Description de service : <<Advanced Services – Fixed Price

Cisco Security Advisory Services: Blackbox Web Application Assessment (L)>> Services de conseils en sécurité de Cisco : évaluation des applications Web en mode boîte noire (L)

ASF-CORE-BBAPP-120

Ce document décrit le Service à prix fixe d'évaluation des applications Web en mode boîte noire (L) de Cisco, réalisé pour un maximum de 120 pages Web dynamiques.

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 des applications Web en mode boîte noire

Résumé du service

Cisco procédera à une évaluation des applications en mode boîte noire pour un maximum de 120 pages Web dynamiques et douze (12) rôles authentifiés, définis comme un ensemble commun de droits d'accès accordés à un groupe d'utilisateurs. L'évaluation permet de repérer la surface d'attaque immédiate de l'application. Cisco analyse alors la surface pour détecter les vulnérabilités grâce à des techniques de test manuelles et automatisées. Une fois les renseignements d'authentification fournis, Cisco réalisera des tests en mode authentifié. Le principal objectif des tests est de repérer les vulnérabilités de la couche applicative dans le code d'application. Toutefois, la méthodologie de test peut également mener à la découverte de vulnérabilités dans les dépendances immédiates de l'application.

Lieu de la prestation

Les Services sont fournis à distance.

Analyse

Responsabilités de Cisco

- Effectuer une analyse à l'aide d'une série de techniques conçues pour repérer les vulnérabilités présentant un risque pour la sécurité. Pour réaliser cette évaluation, Cisco appliquera les stratégies principales suivantes :
    - Recensement de la surface d'attaque : tentative de détection des fonctionnalités de l'application grâce à la traversée automatisée de l'arborescence du site et à la permutation des variantes courantes sur les conventions de nomenclature populaires
    - Injection manuelle d'erreurs : envoi manuel de données malveillantes pour repérer les vulnérabilités relatives à la sécurité sur le chemin de requête
    - Injection automatisée d'erreurs : envoi automatisé de données malveillantes pour repérer les vulnérabilités relatives à la sécurité sur le chemin de requête
    - Test de vulnérabilité connue : repérage des vulnérabilités sur la plateforme d'hébergement (serveur Web, conteneur de servlet) à l'aide, principalement, de techniques d'analyse automatisée
    - Repérage des risques de vulnérabilités : analyse automatisée permettant de repérer des schémas de vulnérabilité connus, suivie d'une analyse manuelle pour valider toute vulnérabilité suspectée
    - Corrélation de données
    - Recherche des vulnérabilités
    - Élimination des faux positifs
    - Étude de l'étendue des résultats

Évaluation

Responsabilités de Cisco

- Mener une téléconférence de lancement afin d'examiner le plan de projet et d'identifier les principales parties prenantes chez Cisco et chez le Client.
- Évaluer au maximum 120 pages Web dynamiques et 12 rôles, afin de repérer les problèmes de sécurité pertinents, notamment les classes de vulnérabilités suivantes :
    - Vulnérabilités d'injection (injection de commande, injection SQL)
    - Vulnérabilités aux attaques sur les éléments dynamiques (XSS) et autres vulnérabilités d'injection basées sur script
    - Falsification de requêtes intersites (CSRF)
    - Vulnérabilités de gestion la mémoire
    - Vulnérabilités de validation d'entrée et de sortie
    - Vulnérabilités de gestion des sessions
    - Vulnérabilités de contrôle d'accès
    - Vulnérabilités de canonisation de chemin
    - Utilisation inefficace ou insuffisante du cryptage
    - Déni de service lié à l'application
    - Propagation de renseignements sensibles
    - Stockage sécurisé de secrets
    - Vulnérabilités relatives au traitement général des données
    - Références non sécurisées à un objet
    - Conception ou logique pouvant provoquer des failles de sécurité
    - Problèmes applicables non mentionnés explicitement ci-dessus, mais couverts par les normes pertinentes (Top 10 OWASP, Top 20 SANS)
    - Failles relatives à la configuration
    - Failles de sécurité des communications

Responsabilités du Client

- S'assurer que les personnes clés se prêtent à des entretiens avec Cisco et participent à la résolution des problèmes techniques.
- Fournir à Cisco les schémas d'application et autres documents existants (le cas échéant).
- Déterminer deux (2) comptes utilisateurs pour chaque rôle qui fera l'objet d'un test pendant l'évaluation.
- Fournir à Cisco les URL des applications évaluées (le cas échéant).
- Convenir avec Cisco d'une plage horaire pour la réalisation des tests.
- Fournir à Cisco un accès de niveau administrateur aux systèmes évalués ou mettre à sa disposition du personnel capable d'effectuer les tâches administratives en cas de problèmes techniques.
- Fournir des versions de débogage et de production du logiciel cible (le cas échéant).
- Autoriser l'installation et l'utilisation des équipements et outils de Cisco dans l'environnement cible.
- S'assurer que l'application contient assez de données pour permettre l'accès à toutes les fonctionnalités.
- Fournir toute donnée, numérique ou autre, spécifique. Il s'agit de renseignements uniques existant sur le système qui seraient connus de l'utilisateur réel, mais pas nécessairement de Cisco.
- Fournir tout matériel d'authentification nécessaire.

Création de rapports

Responsabilités de Cisco

- Transmettre au Client un rapport d'évaluation d'applications en mode boîte noire, comprenant les éléments suivants :
    - Portée et approche
    - Liste hiérarchisée des résultats
    - Détails des vulnérabilités découvertes.
- Planifier une téléconférence avec les principales parties prenantes identifiées au sein de la direction du Client afin de passer en revue les résultats

Responsabilités du Client

- Trouver les parties prenantes devant participer à la téléconférence d'examen des résultats avec Cisco.
- En collaboration avec Cisco, examiner le rapport d'évaluation des applications en mode boîte noire.
- Approuver le rapport afin de clôturer la prestation de services d'évaluation d'applications en mode boîte noire.

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 sera tenu responsable de tout retard dans le provisionnement des accès, environnements, connexions RPV, comptes d'utilisateur et accès administratifs ou autres éléments techniques nécessaires à l'évaluation.
- 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 choisira les membres du personnel 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 qu'une page Web non évaluée dans le cadre du Service n'entraînera pas de crédit.
- 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

- Sauf indication contraire dans les présentes, le Client est responsable de la fourniture des équipements de test.
- 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 définitive de vulnérabilités.

- Le Client comprend et reconnaît que, dans la mesure où Cisco a pris des précautions raisonnables dans l'exécution des Services, il n'est pas responsable des indisponibilités du système, de la dégradation des performances ou autres conséquences adverses pour l'environnement technologique découlant des tâches que le Client a autorisé Cisco à exécuter.
- Cisco recommande au Client de sauvegarder son environnement et d'effectuer une maintenance avant le début de la prestation de Services et rappelle au Client qu'une telle sauvegarde tient de son entière responsabilité.