FORMATION COURTE

INFORMATIQUE, SÉCURITÉ, SI

PROTECTION : PRÉVENIR ET PROTÉGER LES SYSTÈMES INFORMATIQUES

inter/intra entreprise

Dates : consulter le calendrier
Durée : 4 jours ; 28 heures (une journée par semaine sur 4 semaines)
Lieu : Compiègne
Tarif : consulter le dépliant « Tarifs »
Prérequis : avoir suivi la formation Risque : comprendre et analyser les risques des systèmes informatiques ou avoir les compétences associées à la formation (CYBERISK)
Référence produit : CYBERPROT

LES POINTS FORTS

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

POUR ALLER PLUS LOIN

Formations : Cryptographie : Comprendre et utiliser les moyens cryptographiques pour sécuriser un SI (CYBERCRYPT) ; Architectures résilientes : concevoir une infrastructure informatique résiliente (CYBERRES) ; Défense : défendre un système informatique (CYBERDEF)

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

Ce module s'intéresse à la protection des systèmes informatiques. Il introduit les fonctionnalités majeures de sécurité et les meilleures pratiques, le développement robuste d'applications, la protection des systèmes d'information et les plans de continuité d'activité, le management de la sécurité en entreprise et la cyber-résilience.

Objectifs

- S'initier à la cyber-résilience ;
- Savoir sécuriser les services ;
- Comprendre et pratiquer le développement informatique robuste ;
- Détecter les vulnérabilités applicatives ;
- Comprendre les fonctionnalités de sécurité et les meilleures pratiques ;
- Comprendre les architectures sécurisées ;
- Concevoir un plan de continuité d'activité ;
- Comprendre le management de la sécurité, les audits et la gestion de crises.

Public

Informaticiens (niveau en sécurité débutant et intermédiaire).

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

Connaître et pratiquer les méthodes de développement robuste

- Développement robuste en C ; bonnes pratiques et études de cas ;
- Développement web robuste ; durcissement de code ;
- Choix des applicatifs, détection de vulnérabilités applicatives.

Connaître les fonctionnalités de sécurité
- Techniques d'authentification, de contrôle d'accès (locaux, réseaux, systèmes...) ;
- Techniques de filtrages ;
- Isolation des systèmes, DMZ.

Protéger les systèmes d'information
- Méthodologie de protection des SI ; actions avant/pendant/après ;
- Gestion des incidents ;
- Plan de reprise d'activité ; plan de continuité d'activité ; résilience du SI.

Organiser la sécurité en entreprise
- Comprendre le management de la sécurité ;
- Audits, gestion de crises, s'initier à la cyber-résilience ;
- Plan de communication et sensibilisation des personnels.

Exploiter les référentiels sur une étude de cas

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.