Formation État de l'art de la sécurité des Systèmes d'Information

Définition de la politique de sécurité et maîtrise des risques

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

Pour faire face à la montée en puissance des nouvelles menaces qui pèsent sur nos systèmes d'information, le monde de la sécurité doit s'adapter, et est de fait en perpétuelle évolution aussi bien sur le plan des technologies que des méthodes et modèles conceptuels sous-jacents. Ce séminaire de 3 jours dresse un état de l'art complet des outils organisationnels, méthodologiques et techniques de maîtrise du risque informatique. Il permettra aux participants de disposer des informations nécessaires à l'élaboration d'une feuille de route menant à la mise en place d'une politique de sécurité efficace.

Référence	MAG54
Durée	3 jours (21h)
Tarif	2 590 €HT

Objectifs

| Identifier les différents domaines de la sécurité et de la maîtrise des risques liés aux informations
| Identifier les principes et les normes de chaque domaine de la SSI
| Disposer d'informations sur les tendances actuelles au niveau des menaces et des solutions à notre disposition
| Pouvoir améliorer la communication entre la maitrise d'ouvrage, la maitrise d'oeuvre et la SSI
| effectuer des choix techniques

Public

| Directeurs des systèmes d'information ou responsable informatique, RSSI, chefs de projet sécurité, architectes informatiques

Prérequis

| Bonne connaissance générale des systèmes d'information

Programme de la formation

Introduction
Évolutions des menaces et les risques
| Statistiques sur la sécurité
| Tendances dans l'évolution des menaces

Modèle d'approche et maturité effective de l'organisme
| Identification des acteurs : organisation et responsabilités
| Exigences SSI : obligations légales métiers, responsabilités civiles, responsabilités pénales, règlements, délégations

L'identification des besoins DICP consécutifs aux enjeux
| Classification SSI : informations, données et documents, processus, ressources, les pièges
| Identification des menaces et des vulnérabilités : contextuelles métiers, contextuelles IT
| Cartographie des risques : gravité / vraisemblance, niveaux, traitement du risque, validation des risques résiduels

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 23 au 25 juin 2025
du 6 au 8 octobre 2025

PARIS
du 23 au 25 juin 2025
du 6 au 8 octobre 2025

AIX-EN-PROVENCE
du 23 au 25 juin 2025
du 8 au 10 décembre 2025

BORDEAUX
du 6 au 8 octobre 2025

GRENOBLE
du 6 au 8 octobre 2025

LILLE
du 6 au 8 octobre 2025

LYON
du 6 au 8 octobre 2025

NANTES
du 23 au 25 juin 2025
du 8 au 10 décembre 2025

RENNES
du 23 au 25 juin 2025
du 8 au 10 décembre 2025

VOIR TOUTES LES DATES

L'état de l'art des méthodologies et des normes
| Bonnes pratiques SSI : les acteurs, les textes de référence, avantages et inconvénients ; les règles d'hygiène ANSSI, les fiches CNIL, le chapitre 7 RGS
| Approche enjeux : les acteurs, les textes de référence, avantages et inconvénients ; ISO 27002
| Approche SMSI : les acteurs, les textes de référence, avantages et inconvénients ; ISO 27001

Modélisation des niveaux de maturité des technologies SSI
| Les choix structurants et non structurants et positionnements dans la courbe de la pérennité
| La sécurité des accès : filtrage réseau, identification, authentification (faible, moyenne, forte), gestion des identités vs. SSO, habilitation, filtrage applicatif (WAF, CASB et protection du Cloud), détection/protection d'intrusion, journalisation, supervision
| La sécurité des échanges : algorithmes, protocoles, combinaisons symétriques et asymétriques TLS, certificats, IGCP, les recommandations ANSSI
| Infrastructures de clés publiques : autorités de certification et d'enregistrement, révocation
| Le cas du DLP : architecture

Nomadisme
| Sécurité des postes nomades : problèmes de sécurité liés au nomadisme
| Protection d'un poste vs. solutions spécifiques
| Mise en quarantaine
| Accès distants
| VPN : concept et standards de VPN sécurisé, intérêts du VPN, contrôle du point d'accès

Les architectures de cloisonnement
| La sécurité des VLAN et hébergements, DMZ et échanges, sécurisation des tunnels, VPN Peer to Peer et télé accès, de la sécurité périphérique à la sécurité en profondeur

La sécurité des end point
| Le durcissement : postes de travail, ordi phones, serveurs
| L'adjonction d'outils : postes de travail, ordi phones, serveurs
| La sécurité des applications : les standards et les bonnes pratiques

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.

HUB Formation - 14 avenue de l'Opéra - 75001 Paris
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

| 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.