État de l’art de la sécurité des systèmes d’information

Informatique

Sécurité logicielle

Référence : 3-SE-ETAR
Durée : 3 jours
Présentiel ou en classe à distance

Tarif Inter : 750 € Prix HT jour / personne
Tarif Intra : 1500 € Prix HT jour / groupe

Mise à jour : 27/11/2023

Durée de validité : du 01/01/2026 au 31/12/2026

Objectifs

- Comprendre les menaces sur les équipements de l'infrastructure
- Mettre en place une politique interne (technologique et humaine) de sécurité des informations
- Choisir les dispositifs et emplacements de sécurité
- Concevoir le Plan de Sécurité

Prérequis

Aucun prérequis obligatoire

Niveau recommandé

DSI, RSSI, RSI, Technicien sécurité

Contenu pédagogique

Domaines et contours de la sécurité

- Les systèmes de gouvernance
- Présentation des risques involontaires
- Cybercriminalité
- Le cycle de la gouvernance
- Les organes de contrôle
- Le contrôle Interne
- Les audits externes
- Les acteurs de la sécurité
- Environnement juridiques
- Droits et obligations des entreprises en termes de sécurité
- La loi Sécurité Financière SOX (Sarbane Oxley) , La CNIL

Analyse des risques

- Connaître son SI
- PC final
- Serveur
- Utilisation d'une ferme de serveurs
- Quelles sont les données externalisées (cloud) ?
- Matériel réseau
- Méthodes d'accès aux réseaux
- Méthodes d'identification
- Gestion des autorisation
- Risques de piratage
- Risques de perte d'information
- Risques de vols d'information
- Risques naturels
- Les pannes matérielles
- Les risques d'ingénierie sociale

Mise en oeuvre d'une politique de sécurité

- La sécurité physique
- Accès aux installations
- Sécurité des installations (incendies, inondations, vols...)
- Prévision d'un plan de continuité et de reprise
- Contrôler les accès
- La sécurité des services
- Sécuriser les applications
- Cryptage
- Technologies VPN
- VPN SSL
- HTTPS
- Sécurité des protocoles Peer-to-peer
- Blocage des applications
- Sécurité des terminaux mobiles
- Utilisation d'une DMZ
- Comment intégrer la disponibilité et la mobilité des collaborateurs
- Généralités sur les outils disponibles

Les aspects organisationnels de la sécurité

- Définition des risques
- Confidentialité
- Intégrité
- Supervision
- La veille technologique
- Publication des failles
- Principe du modèle de maturité
- Sécurité du système d'exploitation
- Gestion des privilèges
- Documentation

Management de la sécurité

- Les méthodes Méhari EBIOS ISO 27001 Cobit
- Les limites de ces méthodes
- Les audits de sécurité
- Mener un audit dans une entreprise multisites
- Trop de sécurité tue la sécurité, comment éviter les faux-positifs
- Expliquer les enjeux de la sécurité aux utilisateurs finaux et aux directions
- La roue de la sécurité
- Mise en oeuvre technique de la sécurité
- Stress du système
- Amélioration de la sécurité
- Savoir protéger les investissements au meilleur coût pour les meilleures raison
- Communications sur la politique de sécurité
- Comment réagir à une attaque (en interne, en externe)
- Les limites du plan de sécurité et les dispositions juridiques
- Définition et rôle du RSSI

Méthodologie et technologie

- La vision de la sécurité selon les interlocuteurs
- Les objectifs
- Les moyens techniques et financiers mis en oeuvre

- La stratégie
- L'adaptation et la gestion du changement
- Elaboration du plan de sécurité
- L'audit de conformité
- Les indicateurs
- Les tableaux de bords à établir
- Les méthodologies d'audit

Les outils

- Fonction d'un firewall
- Documentation des accès autorisés sur le réseau
- Création d'une charte d'utilisation du réseau pour les collaborateurs
- Fonction d'un système de détection d'intrusion
- Les logiciels clients de sécurité (firewall, antivirus, antispyware...)
- Superviser la sécurité
- Faire évoluer la sécurité
- Contraction d'assurances : quelles sont les garanties ? qu'est ce qui peut et doit être assuré ? l'importance de la disponibilité du système
- Validation technique de l'architecture
- Formation des personnels du SI
- Formation des utilisateurs du SI
- Avenir de la sécurité informatique
- Les 6 idées les plus stupides selon Marcus J. Ranum
- La vision géostratégique de la sécurité
- Les phénomènes de monopole

Rédaction de chartes d'utilisation et / ou de configuration

- Le secret professionnel
- Le respect de la législation
- Les règles de confidentialité
- L'usage des services Internet
- Définir sa charte d'utilisation
- Responsabilités du comité de coordination du SI
- Responsabilités du conseil d'administration et des représentants

---

Moyens pédagogiques

- Réflexion de groupe et apports théoriques du formateur.
- Travail d'échange avec les apprenants sous forme de réunion - discussion.
- Utilisation de cas concrets issus de l'expérience professionnelle.
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques.
- Alternance entre apports théoriques et exercices pratiques (en moyenne sur 30 à 50% du temps)

Modalités pédagogiques : Présentiel, Distanciel et AFEST

Moyens techniques

En formation présentielle

Accueil des apprenants dans une salle dédiée à la formation et équipée avec :

- Ordinateurs
- Vidéo projecteur ou Écran TV interactif
- Tableau blanc ou Paper-Board

En formation distancielle

A l'aide d'un logiciel comme ® Microsoft Teams ou Zoom, un micro et une caméra pour l'apprenant.

- Suivez une formation en temps réel et entièrement à distance. Lors de la session en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise.
- L'accès à l'environnement d'apprentissage (support de cours, ressources formateur, fichiers d'exercices ...) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
- Les participants recevront une convocation avec le lien de connexion à la session de formation.

- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 02 35 12 25 55 ou par email à commercial@xxlformation.com

Modalités d'évaluation

- Positionnement préalable oral ou écrit.
- Feuille de présence signée en demi-journée.
- Evaluation des acquis tout au long de la formation.
- Questionnaire de satisfaction
- Attestation de stage à chaque apprenant
- Evaluation formative tout au long de la formation.
- Evaluation sommative faite par le formateur.

Profil du formateur

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité

Adaptation pédagogique et matérielle

Si vous avez besoin d'adaptation matérielle ou pédagogique, merci de prendre contact avec notre référent Handicap par téléphone au 02 35 12 25 55 ou par email à handicap@xxlformation.com

Modalités et délais d'accès à la formation

Les formations sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.

Les conditions d'accès à la formation dans le cadre du CPF sont celles implicitement présentées dans les CGU disponibles sur le site Mon Compte Formation en vigueur à date d'inscription.

Voir CG_MCF_V16_VF.pdf Article 5.1.

Nos sessions INTER 2026

Sessions de formation à venir :

- Aucune session à venir pour cette formation.

Nos sessions INTRA 2026

Pour organiser cette formation en intra-entreprise, veuillez nous contacter par mail à commercial@xxlformation.com ou par téléphone au 02 35 12 25 55