État de l’art de la sécurité réseaux et des méthodes

Programme *(Mis à jour le 14/03/2025)*

Introduction à la SSI

- De l’importance de la SSI : statistiques et tendances
- La place de la SSI dans l’entreprise
- Contraintes règlementaires et SSI : ce que dit la loi

La gestion par les risques

- La gestion des risques dans le cadre du SMSI avec l’ISO 27001
- La notion d’amélioration continue et de PDCA
- Les principales méthodes francophones disponibles : ISO 27005, EBIOS, MEHARI
- Les critères pour une bonne appréciation des risques
- Les étapes de l’ISO 27005 : Le pilotage de la SSI
- Les besoins de sécurité DICT

Les vulnérabilités et les menaces

- Quelques rappels sur les principales failles de sécurité OS, WEB, Réseau
- Les vulnérabilités
- Les vulnérabilités matérielles
- Les vulnérabilités logicielles
- Les vulnérabilités réseau
- Les vulnérabilités personnelles
- Les vulnérabilités du site
- Les vulnérabilités de l’organisme
- Les menaces
- Les menaces environnementales
- Les menaces techniques
- Les menaces humaines

Evaluation des risques

- L’identification des mesures de sécurité existantes
- Vraisemblance des risques et de leurs composantes
- Impact et Conséquences métiers des risques
- Identification et valorisation des risques de sécurité

Les stratégies de traitement des risques

- Les traitements des risques :
  – La sécurité organisationnelle
  – L’analyse de risques
  – La politique de sécurité
  – Organisation et responsabilité
  – La gestion des biens
  – La gestion des personnes
  – La formation, la sensibilisation et la communication
  – La sécurité physique et environnementale
  – La gestion des incidents
  – La continuité d’activité
  – La conformité
  – Le contrôle et l’audit
  – La démarche SMSI

Référence
THIS2991

Durée
3 jours / 21 heures

Prix HT / stagiaire
2550€

Objectifs pédagogiques

- Connaître les principes de management de la sécurité informatique

Niveau requis

- Connaissance généraliste d’un SI

Public concerné

- DSI, Directeur Informatique, RSSI

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d’accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N’hésitez pas à nous contacter pour en discuter) équipée d’un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD
Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices
Mise à disposition en ligne de documents supports à la suite de la formation

Dispositif de suivi de l'éxécution de l'évaluation des résultats de la formation

Feuilles d’émargement (signature électronique privilégiée)
Evaluations formatives et des acquis sous forme de questions orales et/ou écrites (QCM) et/ou mises en situation
Questionnaires de satisfaction (enquête électronique privilégiée)

- La sécurité technique :
  – La protection contre les codes malveillants (virus)
  – Les sauvegardes
  – La sécurité des réseaux
  – La gestion des supports mobiles et amovibles
  – La messagerie
  – La surveillance et l'audit technique
  – Le contrôle d'accès
  – La sécurité dans les développements
  – La cryptographie
  – La gestion des vulnérabilités techniques

Amélioration continue de la sécurité

- La communication du risque
- La supervision du risque
- Audit récurrent
- Les différents types d'audit : organisationnel, technique
- Les différentes façons de réaliser un audit technique : blackbox, whitebox, greybox
- La planning typique d'un audit de sécurité technique
- Les grandes phases de l'audit de sécurité technique :
  – Collecte passive d'informations / Collecte active d'informations
  – Identification des vulnérabilités
  – Exploitation des vulnérabilités
  – Persistance et post-exploitation
- Les outils du Pentester :
  – Scanner un réseau pour identifier des vulnérabilités
  – Le framework d'exploitation Metasploit
  – Attaquer les mots de passe
  – Post-Exploitation avec le meterpreter

Conclusion