Centre de Formation Professionnelle

FORMATION

CYBERSECURITE

Type de cours : Stage pratique en présentiel

Référence : CYBER

Durée: 5 jours - 35h de formation

Lieu : Paris ou intra

ATTESTATION DE FORMATION DELIVRÉE EN FIN DE STAGE

Objectifs

Acquérir une vision globale , théorique et pratique , de la sécurité sur le plan des lois mais aussi des outils, concepts et mécanismes permettant de faire face aux attaques visant sécurité des systèmes informatiques.
Sont abordés sous la forme de travaux pratiques, les thématiques suivantes :
Les infiltrations - La manipulation - Les extractions de données - La détection des attaques réseau - Les écoutes de réseaux - La vulnérabilités des réseaux sans fil - Les méthodes utilisées par les pirates informatiques - Le Scan de réseaux - Le Cryptage des données.
Cette formation permettra d'apprendre les mesures de sécurité susceptibles d'être prises pour se défendre contre des attaques d'un système d'information. Sont abordés également les aspects légaux et règlementaires.

Permettre également l' établissement d'un audit et d'u diagnostique destiné à évaluer le niveau de sécurité de l'entreprise, d'avoir conscience des failles sécuritaires et de pouvoir mettre en place une stratégie de défense.
Mieux comprendre les enjeux actuels en matière de sécurité et analyser les risques, la sécurité des systèmes informatiques (postes et serveurs).

FORMATION ANIMEE PAR UN EXPERT EN INFORMATIQUE

Pré-requis :

Notions de réseaux informatiques et d'internet.

Public visé :

Responsables sécurité informatique, Administrateurs sécurité, Gérants d'entreprise, Managers.

Méthodes pédagogiques

- Un poste de travail par stagiaire
- Accès Internet
- Exercices individuels sur PC
- Supports de cours
- Mises en application des logiciels

Centre de Formation Professionnelle CFORPRO - Tour de l 'horloge- 4 Place louis Armand 75603 Paris- Siret 50218786700010 - Déclaration N°11754276775 - Tél: 01.75.50.92.30 - Fax: 01.79.73.89.51 - Mail : contact@cforpro.com

Programme du stage

1. Rappels et généralités
Système informatique et Système d'information
Sensibilisation aux aspects légaux et aux normes applicables
Le contexte international, européen et français
Les risques concernant la sécurité en général, le pays et la société, ceux qui relèvent des organisations, et des personnes

2. Analyse du risque et du coût
Que veut t'on protéger ? Pourquoi ?
Return On security Investment (ROSI)
Définition correct des accès suivant les utilisateurs
Qui accède à quoi ?
Qualification de la typologie des utilisateurs
Gestion de la politique de mot de passe

3. Sécurité des réseaux
Principaux types d'attaques référencés
Firewall
Proxy
IPS
VPN
Wi-Fi

4. Sécurité postes et serveurs
GPO
Antivirus
Chiffrement

5. Sauvegarde et mise à jour
Politique de sauvegarde des équipements
Politique de mise à jour
Redondance des infrastructures

6. Supervision et analyse
Centralisation des logs
Indicateur de suivi
Rapport régulier sur les accès (Type, nombre, évolution)
Réglementation

7. Continuité de service
Définition d'un PRA
Définition d'un PSI
Recensement des métiers et des postes clés

8. Sensibilisation des utilisateurs
Formation
Affichage
Mailling
Anticipation des erreurs courantes

9. Benchmark
Méthodes pour tester la sécurité de son SI

10. Veille technologique
Adaptation et ajustements
Évolution du SI et des infrastructures

11.Techniques et travaux pratiques avancés
Les infiltrations - La manipulation - Les extractions de données
Détection des attaques réseau - Ecoutes de réseaux - Vulnérabilités des réseaux sans fil Méthodes utilisées par les pirates - Scan de réseaux - Cryptage.

TRAVAUX PRATIQUES

- Mise en place d'un environnement de test et d'expérimentation comprenant les postes de travail utilisés pendant le stage, avec des machines virtuelles déployées sur ces postes pour découvrir et aborder un premier niveau maîtrise de la distribution Kali Linux et des outils usuels de tests de pénétration et d'évaluation de la sécurité d'un système informatique sous les environnements d'exploitation Windows Server et Linux.

- Outils et mise en œuvre d'inventaires de parc, matériel, logiciels, réseau

- Attaques Wifi

- Attaques accès exploitation et bases de données

- Analyse et résolution de problèmes liés aux maliciels provenant des usages Internet

- Outils d'analyse et de mesure des trafics réseaux (Wireshark)