Les essentiels de la Cybersécurité

Durée: 3 Jours **Réf de cours: CYBER** **Version: 2**

Résumé:

Ce module de formation permet de présenter les bases de la cybersécurité.
Il permettra de comprendre les problématiques et les enjeux de la sécurité informatique, d'identifier ses différents acteurs, ainsi que de comprendre son organisation.
Il sert d'introduction aux modules avancés en cybersécurité.

Public visé:

Cette formation s'adresse à toute personne souhaitant se former aux fondamentaux de la cybersécurité ou souhaitant s'orienter vers les métiers de la cybersécurité.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Expliquer les enjeux de la cybersécurité
- Identifier les principaux types d'attaques et leurs conséquences
- Identifier les risques juridiques autour de la cybersécurité
- Enumérer les méthodes de protection

Pré-requis:

Le stagiaire doit avoir des connaissances générales des systèmes d'information et une connaissance du Guide d'hygiène de l'ANSSI et en option avoir suivi le MOOC de l'ANSSI (https://secnumacademie.gouv.fr/).

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

- CYBNR - Cybersécurité : conformité et évolution des normes
- CYBTO - Organisation et sécurité du Système d'Information

Contenu:

Environnement général de la cybersécurité

- La définition de la sécurité
- Les acteurs de la sécurité
- Les composants de la sécurité

Organisation de la cybersécurité

- Les métiers de la cybersécurité
- Le management de la sécurité
- Rôle des Ressources Humaines
- Vérification des antécédents
- Définition des rôles
- Sensibilisation des utilisateurs

Les nouveaux enjeux

- Le phénomène de la cybersécurité aujourd'hui
- Changement de paradigme : la quantité astronomique de données à gérer, l'essor du cloud computing, l'omniprésence des systèmes d'information, etc.
- Menaces, vulnérabilités et risques dans le cyber monde

Les axes majeurs

- La cybersécurité d'un point de vue juridique
- La cybersécurité d'un point de vue organisationnel
- La cybersécurité d'un point de vue technique
- La cybersécurité d'un point de vue humain : l'ingénierie sociale
- La gestion des risques : ?définition du risque, définition de la vulnérabilité, la menace, l'impact.
- Cycle de vie de gestion de risques : identification, appréciation, traitement, réponse

La cybersécurité d'un point de vue juridique

- Le cadre légal de la cybersécurité
- Les risques juridiques et les solutions
- La cybersécurité du point de vue du droit
- Périmètre et domaines d'application de la loi en matière de cyber sécurité : exemple, le RGPD, la territorialité des données
- Le rôle des autorités de contrôle, le rôle des agences spécialisées (ANSII, Clusif, Cnil, Enisa, etc.)

L'exploitation des vulnérabilités, les différents types d'attaque et les vecteurs de compromission

- Connaître les menaces et les principales attaques du SI
- Les différents profils des attaquants
- Les différentes facettes de la cybersécurité : du codeur au hacker
- Le cyber espionnage
- La cybercriminalité
- Le cyber activisme
- Le cyber terrorisme
- La cyber guerre au service des gouvernements et de l'espionnage
- Les principaux outils utilisés lors des attaques
- Les étapes d'une attaque et savoir comment sont utilisées les vulnérabilités
- Les outils de protection (Antivirus, antispyware, pare-feu, sondes)

Labs

- Lab : Menaces et attaques (LAB 2 – G013)
- Lab : Vulnérabilités Réseau (LAB 3 – G013)
- Lab : Renforcer les services réseau (LAB 8_9701)
- Lab : Détecter les Malwares (LAB 9 – 9701)
- Lab : Surveillance des Systèmes (LAB 12 – 9701)

Méthodes pédagogiques :

Supports de cours en français remis aux participants.
Les Labs sont en anglais.

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.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est 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 vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.