Description de service : <<Advanced Services – Fixed Price

Cisco Security Advisory Services: Internal Network Penetration Assessment (M)>> Services de conseils en sécurité de Cisco : évaluation des intrusions dans le réseau interne

ASF-CORE-INPEN-800

Le présent document décrit le Service à prix fixe de Test d'intrusion depuis un réseau interne (M) de Cisco.

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 intrusions dans le réseau interne

Résumé du service
Cisco réalisera un test d'intrusion dans le réseau interne pour un maximum de 800 adresses IP privées actives. Le test visera à repérer les vulnérabilités exploitables et à déterminer l'efficacité des investissements en matière de sécurité dans le cadre d'une attaque simulée.

Lieu de la prestation
Le test d'intrusion dans le réseau interne sera réalisé dans les locaux du Client ou à partir d'un ou de plusieurs des sites distants par l'entremise d'une connexion à distance sécurisée.

Les déplacements de Cisco seront limités à six (6) visites d'au maximum vingt-trois (23) jours sur site à un emplacement unique du client.

Collecte de renseignements avant l'évaluation

Responsabilités de Cisco

- Mener une téléconférence de lancement afin d'examiner le plan de projet, de définir les objectifs du test et de repérer les principales parties prenantes chez Cisco et chez le Client.
- Essayer de recueillir les renseignements nécessaires, de la manière suivante :
    - Effectuer une analyse de périmètre des protocoles, services, systèmes d'exploitation et autres technologies
    - Repérer les défenses de sécurité à contourner
    - Repérer les utilisateurs et administrateurs du système
    - Repérer les composants du système
    - Créer un aperçu de la surface d'attaque
- Réaliser la modélisation des menaces, la détection des vulnérabilités et l'analyse de la surface d'attaque comme suit :
    - Réaliser une analyse manuelle et automatisée afin de repérer les vulnérabilités
    - Utiliser, s'il y a lieu, des techniques de test à données aléatoires ou de rétro-ingénierie sur les services découverts
    - Rechercher les menaces applicables aux logiciels et aux actifs de systèmes découverts
    - Hiérarchiser les attaques en fonction des objectifs de l'analyse

Responsabilités du Client

- Fournir une documentation technique précise et détaillée pour les réseaux, notamment les caractéristiques techniques, les schémas de conception globale, les technologies utilisées, la documentation de développement, la documentation de conception et les schémas utilisés dans les études de cas.
- Garantir un accès aux personnes clés pour les questions techniques

Exploitation

Responsabilités de Cisco

- Réaliser les activités d'exploitation suivantes sur un maximum de 800 adresses IP privées actives, indiquées par le Client, le cas échéant :
    - Tirer parti des faiblesses de conception et d'architecture en réalisant une écoute passive du réseau et des attaques de l'intercepteur
    - Compromettre les composants du système en exploitant les failles de mise en œuvre dans le logiciel au moyen de débordements de mémoire tampon, d'exécutions de codes à distance, d'attaques sur les éléments dynamiques (XSS), d'injections SQL et d'autres attaques d'injection de commande
    - Tester les failles opérationnelles liées aux pratiques de gestion des correctifs, de gestion de la configuration et de déploiement de système
    - Exploiter les faiblesses de l'utilisateur en essayant de deviner les mots de passe ou en lançant des attaques pour les décoder
    - Contourner les contrôles de sécurité en échappant aux pare-feu, aux systèmes de détection des intrusions, aux antivirus, aux contrôles d'accès, aux protections cryptographiques et aux systèmes de prévention des pertes de données

Responsabilités du Client

- Indiquer une plage horaire pour la réalisation du test
- Fournir jusqu'à 800 adresses IP privées actives à tester
- Fournir des renseignements d'identification supplémentaires sur la cible (p. ex. : noms d'hôtes, URL)

Postexploitation

Responsabilités de Cisco

- Réaliser les activités de postexploitation suivantes, lorsqu'elles sont applicables et validées par le Client :
    - Exploiter les vulnérabilités découvertes pour établir une menace persistante
    - Exploiter les vulnérabilités découvertes pour obtenir des droits d'accès supplémentaires
    - Effectuer une recherche de données sensibles et de renseignements d'identification (p. ex. : renseignements personnels, numéros de carte de crédit)
    - Essayer de rediriger les attaques vers des cibles supplémentaires
    - Essayer d'exfiltrer les données, lorsque cela est possible et conforme aux objectifs du projet
- Fournir les rapports suivants :
    - Éliminer les faux positifs, si possible
    - Problèmes détectés en tentant d'atteindre les objectifs du projet
    - Analyser les incidences possibles sur l'entreprise
    - Étudier et élaborer des stratégies de correction
- Fournir au Client un document détaillant les résultats du test d'intrusion interne
- 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.
- Examiner avec Cisco le Rapport de test d'intrusion dans le réseau interne.
- Approuver le rapport afin de clôturer la prestation des Services de test des intrusions dans le réseau interne.

Responsabilités générales du Client

- 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.
- 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.
- 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.
- 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 adresse IP non utilisée 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.
- 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.