NOTRE EXPERTISE

En tant qu'organisation de cybersécurité de premier plan et entreprise certifiée Qualified Security Assessor (QSA), GoSecure possède l'expertise et les capacités requises pour fournir une vaste gamme de services essentiels pour aider toute organisation à atteindre et à maintenir la conformité PCI DSS.

Les **Évaluateurs de sécurité qualifiés (QSA)** s'agissent d'organisations de sécurité indépendantes qui sont certifiées par le PCI SSC pour effectuer des évaluations et des audits de la conformité des entreprises avec la norme PCI DSS. Les QSA effectuent des évaluations sur site, examinent la documentation et fournissent des recommandations pour atteindre et maintenir la conformité.

Les **Prestataires de services d'analyse agréés (ASV)** sont des organisations autorisées par le PCI SSC à effectuer des analyses de vulnérabilité sur les réseaux et systèmes externes. Ils aident à identifier les failles de sécurité qui pourraient être exploitées par des pirates. Les ASV fournissent des rapports et des recommandations pour aider les organisations à remédier aux vulnérabilités découvertes au cours du processus d'analyse.

Le **Conseil des normes de sécurité PCI (PCI SSC)** est l'organe directeur qui gère le PCI DSS et les normes connexes. Bien que le PCI SSC ne fournisse pas directement de services PCI DSS, il définit les normes et les exigences de certification pour les QSA et les ASV.

NORMES DE SÉCURITÉ DES DONNÉES DE L'INDUSTRIE DES CARTES DE PAIEMENT (PCI DSS)

2023

[Transactions sécurisées, conformité assurée]

La Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) est un ensemble de normes de sécurité conçues pour garantir que toutes les entreprises qui acceptent, traitent, stockent ou transmettent des informations de cartes de crédit maintiennent un environnement sécurisé. Il aide les organisations à protéger les données des cartes de paiement et à répondre aux normes de l'industrie.

L'offre de conseil et de conformité PCI DSS de GoSecure comprend :

- **Établissement du champ d'application/réduction du champ d'application :** Notre équipe QSA est spécialisée dans la fourniture de conseils rentables pour atteindre la conformité PCI DSS, réduisant efficacement l'exposition des clients à la manipulation des données de cartes et l'empreinte globale de la conformité.

- **Analyse des lacunes :** Une fois le champ d'application défini, les spécialistes de GoSecure s'engagent avec le client à évaluer les activités et les pratiques de traitement des données des titulaires de cartes, en les comparant à la norme afin d'identifier toute lacune en matière de conformité. Grâce à l'analyse des écarts, nous développerons en collaboration une stratégie de conformité.

- **Mise en œuvre et remédiation :** En fonction du niveau de conformité et des besoins spécifiques, il peut s'agir d'une variété de services comprenant l'aide à la documentation, la sensibilisation et la formation à la sécurité ou des conseils ad hoc.

- **Audits ou auto-évaluations assistées :** Y compris des audits complets aboutissant à la délivrance d'un rapport de conformité (ROC), ainsi qu'une assistance dirigée par un QSA pour les questionnaires d'auto-évaluation (SAQ) par rapport à n'importe quelle version valide de la norme.

- **Consultation PCI DSS :** Grâce à une banque d'heures de services professionnels à échéance annuelle, les clients de GoSecure ont accès tout au long de l'année à notre équipe de conseillers QSA, ce qui leur permet d'obtenir à tout moment des conseils et un soutien concernant leur conformité à la norme PCI DSS.

L'orientation du mandat sera déterminée par vos objectifs et besoins uniques. En conséquence, nous exécuterons une ou plusieurs des activités détaillées dans la section précédente, conformément à la portée définie du projet.

Remarque : les QSA sont les seules entités tierces qui peuvent officiellement cosigner votre Attestation de conformité (AoC) et votre ROC PCI DSS. Nous desservons le Canada, l'Amérique latine et les Caraïbes.

[CONTACTEZ-NOUS : +1 855 893-5428]

PLAN DE TRAVAIL PCI DSS DE GOSECURE

- **Détermination de la portée/réduction de la portée**

Cette phase implique la tâche critique de définir les limites de l'environnement des données du titulaire de la carte (CDE). La phase de détermination de la portée est d'une importance capitale dans le processus de GoSecure, car elle jette les bases de toutes les phases suivantes, en façonnant les actions et les stratégies qui, en fin de compte, ouvriront la voie à la mise en conformité.

- **Entretiens et observations**

Comprend l'évaluation des pratiques de sécurité actuelles (y compris les politiques, les procédures et les contrôles techniques) dans le cadre défini de la conformité PCI DSS afin d'identifier les domaines et les systèmes qui ne s'alignent pas sur les exigences PCI DSS.

- **Mise en œuvre et remédiation**

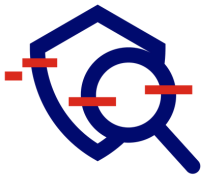
Comprend les conseils pour tous les problèmes identifiés afin de répondre aux exigences de la norme PCI DSS.

- **Rapport**

Comprend le processus d'établissement de rapports sur la conformité. Selon l'organisation, cela peut prendre la forme d'un questionnaire d'auto-évaluation que GoSecure remplit au nom du client, avec ou sans la validation expresse d'un évaluateur de sécurité qualifié (QSA), ou la réalisation d'un ROC et de l'AOC et de l'INFI associés. GoSecure remplit un rapport de fin de projet supplémentaire pour chaque projet PCI DSS.

PROCESSUS GÉNÉRAL POUR LA PLUPART DES MANDATS DE PCI DSS

- Définition des limites de l'environnement des données du titulaire de la carte (CDE).
- Identification et compréhension des processus de paiement actuels.



PORTÉE

ENTRETIENS ET OBSERVATIONS

- Identification des domaines qui ne sont pas conformes aux exigences de la norme PCI DSS.

- Mise en œuvre de la stratégie de conformité.

CONSEILS DE MISE EN ŒUVRE

RAPPORTS

- Il s'agit soit d'un audit complet, soit d'une auto-évaluation assistée.

[CONTACTEZ- NOUS : +1 855 893 5428]

GoSecure est un leader et un innovateur reconnu en matière de cybersécurité, pionnier de l'intégration de la détection des menaces au niveau des points d'extrémité, du réseau et de la messagerie électronique en un seul service géré de détection et de réponse étendues (MXDR). La plateforme GoSecure TitanMC offre une détection prédictive multi-vectorielle, une prévention et une réponse pour contrer les cybermenaces modernes. GoSecure TitanMC MXDR offre une réponse rapide et des services d'atténuation active qui touchent directement le réseau et les points de terminaison des clients. Depuis plus de 20 ans, GoSecure aide ses clients à mieux comprendre leurs lacunes en matière de sécurité et à améliorer leurs risques organisationnels et leur maturité en matière de sécurité grâce aux solutions MXDR et aux services professionnels fournis par l'une des équipes les plus fiables et les plus compétentes de l'industrie. Pour en savoir plus, visitez le site :

www.gosecure.ai/fr

Votre allié pour consolider, évoluer et prospérer

GoSecure