<<Service Description: Cisco Optimization Service for Security Enterprise License Agreement>>
Description de service : Contrat de licence de grand compte pour le service d'optimisation de la sécurité Cisco

Le présent document décrit le Contrat de licence de grand compte pour le service d'optimisation de la sécurité Cisco.

Documents connexes : ce document doit être lu conjointement avec les documents suivants, également disponibles à l'adresse www.cisco.com/ca/aller/descriptionsduservice/ : (1) Glossaire; (2) Liste des services non couverts; et (3) Directives en matière de gravité et de signalisation progressive. 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 aux Services directement auprès de Cisco, ce document fait partie intégrante de votre Contrat-cadre de services (MSA, Master Services Agreement) convenu avec Cisco. En cas de conflit entre la présente description de service et votre contrat MSA, la présente description de service prévaudra.

Vente par un revendeur agréé Cisco. Si vous avez souscrit à 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, le cas échéant, 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.

Résumé du service

L'ALE relatif au service d'optimisation de la sécurité de Cisco vise à compléter un contrat d'assistance en vigueur pour des produits Cisco. Cisco s'engage à fournir le Service d'optimisation de la sécurité décrit ci-dessous comme sélectionné et détaillé sur le Bon de commande pour lequel Cisco a reçu le paiement correspondant. Cisco doit fournir un devis pour les services (le « Devis ») précisant l'étendue des services et la durée de prestation de ces derniers par Cisco. Cisco doit recevoir un Bon de commande qui fait référence au Devis convenu entre les parties et qui reconnaît et accepte en outre les conditions dudit document.

Responsabilités générales induites par le Service

Cisco et le Client devront assumer les responsabilités générales indiquées dans la section ci-dessous.

Responsabilités générales de Cisco par rapport au service

Cisco devra se conformer aux dispositions générales suivantes pour tout Service d'optimisation de la sécurité spécifié dans le Devis :

- En vertu de ce Service, et sauf indication contraire, Cisco devra fournir l'ALE relatif au Service d'optimisation de la sécurité de Cisco au cours des Heures d'ouverture normales.
- Désigner un interlocuteur unique (le « Gestionnaire de projet Cisco ») pour tous les problèmes liés aux Services.
- Participer à des réunions périodiques avec le Client pour évaluer l'état des Services.
- Veiller à ce que les employés et sous-traitants de Cisco respectent les règles raisonnables du Client relatives au milieu de travail, ainsi que ses conditions et règles de sécurité communiquées par écrit à Cisco avant le début des Services, dans la limite des obligations de Cisco définies dans la présente description de service. Il est toutefois entendu que le personnel et les sous-traitants de Cisco ne doivent être contraints ni de signer des accords individuels avec le Client ni de renoncer à des droits personnels.
- Fournir au personnel de l'équipe du projet de Cisco des badges qu'ils porteront en permanence pendant les activités du service menées sur le site du Client.

- Cisco se réserve le droit de déterminer quels membres de son personnel doivent être affectés à un projet en particulier, de remplacer ou de réaffecter ce personnel et/ou de sous-traiter à des tiers qualifiés tout ou partie du Service d'optimisation de la sécurité aux termes des présentes. Le Client peut demander le retrait ou la réaffectation du personnel de Cisco à tout moment, toutefois il devra alors prendre en charge les coûts supplémentaires engendrés par ce retrait ou cette réaffectation du personnel de Cisco. Cisco ne saurait prendre en charge les frais entraînés par les retards engendrés par le retrait ou la réaffectation du personnel de Cisco.

Responsabilités générales du client

Services généraux

Le Client doit se conformer aux obligations suivantes afférentes aux Services généraux pour tout contrat de licence d'entreprise relatif au service d'optimisation de la sécurité indiqué dans le Devis :

- Désigner entre deux (2) et six (6) représentants techniques. Il doit s'agir d'employés du Client qui ont des fonctions d'administrateurs ou de spécialistes en ingénierie et qui joueront le rôle d'interlocuteurs techniques privilégiés du ou des spécialistes en ingénierie désignés par Cisco. Le Client désignera comme personnes-ressources des spécialistes en ingénierie expérimentés, dotés des compétences appropriées pour apporter les modifications nécessaires à la configuration du Réseau. Une personne, membre expérimenté de l'équipe de gestion ou technique, est désignée comme interlocuteur privilégié du Client pour gérer la mise en œuvre des services dans cette Description de service (par exemple, présider les audioconférences hebdomadaires, faciliter la hiérarchisation des projets et des activités).
- S'assurer que le personnel d'ingénierie, réseau et d'exécution clé est disponible afin de participer à des entretiens et d'examiner des rapports, et ainsi permettre à Cisco de réaliser le Service.
- Le centre d'assistance technique du Client doit maintenir une administration centralisée du réseau et de la sécurité pour son Réseau pris en charge en vertu de la présente description de service, et être capable de fournir une assistance de Niveau 1 et de Niveau 2.
- Fournir un accès électronique raisonnable au Réseau du Client pour permettre au spécialiste en ingénierie désigné par Cisco d'apporter son aide.
- Le Client accepte de mettre à disposition son environnement de production et, le cas échéant, son environnement Réseau de test, pour l'installation des Outils de collecte de données. Le client devra s'assurer que Cisco dispose de tous les renseignements sur le Produit nécessaires à l'évaluation.
- Si Cisco fournit des scénarios ou des Outils de collecte de données sur le site du Client, ce dernier devra s'assurer que ces scripts ou outils sont situés dans une zone sécurisée, au sein d'un environnement Réseau protégé au moyen d'un pare-feu et sur un réseau local (LAN) sécurisé, sous clef et avec accès limité aux employés ou sous-traitants du Client qui ont besoin d'accéder aux Outils de collecte de données et de connaître le contenu des résultats de ces outils. Dans le cas où l'Outil de collecte de données fourni par Cisco est un logiciel, le Client s'engage à mettre à disposition des ordinateurs appropriés et à télécharger les logiciels nécessaires. Le Client est responsable de tout dommage, de toute perte ou de tout vol des Outils de collecte de données lorsqu'ils sont en sa possession.
- Fournir une carte de topologie de Réseau, les détails de configuration et des renseignements sur les nouvelles fonctionnalités mises en œuvre, selon les besoins.
- Fournir la documentation sur les exigences, les conceptions de base et détaillées, les plans de mise en œuvre et les plans de test comme requis pour les services spécifiques.
- Informer sans délai Cisco de tout changement important relatif à la politique de sécurité (p. ex. changement de règle de pare-feu ou de politique du système informatique unifié Cisco [ISE]) ou au Réseau (topologie, configuration, nouvelles versions IOS, déplacements, ajouts, modifications ou suppressions d'appareils).
- Si la composition du Réseau ou de la Sécurité a été modifiée après l'entrée en vigueur de cette Description de service, le Client doit en informer Cisco par écrit dans les dix (10) jours suivant la modification. Cisco peut modifier sa tarification si la composition du Réseau dépasse le prix de départ des Services.
- Créer et gérer un alias d'adresse électronique interne pour communiquer avec Cisco.
- Endosser la responsabilité globale de toute incidence des processus opérationnels et de toutes les applications de modification de processus.
- Fournir les politiques, conditions et environnements de travail en vigueur sur le site du Client.
- Mettre à disposition les accès ou agents de sécurité nécessaires pour accéder au site du Client.

- Le Client accepte de ne pas embaucher un employé actuel ou ancien de Cisco, qui participe à la prestation des Services en vertu de la présente description de service, pendant toute la durée du Service et pendant un (1) an après sa résiliation. Si le Client ne respecte pas cette obligation, il s'engage à payer à Cisco, à la date d'embauche de cet employé, des dommages-intérêts prédéterminés, et non une pénalité, équivalents à trois (3) fois le salaire annuel de cet employé. Si le paiement n'est pas effectué à cette date, le paiement des dommages-intérêts prédéterminés correspondra à six (6) fois la rémunération annuelle de cet employé.

En plus des Responsabilités générales, Cisco et le Client doivent respecter les obligations associées aux services de sécurité spécifiques d'intégration (CON-AS-SELA) et de conseil (CON-AS-SELAADV) décrits ci-dessous.

Détails des Services d'intégration spécifiques (CON-AS-SELA)

Cette section fournit les détails de service pour les services suivants :

- Assistance avancée dans le cadre des changements en matière de sécurité (Security Advanced CS)
- Assistance dans le cadre des changements en matière de sécurité (Security Advanced CS)
- Évaluation de conception de sécurité (SDA)
- Assistance dans le cadre du développement d'une conception de sécurité (Security DDS)
- Contrôle de l'intégrité de la sécurité (Security HC)
- Assistance pour la planification de la sécurité et la résolution des problèmes de sécurité (Security IRPS)
- Assistance pour la stimulation de la sécurité (SKSS)
- Assistance souple continue en matière de sécurité (Security OFS)
- Assistance en matière d'adaptation des performances de sécurité (Security PTS)
- Recommandations logicielles proactives pour la sécurité (Security PSR)
- Assistance de premier plan pour la réalisation de tests et la validation de la sécurité (Security VTPS)
- Alerte de sécurité logicielle (SSA)

Assistance avancée pour les modifications en matière de sécurité (**OPT-SOS-ACS**)

Responsabilités spécifiques de Cisco par rapport au Service

Dans le cadre du service d'assistance avancée pour les modifications en matière de sécurité, un expert-conseil en ingénierie de sécurité Cisco aide le Client dans la conception des plans (schémas du réseau; plans de mise en œuvre, de test et de restauration) et des modifications de configurations (configurations des périphériques et modifications du câblage).

Modifications urgentes. La capacité de Cisco à fournir son assistance dans le cadre d'une modification urgente dépend de la disponibilité de ses ressources. Cisco n'a aucunement l'obligation de fournir son assistance dans le cadre d'une modification urgente si elle est dans l'impossibilité d'affecter un expert-conseil en ingénierie de sécurité Cisco pour la tâche.

Modifications planifiées. Pour les modifications planifiées (programmées vingt et un (21) jours civils en avance), un expert-conseil en ingénierie de sécurité Cisco sera affecté par Cisco.

Au cours de la période de modifications, l'expert-conseil en ingénierie de sécurité Cisco observe, émet des idées et des commentaires et intervient directement lorsqu'il en a l'autorisation. Dans le cas d'une restauration, l'expert-conseil en ingénierie de sécurité Cisco prend en charge des activités de compte-rendu, les enseignements à tirer et la planification de la progression. L'expert-conseil en ingénierie de sécurité Cisco fournit son assistance dans le cadre des efforts post-modifications visant à valider la stabilité et la fonctionnalité opérationnelle. Autres responsabilités de Cisco :

- Planifier le développement des plans existants et passer ces derniers en revue (p. ex., schémas du réseau; plans de mise en œuvre, de test et de restauration).
- Communiquer des idées et faire des recommandations et des commentaires sur les plans.
- Planifier le développement des modifications et passer en revue les modifications planifiées (p. ex., configurations des périphériques, modifications du câblage).
- Fournir le Rapport sur les configurations des périphériques et le Plan de modifications.
- Période d'assistance dans le cadre des modifications (p. ex., assistance dépannage, assistance à la mise en œuvre, prise en charge des dossiers du TAC (centre d'assistance technique) ouverts et pertinents du Client).
- Assistance après la mise en œuvre des modifications (p. ex., assistance dépannage, évaluation des performances, efforts de stabilisation).

Limitations :

- Les modifications ne peuvent pas inclure plus de deux (2) périphériques de sécurité ou deux (2) paires de périphériques de sécurité (p. ex., paires de pare-feu actifs en veille).
- Les modifications ne peuvent pas inclure plus de dix (10) périphériques réseau.
- Cisco détermine le contenu et le format des produits livrables.
- La période d'assistance dans le cadre des modifications ne peut pas excéder huit (8) heures. Il ne peut pas y avoir plus de deux (2) périodes d'assistance pour les modifications. L'assistance en matière de modifications peut avoir lieu après les Heures d'ouverture standard.

Responsabilités spécifiques du Client par rapport au Service

Responsabilités du Client :

- Désigner une ou plusieurs personnes au sein de son service d'assistance technique pour servir de point de contact au spécialiste en ingénierie désigné par Cisco.
- Fournir aux personnes désignées des instructions sur la procédure et le processus pour collaborer avec le spécialiste en ingénierie désigné par Cisco.
- Fournir les renseignements suivants : le programme, les renseignements sur les périodes de modifications, le processus de contrôle des modifications, le processus de signalisation progressive, les procédures normales d'exploitation, la nomenclature pertinente et tout autre élément contraignant connu et pertinent.
- Soutenir le développement des plans de modifications et passer ces derniers en revue (p. ex., schémas du réseau; plans de mise en œuvre, de test et de restauration) avec le spécialiste en ingénierie désigné par Cisco.
- Fournir des recommandations et des commentaires sur les plans; approuver ou refuser explicitement les recommandations.
- Soutenir le développement des modifications planifiées et passer ces dernières en revue (p. ex., configurations des périphériques, modifications du câblage) avec le spécialiste en ingénierie de sécurité Cisco.
- Fournir des recommandations et des commentaires sur les modifications planifiées; approuver ou refuser explicitement les recommandations.
- Fournir des autorisations suffisantes à Cisco afin qu'elle puisse accéder aux périphériques Réseau et aux périphériques de sécurité du Client et apporter ainsi son aide.
- Le Client est responsable de la migration de tout contenu vers un de ses modèles ou de toute personnalisation.
- Le Client est responsable des formulaires et des documents qui lui sont propres, de ses processus internes; il assume les responsabilités de programmation, etc.
- Le Client est responsable de l'ouverture de tout dossier auprès du centre d'assistance technique du fournisseur (p. ex., le centre d'assistance technique de Cisco [Cisco TAC]) au cours de la période de modifications.
- Le Client est responsable des modifications apportées aux configurations des périphériques.

Assistance pour les modifications en matière de sécurité (**OPT-SOS-CS**)

Responsabilités spécifiques de Cisco par rapport au Service

Dans le cadre du service d'assistance pour les modifications en matière de sécurité (Security CS), Cisco met à disposition un spécialiste en ingénierie désigné par ses soins pendant les modifications programmées (planifiées ou urgentes) apportées au réseau ainsi qu'aux périphériques et aux politiques de sécurité pour les environnements de production.

Modifications urgentes. La capacité de Cisco à fournir son assistance dans le cadre d'une modification urgente dépend de la disponibilité de ses ressources. Cisco n'a aucunement l'obligation de fournir une assistance dans le cadre d'une modification urgente si elle est dans l'impossibilité d'affecter un spécialiste en ingénierie désigné par Cisco pour la tâche.

Modifications planifiées. Pour les modifications planifiées (programmées vingt et un (21) jours civils en avance), Cisco affectera un spécialiste en ingénierie qu'elle aura désigné.

Au cours de la période de modifications, le spécialiste en ingénierie désigné par Cisco observe la progression de l'exécution du plan, émet des recommandations et des commentaires (le cas échéant) et intervient directement lorsqu'il en a l'autorisation. Dans le cas d'une restauration, le spécialiste en ingénierie désigné par Cisco prend en charge des activités de compte-rendu, les enseignements à tirer et la planification de la progression. Le spécialiste en ingénierie désigné par Cisco prend en charge les efforts après mise en œuvre visant à vérifier la stabilité et la fonctionnalité opérationnelle. Les activités associées à ce service ne doivent pas excéder une période de sept (7) jours civils et incluent les suivantes :

- Étude des plans du Client (p. ex., schémas du réseau; plans de mise en œuvre, de test et de restauration).
- Recommandations et commentaires sur les plans du Client.
- Étude des modifications planifiées du Client (p. ex., configurations des périphériques, modifications du câblage).
- Recommandations et commentaires sur les modifications planifiées du Client.
- Assistance pendant la période de modifications (p. ex., assistance dépannage, assistance à la mise en œuvre, prise en charge des dossiers du TAC [centre d'assistance technique] ouverts et pertinents du Client).
- Assistance après la mise en œuvre (p. ex., assistance dépannage, évaluation des performances, efforts de stabilisation).

Assistance réactive : l'assistance dans le cadre des modifications en matière de sécurité est dédiée aux modifications planifiées. Cependant, les Clients peuvent utiliser et appliquer leur droit à ce service lors de situations réactives sans rapport avec les modifications planifiées. Dans ces cas, Cisco assure les tâches suivantes :

- effectue une évaluation technique du diagnostic initial du problème effectué par le TAC en se basant sur ses connaissances du réseau du Client,
- effectue une évaluation technique de la recommandation de modification non planifiée à apporter au réseau,
- fournit un représentant technique lors de conférences téléphoniques programmées régulièrement.

Dans le cadre des situations réactives (p. ex., panne de périphérique, du réseau), le Client peut utiliser le service d'assistance pour les modifications en matière de sécurité en tant qu'assistance de secours. Cependant, les conditions suivantes s'appliquent :

- Le Client doit ouvrir une demande de service auprès du centre d'assistance technique du fournisseur (p. ex. Cisco TAC [centre d'assistance technique]) avant de demander une assistance dans le cadre des modifications en matière de sécurité.
- Une (1) unité d'assistance en matière de modifications ne peut pas dépasser quarante (40) heures.
- Une (1) unité d'assistance en matière de modifications ne peut pas dépasser sept (7) jours civils.
- L'analyse de cause première est exclue explicitement; l'assistance pour la planification et la résolution des problèmes de sécurité offre une aide dans le cadre de l'analyse de la cause première.

Limitations :

- La période d'assistance dans le cadre des modifications ne peut pas excéder huit (8) heures. Il ne peut pas y avoir plus de deux (2) périodes d'assistance pour les modifications. L'assistance en matière de modifications peut avoir lieu après les Heures d'ouverture standard.

Responsabilités spécifiques du Client par rapport au Service

Responsabilités du Client :

- Désigner une ou plusieurs personnes au sein de son service d'assistance technique pour servir de point de contact au spécialiste en ingénierie désigné par Cisco.
- Fournir aux personnes désignées des instructions sur la procédure et le processus pour collaborer avec le spécialiste en ingénierie désigné par Cisco.
- Fournir les renseignements suivants : le programme, les renseignements sur les périodes de modifications, le processus de contrôle des modifications, le processus de signalisation progressive, les procédures normales d'exploitation, la nomenclature pertinente et tout autre élément contraignant connu et pertinent.
- Fournir et passer en revue les plans de modification du Client (p. ex., schémas du réseau; plans de mise en œuvre, de test et de restauration) avec le spécialiste en ingénierie de sécurité Cisco.
- Prendre en compte les recommandations et commentaires de Cisco sur les plans du Client; approuver ou refuser explicitement les recommandations.
- Indiquer les modifications planifiées du Client (p. ex., configurations des périphériques, modifications du câblage) au spécialiste en ingénierie de sécurité Cisco.
- Prendre en compte les recommandations et commentaires sur les modifications planifiées du Client; approuver ou refuser explicitement les recommandations.
- Fournir des autorisations suffisantes à Cisco afin qu'elle puisse accéder aux périphériques Réseau et aux périphériques de sécurité du Client et apporter ainsi son aide.
- Modifier les configurations des périphériques.

Dans le cadre de l'**assistance réactive** (p. ex., panne de périphérique, du réseau) sans rapport avec les modifications planifiées, les Clients peuvent utiliser leur droit à l'assistance pour les modifications en matière de sécurité pour demander une assistance. Dans ce cas, les responsabilités du Client incluent :

- l'ouverture d'une demande de service auprès du centre d'assistance technique du fournisseur (p. ex. Cisco TAC [centre d'assistance technique]) avant de requérir le droit à l'assistance réactive,
- la garantie que le spécialiste en ingénierie de sécurité Cisco a accès au dossier TAC et aux remarques, s'il ne s'agit pas du centre d'assistance technique de Cisco,
- la garantie que le spécialiste en ingénierie de sécurité Cisco est inclus dans tous les appels et discussions avec le centre d'assistance technique,
- l'étude de toute modification proposée avec le spécialiste en ingénierie de sécurité Cisco.

Évaluation de conception de sécurité (**OPT-SOS-SDA**)

Le Service d'évaluation de conception de sécurité évalue la capacité de l'infrastructure réseau à protéger les ressources stratégiques essentielles reconnues et à fournir un ensemble de recommandations permettant de résoudre ou d'atténuer les failles de sécurité détectées pour les ressources concernées. Les recommandations comprennent l'amélioration de la topologie, des protocoles, des configurations des périphériques et des contrôles de sécurité, et se limitent à une ressource stratégique ainsi qu'à l'échantillonnage de périphériques sur chacune des zones de réseau suivantes : centre de données, réseau interne et réseau périphérique.

Responsabilités spécifiques du Client par rapport au Service

Responsabilités du Client :

- Fournir aux ressources appropriées les connaissances et l'autorité dont elles ont besoin pour fournir les renseignements suivants à Cisco :
  - liste des principales ressources stratégiques;
  - évaluation des menaces propres aux ressources stratégiques reconnues;
  - schémas physiques et logiques de la topologie de réseau, comprenant notamment l'emplacement des périphériques inclus dans l'évaluation;
  - description de l'architecture réseau;
  - politiques, normes et procédures en matière de sécurité;
  - services passant par le réseau périphérique;
  - applications et services s'exécutant sur le réseau (VoIP, vidéo continue, émulation de terminal, http, ftp, etc.);
  - architecture globale du centre de données, des serveurs internes, de la connectivité de l'hôte de l'utilisateur et de la connectivité Internet;
  - architecture du système d'administration réseau;
  - données empiriques nécessaires pour créer les indicateurs du cadre de contrôle de sécurité de Cisco.

De plus amples renseignements sur l'évaluation de la conception de sécurité sont disponibles dans la Description de service propre à la SDA à l'adresse www.cisco.com/ca/aller/descriptionsduservice/, intégrée aux présentes par renvoi.

Assistance pour le développement d'une conception de sécurité (**OPT-SOS-DDS**)

Responsabilités spécifiques de Cisco par rapport au Service

Les responsabilités de Cisco dans le cadre de l'Assistance pour le développement d'une conception de sécurité sont limitées à un (1) ensemble de solutions complexes (p. ex., le système informatique unifié Cisco (ISE), le serveur ACS sécurisé de Cisco, des déploiements 802.1x) ou à un (1) ensemble de solutions non complexes intégrant jusqu'à quarante (40) périphériques et incluent les tâches suivantes :

- fournir un Questionnaire sur le développement d'une conception,
- créer le Document des exigences du Client ou aider le client à le créer, comme indiqué sur le Devis,
- passer en revue la documentation relative aux besoins du Client et valider à nouveau les exigences avec le Client,
- aider le Client à créer les documents sur les conceptions de base et détaillées.

Responsabilités spécifiques du Client par rapport au Service

Responsabilités du Client :

- Fournir un Questionnaire rempli sur le développement d'une conception, qui collecte des renseignements tels que les conceptions des infrastructures réseau et de sécurité existantes, les conceptions planifiées, les exigences de croissance plus approfondies et les exigences supplémentaires du client.
- Fournir le document de conception globale ou le document de conception détaillée qui décrit l'ensemble spécifique des besoins techniques et des objectifs de conception et indique les plans résultants de mise en place et de l'architecture réseau du client visant à répondre à ces besoins. Le niveau de détail doit être suffisant pour que ce document puisse faire l'objet d'un plan de mise en œuvre.
- Fournir ou extraire les renseignements supplémentaires nécessaires pour réaliser la conception (p. ex., caractéristiques du trafic planifié et actuel).
- Fournir la documentation des exigences commerciales et techniques pour la nouvelle conception.
- Veiller à ce que toutes ses parties prenantes assistent à la présentation interactive des recommandations pour le Document de conception faite par Cisco.
- Étudier et soumettre des commentaires et des demandes de révision dans les 10 jours ouvrables suivant la présentation interactive du Document de conception faite par Cisco.

Contrôle de l'intégrité de la sécurité (**OPT-SOS-HC**)

Responsabilités spécifiques de Cisco par rapport au Service

Cisco réalise un Contrôle de l'intégrité de la sécurité limité à un (1) ensemble de solutions ou à un (1) système complexe (p. ex., le système informatique unifié Cisco (ISE), le serveur ACS sécurisé de Cisco, des déploiements 802.1x) et jusqu'à vingt (20) périphériques. Les responsabilités seront les suivantes :

- Passer en revue le Questionnaire de demande de contrôle de l'intégrité de la sécurité du Client.

- Définir les besoins, les stratégies et les programmes de contrôle de l'intégrité avec le Client.
- Analyser les mises en œuvre des politiques et des configurations et harmoniser ces éléments avec les politiques et procédures de sécurité de l'entreprise ainsi que les pratiques exemplaires de Cisco.
- Analyser les périphériques de sécurité.
- Recommander des modifications d'adaptation à apporter aux configurations des périphériques et aux politiques.
- Recommander un examen de la conception ou de l'architecture, si nécessaire.
- Déterminer les capacités pertinentes sous-utilisées des produits et des solutions.
- Réaliser une transmission de connaissances informelle sur les capacités sous-utilisées pertinentes repérées (2 heures au maximum).
- Organiser une (1) session interactive d'adaptation avec le Client en vue de mettre en œuvre les recommandations d'adaptation.
- Fournir un Rapport sur le contrôle de l'intégrité de la sécurité.

Limitations :
- L'adaptation des performances peut avoir lieu après les Heures d'ouverture normales.

Responsabilités spécifiques du Client par rapport au Service

Responsabilités du Client :
- remplir le Questionnaire de demande de contrôle de l'intégrité de la sécurité,
- passer en revue le Questionnaire de demande de contrôle de l'intégrité de la sécurité rempli avec Cisco,
- définir les besoins, les stratégies et le programme de contrôle de l'intégrité avec Cisco,
- fournir un accès électronique aux périphériques afin de permettre à Cisco d'effectuer l'analyse et l'adaptation,
- passer en revue les recommandations de Cisco et autoriser leur adaptation,
- modifier la gestion et la programmation de l'adaptation des performances,
- aider lors de la session d'adaptation interactive avec Cisco pour mettre en œuvre les recommandations d'adaptation.

Assistance pour la planification de la sécurité et la résolution des problèmes de sécurité (OPT-SOS-ISUPP)

Responsabilités spécifiques de Cisco par rapport au Service

Cisco passe en revue les problèmes de sécurité, détermine la cause, teste et valide pour confirmer que les problèmes ont été identifiés et propose un plan visant à traiter ces problèmes. Responsabilités de Cisco :
- recueillir tous les renseignements pertinents concernant le problème,
- analyser les renseignements,
- passer en revue les besoins et les objectifs de sécurité des périphériques du Client,
- fournir une méthode cryptée et sécurisée permettant au Client de transmettre les politiques et les configurations des périphériques,
- effectuer une présentation interactive des résultats, des analyses et des recommandations.

Limitations :
En raison de la diversité des situations et des problèmes qu'il est possible de rencontrer dans les environnements de production, il peut s'avérer nécessaire de compléter ce service avec divers autres services. Par exemple :
- le service Security VTS ou Security VTPS peut être requis pour tester et confirmer les causes dans un environnement de laboratoire.
- Les problèmes liés à la conception peuvent nécessiter des services liés à la conception pour l'élaboration d'un plan viable.
- Le service Security IRPS fournit un aperçu des causes et un plan de résolution. Cependant, l'exécution du plan peut requérir des services de suivi.

Autres limitations possibles :
- Il n'est pas garanti que l'analyse de cause première permettra de déterminer ou de confirmer une cause première.
- Des efforts raisonnables seront déployés afin de fournir des résultats concluants et un plan de résolution des problèmes. Quoi qu'il en soit, le droit à un nombre approprié d'unités de services sera retiré. Par exemple, si aucun problème n'est trouvé au terme d'un effort raisonnable, incluant une recréation en laboratoire avec le service Security VTPS, pour déduire la cause première de la panne d'un (1) périphérique de sécurité, le droit à une (1) unité de service Security IRPS et à une (1) unité de service Security VTPS sera retiré.
- Il se peut que les services de Cisco doivent s'en remettre au service d'ingénierie de développement des produits.
- L'exécution des travaux peut avoir lieu en dehors des Heures de travail normales.

Chaque unité de service Security IRPS inclut :
- une (1) analyse de cause première, bien qu'il puisse y avoir plusieurs causes,
- jusqu'à six (6) périphériques réseau et/ou de sécurité,
- une limitation à 80 heures.

Responsabilités spécifiques du Client par rapport au Service

Responsabilités du Client :
- Fournir toutes les versions et configurations des périphériques grâce à une méthode cryptée et sécurisée.
- Veiller à ce que toutes les versions et configurations des périphériques soient exactes et à jour.
- Veiller à ce que toutes les parties prenantes concernées assistent à la présentation interactive des résultats, des analyses et des recommandations faite par Cisco.
- Désigner une ou plusieurs personnes au sein de son service d'assistance technique pour servir de point de contact au spécialiste en ingénierie désigné par Cisco.
- Fournir des autorisations suffisantes à Cisco afin qu'elle puisse accéder aux périphériques Réseau et aux périphériques de sécurité du Client et apporter ainsi son aide.
- Ouvrir des dossiers nécessaires auprès du centre d'assi stance technique du fournisseur (p. ex. centre d'assistance technique Cisco TAC (système informatique unifié)).

Assistance pour la stimulation de la sécurité (OPT-SOS-KICK)

L'assistance pour la stimulation commence généralement après la réalisation du Contrôle de l'intégrité de la sécurité, dans lequel Cisco a trouvé des capacités de solutions ou de produits qui peuvent être sous-utilisées par le Client. Cisco consulte le Client afin d'élaborer un plan et un programme pour la transmission à distance de connaissances relatives à la sécurité, de prise en charge et d'examen de la conception de sécurité, de prise en charge des changements relatifs à la sécurité et d'adaptation des performances de sécurité décrits plus loin dans cette Description de service.

Assistance souple continue en matière de sécurité (OPT-SOS-OFS)

Responsabilités spécifiques de Cisco par rapport au Service

Cisco offrira une assistance souple, informelle et continue pour des modifications progressives de l'architecture de sécurité des réseaux. L'assistance souple peut être appliquée à d'autres éléments de travail dans le cadre du Service d'optimisation de la sécurité, et une unité ne dépasse pas 40 heures de travail pour le spécialiste en ingénierie affecté. Les spécialistes en ingénierie de Cisco seront affectés à mesure que les éléments de travail seront sélectionnés pendant la durée du contrat de service.

Responsabilités spécifiques du Client par rapport au Service

Responsabilités du Client :
- Fournir à Cisco les détails sur le type d'assistance requis lorsqu'une demande est effectuée.

Assistance en matière d'adaptation des performances de sécurité (OPT-SOS-PTS)

Responsabilités spécifiques de Cisco par rapport au Service

Dans le cadre de l'assistance en matière d'adaptation des performances de sécurité, Cisco aura les responsabilités suivantes :
- rencontrer le Client afin de passer en revue le Questionnaire d'assistance en matière d'adaptation des performances de sécurité,
- rencontrer le Client pour établir les exigences, stratégies et plans d'adaptation des performances,
- analyser les mises en œuvre des politiques et des configurations et harmoniser ces éléments avec les politiques et procédures de sécurité de l'entreprise ainsi que les pratiques exemplaires de Cisco,
- analyser les périphériques de sécurité,
- recommander des modifications d'adaptation à apporter aux configurations des périphériques et aux politiques,
- recommander un examen de la conception ou de l'architecture, si nécessaire,
- organiser une (1) session interactive d'adaptation avec le Client pour mettre en œuvre les recommandations d'adaptation,
- fournir une synthèse informelle (courriel) des résultats clés, des recommandations d'adaptation et des adaptations réalisées, une unité supplémentaire d'assistance en matière d'adaptation des performances de sécurité sera facturée au Client si une documentation formelle est requise.

Limitations :
L'assistance en matière d'adaptation des performances de sécurité n'est pas destinée à des systèmes et solutions complexes comme :
- les environnements de système informatique unifié Cisco (ISE),
- les déploiements du serveur Cisco Secure Access Control (ACS),
- les périphériques réseau prenant en charge les déploiements complexes 802.1x.

Chaque unité d'assistance en matière d'adaptation des performances de sécurité comprend :
- jusqu'à un (1) ensemble de solutions (p. ex. une solution de pare-feu, une solution RPV, un système de prévention des intrusions) OU jusqu'à un (1) type de dispositif de sécurité (p. ex. un pare-feu prenant en charge un dispositif de sécurité multifonction, RPV et IPS).
- Pour les ensembles de solutions : jusqu'à cinq (5) périphériques avec un ensemble de solutions donné pour la première unité de service d'assistance en matière d'adaptation des performances de sécurité (Security PTS).
- Pour les ensembles de solutions : jusqu'à cinq (5) périphériques supplémentaires pour les unités de service Security PTS supplémentaires SI une nouvelle solution est ajoutée. Par exemple, si le service d'assistance en matière d'adaptation des performances de sécurité (Security PTS) inclut des solutions pare-feu et RPV, alors deux unités de service Security PTS prennent en charge jusqu'à (10) dispositifs de pare-feu et/ou RPV à analyser et à adapter.
- Pour les ensembles de solutions : jusqu'à quinze (15) appareils supplémentaires pour les unités de service Security PTS supplémentaires SI l'ensemble de solutions ne change pas. Par exemple, si le service Security PTS inclut une solution RPV, alors deux unités de service Security PTS prennent en charge jusqu'à (20) dispositifs RPV à analyser et à adapter.
- Pour le type de dispositif de sécurité : jusqu'à deux (2) dispositifs de sécurité.
- L'exécution des travaux peut avoir lieu en dehors des Heures de travail normales.

Responsabilités spécifiques du Client par rapport au Service
Le Client est tenu d'effectuer les tâches suivantes :
- remplir le Questionnaire d'assistance en matière d'adaptation des performances de sécurité,
- rencontrer Cisco afin de passer en revue le Formulaire de demande d'assistance en matière d'adaptation des performances de sécurité,
- rencontrer Cisco pour établir les exigences, stratégies et plans d'adaptation des performances,
- fournir un accès électronique aux périphériques afin de permettre à Cisco d'effectuer l'analyse et l'adaptation,
- passer en revue et autoriser les recommandations de Cisco pour l'adaptation,
- modifier la gestion et la programmation de l'adaptation des performances,
- aider lors de la session d'adaptation interactive avec Cisco pour mettre en œuvre les recommandations d'adaptation.

Recommandations logicielles proactives pour la sécurité (OPT-SOS-PSR)

Responsabilités spécifiques de Cisco par rapport au Service

Cisco fournira des recommandations logicielles préventives évaluant les diverses versions de Logiciel de sécurité par rapport aux bases de données de mises en garde internes de Cisco. Cisco est tenue d'effectuer les tâches suivantes :
- fournir le Questionnaire de recommandations logicielles préventives de sécurité,
- réunir les exigences communiquées par le Client en ce qui concerne les renseignements sur le logiciel de sécurité, les attributs, les fonctionnalités et la capacité,
- passer en revue les nouvelles fonctionnalités de Logiciel de sécurité demandées par le Client,
- documenter toutes les fonctionnalités à inclure dans la recommandation de logiciel de sécurité,
- évaluer l'interopérabilité entre les versions installées et les nouvelles versions de Logiciel ainsi que leur capacité de prendre en charge les besoins commerciaux et techniques actuels et futurs,
- fournir un rapport détaillé comprenant les risques connus qu'encourt le Client et, si possible, des solutions pour les contourner afin d'atteindre les objectifs commerciaux et techniques actuels et futurs.

Limitations :
Chaque unité de recommandation logicielle préventive de sécurité comprend :
- jusqu'à une (1) recommandation logicielle pour un (1) produit Cisco,
- jusqu'à trois (3) profils d'ensemble de fonctionnalités, basés sur cinq (5) exemples de configuration (au maximum) pour chaque profil, fournis par le client en tant que représentants des produits déployés.

Responsabilités spécifiques du Client par rapport au Service
Le Client est tenu d'effectuer les tâches suivantes :
- remplir le questionnaire de recommandations logicielles préventives de sécurité,
- fournir à Cisco des exemples de configurations du logiciel examiné,

- fournir à Cisco un schéma du réseau montrant les dispositifs et leur relation avec les autres équipements dans le réseau du client,
- fournir à Cisco une liste des nouvelles fonctionnalités qui doivent être prises en charge par le logiciel à réviser,
- passer en revue et accepter la liste de fonctionnalités à inclure dans la recommandation fournie par Cisco,
- passer en revue et approuver les résultats de la recommandation si celle-ci satisfait aux besoins du Client.

Assistance de premier plan pour la réalisation de tests et la validation de la sécurité (OPT-SOS-PVTS)

Responsabilités spécifiques de Cisco par rapport au Service

Cisco organisera une série de réunions au cours desquelles elle discutera avec le Client pour bien comprendre les besoins et objectifs du Client concernant les tests axés sur les solutions. Cisco testera le réseau et communiquera les résultats au Client. L'assistance peut comprendre, entre autres, les tâches suivantes :

- Fournir au Client le Questionnaire de demande d'assistance en matière de tests et de validation, ainsi qu'un exemple de rapport.
- Passer en revue les réponses au Questionnaire de demande d'assistance en matière de tests et de validation.
- Rencontrer le Client pour discuter des réponses au Questionnaire de demande d'assistance en matière de tests et de validation. Ces réponses peuvent inclure les objectifs, les exigences techniques et commerciales, les méthodes de test, ainsi que le format du document livrable standard de Cisco pour les tests et la validation.
- Créer et passer en revue le Plan de tests avec le Client.
- Indiquer au Client les exigences, notamment en ce qui concerne le laboratoire, l'équipement, le logiciel, le câblage et l'interface.
- Exécuter le Plan de tests une fois que le Client a approuvé le Calendrier de test et le plan en question.
- Analyser et rendre compte des résultats de test.
- Passer en revue le Rapport de validation et de test avec le Client.
- Passer en revue les commentaires du Client.
- Finaliser le Rapport de validation et de test et le soumettre au Client.
- Le cas échéant, fournir une assistance au niveau du laboratoire Cisco durant le test à distance. Par exemple, si un câble ou un connecteur est défaillant durant le test, Cisco est tenue de fournir un câble ou un connecteur de remplacement.
- Mettre à disposition le laboratoire, l'équipement, les logiciels, les câbles, les connecteurs, ainsi que les autres éléments nécessaires pour effectuer les tests.
  Préparer le laboratoire : effectuer l'installation de l'équipement dans le bâti ainsi que l'empilage, effectuer le câblage des connecteurs électriques et des connecteurs réseau, vérifier que l'équipement s'exécute automatiquement à sa mise sous tension, vérifier la version de logiciel et effectuer la configuration initiale des périphériques.

Pour fournir le service VTPS Sécurité, Cisco utilisera les services et équipements de laboratoire suivants :
- 320 à 400 heures d'expertise, assurée par un spécialiste en ingénierie de test;
- 80 heures consacrées à la gestion du programme;
- liste de matériel dont le montant est inférieur ou égal à 1,5 million de dollars sur la liste de prix générale (fournie).

Limitations :
Chaque unité d'assistance dédiée aux tests et à la validation de la sécurité inclut :
- jusqu'à deux (2) semaines pour l'élaboration des méthodes;
- jusqu'à deux (2) semaines pour l'élaboration du plan de tests;
- jusqu'à une (1) semaine durant laquelle Cisco aménagera le laboratoire de test sur son site;
- jusqu'à deux (2) semaines pour les tests de validation de la conception;
- jusqu'à une (1) semaine pour l'analyse des résultats.

La plupart des missions se dérouleront pendant une période de huit (8) à dix (10) semaines.

Responsabilités spécifiques du Client par rapport au service

Le Client est tenu d'effectuer les tâches suivantes :
- Répondre au Questionnaire de demande d'assistance en matière de tests et de validation. Les réponses peuvent comprendre les objectifs, les exigences techniques, commerciales et opérationnelles, les fonctionnalités requises, les schémas de réseau, le plan de tests souhaité et les critères de réussite, ainsi que les méthodes de test souhaitées.
- Au besoin, fournir les configurations des périphériques de production nécessaires à l'exécution des tests.
- Désigner un point de contact unique habilité à approuver les décisions.
- Offrir l'assistance nécessaire pour la prise en charge des produits tiers ou des produits des concurrents de Cisco.
- Expédier au laboratoire Cisco, l'équipement requis pour la prise en charge des produits tiers ou de ceux conçus par les concurrents de Cisco.

Alerte de sécurité des logiciels (**OPT-SOS-SA**)

Cisco fournira une analyse préventive des avis de sécurité (PSIRT) qu'elle génère lors de la détection de problèmes de sécurité pouvant influer sur les réseaux sur lesquels s'exécutent les produits Cisco. Par ailleurs, Cisco indiquera les actions nécessaires pour réparer le réseau et le protéger de ces problèmes. Après que Cisco a publié les avis de sécurité, l'évaluation est transmise au Client au moyen de l'alerte de sécurité logicielle (SSA). Cisco fournira une analyse de la vulnérabilité et de sa résolution en considérant les conséquences possibles sur les solutions de sécurité du Client.

- Analyse de la manière dont un avis de sécurité Cisco peut influer ou non sur le réseau le Réseau du Client.
- Recommandations destinées à atténuer les risques et
- la liste des périphériques réseau touchés ou risquant de l'être.

Responsabilités spécifiques du Client par rapport au service

Le Client est tenu d'effectuer les tâches suivantes :

- Mettre à la disposition de Cisco une personne-ressource désignée pour traiter toutes les annonces liées à la Sécurité.

Détails propres au service d'alerte (CON-AS-SELAADV)

Cette section fournit les détails de service pour les services suivants :

Service de conservation des réponses aux incidents (**OPT-SOS ADV-SELA IR**)

Responsabilités spécifiques de Cisco par rapport au Service

Cisco peut fournir une partie ou l'ensemble des éléments livrables associés à la Gestion des incidents (IR) dans le cadre du service de conservation : activités de préparation aux incidents, triage des incidents, évaluation et recommandation d'actions de confinement, offre d'assistance technique (p. ex. analyses et investigations) et gestion de projet/coordination des incidents, au besoin. Cisco effectuera un examen complet de la stratégie de Gestion des incidents du Client. Si ce dernier n'a mis en place aucune stratégie, Cisco tâchera de créer une stratégie de Gestion des incidents afin de permettre au Client de mieux répondre à chaque incident affectant la sécurité. La stratégie permettra éventuellement de déterminer la source de l'incident ou la vulnérabilité, de répondre efficacement à l'incident et d'atténuer les problèmes et dommages que ce dernier pourrait causer. Responsabilités de Cisco :

- Fournir l'accès aux services de Gestion des incidents pendant la période d'abonnement.
- Mettre à disposition une ressource de Gestion des incidents à distance par téléphone dans un délai de deux heures.
- Selon les besoins du Client, commencer le déploiement du personnel sur le site du Client dans un délai de 24 heures.

Limitations :
En raison de la diversité des situations et des problèmes pouvant se produire, la gestion des incidents peut nécessiter l'utilisation de différents services en compléments du présent service. Par exemple, les incidents peuvent nécessiter l'utilisation d'outils spécialisés pour améliorer la visibilité et l'accès au réseau.

Autres limitations possibles :

- Il n'est pas garanti que l'analyse de la cause première permettra de déterminer ou de confirmer la cause fondamentale d'un incident
- Des efforts raisonnables seront déployés afin de fournir des résultats concluants et un plan de résolution des problèmes.
- Les services de Gestion des incidents peuvent donner un aperçu des défaillances d'une stratégie de gestion des incidents et fournir un plan de résolution. Toutefois, l'exécution du plan peut nécessiter des services de suivi.
- L'exécution des travaux peut avoir lieu en dehors des Heures de travail normales.
- Toutes les heures non utilisées pendant la durée de l'abonnement au service de conservation seront irrécupérables.

Responsabilités spécifiques du Client par rapport au Service

Responsabilités du Client :

- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de l'entreprise.
- Fournir des autorisations suffisantes à Cisco afin qu'elle puisse accéder aux périphériques Réseau et aux périphériques de sécurité du Client et apporter ainsi son aide.
- Garantir l'accès aux renseignements sur la stratégie de gestion des incidents afin de mettre les processus, les flux de travail et l'historique des incidents à la disposition de Cisco.

Conseiller en matière de sécurité de l'entreprise (OPT-SOS ADV-SELA SAA)

Responsabilités spécifiques de Cisco par rapport au Service

Cisco fournira un Architecte de sécurité d'entreprise à temps partiel indépendant pour assister la stratégie et la planification de la sécurité du Client, afin de faciliter le déploiement et l'alignement des produits et des services de sécurité avec un programme de sécurité, de risques et de conformité accru du Client. Ce service est livré avec souplesse, comme convenu par les parties, avec l'intention de permettre au Client de mieux atteindre les objectifs commerciaux. La première livraison comprend 2 à 4 semaines pour passer en revue les initiatives, les projets en cours, les objectifs de sécurité, pour identifier les produits livrables initiaux et définir la cadence des réunions et des communications continues, comme convenu par les parties. Au fur et à mesure que l'environnement du Client évolue, l'Architecte de sécurité participera et assistera à l'évolution des programmes de sécurité, de risque et de conformité correspondants, qui peuvent inclure les principales activités suivantes :

- examiner et faciliter la cohérence des exigences commerciales avec les objectifs de sécurité, les politiques et les mises en œuvre de technologie;
- selon une cadence convenue par les parties, conduire régulièrement des réunions de planification et d'état afin de convenir des activités de mission, des produits livrables et des échéances;
- selon une cadence convenue par les parties, participer à des réunions régulières concernant la gamme des projets actifs/planifiés et des projets planifiés pour fournir des recommandations sur les besoins liés au calendrier, aux activités d'intégration, aux dépendances, aux politiques, aux processus et à la procédure;
- collaborer avec le Client et d'autres experts de Cisco pour soutenir la planification et la mise en œuvre de l'architecture de sécurité cible en vue d'atteindre les objectifs de sécurité;
- assurer une surveillance de la production de conception globale pour les technologies Cisco, en collaborant avec le Client ainsi qu'avec les équipes de Cisco et faciliter l'adaptation à l'architecture de sécurité d'entreprise du Client;
- examiner les conceptions détaillées pour l'alignement sur les conceptions globales convenues ainsi que les exigences relatives à l'architecture et à l'ingénierie des clients; comme requis et convenu, aider le Client avec la production d'exigences relatives à l'architecture et à l'ingénierie;
- assister le développement des politiques et des normes pour les programmes de sécurité, de risque et de conformité, au besoin, en vue de soutenir les améliorations opérationnelles et technologiques;
- aider le Client à créer des processus opérationnels pour une gestion appropriée des technologies mises en œuvre;
- assister et accompagner le Client avec les meilleures pratiques, les tendances du secteur, les matériaux de référence et l'expertise mise à disposition par Cisco;
- fournir des services à travers une combinaison de collaboration à distance et de collaboration sur site selon un calendrier convenu par les parties;
- soutenir les demandes ad hoc du Client concernant la structure de l'architecture de sécurité selon les calendriers convenus par les parties;
- fournir à l'architecte de sécurité et au Client de Cisco une assistance planifiée de la part d'un expert si nécessaire, comme convenu par les parties.

Responsabilités spécifiques du Client par rapport au Service

- Attribuer un commanditaire de projet ayant l'autorité de prendre des décisions relatives à l'exécution du projet.
- Attribuer un gestionnaire de projet du Client pour planifier les réunions des intervenants et pour répondre aux demandes de renseignements.
- Garantir un accès opportun aux personnes clés pour les entretiens et les questions techniques.
- Fournir un accès opportun à la documentation fournie, qui peut notamment inclure : les stratégies et objectifs commerciaux de l'entreprise; les stratégies, politiques et procédures informatiques et de sécurité existantes; tout renseignement pertinent sur les réglementations; les évaluations de sécurité et vérifications antérieures.
- Convenir avec Cisco d'un calendrier de réunions régulières ainsi que des objectifs, des produits livrables et des délais de la mission.
- Planifier des réunions comme convenu.
- Fournir des renseignements et des évaluations en temps opportun sur les produits livrables convenus.
- Communiquer les demandes ad hoc concernant les activités et les produits livrables en temps opportun. Le Client comprend et reconnaît que l'architecte attribué n'est pas une ressource dédiée. Les parties conviendront mutuellement des activités, du calendrier et des produits livrables ad hoc.