PCI-DSS : protection des données des cartes bancaires, synthèse les points de contrôle et la mise en conformité

★★★★★

SII-361 **2 Jours (14 Heures)**

Description

Cette formation vous permettra de comprendre la nouvelle version du standard PCI-DSS relatif à la protection des données de comptes bancaires, dont le paiement par carte et les éléments de sécurité clés nécessaires pour mettre en conformité son entreprise, tout en tenant compte des spécificités de son contexte.

À qui s'adresse cette formation ?

Pour qui

RSSI ou correspondants sécurité, architectes de sécurité, ingénieurs sécurité, chefs de projets (MOE, MOA) devant intégrer des exigences de sécurité réglementaires.

Prérequis

Bonnes connaissances dans la gestion de la sécurité des SI.

Les objectifs de la formation

- Appréhender la protection des données bancaires
- Comprendre le standard actuel PCI-DSS 3.x et se préparer à la version 4.0
- Mettre en œuvre les solutions de sécurité PCI compliant
- Définir le projet de mise en conformité de son entreprise

Programme de la formation

Introduction

- La participation des marques VISA, MASTERCARD, AMEX, etc.
- La relation entre PADSS et PCI DSS.
- Appréhender l'écosystème des acteurs (QSA, ASV, éditeurs certifiés).
- Le standard DSS et les autres standards PCI (PA DSS, PTS, CP, etc).

La préparation de son projet

- Être ou ne pas être PCI DSS ? marchand, PSP, banque émetteur et/ou acquéreur, fournisseur tiers.
- Les différents contextes d'applicabilité de la réglementation, le rôle des marques.
- Le « bon » choix du scope : du « flat network » au « controlled network ».
- L'impact de PCI DSS sur les choix de virtualisation.
- Le partage de la sécurité PCI dans le cloud : quel service cloud choisir ?
- La base documentaire disponible.
- Savoir utiliser les FAQ et les « guidances » officiels.
- A quel moment du projet recourir aux conseils éclairés des auditeurs QSA.

Les douze exigences « historiques » du standard PCI DSS

- Condition 1 : installer et gérer une configuration de pare-feu pour protéger les données CB.
- Condition 2 : ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut.
- Condition 3 : protéger les données de titulaires de cartes stockées.
- Condition 4, 5, 6, 7, 8, 9, 10, 11 et 12.

Les objectifs de conformité et la certification

- Le champ d'application de l'évaluation de la conformité aux conditions de la norme PCI DSS.
- Le choix non contestable des devices en zone contaminante et contaminée.
- La préparation des SAQ : effectuer une auto-évaluation et un audit à blanc.
- Bien réaliser ses pentests et scan de vulnérabilité officiels.
- Se préparer aux audits de conformité et anticiper les écarts.
- La présentation obligatoire de son AOC aux parties prenantes.

La gestion de votre projet PCI-DSS

- Adopter l'approche par priorité proposée par PCI.
- Eviter un effet tunnel à son projet : les étapes vers l' AOC.
- Définir une road map vers la certification PCI DSS.
- La norme PCI-DSS en lien avec la conformité SSI globale.
- Auditeurs QSA et préparation de la méthodologie de tests.
- Le maintien de sa conformité dans le temps : évaluer les couts récurrents.
- Anticiper les nouveautés de la version 4.0 afin de maintenir sa conformité en 202x.
- Les liens nécessaires entre projets sous conformité PCI.