Séminaire de 3 jour(s)
Réf : SSI

Participants

Ingénieurs prenant les fonctions de RSSI, directeurs ou responsables informatiques, ingénieurs ou correspondants sécurité, chefs de projet intégrant des contraintes de sécurité.

Pré-requis

Aucune connaissance particulière.

Prix 2019 : 2680€ HT

Dates des sessions

AIX
19 nov. 2019
ANGERS
26 nov. 2019
BORDEAUX
19 nov. 2019
BRUXELLES
12 nov. 2019
DIJON
26 nov. 2019
GENEVE
26 nov. 2019
GRENOBLE
12 nov. 2019
LILLE
19 nov. 2019
LIMOGES
26 nov. 2019
LUXEMBOURG
26 nov. 2019
LYON
19 nov. 2019
MONTPELLIER
12 nov. 2019
NANCY
26 nov. 2019
NANTES
19 nov. 2019
NIORT
26 nov. 2019
ORLEANS
12 nov. 2019
PARIS
21 mai 2019, 24 juin 2019
10 sep. 2019, 08 oct. 2019
19 nov. 2019, 17 déc. 2019
REIMS
26 nov. 2019
RENNES
12 nov. 2019
ROUEN
26 nov. 2019
SOPHIA-ANTIPOLIS
19 nov. 2019
STRASBOURG
19 nov. 2019
TOULON

Sécurité des Systèmes d'Information, synthèse

Avec l'explosion du digital qui a multiplié les opportunités de développement, le management de la sécurité des Systèmes d'Information est devenu un enjeu majeur pour toutes les entreprises. Ce séminaire très riche vous présentera l'ensemble des actions et des solutions permettant d'assurer la sécurité de votre SI : de l'analyse des risques à la mise en œuvre optimale de solutions de sécurité. Vous verrez également les thématiques assurantielles et juridiques intimement liées à l'application d'une politique de sécurité.

OBJECTIFS PEDAGOGIQUES

Maîtriser le processus de gestion des risques de sécurité de l'information
Utiliser les référentiels et les normes associées
Connaître le cadre juridique
Définir et piloter la mise en œuvre de solutions

1) Introduction à la gestion des risques

- La définition du risque et ses caractéristiques : potentialité, impact, gravité.
- Les différents types de risques : accident, erreur, malveillance.
- La classification DIC : Disponibilité, Intégrité et Confidentialité d'une information.
- Les contre-mesures en gestion des risques : prévention, protection, report de risque, externalisation.

2) RSSI : chef d'orchestre de la sécurité

- Quels sont le rôle et les responsabilités du Responsable Sécurité SI ?
- Vers une organisation de la sécurité, le rôle des "Assets Owners".
- Gestion optimale des moyens et des ressources alloués.
- Le Risk Manager dans l'entreprise ; son rôle par rapport au Responsable Sécurité SI.

3) Les cadres normatifs et réglementaires

- Les réglementations SOX, COSO, COBIT. Pour qui ? Pour quoi ?
- Vers la gouvernance du Système d'Information. Les liens avec ITIL® et CMMI.
- La norme ISO 27001 dans une démarche système de management de la sécurité de l'information.
- Les liens avec ISO 15408 : critères communs, ITSEC, TCSEC.
- Les atouts de la certification ISO 27001 pour les organisations.

4) Le processus d'analyse des risques

- Identification et classification des risques.
- Risques opérationnels, physiques, logiques.
- Comment constituer sa propre base de connaissances des menaces et vulnérabilités ?
- Utiliser les méthodes et référentiels : EBIOS/FEROS, MEHARI.
- La démarche d'analyse de risques dans le cadre de l'ISO 27001, l'approche PDCA (Plan, Do, Check, Act).
- Le standard ISO 27005 et les évolutions des méthodes françaises.
- De l'appréciation des risques au plan de traitement des risques : les bonnes pratiques.

5) Les audits de sécurité et le plan de sensibilisation

- Processus continu et complet.
- Les catégories d'audits, de l'audit organisationnel au test d'intrusion.
- Les bonnes pratiques de la norme 19011 appliquées à la sécurité.
- Comment créer son programme d'audit interne ? Comment qualifier ses auditeurs ?
- Apports comparés, démarche récursive, les implications humaines.
- Sensibilisation à la sécurité : qui ? Quoi ? Comment ?
- Définitions de Morale/Déontologie/Ethique.
- La charte de sécurité, son existence légale, son contenu, sa validation.

6) Le coût de la sécurité et les plans de secours

- Les budgets sécurité.
- La définition du Return On Security Investment (ROSI).
- Les techniques d'évaluation des coûts, les différentes méthodes de calcul, le Total Cost of Ownership (TCO).
- La notion anglo-saxonne du "Payback Period".

26 nov. 2019
TOULOUSE
19 nov. 2019
TOURS
26 nov. 2019

Modalités d'évaluation

Les apports théoriques et les panoramas des techniques et outils ne nécessitent pas d'avoir recours à une évaluation des acquis.

Compétences du formateur

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Moyens pédagogiques et techniques

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.

• A l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.

• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

- La couverture des risques et la stratégie de continuité.
- Plans de secours, de continuité, de reprise et de gestion de crise, PCA/PRA, PSI, RTO/RPO.
- Développer un plan de continuité, l'insérer dans une démarche qualité.

7) Concevoir des solutions optimales

- Démarche de sélection des solutions de sécurisation adaptées pour chaque action.
- Définition d'une architecture cible.
- La norme ISO 1540 comme critère de choix.
- Choisir entre IDS et IPS, le contrôle de contenu comme nécessité.
- Comment déployer un projet PKI ? Les pièges à éviter.
- Les techniques d'authentification, vers des projets SSO, fédération d'identité.
- La démarche sécurité dans les projets SI, le cycle PDCA idéal.

8) Supervision de la sécurité

- Gestion des risques : constats, certitudes...
- Indicateurs et tableaux de bord clés, vers une démarche ISO et PDCA.
- Externalisation : intérêts et limites.

9) Les atteintes juridiques au Système de Traitement Automatique des Données

- Rappel, définition du Système de Traitement Automatique des Données (STAD).
- Types d'atteintes, contexte européen, la loi LCEN.
- Quels risques juridiques pour l'entreprise, ses dirigeants, le RSSI ?

10) Recommandations pour une sécurisation "légale" du SI

- La protection des données à caractère personnel, sanctions prévues en cas de non-respect.
- De l'usage de la biométrie en France.
- La cybersurveillance des salariés : limites et contraintes légales.
- Le droit des salariés et les sanctions encourues par l'employeur.