Formation Sécurité informatique : vocabulaire, concepts et technologies pour non-initiés

Comprendre la sécurité informatique

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

La sécurité informatique est devenue une préoccupation de tous les utilisateurs d'Internet et des Systèmes d'Information au même titre qu'elle l'est (depuis longtemps déjà) pour les professionnels de l'informatique. Si, pour certains d'entre nous, la notion de sécurité informatique reste encore confuse, voire même abstraite, il n'en reste pas moins vrai que tous autant que nous sommes, nous commençons dans notre quotidien à en mesurer l'importance. Ce séminaire de "vulgarisation" explique son concept, ses acronymes, son jargon et présente les différents moyens disponibles pour la mettre en oeuvre. Il permet donc clairement aux participants de se familiariser avec la sécurité informatique et de disposer des connaissances nécessaires pour communiquer et collaborer avec des équipes techniques internes, des prestataires ou des fournisseurs spécialisés dans le domaine.

Référence	SEC105
Durée	2 jours (14h)
Tarif	1 650 €HT

Objectifs

| Identifier les concepts, les technologies et les solutions de sécurité des réseaux informatiques pour travailler avec les spécialistes et piloter les prestataires
| Acquérir la vision globale de la sécurité
| Identifier les rôles des intervenants du secteur et leurs métiers
| Identifier les nouveaux enjeux associés à la sécurité informatique

Public

| Commerciaux, spécialistes du marketing, futurs consultants, chefs de projets ou responsables de formation amenés à évoluer dans l'univers de la sécurité informatique
| Toute personne souhaitant comprendre la sécurité informatique pour optimiser leur collab

Prérequis

| Aucun

Programme de la formation

Principes généraux de la sécurité informatique
| Domaines concernés : intégrité, disponibilité, confidentialité, authentification, imputation, traçabilité...
| Démarche générale à entreprendre / analyse de risques
| Notions à connaître : authentification simple et forte - Système de confirmation 3D, défense en profondeur, PRA/PCA...

Comprendre les différents types de vulnérabilités et d'attaques
| Malwares : cheval de Troie, Virus, Rootkit, Spyware...
| Attaques : terminal, réseaux, applications (Sniffing, DCI/DCI, DDoS...)
| Attaques de mots de passe, injection SQL, vol d'identité et de données
| Attaques non-malwares : attaques de phishing (hameçonnage)
| Évaluation des risques

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
- du 12 au 13 juin 2025
- du 8 au 9 septembre 2025

PARIS
- du 12 au 13 juin 2025
- du 8 au 9 septembre 2025

AIX-EN-PROVENCE
- du 12 au 13 juin 2025
- du 20 au 21 novembre 2025

BORDEAUX
- du 8 au 9 septembre 2025

GRENOBLE
- du 8 au 9 septembre 2025

LILLE
- du 12 au 13 juin 2025
- du 8 au 9 septembre 2025

LYON
- du 8 au 9 septembre 2025

NANTES
- du 8 au 9 septembre 2025
- du 20 au 21 novembre 2025

RENNES
- du 8 au 9 septembre 2025
- du 20 au 21 novembre 2025

VOIR TOUTES LES DATES

Connaître le fonctionnement des équipements de protection dédiés aux :
| Solution de gestion des mots de passe
| Cryptage : triple DES / AES
| Séparation des flux par la formation des réseaux virtuels (VLAN)
| Cryptage des données en ligne (VPN SSL et VPN IPSec)
| Authentification d'accès : authentification forte, Network Access Control (NAC) et Role Based Access Control (RBAC)
| Filtrage : firewalls protocolaires, de contenus, d'applications, d'identité...
| Filtrage des applications Web : WAF (Web Access Firewall)
| SIEM (Security Information and Event Management)
| IAM (Identity et Access Management)
| DLP (Data Lost Prevention) - Data Masking - Cryptage
| Empreintes logicielles et MAC (Mandatory Access Control)
| Autres domaines spécifiques

Exploiter les plates-formes spécialisées de sécurité
| Plate-forme de Cloud de Sécurité (SecaaS : Security as a Service)
| Plate-forme de gestion et de sécurité des mobiles EMM (Entreprise Mobility Management)
| Plate-forme de sécurité NGFW (Next Generation of Firewall)

Utiliser la combinaison des équipements pour sécuriser
| L'Internet (communication et transaction) : cryptologie PKI (Public Key Infrastructure)
| Les réseaux sans-fil Wifi : 802.11i (802.1X/EAP...) / WPA / WPA2 / WPA3
| Terminaux et applications mobiles et le télétravail (ODE, conteneurisation, App Stores, empreintes logicielles, App Wrapping...) / Banalisation du terminal et publication d'application (TS-WEB, VDI...)
| Le BYOD (utilisation des équipements personnels dans le cadre professionnel)
| La protection du Cloud et du Big Data (encryptions, vol de données, flux de données...)

Mesurer les impacts de la mise en place de la sécurité sur :
| La performance du système global du système informatique
| L'architecture du système d'information

S'appuyer sur les référentiels pour gérer la sécurité informatique
| ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
| ENISA (organisme Européen - gestion des risques), NIST (standards suivis par des grands acteurs du secteur de sécurité)
| CSA (Cloud Alliance Security) / CSA Big Data / CSA Mobile
| CNIL/RGPD (Obligation Légale de sécurité)
| Critères communs
| CVE

Grandes tendances
| Limites des solutions actuelles de sécurité
| Cybersécurité : recours à l'intelligence artificielle et à la machine learning
| Security Self Healing System et Software Defined Security
| BlockChain

Méthode pédagogique

Une description des technologies et concepts illustrée d'exemples de solutions concrètes et des usages actuels.Un effort particulier de vulgarisation des technologies complexes rendant le séminaire accessible aux non spécialistes de l'informatique et de la sécurité.

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.