INFORMATIQUE, SÉCURITÉ DES SI - ARCHITECTURE SI ET INFRASTRUCTURES

Risque : comprendre et analyser les risques des systèmes informatiques

Cette formation peut être organisée en intra entreprise.
Ce module introduit la sécurité informatique, l'intelligence économique, l'analyse de risque, les référentiels pour la sécurité et le droit informatique (risque légal). Il initie à la sûreté de fonctionnement et à la méthode d'analyse de risques EBIOS.

PUBLIC ET PRÉ-REQUIS

Tout informaticien.
Prérequis : avoir des connaissances de base en systèmes informatiques

PROGRAMME

Comprendre les enjeux de la cybersécurité

- histoire de la sécurité informatique, explication de quelques affaires récentes ;
- évolution et coûts de la cybercriminalité ;
- lutte contre la cybercriminalité ;
- tour d'horizon, principales définitions, autorités compétentes, acteurs majeurs ;
- démarche sécurité en entreprise, PSSI, traitement des incidents.

Comprendre les vulnérabilités intrinsèques des systèmes informatiques

- rappels sur les architectures informatiques (OS, réseaux, applications...) ;
- évolution des architectures des SI, tendances actuelles, menaces associées.

Comprendre les enjeux de l'intelligence économique

- histoire de l'intelligence économique, organisation par pays, enjeux et menaces ;
- grands principes (cycle du renseignement, approche moderne, fonctions de l'IE).

Comprendre et pratiquer l'analyse de risque d'un SI

- méthodes d'analyse d'un SI, enjeux humains ;
- définitions du risque ; concept de menace, de vulnérabilité, de sensibilité ;
- classement des menaces, cycle de l'information, menaces génériques.

Comprendre une politique de sécurité

- principales exigences de sécurité (CIDP), métriques ; fonctions de sécurité ;
- élaboration d'une PSSI.

Connaître les référentiels pour la sécurité

- description des principales méthodes ;
- familles de normes ISO 27k ; critères communs ; certification ;
- référentiel Général de Sécurité, Règlement Général de Protection des Données.

Connaître les grands principes du Droit Informatique français

- rappels sur le droit et son organisation en France ;
- principales lois (LIL, Godfrain, Bases de données, preuve, LCEN, LCI, LPM...) ;
- droit d'auteur ; protection des œuvres ; protection des logiciels.

Sécurisation de systèmes (travaux pratiques)

- rappels sur Linux ;
- sécurisation de Linux ;
- sécurisation des services Linux ;
- sécurisation Windows.

Informations clés

Durée :
28 heures

€ Tarif :
Sur mesure

694 € par jour en inter / nous consulter pour un tarif sur mesure en intra

Contact

fc@utc.fr

OBJECTIFS & COMPÉTENCES

- Comprendre les enjeux de la cybercriminalité et les risques pour l'entreprise ;
- Être sensibilisé aux vulnérabilités des systèmes informatiques y compris humaines ;
- Comprendre les enjeux de l'intelligence économique et les menaces associées ;
- Savoir mener une analyse de risque ; connaître les principales exigences de sécurité ;
- Connaître et exploiter les principaux référentiels pour la sécurité;
- Connaître les principales lois du Droit Informatique français ;
- Déployer un SI, comprendre la PSSI.

LES + DE LA FORMATION

Entraînement sur des situations réelles ; pédagogie tournée vers la pratique ;
Un temps réservé pour les questions propres aux spécificités des activités de l'entreprise ;
formation partagée avec des étudiants ingénieurs.

MÉTHODES PÉDAGOGIQUES

Modalités pédagogiques
Cours, exercices ; études de cas ; ateliers-projets et études de cas pour un SI d'entreprise.
Modalités d'évaluation
Évaluation effectuée à l'occasion de tests de connaissances ; travaux de mise en application ; étude.

POUR CANDIDATER

Inscription via formulaire (voir site web).