

Formations PCI (Payment Card Industry)

La sécurisation des transactions électroniques a toujours été au cœur des préoccupations des acteurs du paiement, qu'ils soient commerçants, institutions financières ou fournisseurs de services.

L'industrie s'est dotée depuis quelques temps déjà, de normes et standards de sécurisation des données sensibles, connues sous le sigle PCI (Payment Card Industry).

Comprendre la sécurisation des données sensibles, percevoir les attentes des institutions internationales membres de PCI-SSC (telles que VISA, MasterCard, AMEX, ...), appréhender les efforts pour être et rester en conformité, c'est l'objet de nos formations concrètes et pragmatiques.

EESTEL propose en 2012, un cycle nouveau de formations adaptées aux bonnes pratiques d'applications des normes et règles PCI grandissant la sécurisation de vos transactions. Ce cycle s'appuie sur les dernières normes en vigueur.

Ce cycle se compose de 2 modules :

Réf.	Module	Public ciblé	Durée	Contenu
P12	PCI : Concepts et Stratégies	Décideurs du secteur Commerce ou des Institutions financières concernées par le paiement Responsables monétiques Responsables e-Commerce Responsables sécurité Responsables informatiques et DSI Directeur Administratif et Financier Responsable juridique Direction générale	0,5 jour	Introduction sur le contexte PCI Concepts PCI Stratégie de mise en place Les facteurs clés de succès Prospectives Conclusions
Q12	PCI : Mise en œuvre opérationnelle	Toute personne impliquée en terme de management ou de mise en place opérationnelle dans PCI. Chefs de projets monétiques Responsables et ingénieurs sécurité Responsable et ingénieurs systèmes Responsable et ingénieurs réseaux Responsable et ingénieurs base de données Exploitant de centres de traitement financiers Pour le 1^{er} jour seulement : Directeur Administratif et Financier Directeur des systèmes d'informations	2 jours	Rappel du contexte PCI-DSS Le standard PCI-DSS Les clefs du succès d'un projet PCI DSS PCI DSS - Impact sur les équipes Sécurité SI PCI DSS - Sujets techniques transverses PCI DSS - Impact sur les équipes Socle technique PCI DSS - Impact sur les équipes Applicatives Guidelines spécifiques PCI Council Conclusions - Questions/Réponses

Le contenu de ces programmes est conçu et dispensé par les experts d'EESTEL.

Module PCI (Payment Card Industry) : Concepts et stratégies

Durée : 0,5 jour

Réf. : P12

Audience

Décideurs du secteur Commerce ou des Institutions financières concernés par le paiement.

- Direction générale
- Responsables monétiques
- Responsables e-Commerce
- Responsables sécurité
- Responsables informatiques et DSI
- Directeur Administratif et Financier
- Responsable juridique

Prérequis

- Connaissances générales sur le paiement et les systèmes d'informations
- Connaissance des contraintes du Commerce

Intervenants

- Consultants seniors en sécurité, membres d'EESTEL
- Expériences d'accompagnement concrètes (Grand Commerçant, Institution, Centre de traitement)



Documentation

- Support de cours
- Glossaire sécurité

Dates et Lieu de la formation

- 25/04/2012 matin
- 24/10/2012 matin

Lieu : Issy-les-Moulineaux (215, rue Jean-Jacques Rousseau)

Tarif

500 € HT par personne.

Formation intra-entreprise

Nous consulter : formation@eestel.com

Contenu de la session

Introduction

- Historique - Sécurisation des systèmes d'informations
- Pourquoi PCI-DSS ?
 - Les données qui ne nous appartiennent pas...
- Les différents standards PCI selon le domaine couvert
 - PCI-PTS, PCI-PA-DSS et PCI-DSS
- Périmètre d'action dans le système d'informations commerçant
- Risques couverts par PCI

Concepts PCI

- Rappels de fondamentaux sur la Monétique
- Chaîne de valeur des acteurs :
 - Commerce, fournisseur, établissement bancaire, institution
- Les acteurs du PCI : PCI Council, Réseaux internationaux
- Qui est concerné ?
 - Chaînes de responsabilité, pénalités, dates limites
- Les données sensibles à protéger (PAN, PIN, etc.)
- Les 4 niveaux de conformité pour les commerçants
- Synthèse des 12 exigences de PCI-DSS
- Conséquences d'un problème en production

Stratégie de mise en place

- La théorie... et la pratique !
- Stratégie PCI à moindre coût
 - Réduire le périmètre
 - Business domestique ou International ?
- Conformité dans la durée
- Sélection des systèmes à sécuriser
- Mesure du risque - Mesures préventives/curatives
- Approche budgétaire

Les facteurs clés de succès

- Exigences des institutions : TIP, autoévaluation, certifications
- Démarche de progrès en 6 étapes
- Préparation des travaux et Plan d'actions : Adapter le périmètre
- Comment transformer PCI en avantage concurrentiel ?
- PCI dans la stratégie de l'entreprise

Prospectives

- Peut-on se passer de PCI et comment ?
- Wallet, e2e encryption, sous-traitance PSP, ...

Conclusions - Questions/Réponses

Module PCI : Mise en œuvre opérationnelle

Durée : 2 jours

Réf. : Q12

Audience

Toute personne impliquée en terme de management ou de mise en place opérationnelle dans PCI.

- Chefs de projets monétiques
- Responsables et ingénieurs sécurité
- Responsable et ingénieurs systèmes
- Responsable et ingénieurs réseaux
- Responsable et ingénieurs base de données
- Exploitant de centres de traitement financiers

Pour le premier jour seulement :

- Directeur Administratif et Financier
- Directeur des systèmes d'informations

Prérequis

- Connaissances générales sur le paiement et les systèmes d'informations
- Connaissance des contraintes du Commerce

Intervenants

- Consultants seniors en sécurité
- Expériences concrètes de mise en place de PCI chez un hébergeur reconnu de services financiers

Documentation

- Support de cours
- Glossaire sécurité

Dates et lieu de la formation

- 11 et 12/06/2012
- 19 et 20/11/2012

Lieu : Issy-les-Moulineaux (215, rue Jean-Jacques Rousseau)

Tarif

1 000 € HT par personne.

Formation intra-entreprise

Nous consulter : formation@eestel.com

Contenu de la session

Rappel du contexte PCI-DSS

- Historique
- Rappels sur la sécurisation des systèmes d'informations
 - Topologie des risques, approche globale
- Pourquoi PCI-DSS ?
- Risques couverts par PCI-DSS
- Qui est concerné ?
- Chaînes de responsabilité, pénalités, deadline
- Les différents standards PCI selon le domaine couvert
 - PCI-PTS, PCI-PA-DSS et PCI-DSS : besoins, périmètres
- Les acteurs du PCI DSS : PCI Council, Réseaux internationaux...

Le standard PCI-DSS

- Données sensibles à protéger
- Cycle de vie du standard PCI
- Vocabulaire et acteurs selon le PCI Council [QSA, ASV, ISA, PFI]
- Synthèse des 12 exigences du PCI-DSS
- Contrôles de la conformité
 - Audit sur site QSA, ASV, tests d'intrusion, auto-évaluation etc.

Les clefs du succès d'un projet PCI DSS

- Projet d'entreprise
- Approche préconisée
- Définition du périmètre
- Analyse d'écarts
- Mise en conformité
 - Choix de mesures de contournement
 - Auto-évaluation
 - Certification avec QSA
- Evaluation des ressources et des budgets

PCI DSS - Impact sur les équipes Sécurité SI

- Gouvernance
 - Politique de sécurité, Gestion des incidents de sécurité, Analyse de risque, etc.
- Surveillance (IDS, contrôle d'intégrité, supervision des logs etc.)
- Contrôle interne (ASV, Scan applicatifs, tests d'intrusion etc.)
- Veille sécurité / CERT / Patch management
- Guidelines sécurité
- Sensibilisation du personnel
- Départ des collaborateurs
- Contrôle des accès

PCI DSS - Sujets techniques transverses

- Accès logique aux équipements de production
- Patch management
- Guidelines sécurité
- Gestion du changement
- Cryptage des échanges sur les réseaux publics
- ID unique
- Politique de mot de passe

Règle du « Business need to know »
Traçabilité

PCI DSS - Impact sur les équipes Socle technique

Exploitation physique du centre de données

- Vidéosurveillance
- Contrôle d'accès
- Gestion des sauvegardes
- Exploitation informatique
- Guidelines sécurité
- Patch management
- Centralisation des logs

Réseau

- Architecture (segmentation réseau, DMZ, etc.)
- Gestion des pare-feu
- Revue des règles FW
- Détection d'intrusion
- Accès distant
- Documentation

Système et bureautique

- Anti-malware
- Guidelines sécurité
- Patch management
- Contrôle d'intégrité
- Centralisation des logs

BDD

- Directives de sécurité (Guidelines)
- « Patch management »
- Centralisation des logs

PCI DSS - Impact sur les équipes Applicatives

Cartographie des données sensibles
Politique de rétention des données sensibles
Cryptage/hachage/troncage
Gestion des clefs (Key Management)
Développement sécurisé
Sécurité des applications web / OWASP
Gestion des habilitations
Guide de développement
Audit de code
« Tokenisation »
Chiffrement P2P
Approche par priorité

Guidelines spécifiques PCI Council

Sans contact (Wireless)
Centre d'appels (Call Centre)
Virtualisation des systèmes
Prévention des fraudes de Skimming

Conclusions - Questions/Réponses