

Mise en œuvre de PCI

Comprendre les normes PCI, dont PCI DSS,
et leurs rôles sur la protection des données sensibles

Présentation

Cette formation permet de bien comprendre les différents standards PCI : PCI DSS, PCI P2PE, PA-DSS, PCI PTS-POI et PCI PTS-HSM ainsi que les relations entre ces standards de sécurité des données cartes et du PIN. Cette compréhension a pour objectif d'aider à assurer la conformité des systèmes concernés aux exigences PCI que ce soit lors de la mise en place de nouveaux systèmes ou pour des systèmes existants

Points forts

- Perspectives historiques et géographiques sur les démarches de protection des données cartes et analyse de cas tirés de l'actualité
- Dernier état de l'art sur les standards PCI ainsi que sur leur implémentation
- Nombreuses définitions et sources documentaires

Public

Cette formation est destinée à toute personne ayant des connaissances générales en monétique, confrontée aux problématiques de sécurité des données cartes : RSSI, Responsable monétique, Chef de projet, «Compliance officer»...

Durée

- 1 journée
- Accueil à partir de 9h
- Formation de 9h30 à 17h30

Prochaines sessions

- 14 novembre 2017
- 13 mars 2018

Formation Intra-entreprise

Nous consulter pour connaître les disponibilités. Le contenu de cette formation, organisée au sein de votre entreprise, peut être adapté à vos objectifs particuliers, après analyse de vos besoins et réalisation d'une proposition détaillée

Animateurs

Experts en systèmes de paiement et sécurité

Langue

Français

Tarif

Nous consulter

Documentation

Support de cours
Liste des sigles monétiques

Lieu

Région parisienne

Programme

Matin

1. Présentation générale

- **Contexte**
Besoins résultant de nouveaux modes de paiement
- **Historique**
Fraudes de très grande ampleur
- **Concepts de PCI**
 - Standard PCI DSS
 - Standard PA-DSS
 - Standards PCI PTS
 - Standard P2PE
 - Standard PCI Card Production
- **Rôles et responsabilités des acteurs**
 - PCI Council
 - Réseaux internationaux
 - Banques acquéreurs
 - Commerçants
- **Articulation entre les standards de PCI**
 - Relations entre PCI DSS et PA-DSS
 - Relations entre PCI DSS et PCI PTS
 - Relations entre PCI DSS et PCI P2PE

2. Standard PCI DSS

- **Champ d'application**
Intervenants impactés et non impactés
- **Obligation en fonction des catégories et des seuils**
4 niveaux
- **Exigences PCI DSS**
 - 12 groupes d'exigences couvrant 6 grands thèmes
 - Exemples
- **Le cycle de vie de la norme PCI DSS**
- **Démarche type de mise en conformité et bonnes pratiques**
 - E-commerce / M-commerce
 - Canal de proximité
- **Opportunités de réduction du périmètre**
- **Mesures compensatoires**
- **Approche par priorisation**

Après-midi

3. Standard PA-DSS

- **Champ d'application**
- **Critères d'éligibilité à la certification PA-DSS**
- **Exigences PA-DSS**

4. Standard PCI PTS-POI

- **Champ d'application**
- **Standard PCI PTS-POI**
Approche modulaire selon les fonctionnalités du terminal
- **Exigences du standard PCI PTS-POI**
5 modules décomposés en 13 groupes d'exigences
- **Exigences du standard PCI PTS-HSM**
4 groupes d'exigences

5. Standard PCI P2PE

- **Champ d'application**
- **Exigences P2PE**

6. Standard PCI CP

- **Champ d'application**
- **Exigences PCI CP**

7. Tokenisation PCI

- **Concept de « non-payment tokenization »**
Intérêts pour les systèmes monétiques
- **Comparaison entre « non-payment tokenization » et « payment tokenization »**
Principales différences entre la tokenisation de PCI et la tokenisation de EMVCo
- **Principales fonctionnalités de la tokenisation**
Formatage, multi-usages, multi-sites...
- **Exigences sécurités des solutions de tokenisation**
Selon la classification « Reversible Cryptographic », « Irreversible - Authenticatable »...
- **Grandes catégories de solutions**
Vault ou Vaultless...

Contenu susceptible d'évoluer