SETC Training Corporate Logo

Formation sécurité informatique: Concepts essentiels (SECCOPMFR, 4 jours)

Description

Le cours Formation sécurité informatique : Concepts essentiels présente l'art et la science de la sécurité informatique. La formation commence par un aperçu de la gestion de la sécurité informatique et de ses différentes disciplines. Le cours aborde ensuite les types de menaces et le cycle de vie complet Planifier, Détecter, Répondre et Protéger. La formation comprend l'utilisation de pare-feu, d'anti-virus, de politiques de sécurité de l'information, de gestion des utilisateurs, de gestion du réseau et plus encore. Si vous devez créer, publier, mettre en œuvre et maintenir une politique de sécurité de l'information de l'entreprise, ce cours est fait pour vous.

Tarifs

- Tarification: $3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Concepts de sécurité essentiels

- Comprendre les couches : Gestion des affaires, de l'information et de l'accès
- À propos de la gestion de la sécurité des entreprises
- La discipline de la gestion de la sécurité de l'information
- La discipline de la gestion de l'accès
- À propos de l'ISM et de la gestion du changement
- Le rôle de la politique de sécurité de l'information

Menaces et vulnérabilités

- Comprendre la topologie de l'organisation
- Les actifs informatiques : Topologie et menaces
- L'anatomie d'une attaque
- À propos de l'escalade de privilèges

Stratégies d'attaque courantes

- Comprendre les communications en réseau : Le monde câblé
- Comprendre les communications en réseau : Le monde sans fil
- Protection des communications réseau : Vérification et validation des messages
- Aperçu des stratégies d'attaque courantes
- Attaques par déni de service
- Écoute clandestine, usurpation d'identité et reniflage
- Chevaux de Troie et virus
- Autres stratégies d'attaque

Comprendre la cryptographie

- À propos de la validation et de la vérification des messages
- Les bases de la cryptographie : Clés et algorithmes
- Choix de la longueur des clés et des algorithmes cryptographiques
- Comprendre les digests de messages et les algorithmes associés
- Comprendre le chiffrement à clé publique-privée et RSA
- Travailler avec SSL et les certificats
- À propos de l'autorité de certification : Choix et utilisation
- À propos de l'utilisation d'une signature numérique
- Autres algorithmes d'intérêt : BlowFish, PGP et autres

Création et mise en œuvre d'une bonne politique de sécurité de l'information

- Contenu type d'une politique de sécurité de l'information
- Communication de la politique
- Création et mise en œuvre d'une politique de mot de passe
- À propos de la force et de l'expiration des mots de passe
- Se protéger contre les attaques d'ingénierie sociale
- A propos du cryptage des mots de passe
- Utilisation de mots de passe à usage unique et à jeton
- Comprendre l'authentification multifactorielle : 2, 3, 4 et plus

Réseaux et sécurité IP

- Comprendre les communications réseau IPv4 et IPv6
- À propos de l'IP et de ses vulnérabilités
- Comprendre la topologie logique et physique d'un réseau IP
- Comprendre le réseau global : le LAN et le WAN
- Comprendre et se protéger contre les attaques basées sur le MAC
- Comprendre et se protéger contre les attaques DNS, DHCP, DFS et WINS
- Comprendre et se protéger contre les attaques de IIS

Protection des actifs informatiques

- Les outils du métier : Trouver les vulnérabilités
- Planification de la mise en œuvre de la politique de sécurité
- Identifier les vulnérabilités du réseau et du système d'exploitation
- Restreindre le réseau : Règles et pare-feu
- Restreindre les comptes d'utilisateurs : Verrouillage des comptes d'administrateur et de service
- Restreindre les comptes d'utilisateurs : La politique en matière de mot de passe
- Restreindre les comptes d'utilisateur : Création d'objets de stratégie de groupe
- Verrouillage des applications
- Verrouillage des fichiers locaux et distants

Prévention des attaques courantes contre les systèmes d'exploitation

- Vulnérabilités du système d'exploitation
- Utilisation des pare-feu et des politiques de sécurité
- Utilisation des services de cryptographie et de protection
- Gestion des applications existantes
- Traiter les applications Java et .NET
- Prévention des débordements de mémoire tampon
- Prévention des attaques par déni de service
- Utilisation des journaux d'événements
- Utilisation de renifleurs de réseau

Un laboratoire de sécurité complet