Formation **Sécurité du SI : synthèse**

A l'ère du Big Data, de la Business Intelligence et de la digitalisation généralisée de nos activités, la sécurité informatique prend une importance toujours plus capitale dans le bon fonctionnement de nos opérations. Cette formation Sécurité du SI vous permettra de prendre toute la mesure de l'importance de la sécurité dans votre organisation. Elle vous offrira également les clés et les outils pour comprendre et connaître vos besoins en cybersécurité, ainsi que les solutions adaptées à ces derniers. Appréhendez la fragilité du système d'information afin de vous prémunir au mieux des risques qui pèsent sur celui-ci avec cette formation d'introduction à la sécurité des systèmes d'informations (SSI) de 3 jours, également disponible en distanciel !

Durée
3 jours

Objectifs pédagogiques

- Synthétiser les concepts de base de la sécurité des systèmes d'information
- Comprendre les étapes de la gestion des risques
- Identifier les référentiels et normes liés à la sécurité du SI
- Evaluer les conséquences juridiques des violations de sécurité des systèmes d'information
- Connaître les meilleures pratiques de sécurité et expliquer comment les mettre en place
- S'approprier les concepts de continuité d'activité et de gestion des incidents de sécurité

Public
DSI, chefs de projet, administrateurs, ingénieurs sécurité...

Prérequis
Des connaissances générales en informatique.

Programme de formation

Introduction à la sécurité des systèmes d'information
Définition de la sécurité des systèmes d'information
Les différents types de menaces (virus, logiciels espions, hameçonnage)
Définition de vulnérabilité et exemples
Définition de risque et son calcul
Les menaces physiques (incendie, inondation, vol)
Les menaces logicielles (virus, chevaux de Troie, ransomwares)
Les menaces humaines (erreurs humaines, sabotage, espionnage)
Les vulnérabilités liées aux logiciels
Les vulnérabilités liées aux configurations des systèmes

Les vulnérabilités liées aux utilisateurs
Définition de risque
Les différents types de risques (risques financiers, risques réputationnels, risques juridiques)
Comment calculer un risque (matrice d'évaluation des risques)
Présentation des principaux organismes de la sécurité des systèmes d'information (ANSSI, CNIL, CLUSIF, ENISA, OWASP, ISACA, etc.), les missions et les responsabilités de ces organismes, les ressources disponibles pour les participants (guides, outils, etc.)
Résumé des différents concepts étudiés
Importance de la sécurité des systèmes d'information pour les entreprises

Gestion des risques de sécurité de l'information

Définition de la gestion des risques de sécurité de l'information
Les étapes du processus de gestion des risques (identification, évaluation, mise en œuvre de mesures de sécurité)
Les différents types de risques (risques techniques, risques opérationnels, risques juridiques)
Présentation de la méthode EBIOS: définition, étape de mise en place, exemples d'utilisation
Présentation de la méthode MEHARI: définition, étape de mise en place, exemples d'utilisation
Les différentes sources d'information pour l'identification des risques (analyse des données, enquêtes, audits)
Les méthodes d'identification des risques (analyse de risques, cartographie des risques)
Les différentes méthodes d'évaluation des risques (matrices d'évaluation des risques, analyse de criticité)
Comment évaluer l'impact et la probabilité des risques
Les différentes catégories de mesures de sécurité (administratives, techniques, physiques)
Comment choisir les mesures de sécurité appropriées pour chaque risque identifié
Comment mettre en place et maintenir les mesures de sécurité
Comment suivre l'efficacité des mesures de sécurité mises en place
Comment gérer les incidents de sécurité
Comment améliorer continuellement le processus de gestion des risques de sécurité de l'information
Résumé des différents concepts étudiés
Importance de la gestion des risques de sécurité de l'information pour les entreprises

Référentiels et normes associées à la sécurité des systèmes d'information

Définition des référentiels et normes de sécurité des systèmes d'information
Les différents types de référentiels et normes (normes sectorielles, normes internationales, normes de certification)
Exemples de référentiels et normes sectorielles (PCI-DSS pour les cartes de crédit, HIPAA pour la santé)
Comment ces référentiels et normes s'appliquent à un secteur d'activité spécifique
Exemples de normes internationales de sécurité des systèmes d'information (ISO 27001, NIST SP 800-53)
Comment ces normes peuvent être utilisées pour élaborer une stratégie de sécurité des systèmes d'information
Exemples de normes de certification (SOC 2, PCI-DSS)
Comment les entreprises peuvent obtenir une certification de sécurité des systèmes d'information
Résumé des différents référentiels et normes étudiés
Importance de se conformer aux référentiels et normes de sécurité des systèmes d'information

Cadre juridique de la sécurité des systèmes d'information

Définition des lois et réglementations associées à la sécurité des systèmes d'information
Comment ces lois et réglementations peuvent impacter les entreprises
Présentation de la loi sur la protection des données personnelles (RGPD en Europe, CCPA aux Etats-Unis)
Comment les entreprises peuvent se conformer à ces lois
Exemples de violations de sécurité des systèmes d'information et les conséquences juridiques pour les entreprises
Comment les entreprises peuvent se protéger contre les poursuites juridiques liées à des violations de sécurité des systèmes d'information

Résumé des différentes lois et réglementations étudiées
Importance de se conformer aux lois et réglementations de sécurité des systèmes d'information

Mise en pratique de la sécurité des systèmes d'information

Présentation des étapes de mise en place d'une stratégie de sécurité des systèmes d'information : identification des risques, évaluation des risques, mise en place des contrôles, surveillance et audit
Présentation des normes ISO 27001 et ISO 27002
Comment mettre en place un ISMS (système de gestion de la sécurité des informations) conforme à ces normes
Présentation des pratiques de sécurité courantes : pare-feu, chiffrement, authentification à deux facteurs, gestion des privilèges d'utilisateur, gestion des mots de passe
Comment mettre en place ces pratiques de sécurité dans un environnement informatique
Présentation des différents outils de surveillance de la sécurité : analyse de logs, détection d'intrusion, surveillance réseau
Comment utiliser ces outils pour surveiller efficacement la sécurité des systèmes d'information
Présentation des différents types d'audit de sécurité : interne, externe, normatif
Comment planifier et effectuer un audit de sécurité efficacement

Continuité d'activité et gestion des incidents

Définition de la continuité d'activité et de la gestion des incidents
Importance de la continuité d'activité et de la gestion des incidents pour assurer la résilience des systèmes d'information
Techniques pour identifier les risques pour la continuité d'activité : analyse de risque, étude de menaces, etc.
Évaluation des impacts potentiels des risques identifiés sur les systèmes d'information
Présentation des différents éléments d'un plan de continuité d'activité : politiques, procédures, plans d'urgence, etc.
Comment élaborer et mettre en place un plan de continuité d'activité adapté aux besoins de l'organisation
Présentation des étapes de la gestion des incidents : détection, analyse, contournement, résolution, etc.
Comment élaborer et mettre en place des procédures de gestion des incidents pour assurer une réponse rapide et efficace aux incidents de sécurité
Exemple de cas pratique : simulation d'un incident de sécurité et mise en pratique des étapes de la gestion des incidents
Évaluation des performances et discussion des résultats

Conclusion et synthèse de la formation

Récapitulatif des principaux enseignements de la formation
Mise en place d'un plan d'action pour mettre en pratique les enseignements de la formation
Questions/Réponses selon les besoins des apprenants
Questionnaires de satisfaction

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques.
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d’évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.

- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience.

- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l’auto-positionnement, permettant ainsi une analyse détaillée de leur progression.