PROGRAMME DE FORMATION

Les essentiels de la cybersécurité

Organisation

Mode d'organisation : Présentiel ou distanciel **Durée :** 5 jour(s) · 35 heures

Contenu pédagogique

Type

Action de formation

Public visé

Professionnels de la sécurité informatique, personnels d'exploitation, administrateurs réseau et consultants en sécurité
Cette formation est accessible aux publics en situation de handicap et aux personnes à mobilité réduite. Des aménagements peuvent être prévus en fonction des profils. Nous contacter pour plus d'information.

Prérequis

Connaissances en réseaux TCP/IP

Objectifs pédagogiques

Présentation des cyber-menaces actuelles et sites de référence sur la cybersécurité

Directives et exigences de conformité

Cyber rôles nécessaires à la conception de systèmes sûrs

Cycle des attaques processus de gestion des risques

Stratégies optimales pour sécuriser le réseau d'entreprise

Zones de sécurité et solutions standards de protection

Description

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

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