

SECURITE SYSTEMES ET RESEAUX

PROGRAMME DETAILLE
CERTIFICAT D'ENSEIGNEMENT SPECIALISE
Accrédité B.A.D.G.E par la Conférence des Grandes Ecoles

Date de démarrage prévu : 26 mars 2012 (1^{er} présentiel).

PROGRAMME TOTAL : 248 h

Sur 5 mois.

Alternance de Présentiel, Cours à distance et Travail Personnel

- Présentiel : 120 h (48%)
- Travail à distance et personnel (e-learning..): 128 h (52%)

- . Présentiel de 120 h réparties en :
 - 16 jours de cours – (7h) total de 112 h
 - 4 conférences téléphoniques de 2 heures (8h)
- . Enseignement à distance
(plate-forme e-learning,QCM, Etude de cas...) : - 2h/jour sur 64 jours (128 h)

Sessions prévisionnelles de présentiel (*)

26-27-28-29 mars 2012
24-25-26-27 avril 2012
21-22-23-24 mai 2012
25-26-27-28-29 juin 2012
3 septembre 2012

(*) Les dates sont susceptibles d'être modifiées

Objectifs de la formation :

L'objectif de cette formation est de répondre aux exigences de la gouvernance de la sécurité dans les entreprises avec une approche globale couvrant les aspects techniques, méthodologiques, organisationnels et réglementaires.

Elle permet d'apporter les connaissances nécessaires à l'élaboration et la mise en place d'un plan de sécurité destiné à la protection des ressources vitales de l'entreprise, contre les agressions internes et externes de toute nature : intrusions, destructions ou vols.

Les compétences acquises au cours de cette formation permettront aux stagiaires :

- de participer à l'ensemble du processus d'une étude de sécurité, depuis le recensement des besoins et des risques, à la mise en oeuvre de solutions de sécurité ;
- d'intégrer les aspects organisationnels, méthodologiques et réglementaires ;
- de mieux appréhender les techniques, outils et protocoles de sécurité ;
- de disposer des compétences nécessaires pour concevoir et mettre en oeuvre une architecture de sécurité.

Le volume important consacré aux bureaux d'étude et aux travaux pratiques permettra la maîtrise des produits et outils de sécurité, comme :

- le montage d'un schéma directeur de la sécurité
- la pratique des techniques cryptographiques
- l'étude d'une PKI
- la recherche de failles de sécurité et les tests d'intrusion
- la configuration et l'exploitation de firewalls
- l'installation de réseaux privés virtuels sécurisés
- la mise en oeuvre des protocoles de sécurité

Programme :

Module 1 : Aspects méthodologiques, organisationnels et réglementaires de la sécurité des systèmes d'information de l'entreprise

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

- Analyse des menaces pour protéger les systèmes/données de l'entreprise
- Gestion des risques engendrés par l'utilisation d'Internet et Extranet.
- Identification des acteurs et métiers de la sécurité
- Services et mécanismes de sécurité
- Législation, normes, certifications et organismes associés.
- Conception d'un plan global de sécurité
- Identifier les risques de sécurité qui nécessitent une politique de sécurité
- Evaluation de l'éthique de l'informatique et des pirates informatiques
- Déploiement d'une politique de sécurité.

Contenu :

- Principes généraux et concepts de base
- Schémas directeur – Schéma organisationnel
- Audit et conseil
- Plans de secours et de sauvegarde
- Méthodologies d'analyse des risques
- Droit de la SSI
- Politiques de sécurité

- Evaluation selon les critères communs
- Méthodologies d'analyse des risques

Ce module est illustré par une étude de cas basé sur l'outil RISICARE.

Module 2 : *Systèmes cryptographiques*

Ce module est consacré à l'étude des systèmes cryptographiques qui contribuent à la mise en place des services de sécurité.

Il permet de mieux comprendre 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).

Ce module est illustré par des travaux pratiques sur l'implémentation des techniques cryptographiques dans la messagerie (PGP) et les cartes à puces.

Il est ainsi nécessaire de :

- Maîtriser les caractéristiques des différentes familles d'algorithmes cryptographiques
- Comprendre l'importance des techniques cryptographiques dans la mise en place des services de sécurité.
- Etre en mesure de proposer le type d'algorithme en fonction du service de sécurité à mettre en place, selon des critères techniques et juridiques.
- Comprendre les problèmes liés à la gestion des clés de chiffrement
- Mettre en place une infrastructure de gestion de clés publiques (PKI)

Contenu :

- Techniques cryptographiques
- Protocoles cryptographiques
- Sécurité de la messagerie (PGP)
- Gestion des clés - PKI
- Moyens d'authentification

Module 3 : *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 fournit une vision complète des mécanismes de sécurité offerts par un système d'exploitation (contrôle d'accès aux fichiers, identification/authentification, contrôles sur les processus, virus...) et des outils d'administration de la sécurité.

Contenu :

- Cybercriminalité
- Sécurité physique et logique
- Infections informatiques
- Plan de secours et de sauvegarde
- Audit
- Détection d'intrusion

- Contrôles d'accès
- Sécurité des systèmes d'exploitation (Windows, Linux)

Module 4 : Sécurité des réseaux et des applications

Ce module permet d'acquérir les connaissances et d'approcher 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.

Ce module est illustré par des travaux pratiques (configuration de firewalls, filtrage de trafic, mise en place d'un proxy Web et VPN, Chiffrement WIFI, ...).

Contenu :

- Vulnérabilité des protocoles et des services
- Protocoles de sécurité (IPsec, SSL, VPN)
- Equipements de sécurité (firewall, routeur)
- Sécurité et mobilité
- Architectures de sécurité
- Supervision de la sécurité, détection d'intrusion
- Travaux Pratiques :
 - Filtrage de trafic
 - Mise en place d'un proxy Web
 - VPN / IPsec sur routeur

Travaux Pratiques en Laboratoire et plates-formes proposés

1. Salle « Réseaux »

La salle de travaux pratiques « Réseaux et Sécurité » est entièrement pré-câblée. Un Hub central, auquel arrivent toutes les connexions des prises murales, permet de relier la salle TP à l'extérieur, à travers un routeur.

Huit postes de travail sont disponibles ; Chaque poste de travail est composé d'un routeur Cisco, d'un Hub et de deux PC qui jouent alternativement le rôle d'analyseur réseau, de firewall ou de station de travail en fonction des thèmes traités dans les travaux pratiques. Il représente un « site » d'une entreprise. Les sites sont reliés entre eux par un réseau longue distance symbolisé par le réseau de la salle.

2. Salles « Stations de travail»

Deux salles de Travaux Pratiques équipées chacune de 16 Stations de travail Unix de type Ultra5 sous Solaris7, seront également utilisées.