?

FL9CS01 **8 500 €** **19 jour(s)**

CES Sécurité des Systèmes d'Information et des Réseaux

OBJECTIFS

- 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.

PROGRAMME

Gouvernance de la sécurité : aspects méthodologiques, organisationnels et réglementaires de la sécurité des systèmes d'information (SI) 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

- Méthode EBIOS
- Étude de cas : analyse des risques d'un SI
- 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.

DATES ET LIEUX

Nous contacter pour les sessions à venir

PUBLIC / PREREQUIS

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
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 recommandés pour tirer un meilleur profit de cette formation.

COORDINATEURS

Abdallah M'HAMED

Enseignant-chercheur au département "Réseaux et Services de Télécommunications" à 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.

- 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
- Étude de cas : analyse de protocoles cryptographiques
- Atelier : Contrôle d'accès

Sécurité des systèmes informatiques

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
- Étude de cas : étude des 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, etc.), 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 (Voice over IP – VoIP) 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

ORGANISATION PEDAGOGIQUE

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 raison d'en moyenne 3 jours par mois entre janvier et juin. 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 suivants la formation, les participants regroupés en équipe élaborent une réponse à un besoin client présenté sous la 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.

MODALITES PEDAGOGIQUES

Cours en présentiel, conférences téléphoniques, travail à distance (cours en ligne, suivi pédagogique sur la plateforme Moodle), réalisation d'études de cas.

Travaux pratiques

- Filtrage de trafic, ACL
- VPN/IPsec
- Sécurité WiFi