CNFCPP	**FICHE PROGRAMME D'UNE ACTION DE FORMATION**	Réf: **FORM.FINC.02** Version : 00 Date d'application : 20/04/09

Thème : Sécurité des Systèmes d'Information: un enjeu majeur pour les entreprises
Population cible :

- Directeurs des Systèmes d'Information (DSI);
- Responsables de la Sécurité des Systèmes d'Information (RSSI);
- Ingénieurs et Administrateurs de la Sécurité;
- Auditeurs, Architectes et Consultant en Sécurité;
- Enseignants, Chercheurs et Etudiants en Sécurité.

Objectifs de le formation :	**Objectifs pédagogiques :**
L'environnement lié aux technologies de l'information et de la communication est la cible de nombreuses menaces. L'ouverture des réseaux, la diversité des technologies et leur complexité croissante ont renforcé la vulnérabilité des systèmes d'information face à divers types de menaces intentionnelles et accidentelles. L'objectif de la formation est de: – Prendre connaissance des menaces auxquelles sont exposés les systèmes d'information, ainsi que les risques possibles et les dégats en cas d'attaques Maîtriser les concepts techniques de la Sécurité des Systèmes d'Information (SSI): protocoles, architecture, attaques, fonctionnalités de base, est indispensable pour maintenir un système efficace et un niveau de sécurité répondant à aux besoins actuels et futurs	Connaissance basique des systèmes et des réseaux informatiques.

Jours	**Contenus/ Concepts clés à aborder**	**Méthodes et Moyens Pédagogiques**	**Durée (Heures)**	
			Théorie	**Pratique**
J1	Accueil, enregistrement et ouverture du séminaire **<u>Introduction à la Sécurité du SI</u>** ▪ Problèmes et enjeux de sécurité dans les SI ▪ Objets et objectifs de la sécurité ▪ Vulnérabilités et menaces ▪ Classification des attaques sur un système d'information ▪ Fraudes et malveillance informatique ▪ Risques de sécurité et impacts métier o Sortie d'informations sensibles vers la concurrence o Atteinte à l'image	Exposés, travaux pratiques et échanges interactifs.	**3**	**3**

	○ Defacement du site web ○ Utilisation frauduleuse du SI interne et traçabilité ○ Chantage au déni de service **Politiques de Sécurité** ▪ Politiques de sécurité ○ Politique de sécurité du système d'information (PSSI) ○ Politique de sécurité informatique (PSI) – Politique de sécurité réseau – Politique de sécurité système – Politique des mots de passe – Politique de confidentialité – Politique de sauvegarde des données – Politique pour la protection antivirale ○ Politique de sécurité physique ▪ Concepts de base de la sécurité ○ Défense en profondeur ○ Moindre privilège ○ Séparation des privilèges ○ E/S unique au réseau ○ Simplicité			
J2	**Système de Management de la Sécurité** ▪ Organisation de la sécurité, approche managériale, sécurité globale et connaissance du contexte ▪ Normes ISO/CEI 27001 et 27002, Annexe SLA des Directives de l'ISO ▪ Notion de conformité et de certification ▪ Gestion du risque: Normes ISO/IEC 27005 et ISO 31000 ▪ Méthodes d'analyse des risques ▪ Référentiels tiers : ANSSI, ENISA, etc	Exposés, travaux pratiques et échanges interactifs.	**3**	**3**

	Sécurité des Systèmes d'Exploitation ▪ Sécurité des systèmes d'exploitation o Problèmes de sécurité des systèmes d'exploitation – Points d'entrées – Causes de disfonctionnement – Menaces des malwares – Sécurité de la machine – Sécurité du BIOS – Chargeur du système (boot loader) – Connexion aux réseaux – Verrouillage o Mécanismes de protection des systèmes d'exploitation – Contrôle d'accès machine et gestion des comptes – Protection des fichiers et des données – Durcissement des machines – Veille des vulnérabilités o Outils de protection des systèmes – Antivirus – Parefeux – Anti-espion – Contrôle d'intégrité – Détecteur d'intrusion machine			
J3	**Sécurité des Accès Réseaux** ▪ Sécurité du réseau o Mécanismes de contrôle d'accès réseau o Protocoles, ports et services o Zones, cloisonnement et filtrage IP o Parefeux ▪ Déploiement des parefeux ▪ Traduction d'adresses réseau (NAT) ▪ Filtrage des paquets vs filtrage applicatif o Accès distants (VPN PPTP, IPSec, SSL et SSH) o Détection d'intrusion réseau o Mécanismes de haute disponibilité (fail over, load balancing, ...) o Supervision des équipements réseaux	Exposés, travaux pratiques et échanges interactifs.	3	3

	Sécurité des Systèmes Informatiques (3/3) ▪ Attaques sur les protocoles réseaux o Cas du Dynamic Host Configuration Protocol (DHCP) o Cas du Domain Name Service (DNS) o Cas du File Transfer Protocol (FTP) o Cas du Hypertext Transfer Protocol (HTTP)			
J4	**Sécurité des Applications et des Services** ▪ Contrôle d'accès et privilèges ▪ Vulnérabilités, bogues, erreurs et défauts logiciels ▪ Tests et validation des logiciels ▪ Sureté de fonctionnement ▪ Audit du code source ▪ Sécurité des applications o Cas du Web o Cas des applications mobiles **Audit de Sécurité des Systèmes d'Information (1/2)** ▪ Référentiels de sécurité et contexte normatif relatif à l'audit de sécurité du système d'information ▪ Types d'audits des systèmes d'Information o Audit interne/ externe o Audit technique / organisationnel o Audit en boite noire / en boite blanche o Audit des vulnérabilités o Audit de conformité Audit intrusif	Exposés, travaux pratiques et échanges interactifs.	3	**3**
J5	**Audit de Sécurité des Systèmes d'Information (2/2)** ▪ Démarche d'un audit technique de sécurité o Recueil des informations o Identification des vulnérabilités o Tests de pénétration o Analyse de résultats et rédaction de rapport ▪ Outils d'audit de sécurité o Recueil des informations – NMAP – Ethercap	Exposés, travaux pratiques et échanges interactifs.	2h	**2h**

	– NetworkMiner – NetScan o Identification des vulnérabilités – Acunetix – Nessus – Vega o Tests de pénétration – Metasploit Evaluation des auditeurs Evaluation du séminaire, remise des attestations et clôture de l'atelier.			
Total			**14h**	**14h**

Critères et indicateurs d'évaluation QCM

NB : *Fiche à établir par l'opérateur de formation*

Case réservée à l'administration :

Avis technique : ……

……

……

Fait à ……. le ……..Signature