INFORMATIQUE, SÉCURITÉ DES SI

Executive certificate : Architectures résilientes et défense des SI

Cet executive certificate s'intéresse à la conception d'architectures informatiques résilientes et à la défense des systèmes informatiques. Il permet notamment de comprendre les attaques informatiques et de mettre en oeuvre la détection d'intrusion, la détection de vulnérabilité, les tests de pénétration et la surveillance des systèmes.

PUBLIC ET PRÉ-REQUIS

Professionnels des métiers de l'informatique.

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 oeuvres ; protection des logiciels.

Sécurisation de systèmes (travaux pratiques)

- Rappels sur Linux ;
- Sécurisation de Linux ;
- Sécurisation des services Linux ;
- Sécurisation Windows.

Informations clés

Durée :
56 heures

€ Tarif :
Sur mesure

Nous consulter

Contact

fc@utc.fr

OBJECTIFS & COMPÉTENCES

Cette formation a pour objectif de :

- Comprendre et utiliser des systèmes de gestion d'identité et d'authentification ;
- Comprendre et déployer des systèmes de stockage redondants ;
- Comprendre et déployer des architectures à haute disponibilité ;
- Comprendre et déployer des réseaux d'entreprise sécurisés ;
- Comprendre les attaques informatiques ;
- Savoir détecter les intrusions ;
- Pratiquer le test de pénétration ;
- Surveiller les systèmes.

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 ;
- Ateliers-projets et études de cas.

Modalités d'évaluation

- Évaluation effectuée à l'occasion des tests de connaissances ;
- Travaux de mise en application ;
- Étude.

POUR CANDIDATER

Inscription via formulaire (voir site web).