FORMATION COURTE

INFORMATIQUE, SÉCURITÉ, SI

RISQUE : COMPRENDRE ET ANALYSER LES RISQUES DES SYSTÈMES INFORMATIQUES

inter/intra entreprise

Dates : consulter le calendrier
Durée : 4 jours ; 28 heures
Lieu : Compiègne
Tarif : consulter le dépliant « Tarifs »
Prérequis : avoir des connaissances de base en systèmes informatiques
Référence produit : CYBERISK

LES POINTS FORTS

- 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

POUR ALLER PLUS LOIN

Formations : Cryptographie : Comprendre et utiliser les moyens cryptographiques pour sécuriser un SI (CYBERCRYPT) ; Protection : prévenir et assurer la protection des systèmes informatiques (CYBERPROT) ; Architectures résilientes : concevoir une infrastructure informatique résiliente (CYBERRES) ; Défense : défendre un système informatique (CYBERDEF)

EN SAVOIR +
www.utc.fr
→ Formation continue et VAE

Cette formation 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.

Objectifs

- 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.

Public

Tout informaticien.

Modalités pédagogiques

Cours ; exercices ; ateliers-projets et études de cas pour un SI d'entreprise.

Modalités d'évaluation

Évaluation effectuée à l'occasion des tests de connaissances ; travaux de mise en application ; étude.

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.

Intervenants

Nos intervenants sont issus des secteurs économiques publics, privés, académiques et professionnels. Ils comptent généralement plus de 10 ans d'expérience professionnelle dans leur domaine d'expertise.