PCI-DSS

Durée : 2 jours Référence : PCI-DSS

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

Contenu

- Introduction
- Les six thèmes et les douze exigences du standard PCI DSS
- Les objectifs de conformité et la certification
- La gestion de votre projet PCI-DSS
- Conclusion

Participants

RSSI , Chef de projet en sécurité.

Pré-requis

Connaissances dans la gestion de la sécurité des SI.

Programme

Introduction

- L'historique et les objectifs du comité PCI (PCI Council).
- Menaces spécifiques sur le e-commerce.
- Les obligations de PCI DSS 1.2 et 2.0.
- Les domaines d'application du PCI DSS.
- La relation entre PADSS et PCI DSS.

Les six thèmes et les douze exigences du standard PCI DSS

- Création et gestion d'un réseau sécurisé. Condition 1 : Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes. Condition 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut.
- Protection des données des titulaires de cartes de crédit. Condition 3 : Protéger les données de titulaires de cartes stockées. Condition 4 : Crypter la transmission des données des titulaires de cartes sur les réseaux publics.
- Gestion d'un programme de gestion des vulnérabilités. Condition 5 : Utiliser des logiciels ou des programmes antivirus et les mettre à jour régulièrement. Condition 6 : Développer et gérer des systèmes et des applications sécurisés.
- Application de mesures de contrôle d'accès rigoureuses. Condition 7 : Limiter l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître. Condition 8 : Affecter un ID unique à chaque utilisateur d'ordinateur. Condition 9 : Limiter l'accès physique aux données des titulaires de cartes.
- Surveillance et test réguliers des réseaux. Condition 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes. Condition 11 : Tester régulièrement les processus et les systèmes de sécurité.
- Gestion d'une politique de sécurité des informations. Condition 12 : Gérer une politique de sécurité des informations pour l'ensemble du personnel.

Les objectifs de conformité et la certification

- Définition des objectifs de conformité.
- Champ d'application de l'évaluation de la conformité aux conditions de la norme PCI DSS. Segmentation réseau. Technologie sans fil. Prestataires tiers/Sous-traitance. Echantillonnage des installations de l'entreprise et des composants du système.
- Positionnement dans le système de classement.
- Effectuer une auto-évaluation et un audit à blanc.
- Cadrage du périmètre soumis à la certification.
- Conformité et vérification.
- Préparation et anticipation des écarts.

La gestion de votre projet PCI-DSS

- La norme PCI-DSS en lien avec la conformité globale.
- Choix des auditeurs et préparation de la méthodologie de tests.

- Définition d'une road map vers la certification PCI DSS.

Conclusion

- Les particularités du marché français.
- Le déploiement généralisé du paiement EMV.
- L'émergence de nouveaux standards.
- Panorama des nouvelles méthodes de paiement.