Cybersécurité réseaux/Internet, synthèse protection du SI et des communications d'entreprise

-Réference: **SII-303** -Prix: **5500 DH/P** -Durée: **3 Jours (21 Heures)**

Les objectifs de la formation

- Connaître l'évolution de la cybercriminalité et de ses enjeux
- Maîtriser la sécurité du Cloud, des applications, des postes clients
- Comprendre les principes de la cryptographie
- Gérer les processus de supervision de la sécurité SI

A qui s'adesse cette formation ?

POUR QUI :

- RSSI, DSI, architectes, développeurs, chefs de projets, commerciaux avant-vente, administrateurs système & réseau.

Programme

- **Sécurité de l'information et cybercriminalité**
  - Principes de sécurité : défense en profondeur, politique de sécurité.
  - Notions fondamentales : risque, actif, menace.
  - Les méthodes de gestion de risques (ISO 27005, EBIOS, MEHARI).
  - Panorama des normes ISO 2700x.
  - Evolution de la cybercriminalité.
  - L'identification des agents de menace.
  - Les nouvelles menaces (APT, spear phishing, watering hole, exploit kit.
  -).
  - Les failles de sécurité dans les logiciels.
  - Le déroulement d'une cyberattaque (NIST).
  - Les failles 0day, 0day Exploit et kit d'exploitation.
- **Firewall, virtualisation et Cloud computing**

Programme

- Les serveurs proxy, reverse proxy, le masquage d'adresse.
- La protection périmétrique basée sur les firewalls.
- Différences entre firewalls UTM, enterprise, NG et NG-v2.
- Produits IPS (Intrusion Prevention System) et IPS NG.
- La mise en place de solutions DMZ (zones démilitarisées).
- Les vulnérabilités dans la virtualisation.
- Les risques associés au Cloud Computing selon l'ANSSI, l'ENISA et la CSA.
- Le Cloud Control Matrix et son utilisation pour l'évaluation des fournisseurs de Cloud.

- **Sécurité des postes clients**
  - Comprendre les menaces orientées postes clients.
  - Le rôle du firewall personnel et ses limites.
  - Les logiciels anti-virus / anti-spyware.
  - Comment gérer les correctifs de sécurité sur les postes clients ? Comment sécuriser les périphériques amovibles.
  - Le contrôle de conformité du client Cisco NAC, Microsoft NAP.
  - Les vulnérabilités des navigateurs et des plug-ins.
  - Drive-by download.

- **Fondamentaux de la cryptographie**
  - Législation et principales contraintes d'utilisation en France et dans le monde.
  - Les techniques cryptographiques.
  - Les algorithmes à clé publique et symétriques.
  - Les fonctions de hachage.
  - Les architectures à clés publiques.
  - Programmes de cryptanalyse de la NSA et du GCHQ.

- **Authentification et habilitation des utilisateurs**
  - L'authentification biométrique et les aspects juridiques.
  - L'authentification par challenge/response.
  - Techniques de vol de mot de passe, brute force, entropie des secrets.
  - L'authentification forte.
  - Authentification carte à puce et certificat client X509.
  - Architectures "3A" : concept de SSO, Kerberos.

Programme

- Les plates-formes d'IAM.
- La fédération d'identité via les API des réseaux sociaux.
- La fédération d'identité pour l'entreprise et le Cloud.

- **La sécurité des flux**
  - Crypto API SSL et évolutions de SSL v2 à TLS v1.
  - 3.
  - Les attaques sur les protocoles SSL/TLS.
  - Les attaques sur les flux HTTPS.
  - Le confinement hardware des clés, certifications FIPS-140-2.
  - Evaluer facilement la sécurité d'un serveur HTTPS.
  - Le standard IPsec, les modes AH et ESP, IKE et la gestion des clés.
  - Surmonter les problèmes entre IPSec et NAT.
  - Les VPN SSL.
  - Quel intérêt par rapport à IPSec ? Utilisation de SSH et OpenSSH pour l'administration distante sécurisée.
  - Déchiffrement des flux à la volée : aspects juridiques.
- **Sécurité Wifi**
  - Attaques spécifiques Wifi.
  - Comment détecter les Rogue AP.
  - Mécanismes de sécurité des bornes.
  - Vulnérabilités WEP.
  - Faiblesse de l'algorithme RC4.
  - Description des risques.
  - Le standard de sécurité IEEE 802.
  - 11i.
  - Architecture des WLAN.
  - Authentification des utilisateurs et des terminaux.
  - L'authentification Wifi dans l'entreprise.
  - Outils d'audit, logiciels libres, aircrack-ng, Netstumbler, WifiScanner.
- **Sécurité des Smartphones**
  - Les menaces et attaques sur la mobilité.

Programme

- iOS, Android, Windows mobile : forces et faiblesses.
- Virus et codes malveillants sur mobile.
- Les solutions de MDM et EMM pour la gestion de flotte.

- **Sécurité des applications**
  - La défense en profondeur.
  - Applications Web et mobiles : quelles différences en matière de sécurité ? Les principaux risques selon l'OWASP.
  - Focus sur les attaques XSS, CSRF, SQL injection et session hijacking.
  - Les principales méthodes de développement sécurisé.
  - Quelle clause de sécurité dans les contrats de développement ? Le pare-feu applicatif ou WAF.
  - Evaluer le niveau de sécurité d'une application.

- **Gestion et supervision active de la sécurité**
  - Les tableaux de bord Sécurité.
  - Les audits de sécurité.
  - Les tests d'intrusion.
  - Aspects juridiques des tests d'intrusion.
  - Sondes IDS, scanner VDS, WASS.
  - Comment répondre efficacement aux attaques ? Consigner les éléments de preuve.
  - Mettre en place une solution de SIEM.
  - Les labels ANSSI (PASSI, PDIS & PRIS) pour l'externalisation.
  - Comment réagir en cas d'intrusion ? L'expertise judiciaire : le rôle d'en expert judiciaire (au pénal ou au civil).
  - L'expertise judiciaire privée.

(+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