

PRINCIPES ET NOTIONS FONDAMENTALES ET DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Durée

3 jours

Référence Formation

4-SE-SSI

Objectifs

Connaître le vocabulaire et les principes théoriques de la sécurité des systèmes d'information, mais de manière très pratique, donc très concrète, pour des praticiens

Connaître toutes les bases de la sécurité opérationnelle, à la fois en sécurité réseau, en sécurité des systèmes Windows et Linux et en sécurité applicative

Participants

Pré-requis

PUBLIC : Administrateurs systèmes et réseaux, responsables informatique et/ou sécurité PRÉ-REQUIS : Une réelle connaissance informatique est nécessaire

PROGRAMME

1. Concepts de base des réseaux

Paquets et adresses

Ports de services IP

Protocoles sur IP

TCP / UDP / ICMP

DHCP / DNS

VoIP (SIP)

Réseaux sans fil

2. Sécurité physique

Services généraux

Contrôles techniques

Menaces sur la sécurité physique

3. Principes de base de la SSI

Modèle de risque

Défense en profondeur

Identification, authentification et autorisation

Classification des données

Vulnérabilités

4. Politiques de sécurité informatique

Principe

Rôles et responsabilités

5. Plan de continuité d'activité

Exigences légales et réglementaires

Stratégie et plan de reprise après sinistre

6. Analyse des conséquences

Évaluation de crise

Facteurs de succès

Fonctions business critiques

7. Gestion des mots de passe

Stockage, transmission et attaque des mots de passe Windows

Authentification forte (Tokens, biométrie)

Single Sign On

RADIUS

8. Sécurité Web

Protocoles de sécurité du Web

Contenus dynamiques

Attaques des applications Web

Durcissement des applications Web

9. Détection d'intrusion en local

Détection d'intrusion

A quoi s'attendre

10. Détection d'intrusion en réseau

Outils

Déni de service

Réaction automatisée

Pots de miel

11. Gestion des incidents de sécurité

Préparation, identification et confinement

Éradication, recouvrement et retour d'expérience

Techniques d'enquête et criminalistique informatique

Guerre de l'information offensive et défensive

12. Méthodes d'attaques

Débordement de tampon

Comptes par défaut

Envoi de messages en masse

Navigaison web

Accès concurrents

13. Pare-feu et zones de périmètres (DMZ)

Types de pare-feu

Architectures possibles : avantages et inconvénients

14. Audit et appréciation des risques

Méthodologies d'appréciation des risques

Approches de la gestion du risque

Calcul du risque / SLE / ALE

15. Cryptographie

Besoin de cryptographie

Types de chiffrement

Symétrique / Asymétrique

Empreinte ou condensat

Chiffrement

Algorithmes

Attaques cryptographiques

Types d'accès à distance (VPN, DirectAccess)

Infrastructures de Gestion de Clés

Certificats numériques

Séquestre de clés

16. PGP

Installation et utilisation de PGP

Signature de données

Gestion des clés

Serveurs de clés

17. Stéganographie

Types

Applications

Détection

18. Sécurité opérationnelle

Exigences légales

Gestion administrative

Responsabilité individuelle

Opérations privilégiées

Types de mesures de sécurité

Reporting

Moyens pédagogiques

Accueil des stagiaires dans une salle dédiée à la formation équipée d'un vidéo projecteur, tableau blanc et paperboard ainsi qu'un ordinateur par participant pour les formations informatiques. Positionnement préalable oral ou écrit sous forme de tests d'évaluation, feuille de présence signée en demi-journée, évaluation des acquis tout au long de la formation. En fin de stage : QCM, exercices pratiques ou mises en situation professionnelle, questionnaire de satisfaction, attestation de stage, support de cours remis à chaque participant. Formateur expert dans son domaine d'intervention Apports théoriques et exercices pratiques du formateur Utilisation de cas concrets issus de l'expérience professionnelle des participants Réflexion de groupe et travail d'échanges avec les participants Pour les formations à distance : Classe virtuelle organisée principalement avec l'outil ZOOM. Assistance technique et pédagogique : envoi des coordonnées du formateur par mail avant le début de la formation pour accompagner le bénéficiaire dans le déroulement de son parcours à distance