

Formation Cybersécurité, Les fondamentaux

Présentation

Cette formation en cybersécurité offre une vue d'ensemble des défis liés à la création de systèmes sécurisés. À travers des présentations et des exercices pratiques, les participants découvriront les tendances actuelles des menaces sur Internet et leur impact sur la sécurité des organisations. L'accent est mis sur l'exploitation des vulnérabilités et les solutions pour y remédier.

Durée : 35,00 heures (5 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

À la fin de cette formation, les participants seront capables de :

- Reconnaître les cybermenaces actuelles et identifier les ressources de référence en cybersécurité.
- Comprendre les directives et exigences de conformité.
- Décrire les rôles essentiels pour la conception de systèmes sécurisés.
- Expliquer les différentes phases des attaques.
- Aborder le processus de gestion des risques.
- Définir des stratégies efficaces pour sécuriser les réseaux d'entreprise.
- Mettre en place des zones de sécurité et des solutions de protection standardisées.

Prérequis

Connaissances de base en réseaux TCP/IP.

Public

- Professionnels de la sécurité informatique
- Administrateurs réseau
- Consultants en sécurité



Programme de la formation

1/ Panorama des Menaces

- Expansion mondiale d'Internet
- Principes et objectifs de la sécurité
- Terminologie des menaces et des expositions
- Documentation et procédures de gestion des risques

2/ Architecture de l'Internet et TCP/IP

- Normes de conformité légale
- Leadership de l'Internet par l'IANA
- Modèle TCP/IP

3/ Analyse des Vulnérabilités et Outils

- Vulnérabilités et exploits
- Outils d'évaluation des vulnérabilités
- Techniques d'attaques avancées, outils et mesures de prévention

4/ Sensibilisation à la Cybersécurité

- Ingénierie sociale : objectifs, cibles, attaques, hameçonnage
- Sensibilisation à la cybersécurité : politiques et procédures

5/ Cyberattaques : Reconnaissance et Scannage

- Reconnaissance (Footprinting)
- Identification et portée du réseau cible
- Techniques de scannage de ports

6/ Cyberattaques : Intrusion

- Attaques par mots de passe, escalade des privilèges
- Authentification et décryptage des mots de passe

7/ Cyberattaques : Logiciels Malveillants et Portes Dérobées

- Logiciels malveillants, chevaux de Troie, portes dérobées et contre-mesures
- Communications secrètes
- Logiciels anti-espions
- Pratiques de lutte contre les logiciels malveillants

8/ Évaluation et Gestion des Risques Cybernétiques

- Actifs protégés : Triade CIA
- Processus de détermination des menaces
- Catégories de vulnérabilités
- Actifs de l'entreprise vs risques

9/ Gestion des Politiques de Sécurité

- Politique de sécurité
- Références de politiques

10/ Sécurisation des Serveurs et des Hôtes

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

11/ Sécurisation des Communications

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

12/ Authentification et Solutions de Chiffrement

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

13/ Pare-feu et Dispositifs de Sécurité Avancés

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

14/ Analyse Forensique

- Gestion des incidents
- Réaction aux incidents de sécurité

15/ 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

16/ Cyber-révolution

- Cyberforces, cyberterrorisme et cybersécurité : crime, guerre ou campagne de peur ?

17/ Ateliers

- Atelier 1 : Installation du lab
- Atelier 2 : Comprendre TCP/IP
- Atelier 3 : Évaluation des vulnérabilités
- Atelier 4 : Sensibilisation à la cybersécurité
- Atelier 5 : Scannage
- Atelier 6 : Cyberattaques et mots de passe
- Atelier 7 : Cyberattaques et portes dérobées
- Atelier 8 : Évaluation des risques
- Atelier 9 : Stratégies de sécurité
- Atelier 10 : Sécurité des hôtes
- Atelier 11 : Communications secrètes

- Atelier 12 : Authentification et cryptographie
- Atelier 13 : Snort IDS
- Atelier 14 : Analyse forensique
- Atelier 15 : Plan de continuité des affaires

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation (*évaluations en ligne dans l'extranet apprenant*)

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.