Développez vos talents
Certifiez vos compétences

Sécurité défensive

PKI - Mise en oeuvre

2 jours (14h00) | ★★★★½ 4,6/5 | SEC-PKI | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cybersécurité › Sécurité défensive

À l'issue de ce stage vous serez capable de :

- Reconnaître les éléments structurant une PKI
- Identifier les étapes nécessaires à son implémentation.

Niveau requis

Avoir des connaissances générales sur TCP/IP, le chiffrement et la mise en oeuvre de services réseaux et systèmes.

Public concerné

Administrateurs système et réseau, consultants en sécurité.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Programme

Jour 1

Introduction aux chiffrements

- La sécurité par le chiffrement
- Un peu d'histoire
- Principes généraux
- Les systèmes cryptographiques
- Définitions et concepts
- Systèmes de chiffrement symétrique et asymétrique
- La cryptanalyse
- Principaux algorithmes et techniques
- Les services offerts

Introduction aux systèmes d'infrastructure à clés publiques

- Infrastructure de gestion des clés
- Objectifs d'une infrastructure
- La gestion des clés cryptographiques
- Typologie des architectures de gestion des clés
- Règles et recommandations générales des clés
- Demande, génération, affectation, renouvellement, recouvrement
- Certificate types X.509
- Certificats d'autorité
- Liste de révocation
- Les bonnes pratiques et les bonnes topologies

Exemple de travaux pratiques (à titre indicatif)

- *Mise en place d'une PKI avec Windows Server autonome*

Jour 2

PKI dans un environnement d'entreprise

- Gérer une PKI dans une infrastructure complexe
- Configurer un template de certificat
- Configurer "Certificate Enrollment"
- Archiver et récupérer un certificat
- Configuration entre deux organisations
- Deploying Smart Cards
- Intégrer la PKI
  - Services SSL
  - Scripts Powershell de l'entreprise
  - Technologies VPN de l'entreprise
  - Technologies IPsec de l'entreprise

Exemples de travaux pratiques (à titre indicatif)

- *Ajouter une PKI d'entreprise à la PKI autonome et à l'annuaire de l'entreprise*
- *Faire signer les scripts de l'organisation par la PKI*

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques

– Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)