Formation Parcours introductif à la Cybersécurité

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

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

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.

Référence	MGR847
Durée	10 jours (70h)
Tarif	6 645 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 3 juin au 19 juillet 2024
du 9 sept. au 18 octobre 2024
du 18 nov. au 13 décembre 2024

VOIR TOUTES LES DATES

Objectifs

| 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
| Identifier les principaux risques et menaces ainsi que les mesures de protection
| Identifier les bonnes pratiques en matière de sécurité informatique

Public

| 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

Programme de la formation

1ère partie (3 jours)
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

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

2ème partie (3 jours)
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)

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

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

3ème partie (2 jours)
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

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....

4ème partie (2 jours)
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

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

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

| Le cadre légal
| Exploration du RGPD

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.