<<Service Description: Cisco Security Optimization Service>>
Description de service : Service d'optimisation de la sécurité Cisco

Ce document décrit le Service d'optimisation de la sécurité Cisco.

Documents connexes : Le présent document doit être lu conjointement avec les documents suivants, qui sont également publiés au www.cisco.com/ca/aller/descriptionsduservice : (1) Glossaire; (2) Liste des services non couverts, et (3) Directives de gravité Cisco. Tous les termes en majuscules figurant dans cette description ont le sens qui leur est attribué dans le Glossaire.

Vente directe par Cisco. Si vous avez souscrit ces Services directement auprès de Cisco, ce document est intégré à 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-cadre de services, la présente Description de service aura préséance.

Vente par un Revendeur agréé Cisco. Si vous avez souscrit ces services auprès d'un Revendeur agréé Cisco, le présent document n'a qu'un caractère informatif;il ne constitue pas un contrat entre vous et Cisco. Le contrat, le cas échéant, qui régit la prestation de ce Service est celui qui prévaut entre vous et votre Revendeur agréé Cisco. Votre Revendeur agréé Cisco doit vous fournir le présent document, ou vous pouvez également en obtenir une copie ainsi que d'autres descriptions des services proposés par Cisco à l'adresse www.cisco.com/ca/aller/descriptionsduservice/.

Résumé du Service

Le Service d'optimisation de la sécurité 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 tel qu'il est sélectionné et détaillé sur le Bon de commande pour lequel Cisco a reçu le paiement correspondant. Cisco fournira un Devis de service (« Devis ») identifiant les divers éléments du service avec les UGS correspondantes, comme indiqué à l'Annexe A, en établissant la portée des Services et la durée de prestation desdits Services 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 du présent 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 :

- Pour ce Service, et sauf indication contraire, Cisco devra fournir le Service d'optimisation de la sécurité au cours des Heures de travail 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 et politiques 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 Cisco des cartes d'identification qu'ils porteront en permanence pendant les activités relatives au Service 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 devra se conformer aux obligations suivantes relatives aux Services généraux pour tout Service d'optimisation de la sécurité spécifié 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 de sécurité 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 visés par la présente Description de service (par exemple, présider les conférences téléphoniques 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 devra maintenir une administration et une gestion de la sécurité centralisées de son Réseau pris en charge en vertu de la présente Description de service et être en mesure de fournir une Assistance de niveau 1 et une Assistance 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, s'il y a lieu, 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'examen.
- Si Cisco fournit des scripts 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 clé 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 assume l'entière responsabilité en cas d'endommagement de perte ou de vol des Outils de collecte de données lorsqu'ils sont en sa possession.
- Fournir une carte de topologie du 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 requis pour chaque service.
- Informer sans délai Cisco de toute modification substantielle apportée à la politique de sécurité (p. ex., modifications des règles de pare-feu, de la politique du système informatique unifié Cisco (ISE)) ou au Réseau (p. ex., topologie; configuration; nouvelles versions IOS; déplacements, ajouts, modifications et suppressions de périphériques).
- 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 à compter de la fin du Service. Si le Client ne respecte pas cette obligation, il s'engage à payer à Cisco, à la date d'embauche de cet employé, à titre de dommages-intérêts prédéterminés et non à titre de pénalité, un montant équivalent 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 d'intégration (CON-AS-SEC) et de conseils en matière de sécurité (CON-AS-SECADV) décrits ci-dessous.

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

Cette section fournit les détails des services d'intégration suivants :

- Évaluation de la sécurité des périphériques réseau (NDSA)
- Assistance avancée pour les modifications en matière de sécurité (Security Advanced CS)
- Assistance pour les modifications en matière de sécurité(Security CS)
- Service de simulation d'environnement de cyberdéfense (Security CR3)
- Service de simulation d'environnement de cyberdéfense (Security CR5)
- Assistance pour le développement d'une conception de sécurité(Security DDS)
- Assistance et analyse de la conception de sécurité (Security DRS)
- 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)
- Service de connaissances sur la sécurité (Security KS)
- Assistance et conseils en matière de réseau et de sécurité (Security NCS)
- 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)
- Transfert à distance des connaissances sur la sécurité (Security RKT)
- Assistance en matière de stratégie et de planification de la sécurité (SSPS)
- Évaluation de l'état de préparation des technologies de sécurité (STRA)
- Assistance de premier plan pour la réalisation de tests et la validation de la sécurité (Security VTPS)
- Assistance pour la réalisation de tests et la validation de la sécurité (Security VTS)
- Alerte de sécurité logicielle (SSA)

Évaluation de la sécurité des périphériques réseau

Responsabilités spécifiques de Cisco par rapport au Service

Cisco consultera le Client pour fournir une étude du service NDSA, répondre aux questions et mettre en place des attentes convenues mutuellement sur la portée de l'analyse et le niveau de l'échantillonnage des configurations des périphériques. L'Évaluation de lasécurité des périphériques Réseau peut inclure, entre autres, les tâches suivantes :

- Évaluer jusqu'à 350 configurations de périphériques Cisco. Il faut toutefois noter que seulement 10 de ces dispositifs périphériques peuvent être des pare-feu.
- Passer en revue les modèles de sécurité des périphériques du Client.
- Fournir une méthode cryptée permettant au client de transmettre les politiques et configurations des périphériques.
- Analyser les configurations des périphériques en se concentrant sur le renforcement de la sécurité des configurations de chaque périphérique.
- Analyser les règles de pare-feu relativement aux problèmes de configuration courants.
- Assurer la livraison cryptée et sécurisée du rapport d'analyse, qui inclut : l'évaluation des écarts entre les pratiques actuelles du Client et les meilleures pratiques recommandées par Cisco, et la liste hiérarchisée des vulnérabilités détectées et des résultats les plus importants.
- Effectuer une présentation interactive des résultats, des analyses et des recommandations.
- Supprimer, retirer et détruire les données du Client collectées (liste, politiques et configurations des périphériques) dans les référentiels de Cisco.
- Supprimer, retirer et détruire toutes les versions préliminaires du rapport d'évaluation.

Responsabilités spécifiques du Client par rapport au Service

Le Client accepte d'envoyer à la rencontre de Cisco des personnes possédant l'expertise et les connaissances appropriées sur les périphériques réseau. Ces personnes seront chargées d'indiquer les objectifs du Client et les résultats attendus en matière d'évaluation, et de communiquer les besoins techniques et commerciaux pertinents. Une fois que l'équipe spécialisée en évaluation a commencé l'analyse des configurations, les configurations et la liste des périphériques ne peuvent plus être modifiées. Le Client est tenu d'effectuer les tâches suivantes :

- Fournir la liste des périphériques (350 au maximum, dont 10 peuvent être des pare-feu) à inclure dans l'examen.
- 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 .
- Confirmer que les configurations soumises correspondent à sa liste de périphériques.
- Veiller à ce que toutes les parties prenantes concernées assistent à la présentation interactive des résultats, des analyses et des recommandations faite par Cisco.
- Étudier et soumettre les commentaires et demandes de modification dans les 10 jours ouvrables suivant la présentation interactive des résultats, des analyses et des recommandations menée par Cisco.
- Demander par écrit, par l'intermédiaire d'une personne autorisée, la destruction de l'examen finalisé figurant dans les référentiels de Cisco.

Assistance avancée pour les modifications en matière de sécurité

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 actif et en veille).
- Les modifications ne peuvent pas inclure plus de dix (10) périphériques réseau.
- Cisco détermine le contenu et le format des produits livrables.
- Une 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 de travail normales.

Responsabilités particulières du Client par rapport

au Service Responsabilités du Client :

- Désigner une ou des 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.
- Contribuer à l'élaboration et à des plans de modification 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 de sécurité 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 d'apporter les modifications aux configurations des périphériques.

Assistance pour les modifications en matière de sécurité

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 son 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 :

- Évaluation technique du diagnostic initial du problème effectué par le TAC en se basant sur ses connaissances du réseau du Client.
- Évaluation technique de la recommandation de modification non planifiée à apporter au réseau.
- Affectation d'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 la cause première est explicitement exclue; 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 :

- Une 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 de travail normale..

Responsabilités particulières du Client par rapport

au Service Responsabilités du Client :

- Désigner une ou des 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.

Pour une **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 :

- Ouvrir 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.
- Garantir que le spécialiste en ingénierie de sécurité Cisco a accès au dossier et aux remarques du centre d'assistance technique, s'il ne s'agit pas du centre d'assistance technique Cisco TAC.
- Garantir que le spécialiste en ingénierie de sécurité Cisco est inclus dans tous les appels et discussions avec le centre d'assistance technique.
- Étudier toute modification proposée avec le spécialiste en ingénierie de sécurité Cisco.

Service de simulation d'environnement de cyberdéfense à petite échelle

Responsabilités spécifiques de Cisco par rapport au Service

Dans le cadre du Service de simulation d'environnement de cyberdéfense, Cisco propose un atelier de formation technique spécialisée visant à aider le personnel de sécurité à acquérir les compétences et l'expérience nécessaires pour contrer les cybermenaces modernes. Les activités de Cisco peuvent comprendre les suivantes :

- Indiquer au Client les exigences de l'atelier.
- Indiquer au Client le programme de l'atelier.
- Organiser un atelier de simulation d'environnement de cyberdéfense.
- Effectuer l'atelier de simulation d'environnement de cyberdéfense par l'entremise d'un RPV à distance dans un environnement standard hébergé dans un laboratoire Cisco.
- Fournir aux participants à l'atelier un certificat de participation à l'atelier.
- Fournir aux participants à l'atelier un certificat d'exécution du service.

Limitations :

- Les ateliers sont limités à douze (12) participants.
- Les ateliers sont limités à trois (3) jours sur un site unique désigné du Client pendant les Heures de travail normales, à l'exclusion des jours fériés approuvés par Cisco, des jours fériés du pays reconnus au niveau local, des vacances et des jours de formation, ou si le Client et Cisco en conviennent, l'atelier peut être organisé sur un site désigné de Cisco.

Responsabilités particulières du Client par rapport au Service

Responsabilités du Client :

- Désigner un interlocuteur unique pour toutes les communications Cisco. Cette personne doit être habilitée à agir sur tous les aspects du service fourni.
- Désigner un deuxième interlocuteur en cas d'indisponibilité de l'interlocuteur du Client. Cette personne doit être habilitée à agir sur tous les aspects du service effectué en l'absence de l'interlocuteur principal.
- Fournir un accès raisonnable au site et aux installations du Client, y compris, le cas échéant, au matériel informatique, aux appareils de télécommunication, aux installations et à l'espace de travail. Le Client doit mettre à disposition les accès et agents de sécurité nécessaires pour accéder aux équipements, aux laboratoires, etc.
- Veiller à ce que les contrats établis avec ses propres fournisseurs, avec les utilisateurs finaux et avec les tierces parties soient entièrement exécutés et reflètent les modalités appropriées afin de permettre la prestation de service.
- Le Client est responsable de la gestion, de l'assistance et de l'orientation de la ressource fournie au Client par Cisco.
- Fournir à Cisco une connexion Internet pour accéder à l'environnement de l'atelier de simulation d'environnement de cyberdéfense hébergé dans un laboratoire Cisco si l'atelier a lieu sur le site du Client.
- Le Client confirme avoir rempli les exigences de l'atelier deux (2) semaines avant l'atelier.
- Fournir une liste comportant jusqu'à douze (12) noms de participants à l'atelier.
- Assister à l'atelier de simulation d'environnement de cyberdéfense aux moments prévus.

Service de simulation d'environnement de cyberdéfense à grande échelle

Responsabilités spécifiques de Cisco par rapport au Service

Dans le cadre du Service de simulation d'environnement de cyberdéfense, Cisco propose un atelier de formation technique spécialisée visant à aider le personnel de sécurité à acquérir les compétences et l'expérience nécessaires pour contrer les cybermenaces modernes. Les activités de Cisco peuvent comprendre les suivantes :

- Indiquer au Client les exigences de l'atelier.
- Indiquer au Client le programme de l'atelier.
- Organiser un atelier de simulation d'environnement de cyberdéfense.
- Effectuer l'atelier de simulation d'environnement de cyberdéfense par l'entremise d'un RPV à distance dans un environnement standard hébergé dans un laboratoire Cisco.
- Fournir aux participants à l'atelier un certificat de participation à l'atelier.
- Fournir aux participants à l'atelier un certificat d'exécution du service.

Limitations :

- Les ateliers sont limités à douze (12) participants.
- Les ateliers sont limités à cinq (5) jours sur un site unique désigné du Client pendant les Heures de travail normales, à l'exclusion des jours fériés approuvés par Cisco, des jours fériés du pays reconnus au niveau local, des vacances et des jours de formation, ou si le Client et Cisco en conviennent, l'atelier peut être organisé sur un site désigné de Cisco.

Responsabilités particulières du Client par rapport au Service

Responsabilités du Client :

- Désigner un interlocuteur unique pour toutes les communications Cisco. Cette personne doit être habilitée à agir sur tous les aspects du service fourni.
- Désigner un deuxième interlocuteur en cas d'indisponibilité de l'interlocuteur du Client. Cette personne doit être habilitée à agir sur tous les aspects du service effectué en l'absence de l'interlocuteur principal.
- Fournir un accès raisonnable au site et aux installations du Client, y compris, le cas échéant, au matériel informatique, aux appareils de télécommunication, aux installations et à l'espace de travail. Le Client doit mettre à disposition les accès et agents de sécurité nécessaires pour accéder aux équipements, aux laboratoires, etc.
- Veiller à ce que les contrats établis avec ses propres fournisseurs, avec les utilisateurs finaux et avec les tierces parties soient entièrement exécutés et reflètent les modalités appropriées afin de permettre la prestation de service.
- Le Client est responsable de la gestion, de l'assistance et de l'orientation de la ressource fournie au Client par Cisco.
- Fournir à Cisco une connexion Internet pour accéder à l'environnement de l'atelier de simulation d'environnement de cyberdéfense hébergé dans un laboratoire Cisco si l'atelier a lieu sur le site du Client.
- Le Client confirme avoir rempli les exigences de l'atelier deux (2) semaines avant l'atelier.
- Fournir une liste comportant jusqu'à douze (12) noms de participants à l'atelier.
- Assister à l'atelier de simulation d'environnement de cyberdéfense aux moments prévus.

Assistance pour le développement d'une conception de sécurité

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 exigences du Client et valider à nouveau les exigences auprès du Client.
- Aider le Client à créer le Document de conception de base ou le Document de conception détaillée.

Responsabilités particulières du Client par rapport

au Service Responsabilités du Client :

- Fournir un Questionnaire sur le développement d'une conception rempli, 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 de base ou le Document de conception détaillée qui décrit l'ensemble spécifique des exigences 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 exigences. Le niveau de détail doit être suffisant pour fournir des renseignements servant à la création 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.

Assistance et analyse de la conception de sécurité

Responsabilités spécifiques de Cisco par rapport au Service

Cisco consultera le Client dans le cadre d'une série de réunions à distance, offrant jusqu'à 40 heures d'assistance afin d'acquérir une connaissance approfondie des exigences du Client en matière de conception de sécurité et réalisera les activités suivantes :

- Examen des exigences, des priorités et des objectifs de conception du Client.
- Examen de la topologie et de l'architecture de sécurité.
- Traitement des questions liées à la conception.
- Analyse de l'incidence des nouvelles exigences sur le réseau existant.
- Examen de la conception, de la sélection et de la configuration des protocoles et soutien connexe.
- Examen de la conception, de la sélection et de la configuration des fonctionnalités et soutien connexe.
- Examen des considérations relatives à la sécurité des périphériques.
- Recommandations ou conseils informels sur une conception de sécurité.
- Aide apportée au Client pour résoudre les problèmes mineurs liés à la conception.

Responsabilités particulières du Client par rapport

au Service Responsabilités du Client :

- Fournir le document de conception de base qui décrit l'ensemble spécifique des exigences 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 exigences. Le niveau de détail doit être suffisant pour fournir des renseignements servant à la création d'un plan de mise en œuvre.
- Garantir que les parties prenantes et décideurs clés de la conception détaillée sont en mesure de participer à l'exécution du Service.
- 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.
- Fournir des renseignements sur toutes les caractéristiques ou contraintes du trafic planifié et actuel.

Contrôle de l'intégrité de la sécurité

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., lesystème 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, au besoin.
- 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).
- Mener une (1) séance 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 de travail normales.

Responsabilités particulières 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 et autoriser les recommandations de Cisco relatives à l'adaptation.
- Assurer la gestion du changement et la planification aux fins d'adaptation des performances.
- Participer à la séance interactive sur l'adaptation avec Cisco afin de mettre en œuvre les recommandations d'adaptation.

Assistance pour la planification de la sécurité et la résolution des problèmes de sécurité

Responsabilités spécifiques de Cisco par rapport au Service

Cisco passe en revue les problèmes de sécurité, en détermine la cause, effectue des tests et les 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 exigences et les objectifs du Client en matière de sécurité des périphériques.
- 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 :

Étant donné 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 prévoit :
- une (1) analyse de cause première, bien qu'il puisse y avoir plusieurs causes;
- jusqu'à six (6) périphériques réseau ou de sécurité;
- une limitation à 80 heures.

Responsabilités particulières 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 du Client 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'assistance technique du fournisseur (p. ex., centre d'assistance technique Cisco [système informatique unifié]).

Assistance pour la stimulation de la sécurité

L'assistance pour la stimulation commence généralement après la réalisation d'un contrôle de l'intégrité de la sécurité au cours duquel Cisco a trouvé des capacités de solutions ou de produits qui sont peut-être sous-utilisées par le Client. Cisco consulte le client afin d'élaborer un plan et un programme pour les Services de Transfert à distance des connaissances sur la sécurité, d'Assistance et analyse de la conception de sécurité, d'Assistance pour les modifications en matière de sécurité et d'Assistance en matière d'adaptation des performances de sécurité décrits plus amplement dans la présente Description de service.

Service de connaissances sur la sécurité

Responsabilités spécifiques de Cisco par rapport au Service

Cisco propose un service de connaissances sur la sécurité par l'intermédiaire d'un portail Web (« Portail »). En plus des services de connaissances sur les technologies et les produits de sécurité inclus dans le service, le Client obtient également l'accès au Service de connaissances modulaires sur l'infrastructure réseau sans frais supplémentaires. Responsabilités de Cisco :
- Créer le compte d'utilisateur du Client pour le Portail.
- Contribuer à ce que le Service de connaissances sur la sécurité soit opérationnel et garantir que la communauté d'utilisateurs obtiennent les autorisations et authentifications appropriées.
- Publier le contenu sur la sécurité pour les utilisateurs autorisés et enregistrés.
- Le contenu sur la sécurité peut inclure les documents suivants : documents techniques, documents de formation, études de cas, guides de conception, de configuration, de dépannage et de déploiement, manuels et livres en ligne.
- Archiver les produits livrables propres au Client lorsqu'ils sont fournis dans le cadre d'un contrat de souscription aux Services avancés.
- Mettre à jour le contenu sur la sécurité, car Cisco peut réviser, mettre à jour et supprimer du contenu ou des clips multimédias précédemment publiés.

Responsabilités particulières du Client par rapport

au Service Responsabilités du Client :
- Désigner des personnes responsables de la gestion des comptes du portail au sein de la communauté d'utilisateurs.
- Fournir la liste initiale des utilisateurs autorisés à accéder au portail.

Assistance et conseils en matière de réseau et de sécurité

Lorsque le Service d'assistance et de conseil pour le réseau est disponible, Cisco affectera un spécialiste en ingénierie (« Spécialiste en ingénierie des services avancé ») désigné pour jouer le rôle d'interface principale avec le Client. Il fournira des conseils généraux liés au Réseau du Client, des recommandations d'examen et des plans de correction, et ce, jusqu'à cinq jours par semaine (selon les restrictions locales relatives au travail), pendant les Heures de travail normales et à l'exclusion des jours fériés approuvés par Cisco, des jours fériés du pays reconnus au niveau local, des vacances et des jours de formation. Les tâches que le Client demande au Spécialiste en ingénierie des services avancés de réaliser sont sujettes à l'approbation de Cisco, mais elles ne seront pas refusées sans motif valable.

Responsabilités particulières du Client par rapport

au Service Responsabilités du Client :
- Donner des directives à Cisco à propos des activités et des projets sur lesquels le Client souhaite faire participer le spécialiste en ingénierie de Cisco.

Assistance souple continue en matière de sécurité

Cisco offrira une Assistance souple continue de manière informelle 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 particulières 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

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, les stratégies et le plan 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, au besoin.
- Mener une (1) séance interactive d'adaptation avec le Client en vue de 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 officielle 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., dispositif de sécurité multifonction prenant en charge un pare-feu, un RPV et un IPS).
- Pour les ensembles de solutions : jusqu'à cinq (5) dispositifs 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) dispositifs 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 de pare-feu et de RPV, alors deux unités de service Security PTS prennent en charge jusqu'à dix (10) dispositifs de pare-feu et RPV à analyser et à adapter.
- Pour les ensembles de solutions : jusqu'à quinze (15) dispositifs 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 les dispositifs de sécurité : jusqu'à deux (2) dispositifs de sécurité.
- L'exécution des travaux peut avoir lieu en dehors des Heures de travail normales.

Responsabilités particulières 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 relatives à l'adaptation.
- Assurer la gestion du changementet la planification aux fins d'adaptation des performances.
- Participer à la séance interactive sur l'adaptation avec Cisco afin de mettre en œuvre les recommandations d'adaptation.

Recommandations logicielles proactives pour la sécurité

Responsabilités spécifiques de Cisco par rapport au Service

Cisco fournira des recommandations logicielles proactives 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 proactives pour la sécurité.
- Réunir les renseignements communiqués par le Client en ce qui concerne le logiciel de sécurité et les exigences relatives aux attributs, aux fonctionnalités et à la capacité.
- Passer en revue les nouvelles fonctionnalités de Logiciel de sécurité demandées par le Client.
- Documenter toutes les fonctionnalités à inclure dans les recommandations relatives au 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 proactive pour la 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 qu'éléments représentatifs des produits déployés.

Responsabilités particulières du Client par rapport au Service

Le Client est tenu d'effectuer les tâches suivantes :

- Remplir le Questionnaire de recommandations logicielles proactives pour la 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 examiner.
- Passer en revue et accepter la liste des fonctionnalités à inclure dans la recommandation fournie par Cisco.
- Passer en revue les résultats de la recommandation et les approuver si cette dernière satisfait aux besoins du Client.

Transfert à distance des connaissances sur la sécurité

Responsabilités spécifiques de Cisco par rapport au Service

Cisco communiquera avec le Client afin de déterminer ses besoins et les thèmes à aborder au cours des sessions de formation informelles. Les séances de transfert des connaissances à distance :

- se déroulent en anglais (ou dans d'autres langues, selon les disponibilités);
- sont organisées à distance pour une durée de quatre (4) heures maximum, sans laboratoire ni supports de cours écrits;
- sont en rapport avec les produits et technologies Cisco déployés dans le Réseau de production du Client;
- consistent en des sessions de transfert de connaissances formelles centrées sur les pratiques exemplaires de fonctionnement, d'adaptation, de maintenance et de gestion des solutions de sécurité de Cisco;
- comportent des mises à jour techniques informelles sur un sujet convenu ensemble et pertinent par rapport aux technologies de la sécurité et
  - des présentations,
  - de l'observation et du mentorat, en fonction des besoins, pour aider votre personnel à assumer la responsabilité des solutions de sécurité Cisco;
- une consultation continue en vue de répondre à des questions, le cas échéant, dans les 30 jours suivant un déploiement.

Responsabilités particulières du Client par rapport au Service

Le Client est tenu d'effectuer les tâches suivantes :

- Fournir des détails sur les sujets souhaités/demandés que le client voudrait voir abordés lors des séances de transfert de connaissances et de mentorat.
- Fournir le contexte relatif à l'ensemble de compétences du Client participant en vue des séances de transfert de connaissances et de mentorat.
- Fournir des locaux et équipements (comme des salles de conférence, des tableaux blancs, des projecteurs) et les mettre à disposition pour les séances de mises à jour techniques informelles.

Assistance en matière de stratégie et de planification de la sécurité

Responsabilités spécifiques de Cisco par rapport au Service

Cisco fournira des conseils stratégiques et tactiques au cours d'une série de réunions et d'ateliers autour d'un sujet choisi par le Client se rapportant à la sécurité. Elle organisera ensuite un atelier de trois (3) jours (maximum) permettant de terminer le processus d'incubation et de stratégie couvrant des sujets qui peuvent inclure, sans s'y limiter, les technologies de sécurité, le nuage, TrustSec et l'identité, la gouvernance, la gestion des risques et la conformité (GRC) des TI, le télétravail, la gestion, les centres de données et la sécurité de la collaboration. Responsabilités de Cisco :

- Informer le Client sur le service et les options du service.
- Diriger un atelier de planification préalable pour le client.
- Diriger un atelier de planification pour le client.
- Résumer le contenu de l'atelier et les recommandations en découlant.
- Effectuer une analyse après l'atelier.
- Diriger une réunion de suivi à la suite de l'atelier.
- Résumer le contenu de la réunion suivant l'atelier et les recommandations finales en découlant.
- Établir une Synthèse du travail à soumettre au Client pour révision.

Limitations :

Chaque unité d'Assistance en matière de stratégie et de planification de la sécurité comprend :

- jusqu'à trois (3) domaines de difficultés majeures;
- jusqu'à trois (3) réunions ou une (1) journée entière de réunion préalable à l'atelier;
- jusqu'à trois (3) jours pour un atelier sur site, hors site ou par téléprésence;
- jusqu'à trois (3) réunions de suivi ou une (1) journée entière de réunion après l'atelier;
- jusqu'à quatre (4) participants Cisco simultanés.

Responsabilités particulières du Client par rapport

au Service Responsabilités du Client :

- S'assurer que toutes les parties prenantes principales participent à la séance d'information sur le service et les options du service organisée par Cisco;
- S'assurer que toutes les parties prenantes principales participent aux réunions et ateliers dirigés par Cisco.
- Se préparer pour l'atelier et fournir un résumé détaillé avec des faits à l'appui.
- Passer en revue et approuver la Révision de la Synthèse du travail.

Évaluation de l'état de préparation des technologies de sécurité

Responsabilités spécifiques de Cisco par rapport au Service

Cisco travaillera avec le Client pour définir les besoins commerciaux, techniques et opérationnels du Client, analyser les besoins de mise en œuvre d'une nouvelle solution de sécurité et évaluer l'état de préparation des périphériques, des opérations, des politiques de sécurité et de l'architecture du réseau du Client pour prendre en charge la solution.

- Fournir le questionnaire d'Évaluation de l'état de préparation des technologies de sécurité au moins sept (7) jours ouvrés avant l'atelier de conception.
- Mener l'atelier de conception afin de réviser le questionnaire d'Évaluation de l'état de préparation des technologies de sécurité.
- Analyser les besoins de mise en œuvre d'une nouvelle technologie de sécurité et évaluer l'état de préparation de l'infrastructure, des opérations, des politiques de sécurité et de l'architecture du Client aux fins de prise en charge de la solution.
- Établir le Rapport d'Évaluation de l'état de préparation de la sécurité pour documenter les résultats et recommandations, y compris les recommandations de modifications de l'infrastructure réseau et des paramètres de configuration pour les performances applicatives et la disponibilité.
- Organiser une réunion interactive avec le client afin de passer en revue tous les résultats et de mettre en place des procédures pour combler les écarts et s'assurer que l'environnement est prêt à prendre en charge la nouvelle technologie.

Limitations :

Chaque unité d'Évaluation de l'état de préparation des technologies de sécurité inclut :

- jusqu'à une (1) technologie de sécurité (c.-à-d., déploiements 802.1x, RPV à distance, AnyConnect, système informatique unifié Cisco [ISE]);
- jusqu'à deux (2) segments réseau avec un total de dix (10) classes de périphériques client (maximum). Une classe est définie comme un groupe de périphériques (notamment des pare-feu ou des routeurs) avec des configurations identiques.

Responsabilités particulières du Client par rapport au Service

Le Client est tenud'effectuer les tâches suivantes :

- Répondre au questionnaire d'Évaluation de l'état de préparation des technologies de sécurité (STRA) au moins deux (2) jours ouvrables avant l'atelier de conception.
- S'assurer que les spécialistes en ingénierie et les membres de l'équipe de direction appropriés du Client participent à l'atelier de conception.
- Participer activement à l'élaboration des étapes permettant de gérer les changements nécessaires pour garantir que le réseau peut prendre en charge les nouvelles technologies.

Assistance de premier plan pour la réalisation de tests et la validation de la sécurité

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 porter sur les objectifs, les exigences techniques, commerciales et opérationnelles, 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.
- Effectuer et documenter l'analyse 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 locale à partir 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 exécute un autotest au démarrage, vérifier la version du logiciel et effectuer la configuration initiale des périphériques.

Pour fournir le service Security VTPS, 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 pour la réalisation de tests et 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 et commerciales, 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.

Assistance pour la réalisation de tests et la validation de la sécurité

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 le Questionnaire de demande d'assistance en matière de tests et de validation rempli par le Client.
- Rencontrer le Client pour discuter des réponses au Questionnaire de demande d'assistance en matière de tests et de validation. Ces réponses peuvent porter sur les objectifs, les exigences techniques, commerciales et opérationnelles, 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.
- Effectuer et documenter l'analyse 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.

Limitations relatives au site du client

- Équipement fourni par le Client.
- Jusqu'à une (1) semaine pour la configuration des tests.
- Jusqu'à deux (2) semaines pour l'exécution des tests dans le laboratoire.
- 200 heures d'expertise, assurée par un spécialiste en ingénierie de test.
- 40 heures pour la gestion du programme.
- Tests et évaluations, le cas échéant.

Autres limitations possibles :

- L'assistance pour la validation et les tests de sécurité n'est pas offerte dans toutes les zones géographiques ou sur tous les sites.

Responsabilités particulières 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.
- Mettre à disposition le laboratoire, l'équipement, les logiciels, les câbles, les connecteurs, ainsi que les autres éléments nécessaires pour effectuer les tests.
- Au besoin, fournir les configurations des périphériques de production nécessaires à l'exécution des 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 exécute un autotest au démarrage, vérifier la version du logiciel et effectuer les configurations initiales des périphériques (notamment en cas de recréations de déploiement de production).
- Fournir une assistance locale, le cas échéant, au cours des tests sur site et à distance. Par exemple, si un câble ou un connecteur est défaillant durant le test, le client est tenu de fournir un câble ou un connecteur de remplacement.

Alerte de sécurité logicielle

Cisco fournira une analyse proactive 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 la solution 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.
- Liste des périphériques réseau touchés ou risquant de l'être.

Responsabilités particulières 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-SECADV)

Cette section fournit les détails des services d'alerte suivants :

- Service de conservation des réponses aux incidents
- Assistance souple continue en matière de sécurité
- Services de conseil en sécurité
  - Évaluation du programme de sécurité et feuille de route stratégique
  - Évaluation commerciale du système de contrôle et du programme de sécurité
  - Évaluation des architectures d'application
  - Évaluation des intrusions dans l'application
  - Amélioration SDLC
  - Évaluation de l'application mobile
  - Évaluation des architectures réseau
  - Test d'intrusion dans le réseau;
  - Évaluation de la sécurité des solutions sans fil
  - Évaluation de la sécurité physique
  - Piratage psychologique
  - Piratage électronique
  - Atelier sur la stratégie de sécurité mobile
  - Atelier sur la stratégie de sécurité en nuage
  - Service de contrôle de l'intégrité de la conformité du nuage
  - Évaluation de l'architecture infonuagique
  - Atelier sur les mesures de sécurité
  - Évaluation de tierces parties
  - Analyses de l'incidence sur la confidentialité
  - Augmentation du personnel d'assistance dans le cadre du programme portant sur les risques de sécurité et informatiques
    Développement d'un programme de sécurité de l'information
  - Développement d'un programme de gestion des risques liés à la sécurité de l'information
  - Évaluation des risques liés à la sécurité de l'information
  - Développement d'un programme sur les mesures de sécurité
  - Développement d'un programme de gestion des risques liés aux tierces parties
  - Évaluation de l'alignement de la structure sur la norme ISO 27001
  - Évaluation de l'alignement de la structure sur la norme ISO 27002
  - Évaluation de la conformité aux normes HIPAA et HITECH
  - Service d'analyse assurée par un fournisseur d'analyse agréé PCI
  - Évaluation de la conformité à la norme PCI-DSS
  - Conseiller en matière de sécurité de l'entreprise
  - Service de segmentation de la sécurité

De plus, comme condition à la prestation des Services de conseil suivants, le Client reconnaît, comprend et accepte ce qui suit :

- Le Client a autorisé Cisco à réaliser des tests sur le système dans le cadre de tests correspondants aux modalités de la présente Description de service. Cisco effectuera lesdits tests à sa discrétion au cours d'une période mutuellement convenue. Ces tests peuvent inclure des activités susceptibles d'être interprétées comme contraires à l'éthique et illégales dans un autre contexte. Le Client autorise par les présentes la réalisation desdits tests. Le choix revient au Client d'informer son fournisseur de services Internet (ISP), ou tout autre fournisseur de services concerné, de la réalisation des tests. Le Client accepte, par conséquent, d'endosser la responsabilité dans le cas où un fournisseur de services entrave d'une manière quelconque les résultats des tests ou même entraîne la suspension des tests. Cisco prendra toutes les précautions pour éviter d'endommager le système lors des tests, y compris les données qui y sont stockées. Cependant, le Client doit comprendre et accepter que des risques d'endommagement, quoique minimes, puissent survenir.

Service de conservation des réponses aux incidents

Le Service de conservation des réponses aux incidents de Cisco fournit l'examen et l'évaluation du programme de préparation aux incidents du Client.

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, stratégie et planification de gestion des incidents, exercices sur table, recherche proactive des menaces, et gestion d'urgence des incidents, qui peut inclure le tri, la coordination, l'enquête (p. ex. analyses et investigations), le confinement et la correction. Responsabilités de Cisco :

- Collaborer avec le Client pour définir comment exploiter les heures d'abonnement.
- Fournir un accès d'urgence 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 quatre (4) heures.
- Selon les besoins du Client, commencer le déploiement du personnel sur le site du Client dans un délai de 24 heures.
- Effectuer une mise à jour mensuelle de l'état de l'environnement du Client.

Limitations :
En raison de la diversité des situations et des problèmes pouvant se produire, la réponse aux 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 de ce 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.

Chaque unité de Service de sécurité de Gestion des incidents inclut :

- 160 heures, dont deux (2) déplacements avec huit (8) heures de voyage chacun.

Responsabilités particulières du Client par rapport au Service

Responsabilités du Client :

- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de la structure.
- 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 à Cisco l'accès aux renseignements sur la stratégie de gestion des incidents, y compris les processus et flux de travail.

Assistance souple continue en matière de sécurité

Cisco offrira une Assistance souple continue de manière informelle 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 particulières 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.

Services de conseil en sécurité

L'équipe de conseil en sécurité de Cisco offre une large gamme de services de conseils en sécurité, en gestion des risques et en conformité pour soutenir les opérations de grandes entreprises ou d'organismes publics en matière de sécurité.

Les Services d'évaluation des intrusions comprennent ce qui suit :

- Évaluation des intrusions dans l'application;
- Examen de l'application mobile;
- Test d'intrusion dans le réseau;

- Évaluation de la sécurité des solutions sans fil;
- Évaluation de la sécurité physique;
- Piratage psychologique;
- Piratage électronique;
- Évaluation des risques liés à la sécurité de l'information;
- Évaluation des risques liés à des tierces parties;

Les Services relatifs aux programmes et à l'architecture comprennent ce qui suit :

- Évaluation de l'alignement de la structure sur la norme ISO 27001/27002;
- Évaluation du programme de sécurité et feuille de route stratégique;
- Évaluation commerciale du système de contrôle et du programme de sécurité;
- Atelier sur les mesures de sécurité;
- Évaluation des architectures d'application;
- Évaluation de l'architecture infonuagique;
- Évaluation des architectures réseau;
- Atelier sur la stratégie de sécurité mobile;
- Atelier sur la stratégie de sécurité en nuage;
- Amélioration SDLC;
- Développement d'un programme de gestion des risques liés aux tierces parties;
- Analyses de l'incidence sur la confidentialité;
- Augmentation du personnel d'assistance dans le cadre du programme portant sur les risques de sécurité;
- Service de segmentation de la sécurité;
- Conseiller en matière de sécurité de l'entreprise;
- Développement d'un programme de sécurité de l'information;
- Développement d'un programme de gestion des risques liés à la sécurité de l'information;
- Développement d'un programme sur les mesures de sécurité

Les services d'évaluation de la conformité comprennent ce qui suit :

- Évaluation de la conformité aux normes HIPAA et HITECH;
- Service d'analyse assurée par un fournisseur d'analyse agréé PCI;
- Évaluation de la conformité à la norme PCI-DSS;
- Service de contrôle de l'intégrité de la conformité du nuage;

Les détails de ces services sont présentés ci-dessous.

Évaluation du programme de sécurité et feuille de route stratégique

Responsabilités spécifiques de Cisco par rapport au Service

Cisco collaborera avec le Client pour effectuer les activités suivantes dans le cadre du service d'Évaluation du programme de sécurité et de Feuille de route stratégique.

- Organiser un atelier ou des réunions interactives avec le Client pour examiner les documents et pour effectuer une inspection sous surveillance dans l'ensemble de l'entreprise.
- Collaborer avec le Client afin de déterminer les capacités liées à l'état actuel et celles liées à l'état futur en fonction des exigences commerciales.
- Créer une feuille de route détaillant les initiatives à prendre au fil du temps pour atteindre l'état souhaité.
- Créer un rapport d'Évaluation du programme de sécurité pour documenter les résultats et les recommandations.
- Fournir une Feuille de route stratégique sur les initiatives relatives à l'environnement d'entreprise du Client.
- Fournir une présentation récapitulative.

Responsabilités spécifiques du Client par rapport au service

- Fournir aux ressources appropriées les connaissances et l'autorité dont elles ont besoin pour collaborer avec Cisco pendant l'atelier d'évaluation.
- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de la structure.
- Fournir un accès électronique raisonnable à Cisco afin qu'elle puisse accéder aux périphériques réseau et aux périphériques de sécurité pendant les réunions entrant dans le cadre de l'atelier.

Évaluation commerciale du système de contrôle et du programme de sécurité

Responsabilités spécifiques de Cisco par rapport au Service

- Effectuer une évaluation et des examens de la conception du programme de sécurité d'une structure et des contrôles de prise en charge selon des domaines stratégiques d'analyse.
- Définir l'efficacité de la conception existante ainsi que l'état final requis.
- Proposer une recommandation de feuille de route pour permettre au Client d'atteindre l'état final visé.
- Créer un rapport d'Évaluation du système de contrôle et du programme de sécurité pour documenter les résultats et les recommandations.
- Fournir une présentation récapitulative.

Responsabilités spécifiques du Client par rapport au service

- Fournir aux ressources appropriées les connaissances et l'autorité dont elles ont besoin pour collaborer avec Cisco pendant l'atelier d'évaluation.
- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de la structure.
- Fournir un accès électronique raisonnable à Cisco afin qu'elle puisse accéder aux périphériques réseau et aux périphériques de sécurité pendant les réunions entrant dans le cadre de l'atelier.

Évaluation des architectures d'application

Cisco examinera la documentation sur l'application et effectuera des entretiens avec les experts de l'application pour déterminer de nouvelles méthodes de renforcement de l'application et de son infrastructure. Une seule application sera évaluée et fera l'objet d'un maximum de quarante (40) entrevues et de quatre-vingts (80) examens de la documentation.

Responsabilités spécifiques de Cisco par rapport au Service

- Passer en revue les exigences relatives à l'application avec les représentants commerciaux et techniques désignés du Client pour définir les motivations commerciales, les fonctionnalités du service et les domaines problématiques spécifiques relatifs à la sécurité.
- Évaluer l'architecture existante du Client avec les représentants commerciaux et techniques désignés du Client pour mieux comprendre les systèmes, les contrôles et les exigences.
- Analyser la conception de l'application existante en ce qui concerne les exigences et les pratiques relatives à la sécurité.
- Évaluer les domaines spécifiques de la conception par l'intermédiaire d'entretiens techniques, d'examens de la documentation, d'analyses des flux de données, de la modélisation des menaces et de la réalisation d'ateliers avec les parties prenantes commerciales et techniques.
- Déterminer la zone de stockage des données sensibles et la méthode d'accès à ces données.
- Déterminer les domaines potentiellement vulnérables relativement aux interfaces externes de l'application, à la communication des composants internes, au stockage des données et au traitement des transactions.
- Déterminer les vulnérabilités relatives à la sécurité et l'incidence associée aux scénarios d'exploitation le plus probable et le pire.
- Analyser les composants de l'architecture de sécurité existante de l'application, notamment :
    - Administration
    - Vérification et surveillance
    - Authentification et autorisation
    - Gestion de la configuration
    - Intégrité et confidentialité des renseignements (chiffrement, validation des données, protection des données statiques, protection des données en transit)
    - Journalisation et traitement des erreurs
    - Gestion de session
    - Dépendances des produits tiers
- Déterminer la meilleure approche pour évaluer les composants individuels de l'application en perturbant de manière minimale l'environnement de production, notamment dans les cas suivants :
    - Test d'intrusion
    - Analyse du code source
    - Examen de la configuration de l'application ou du système
- Documenter les recommandations d'amélioration de la sécurité de l'application dans le Rapport d'évaluation de l'architecture d'application qui comprend notamment :
    - Résumé
    - Portée et méthodologie
    - Analyse de l'architecture de sécurité de l'application
    - Schémas logiques architecturaux affichant les flux de données et les composants
    - Recommandations par priorité
    - Recommandations sur les prochaines étapes
- Fournir au Client le Rapport d'évaluation de l'architecture d'application pour examen et approbation.

Responsabilités spécifiques du Client par rapport au service

- S'assurer que le fournisseur de l'application, les architectes, les développeurs, le personnel de la sécurité, les tiers et le personnel des opérations informatiques collaborent au besoin avec Cisco pour la prestation des Services.
- Fournir à Cisco toute documentation existante, y compris les documents sur l'architecture et la conception, ainsi que les politiques et procédures.
- Examiner et approuver le Rapport d'évaluation de l'architecture d'application.

Évaluation des intrusions dans l'application

Cisco effectuera une Évaluation des intrusions dans l'application pour une seule application sur une plateforme donnée. L'évaluation commencera par la définition de la surface d'attaque directe au sein de l'application. La surface d'attaque sera analysée pour la détection de vulnérabilités grâce à des techniques de test manuelles et automatisées. Un code source peut être utilisé pour augmenter l'efficacité des tests. 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 conçu par le Client. Toutefois, les tests peuvent également mener à la découverte de vulnérabilités dans les dépendances directes de l'application. L'application doit comprendre au maximum 250 000 lignes de code. L'évaluation portera sur un maximum de soixante (60) entrées d'application (p. ex., les appels RPC, les demandes HTTP POST ou les messages de services Web traités par l'application) avec une moyenne de quinze (15) paramètres par entrée, pour un maximum de six (6) rôles d'utilisateur.

Responsabilités spécifiques de Cisco par rapport au Service

- Effectuer un examen 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 des scripts
  - 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
  - Failles relatives à la configuration
  - Failles de sécurité des communications
  - Problèmes applicables non mentionnés explicitement ci-dessus, mais couverts par les normes pertinentes (Top 10 de l'OWASP, Top 25 des erreurs de programmation les plus dangereuses selon l'institut SANS)
- Effectuer une analyse à l'aide d'une série de techniques conçues pour repérer les vulnérabilités présentant un risque pour la sécurité avec la méthode la plus efficace. 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 automatisée d'erreurs : envoi automatisé de données malveillantes pour repérer les vulnérabilités relatives à la sécurité sur le chemin de requête
  - Injection manuelle d'erreurs : envoi manuel de données malveillantes pour détecter 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
  - Compréhension du code : analyse manuelle du code source des chemins de code relatifs à la sécurité, si le code est disponible
  - 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, si le code est disponible
  - Corrélation de données (recherche des vulnérabilités, élimination des faux positifs, étude de la portée des résultats)
- Créer le Rapport combiné d'évaluation de l'application qui comprend les éléments suivants :
  - Résumé
  - Portée et approche
  - Liste détaillée des résultats
  - Détails sur les vulnérabilités découvertes (risques, indice de gravité, probabilité de l'attaque ou compétences requises)
  - Recommandations de correction
  - Analyse de l'incidence sur la sécurité
- Fournir au Client le Rapport d'évaluation de l'intrusion dans l'application pour examen et approbation.

Responsabilités spécifiques du Client par rapport au service

- S'assurer que les personnes clés se prêtent à des entretiens avec Cisco et participent à la résolution des problèmes et questions 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 tous les renseignements nécessaires pour accéder à l'application (p. ex., noms de domaine, URL, adresses IP).
- Fournir à Cisco tous les renseignements nécessaires pour l'exécution de toutes les fonctionnalités de l'application (p. ex., code exemple, documentation d'API).
- Convenir avec Cisco d'un créneau 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 à Cisco le code source de l'application, s'il y a lieu.
- Déterminer les modules cibles spécifiques et leur capacité, le cas échéant.
- Déterminer les modules cibles spécifiques et leur capacité, le cas échéant.
- Fournir un accès aux environnements de test et de production, le cas échéant.
- Prendre en charge tous les frais associés à l'augmentation de l'utilisation des ressources sur les systèmes tiers (p. ex., fournisseurs de nuage) nécessaires à la réalisation des tests.
- Informer toutes les tierces parties concernées et obtenir leur autorisation pour la réalisation des tests.
- Autoriser l'installation et l'utilisation des équipements et outils de Cisco dans l'environnement cible.
- Examiner et approuver le Rapport d'évaluation de l'application.

Amélioration SDLC

Cisco vérifiera le Cycle de vie de développement de logiciels (« SDLC ») pour déterminer les failles de sécurité dans le processus de développement. Une évaluation SDLC sécurisée comprend des entretiens, un examen des politiques et des normes de sécurité actuelles, et une analyse des pratiques actuelles. Selon les résultats, Cisco fournira des conseils pour l'élaboration de processus, de politiques et de normes de développement de logiciels et d'assurance de la qualité plus sécuritaires.

Responsabilités spécifiques de Cisco par rapport au Service

- Examiner les références existantes qui sont pertinentes dans le cadre du processus actuel du cycle de vie de développement de logiciels, notamment :
  - Normes d'encodage sécurisé
  - Politiques de classification des données
  - Procédures de test
  - Normes de formation
  - Exigences réglementaires et contractuelles relatives à la conformité
  - Documentation des normes de sécurité appliquées dans la structure
  - Toutes les mesures existantes utilisées pour évaluer les pratiques de sécurité dans la structure
  - Toute autre documentation connexe pertinente
- Interroger le personnel clé du Client, notamment :
  - Personnel de gestion disposant de compétences dans la gestion des pratiques de sécurité existantes
  - Personnel de développement
  - Personnel de tests
  - Personnel informatique
  - Personnel d'assistance
- Créer le Rapport d'évaluation du SDLC qui comprend les éléments suivants :
  - Résumé
  - Portée, description des tâches réalisées et méthodologie
  - Définition des lacunes et des correctifs recommandés relatifs à la gouvernance, aux pratiques opérationnelles et aux contrôles techniques
  - Recommandations sur les prochaines étapes
- Fournir au Client le Rapport d'évaluation du SDLC pour examen et approbation.

Responsabilités spécifiques du Client par rapport au service

- S'assurer que les personnes clés participent à des entretiens avec Cisco et à la résolution des problèmes techniques.
- Fournir à Cisco les schémas existants de développement de logiciels et toute documentation connexe, notamment :
  - Politiques et procédures de développement
  - Documentation de sensibilisation à la sécurité et de formation
  - Politique de sécurité de l'entreprise
  - Procédures et normes de tests
  - Documents spécifiques sur les exemples d'applications (documents UML, flux de données, schéma)
  - Normes de classification des données
  - Accès au répertoire de codes de l'application
- Examiner et approuver le Rapport d'évaluation du SDLC.

Évaluation de l'application mobile

Cisco effectuera une Évaluation de l'application mobile pour une seule application sur une plateforme donnée. L'Évaluation de l'application mobile commencera par la définition de la surface d'attaque directe de l'application. La surface d'attaque sera analysée à la recherche de 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 conçu par le Client. Toutefois, les tests peuvent également mener à la découverte de vulnérabilités dans les dépendances directes de l'application. L'application doit comprendre au maximum 250 000 lignes de code. L'évaluation portera sur un maximum de soixante (60) entrées d'application (p. ex., les appels RPC, les demandes HTTP POST ou les messages de services Web traités par l'application) avec une moyenne de quinze (15) paramètres par entrée, pour un maximum de trois (3) rôles d'utilisateur.

Responsabilités spécifiques de Cisco par rapport au Service

- Effectuer un examen afin de repérer les problèmes de sécurité pertinents, notamment les classes de vulnérabilités suivantes :
    - Vulnérabilités aux attaques par injection
    - Vulnérabilités aux attaques sur les éléments dynamiques (XSS) et autres vulnérabilités d'injection basées sur des scripts
    - 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
    - Utilisation de la mémoire locale non sécurisée
    - Utilisation insuffisante de la protection de couche de transport pour le trafic des données mobiles
    - Utilisation non sécurisée des interfaces de communication inter-processus
    - Vulnérabilités relatives au traitement général des données
    - Vulnérabilités de conception et de logique
    - Services inutiles
    - Interfaces de services pour mobile (p. ex. SMS)
    - Radiocommunication prise en charge (p. ex. Bluetooth)
    - Problèmes applicables non mentionnés explicitement ci-dessus, mais couverts par les normes pertinentes (Top 10 de l'OWASP, Top 25 des erreurs de programmation les plus dangereuses selon l'institut SANS)
- 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 (test à données aléatoires) : 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
    - Compréhension du code : analyse manuelle du code source des chemins de code relatifs à la sécurité
    - 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 la portée des résultats)
- Créer le Rapport d'évaluation de l'application mobile qui comprend les éléments suivants :
    - Résumé
    - Portée et approche
    - Liste détaillée des résultats
    - Détails sur les vulnérabilités découvertes (risques, indice de gravité, probabilité des attaques ou compétences requises)
    - Recommandations de correction
    - Analyse de l'incidence sur la sécurité
- Fournir au Client le Rapport d'évaluation de l'application mobile pour examen et approbation.

Responsabilités spécifiques du Client par rapport au service

- S'assurer que les personnes clés participent à des entretiens avec Cisco et 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 tous les renseignements nécessaires pour accéder à l'application et aux composants connexes (p. ex., services Web, noms de domaine, URL, adresses IP).
- Fournir à Cisco tous les renseignements nécessaires pour l'exécution de toutes les fonctionnalités de l'application (p. ex., code exemple, documentation d'API). Fournir un simulateur d'application mobile et les fichiers de projet pour dupliquer l'environnement d'exécution du développement.
- Fournir à Cisco un appareil cellulaire et les câbles de données pour la connexion à un PC ou un Mac, le cas échéant.
- Fournir une assistance dans la définition des spécifications de l'environnement en émulation et du paramétrage des tests par un accès direct (téléphone ou courriel) à un membre de l'équipe de développement du Client.
- 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 (comme un blocage de compte ou une erreur système).
- Fournir à Cisco le code source de l'application à évaluer, si celui-ci est disponible.
- Déterminer les modules cibles spécifiques et leur taille en nombre de lignes de code source, le cas échéant.
- Fournir les versions de débogage et de production du logiciel cible, le cas échéant.
- Fournir un accès aux environnements de test et de production.
- Informer toutes les tierces parties concernées et obtenir leur autorisation pour la réalisation des tests.
- Autoriser l'installation et l'utilisation des équipements et outils de Cisco dans l'environnement cible.
- Examiner et approuver le Rapport d'évaluation de l'application mobile.

Évaluation des architectures réseau

Cisco organisera une Évaluation des architectures de réseaux pour définir l'architecture de sécurité du réseau cible. L'Évaluation des architectures de réseaux examinera le réseau en fonction des exigences commerciales et techniques du Client. Cisco proposera des solutions pour éliminer les vulnérabilités de sécurité dans la conception et la mise en œuvre du réseau. Au maximum quarante (40) entretiens, quatre-vingts (80) révisions de documentation et vingt (20) révisions de fichiers de configuration seront exécutés pour l'évaluation d'un seul réseau.

Responsabilités spécifiques de Cisco par rapport au Service

- Passer en revue les exigences techniques du réseau, notamment les spécifications techniques, les documents de conception globale et les technologies exploitées.
- Passer en revue les exigences commerciales relatives au réseau avec les représentants commerciaux et techniques désignés pour définir les motivations commerciales, les fonctionnalités du service et les domaines problématiques spécifiques relatifs à la sécurité.
- Évaluer l'architecture avec les représentants commerciaux et techniques désignés pour mieux comprendre les systèmes, les contrôles et les exigences.
- Analyser la conception réseau en ce qui concerne les exigences et les pratiques relatives à la sécurité.
- Passer en revue la documentation pertinente, notamment les documents techniques de conception, les flux de traitement et l'architecture de sécurité pour définir les vulnérabilités potentielles.
- Effectuer des entretiens avec des experts.
- Effectuer une analyse d'un petit échantillon de fichiers de configuration représentatifs.
- Effectuer une analyse des failles au niveau des principaux composants du réseau sécurisé, notamment :
    - Gestion de l'identité et de l'accès (IAM)
    - Système de gestion des clés (KMS)
    - Authentification multifactorielle (MFA)
    - Accès à distance sécurisé (p. ex. RPV)
    - Contrôle d'accès réseau (NAC)
    - Configuration et dispositifs de sécurité sans fil (p. ex., système de prévention des intrusions dans le réseau sans fil WIPS)
    - Systèmes de détection des intrusions et de prévention des intrusions dans les réseaux (NIDS/NIPS)
    - Gestion des appareils mobiles (MDM)
    - Prévention de la fuite des données (DLP)
    - Passerelles de couche d'applications (ALG; p. ex., passerelles Web et de messagerie)
    - Protection des points d'extrémité
    - Gestion des événements de sécurité et d'information (SIEM)
    - Surveillance de l'intégrité des fichiers (FIM)
    - Surveillance de la disponibilité
    - Équilibrage de charge, haute disponibilité et virtualisation
    - Protection contre les attaques DDoS
    - Architecture DNS et NTP

    - Segmentation du réseau
    - Sauvegarde du système
    - Gestion des incidents
    - Inventaire du système
    - Provisionnement du système
    - Gestion des correctifs
    - Gestion de la configuration
    - Gestion du changement
    - Gestion des vulnérabilités
- Créer le Rapport d'évaluation des architectures de réseaux qui comprend les éléments suivants :
    - Résumé
    - Résumé de la gestion qui comprend les objectifs et les renseignements sur les processus
    - Évaluation des mesures de sécurité actuellement en place par rapport aux bonnes pratiques du secteur
    - Analyse de l'architecture de sécurité du réseau
    - Analyse des problèmes de sécurité détectés et de l'impact prévu sur l'entreprise (si possible), et recommandations en matière de mesures correctives
    - Liste hiérarchisée des recommandations
- Fournir au Client le Rapport d'évaluation des architectures de réseaux pour examen et approbation.

Responsabilités spécifiques du Client par rapport au service

- Fournir à Cisco l'accès à ses locaux pendant les Heures de travail normales, notamment les immeubles, parcs de stationnement, systèmes téléphoniques, systèmes d'accès à Internet, salles de serveurs et postes de travail.
- Fournir à Cisco l'accès à une salle de conférence pouvant accueillir les réunions, entretiens et présentations au cours des étapes sur site entrant dans le cadre de la mission.
- Fournir à Cisco une documentation précise et détaillée sur les exigences commerciales relatives aux réseaux, comme les motivations commerciales, les exigences de service, la détermination des préoccupations essentielles relatives au traitement et aux données et les procédures de déploiement.
- Fournir à Cisco une documentation précise et détaillée sur les exigences techniques relatives aux 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 à Cisco l'accès aux architectes de réseau, aux spécialistes en ingénierie, aux administrateurs et autres experts pour effectuer les entretiens et les ateliers.
- Fournir à Cisco les fichiers de configuration, l'inventaire du système, les politiques et les procédures.
- Examiner et approuver le Rapport d'évaluation des architectures de réseaux.

Test d'intrusion dans le réseau;

Cisco réalisera un Test interne ou externe d'intrusions dans les réseaux au niveau d'une instance de réseau du Client. Cisco réalisera un Test interne ou externe d'intrusions dans les réseaux au niveau d'une instance de réseau du Client. Le test visera à repérer les principales menaces, les vulnérabilités exploitables et à fournir la possibilité d'évaluer l'efficacité des investissements en matière de sécurité dans le cadre d'une attaque simulée. Les tests compteront jusqu'à 256 adresses IP externes ou 400 adresses IP internes.

Responsabilités spécifiques de Cisco par rapport au Service

- Effectuer une collecte de 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 :
    - Effectuer des analyses automatisées et manuelles
    - Utiliser, s'il y a lieu, des techniques de test à données aléatoires ou de rétro-ingénierie
    - Rechercher les menaces applicables aux logiciels et aux actifs de systèmes
    - Hiérarchiser les attaques en fonction des objectifs de l'analyse
- Effectuer les activités opérationnelles suivantes, 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 systèmes

    - 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
- Effectuer les activités post-opérationnelles suivantes, s'il y a lieu :
    - 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 nominatifs, numéros de carte de crédit)
    - Essayer de rediriger les attaques vers des cibles supplémentaires
    - Essayer d'extraire des données, selon les approbations du Client
- Fournir les rapports suivants :
    - Éliminer les faux positifs, si possible
    - Analyser l'impact possible sur l'entreprise
    - Étudier et élaborer des stratégies de correction
- Créer le Document de test d'intrusions dans le réseau qui comprend les éléments suivants :
    - Résumé
    - Portée et approche
    - Liste hiérarchisée des résultats
    - Détails sur les problèmes de sécurité découverts, notamment : risques, indice de gravité, probabilité des attaques ou compétences requises, recommandations de correction, analyse de l'incidence sur la sécurité
- Fournir au Client le Document de test d'intrusions dans le réseau pour examen et approbation.

Responsabilités spécifiques du Client par rapport au service

- Fournir à Cisco une documentation précise et détaillée sur les exigences techniques relatives aux 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 à Cisco un accès aux personnes clés pour les questions techniques.
- Indiquer une plage horaire à Cisco pour la réalisation du test.
- Fournir à Cisco des renseignements d'identification supplémentaires sur la cible (p. ex. : adresses IP, noms d'hôtes, URL).
- Autoriser l'installation et l'utilisation des équipements et outils de Cisco dans l'environnement cible
- Examiner et approuver le Document de test d'intrusions dans le réseau.

Évaluation de la sécurité des solutions sans fil

Cisco organisera une Évaluation de la sécurité des solutions sans fil pour un emplacement unique. Cisco énumérera au maximum 5 instances de réseau sans fil identifiées par SSID, et évaluera le déploiement de l'environnement sans fil pour déterminer les vulnérabilités. Les vulnérabilités de sécurité peuvent être démontrées en exploitant les vulnérabilités découvertes après l'approbation du Client.

Responsabilités spécifiques de Cisco par rapport au Service

- Effectuer une reconnaissance pour énumérer les points d'accès sans fil 802.11/b/g/n/ac de l'entreprise.
- Cisco essaiera dans la mesure du possible de recueillir les renseignements suivants pour les points d'accès détectés :
    - SSID
    - État de configuration de la diffusion SSID
    - Type d'authentification et de chiffrement
- Évaluer les risques associés aux périphériques sans fil en essayant de déterminer les éléments suivants :
    - les clients servant de passerelle entre les réseaux sans fil et le réseau de l'entreprise, si les identifiants sont fournis;
    - les clients sans fil qui se connectent généralement aux réseaux sans fil non sécurisés;
    - une configuration d'authentification faible (p. ex., validation de certificat désactivée).
- Évaluer le déploiement sans fil général, notamment :
    - Administration
    - Connectivité de réseau et segmentation
    - Configuration du point d'accès
    - Authentification et chiffrement
- Détecter et valider les vulnérabilités.
- Classer les vulnérabilités en fonction des risques associés.
- Créer le Rapport d'évaluation de la sécurité de la solution sans fil qui comprend les éléments suivants :
    - Résumé
    - Portée et approche
    - Liste hiérarchisée des résultats
    - Détails sur les problèmes de sécurité découverts, notamment : risques, indice de gravité, probabilité des attaques ou compétences requises, recommandations de correction, analyse de l'incidence sur la sécurité
- Fournir au Client le Rapport d'évaluation de la sécurité de la solution sans fil pour examen et approbation.

Responsabilités spécifiques du Client par rapport au service

- Fournir à Cisco l'accès à ses locaux pendant les Heures de travail normales, notamment les immeubles, parcs de stationnement, systèmes téléphoniques, systèmes d'accès à Internet, salles de serveurs et postes de travail.
- Fournir à Cisco l'accès à une salle de conférence pouvant accueillir les réunions, entretiens et présentations au cours des étapes sur site entrant dans le cadre de la mission.
- Fournir à Cisco une documentation précise et détaillée sur les exigences techniques relatives aux réseaux sans fil, notamment les caractéristiques techniques, les schémas de conception globale, les technologies utilisées, la documentation de conception et les schémas utilisés dans les études de cas.
- Garantir à Cisco un accès aux personnes clés pour les questions techniques.
- Indiquer une plage horaire à Cisco pour la réalisation du test.
- Fournir à Cisco les identifiants uniques des périphériques sans fil cibles.
- Fournir à Cisco l'autorisation d'exploiter les vulnérabilités détectées, s'il y a lieu.
- Autoriser l'installation et l'utilisation des équipements et outils de Cisco dans l'environnement cible.
- Examiner et approuver le Rapport d'évaluation de la solution sans fil.

Évaluation de la sécurité physique

Cisco procédera à une Évaluation de la sécurité physique d'une installation unique à faible sécurité. Une installation de faible sécurité ne comporte pas de sas de sécurité, de systèmes biométriques ni de gardes armés. Le principal objectif du test est d'obtenir l'accès aux matériels importants et aux zones sécurisées. Le test tentera d'exploiter les vulnérabilités des contrôles de sécurité physique pour fournir la possibilité d'évaluer l'efficacité des défenses de sécurité physiques et de renforcer les efforts de formation à la sensibilisation à la sécurité.

L'Évaluation de la sécurité physique sera effectuée sur site.

Responsabilités spécifiques de Cisco par rapport au Service

- *Collecte de renseignements et planification*
  - Utiliser les techniques de Renseignement de sources ouvertes (OSINT) pour obtenir des renseignements sur la cible physique et le personnel concerné.
  - Effectuer une étude de site relative au mécanisme et aux procédures de contrôle d'accès de l'emplacement.
  - Définir les défenses de sécurité à contourner.
  - Identifier les utilisateurs et administrateurs du système.
  - Élaborer un plan pour atteindre les objectifs de la mission.
  - Concevoir une trousse d'attaques physiques sur mesure à utiliser lors des phases opérationnelles et post-opérationnelles.

- *Exploitation*
  - Essayer de pénétrer dans le périmètre de chaque emplacement physique à l'aide de plusieurs techniques telles que :
    - Créer un faux identifiant et un faux objectif provisoire pour justifier la présence sur le site.
    - Essayer d'obtenir un accès physique aux installations ou zones données (p. ex., passage en double).
    - Créer de fausses cartes d'identification ou cartes professionnelles, s'il y a lieu.
    - Essayer d'obtenir un accès physique en s'attaquant aux systèmes de contrôle physiques (p. ex., crochetage de serrures, clonage de RFID).
    - Élaborer une infrastructure d'attaques pour surveiller les connexions à partir de périphériques infectés.
    - Intégrer des périphériques USB, CD et petits périphériques informatiques infectés dans des zones à trafic utilisateur élevé.
    - Surveiller les connexions des périphériques USB, CD et petits périphériques pendant la période de test.
    - Se faire passer pour les employés, les fournisseurs ou les clients du Client.
    - Essayer de convaincre le personnel de réaliser des tâches au nom du testeur (p. ex., ouvrir des portes et des serrures).
    - Essayer d'obtenir l'accès à des périphériques ou matériels définis par le Client.
    - Essayer de contourner les contrôles de sécurité physiques et d'en exploiter les faiblesses.
    - Essayer d'éviter les systèmes physiques de détection et de surveillance tels que les caméras et les alarmes de porte.

- *Postexploitation*
  - Essayer d'accéder aux autres emplacements à accès restreint.
  - Essayer d'obtenir un accès aux matériels sensibles.
  - Intégrer des périphériques non autorisés, comme des implants, des enregistreurs de frappe et des périphériques USB, si cela est pertinent.
  - Essayer d'extraire des matériels ou des équipements, selon les approbations du Client.
  - Documenter l'accès et le chemin d'accès aux objectifs définis.
  - Fournir au Client le Rapport d'évaluation de la sécurité physique pour examen et approbation.

Responsabilités spécifiques du Client par rapport au service

- Fournir les adresses de l'emplacement physique à tester.
- Fournir des instructions claires permettant d'atteindre et de repérer l'emplacement physique.
- Indiquer les zones sécurisées.
- Fournir une assistance pour obtenir l'accès à tous les emplacements physiques nécessaires pour commencer à réaliser les tests sur les emplacements physiques visés par le service.
- Fournir les détails sur tous les risques associés à chaque emplacement physique (p. ex., gardes armés ou risques sanitaires).
- Fournir une lettre autorisant les tests et pouvant être remise au personnel de sécurité.
- Indiquer les noms des consultants dans la lettre d'autorisation.
- Indiquer les équipements ou matériels pouvant être retirés du site dans la lettre d'autorisation.
- Intervenir rapidement si les autorités locales arrêtent le personnel de Cisco.
- Coordonner les activités de test entre toutes les parties prenantes et aviser ces dernières (p. ex., le gestionnaire des bâtiments et les agents de sécurité).
- Obtenir une autorisation de réalisation des tests auprès des propriétaires de l'immeuble si l'emplacement physique est partagé ou loué.
- Examiner et approuver le Rapport d'évaluation de la sécurité physique.

Piratage psychologique

Cisco effectuera un piratage psychologique vocal ou par messagerie pour le Client. Le piratage psychologique par messagerie portera sur un maximum de 500 adresses de courriel fournies par le Client ou de 30 adresses découvertes par Cisco, mais dans ce cas, les adresses de courriel agréées par le Client pourront être vulnérables aux attaques par hameçonnage Des tentatives de communication avec 15 employés au maximum seront effectuées pour le piratage psychologique vocal. Le principal objectif du test consiste à détecter les personnes nécessitant une formation supplémentaire de sensibilisation à la sécurité ou à mesurer de manière anonyme la réussite générale de la formation de sensibilisation à la sécurité (c.-à-d. Avec des résultats anonymes) Le test peut utiliser des mécanismes de communication tels que les courriels, la messagerie instantanée, le téléphone et la télécopie pour convaincre les personnes de compromettre la sécurité dans un environnement contrôlé.

L'Évaluation du piratage psychologique sera effectuée à distance, dans un ou plusieurs emplacements.

Responsabilités spécifiques de Cisco par rapport au Service

- *Piratage psychologique par message*
  - Fournir au Client les adresses IP source des serveurs de messagerie utilisés pour l'exécution de la campagne.
  - Détecter les utilisateurs à haut risque en utilisant les méthodes de renseignement de sources ouvertes (OSINT).
  - Élaborer jusqu'à quatre (4) campagnes d'hameçonnage visant à convaincre les utilisateurs cibles de :
    - Révéler les identifiants d'accès
    - Exécuter des tâches pour le compte du testeur
    - Accéder à des sites Web contrôlés par l'attaquant
    - Ouvrir des fichiers fournis par l'attaquant
  - Élaborer et personnaliser une infrastructure d'attaques, qui peut consister à :
    - Créer des sites Web personnalisés
    - Concevoir ou déployer des pseudo-logiciels malveillants, des commandes de système principal et des serveurs de contrôle
  - Réaliser une campagne d'hameçonnage qui peut inclure des communications contenant les éléments suivants :
    - des messages visant à convaincre les utilisateurs d'ouvrir des fichiers, de cliquer sur des liens ou d'effectuer des actions pour le compte du testeur;
    - des liens vers des sites Web contrôlés par les attaquants;
    - des pièces jointes ou des fichiers contenant des pseudo-logiciels malveillants;
    - des liens vers des sites Web imitant des sites Web d'entreprise pour collecter des identifiants;
    - des liens vers des formulaires Web qui demandent à l'utilisateur de soumettre des données sensibles;
    - des identités falsifiées de personnes de confiance.
  - Surveiller et enregistrer les réponses des utilisateurs.

- *Piratage psychologique vocal*
  - Détecter les numéros de téléphone ou périphériques vocaux à haut risque en utilisant les méthodes de renseignement de sources ouvertes (OSINT).
  - Essayer d'usurper l'identité des personnes de confiance du Client, notamment les clients, les employés ou les fournisseurs du Client.
  - Essayer de demander aux personnes de fournir des renseignements sensibles, comme :
    - les identifiants d'accès;
    - les renseignements confidentiels;
    - Les données financières;

    - les renseignements nominatifs des clients ou d'autres employés;
    - les renseignements sensibles définis par le Client.
- Essayer de convaincre le personnel d'effectuer des actions au nom de l'appelant.
- Documenter les tentatives de piratage psychologique réussies.
- Fournir au Client le Rapport sur le piratage psychologique pour examen et approbation.

Responsabilités spécifiques du Client par rapport au service

- *Piratage psychologique par messagerie*
    - Fournir une liste des noms et adresses de courriel cibles.
    - Approuver les adresses de courriel identifiées comme cibles lors de la collecte de renseignements.
    - Approuver les scénarios de piratage psychologique, s'il y a lieu.
    - Configurer les serveurs, les passerelles et les filtres de courriel pour accepter les courriels provenant du serveur de courriel de test de Cisco, quel que soit le taux de transmission ou le contenu.
    - S'assurer que les personnes qui ne doivent pas recevoir de courriels d'hameçonnage sont clairement identifiées.
    - Fournir des renseignements concernant les cibles ayant signalé des tentatives de piratage psychologique, au besoin.

- *Piratage psychologique vocal*
    - Fournir une liste des noms et numéros de téléphone cibles.
    - Approuver les numéros de téléphone identifiés comme cibles lors de la collecte de renseignements.
    - Approuver les scénarios de piratage psychologique, s'il y a lieu.
    - S'assurer que les personnes qui ne doivent pas recevoir d'appels téléphoniques sont clairement identifiées.
    - Fournir des renseignements concernant les cibles ayant signalé des tentatives de piratage psychologique, au besoin.
    - Évaluer et approuver le Rapport sur le piratage psychologique.

Piratage électronique

Cisco effectuera un test de Piratage électronique ciblé du Client. Le principal objectif du test est d'obtenir l'accès à des systèmes et données importants. Le test visera à essayer d'utiliser les fonctionnalités de surveillance et d'intervention et à fournir la possibilité d'évaluer l'efficacité des investissements en matière de sécurité dans le cadre d'une attaque simulée. La mission se limitera aux vecteurs d'attaque à distance (p. ex., les attaques directes contre les ordinateurs et les utilisateurs du Client exposés sur Internet).

Responsabilités spécifiques de Cisco par rapport au Service

- Effectuer une collecte de renseignements nécessaires, de la manière suivante :
    - Collecte de renseignements concernant les ressources électroniques; fouiller les entrepôts en ligne pour trouver les éléments suivants :
        - Les ressources en ligne associées à la structure, notamment, mais sans s'y limiter :
        - les blocs IP appartenant à l'entreprise ou dont elle est copropriétaire;
        - les références croisées entre les renseignements d'enregistrement ou de propriété et les biens connus;
        - l'identification des domaines et des sous-domaines;
        - l'identification des filiales;
        - Analyser le périmètre des services actifs
        - Identifier les systèmes d'exploitation utilisés, ainsi que les autres technologies
        - Repérer les défenses de sécurité à contourner
        - Identifier les technologies utilisées
        - Créer un aperçu de la surface d'attaque
    - Collecter des renseignements sur le personnel
        - Découvrir les adresses de courriel des employés librement accessibles en ligne
        - Recueillir les noms des employés sur les médias sociaux
        - Générer une base de données des courriels en fonction des renseignements collectés
- Réaliser la modélisation des menaces, la détection des vulnérabilités et l'analyse de la surface d'attaque comme suit :
    - Mener des activités d'exploitation sur des environnements vulnérables identifiés lors du profilage numérique ou tels que fournis pas le Client
    - Exploiter les failles de la conception et de l'architecture
    - 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
    - Tester les failles opérationnelles liées aux pratiques de gestion des correctifs, de gestion de la configuration et de déploiement de systèmes
    - 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

- Activités post-exploitation au sein des environnements exploités
    - Utiliser les têtes de pont mises en place au sein de la structure afin d'établir une menace persistante
    - Utiliser les têtes de pont mises en place au sein de la structure afin d'obtenir des droits d'accès supplémentaires
    - Effectuer une recherche de données sensibles et de renseignements d'identification (p. ex. : renseignements nominatifs, numéros de carte de crédit)

Responsabilités spécifiques du Client par rapport au service

- Garantir à Cisco un accès aux personnes clés pour les questions techniques.
- Garantir à Cisco l'accès à des personnes clés en cas de besoin, par exemple lors d'un comportement inattendu découlant de cette évaluation.
- Indiquer une plage horaire à Cisco pour la réalisation du test.
- Fournir à Cisco une approbation pour le test et l'analyse automatique des environnements dans le cadre de cette mission (effectuée à partir du profil numérique ou des renseignements fournis par le Client).
- Autoriser l'installation et l'utilisation des équipements et outils de Cisco dans l'environnement cible.
- Examiner et approuver le Document de piratage électronique.

Atelier sur la stratégie de sécurité mobile

Responsabilités spécifiques de Cisco par rapport au Service

- En se référant au Cadre de sécurité mobile de Cisco, organiser un seul atelier de plusieurs jours avec le Client pour définir les occasions commerciales de mobilité, pour le former sur la sécurité mobile et pour permettre une évaluation de la capacité actuelle afin de gérer de manière globale tous les aspects de la sécurité mobile.
- Concevoir une recommandation relative à l'état futur selon les priorités de l'entreprise.
- Créer une feuille de route sur les initiatives à prendre au fil du temps pour atteindre l'état souhaité.
- Créer un rapport sur la Stratégie de sécurité mobile pour documenter les résultats et les recommandations.
- Fournir une présentation récapitulative.

Responsabilités spécifiques du Client par rapport au service

- Fournir aux ressources appropriées les connaissances et l'autorité dont elles ont besoin pour collaborer avec Cisco pendant l'atelier d'évaluation.
- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de la structure.
- Fournir un accès électronique raisonnable à Cisco afin qu'elle puisse accéder aux périphériques réseau et aux périphériques de sécurité du Client pendant les réunions entrant dans le cadre de l'atelier.

Atelier sur la stratégie de sécurité en nuage

Responsabilités spécifiques de Cisco par rapport au Service

- En se référant au Cadre de sécurité en nuage de Cisco, organiser un seul atelier de plusieurs jours avec le Client pour le former sur la sécurité en nuage et pour permettre une évaluation de la capacité actuelle afin de gérer de manière globale tous les aspects de la sécurité en nuage.
- Concevoir une recommandation relative à l'état futur selon les priorités de l'entreprise.
- Créer une feuille de route sur les initiatives à prendre au fil du temps pour atteindre l'état souhaité.
- Créer un rapport sur la Stratégie de sécurité en nuage pour documenter les résultats et les recommandations.
- Fournir une présentation récapitulative.

Responsabilités spécifiques du Client par rapport au service

- Fournir aux ressources appropriées les connaissances et l'autorité dont elles ont besoin pour collaborer avec Cisco pendant l'atelier d'évaluation.
- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de la structure.
- Fournir un accès électronique raisonnable à Cisco afin qu'elle puisse accéder aux périphériques réseau et aux périphériques de sécurité du Client pendant les réunions entrant dans le cadre de l'atelier.

Service de contrôle de l'intégrité de la conformité du nuage

Responsabilités spécifiques de Cisco par rapport au Service

- En se référant à la norme du cadre de vérification de la conformité à la sécurité ou à une des exigences du client (comme PCI, HIPAA, etc.), examiner un environnement en nuage unique pour définir les problèmes ou les écarts de conformité éventuels.
- En se référant à la norme du cadre de conformité, les résultats seront mis en correspondance avec les exigences réglementaires et légales du Client relatives à la sécurité de l'information.
- Le délai de livraison standard correspond aux exigences en vigueur dans un pays. Si d'autres pays sont concernés, 24 heures seront ajoutées par pays.
- Créer un rapport sur l'Intégrité de la conformité du nuage pour documenter les résultats et les recommandations.
- Fournir une présentation récapitulative.

Responsabilités spécifiques du Client par rapport au service

- Fournir aux ressources appropriées les connaissances et l'autorité dont elles ont besoin pour collaborer avec Cisco pendant l'atelier d'évaluation.
- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de la structure.
- Fournir un accès électronique raisonnable à Cisco afin qu'elle puisse accéder aux périphériques réseau et aux périphériques de sécurité du Client pendant les réunions entrant dans le cadre de l'atelier.

Évaluation de l'architecture infonuagique

Responsabilités spécifiques de Cisco par rapport au Service

- Évaluer l'architecture de sécurité de l'un des environnements en nuage du Client grâce à des séances sur tableau blanc, à des entretiens ainsi qu'à des séances dédiées à l'examen des documents.
- Analyser les domaines comme la gestion des identités et des accès, l'autorisation, l'isolation, la connectivité de réseau, l'orchestration, la résilience, le chiffrement et la surveillance.
- Repérer et documenter les failles éventuelles dans l'architecture ou la conception.
- Créer un rapport d'Évaluation de l'architecture infonuagique pour documenter les résultats et les recommandations.
- Fournir une présentation récapitulative.

Responsabilités spécifiques du Client par rapport au service

- Fournir aux ressources appropriées les connaissances et l'autorité dont elles ont besoin pour collaborer avec Cisco pendant l'atelier d'évaluation.
- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de la structure.
- Fournir un accès électronique raisonnable à Cisco afin qu'elle puisse accéder aux périphériques réseau et aux périphériques de sécurité du Client pendant les réunions entrant dans le cadre de l'atelier.

Atelier sur les mesures de sécurité

Responsabilités spécifiques de Cisco par rapport au Service

- Effectuer un atelier avec le Client et définir les principales questions et mesures de sécurité qui doivent être traitées et signalées sur une base régulière.
- Élaborer un tableau de bord personnalisé sur les mesures qui sera utilisé dans les rapports réguliers sur les mesures visées.
- Proposer une recommandation sur la méthodologie de calcul, sur les seuils et sur les dépendances ainsi qu'une feuille de route relatives l'exploitabilité des mesures si les mesures recommandées ne peuvent pas être actuellement recueillies.
- Créer un rapport de l'Atelier sur les mesures de sécurité pour documenter les résultats et les recommandations.
- Fournir un exemple de tableau de bord.

Responsabilités spécifiques du Client par rapport au service

- Fournir aux ressources appropriées les connaissances et l'autorité dont elles ont besoin pour collaborer avec Cisco pendant l'atelier d'évaluation.
- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de la structure.
- Fournir un accès électronique raisonnable à Cisco afin qu'elle puisse accéder aux périphériques réseau et aux périphériques de sécurité du Client pendant les réunions entrant dans le cadre de l'atelier.

Évaluation de tierces parties

Responsabilités spécifiques de Cisco par rapport au Service

- Cisco évaluera le programme de sécurité du fournisseur du Client ou d'une tierce partie sélectionnée pour repérer les éventuelles failles de sécurité pouvant présenter des risques pour le Client.
- L'évaluation peut inclure une des activités suivantes :
    - Fournir une évaluation exhaustive sur site des risques d'un environnement de fournisseur tiers.
    - Effectuer deux opérations rapides de contrôle de conformité à la norme ISO 27002 sur les sites de différentes tierces parties.
    - Effectuer deux évaluations légères à distance des risques associés à deux tierces parties.
- Créer un rapport d'Évaluation de tierces parties pour documenter les résultats et les recommandations.

Responsabilités spécifiques du Client par rapport au service

- Obtenir les approbations et autorisations nécessaires pour permettre à Cisco d'effectuer une évaluation du fournisseur ou des tiers désignés.
- Fournir aux ressources appropriées les connaissances et l'autorité dont elles ont besoin pour collaborer avec Cisco pendant l'atelier d'évaluation.
- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de la structure.
- Fournir un accès électronique raisonnable à Cisco afin qu'elle puisse accéder aux périphériques réseau et aux périphériques de sécurité du Client pendant les réunions entrant dans le cadre de l'atelier.

Analyses de l'incidence sur la confidentialité

Responsabilités spécifiques de Cisco par rapport au Service

- En se référant à son Cadre de confidentialité, Cisco mènera un atelier de deux jours pour comprendre les exigences commerciales, les problèmes, les obligations et les éventuelles approches relatives à la conformité dans le traitement des Renseignements nominatifs dans le cadre d'une entreprise particulière ou d'une initiative technologique. Elle effectuera ensuite une évaluation des capacités actuelles.
- Définir un ensemble personnalisé d'exigences en matière de confidentialité et d'objectifs d'exploitabilité conformément aux exigences commerciales et aux obligations de confidentialité appropriées en vue de réaliser l'initiative commerciale cible.
- Créer une feuille de route pour la mise en œuvre des pratiques de gestion responsable des renseignements.
- Fournir des recommandations relatives au test de vérification de la conformité.
- Fournir un rapport et une présentation de synthèse de l'Analyse de l'incidence sur la confidentialité.

Responsabilités spécifiques du Client par rapport au service

- Fournir aux ressources appropriées les connaissances et l'autorité dont elles ont besoin pour collaborer avec Cisco pendant l'atelier d'évaluation.
- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de la structure.
- Fournir un accès électronique raisonnable à Cisco afin qu'elle puisse accéder aux périphériques réseau et aux périphériques de sécurité du Client pendant les réunions entrant dans le cadre de l'atelier.

Augmentation du personnel d'assistance dans le cadre du programme portant sur les risques de sécurité et informatiques

Responsabilités spécifiques de Cisco par rapport au Service

- Cisco doit assigner des responsables de la sécurité des renseignements (des conseillers principaux ou des responsables ou des responsables principaux) aux fonctions d'appui au personnel pour soutenir et diriger les programmes et les initiatives de sécurité du Client. La durée de ce service sera de 6 semaines.

Responsabilités spécifiques du Client par rapport au Service

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

Développement d'un programme de sécurité de l'information

Au cours de cette mission, Cisco procédera à une évaluation des processus et du programme d'évaluation des risques informatiques du Client afin d'identifier, le cas échéant, les domaines nécessitant l'amélioration ou l'optimisation des programmes.

Responsabilités spécifiques de Cisco par rapport au Service

- Déterminer le contexte des risques informatiques du Client, notamment les éléments suivants :
    a. Exigences externes
        - Collecter des renseignements auprès des représentants juridiques, de la gestion des risques et de la conformité du Client afin d'identifier les obligations externes concernant la gestion des risques informatiques.
    b. Exigences internes
        - Documenter les attentes et les facteurs de réussite du service informatique et des acteurs économiques concernant les risques informatiques.
        - Documenter les sentiments d'insatisfaction par rapport au processus actuel.
    c. Gestion des risques opérationnels
        - Acquérir une compréhension du rôle que les risques informatiques jouent dans le cadre des risques opérationnels de la structure et dans sa stratégie de gestion des risques.
    d. Organisation et culture au sein du service informatique
        - Interroger les parties prenantes et le personnel du service informatique afin d'identifier les facteurs culturels qui influencent l'identification des risques.
    e. Examiner l'approche, les activités et les commentaires actuels relatifs à l'évaluation des risques informatiques du Client et les comparer aux attentes.
    f. Examen des processus actuels liés aux risques informatiques
        - Examiner la structure organisationnelle, le nombre d'équipes et le champ de vision liés aux risques informatiques.
        - Examiner la documentation des processus.
        - Examiner l'utilisation de l'automatisation.

        - Étudier l'efficacité de l'exécution par la ou les personnes responsables.
        - Déterminer quels sont les apports et les perceptions des contributeurs en menant des entrevues.
        - Production de rapports et mesures
            - Examiner la production de rapports sur l'évaluation des risques informatiques.
            - Étudier les résultats exploitables et les réponses organisationnelles face aux conclusions de l'évaluation des risques informatiques.
- Documenter les conclusions et les recommandations détaillées dans le Rapport récapitulatif sur les découvertes et les recommandations.
- Organiser une présentation récapitulative des recommandations à l'équipe dirigeante du Client.

Responsabilités spécifiques du Client par rapport au Service

- Trouver un commanditaire de projet qui aura pour responsabilité de mener à bien le projet et aura le pouvoir de prendre les décisions relatives à l'exécution du projet.
- Désigner un chef de projet pour planifier les réunions des parties prenantes et pour répondre aux demandes de renseignements.
- Garantir un accès aux personnes clés pour les entrevues et les questions.
- Communiquer à Cisco les conclusions de toute évaluation récente des risques informatiques.
- Garantir à Cisco un accès à toutes les politiques relatives aux risques informatiques et à toute autre documentation opérationnelle utile concernant les risques informatiques.

Développement d'un programme de gestion des risques liés à la sécurité de l'information

Au cours de cette mission, Cisco procèdera à une évaluation des processus et du programme d'évaluation des risques informatiques du Client afin d'identifier, le cas échéant, les domaines nécessitant l'amélioration ou l'optimisation des programmes.

Responsabilités spécifiques de Cisco par rapport au Service

- Déterminer le contexte des risques informatiques du Client, notamment les éléments suivants :
    a. Exigences externes
        - Collecter des renseignements auprès des représentants juridiques, de la gestion des risques et de la conformité du Client afin d'identifier les obligations externes concernant la gestion des risques informatiques.
    b. Exigences internes
        - Documenter les attentes et les facteurs de réussite du service informatique et des acteurs économiques concernant les risques informatiques.
        - Documenter les sentiments d'insatisfaction par rapport au processus actuel.
    c. Gestion des risques opérationnels
        - Acquérir une compréhension du rôle que les risques informatiques jouent dans le cadre des risques opérationnels de la structure et dans sa stratégie de gestion des risques.
    d. Organisation et culture au sein du service informatique
        - Interroger les parties prenantes et le personnel du service informatique afin d'identifier les facteurs culturels qui influencent l'identification des risques.
    e. Examiner l'approche, les activités et les commentaires actuels relatifs à l'évaluation des risques informatiques du Client et les comparer aux attentes.
    f. Examen des processus actuels liés aux risques informatiques
        - Examiner la structure organisationnelle, le nombre d'équipes et le champ de vision liés aux risques informatiques.
        - Examiner la documentation des processus.
        - Examiner l'utilisation de l'automatisation.
        - Étudier l'efficacité de l'exécution par la ou les personnes responsables.
        - Déterminer quels sont les apports et les perceptions des contributeurs en menant des entrevues.
        - Production de rapports et mesures
            - Examiner la production de rapports sur l'évaluation des risques informatiques.
            - Étudier les résultats exploitables et les réponses organisationnelles face aux conclusions de l'évaluation des risques informatiques.
- Documenter les conclusions et les recommandations détaillées dans le Rapport récapitulatif sur les découvertes et les recommandations.
- Organiser une présentation récapitulative des recommandations à l'équipe dirigeante du Client.

Responsabilités spécifiques du Client par rapport au Service

- Trouver un commanditaire de projet qui aura pour responsabilité de mener à bien le projet et aura le pouvoir de prendre les décisions relatives à l'exécution du projet.
- Désigner un chef de projet pour planifier les réunions des parties prenantes et pour répondre aux demandes de renseignements.
- Garantir un accès aux personnes clés pour les entrevues et les questions.
- Communiquer à Cisco les conclusions de toute évaluation récente des risques informatiques.
- Garantir à Cisco un accès à toutes les politiques relatives aux risques informatiques et à toute autre documentation opérationnelle utile concernant les risques informatiques.

Évaluation des risques liés à la sécurité de l'information

Cisco procèdera à une Évaluation des risques de sécurité de l'information afin d'identifier, d'évaluer et de recommander l'atténuation des risques stratégiques et opérationnels liés à la sécurité qui peuvent toucher les activités du Client. L'évaluation des risques permettra d'examiner les stratégies commerciales et informatiques et de déterminer les risques de sécurité liés à l'information professionnelle qui menacent la réalisation des stratégies adoptées. L'évaluation visera à identifier les risques critiques par un mélange d'analyses stratégiques, d'examen des documentations, d'entrevues, d'observations du contrôle et d'évaluation simplifiée des risques. L'évaluation des risques permet d'apprécier les contrôles actuels des risques et de chercher à déterminer les risques résiduels. En fonction des priorités de l'entreprise et de la compréhension de la tolérance aux risques que Cisco a acquise au fil d'entrevues avec les cadres, Cisco établira un profil personnalisé des risques de sécurité de l'information et une feuille de route d'atténuation.

Responsabilités spécifiques de Cisco par rapport au Service

- Acquérir une compréhension du contexte commercial et personnaliser l'Évaluation des risques :
    a. Interroger les principales parties prenantes du service commercial et du service informatique pour mieux comprendre les stratégies et les objectifs commerciaux et technologiques, ainsi que les autres éléments clés dépendant du service informatique.
    b. Identifier les processus opérationnels critiques et les dépendances connues de leurs applications (cela s'applique uniquement aux analyses des processus opérationnels ou des ressources, c'est-à-dire uniquement aux évaluations approfondies des risques.)
    c. Examiner les processus de contrôle des risques et de gouvernance au niveau des entités.
    d. Formaliser et accepter le niveau de tolérance aux risques de sécurité de l'information et les critères pertinents d'évaluation des risques commerciaux.
- Analyser les tendances stratégiques clés; l'analyse stratégique prendra en considération :
    a. les stratégies commerciales, les attentes du client et les tendances du secteur identifiées par les parties prenantes;
    b. les stratégies technologiques pertinentes;
    c. les tendances en matière de réglementation et de législation;
    d. les tendances pertinentes en matière de sécurité de l'information et de menaces externes.
- Examiner et essayer d'identifier les risques de sécurité de l'information dans les processus opérationnels et les processus relatifs à l'architecture, à l'infrastructure et aux opérations informatiques qui prennent en charge des ressources informatiques critiques. Cela comprend l'identification des risques potentiels et l'examen des contrôles actuels, grâce à :
    a. l'examen des conclusions des évaluations des risques de sécurité de l'information précédemment effectué;
    b. l'examen des politiques, des normes et des procédures disponibles et relatives à la sécurité de l'information;
    c. l'examen de la documentation pertinente sur les processus opérationnels, notamment ceux qui ont trait à l'informatique;
    d. l'animation d'ateliers en groupe sur l'évaluation des risques avec un sous-groupe de parties prenantes pour mettre en évidence et pour évaluer les risques en fonction de connaissances institutionnelles informelles;
    e. des entrevues avec les principales parties prenantes et des experts;
    f. l'examen de l'architecture et de la documentation de soutien;
    g. l'analyse des résultats des vérifications antérieures;
    h. l'examen des sources de risques disponibles, telles que les rapports de gestion des problèmes et des incidents et les mesures de rendement du service informatique.
    i. Les domaines d'analyse peuvent inclure, le cas échéant :
        a) la gouvernance et la supervision de la sécurité de l'information;
        b) les politiques, normes et procédures de sécurité de l'information;
        c) la classification et la gestion des renseignements;
        d) les processus de conformité;
        e) l'évaluation et la gestion des risques;
        f) l'architecture de sécurité d'entreprise;
        g) la gestion du rendement et des mesures de la sécurité;
        h) la sensibilisation et la formation;
        i) la gestion de la vulnérabilité, des correctifs, du changement et des ressources;
        j) la surveillance de la sécurité;
        k) la gestion des incidents;
        l) l'acquisition, le développement et la maintenance des logiciels;
        m) la reprise après sinistre et la résilience du système;
        n) la gestion des risques liés à des tiers;
        o) la gestion de l'identité et de l'accès;
        p) la sécurité des ressources humaines;
        q) la sécurité environnementale et physique;
        r) La sécurité du réseau;
        s) la sécurité du système;

t) le chiffrage et la sécurité des données;
u) La sécurité des supports et appareils mobiles;
v) la protection contre les codes malveillants.

- Évaluer les risques : La sécurité du réseau;
  a. regrouper et analyser les risques potentiels en fonction du type d'incidence;
  b. évaluer les risques identifiés; les classer selon la probabilité qu'ils se concrétisent et selon leur incidence potentielle, le cas échéant;
  c. examiner les risques évalués par rapport aux critères personnalisés de notation des risques afin de les classer par ordre de priorité et d'identifier ceux qui nécessitent une intervention.
- Établir une feuille de route d'atténuation comprenant :
  a. les recommandations liées au traitement des risques;
  b. des améliorations recommandées qui établissent les initiatives dans un délai prédéterminé.
- Fournir au Client le Rapport d'évaluation des risques de sécurité de l'information.

Responsabilités spécifiques du Client par rapport au Service

- Trouver un commanditaire de projet qui aura pour responsabilité de mener à bien le projet et aura le pouvoir de prendre les décisions relatives à l'exécution du projet.
- Désigner un chef de projet pour planifier les réunions des parties prenantes et pour répondre aux demandes de renseignements.
- S'assurer que les parties prenantes des services commerciaux et informatique participent à l'examen et à l'approbation des produits de travail et des produits livrables du projet.
- Fournir la documentation demandée notamment, sans s'y limiter, les politiques, les normes et les procédures de gestion des risques et de sécurité de l'information, la documentation sur les processus opérationnels et informatiques, les plans de reprise après sinistre et de gestion des incidents, les configurations du système et de l'infrastructure, les contrats avec des tierces parties et les rapports de gestion.
- Fournir aux membres de l'équipe de Cisco un accès aux cartes d'identification et aux bâtiments appropriés, à un espace de travail et à une salle de réunion, ainsi qu'au téléphone et au réseau local.

Développement d'un programme sur les mesures de sécurité

Cisco aidera le Client dans l'élaboration d'un programme complet sur les mesures de la sécurité, comprenant l'analyse et la création d'un catalogue initial des mesures relatives à la sécurité selon les besoins et les exigences du Client.

Cisco utilisera les normes reconnues pour les mesures de la sécurité, notamment la norme ISO 27004 : Technologies de l'information – Techniques de sécurité –Gestion de la sécurité de l'information –Mesures. Cisco utilise des approches combinées pour assurer le Développement d'un programme sur les mesures de sécurité, notamment des ateliers de formation, des séances de travail individuelles ou de groupe, et un examen des objets. Les produits livrables qui en découlent comprendront des recommandations d'amélioration stratégiques et tactiques du programme de mesure, ainsi que des mesures spécifiques développées tout au long de la livraison.

Responsabilités spécifiques de Cisco par rapport au Service

- Examiner la maturité du Programme existant de mesure de la sécurité de l'information et du service informatique du Client.
- Animer des ateliers d'introduction aux mesures de la sécurité avec des ressources commerciales et techniques qui :
  a) fourniront un aperçu des mesures utilisées dans le secteur;
  b) fourniront un aperçu des applications spécifiques de mesure de la sécurité de l'information et de la sécurité informatique;
  c) fourniront un aperçu de la norme ISO 27004 et des autres normes et cadres appropriés de mesure de la sécurité;
  d) expliqueront la méthodologie Goal-Question-Metric ou GQM (approche par les buts);
  e) aborderont des exemples et des études de cas spécifiques à la mesure de la sécurité.
- Analyser les résultats des ateliers et leur applicabilité à l'ensemble de l'engagement.
- Évaluer et examiner les fonctionnalités, la maturité et les processus du programme de mesure de la sécurité existant.
  a) Interroger les parties prenantes.
  b) Examiner la documentation et les objets du programme.
  c) Comparer le programme existant aux recommandations et exigences de la norme ISO 27004 et des autres cadres de mesure.
  d) Communiquer les résultats initiaux aux parties prenantes du Client.
- Animer des ateliers GQM avec les ressources commerciales et techniques afin d'élaborer et d'améliorer le catalogue de mesures du Client.
  a) Fournir une formation détaillée sur la méthodologie GQM.
  b) Utiliser les techniques GQM pour définir et explorer des scénarios spécifiques de mesure stratégique pour les mesures existantes ou nouvelles de la sécurité du Client.
  c) Analyser les résultats GQM et les intégrer au catalogue des mesures.

- Fournir au Client un Rapport sur le développement d'un programme sur les mesures de sécurité et organiser une présentation récapitulative.

Responsabilités spécifiques du Client par rapport au Service

- Trouver un commanditaire de projet qui aura pour responsabilité de mener à bien le projet et aura le pouvoir de prendre les décisions relatives à l'exécution du projet.
- Désigner un chef de projet pour planifier les réunions des parties prenantes et pour répondre aux demandes de renseignements.
- S'assurer que les parties prenantes des services commerciaux et informatique participent à l'examen et à l'approbation des produits livrables du projet en collaboration avec Cisco.
- Fournir un accès à la documentation demandée, notamment les mesures actuelles de la sécurité, les processus opérationnels et les tableaux de bord de gestion.
- Collaborer avec Cisco pour programmer les ateliers et garantir la disponibilité des parties prenantes.
- Fournir aux membres de l'équipe de Cisco un accès aux cartes d'identification et aux bâtiments appropriés, à un espace de travail et à une salle de réunion, ainsi qu'au téléphone et au réseau local.

Développement d'un programme de gestion des risques liés aux tierces parties

Cisco effectuera une évaluation du Programme de gestion des risques liés aux fournisseurs et aux tierces parties du Client. L'évaluation permettra d'examiner les processus du programme afin d'évaluer l'efficacité de l'identification, du traitement, de la gouvernance et de la surveillance des risques liés aux tiers.

L'évaluation couvre tout le cycle de vie des engagements avec des tierces parties, dont le développement des exigences, la diligence et le contrôle raisonnables, la négociation, la transition et la transformation, ainsi que les opérations permanentes et la résiliation. Les problèmes identifiés seront hiérarchisés en fonction des risques, puis signalés. Des recommandations utiles seront fournies avec un plan d'amélioration proposé.

Responsabilités spécifiques de Cisco par rapport au Service

- Examiner le contexte du Programme de gestion des risques liés aux tierces parties.
- Examiner les principales stratégies commerciales, les objectifs et les initiatives qui dépendent des tierces parties ainsi que les éléments connexes de la stratégie globale.
- Définir les relations essentielles avec des tierces parties, ainsi que les services, les technologies et les produits qui en découlent et leur importance dans les processus opérationnels du Client.
- Définir la tolérance générale aux risques et formaliser les critères pertinents d'évaluation des risques commerciaux.
- Examiner les processus de gestion des risques liés aux tierces parties et déterminer les problèmes potentiels.
- Déterminer les processus pertinents de gouvernance, d'achat, de vérification préalable, de gestion des relations, de garantie et de gestion des risques.
- Améliorer la compréhension des interactions du Client avec les tierces parties.
- Examiner la documentation sur les processus et effectuer un entretien avec les principales parties prenantes pour déterminer les problèmes potentiels selon les exigences commerciales et les modèles de meilleures pratiques. Les domaines d'analyse peuvent inclure, s'il y a lieu, les éléments suivants :
    1. Inventaire des tierces parties
    2. Hiérarchisation
    3. Élaboration des exigences
    4. Évaluation des risques
    5. Planification de la continuité des activités
    6. Exigences relatives aux risques
    7. Définition de l'ANS
    8. Normes et modèles de contrat
    9. Critères de négociation et analyses de l'incidence
    10. Procédures de vérification préalable
    11. Gestion de la transition et de la transformation
    12. Surveillance des performances
    13. Processus de sécurité et d'assurance de la conformité
    14. Structures de gestion, mécanismes de contrôle et de responsabilité
- Évaluer les relations représentatives.
    1. Valider les exigences du client.
    2. Définir un échantillon de relations avec les tierces parties selon la hiérarchisation du client et les risques.
    3. Effectuer une évaluation générale par rapport aux exigences pour essayer de définir les risques et de

déterminer leur méthode d'identification, de gestion et de surveillance. Cette évaluation vise à valider les conclusions précédentes et à déterminer les nouveaux problèmes causés par la qualité de l'exécution.

4. L'évaluation reposera sur un entretien avec les principales parties prenantes et les représentants des tierces parties, et elle portera sur les éléments suivants :
   - Gouvernance et protection des renseignements
   - Exigences de conformité
   - Attentes opérationnelles
   - Continuité des activités et résilience opérationnelle
   - Gestion du changement

- Évaluer les risques
  1. Évaluer et classer les risques par ordre de priorité selon la tolérance aux risques commerciaux et selon les critères convenus d'évaluation des risques.
  2. Définir les profils de risque.
- Concevoir une Feuille de route de perfectionnement du Programme de gestion des risques liés aux tierces parties.
  1. Concevoir une feuille de route de perfectionnement comprenant des recommandations utiles de perfectionnement et des étapes provisoires concrètes, selon les risques hiérarchisés.
  2. Évaluer, dans la mesure du possible, les frais, la durée et les ressources nécessaires pour la mise en œuvre de la feuille de route de perfectionnement.
- Fournir au Client le Rapport d'évaluation du programme de gestion des risques liés aux tierces parties et le Résumé.

Responsabilités spécifiques du Client par rapport au Service

- Trouver un commanditaire de projet qui aura pour responsabilité de mener à bien le projet et aura le pouvoir de prendre les décisions relatives à l'exécution du projet.
- Désigner un chef de projet du Client pour planifier les réunions des parties prenantes, traiter les demandes de renseignements et gérer les interactions avec les tierces parties.
- S'assurer que les parties prenantes des services commerciaux et informatique participent à l'examen et à l'approbation des produits livrables du projet en collaboration avec Cisco.
- Fournir un accès aux ressources tierces appropriées. La réussite du projet nécessite la participation active et l'évaluation de la tierce partie en temps opportun.
- S'assurer de la fourniture en temps opportun de la documentation demandée au Client et à la tierce partie.
- Fournir aux membres de l'équipe de Cisco un accès aux cartes d'identification et aux bâtiments appropriés, à un espace de travail et à une salle de réunion, ainsi qu'au téléphone et au réseau local.

Évaluation de l'alignement de la structure sur la norme ISO 27001

Cisco comprend que le Client envisage d'obtenir une certification ISO 27001:2013 (ISO 27001 dans les présentes) dans le futur et souhaite recourir à des services de conseil pour comprendre la procédure et évaluer l'état général du niveau de préparation pour cette certification. Ce projet vise à fournir une présentation de la procédure de certification ISO 27001, à assister dans la définition d'un cadre potentiel pour la certification ISO 27001 et à fournir une évaluation générale de la procédure, ainsi qu'à contrôler l'alignement sur les normes afin de déterminer le niveau de préparation actuel du Client.

Cisco effectuera une évaluation de l'alignement actuel du Client sur la norme ISO 27001, y compris l'annexe A et les contrôles couverts par la norme ISO 27002:2013. L'évaluation comprendra un examen de la documentation et des entretiens pour déterminer l'alignement actuel sur les exigences de contrôle de la norme ISO. Cisco fournira des recommandations et une feuille de route pour la préparation à la certification ISO 27001.

Responsabilités spécifiques de Cisco par rapport au Service

- Organiser un atelier d'une demi-journée avec les principales parties prenantes pour présenter la norme ISO 27001 et la procédure générale requise pour obtenir la certification.
- Collaborer avec le Client pour examiner les options de cadre et définir une proposition de cadre de la certification ISO.
  a) Examiner les objectifs commerciaux et les objectifs en matière de sécurité de l'information.
  b) Effectuer un entretien avec les principales parties prenantes pour passer en revue les stratégies de sécurité de l'information et leurs liens avec les objectifs commerciaux.
  c) Définir les processus, les systèmes connexes et les équipes d'assistance dans le cadre du champ d'application.
  d) Déterminer si les contrôles de l'annexe A peuvent être considérés hors du champ d'application.
- Effectuer un examen général de l'alignement actuel sur les exigences ISO :
  a) Pour la norme ISO 27001
     - Examiner l'architecture globale de sécurité.
     - Examiner les processus de gouvernance appropriés en matière de sécurité.

        - Examiner la charte et la politique sur la sécurité de l'information et toute autre documentation connexe.
        - Examiner les documents et dossiers obligatoires sur la norme ISO 27001.
        - Examiner la méthodologie de gestion des risques et la documentation la plus récente sur l'évaluation des risques de sécurité de l'information.
        - Interroger un responsable de la sécurité de l'information et la haute direction, au besoin, pour évaluer les pratiques et la conformité aux objectifs définis.
        - Documenter les conclusions et les lacunes.
- Concevoir des recommandations pour combler les lacunes et une feuille de route définissant la priorité recommandée.
- Fournir une présentation sommaire des conclusions de l'évaluation.

Responsabilités spécifiques du Client par rapport au Service

- Trouver un commanditaire de projet qui aura pour responsabilité de mener à bien le projet et aura le pouvoir de prendre les décisions relatives à l'exécution du projet.
- Désigner un chef de projet pour planifier les réunions des parties prenantes et pour répondre aux demandes de renseignements.
- S'assurer que les parties prenantes des services commerciaux et informatique participent à l'examen et à l'approbation des produits livrables du projet en collaboration avec Cisco.
- Fournir un accès à la documentation accessible notamment : les objectifs et stratégies opérationnels de l'entreprise; les stratégies, les politiques et les procédures informatiques et de sécurité existantes; tout renseignement pertinent sur les réglementations, et les évaluations de sécurité et vérifications antérieures.
- Fournir aux membres de l'équipe de Cisco un accès aux cartes d'identification et aux bâtiments appropriés, à un espace de travail et à une salle de réunion, ainsi qu'au téléphone et au réseau local.
- Fournir la documentation relative à la norme ISO, y compris, le cas échéant, les éléments suivants :
    - Documents obligatoires sur la norme ISO 27001 :
        - la portée du système de gestion de la sécurité de l'information;
        - la politique de sécurité de l'information et les objectifs;
        - la méthodologie d'évaluation des risques et de traitement des risques;
        - la déclaration d'applicabilité;
        - le plan de traitement des risques;
        - le rapport d'évaluation des risques;
        - la définition des rôles et des responsabilités de sécurité;
        - l'inventaire des équipements;
        - l'utilisation acceptable des équipements;
        - la politique de contrôle des accès;
        - les procédures opérationnelles de gestion des TI;
        - les principes d'ingénierie de systèmes sécurisés;
        - la politique de sécurité du fournisseur;
        - la procédure de gestion des incidents;
        - Les procédures de continuité des activités;
        - les exigences légales, réglementaires et contractuelles.
    - Dossiers obligatoires :
        - les dossiers relatifs à la formation, aux compétences, à l'expérience et aux qualifications;
        - les résultats de la surveillance et des mesures;
        - le programme d'évaluation interne;
        - les résultats des vérifications internes;
        - les résultats de l'analyse de la gestion;
        - les résultats des mesures correctives;
        - les journaux des activités des utilisateurs, des exceptions et des événements de sécurité.
    - Documents non obligatoires, mais généralement fournis :
        - la procédure de contrôle des documents;
        - les contrôles pour la gestion des dossiers;
        - la procédure de vérification interne;
        - la procédure pour les mesures correctives;
        - la politique PAP (Prenez votre propre appareil);
        - la politique relative aux appareils cellulaires et au télétravail;
        - la politique de classification des renseignements;
        - la politique relative aux mots de passe;
        - la politique d'élimination et de destruction;
        - les procédures à suivre pour travailler dans les zones sécurisées;
        - la politique de bureau propre et d'écran vide;
        - la politique de gestion du changement;

- la politique de sauvegarde;
- la politique de transfert des renseignements;
- l'analyse de l'impact sur l'entreprise;
- le plan d'exécution et de tests;
- le plan de maintenance et d'examen;
- la stratégie de continuité des activités.

Évaluation de l'alignement de la structure sur la norme ISO 27002

Cisco effectuera une évaluation de la sécurité visant à déterminer la conformité à chaque domaine de la norme ISO 27002:2013. L'évaluation comprendra un examen de la documentation et des entretiens pour déterminer la sélection des contrôles et l'efficacité de la conception. Cisco fournira également

une évaluation de l'efficacité opérationnelle des contrôles grâce à des examens généraux de certains échantillons et à des examens des sites physiques des centres de données et des opérations des TI. Cisco classera les recommandations par ordre de priorité et les appliquera pour fournir une feuille de route de la norme ISO 27002.

Responsabilités spécifiques de Cisco par rapport au Service

- Examiner les objectifs en matière de sécurité de la structure et de l'information.
- Examiner la structure organisationnelle de sécurité de l'information.
  - Effectuer un entretien avec les principales parties prenantes pour comprendre les stratégies de sécurité de l'information et leur importance dans les objectifs commerciaux.
  - Obtenir une compréhension globale de l'architecture de sécurité.
  - Examiner les processus appropriés de gouvernance en matière de sécurité.
- Choisir les parties prenantes qui participeront aux entretiens entrant dans le cadre de l'examen.
- Examiner la documentation, notamment :
  - la dernière évaluation des risques de sécurité de l'information;
  - les politiques et normes de sécurité de l'information;
  - la documentation des contrôles pour une sélection et une conception adéquates des contrôles, conformément à la norme ISO 27002.
- Identifier les lacunes de la norme ISO 27002 en matière d'évaluation des risques liés à la sécurité de l'information, de sélection des contrôles et de conception documentée.
- Effectuer un entretien avec les parties prenantes en utilisant le questionnaire sur la norme ISO 27002. Les entretiens visent à :
  - valider la documentation de conception des contrôles;
  - comprendre les lacunes connues et évaluer l'efficacité opérationnelle des contrôles;
  - comprendre les procédures de contrôle non documentées;
  - déterminer les risques systémiques potentiels des opérations de TI.
- Effectuer des examens globaux de l'efficacité des contrôles par rapport aux échantillons avec l'une des deux méthodes suivantes :
  - examiner la preuve de l'exécution et de l'achèvement des contrôles;
  - faire un suivi de l'exécution des contrôles.
- Effectuer un examen du site physique des centres de données et des opérations des TI afin de faire un suivi de la mise en œuvre des contrôles.
- Documenter les conclusions, notamment les lacunes et problèmes définis et les recommandations de correction dans le Rapport d'évaluation de la norme ISO 27002.
- Fournir au Client le Rapport d'évaluation de la norme ISO 27002 et le Résumé.

Responsabilités spécifiques du Client par rapport au service

- Trouver un commanditaire de projet qui aura pour responsabilité de mener à bien le projet et aura le pouvoir de prendre les décisions relatives à l'exécution du projet.
- Désigner un chef de projet pour planifier les réunions des parties prenantes et pour traiter les demandes de renseignements.
- S'assurer que les parties prenantes des services commerciaux et informatique participent à l'examen et à l'approbation des produits livrables du projet en collaboration avec Cisco.
- Fournir un accès à la documentation accessible notamment : les objectifs et stratégies opérationnels de l'entreprise; les stratégies, les politiques et les procédures informatiques et de sécurité existantes; tout renseignement pertinent sur les réglementations, et les évaluations de sécurité et vérifications antérieures.
- Fournir aux membres de l'équipe de Cisco un accès aux cartes d'identification et aux bâtiments appropriés, à un espace de travail et à une salle de réunion, ainsi qu'au téléphone et au réseau local.

Évaluation de la conformité aux normes HIPAA et HITECH

Cisco effectuera une Évaluation de l'état de préparation HIPAA et HITECH afin de déterminer la conformité aux exigences des règles de sécurité de la loi HIPAA (*Health Insurance Portability and Accountability Act*) et aux exigences pertinentes supplémentaires de la loi HITECH (*Health Information Technology for Economic and Clinical Health Act*). L'évaluation comprendra un examen de la documentation et des entretiens pour déterminer les sélections de contrôle et l'efficacité de la conception. Cisco classera les conclusions par ordre priorité et appliquera les efforts de correction correspondants afin de fournir une Feuille de route de préparation de la sécurité conforme à la norme HIPAA.

Responsabilités spécifiques de Cisco par rapport au Service

- Examiner la structure organisationnelle du Client, les motivations commerciales, l'environnement réglementaire et les objectifs de sécurité de l'information :
  - Examiner la structure organisationnelle de sécurité de l'information.
  - Effectuer un entretien avec les principales parties prenantes pour comprendre les stratégies de sécurité de l'information et leur importance dans les objectifs commerciaux.
  - Examiner la documentation sur l'architecture de sécurité.
  - Examiner les processus pertinents de gouvernance en matière de sécurité et de vérification interne.
- Déterminer la conformité aux normes HIPAA/HITECH :
  - Définir les processus opérationnels et les transactions utilisant des renseignements médicaux électroniques protégés (ePHI), par le biais d'entretiens avec le personnel pertinent.
  - Définir, selon les entretiens avec le Client, les limites de la portée des ressources de renseignement par l'identification des applications et infrastructures pertinentes stockant ou traitant les ePHI.
- Déterminer les emplacements physiques entrant dans le cadre de l'évaluation et définir les contrôles correspondant à chaque emplacement.
- Concevoir un énoncé de la portée pour définir le champ d'application de la norme et le passer en revue avec le Client.
- Désigner les parties prenantes qui participeront aux entretiens avec Cisco dans le cadre de l'évaluation.
- Passer en revue l'évaluation des risques existants, les politiques et la documentation des contrôles du Client :
  - Passer en revue les politiques et normes de sécurité de l'information.
  - Passer en revue la dernière évaluation des risques de sécurité de l'information.
  - Passer en revue les rapports de vérification liés à la sécurité de l'information.
  - Passer en revue la documentation sur les contrôles pour une sélection et une conception adéquates des contrôles.
- Effectuer des entretiens, des examens de l'efficacité des contrôles et une inspection du site physique. Les entretiens des parties prenantes définis visent à :
  - valider la documentation de conception des contrôles;
  - examiner l'efficacité opérationnelle des contrôles;
  - étudier les processus de contrôle non documentés ou découvrir une documentation supplémentaire disponible pour l'évaluation.
- Sélectionner les contrôles d'échantillons correspondant aux exigences de la norme HIPAA et effectuer des examens sur leur efficacité opérationnelle afin de qualifier l'efficacité de la mise en œuvre des contrôles. Les examens globaux de l'efficacité seront effectués par rapport aux contrôles d'échantillons avec l'une des trois méthodes suivantes :
  - examiner la preuve de l'exécution et de l'achèvement des contrôles;
  - faire un suivi de l'exécution des contrôles;
  - examiner l'évaluation des contrôles dans le cadre du rapport de conformité à la norme PCI ou de toute autre évaluation pertinente.
- Effectuer une inspection du site physique des centres de données afin de faire un suivi de la mise en œuvre des contrôles.
- Effectuer une inspection du site physique des opérations des TI et des domaines de gestion dans les sièges sociaux.
- Fournir au Client un Rapport d'évaluation détaillée décrivant les conclusions de l'évaluation.
- Documenter les écarts de conformité constatés aux règles de sécurité HIPAA/HITECH et les problèmes d'efficacité des contrôles.
- Concevoir des recommandations de correction et une feuille de route de conformité.
- Fournir au Client le Résumé de l'évaluation de l'état de préparation à la conformité aux règles de sécurité HIPAA et HITECH.

Responsabilités spécifiques du Client par rapport au Service

- Trouver un commanditaire de projet qui aura pour responsabilité de mener à bien le projet et aura le pouvoir de prendre les décisions relatives à l'exécution du projet.
- Désigner un chef de projet pour planifier les réunions des parties prenantes et pour traiter les demandes de renseignements.
- Garantir un accès aux personnes clés pour les entretiens et les questions techniques.
- Fournir la documentation disponible pour permettre à Cisco d'exécuter ses responsabilités définies dans les présentes.
- Fournir un accès à toutes les ressources entrant dans le cadre d'application, aux fins de l'évaluation de la conformité aux directives de la norme HIPAA.
- Fournir à Cisco un accès aux locaux de bureau pertinents pour les réunions, les entretiens et les présentations dans le cadre des travaux effectués sur le site du Client.

Service d'analyse assurée par un fournisseur d'analyse agréé PCI

Cisco effectuera quatre (4) analyses de la sécurité externe des réseaux à intervalles de 90 jours, selon les exigences de la Norme de sécurité des données du secteur des cartes de paiement (« PCI »). Cisco effectuera une analyse de la sécurité selon un nombre prédéfini d'adresses IP individuelles.

Responsabilités spécifiques de Cisco par rapport au Service

- Organiser une réunion avec le Client pour la préparation de chaque analyse trimestrielle :
  - Vérifier la validité des coordonnées enregistrées et les modifier, au besoin.
  - Assister le Client par l'intermédiaire d'un Outil d'assistance pour les ressources dans le portail Web des services de sécurité de Cisco afin de :
    - vérifier que toutes les adresses IP visées nécessaires pour garantir la conformité à la norme PCI sont incluses dans l'analyse;
    - déterminer si des systèmes d'équilibrage de charge sont inclus dans le cadre de l'analyse et, le cas échéant, si toutes les configurations des appareils d'équilibrage de charge sont synchronisées;
    - vérifier que toutes les technologies IPS/IDS et tous les autres périphériques de l'infrastructure réseau sont configurés de manière à ne pas interférer avec les analyses.
  - Déterminer la date et l'heure de l'analyse et toutes les restrictions temporelles à définir.
- Effectuer une analyse trimestrielle en utilisant la solution d'analyse assurée par un fournisseur d'analyse Cisco qui a été agréée par le Conseil des normes de sécurité PCI, et ce en utilisant les paramétrages d'analyse stipulés par ce dernier.
- Fournir au Client la version PDF du Résumé de l'analyse trimestrielle assurée par un fournisseur d'analyse PCI et les rapports sur les détails (rapports d'analyse de la sécurité externe) au format exigé par le Conseil des normes de sécurité PCI.
- Collaborer avec le Client pour résoudre les vulnérabilités non conformes aux normes PCI, que le Client juge être des faux positifs.
- Effectuer une (1) nouvelle analyse trimestrielle de toutes les adresses IP présentant des vulnérabilités non conformes aux normes PCI qui ont été signalées dans l'analyse trimestrielle initiale.
- Cisco confirmera et certifiera chaque analyse trimestrielle si, et seulement si, le Client a fourni une preuve adéquate de toute vulnérabilité constituant un faux positif contesté et que toute vulnérabilité constituant un cas de non-conformité à la norme PCI détectée dans l'analyse initiale a fait l'objet d'une correction et n'est plus détectée dans la nouvelle analyse.

Responsabilités spécifiques du Client par rapport au Service

- Trouver un commanditaire de projet qui aura pour responsabilité de mener à bien le projet et aura le pouvoir de prendre les décisions relatives à l'exécution du projet.
- Désigner un chef de projet pour planifier les réunions des parties prenantes et pour traiter les demandes de renseignements.
- Garantir un accès aux personnes clés pour les entretiens et les questions techniques.
- Fournir un accès à toutes les ressources entrant dans le cadre d'application, aux fins de l'évaluation de la conformité à la norme de sécurité des données des cartes de paiement (PCI).
- Indiquer des coordonnées d'urgence notamment le nom, la fonction, l'adresse de courriel, ainsi que les numéros de téléphone professionnel et cellulaire.
- Le Client sera responsable :
  - de vérifier et d'attester que toutes les adresses IP dans le champ d'application relatives au maintien de la conformité à la norme PCI ont été signalées à Cisco;
  - de signaler la présence des systèmes d'équilibrage de charge inclus dans le cadre de l'analyse;
  - d'attester que toutes les configurations de périphériques de charge équilibrée sont synchronisées et de confirmer que les configurations sont effectivement synchronisées, ou le Client doit fournir les copies des analyses de vulnérabilités internes détaillées qu'il a effectuées et valider qu'il n'y a pas de vulnérabilités non conformes à la norme PCI signalées;
  - Configurer les technologies IPS/IDS et tous les autres périphériques de l'infrastructure réseau de sorte qu'ils n'interfèrent avec aucune analyse.
- Fournir une date et une heure pour chaque analyse et toutes les restrictions temporelles à définir pour l'analyse.
- Dans les vingt-cinq (25) jours civils suivant une analyse trimestrielle finale et la réception du rapport par le Client :
  - le Client doit corriger toutes les vulnérabilités non conformes à la norme PCI ou fournir les justificatifs suffisants afin que Cisco puisse prendre une décision sur toute vulnérabilité signalée comme étant un faux positif;
  - le Client doit produire un rapport et une demande selon lesquels Cisco atteste et certifie l'analyse.

Évaluation de la conformité à la norme PCI-DSS

Responsabilités spécifiques de Cisco par rapport au Service

- Il s'agit d'une évaluation délimitée dans le temps durant laquelle Cisco effectue un examen par rapport à la norme de sécurité PCI (comme DSS 3.1) en vigueur.
- Le service fournit un aperçu du niveau de conformité à la norme PCI d'un environnement de données du titulaire de carte (CDE).
- Effectuer une évaluation par l'intermédiaire d'entretiens et de la documentation clé pour respecter toutes les exigences relatives à la norme PCI-DSS (remarque : cette évaluation diffère d'un rapport de conformité [ROC] en cela que l'échantillonnage complet de l'ensemble des preuves peut ne pas être nécessaire).
- Fournir un rapport détaillé décrivant les corrections et les recommandations relatives à la tactique et aux stratégies.
- Fournir une matrice de planification détaillée au format Microsoft Excel pour les corrections requises.

Responsabilités spécifiques du Client par rapport au service

- Fournir aux ressources appropriées les connaissances et l'autorité dont elles ont besoin pour collaborer avec Cisco pendant l'atelier d'évaluation.
- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de l'entreprise.
- Fournir un accès électronique raisonnable à Cisco afin qu'elle puisse accéder aux périphériques réseau et aux périphériques de sécurité du Client pendant les réunions entrant dans le cadre de l'atelier.

Conseiller en matière de sécurité de l'entreprise

Responsabilités spécifiques de Cisco par rapport au Service

Cisco fournira un Conseiller 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 des produits et des services de sécurité et leur alignement sur le programme plus général de sécurité, de risques et de conformité du Client. Ce service est offert de manière flexible, comme convenu par les parties, avec l'intention de permettre au Client de mieux atteindre ses objectifs commerciaux. La première partie de la prestation comprend 2 à 4 semaines pour passer en revue les initiatives, les projets en cours, les objectifs de sécurité, et 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 contribuera à l'évolution des programmes de sécurité, de risque et de conformité correspondants, ce qui peut 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 la 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 relative à la technologie 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 et vérifier leur alignement sur les conceptions globales convenues ainsi que sur les exigences relatives à l'architecture et à l'ingénierie du Client. Comme requis et convenu, aider le Client à produire des exigences relatives à l'architecture et à l'ingénierie.
- Aider au 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 relativement aux pratiques exemplaires, aux tendances du secteur, aux matériaux de référence et à l'expertise mise à disposition par Cisco.
- Fournir des services grâce à 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 traiter les demandes de renseignements.
- Garantir un accès opportun aux personnes clés pour les entretiens et les questions techniques.
- Fournir un accès opportun à la documentation accessible, 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 échéanciers 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.

Service de segmentation de sécurité

À l'aide de la méthodologie d'Architecture de segmentation de sécurité de Cisco, Cisco développe et fournit une conception de haut niveau (HLD) pour l'architecture de sécurité du réseau de l'entreprise. La conception de haut niveau définira un ensemble de modèles d'architecture de sécurité segmentée, notamment des capacités de contrôle technique et un schéma de mise en œuvre logique pour chaque type de segment. Dans le cadre de la conception de haut niveau, Cisco fournira un Processus de placement de l'application qui comprend le processus décisionnel et les critères permettant de déterminer l'instanciation et l'application des modèles de conception développés. Cisco fournira également une feuille de route sur la mise en œuvre pour la nouvelle architecture.

Les principales méthodes d'obtention de renseignements auprès du Client sont un atelier sur la Segmentation de la sécurité, des entretiens et des commentaires sur les ébauches des livrables.

Responsabilités spécifiques de Cisco par rapport au Service

- Effectuer un appel de lancement pour présenter les équipes, discuter de la logistique et examiner les attentes pour l'atelier de Segmentation de sécurité sur site.
- Collaborer avec le chef de projet du Client pour définir les parties prenantes principales et éventuelles qui vont participer à l'atelier; il est prévu d'y inclure des représentants de l'équipe d'architecture, de la gestion des applications, de la sécurité et du réseau.
- Recueillir et examiner des renseignements généraux et des documents relatifs aux exigences commerciales et techniques. L'examen de la documentation doit inclure les éléments suivants autant que possible : a) politiques de sécurité, normes et procédures applicables; b) directives et inventaires de classification des données et du système; c) structure organisationnelle du Client; d) ressources commerciales critiques; e) principales menaces connues pour les ressources commerciales critiques; f) schémas de topologie des réseaux physique et logique; g) descriptions de l'architecture réseau;
- h) services traversant le réseau; i) applications et services s'exécutant sur le réseau; j) architecture de haut niveau du centre de données, des serveurs internes, de la connectivité de l'hôte de l'utilisateur et de la connectivité Internet; k) architecture du système d'administration de réseau; et l) évaluations ou documentation stratégique de sécurité adéquates et récentes, effectuées par des tiers ou par le Client.
- Planifier les premiers entretiens et séances d'examen avant de procéder à l'atelier sur site.
- Distribuer des questionnaires préalables aux ateliers aux participants de celui-ci.
- Fournir au Client le programme des ateliers et des entretiens.
- Examiner la documentation et les données fournies par le Client.
- Réaliser des entretiens en tête à tête ou à plusieurs avec les parties prenantes clés afin de recueillir des renseignements avant l'atelier, au besoin.
- Préparer les documents de l'atelier.
- Organiser l'Atelier sur la Segmentation de sécurité sur site. L'ordre du jour de l'atelier sera conçu pour recueillir l'opinion du Client sur l'architecture, les moteurs commerciaux et technologiques, et les paramètres de décision actuels pour la Segmentation de sécurité ainsi que sur l'architecture cible.
- Créer et fournir une présentation récapitulative des résultats initiaux de l'Atelier.
- Organiser des entretiens de suivi ou demander et examiner une documentation supplémentaire provenant du Client.
- Développer des directives de création de segments et de placement des actifs.
- Créer et documenter les modèles de définitions et de conception de segment recommandés qui incluent des schémas logiques de haut niveau, notamment les contrôles de sécurité recommandés.
- Élaborer des recommandations supplémentaires sur la hiérarchisation des segments, la mise en œuvre de contrôle de sécurité et le flux de données de haut niveau entre les segments.
- Documenter un renvoi unique à une norme de sécurité commune du secteur que les parties jugent être pertinente (p. ex., NIST 800-53, PCI-DSS ou ISO 27001).

- Examiner régulièrement les conceptions d'ébauche avec le Client pour permettre des commentaires rapides.
- Créer une conception de haut niveau qui comprend : a) une présentation récapitulative; b) une conception de haut niveau avec les segments et les contrôles associés recommandés; c) un processus de placement de l'application.
- Transmettre la conception de haut niveau au Client pour examen et approbation.
- Définir la structure de répartition des tâches de haut niveau pour délimiter les projets ou les programmes de tâches nécessaires en vue d'atteindre la conception de haut niveau recommandée.
- Collaborer avec le Client pour représenter les tâches requises sur un calendrier.
- Collaborer avec le Client pour développer un niveau d'effort estimé ou un ordre de grandeur approximatif pour la mise en œuvre de la conception de haut niveau (HLD).
- Créer une Feuille de route stratégique sur la segmentation de sécurité et la remettre au Client pour examen et approbation.
- Organiser une présentation récapitulative finale résumant les recommandations, la conception de haut niveau (HLD) et la Feuille de route stratégique sur la segmentation de sécurité.

Responsabilités spécifiques du Client par rapport au Service

- Collaborer avec Cisco pour programmer les ateliers et garantir la disponibilité des parties prenantes.
- Fournir aux membres de l'équipe de Cisco un accès aux cartes d'identification et aux bâtiments appropriés, à un espace de travail et à une salle de réunion, ainsi qu'au téléphone et au réseau local.
- Choisir les parties prenantes clés pour l'Atelier sur la segmentation de sécurité.
- Consulter l'ordre du jour de l'atelier et fournir des commentaires.
- Sauf disposition contraire prise entre les parties, le Client doit veiller à ce que toute demande de documentation supplémentaire ou de renseignements par Cisco soit satisfaite dans les trois (3) jours ouvrables.
- Mettre à disposition de Cisco les accès ou agents de sécurité nécessaires pour accéder au site du Client.
- Mettre à disposition des installations adéquates pour mener les entretiens et l'atelier, notamment : une alimentation, un espace de bureau, du matériel audiovisuel, des projecteurs ou écrans, des tableaux blancs appropriés et au moins un tableau à feuilles blanches.
- Fournir à Cisco un accès aux réseaux sans fil pour invité avec accès à Internet, si ceux-ci sont disponibles dans l'installation.
- Fournir à Cisco les politiques, les conditions et les milieux de travail en vigueur sur le site du Client.
- Fournir à Cisco les commentaires demandés en ce qui concerne les conceptions lors des conférences téléphoniques ou par demande écrite dans les deux (2) jours ouvrables.
- Examiner et approuver la conception de haut niveau en conséquence.
- Collaborer de façon interactive avec Cisco afin de définir la structure de répartition des tâches, les échéances et les estimations de l'effort.
- Examiner et approuver la Feuille de route de segmentation stratégique de la sécurité.
- Coordonner la planification des principales parties prenantes commerciales et technologiques compétentes qui assisteront à la présentation récapitulative.
- Mettre à disposition des locaux adéquats pour mener la présentation récapitulative, notamment une alimentation, de l'équipement audiovisuel et des projecteurs ou des écrans adéquats.
- Veiller à ce que les parties prenantes clés du Client assistent à la dernière présentation récapitulative de Cisco.

Annexe-A

Unités de gestion de stock (UGS) de service

La liste suivante d'Éléments de travail sur les services (Étiquettes de prestation) destinée aux services-conseils et aux services d'intégration est fournie à titre de référence :

Produits livrables et étiquettes des services d'intégration

Produits livrables	Éléments de travail	
Évaluation de la sécurité des périphériques réseau (NDSA)	OPT-SOS-NDSA	OPT-RS NOS-NDSA
Assistance avancée dans le cadre des changements en matière de sécurité (Security Advanced CS)	OPT-SOS-ACS	OPT-SO NOS-ACS
Assistance dans le cadre des changements en matière de sécurité (Security CS)	OPT-SOS-CS	OPT-SO NOS-CS
Service de simulation d'environnement de cyberdéfense (Security CR3)	OPT-SOS-CR3	OPT-SO NOS-CR3
Service de simulation d'environnement de cyberdéfense (Security CR5)	OPT-SOS-CR5	OPT-SO NOS-CR5

Assistance dans le cadre du développement d'une conception de sécurité (Security DDS)	OPT-SOS-DDS	OPT-SO NOS-DDS
Assistance et analyse de la conception de sécurité (Security DRS)	OPT-SOS-DRS	OPT-SO NOS-DR
Contrôle de l'intégrité de la sécurité (Security HC)	OPT-SOS-HC	OPT-SO NOS-HC
Assistance pour la planification de la sécurité et la résolution des problèmes de sécurité (Security IRPS)	OPT-SOS-ISUPP	OPT-SO NOS-ISUPP
Assistance pour la stimulation de la sécurité (SKSS)	OPT-SOS-KICK	OPT-SO NOS-KICK
Assistance et conseils en matière de réseau et de sécurité (Security NCS)	OPT-SOS-NCS	OPT-SO NOS-NCS
Assistance souple continue en matière de sécurité (Security OFS)	OPT-SOS-OFS	OPT-SO NOS-OFS
Assistance en matière d'adaptation des performances de sécurité (Security PTS)	OPT-SOS-PTS	OPT-SO NOS-PTS
Recommandations logicielles proactives pour la sécurité (Security PSR)	OPT-SOS-PSR	OPT-SO NOS-PSR
Assistance en matière de stratégie et de planification de la sécurité (SSPS)	OPT-SOS-SPS	OPT-SO NOS-SPS
Évaluation de l'état de préparation des technologies de sécurité (STRA)	OPT-SOS-TRA	OPT-SO NOS-TRA
Assistance de premier plan pour la réalisation de tests et la validation de la sécurité (Security VTPS)	OPT-SOS-PVTS	OPT-SO NOS-VTPS
Assistance pour la réalisation de tests et la validation de la sécurité (Security VTS)	OPT-SOS-PVTS	OPT-SO NOS-VTS
Alerte de sécurité logicielle (SSA)	OPT-SOS-SA	OPT-SO NOS-SSA
Service de connaissances de la sécurité (Security KS)	OPT-SOS-KS	OPT-SO NOS-SMKS
Transfert à distance des connaissances sur la sécurité (Security RKT)	OPT-SOS-KTM	OPT-SO NOS-RKT

Produits livrables et étiquettes des services-conseils

Produits livrables	Éléments de travail	
Service de conservation des réponses aux incidents	OPT-SOS ADV IR	OPT-SO NOS-ADV IR
Assistance souple soutenue	OPT-SOS ADV OFS	OPT-SO NOS-ADV OFS
Gestion de projet consultatif	OPT-SOS ADV PM	OPT-SO NOS-ADV PM
Services de conseil en sécurité		
Évaluation du programme de sécurité et feuille de route stratégique	OPT-SOS ADV-SCS PASR	OPT-SO NOS-ASCS PASR
Évaluation commerciale du système de contrôle et du programme de sécurité	OPT-SOS ADV-SCS PCDA	OPT-SO NOS-ASCS PCDA
Atelier sur la stratégie de sécurité mobile	OPT-SOS ADV-SCS MSW	OPT-SO NOS-ASCS MSW
Atelier sur la stratégie de sécurité en nuage	OPT-SOS ADV-SCS CSW	OPT-SO NOS-ASCS CSW
Service de contrôle de l'intégrité de la conformité du nuage	OPT-SOS ADV-SCS CCHC	OPT-SO NOS-ASCS CCHC
Évaluation de l'architecture infonuagique	OPT-SOS ADV-SCS CAA	OPT-SO NOS-ASCS CAA
Évaluation de la conformité à la norme PCI-DSS	OPT-SOS ADV-SCS PIRA	OPT-SO NOS-ASCS PIRA
Atelier sur les mesures de sécurité	OPT-SOS ADV-SCS SMW	OPT-SO NOS-ASCS SMW
Évaluation de tierces parties en matière de sécurité	OPT-SOS ADV-SCS TPA	OPT-SO NOS-ASCS TPA
Analyses de l'incidence sur la confidentialité	OPT-SOS ADV-SCS PIA	OPT-SO NOS-ASCS PIA
Augmentation du personnel d'assistance dans le cadre du programme portant sur les risques de sécurité	OPT-SOS ADV-SCS PSSA	OPT-SO NOS-ASCS PSSA
Évaluation des architectures d'application	OPT-SOS ADV-SCS AAA	OPT-SO NOS-ASCS AAA
Évaluation des intrusions dans l'application	OPT-SOS ADV-SCS APA	OPT-SO NOS-ASCS APA
Amélioration SDLC	OPT-SOS ADV-SCS SDLC	OPT-SO NOS-ASCS SDLC

Évaluation de l’application mobile	OPT-SOS ADV-SCS MAA	OPT-SO NOS-ASCS MAA
Évaluation des architectures de réseaux	OPT-SOS ADV-SCS NAA	OPT-SO NOS-ASCS NAA
Test d’intrusion dans le réseau	OPT-SOS ADV-SCS TNP	OPT-SO NOS-ASCS NPT
Évaluation de la sécurité des solutions sans fil	OPT-SOS ADV-SCS WSA	OPT-SO NOS-ASCS WSA
Évaluation de la sécurité physique	OPT-SOS ADV-SCS PSA	OPT-SO NOS-ASCS PSA
Piratage psychologique	OPT-SOS ADV-SCS SE	OPT-SO NOS-ASCS SE
Piratage électronique	OPT-SOS ADV-SCS RTBT	OPT-SO NOS-ASCS RTBT
Développement de programmes	OPT-SOS ADV-SCS PD	OPT-SO NOS-ASCS PD
Développement d’un programme sur les risques	OPT-SOS ADV-SCS RPD	OPT-SO NOS-ASCS RPD
Évaluation des risques liés aux technologies de l’information (TI)	OPT-SOS ADV-SCS ITRA	OPT-SO NOS-ASCS ITRA
Évaluation de l’alignement de la structure sur la norme ISO 27001	OPT-SOS ADV-SCS OAI	OPT-SO NOS-ASCS OAI
Prise en charge des indicateurs de sécurité et de risque	OPT-SOS ADV-SCS SRMS	OPT-SO NOS-ASCS SRMS
Développement d’un programme de gestion des risques liés aux tierces parties	OPT-SOS ADV-SCS TRPD	OPT-SO NOS-ASCS TRPD
Évaluation de la conformité aux normes HIPAA et HITECH	OPT-SOS ADV-SCS HHA	OPT-SO NOS-ASCS HHA
Analyse assurée par un fournisseur d’analyse agréé PCI	OPT-SOS ADV-SCS PASV	OPT-SO NOS-ASCS PASV
Services de conseil en sécurité personnalisés	OPT-SOS ADV-SCS CSC	OPT-SO NOS-ASCS CSC
Service de segmentation de sécurité	OPT-SOS ADV-SCS SSS	OPT-SO NOS-ASCS SSS
Conseiller en matière de sécurité de l’entreprise	OPT-SOS ADV-SCS SAA	OPT-SO NOS-ASCS SAA