LES FONDAMENTAUX DE LA CYBERSÉCURITÉ

RÉSUMÉ DE LA FORMATION

Type de diplôme : Formation qualifiante
Domaine ministériel : Sciences, Technologies, Santé

Responsable

- Prométhée Spathis

Thématique : Informatique

Public et prérequis

Toute personne souhaitant se former aux fondamentaux de la Cybersécurité ayant une culture technique ou scientifique dans le domaine d'informatique, notamment la structure des systèmes d'information.

Prérequis:

Les connaissances suivantes sont souhaitables :

- Connaissances de base sur les systèmes d'information (Composition, structure, fonctionnement, etc.) ;
- Connaissances de base sur le fonctionnement technique des systèmes d'exploitation (Linux ou/ et Windows) et des réseaux

Objectifs

Les objectifs de ce parcours sont de sensibiliser les apprenants aux enjeux liés à la sécurité des systèmes d'information (SSI) et de donner à la fois les connaissances nécessaires pour évaluer les points faibles de ces systèmes et la méthodologie de renforcement du niveau de leur sécurisation.

Ces objectifs sont atteints à travers les connaissances et les capacités acquises par ce parcours, à savoir :

- Acquérir les principes de sécurité
- Connaître les référentiels de normes de la sécurité.
- Établir une politique de sécurité des SI.
- Apprendre à organiser les processus liés à la gestion des incidents de sécurité (normes, préservation de l'intégrité des preuves techniques pour réaliser une analyse post-mortem,...)
- Identifier les menaces potentielles et les vulnérabilités critiques d'un système de sécurité.
- Acquérir des compétences en métrologie et détection d'intrusion.

Contenu

Les systèmes d'information

- Les composants du SI et leurs points faibles
- Les enjeux d'une politique de sécurité des SI

Types de réseau et interconnexion (Wifi, DMZ, VPN etc…)
Gestion des utilisateurs

- Gestion des privilèges et des moyens d'authentification
- Sensibilisation des utilisateurs

Les protocoles et leur sécurité IP, ICMP, UDP, TCP, etc…

- Méthodes de la sécurisation
- Les techniques d'attaques

La réalisation d'architectures sécurisées

- Pare feu, Reverse proxy, IDS, VPN etc…

La cryptographie

- Les techniques de chiffrement (symétrique/asymétrique, …)

- Les algorithmes de chiffrement (hachage,…)

La sécurité des applications Web
- Les différentes attaques (XSS, injection SQL, etc…)

La sécurité dans les projets
- Prise en compte de la sécurité dans le cycle de vie d'un projet
- Homologation de sécurité

L'analyse et le traitement du risque
- Ex : EBIOS

La réglementation et les normes (CNIL, RGPD, RGS, ISO27000, …)
Les tests d'intrusions et la détection des vulnérabilités (outils, méthodes, …)

Effectif : 4 à 15

Tarifs

Nous consulter

Organisation/Calendrier

Organisation

5 jours.

Tous les concepts abordés sont illustrés par de nombreuses séances pratiques.

Utilisation obligatoire du MOOC SecNumacadémie, de l'ANSSI sur la Cybersécurité

Une salle cours et une salle machine de 24 postes de travail sont dédiées à la formation.

Lieu(x)

- Campus Jussieu

Durée : 35 heures

Contacts/Inscription

Inscription

Inscription administrative

Formation Continue - email : formation.continue@sorbonne-universite.fr

Tour 14/24 - 5ème étage - 4 Place Jussieu - 75252 PARIS CEDEX 05

01 44 27 82 82 -

Evaluation/Validation

Validation : Attestation de fin de formation