Cybersecurity Foundations

Formation Informatique / Réseaux et Sécurité / Sécurité

Ce cours de cyber sécurité offre 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. Exploitation des failles et remèdes y sont traités également.

OBJECTIFS

- Connaitre les Cyber-menaces actuelles et sites de référence sur la cyber sécurité
- Maitriser les Directives et exigences de conformité
- Connaitre les Cyber rôles nécessaires à la conception de systèmes sûrs
- Se familiariser avec les Cycle des attaques
- Maitriser les Processus de gestion des risques
- Maitriser les Stratégies optimales pour sécuriser le réseau d'entreprise
- Mettre en œuvre des Zones de sécurité et solutions standards de protection

PUBLIC

Professionnels de la sécurité informatique, personnels d'exploitation, administrateurs réseau et consultants en sécurité

PRE-REQUIS

Connaissances en réseaux TCP/IP

PROGRAMME

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

A retenir

Durée : **5 jours** soit 35h.
Réf. **9701**

01 42 93 52 72

Dates des sessions

Paris
04/12/2017
19/02/2018
14/05/2018
27/08/2018
12/11/2018
Lyon
18/06/2018

Cette formation est également proposée en formule INTRA-ENTREPRISE.

Inclus dans cette formation

Coaching Après-COURS

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

100% SATISFACTION GARANTIE

Votre garantie 100% SATISFACTION

- 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

Horaires, Planning et Déroulement de cette formation

Horaires

• Formation de 9h00 (9h30 le premier jour) à 17h30.
• Deux pauses de 15 minutes le matin et l'après-midi.
• 1 heure de pause déjeuner

DEROULEMENT

• Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.
• Une attestation de suivi de formation vous sera remise en fin de formation.

• Cette formation est organisée pour un maximum de 14 participants.

PROCHAINES FORMATIONS

Réussir la Certification Gestion de Projet PMP du PMI
Réussir la Certification PRINCE2 Foundation
Réussir les Certifications PRINCE2 Foundation et PRINCE2 Practitioner
Réussir la Certification ITIL Foundation
Réussir la Certification Agile certifié SCRUM Master
Réussir les Certifications TOGAF Certified et TOGAF Foundation

Retrouvez cette formation sur notre site :
Cybersecurity Foundations