Certification professionnelle à la Gouvernance de la Sécurité des Systèmes d'Information et des Réseaux

PRÉSENTATION GÉNÉRALE

Aujourd'hui, les entreprises doivent ouvrir de plus en plus leur système d'information non seulement entre leurs sites, mais aussi à leurs clients, à leurs fournisseurs, à leurs partenaires et, plus généralement, aux utilisateurs d'internet. La sécurité dans les SI et les réseaux constitue un enjeu stratégique pour tous les responsables de réseaux, de systèmes informatiques, de services web, de paiements sécurisés...
La formation répond aux exigences de la gouvernance de la sécurité avec une approche globale couvrant les aspects techniques, méthodologiques, organisationnels et réglementaires. Elle permet d'acquérir les compétences nécessaires à l'élaboration et la mise en place un plan de sécurité destiné à la protection des ressources vitales, contre les attaques internes et externes.
Elle est organisée à temps partiel à raison de quelques jours par mois pour permettre la poursuite d'une activité professionnelle.

OBJECTIFS ET COMPÉTENCES VISÉES

Cette formation fournit aux stagiaires les compétences techniques et organisationnelles pour définir, déployer et gérer une architecture de sécurité dans les différents contextes professionnels auxquels ils seront confrontés.

À l'issue de la formation, les participant seront capables de :

- Définir la gouvernance de la sécurité des systèmes d'information de l'entreprise
- Mettre en place des mécanismes de sécurité
- Élaborer et mettre en œuvre un plan de sécurité destiné à la protection des ressources vitales de l'entreprise
- Concevoir une architecture de sécurité

CONDITIONS DE PARTICIPATION

- Dossier de candidature
- Test de niveau
- Entretien individuel pour valider le projet professionnel

PARTICIPANTS CONCERNÉS ET PRÉREQUIS

- Techniciens ou ingénieurs réseaux sans expérience en sécurité
- Chefs de projets ou responsables de solutions intégrant des contraintes de sécurité
- Consultants, architectes de systèmes
- Administrateurs systèmes et réseaux, équipes sécurité des réseaux, responsables informatiques, responsables des systèmes d'information
- Intégrateurs de systèmes et managers impliqués dans la sélection, la mise en œuvre ou le support d'un accès sécurisé à l'entreprise

Des connaissances de base sur les réseaux (TCP/IP) et les systèmes informatiques, sont vivement recommandées pour tirer un meilleur profit de cette formation.

PROGRAMME :

Gouvernance de la sécurité : aspects méthodologiques, organisationnels et réglementaires de la sécurité des systèmes d'information de l'entreprise.

Ce module est dédié à l'étude des concepts, des méthodes liées à la sécurité ainsi que les différentes phases d'élaboration d'un plan de sécurité du SI de l'entreprise.

- Gestion des risques
- Identification des acteurs et métiers de la sécurité
- Législation SSI et RGPD
- Normes ISO 27000
- Évaluation Critères Communs
- Politique de sécurité
- Métiers de la sécurité

Travaux pratiques :

- Méthodologie EBIOS
- Étude de cas : analyse des risques d'un SI et études scénarios de menace
- Atelier de mise en œuvre d'un cadre réglementaire et normatif

Outils et Mécanismes de Sécurité

Ce module est consacré à l'étude des systèmes cryptographiques qui contribuent à la mise en place des services de sécurité.
Il présente les méthodes de chiffrement et leur mise en œuvre pour assurer les services de confidentialité, d'intégrité, d'authentification ou de signature numérique. Il traite également des mécanismes de gestion des clés de chiffrement et de déploiement des infrastructures de gestion de clés publiques (PKI).
Il dresse le panorama des outils associés à la gestion d'identité et les moyens d'authentification.

- Algorithmes cryptographiques
- Protocoles cryptographiques
- Sécurité de la messagerie
- Gestion des clés - PKI
- Moyens d'authentification
- Gestion d'identités
- Cartes bancaires
- Techniques biométriques

Travaux pratiques :.

- Techniques cryptographiques du protocole de messagerie
- Étude de cas : analyse de protocoles cryptographiques d'applications de commerce électronique
- Atelier : contrôle d'accès

Sécurité des Systèmes d'Information

Ce module est consacré à l'étude des moyens de sécurisation d'un système informatique, élément vital du système d'information de l'entreprise.
Il permet d'aborder les plans de secours et de sauvegarde des moyens techniques, organisationnels et humains nécessaires à la continuité des services et la protection du patrimoine informationnel de l'entreprise.
Il permet également de connaître les techniques d'audit et de détection d'intrusion pour la recherche de vulnérabilités.
Il donne une vision complète des mécanismes de sécurité offerts par un système d'exploitation et des outils d'administration de la sécurité.

- Cybercriminalité
- Infections informatiques
- Audit
- Contrôles d'accès physiques et logiques
- Sécurité des postes de travail et des systèmes d'exploitation

Travaux pratiques :

- Étude cas : recherche et correction de vulnérabilités

Sécurité des réseaux et des applications

Ce module permet d'acquérir les connaissances et de choisir les outils nécessaires pour concevoir des architectures de sécurité dans les environnements Intranet/Extranet de l'entreprise.
Il présente les différents protocoles offrant des services de sécurité basés sur les réseaux fixes (IPsec, SSL…), mobiles (GSM, GPRS, UMTS) et WIFI (WEP, WPA) puis décrit les fonctions de sécurité disponibles (filtrage, NAT, VPN) dans les équipements comme les routeurs ou les firewalls. La sécurité des applications comme la Voix sur IP et les réseaux de capteurs y est également traitée.

- Vulnérabilité des protocoles et des services
- Protocoles de sécurité (IPsec, SSL)
- Équipements de sécurité (firewall, routeur)
- Sécurité des réseaux mobiles
- Sécurité de la téléphonie sur IP
- Architectures de sécurité
- Supervision de la sécurité, détection d'intrusion

Travaux Pratiques :

- Filtrage de trafic, ACL
- VPN / IPsec
- Sécurité WiFi : Protocole WEP, Authentification EAP / Radius
- Atelier d'élaboration et de test d'une architecture de réseau privé virtuel

RESPONSABLE PÉDAGOGIQUE

Abdallah M'HAMED
Enseignant-chercheur au département "Réseaux et Services de Télécommunications" de Télécom SudParis, ses enseignements sont principalement axés sur les services et mécanismes de sécurité, les systèmes cryptographiques et les modèles de contrôle d'accès. Ses travaux de recherche portent sur les protocoles d'authentification, la préservation de la vie privée et les modèles de confiance dans les environnements intelligents dédiés aux personnes dépendantes.

ÉVALUATION ET CERTIFICATION

Les participants ayant réussi l'ensemble des épreuves se verront attribuer la certification professionnelle « Gouvernance de la sécurité des systèmes d'information et des réseaux » de Télécom SudParis inscrite au Répertoire Spécifique de France Compétence sous le numéro RS5053.

Les modalités d'évaluation sont les suivantes :

- Tests d'évaluation des connaissances acquises
- Ateliers de mise en œuvre et de simulation de cas pratiques
- Études de cas relatives à des problématiques de sécurité
- Rédaction d'une réponse à un appel d'offres et restitution orale devant un jury

ORGANISATION PÉDAGOGIQUE

Le parcours est proposé **à temps partiel sur 9 mois**. Il comprend une formation suivie d'une période de 2 mois dédiée à l'élaboration d'une réponse à appel d'offres.

- La formation comprend **19 jours de présentiel à Paris, à raison d'en moyenne 3 jours par mois sur 6 mois**. Elle compte des enseignements académiques, des études de cas, des travaux pratiques et des ateliers de mises en situation professionnelle
- Au cours des 2 mois suivant la formation, les participants regroupés en équipe élaborent une **réponse à un besoin client présenté sous forme d'un appel d'offres**. Elle donne lieu à la rédaction d'un document présentant la solution proposée, puis à une **restitution orale devant un jury**.

INFORMATIONS ET CONTACT

La prochaine session inter-entreprises est en cours de planification avec notre partenaire.

- **Prix : 8 900€** nets de taxe
- **Durée :** 19 jour(s) de formation en présentiel (133 heures)
- **Lieu :** Paris (2e arrondissement)

Pour plus d'information, contacter : Joelle.monange@telecom-sudparis.eu