PROGRAMME DE FORMATION

Principes et notions fondamentales et de la sécurité des systèmes d'information

Organisation

Mode d'organisation : Présentiel ou distanciel **Durée :** 3 jour(s) · 21 heures

Contenu pédagogique

Type

Action de formation

Prérequis

PUBLIC : Administrateurs systèmes et réseaux, responsables informatique et/ou sécurité

PRÉ-REQUIS : Une réelle connaissance informatique est nécessaire

Objectifs pédagogiques

- 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 base de la sécurité opérationnelle, à la fois en sécurité réseau, en sécurité des systèmes Windows et Linux et en sécurité applicative

Description

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
    - Navigation 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

Modalités pédagogiques

Réflexion de groupe et apports théoriques du formateur - Travail d'échange avec les participants sous forme de discussion - Utilisation de cas concrets issus de l'expérience professionnelle - Exercices pratiques (études de cas, jeux de rôle, questionnaires, quiz, mises en situation, ...) sont proposés pour vérifier le niveau de compréhension et d'intégration du contenu pédagogique - Remise d'un support de cours complet pour référence ultérieure

Moyens et supports pédagogiques

Accueil des apprenants dans une salle dédiée à la formation. Chaque participant disposera d'un ordinateur (si besoin), d'un support de cours, d'un bloc-notes et d'un stylo. La formation se déroulera avec l'appui d'un vidéoprojecteur et d'un tableau blanc.

Modalités d'évaluation

Avant la formation :

Nous mettons en place une évaluation de chaque participant via un questionnaire d'évaluation

des besoins et de niveau.
Un audit complémentaire peut-être proposé pour parfaire cette évaluation

Pendant la formation :
Des exercices pratiques (études de cas, jeux de rôle, questionnaires, quiz, mises en situation, ...) sont proposés pour vérifier le niveau de compréhension et d'intégration du contenu pédagogique.

À la fin de la formation :
Le participant auto-évalue son niveau d'atteinte des objectifs de la formation qu'il vient de suivre.
Le formateur remplit une synthèse dans laquelle il indique le niveau d'acquisition pour chaque apprenant : « connaissances maîtrisées, en cours d'acquisition ou non acquises ». Il évalue ce niveau en se basant sur les exercices et tests réalisés tout au long de la formation.
Le participant remplit également un questionnaire de satisfaction dans lequel il évalue la qualité de la session.

À la demande du stagiaire, le niveau peut aussi être évalué par le passage d'une certification TOSA pour les outils bureautiques, CLOE pour les langues.

Modalités de suivi

Emargement réalisé par 1/2 journée - Certificat de réalisation remis à l'employeur à l'issue de la formation - Assistance par téléphone et messagerie - Support de cours remis à chaque participant à l'issue de sa formation - Suivi de la progression 2 mois après la formation