Cycle certifiant Responsable Sécurité SI certificat professionnel FFP

-Réference: **PL-76** -Durée: **12 Jours (84 Heures)**

Les objectifs de la formation

- Connaître les différents domaines de la sécurité SI
- Faire une analyse des risques de sécurité
- Sécuriser le réseau et les applications
- Définir un plan de secours et de continuité

A qui s'adesse cette formation ?

POUR QUI :

- Ingénieurs, experts, consultants en informatique.

PRÉREQUIS :

- Bonnes connaissances en systèmes et réseaux informatiques.

Programme

- **La sécurité des systèmes d'information**
  - La notion et les types de risque (potentialité, impact, accident, erreur, malveillance).
  - La classification DIC.
  - La gestion du risque (prévention, protection, report de risque, externalisation).
  - RSSI, chef d'orchestre de la sécurité.
  - Rôle et responsabilité.
  - Les cadres normatifs et réglementaires.
  - Vers la gouvernance informatique, les liens avec ITIL et CMMI.
  - La norme ISO dans une démarche Systèmes de management.
  - La certification ISO 27001.
  - L'analyse de risque.
  - Comment constituer sa propre base de connaissances menaces/vulnérabilités ? Les méthodes en activité : EBIOS/FEROS, MEHARI.
  - Les audits de sécurité.

Programme

- Les bonnes pratiques de la norme 19011 appliquées à la sécurité.

- **Sensibilisation et communication**
  - Mettre en place un plan de sensibilisation et de communication.
  - La charte de sécurité, son existence légale, son contenu, sa validation.
  - Couverture des risques.
  - Plans de secours, de continuité, de reprise et de gestion de crise.
  - Concevoir des solutions optimales.
  - Démarche pour les solutions de sécurisation adaptées pour chaque action.
  - Définition d'une architecture cible.
  - Choisir entre IDS et IPS, le contrôle de contenu comme nécessité.
  - Déployer un projet PKI, les pièges à éviter.
  - Les techniques d'authentification, SSO, fédération d'identité.
  - Les principes juridiques applicables au SI.
  - La responsabilité civile délictuelle et contractuelle.
  - Recommandations pour une sécurisation légale du SI.
  - La cybersurveillance des salariés, limites et contraintes légales.

- **La sécurité des réseaux et de l'Internet**
  - Evolution de la cybercriminalité. Nouveaux usages (Web 2.0, virtualisation, Cloud Computing...) et risques associés.
  - - Outils et méthodes d'intrusion par TCP-IP. Les attaques applicatives (DNS, HTTP, SMTP, etc.).
  - - Sécurité des postes clients. Les menaces : backdoor, virus, rootkit... Le rôle du firewall personnel et ses limites.
  - - Sécurité du sans-fil (Wi-Fi et Bluetooth). Attaques spécifiques (Wardriving, failles WEP et EAP).
  - - Technologie firewall et proxy. Evolution de l'offre Firewall (appliance, VPN, IPS, UTM...).
  - - Techniques cryptographiques. Algorithmes à clé publique : Diffie Hellman, RSA... Scellement et signature électronique.
  - - Sécurité pour l'Intranet/Extranet. Les attaques sur SSL/TLS (sslstrip, sslnif...). Annuaire LDAP et sécurité. - Réseaux Privés Virtuels (VPN). IPSec. Les modes AH et ESP, IKE et la gestion des clés.

- **La sécurité des applications et la supervision**
  - Les principales techniques d'attaque des applications (buffer overflow, XSS, SQL Injection, vol de session).
  - Le processus SDL (Security Development Lifecycle).

Programme

- Utilisation de la technique de "fuzzing".
- Les outils de revue de code orientés sécurité.
- Le Firewall applicatif (WAF).
- Hardening et vérification d'intégrité.
- Gestion et supervision active de la sécurité.
- Les tableaux de bord Sécurité.
- La norme ISO 27004.
- Les missions du RSSI dans le suivi de la sécurité.
- Les audits de sécurité (techniques ou organisationnels).
- Les tests de vulnérabilité ou tests d'intrusion.
- Les outils Sondes IDS, Scanner VDS, Firewall IPS.
- Consigner les preuves et riposter efficacement.
- Se tenir informé des nouvelles vulnérabilités.
- Gérer les mises à niveaux.
- Savoir réagir en cas d'incidents.
- Les services indispensables : où les trouver ?

L'analyse de risques

- Rappels sur les terminologies ISO 27000.
- Identification et classification des risques.
- L'analyse de risques selon l'ISO.
- Les méthodes d'analyse de risques EBIOS 2010 et MEHARI 2010.
- Les autres méthodes internationales.
- Comment choisir la meilleure méthode sur la base d'exemples et étude de cas pratiques ? Une méthode globale ou une méthode par projet.
- Le vrai coût d'une analyse de risques.

Le plan de secours et de continuité

- Les enjeux pour l'entreprise d'une stratégie de continuité : lois et réglementations, normes et standards.
- Définir la stratégie de continuité.
- Les phases d'un projet plan de continuité.
- L'analyse des risques pour le plan de continuité.
- L'identification des activités critiques.

Programme

- Les éléments et le budget pour élaborer les scénarios.
- Les équipes de secours : constitution, rôles.
- Les principes de déclenchement du plan de secours.

(+212) 5 22 27 99 01

(+212) 6 60 10 42 56

Contact@skills-group.com

Nous sommes à votre disposition :
De Lun - Ven 09h00-18h00 et Sam 09H00 – 13H00

Angle bd Abdelmoumen et rue Soumaya, Résidence Shehrazade 3, 7éme étage N° 30
Casablanca 20340, Maroc