Parcours introductif à la Cybersécurité

Mettre en oeuvre de manière opérationnelle les principes fondamentaux, les normes et les outils de la sécurité informatique

Présentiel ou en classe à distance

Durée : 10 jours (70 h)
+ activité à distance

Réf. : MG847

Prix inter : 6.645,00 € HT

Dans un contexte de transformation numérique accélérée, de digitalisation des flux et des activités, d'évolution des modes de vie (nomadisme, télétravail,...) et de tensions internationales, les risques liés à la cybercriminalité sont chaque jour plus importants. Il est donc logique que la cybersécurité soit aujourd'hui au coeur des préoccupations de tous. Mais de quoi parle-t-on réellement ? Que se cache-t-il derrière ce terme ?Ce parcours est précisément étudié pour apporter une vision élargie de ce qu'est la cybersécurité aux personnes s'orientant vers ce domaine comme à celle souhaitant plus simplement étendre leurs connaissances sur le sujet. A l'issue de 10 journées de formation, les participants disposeront d'un bon niveau de compréhension des menaces et des risques qui pèsent sur les organisations et des dispositifs (règlements, normes, outils, bonnes pratiques...) permettant de s'en prémunir.

Les objectifs de la formation

- Disposer d'une vision globale de la cybersécurité et son environnement (enjeux, écosystème...)
- Connaître les différents référentiels, normes et outils de la cybersécurité
- Appréhender les métiers liés à la cybersécurité
- Connaître les obligations juridiques liées à la cybersécurité
- Comprendre les principaux risques et menaces ainsi que les mesures de protection
- Identifier les bonnes pratiques en matière de sécurité informatique

A qui s'adresse cette formation ?

Pour qui

- Toute personne souhaitant apprendre les fondamentaux de la sécurité informatique et/ou souhaitant s'orienter vers les métiers de la cybersécurité, notamment les techniciens et administrateurs systèmes et réseaux

Prérequis

- Connaissances générales dans les systèmes d'information et connaître le guide d'hygiène sécurité de l'ANSSI
- Disposez-vous des compétences nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - 1ère partie (3 jours)

2 - 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
- Exemples d'attaques connues et leurs modes opératoires
- Les différents types de Malwares

3 - 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

4 - 2ème partie (3 jours)

5 - Sécurité des réseaux : translation et filtrage du trafic réseau

- La pile protocolaire TCP/IP
- Les différents mécanismes de translation d'adresses IP (NAT, PAT)
- Les contrôle d'accès vie des listes d'accès (ACL)

6 - Sécurité des réseaux : firewalls et architectures de sécurité

- Les pare-feu, Proxy et Reverse Proxy
- Architecture de sécurité et scénarios de déploiement
- Cloisonnement et segmentation logique

7 - Sécurité des réseaux : VPN, IDS/IPS et sécurité des réseaux sans-fil

- Les systèmes de détection d'intrusion IDS/IPS
- Les réseaux virtuels privés (VPN)
- Sécurité des réseaux sans-fil

8 - 3ème partie (2 jours)

9 - 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 numériqueLe protocole SSL

10 - Concepts fondamentaux de la sécurité applicative et OWASP

- Qu'est-ce que la sécurité applicative ?

- Statistiques et évolution des failles liées au Web et impacts
- Le nouveau périmètre de la sécurité
- Présentation de l'OWASP
- Les risques majeurs des applications Web selon l'OWASP
- Les attaques par injection (commandes injection, SQL Injection, LDAP injection, XXE...)
- Les attaques par violation de l'authentification et du contrôle d'accès
- Les mauvaises configurations de sécurité et l'insuffisance de la surveillance et de la journalisation
- L'exposition des données sensibles
- Les attaques "Cross Site Scripting" ou XSS
- L'utilisation de composants présentant des vulnérabilités connues
- Les attaques par dé sérialisation non sécurisée
- Autres outils OWASP : OWASP Application Security Guide, OWASP Cheat Sheets, OWASP ASVS, OWASP Dependency Check, OWASP ZAP, OWASP ModSecurity....

11 - 4ème partie (2 jours)

12 - 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, système de management de la sécurité de l'information (ISO 27001), code de bonnes pratiques pour le management de la sécurité de l'information (ISO 27002), gestion des risques (ISO 27005), classification des informations, gestion des ressources humaines
- Intégrer la sécurité dans les projets : sécurité dans l'ensemble du cycle de vie d'un projet, approche par l'analyse et le traitement du risque et plan d'action SSI
- Difficultés liées à la prise en compte de la sécurité : compréhension insuffisante des enjeux, implication nécessaire de la direction, difficultés pour faire des choix en toute confiance, délicat arbitrage entre commodité et sécurité, frontières floues entre sphères professionnelle, publique, et privée
- Métiers liés à la cybersécurité

13 - 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

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Les nombreux retours d'expériences de consultants expérimentés permettent d'illustrer les concepts et d'accroître la pertinence des réponses fournies.
- Un programme étudié pour permettre aux participants de bénéficier de nombreuses mises en situations et de disposer de beaucoup de pratique (environ 65% du temps), pour une meilleure assimilation des concepts techniques liés à la sécurité.

Dates et villes 2024 - Référence MG847

A distance

du 3 juin au 19 juil.	du 9 sept. au 18 oct.	du 18 nov. au 13 déc.
du 3 juin au 5 juin	du 9 sept. au 11 sept.	du 18 nov. au 20 nov.
du 17 juin au 19 juin	du 23 sept. au 25 sept.	du 25 nov. au 27 nov.
du 4 juil. au 5 juil.	du 10 oct. au 11 oct.	du 12 déc. au 13 déc.
du 18 juil. au 19 juil.	du 17 oct. au 18 oct.	du 19 déc. au 20 déc.

Paris

du 3 juin au 19 juil.	du 9 sept. au 18 oct.	du 18 nov. au 13 déc.
du 3 juin au 5 juin	du 9 sept. au 11 sept.	du 18 nov. au 20 nov.
du 17 juin au 19 juin	du 23 sept. au 25 sept.	du 25 nov. au 27 nov.
du 4 juil. au 5 juil.	du 10 oct. au 11 oct.	du 12 déc. au 13 déc.
du 18 juil. au 19 juil.	du 17 oct. au 18 oct.	du 19 déc. au 20 déc.