Description de service : <<Advanced Services – Fixed Price Cisco Security Advisory Services: PCI-DSS Readiness Assessment>> Services de conseil en sécurité de Cisco : Évaluation de la conformité à la norme PCI-DSS

ASF-CORE-PCI-DSS

Le présent document décrit le Service à prix fixe de conseil en sécurité de Cisco : évaluation de la conformité à la norme PCI-DSS.

Documents connexes : le présent document doit être lu conjointement avec les documents suivants, également présents sur le site www.cisco.com/ca/aller/descriptionsduservice/ : (1) Glossaire; (2) Liste des services non couverts. Tous les termes en lettres majuscules figurant dans cette description revêtent la signification qui leur est donnée dans le glossaire.

Vente directe par Cisco Si vous avez souscrit ces Services directement auprès de Cisco pour votre propre usage interne, ce document est intégré à votre Contrat-cadre de services (MSA, Master Services Agreement), à votre Contrat de services avancés (ASA, Advanced Services Agreement) ou à tout autre contrat de services avancés conclu avec Cisco (le « Contrat-cadre »). Si aucun Contrat-cadre de ce type n'a été conclu entre vous et Cisco, la présente Description de service est alors régie par les conditions générales figurant dans le Contrat de conditions générales accessible à l'adresse suivante : http://www.cisco.com/web/CA/about/doing_business/legal/terms_conditions_fr.html. Si vous avez souscrit ces services directement auprès de Cisco à des fins de revente, ce document est intégré à votre Contrat pour les intégrateurs de systèmes ou à tout autre contrat de service couvrant la revente des Services avancés (le « Contrat-cadre de revente »). Si le Contrat-cadre de revente ne renferme pas les modalités d'Achat et de Revente des Services avancés Cisco ou des conditions générales analogues, la présente Description de service est régie par les conditions générales du Contrat-cadre de revente, ainsi que par les conditions générales exposées dans le Contrat de conditions générales de revente EDT, accessible à l'adresse http://www.cisco.com/web/CA/about/doing_business/legal/terms_conditions_fr.html. Aux fins du Contrat susmentionné, la présente description de service doit être considérée comme un Énoncé des travaux (« EDT »). En cas de conflit entre la présente description de service et le Contrat-cadre (ou annexe ou entente équivalente), cette description de service fait foi.

Vente par un revendeur agréé Cisco. Si vous avez souscrit ces Services auprès d'un revendeur agréé Cisco, ce document n'a qu'un caractère informatif et ne constitue en aucun cas un contrat entre vous et Cisco. Le contrat (s'il y a lieu) qui régit la prestation de ce Service est celui établi entre vous et votre Revendeur agréé Cisco. Votre Revendeur agréé Cisco doit vous fournir ce document. Vous pouvez également en obtenir une copie, ainsi que d'autres descriptions des services proposés par Cisco, à l'adresse suivante : www.cisco.com/ca/aller/descriptionsduservice/.

Évaluation de la conformité à la norme PCI-DSS

Résumé du service
Cisco évaluera l'environnement de données de titulaires de cartes (« CDE ») du Client par rapport à la norme du secteur des cartes de paiement (« SCP ») pour repérer les écarts de conformité et fournir des recommandations en vue de garantir la conformité aux exigences actuelles de la norme PCI DSS et le respect des procédures d'évaluation de la sécurité en vigueur. Ces renseignements sont fournis sur le site Web des normes PCI, à l'adresse suivante : <https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security>.

L'évaluation se tiendra dans un (1) local professionnel du Client et comprendra l'examen de la documentation, jusqu'à douze (12) entretiens avec les parties prenantes clés et une (1) inspection des données ou du centre d'appels.

Lieu de la prestation
Le service sera fourni sur site dans un local du Client.

Les déplacements de Cisco seront limités à deux (2) visites de cinq (5) jours sur site au maximum à un emplacement unique du Client.

Collecte de renseignements avant l'évaluation

Responsabilités de Cisco

- S'assurer que le Client a trouvé les personnes, les processus et les technologies appropriés dans le cadre du service, conformément à la section des « Champ d'application des exigences de la norme PCI DSS » du document sur les procédures PCI DSS en vigueur.
- Fournir au Client une liste de vérification détaillée sur la documentation nécessaire aux fins de cette mission.
- Examiner les besoins du Client concernant la production de rapports et l'évaluation par rapport à la norme PCI.

Responsabilités du Client

- Trouver un commanditaire de projet qui aura pour responsabilité de mener à bien le projet et aura le pouvoir de prendre les décisions relatives à l'exécution du projet.
- Désigner un chef de projet pour planifier les réunions des parties prenantes et pour remplir les demandes de renseignements.
- Avant ou lors du lancement du projet, le Client doit confirmer l'accès aux ressources identifiées entrant dans le champ d'application, aux fins de l'évaluation par rapport à la norme de sécurité des données des cartes de paiement.
- Fournir à Cisco un accès aux locaux de bureau pertinents pour les réunions, les entretiens et les présentations dans le cadre des travaux effectués sur le site du Client.
- Indiquer les coordonnées d'urgence notamment le nom, la fonction, l'adresse de courriel, ainsi que les numéros de téléphone professionnel et cellulaire.

Évaluation, analyse et tests

Responsabilités de Cisco

- Analyser et documenter le champ d'application de l'évaluation de la conformité à la norme PCI DSS en précisant les éléments suivants :
  - Emplacements
  - Connexions de transfert de paiement
  - Canaux de paiement
  - Responsabilités et rôles du personnel
  - Segments du réseau informatique
  - Emplacements de stockage des données des titulaires de cartes
  - Matériel et logiciels
  - Fournisseurs de services et tierces parties
- Effectuer une évaluation détaillée de l'environnement des titulaires de cartes du Client. L'évaluation comprendra :
  - des entretiens avec les parties prenantes du Client.
- Examiner les politiques et procédures pour repérer les écarts existants et les corrections requises pour se conformer à la norme PCI DSS. L'examen sera effectué en se conformant aux exigences de la norme PCI alors en vigueur, accessibles sur le site Web des normes PCI, à l'adresse suivante : <https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security>.
- Effectuer des analyses de contrôles substitutifs.

Après l'évaluation

Responsabilités de Cisco

- Créer un plan d'action stratégique, opérationnel et tactique pour traiter les cas de non-conformité détectés.
- Fournir au Client le Rapport d'évaluation de la conformité à la norme PCI.
- Fournir au Client une présentation sommaire. La présentation ne doit pas durer plus d'une (1) heure.

Responsabilités du Client

- Désigner les parties prenantes qui assisteront à la présentation sommaire.
- Examiner le Rapport d'évaluation de la conformité à la norme PCI.

Responsabilités générales du Client

- Le Client déclare et garantit qu'il dispose de l'autorité et des droits nécessaires pour fournir et/ou prendre les dispositions nécessaires pour garantir à Cisco l'accès aux renseignements, aux données, aux réseaux, aux systèmes et aux supports liés à ces Services.
- Pour toute demande du Client, en vertu de cette Description de service, nécessitant que Cisco possède, accède ou analyse des supports, ordinateurs, réseaux informatiques, réseaux de communications ou autres systèmes et équipement particuliers, dans la mesure où le Client fournit ou prend les dispositions nécessaires pour garantir à Cisco l'accès à ces éléments, le Client déclare et garantit qu'il détient tous les droits, titres, licences et autorisations nécessaires pour réaliser une telle demande et autoriser ledit accès, y compris le cas échéant la permission de propriétaires tiers de licences ou ressources partagées.
- IL EST DE LA RESPONSABILITÉ DU CLIENT D'OBTENIR L'ENSEMBLE DES LICENCES, PERMISSIONS ET AUTORISATIONS NÉCESSAIRES POUR PERMETTRE À CISCO D'ACCÉDER AUX RESSOURCES QUI SONT HÉBERGÉES OU DÉTENUES PAR UNE TIERCE PARTIE, OU LEUR SONT TRANSMISES.
- Le Client est responsable du provisionnement des accès, environnements, connexions RPV, comptes d'utilisateur, accès administratifs ou autres éléments techniques nécessaires au test.
- Tous les renseignements (notamment les conceptions, les topologies et les exigences) que le Client fournit sont supposés être à jour et valides pour son environnement actuel. Les Services réalisés par Cisco sont basés sur les renseignements fournis à ce dernier par le Client au moment des services.
- Le Client reconnaît que l'achèvement des Services dépend du fait qu'il s'acquitte de ses responsabilités, comme indiqué ci-après.
- Le Client identifiera le personnel du Client et définira le rôle de chacun dans la participation aux Services. Les membres d'un tel personnel peuvent comprendre, sans toutefois s'y limiter, les spécialistes en ingénierie de planification et de conception de l'architecture et les spécialistes en ingénierie de réseau.

- Le Client veillera à ce que son personnel soit disponible pendant l'exécution des Services pour fournir des renseignements et participer aux séances de collecte de renseignements prévues, aux entretiens, aux réunions et aux conférences téléphoniques.
- Le Client comprend et convient expressément que les services d'assistance fournis par Cisco comprennent conseils, assistance et orientation techniques seulement.
- Le Client comprend et accepte expressément que les Services seront exécutés dans un délai de quatre-vingt-dix (90) jours civils à compter de l'envoi d'un Bon de commande à Cisco pour les Services décrits aux présentes; toutes les heures inutilisées seront perdues.

Facturation et achèvement

Facturation

Les Services sont facturés après leur réalisation.

Achèvement des Services

Cisco informera le Client par écrit une fois les Services réalisés. Le Client devra accuser réception de cette notification dans les cinq (5) jours ouvrables et attester par écrit que Cisco a bien réalisé les Services. Si le Client ne confirme pas la réalisation des Services ou ne justifie pas le refus des Services dans les cinq (5) jours ouvrables, la réalisation des Services est considérée comme acceptée conformément à la présente description de service.

Hypothèses et exclusions

- Il incombe entièrement au Client de déterminer et de mettre en œuvre les exigences de réseau, de conception, commerciales ou autres, ainsi que d'appliquer les recommandations éventuelles fournies par Cisco. Les recommandations de Cisco sont fondées sur les renseignements sur le Client qui lui ont été fournis. Cisco ne peut en aucune circonstance être tenue responsable de l'exactitude ou de l'exhaustivité des renseignements sur le Client contenus dans les recommandations de Cisco.
- Tous les documents seront fournis au format électronique en anglais.
- Le Client demeure entièrement responsable de la sécurité de ses environnements techniques. Cisco n'est en aucun cas responsable de toute faille dans la sécurité de l'environnement du Client. Cisco ne peut garantir que la vulnérabilité, ou au contraire l'invulnérabilité, de la sécurité du Client face à des instances incluses, omises ou négligées présentées ou non dans les Services ou Éléments livrables associés à la présente Description de service.
- Les services d'évaluation de la sécurité ne prouveront en aucun cas l'absence de vulnérabilités (uniquement la conformité).