DAWAN

Plan de la formation

www.dawan.fr

Formation Sécurité des paiements et conformité PCI-DSS

Durée :	2 jours (14 heures)
Tarifs inter-entreprise :	1 775,00 € HT (standard) 1 420,00 € HT (remisé)
Public :	Responsables sécurité / RSSI d'e-commerçants, PSP, fintech, ESN, acteurs manipulant des données de paiement - Responsables IT, architectes techniques, responsables projets paiement - Responsables conformité / risk managers impliqués dans la sécurité des données de cartes
Pré-requis :	Connaissances générales en sécurité des SI et compréhension globale des architectures de paiement (e-commerce, terminaux, PSP, etc.)
Objectifs :	Comprendre le cadre et les exigences de la norme PCI-DSS v4.0 - Identifier les systèmes, flux et acteurs impliqués dans le traitement des données de carte bancaire - Définir le périmètre PCI-DSS de son organisation (CDE, segmentation, prestataires) - Appréhender les principales exigences techniques et organisationnelles de PCI-DSS - Élaborer un premier plan de mise en conformité ou de maintien de conformité
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.

Modalités d’évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102758-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d’accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Comprendre le rôle de PCI-DSS dans la sécurité des paiements

Présenter le Payment Card Industry Data Security Standard (PCI-DSS) et le rôle du PCI Security Standards Council
Comprendre les objectifs de PCI-DSS : protéger les données de carte et réduire la fraude
Situer PCI-DSS par rapport aux autres cadres (RGPD, DSP2, NIS2, exigences des banques et acquéreurs)
Identifier les acteurs concernés : commerçants, prestataires de services, hébergeurs, PSP, fournisseurs de solutions de paiement
Atelier fil rouge : cartographier les flux de paiement d’une boutique en ligne ou d’un cas d’école et identifier les acteurs impliqués

Délimiter le périmètre PCI-DSS et identifier les données de carte

Clarifier les notions de Cardholder Data Environment (CDE) et de données de carte (PAN, CVV, pistes, tokens)
Identifier les systèmes et composants en périmètre : serveurs, postes, réseaux,

terminaux, applications, solutions SaaS
Comprendre les techniques de réduction de périmètre : tokenisation, chiffrement, externalisation, segmentation réseau
Analyser les différents modèles de paiement en ligne (redirection, iFrame, API, paiement sur site) et leurs impacts sur le périmètre
Atelier fil rouge : délimiter un périmètre PCI-DSS pour un scénario concret (e-commerce ou point de vente) et proposer des options de réduction

Approfondir les exigences clés de PCI-DSS v4.0

Passer en revue les grandes familles d'exigences : réseau sécurisé, protection des données de carte, gestion des vulnérabilités, contrôles d'accès, monitoring, politique de sécurité
Identifier les évolutions majeures introduites par PCI-DSS v4.0 (approche continue, flexibilité, MFA, mots de passe, tests, etc.)
Comprendre les impacts sur l'architecture, l'administration, les développements applicatifs et l'exploitation
Relier quelques exigences emblématiques à des mesures concrètes (pare-feu, chiffrement, journalisation, tests de sécurité)
Atelier fil rouge : associer les principales exigences PCI-DSS à des mesures techniques ou organisationnelles déjà en place ou à mettre en œuvre

Organiser la démarche de conformité PCI-DSS

Distinguer les types de validation : SAQ (Self-Assessment Questionnaire), ROC (Report on Compliance), scans ASV, etc.
Comprendre le rôle des acquéreurs, des banques et des prestataires dans la chaîne de conformité
Structurer un projet PCI-DSS : diagnostic initial, analyse de risques, plan de remédiation, validation, maintien en condition
Intégrer PCI-DSS dans la gouvernance sécurité : politiques, procédures, gestion des changements et des incidents
Atelier fil rouge : élaborer une trame de plan de projet PCI-DSS pour une organisation type (PME e-commerce ou fintech)

Travailler avec les prestataires et sécuriser la chaîne de valeur

Identifier les prestataires critiques dans la chaîne de paiement (PSP, hébergeurs, intégrateurs, éditeurs)
Analyser les responsabilités partagées en matière de PCI-DSS (modèles de responsabilité, attestations de conformité, AOC)

Intégrer PCI-DSS dans les contrats : clauses, preuves, audits, exigences de sécurité et de continuité
Prévoir le suivi régulier des prestataires : indicateurs, revues, mises à jour de conformité et de versions PCI-DSS
Atelier fil rouge : construire une fiche de suivi PCI-DSS pour un prestataire de paiement ou d'hébergement

Construire un plan d'actions et maintenir la conformité dans le temps

Prioriser les actions à partir du diagnostic initial et des écarts identifiés
Définir des indicateurs de suivi et un tableau de bord PCI-DSS pour la direction et les équipes opérationnelles
Anticiper les audits, les renouvellements et les évolutions du standard (cycle de vie de PCI-DSS v4.0)
Sensibiliser les équipes (IT, métier, front-office, support) aux bonnes pratiques de sécurité des paiements
Atelier fil rouge final : formaliser une feuille de route PCI-DSS sur 12 à 24 mois, incluant les priorités techniques et organisationnelles