présentiel ou distanciel (cf. fin du document)
- Envoi d'un support de cours électronique avec la convocation
- Approche dynamique et interactive via des exposés et des mises en situations
- Présentation théorique commentée et agrémentée d'exemples professionnels concrets
- Mise en commun des expériences à travers des situations actuelles et du vécu en entreprise
- QCM de validation des acquis
- Remise d'une attestation de fin de formation validant les objectifs

13, boulevard Voltaire / 75011 Paris
Tél. : 01 43 67 32 52
contact@fctsolutions.com

www.fctsolutions.com
Organisme de formation et de certification - SARL au capital de 100 000 euros / Siret n° 450 005 459 00034 / Enregistrement (ce numéro ne vaut pas agrément) n° 11 75 38 056 75
Dernière mise à jour : Mars 2023

CYBERSECURITE – LES FONDAMENTAUX

FORMATION

PROGRAMME DE LA FORMATION

JOUR 1

1/ Présentation et Introduction

- Tour de table et recensement des attentes
- Evaluation des connaissances du groupe
- Présentation du programme de formation et des objectifs

2/ Les Concepts fondamentaux

- Les enjeux de la sécurité des SI
- Les besoins de sécurité
- Les conseils pour se défendre contre ces attaques
- Cartographie des métiers de la Cybersécurité

3/ Les bonnes pratiques pour l'usager du SI

- Connaissance du SI et gestion de l'utilisateur
- Identifiants et mots de passe
- Gestion des documents et confidentialité
- Utilisation de la messagerie

Exercice pratique n°1 : Vérifier la robustesse des mots de passe

4/ Les référentiels et les certifications

- Référentiels : OWASP, ISO 27000, ANSSI, SANS, MITRE
- Les certifications pour produits : CC, CSPN
- Les certifications pour entreprises
- Les certifications pour les personnes : CEH, CISSP

5/ Sécurité de l'infrastructure

- Sécurisation d'un terminal
- Sécurisation d'un serveur
- Sécurisation physique
- Sécurité périmétrique (sécurité d'un réseau)
- Les principes d'une segmentation réseau

Exercice pratique n°2 : manipuler un firewall et créer des règles

JOUR 2

6/ Cryptographie

- Le chiffrement : fondamentaux et méthodes (symétriques et asymétriques)
- Hashage : principes fondamentaux et enjeux
- ***Exercice pratique n°3 : créer un certificat SSL et configurer un serveur HTTPS***

7/ L'analyse de risques

- Principes théoriques de l'analyse de risques
- Les limites de l'analyse de risques
- Exemples pratiques et cas concrets

8/ La sécurité applicative

- Intégrer la sécurité dans les projets
- Les concepts de sécurité applicative (Secure-SDLC, Security by Design, Shift Security to the Left
- La sécurité des applications web
- Présentation des référentiels CVE, CWE et OWASP Top10
- Bonnes pratiques de développement pour éviter les vulnérabilités applicatives
- Introduction au DevSecOps

Exercice pratique n° 4 : exploiter des failles sur un DVWA

9/ Ethical hacking et audits

- Introduction au Hacking
- Méthodologie d'audit et boîte à outil de l'auditeur
- Les différentes approches de l'audit : pentest, red team, bug bounty

10/ Les champs d'application de la Cybersécurité et l'innovation

- Le Cloud computing
- IoT et applications mobiles
- Le BIG DATA
- La Blockchain
- Le Hype cycle

13, boulevard Voltaire / 75011 Paris
Tél. : 01 43 67 32 52
contact@fctsolutions.com

www.fctsolutions.com
Organisme de formation et de certification - SARL au capital de 100 000 euros / Siret n° 450 005 459 00034 / Enregistrement (ce numéro ne vaut pas agrément) n° 11 75 38 056 75
Dernière mise à jour : Mars 2023

CYBERSECURITE – LES FONDAMENTAUX

PROGRAMME DE LA FORMATION

Jour 3

11/ La sécurité applicative

- Intégrer la sécurité dans les projets
- Les concepts de sécurité applicative (Secure-SDLC, Security by Design, Shift Security to the Left
- La sécurité des applications web
- Présentation des référentiels CVE, CWE et OWASP Top10
- Bonnes pratiques de développement pour éviter les vulnérabilités applicatives
- Introduction au DevSecOps

Exercice pratique n° 4 : exploiter des failles sur un DVWA

12/ Ethical hacking et audits

- Introduction au Hacking
- Méthodologie d'audit et boîte à outil de l'auditeur
- Les différentes approches de l'audit : pentest, red team, bug bounty
- Acquisition d'un glossaire 3 (20 termes)

13/ Les champs d'application de la Cybersécurité et l'innovation

- Le Cloud computing
- IoT et applications mobiles
- Le BIG DATA
- La Blockchain
- Le Hype cycle
- *Evaluation (quizz interactif 7)*

Exercice pratique n°5 : Analyse d'un Malware po

MODES DE DIFFUSION DE LA FORMATION

Présentiel

Cette formation peut être suivie en présentiel. Le participant reçoit par courriel une convocation indiquant les modalités d'accès à la formation. La formation est assurée entièrement par le formateur FCT Solutions sur le lieu de la formation.

Distanciel

Cette formation peut être suivie sur le mode distanciel sur simple demande.
Le participant reçoit par courriel un lien lui permettant de rejoindre la classe virtuelle à partir d'un terminal connecté à internet et disposant du son et d'une webcam intégrée (ordinateur, tablette).
En temps réel (formation synchrone), il suit la formation affichée au centre de l'écran (support de cours déroulé par le formateur) et écoute le formateur, le voit parler, peut interagir avec lui, poser des questions, faire répéter. Au même titre qu'une formation en présentiel, le formateur écoute les questions, répond, instaure le débat en temps réel, maîtrise la cadence et diffuse l'apprentissage tout en contrôlant à tout moment la bonne acquisition.

Le formateur peut diffuser sur son écran des outils pédagogiques complémentaires (tableaux, schémas, graphiques) au fur et à mesure de la formation.
Le participant est évalué pendant la formation au moyen de QCM corrigés avec le formateur afin de déterminer les acquis.
Tout au long de la formation, le participant peut interagir avec le formateur et même avec d'autres participants, toujours avec l'encadrement du formateur.

13, boulevard Voltaire / 75011 Paris
Tél. : 01 43 67 32 52
contact@fctsolutions.com

www.fctsolutions.com
Organisme de formation et de certification - SARL au capital de 100 000 euros / Siret n° 450 005 459 00034 / Enregistrement (ce numéro ne vaut pas agrément) n° 11 75 38 056 75
Dernière mise à jour : Mars 2023