Formation SSI : Etat de l'art de la sécurité des systèmes d'information

PLUS D'INFOS

- Contactez-nous

CONTACT REFERENT

- Commercial@ageris-group.com
- +33 3 87 62 06 00

MODALITES D'ACCES

- Inscription en réservant votre place sur une session disponible ou par téléphone, par mail, par demande de contact. Vous recevrez un devis à nous retourner avec votre accord pour confirmer votre inscription.

DELAI D'ACCES

- La durée estimée entre la demande du stagiaire et le début de la formation est de 7 jours (peut être raccourci pour le mode distanciel)

ACCESSIBILITE AUX PERSONNES EN SITUATION D'HANDICAP

- Accessible à distance pour les personnes à mobilité réduite
- Pour connaître l'accessibilité aux salles de formation, vous pouvez nous joindre au +33 3 87 62 06 00

REFERENCE

- SSIEARTSSI

TARIF

- 2050 € HT

DUREE DE LA FORMATION

- 3 jours – 21 heures

DATES DES SESSIONS

- Voir site internet

FINANCEMENT

- OPCO

FORMULE INTRA-ENTREPRISE

Formulaire : soumettez votre projet

RESSOURCES PEDAGOGIQUES

- Cours théorique
- Exemples concrets
- Evaluation des compétences par un quizz en cours et en fin de formation

PRESENTATION DE LA FORMATION

Pour faire face à la montée en puissance des nouvelles menaces qui pèsent sur les 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 des risques liés au système d'information.

OBJECTIFS DE CETTE FORMATION

A l'issue de cette formation, le stagiaire aura les compétences pour :

- Identifier les différents domaines de la sécurité et de la maîtrise des risques liés à la protection du patrimoine informationnel
- Connaître l'état de l'art de la normalisation de la SSI
- Disposer d'informations sur les tendances actuelles, que ce soit dans les menaces ou dans les solutions à notre disposition
- Améliorer la communication entre la maitrise d'ouvrage, la maitrise d'œuvre et la SSI
- Faciliter les choix techniques

PUBLIC

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

PREREQUIS

Aucun prérequis n'est nécessaire.

PROGRAMME DETAILLE

Chapitre 1 : Introduction- objectif de la formation

Chapitre 2 : Evolutions des menaces et les risques

- Statistiques sur la sécurité
  - Tendances dans l'évolution des menaces

Chapitre 3 : 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

Chapitre 4 : 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

Formation SSI : Etat de l'art de la sécurité des systèmes d'information

- Support de cours remis au stagiaire en fin de formation
- Outil distanciel : Teams

POUR ALLER PLUS LOIN

- SSI – Maîtriser l'analyse des risques du système d'information
- SSI – Auditer et contrôler la sécurité du Système d'Information

PLUS D'INFOS

- Contactez-nous

- Cartographie des risques
  - Gravité / vraisemblance
  - Niveaux
  - Traitement du risque
  - Validation des risques résiduels

Chapitre 5 : 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 fiches CNIL
  - Les acteurs, les textes de référence, avantages et inconvénients
  - ISO 27002
- Approche SMSI
  - Les acteurs, les textes de référence, avantages et inconvénients
  - ISO 27001

Chapitre 6 : Modélisation des niveaux de maturité des technologies SSI

- Les choix structurants et non structurants et positionnements dans la courbe de la pérennité
  - Critères de choix
  - Acteurs concernés
- La sécurité des accès
  - Filtrage réseau
  - Identification
  - Authentification, faible, moyenne, forte
  - Gestion des identités vs. SSO
  - Habilitation
  - Filtrage applicatif
  - 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

Chapitre 7 : 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

Chapitre 8 : 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

Chapitre 9 : La sécurité des end point

- Le durcissement
  - Postes de travail
  - Ordi phones
  - Serveurs
- L'adjonction d'outils
  - Postes de travail
  - Ordi phones
  - Serveurs
- Postes de travail
- Ordi phones
- Serveurs
  - Les standards et les bonnes pratiques

Chapitre 10 : Conclusion

MODALITES D'EVALUATION

Validation des connaissances et compétences par un quizz à la fin de chaque chapitre.