Sécurité avancée (SI)

https://www.estim-formation.com/formation-securite-avancee-si

Objectifs de la formation

- Acquérir des connaissances plus poussées dans le domaine de la sécurité et des réseaux.
- Acquérir des aptitudes en gestion de la sécurité et des risques.
- Comprendre les besoins en sécurité de l'information pour toute son organisation.
- Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures.
- Pratiques en gestion de la sécurité de l'information.
- Développer une vision globale (organisationnelle, fonctionnelle, juridique) et pas seulement technologique des besoins en sécurité de l'entreprise.

Programme pédagogique

Gouvernance de sécurité de l'information et gestion des risques

- Gestion de la sécurité / DICP
- Modèle de sécurité organisationnelle / PDCA / politique de sécurité et procédures
- Gestion des risques informationnels EBIOS, MEHARI
- Analyse des risques, ISO 2700X
- Classification des informations
- Rôle et niveaux de responsabilité RACI
- Architecture de sécurité et conception

Architecture des ordinateurs / des systèmes

- Modèles de sécurité
- Modes des opérations de la sécurité
- Méthodes d'évaluation des systèmes
- Critères d'évaluation de la sécurité
- Systèmes ouverts / systèmes fermés
  - Livre Orange (TCSEC)
  - Livre rouge (TNI), ITSEC
  - Livres Arc-en-Ciel
- Critères communs
- Certification et accréditation, EAL
  - Menace à la sécurité des architectures

Sécurité des réseaux et des télécommunications

- Modèles OSI et TCP/IP (DOD)
- Types de transmission
- Réseaux LAN, VLAN, WLAN, MAN et WAN
- Protocoles de routage RIP, OSPF, BGP
- Périphériques réseaux
- Protocoles et services réseaux, IPV4 et IPV6
- Intranet et Extranet
- Accès distants, VPN, SSL
- Filtrage de contenu et inspection
- Détection des intrusions

Cryptographie

- Histoire de la cryptographie
  - Implication des gouvernements dans la cryptographie
  - Types d'algorithmes cryptographiques
  - Différents types de systèmes symétriques et asymétriques
  - PKI, gestion des clés
  - Cryptage des liens et cryptage de bout-en-bout
  - Standards d'e-mails
  - Sécurité Internet
- Cryptanalyse et attaques

Continuité des opérations et reprise après désastre

- Introduction et objectifs de la continuité des activités
- Assurances cybernétiques / Backups
- Exigences de la planification
- Processus (PRA/PCA) ou (BCP/DRP)
  - Phase 1 : management du projet BCP et initiation
  - Phase 2 : Business Impact Analysis (BIA)
  - Phase 3 : stratégie de reprise
  - Phase 4 : développement du plan et implémentation
  - Phase 5 : tests, révision des plans et mise à jour, sensibilisation et formation

Lois, règlementations, conformité et investigations

- Problématiques des lois cybernétiques
- Droit international / droit civil / Common Law (HIPAA, GLB, SOX)
  - Exemples : Etats-Unis / France
- Complexité des crimes cybernétiques
  - Propriété intellectuelle et code de la confidentialité
- Informations à caractère personnel
- Investigations cybercriminelles / collecte d'informations
  - Ethique : fondements d'éthique / code d'éthique (ISC) ²
  - Les dix commandements de l'info éthique de l'Institut de Déontologie CEI
  - Ethique et Internet (RFC 1087) de l'IAB (Internet Activities Board)
  - Principes généralement acceptés de sécurité du système (GASSAP)

Prérequis et public cible

Prérequis de formation :

Ce programme de formation ne nécessite pas de pré-requis particulier.

Cette formation est ouverte à tous les publics.

Modalité d'évaluation pédagogique

Evalution des compétences acquises par les stagiaires :

A l'issue de la formation, un contrôle de connaissances permettra d'évaluer les compétences acquises par chaque participant.