INFORMATIQUE, SÉCURITÉ DES SI

Executive certificate : Risques et protection des SI

Cet executive certificate 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. Il introduit par ailleurs la cryptographie, les principales techniques de chiffrement, la cryptanalyse, les architectures de confiance, la sécurité des données et les chaînes de blocs. Il aborde les fondamentaux de la cryptographie et présente les applications pour sécuriser les SI. Enfin, 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.

Informations clés

Durée :
84 heures

€ Tarif :
Sur mesure

Nous consulter

Contact

fc@utc.fr

PUBLIC ET PRÉ-REQUIS

Professionnels des métiers de l'informatique.

PROGRAMME

Comprendre et analyser les risques des systèmes informatiques

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.

Comprendre et utiliser les moyens cryptographiques pour sécuriser un SI

Comprendre la cryptanalyse

- Histoire de la cryptographie ; rappels mathématiques ;
- Cryptographie, stéganographie, cryptanalyse, cryptographie quantique (BB84) ;
- Pratiquer la cryptanalyse sur un exemple simple.

Maîtriser les techniques de chiffrement

- Chiffrements asymétriques et symétriques ;
- Principaux algorithmes (RC4, DES, AES, Diffie-Helmann, RSA, courbes elliptiques) ;
- Chiffrement des données sur place, chiffrement de partitions (crypt, encrypt, scrypt, luks, GPG, SMIME) ;
- Chiffrement de flux de données (SSH, SSL, négociation TLS, HTTPS).

Utiliser la signature électronique

- Fonctions de hachage (md5sum, SHA) ;
- Mise en oeuvre de la signature numérique (OpenSSL), best practices.

Comprendre et déployer des architectures à clé publique

- Certificats (norme X509v3), standard PKCS ;
- Mise en oeuvre d'une PKI.

Comprendre la mise en place d'écosystèmes de confiance

- Protection des données ;
- Best practices

Prévenir et protéger les systèmes informatiques

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 ;
- Comprendre les enjeux de la cybersécurité.

OBJECTIFS & COMPÉTENCES

Cette formation a pour objectif de :

- 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.
- Comprendre la cryptographie ;
- Savoir chiffrer, déchiffrer des données et des flux de données ;
- • Utiliser la signature électronique ;
- Connaître les best practices et les principaux algorithmes ;
- Comprendre les certificats ; déployer une PKI ;
- Construire un écosystème de confiance et protéger les données.
- 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.

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.

ET APRÈS ?

Executive certificate en cybersécurité Architectures Résilientes et Défense des Systèmes d'Information

POUR CANDIDATER

Inscription via formulaire (voir site web).