« Service Description: Advanced Services – Fixed Price Cisco Talos Incident Response Service (80 hours)

(ASF-CORE-IN-RESP-S) »

Description du service : Services avancés – Prix fixe Service d'intervention Cisco pour les incidents Talos (80 heures)

(ASF-CORE-IN-RESP-S)

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 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 URL suivante : www.cisco.com/web/CA/about/doing_business/legal/terms_conditions_fr.htm. 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 qui régit la prestation de ce service, le cas échéant, 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 qu'une copie des 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 Talos fournit au Client jusqu'à 80 heures d'assistance Cisco pour l'aider à prévenir et à remédier à un incident de sécurité qui pourrait l'affecter.

Cisco s'engage à fournir le Service d'intervention pour les incidents Talos pour l'une (1) des options de service suivantes :

- **Évaluation de l'état de préparation à l'intervention pour les incidents et Rapport**. Dans le cadre de l'Évaluation de l'état de préparation à l'intervention pour les incidents, Cisco évaluera la capacité du Client à détecter et à gérer un incident, et à y remédier rapidement.
- **Exercice sur table d'intervention pour les incidents et Rapport**. Dans le cadre de l'Exercice sur table, Cisco organisera une ou plusieurs séance(s) de travail avec le Client pour évaluer les scénarios d'incidents. Cisco développera des scénarios personnalisés avant la séance de travail, en fonction des problèmes de sécurité actuels du Client. Au cours de l'exercice, Cisco surveillera et recueillera des données sur le plan d'intervention, sur l'identification des outils et sur les capacités et regroupera les discussions interactives à inclure dans le Rapport d'exercice sur table**.**
- Document de stratégie, planification et guide de gestion des incidents
- Intervention d'urgence pour les incidents et rapport d'intervention d'urgence pour les incidents

Chaque option de service sélectionnée ci-dessus comprend une (1) visite d'un spécialiste en ingénierie sur site pour une période de trois (3) jours maximum.

Lieu de la prestation
Les Services sont fournis à distance et sur site 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 :

Évaluation de l'état de préparation à l'intervention pour les incidents / Plans et guide d'intervention pour les incidents

- Examiner les exigences commerciales du Client pour l'intervention en cas d'incident lié à la sécurité
- Entretien avec la partie prenante du Client chargée de la sécurité de l'information, du service informatique et de la gestion des comptes et des services juridiques
- Examiner les exigences réglementaires liées aux interventions pour les incidents, y compris toute exigence juridique ou réglementaire applicable, ou toute exigence spécifique au Client concernant les notifications de violation
- Examiner la documentation opérationnelle existante du Client sur l'intervention pour les incidents liés à la sécurité

Exercice sur table

- Concevoir des scénarios d'exercice sur table pour le Client en fonction des renseignements qu'il fournit.
- Développer des scénarios et des situations de test et faciliter le test avec le Client. À la fin de l'engagement, fournir un rapport d'exercice sur table qui résume les scénarios de test à utiliser, les paramètres et la portée du test, ainsi que d'autres renseignements similaires.

Intervention d'urgence en cas d'incidente

- 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.

Analyse

Responsabilités de Cisco

Évaluation de l'état de préparation des IR

- Élaborer un processus d'intervention pour les incidents liés à la sécurité qui facilite la gestion des incidents liés à la sécurité des renseignements conformément aux exigences des parties prenantes
- Examiner, avec le Client, le processus recommandé et apporter des modifications conformément à ses demandes
- Créer des modèles pour l'enregistrement des incidents et des communications du Client
- Fournir au Client des documents et modèles d'intervention pour les incidents liés à la sécurité en vue de leur examen et de leur approbation
- Fournir des exigences réglementaires et des exigences Client applicables et effectuer toute analyse juridique requise.

Plans et guide d'intervention pour les incidents

- Élaborer un processus d'intervention en cas d'incidents de sécurité pour prendre en charge la coordination des interventions et des communications en cas d'incidents de sécurité de l'information

Exercice sur table

- Organiser une séance de travail sur site avec le personnel clé du Client pour mettre en pratique l'un des scénarios de ce dernier (au maximum, quatre heures ouvrables)
- Réaliser des entretiens avec les parties prenantes clés du Client une fois l'exercice terminé, afin de recueillir des commentaires, fournir des orientations supplémentaires et identifier d'autres domaines d'évaluation devant être menés à bien par le Client.

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)
- Utiliser les techniques suivantes :

Triage – Évaluation de la situation actuelle afin de déterminer la meilleure façon de concevoir et d'amorcer 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 est 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.

Création de rapports

Responsabilités de Cisco

Évaluation de l'état de préparation des IR

- Fournir un Rapport d'évaluation de l'état de préparation à l'intervention pour les incidents décrivant la documentation relative au processus d'intervention pour les incidents, notamment :
    - Les rôles et responsabilités pour les interventions en cas d'incident
    - Les critères et le procédé de classification pour déterminer les incidents liés à la sécurité

- L'échelle d'évaluation de la criticité de l'incident
- Les procédures et directives

Plans et guide d'intervention pour les incidents

- Fournir les documents des plans et du guide d'intervention pour les incidents

Exercice sur table

- Fournir un rapport d'exercice sur table comprenant :
  - Un résumé
  - La portée et l'approche générale
  - L'intervention pour les incidents en fonction du scénario
  - Les observations et recommandations en matière d'amélioration

Intervention d'urgence en cas d'incident

- Fournir au Client le Rapport d'intervention d'incident à la fin de l'engagement

Responsabilités du Client

- Participer à l'appel pour la réunion 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; toutes les heures inutilisées 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.