

CASE STUDY: Reflectiz valide les capacités de sa plateforme PCI DSS avec Integrity360

Le client

Reflectiz propose une plateforme de gestion de l'exposition web sans agent qui aide les organisations à identifier et gérer les scripts, composants tiers et chaînes d'approvisionnement numériques présents sur leurs sites web.

Sa plateforme dédiée PCI DSS accompagne les organisations de commerce électronique dans les exigences de surveillance, d'autorisation et de collecte de preuves associées aux exigences 6.4.3 et 11.6.1 de PCI DSS v4.0.1.

La plateforme surveille à distance les pages de paiement sans nécessiter de modification du code, d'installation logicielle ou de balise de surveillance intégrée.

Critères de sélection

Reflectiz recherchait un évaluateur capable de:

- Fournir une expertise spécialisée PCI DSS
- Évaluer les capacités techniques et procédurales de la plateforme
- Vérifier l'alignement avec les exigences 6.4.3 et 11.6.1
- Examiner les processus de surveillance, d'approbation et de reporting
- Fournir une évaluation indépendante et crédible
- Comprendre les attentes en matière de preuves dans le cadre d'une évaluation QSA

Integrity360 Europe est PCI Qualified Security Assessor Company et membre du Global Executive Assessor Roundtable du PCI Security Standards Council.

reflectiz



Secteur

Conformité des paiements



Défi

Reflectiz souhaitait obtenir une évaluation indépendante de l'alignement de sa plateforme PCI DSS avec les exigences 6.4.3 et 11.6.1 de PCI DSS v4.0.1.

L'évaluation devait déterminer si la plateforme pouvait efficacement prendre en charge:

- L'inventaire et l'autorisation des scripts des pages de paiement
- La vérification de l'intégrité des scripts
- Les justifications métier et techniques documentées
- La détection des altérations des pages de paiement et des en-têtes HTTP
- La surveillance continue et les alertes
- La collecte des preuves pour les évaluations PCI DSS

Cette mission constituait un examen des capacités de la plateforme et non une certification ou une évaluation de conformité d'un environnement client spécifique.

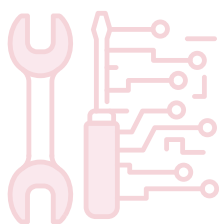
Solution

Integrity360 a examiné l'architecture, les capacités de surveillance et les processus de conformité de la plateforme PCI DSS de Reflectiz.

L'évaluation a analysé la manière dont Reflectiz:

- Découvre les scripts de première, troisième et quatrième parties
- Surveille le comportement des scripts dans le navigateur
- Détecte les modifications des pages de paiement et des en-têtes HTTP
- Maintient des inventaires de scripts et des justifications documentées
- Enregistre les approbations grâce à des pistes d'audit horodatées
- Génère des alertes et des preuves prêtes pour les évaluations

Integrity360 a également examiné le modèle de déploiement sans agent, la fréquence de surveillance configurable, les fonctionnalités Smart Approval ainsi que les intégrations avec les plateformes de sécurité et de gestion de workflows.



Évaluation d'Integrity360

Integrity360 a conclu que la plateforme PCI DSS de Reflectiz est particulièrement bien positionnée pour aider les organisations à répondre aux exigences 6.4.3 et 11.6.1 de PCI DSS v4.0.1.

L'inventaire automatisé des scripts, l'analyse comportementale de l'intégrité, le workflow structuré d'approbation, la surveillance continue des en-têtes HTTP ainsi que les fonctions d'audit et de reporting soutiennent directement les objectifs de contrôle concernés. Son architecture sans agent



Les équipes en charge de la conformité ont raison d'être sceptiques face aux affirmations des fournisseurs. Le fait qu'Integrity360 Europe, une Qualified Security Assessor Company indépendante, ait examiné la manière dont notre plateforme s'aligne sur les exigences PCI DSS 6.4.3 et 11.6.1 transforme nos déclarations en éléments qu'un commerçant peut évaluer objectivement. C'est précisément cette indépendance qui donne toute sa valeur à cette évaluation."

Idan Cohen

Cofondateur et PDG de Reflectiz



Les bénéfices

- Validation indépendante par une PCI Qualified Security Assessor Company
- Alignement clair avec les principaux objectifs de contrôle PCI DSS
- Confiance renforcée pour les clients et les évaluateurs
- Support démontré pour l'inventaire et l'autorisation des scripts
- Surveillance basée sur le comportement au-delà des empreintes statiques de fichiers
- Surveillance continue des pages de paiement et des en-têtes HTTP
- Réduction du travail de préparation des preuves pour les évaluations QSA
- Reconnaissance d'une valeur ajoutée plus large en matière de sécurité de la chaîne d'approvisionnement

permet également d'améliorer la surveillance des pages de paiement sans modifications importantes du code ni charge technique excessive.

Lorsqu'elle est correctement configurée et intégrée à un programme plus large de gouvernance, de gestion des risques et de conformité, Reflectiz peut constituer une alternative plus efficace et plus durable aux examens manuels des scripts et aux approches de surveillance statiques.

Perspectives

Cette évaluation indépendante fournit à Reflectiz une base solide pour démontrer comment sa plateforme peut aider les organisations à répondre aux exigences PCI DSS relatives à la sécurité des pages de paiement.

La plateforme peut également apporter une valeur plus large en améliorant la visibilité sur les chaînes d'approvisionnement numériques, en identifiant les menaces côté client et en soutenant des programmes plus vastes de gouvernance, de protection de la vie privée et de conformité réglementaire.

Pour les commerçants éligibles au SAQ A, une mise en œuvre correcte peut également contribuer à démontrer que les pages de paiement ne sont pas vulnérables aux attaques basées sur des scripts. L'éligibilité et les résultats de conformité dépendent toutefois de l'environnement et des contrôles propres à chaque commerçant.



À propos d'Integrity360

Integrity360 est un spécialiste indépendant de premier plan en cybersécurité et PCI, opérant dans la région EMEA et en Amérique du Nord, avec des bureaux au Royaume-Uni et en Irlande, en Bulgarie, en Italie, en Suède, en Espagne, en Allemagne, en Suisse, en France, en Belgique, en Lituanie, en Ukraine, en Afrique, dans les Caraïbes et au Canada. L'entreprise exploite des Centres d'Opérations de Sécurité (SOC) à Dublin, Madrid, Sofia, Stockholm, Rome et Le Cap, assurant une surveillance et une réponse continues à travers plusieurs fuseaux horaires. Avec plus de 700 collaborateurs, dont plus de 580 professionnels dédiés à la cybersécurité, Integrity360 propose une gamme complète de services professionnels, de support et de sécurité managée couvrant l'ensemble du cycle de vie du risque cyber, de l'identification et de la prévention jusqu'à la détection, la réponse et la remédiation.



Gartner

Integrity360 figure dans six guides de marché de Gartner consacrés aux fournisseurs de services de sécurité gérés, aux services SIEM gérés, à la détection et à la réponse gérées, ainsi qu'aux services de sécurité cogérés, à la réponse aux incidents et à l'analyse forensic.

3000+

Clients
professionnels

585+

Professionnels de
la cybersécurité