<<Service Description: Advanced Services – Fixed Price

Cisco Security Incident Response Service (120 hours) (ASF-CORE-IN-RESP) >>

Description du service : Services avancés –Prix fixe

Service d'intervention Cisco pour les incidents liés à la sécurité (120 heures) (ASF-CORE-IN-RESP)

Ce document décrit le prix fixe du Service d'intervention Cisco pour les incidents liés à la sécurité.

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, alors 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, accessibles 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/.

Service d'intervention pour les incidents liés à la sécurité

Résumé du service

Le Service d'intervention Cisco pour les incidents liés à la sécurité fournit au Client une assistance liée aux services d'intervention pour les incidents dans la limite maximale de 120 heures.

Cisco fournit des services d'intervention pour les incidents pour l'une (1) des options de service suivantes (décrites ci-dessous) et les livrables associés :

- Intervention d'urgence pour les incidents et rapport d'intervention d'urgence pour les incidents
- Recherche des menaces (évaluation de compromis) et création de rapport sur la recherche des menaces.

Chaque option comprend deux (2) voyages pour un spécialiste en ingénierie sur site pour une période de trois (3) jours maximum chacun.

Lieu de la prestation

Les Services sont fournis à la fois sur site et à distance au Client.

Analyse préalable

Responsabilités de Cisco

Les responsabilités des parties dépendent de l'option de service que le Client choisit parmi les options ci-dessus et sont les suivantes :

Intervention d'urgence pour les incidents
- Collaborer avec le Client, afin de définir un plan personnalisé pour effectuer toute collecte de données nécessaires, investigation informatique ou installation des outils, et en fonction du besoin afin de répondre à un Incident de sécurité.

Recherche des menaces (Évaluation de compromis)
- Collaborer avec le Client pour définir un plan personnalisé de recherche et effectuer cette recherche. À la fin de l'engagement, fournir un rapport sur la Recherche des menaces.

Analyse

Responsabilités de Cisco

Intervention d'urgence pour les incidents
- Fournir une ressource d'intervention pour les incidents afin d'apporter une assistance de dépannage à distance (par téléphone)
- Commencer le déploiement du personnel vers le site du client dans les 24 heures suivant la réception de la demande écrite
- Utiliser les techniques suivantes :

Triage – Évaluation du contexte actuel pour mieux comprendre comment lancer et concevoir une stratégie d'intervention

Coordination – Suivi de l'état, mesures à prendre et compilation des mises à jour au besoin, afin de s'assurer que l'incident soit correctement géré

Étude – Analyse de la portée de l'attaque par le déploiement et l'utilisation des outils nécessaires, en examinant les sources de journal, afin d'analyser les modèles et les problèmes, en réalisant des investigations informatiques nécessaires et des opérations d'ingénierie inverse pour les maliciels

Retenue – Mise en quarantaine et interruption des autres mesures de l'attaquant

Surveillance – Développement de signatures et surveillance continue de l'environnement tout au long de l'engagement, afin de veiller au maintien du bon état du réseau en fonction du besoin, afin d'aider le Client à gérer l'incident et à y remédier. L'utilisation d'outils Cisco supplémentaires tels que l'AMP, le système Stealthwatch, Umbrella ou des outils tiers peut engendrer des frais supplémentaires et sera acceptée par les parties avant que Cisco ne les fournisse.

Recherche des menaces (Évaluation de compromis)
- Collaborer avec le Client afin de recueillir les exigences en examinant les attaques, les intrusions et les violations antérieures, ainsi que les préoccupations existantes portant sur des acteurs, des événements, des observations spécifiques ou sur des cibles ou des biens de grande valeur
- Confirmer la compréhension des adversaires et les tactiques, techniques et procédures associées
- Développer un contexte portant sur la visibilité du réseau du Client en évaluant les outils disponibles ainsi que les outils et journaux Client dans l'environnement
- Définir les cas d'utilisation de la recherche de menaces
- Identifier les journaux et les accès exigés
- Procéder à la Recherche de menaces en suivant les cas d'utilisation définis

Création de rapports

Responsabilités de Cisco

Intervention d'urgence pour les incidents
- Fournir au Client le Rapport d'intervention pour les incidents dans un délai de 2 semaines après la fin de l'engagement

Recherche des menaces (Évaluation de compromis)
- Fournir au Client le Rapport de recherche des menaces dans un délai de 2 semaines après la fin de l'engagement

Responsabilités du Client

- Participer à la téléconférence de lancement et fournir à Cisco :
  - les coordonnées des principales parties prenantes;
- Examiner avec Cisco le Rapport convenu et l'approuver.

Responsabilités générales du Client

- Tous les renseignements (notamment les conceptions, les topologies et les exigences) que le Client fournit sont censés être à jour et valides pour son environnement actuel. Les Services 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 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 et toutes les heures inutilisées expireront et seront perdues.
  Il incombe au Client de déterminer si la réception et l'utilisation des Services sont conformes aux exigences internes, aux contrats de tiers, et aux lois ou réglementations applicables.

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.