Tableau de conformité PCI DSS v4.0

Découvrez les modifications apportées à la nouvelle version de PCI et comment Reflectiz peut aider votre organisation à répondre aux exigences de chaque section :

Item	Exigence	Réponse de Reflectiz
PCI 6.3.1	Les vulnérabilités de sécurité sont identifiées et gérées comme suit : • Les nouvelles failles de sécurité sont identifiés à l'aide de sources reconnues par l'industrie pour les informations sur les vulnérabilités de sécurité, y compris les alertes des équipes internationales et nationales d'intervention d'urgence informatique (CERT). • Les vulnérabilités se voient attribuer un classement des risques basé sur les meilleures pratiques de l'industrie et la prise en compte de l'impact potentiel. • Les classements des risques identifient, au minimum, toutes les vulnérabilités considérées comme à haut risque ou critiques pour l'environnement. • Les vulnérabilités des logiciels sur mesure, personnalisés et tiers (par exemple, les systèmes d'exploitation et les bases de données) sont couvertes	Reflectiz analyse en permanence le site Web à la recherche de scripts malveillants, de domaines, de vulnérabilités et de CVE connus. Nous utilisons le service VirusTotal, la base de données CVE, le service Whois et la base de données interne Reflectiz des vulnérabilités, des scripts malveillants et des domaines. Et puisque la méthodologie NIST ne couvre pas tous les aspects pertinents de l'évaluation des risques, Reflectiz utilise également son propre mécanisme d'évaluation des risques.
PCI 6.3.2	Un inventaire de logiciels sur mesure et personnalisés et de composants logiciels tiers intégrés dans des logiciels sur mesure et personnalisés est maintenu pour faciliter la gestion des vulnérabilités et des correctifs.	Un inventaire de tous les scripts (sur mesure et tiers) est disponible via le rapport d'inventaire. De plus, Reflectiz fournit un sous-ensemble important de cet inventaire : un journal de tous les scripts qui touchent aux données sensibles, une explication de la raison pour laquelle chacun d'eux est nécessaire pour l'entreprise, un avis de tout changement, l'identification du code malveillant et les mesures prises pour l'empêcher ou le supprimer.
PCI 6.4.1	Des outils ou des méthodes d'évaluation de la sécurité des vulnérabilités manuelles ou automatisées examinent et/ou testent l'application pour les vulnérabilités. Les outils d'évaluation courants incluent des analyseurs Web spécialisés qui effectuent une analyse automatique de la protection des applications Web.	Reflectiz analyse en permanence le site Web à la recherche de scripts et de domaines malveillants, de vulnérabilités et de CVE connus. S'il en est trouvé, le système déclenche une alerte, attribuant à chacun une gravité appropriée selon un mécanisme d'évaluation des risques.

Item	Exigence	Réponse de Reflectiz
PCI 6.4.2	Pour les applications Web destinées au public, une solution technique automatisée est déployée qui détecte et empêche en permanence les attaques Web, avec au moins les éléments suivants : • Est installée devant les applications Web publiques et est configurée pour détecter et prévenir les attaques Web. • Est en cours d'exécution active et à jour, le cas échéant. • Génère des journaux d'audit • Est configurée soit pour bloquer les attaques Web, soit pour générer une alerte qui fait immédiatement l'objet d'une enquête.	Reflectiz déclenche une alerte de haute gravité lorsqu'il détecte chacun de ces éléments : • Modification de script qui semble malveillante • Changement de comportement de l'application, par exemple, une application commence à collecter des données sensibles • Une application commence à envoyer des données à un domaine malveillant • Une nouvelle application (script) est ajoutée et semble malveillante • Une nouvelle version de l'application est ajoutée à la base de données des vulnérabilités connues et fait partie de l'application Web
PCI 6.4.3	Tous les scripts de page de paiement chargés et exécutés dans le navigateur du consommateur sont gérés.	Cette section étend l'exigence ci-dessus à tous les scripts chargés sur des pages sensibles, qu'ils accèdent ou non à des données sensibles.
PCI 11.6.1	Les modifications non autorisées sur les pages de paiement sont détectées et traitées.	Identifie les modifications apportées aux en-têtes de page sensibles et empêche ou supprime tout ajout malveillant.