


Les fondamentaux de la cybersécurité

Découverte des principes fondamentaux de la cybersécurité. Mise en œuvre des bonnes pratiques de sécurité numérique en entreprise et dans sa vie personnelle.

 Cours en présentiel ou distanciel

 Durée : 2 jours (14 h)



Ce cours est basé sur les recommandations de sécurité de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

Votre formateur, un professionnel de l'informatique diplômé, expérimenté et spécialisé dans les problématiques de cybersécurité, utilisera principalement les supports de cours « CyberEdu », rédigés par un consortium regroupant des enseignants-chercheurs et des professionnels du secteur de la cybersécurité, mis à disposition du grand public par l'ANSSI afin d'initier les participants à la sécurité numérique en entreprise.

Les objectifs de la formation

L'objectif de cette formation est de vous initier aux principaux concepts de la cybersécurité et d'approfondir vos connaissances générales relatives aux menaces informatiques et enjeux de sécurité.

Votre formateur vous présentera les bonnes pratiques applicables à l'ensemble des professionnels de l'informatique, qu'ils soient en formation ou en activité.

Pour qui ?

Pour qui ?

- Technicien informatique, administrateur système et réseau, RSSI, DSI.
- Etudiant en informatique.

Prérequis :

- Aucun, cependant des connaissances basiques sur le fonctionnement des systèmes d'information, des réseaux, des systèmes d'exploitation et des applications faciliteront la compréhension mais ne sont pas impératives.

Prérequis techniques

Pour les formations en distanciel, il est impératif d'avoir un ordinateur équipé d'une carte son et idéalement posséder un casque avec micro intégré. La Webcam est un plus mais n'est pas obligatoire.

Méthode et Moyens pédagogiques

- Cette formation alterne les exposés théoriques et les travaux pratiques : 60 % d'apports théoriques et 40 % d'exercices pratiques.
- Méthode active à travers l'articulation de situations d'apprentissage et de techniques pédagogiques multiples.

Evaluation des connaissances et suivi de l'exécution de la prestation

- Un questionnaire est envoyé en amont de la formation pour recueillir les attentes des stagiaires et adapter la formation au plus près des attentes de chacun
- Un questionnaire d'évaluation des acquis de la formation est soumis en fin de formation ainsi qu'un questionnaire de satisfaction
- Un Support pédagogique et une attestation de formation est fournie à chaque stagiaire en fin de la formation.

Programme de la formation

Module 1	Cybersécurité : notions de base
Durée estimée : 4 heures	Objectifs : <ul style="list-style-type: none">• Comprendre les motivations et le besoin de sécurité des systèmes d'information• Connaître les définitions de base et la typologie des menaces
Les enjeux de la sécurité des S.I. <ul style="list-style-type: none">• La nouvelle économie de la cybercriminalité• Les impacts sur la vie privée• Quelques exemples d'attaques Propriétés de sécurité <ul style="list-style-type: none">• Disponibilité, Intégrité, Confidentialité, Preuve/Traçabilité• Exemples de mécanismes offrant des propriétés de sécurité	

Présentation des notions de menaces, vulnérabilités, attaques

- Notions de « Vulnérabilité », « Menace », « Attaque »
- Exemple de vulnérabilité lors de la conception d'une application
- Illustration de l'exploitation d'une vulnérabilité

Panorama de quelques menaces

- Les principales sources de menaces
- Hameçonnage & ingénierie sociale
- Fraude interne
- Intrusion informatique
- Virus informatique
- Dénî de service

Le droit des T.I.C. et l'organisation de la sécurité en France

- L'organisation de la sécurité en France
- Le contexte juridique
- Le droit des T.I.C.
- Dispositif juridique français de lutte contre la cybercriminalité
- Protection des données à caractère personnel

Quizz partie 1 (30 minutes)

- Notions de base à connaître

Module 2	Les règles d'hygiène informatique
Durée estimée : 5 heures	Objectifs : <ul style="list-style-type: none">• Appréhender et adopter les règles d'hygiène de base de la cyber-sécurité, pour les organisations et les individus
Connaître le S.I. <ul style="list-style-type: none">• Identifier et inventorier les composants du SI• Types de réseau et interconnexion Maîtriser le réseau <ul style="list-style-type: none">• Sécuriser le réseau interne• Accès distant• Sécuriser l'administration• Wifi Sécuriser les terminaux <ul style="list-style-type: none">• Applications et mises à jour logicielles et systèmes• Protéger contre les codes malveillants• Protéger les données• Durcir les configurations Gérer les utilisateurs	

- Gestion des privilèges
- Mots de passe et autres moyens d'authentification
- Sensibilisation des utilisateurs

Sécuriser physiquement

Contrôler la sécurité du S.I.

- Contrat de maintenance, d'assurance, de support
- Surveiller et superviser et gérer les incidents de sécurité
- Plan de secours
- Audit

Quizz partie 2 (30 minutes)

- Recommandations et bonnes pratiques pour chacun

Module 3	Cybersécurité : les aspects réseaux et applicatifs
Durée estimée : 3 heures	Objectifs : <ul style="list-style-type: none">• Comprendre les vulnérabilités inhérentes aux mécanismes réseaux et applicatifs couramment utilisés• Connaître le panorama des solutions techniques de sécurité
La sécurité des protocoles IP, ICMP, TCP, UDP <ul style="list-style-type: none">• Présentation synthétique des faiblesses inhérentes à ces protocoles	
Revue d'architectures réseaux (sécurisation) <ul style="list-style-type: none">• Sécuriser le réseau interne• Accès distant• Sécuriser l'administration• Wifi	
Sécuriser les terminaux <ul style="list-style-type: none">• Pare-feu• Répartiteur de charge• Anti-virus• IDS/IPS (Intrusion Detection & Prevention Systems)• VPN (Virtual Private Network) IPsec et SSL• Segmentation• Exemple pratique de sécurisation d'un réseau	
Cryptographie <ul style="list-style-type: none">• Vocabulaire relatif à la cryptographie• Un peu d'histoire (Chiffrement de César, Machine Enigma)• Présentation des concepts de chiffrement (symétrique, asymétrique, chiffrement, hashage, signature électronique, certificats et tokens)	

- Présentation des applications pratiques de la cryptographie dans les services et usages quotidiens

La sécurité des applications Web

- Usurpation d'identité via les cookies
- Injection SQL

Quizz partie 3 (30 minutes)

- Mécanismes techniques à connaître

Module 4	La gestion opérationnelle de la cybersécurité au sein d'une organisation
Durée estimée : 2 heures	Objectifs : <ul style="list-style-type: none"> • Appréhender les méthodes et normes de prise en compte de la sécurité : de façon globale au sein d'une organisation dont l'activité est supportée par un système d'information, et de façon plus unitaire au sein des projets, une activité étant gérée en mode projet • Comprendre et anticiper les difficultés couramment rencontrées dans la gestion de la sécurité dans une organisation • Présenter les filières métiers de la cybersécurité dans l'environnement d'exercice de leur fonction au sein des organisations
Intégrer la sécurité au sein d'une organisation à travers une présentation synthétique de la famille des normes ISO/IEC 27000, notamment <ul style="list-style-type: none"> • Préambule de présentation du chapitre • Panorama des normes ISO 27000 • Système de Management de la Sécurité de l'Information (27001) • Code de bonnes pratiques (27002) • Gestion des risques (27005) • Classification des informations • Gestion des ressources humaines 	
Intégrer la sécurité dans les projets <ul style="list-style-type: none"> • Préambule de présentation du chapitre • Prise en compte de la sécurité dans le cycle de vie d'un projet • Contre-exemple de prise en compte en fin de développement • Approche par l'analyse et le traitement du risque • Plan d'action SSI : la défense en profondeur 	
Les difficultés couramment rencontrées dans la prise en compte de sécurité <ul style="list-style-type: none"> • Compréhension insuffisante des enjeux • Implication nécessaire de la direction • Difficulté de faire des choix en toute confiance • Arbitrage délicat entre commodité et sécurité • Suivre l'évolution des technologies • Frontières floues entre sphères professionnelle, publique et privée 	

Présentation de métiers liés à la cybersécurité

- Positionnement des métiers au sein des organisations
- Cartographie des métiers et compétences
- Profils et carrières
- Perspectives d'embauche

Quizz partie 4 (30 minutes)

- L'organisation de la sécurité