Cybersecurity Foundations

Durée: 5 Jours **Réf de cours: 9701**

Résumé:

Cette formation permet aux participants d'avoir une vue globale des défis que présente la conception d'un système sécurisé. Au moyen d'exposés et de labs, les tendances des menaces actuelles sur l'Internet et leur impact sur la sécurité de l'organisation sont exposés. L'exploitation des failles et les remèdes existants y sont traités également.

Public visé:

Cette formation s'adresse aux professionnels de la sécurité informatique, personnels d'exploitation, administrateurs réseau et consultants en sécurité.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Identifier les cyber-menaces actuelles et les sites de référence sur la Cybersécurité
- Expliquer les directives et exigences de conformité
- Décrire les Cyber rôles nécessaires à la conception de systèmes sûrs
- Expliquer le cycle des attaques
- Discuter du processus de gestion des risques
- Définir les stratégies optimales pour sécuriser le réseau d'entreprise
- Mettre en oeuvre les zones de sécurité et les solutions standards de protection

Pré-requis:

Connaissances en réseaux TCP/IP

Contenu:

Le champ de bataille

- La croissance d'Internet dans le monde entier
- Principes et objectifs de sécurité
- Terminologie des menaces et de l'exposition
- Documents et procédures de gestion des risques

Structure de l'Internet et TCP/IP

- Normes de conformité juridique
- Internet Leadership IANA
- Modèle TCP/IP

Évaluation de la vulnérabilité et outils

- Vulnérabilités et exploits
- Outils d'évaluation de la vulnérabilité
- Techniques d'attaques avancées, outils et préventions

Sensibilisation à la cyber sécurité

- Ingénierie sociale : Objectifs de l'ingénierie sociale, cibles, attaque, hameçonnage
- Sensibilisation à la cyber sécurité : Politiques et procédures

Cyber-attaques : Footprinting et scannage

- Footprinting
- Identification du réseau cible et sa portée
- Techniques de scannage de port

Cyberattaques : Effraction

- Attaque des mots de passe, escalade des privilèges
- Authentification et décodage du mot de passe

Cyberattaques : Porte dérobée et cheval de Troie (Backdoor and Trojans)

- Logiciels malveillants, Cheval de Troie, Backdoor et contre-mesures
- Communications secrètes
- Logiciel anti-espion
- Pratiques de lutte contre les logiciels malveillants

Évaluation et gestion des risques cybernétiques

- Actifs protégés : CIA Triad
- Processus de détermination de la menace
- Catégories de vulnérabilités
- Actifs de l'entreprise vs risques

Gestion des politiques de sécurité

- Politique de sécurité
- Références de politiques

Sécurisation des serveurs et des hôtes

- Types d'hôtes
- Directives de configuration générale et correctifs de sécurité
- Renforcement des serveurs et périphériques réseau
- Renforcement de l'accès sans fil et sécurité des VLAN

Sécurisation des communications

- Application de la cryptographie au modèle OSI
- Tunnels et sécurisation des services

Authentification et solutions de chiffrement

- Authentification par mot de passe de systèmes de chiffrage
- Fonctions de hachage
- Avantages cryptographiques de Kerberos
- Composants PKI du chiffrement à clef symétrique, du chiffrement asymétrique, des signatures numériques

Pare-feu et dispositifs de pointe

- Intégration de la sécurité générale
- Prévention et détection d'intrusion et défense en profondeur
- Journalisation

Analyse criminalistique

- Gestion des incidents
- Réaction à l'incident de sécurité

Reprise et continuité d'activité

- Types de catastrophes et Plan de reprise d'activité (PRA)
- Haute disponibilité
- Documentation de collecte de données
- Plan de Reprise d'Activité et Plan de Continuité d'Activité

Cyber-révolution

- Cyberforces, Cyberterrorisme et Cybersécurité : crime, guerre ou campagne de peur ?

LABS

- Lab1: Installation du lab
- Lab 2 : Comprendre TCP/IP
- Lab 3 : Evaluation de la vulnérabilité
- Lab 4 : Sensibilisation à la cybersécurité
- Lab 5 : Scannage
- Lab 6 : Cyber-attaques et mots de passe
- Lab 7 : Cyber-attaques et portes dérobées
- Lab 8 : Évaluation des risques
- Lab 9 : Stratégies de sécurité
- Lab 10 : Sécurité hôte
- Lab 11 : Communications secrètes
- Lab 12 : Authentification et cryptographie
- Lab 13 : Snort IDS
- Lab 14 : Analyse criminalistique
- Lab 15 : Plan de continuité des affaires

Méthodes pédagogiques :

Un support de cours est remis à chaque participant, ainsi que d'autres documents dont les textes de l'ANSSI Agence Nationale de la Sécurité des Systèmes d'Information (législation et avis divers).

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

•Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
•Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
•Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.