

## ÉLÉMENTS DU PROGRAMME

### INITIATION AUX TECHNIQUES DE CYBERSÉCURITÉ

#### 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).
- L'identification des agents de menace.
- Les vulnérabilités dans la virtualisation.

#### 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 ?
- 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.

#### La sécurité des flux

- Les attaques sur les flux HTTPS.
- Evaluer facilement la sécurité d'un serveur HTTPS.
- Utilisation de SSH et OpenSSH pour l'administration distante sécurisée.

#### Sécurité Wifi

- Attaques spécifiques Wifi.
- 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.

#### Sécurité des Smartphones

- Les menaces et attaques sur la mobilité.
- 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

- Applications Web et mobiles : quelles différences en matière de sécurité?
- Focus sur les attaques XSS, CSRF, SQL injection et session hijacking.
- Les principales méthodes de développement sécurisé.

#### Gestion et supervision active de la sécurité

- Les tableaux de bord Sécurité.
- Les audits de sécurité.
- Les tests d'intrusion.

#### Sauvegarde et reprise des données

- Les limites de la sauvegarde manuelle et locale
- Les sauvegardes incrémentales et différentielles
- Le stockage des sauvegardes

#### Social Engineering et contre-mesures

- Apprendre à identifier les attaques par manipulation
- Sensibilisation du personnel
- Évaluer la valeur de l'information

### INITIATION AU RÉGIME GÉNÉRAL DE PROTECTION DES DONNÉES [RGPD / GDPR]

#### Environnement réglementaire

- CNIL, loi informatique et libertés
- ANSSI, CEPD (EDPS), G29 (directive 95/46/CE)
- Réforme européenne de mai 2018
- Statut du DPO
- Registre des traitements & code conduite
- Procédures internes
- Gestion des réclamations, gestion des données
- Bilan annuel