<<Service Description: Cisco Active Threat Analytics>>
Description de service : Analyses des menaces actives de Cisco

Le présent document décrit les services de sécurité Analyses des menaces actives de Cisco.

Documents connexes : le présent document doit être lu conjointement aux documents suivants, également disponibles à l'adresse www.cisco.com/ca/aller/descriptionsduservice/ : (1) Glossaire; (2) Liste des services non couverts et (3) Directives en matière de gravité et de signalisation progressive. Tous les termes en majuscules figurant dans cette description revêtent la signification qui leur est donnée dans le Glossaire.

Vente directe par Cisco. Si vous avez souscrit à ces services directement auprès de Cisco, ce document est intégré à votre entente-cadre de services (ECS), à votre entente de services avancés (ESA) ou à toute autre entente de services équivalente vous liant à Cisco. S'il n'est pas déjà couvert dans votre ECS ou votre entente de services équivalente, ce document doit être consulté conjointement avec les documents connexes mentionnés ci-dessus. Dans le cas de conflit entre la présente description de service et votre contrat-cadre de services (ou contrat de services équivalent), 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, ce document n'a qu'un caractère informatif et ne constitue en aucun cas un contrat entre vous et Cisco. Le contrat (s'il y a lieu) qui régit la prestation de ce Service est celui établi entre vous et votre Revendeur agréé Cisco. Votre revendeur agréé Cisco doit vous fournir ce document. Vous pouvez également en obtenir une copie, ainsi qu'une copie des autres descriptions des services proposés par Cisco, à l'adresse suivante : www.cisco.com/ca/aller/descriptionsduservice/.

Cisco s'engage à fournir les services de sécurité Analyses des menaces actives (ATA) de Cisco décrits ci-dessous tels qu'ils sont choisis et détaillés sur le bon de commande pour lequel Cisco a reçu le paiement correspondant. Cisco doit fournir un devis pour les services (le « Devis ») précisant l'étendue des services et la durée de prestation de ces derniers par Cisco. Cisco doit recevoir un Bon de commande faisant référence au Devis convenu entre les parties et reconnaissant en outre les conditions dudit document.

Résumé du service

La présente description de service est conçue pour offrir au Client une compréhension de base des activités, des éléments livrables et des processus de prestations de services mis en œuvre par Cisco dans le cadre de Cisco ATA. La présente description de service est également conçue pour définir correctement les attentes du client au sujet de ces services.

Cisco ATA peut inclure les offres suivantes, conformément à ce qui a été choisi et détaillé sur le bon de commande.

L'offre de service de base de Cisco ATA comprend deux volets en matière de services. Chaque volet peut être acheté séparément ou en combinaison avec un ou plusieurs Coffrets d'options complémentaires ATA présentés ci-dessous.

Offres de service de base : ATA option Optimisée et ATA

option Premier – **option Optimisée :**

- Une (1) instance de Terminal de collecte de données et d'analyse (DCAP) sur site pour prendre en charge un enregistrement allant jusqu'à 3 000 événements par seconde (EPS) (une crête de 5 000 EPS) et un stockage de rappel allant jusqu'à 100 To de télémétrie brute
- Une (1) instance de système de capteurs ATA sur site pour prendre en charge jusqu'à 1 Gbit/s de débit et 10 To de stockage
- Analyse des renseignements sur les menaces
- Extraction de métadonnées et NetFlow Generation
- Analyse avancée
- Accès au portail actif des clients
- Directeur des enquêtes
- Examen trimestriel d'activité

ATA option **Premier :**

- Une (1) instance de Terminal de collecte de données et d'analyse (DCAP) sur site pour prendre en charge un enregistrement allant jusqu'à 250 000 événements par seconde (EPS) (une crête de 400 000 EPS) et un stockage de rappel allant jusqu'à 400 To de télémétrie brute
- Une (1) instance de système de capteurs ATA sur site avec une fonction de capture intégrale des paquets
- Une (1) option supplémentaire de débit étendu pour capteur ATA pour permettre au capteur de prendre intégralement en charge jusqu'à 4 Gbit/s de débit et 60 To de stockage
- Analyse des renseignements sur les menaces
- Extraction de métadonnées et NetFlow Generation
- Analyse avancée
- Accès au portail actif des clients
- Directeur des enquêtes
- Recherche proactive des menaces
- Examen trimestriel d'activité
- Exposé technique mensuel

Coffrets d'options complémentaires des offres de service de base

Les coffrets d'options complémentaires ATA peuvent uniquement être achetés en supplément d'une des offres de service de base d'Analyses des menaces actives.

Option complémentaire ATA – **système de capteurs ATA supplémentaire** :

- Déployer une instance supplémentaire de système de capteurs ATA qui prend en charge jusqu'à 1 Gbit/s de débit.
- Chaque système de capteurs ATA supplémentaire nécessite une connectivité à un déploiement de DCAP pour la capture et pour l'analyse des données collectées par le capteur; il ne doit pas être acheté en tant qu'option complémentaire autonome.
- Pour le volet Optimisé, le capteur ATA n'inclut pas les fonctionnalités de capture intégrale de paquets et prend en charge jusqu'à 10 To de stockage.
- Pour le volet Premier, le capteur ATA inclut les fonctionnalités de capture intégrale de paquets et prend en charge jusqu'à 20 To de stockage.

Option complémentaire ATA – **Débit étendu pour le capteur ATA** :

- Augmenter le débit d'une seule instance de système de capteurs ATA existante, disponible en incréments de débit de 3 Gbit/s jusqu'à 16 Gbit/s au total pour l'ensemble des capteurs
- Chaque offre complémentaire de débit étendu pour capteur ATA fournit également un stockage supplémentaire de 40 To pour le déploiement du système de capteurs ATA
- L'option doit être uniquement en supplément d'un déploiement existant d'un système de capteurs ATA et être achetée dans le cadre d'un Coffret de base ATA ou en tant qu'option complémentaire pour système de capteurs ATA

Option complémentaire ATA – **Extension de stockage** :

- Étendre le DCAP ou la capacité de stockage des capteurs afin de capturer des données d'analyse de réseau supplémentaires; l'option est disponible en incréments de 400 To de télémétrie brute*

Option complémentaire ATA – **Demandes de développement** :

- Mettre en œuvre des Demandes de développement approuvées en lien avec la solution ATA, comme les rapports sur mesure ou une consommation télémétrique supplémentaire de périphérique

L'achat des Coffrets d'offres complémentaires peut nécessiter l'envoi d'un équipement supplémentaire sur site appartenant à Cisco à installer sur le site du Client

Cisco fournira uniquement l'assistance relative aux offres de services d'Analyses des menaces actives qui ont été choisies sur le bon de commande.

Veuillez lire attentivement ce document, car il contient des informations importantes sur le service d'Analyses des menaces actives que vous avez éventuellement acheté à Cisco.

1. Analyses des menaces actives de Cisco

Les Analyses des menaces actives de Cisco offrent une surveillance à distance en matière de sécurité des réseaux en utilisant des métadonnées de paquets de réseaux et des techniques de détection de comportement des réseaux, en tirant profit d'un vaste ensemble de flux de données de sécurité pour la Durée déterminée, afin de détecter et de répondre rapidement aux incidents et aux événements liés à la sécurité.

La Durée commence au début de la Prestation de service et de surveillance (section 1.4), ou huit (8) semaines après la Réunion de lancement (section 1.1), la première date étant retenue.

La prestation des services ATA comprendra quatre (4) phases, conformément à ce qui est décrit dans ce document :

1. Réunion de lancement
2. Activation
3. Transition
4. Surveillance et Prestation de service

1.1 Réunion de lancement

1.1.1 Gestion de projet

Cisco assignera un Gestionnaire de projet dont le rôle consistera à servir d'interlocuteur unique. Cisco collaborera avec le Client pour élaborer un plan complet de projet, pour gérer les personnes et les processus nécessaires dans le cadre des Services, et pour surveiller que les services sont fournis en conformité avec le plan.

Responsabilités de Cisco :

- Désigner un interlocuteur unique (le « Gestionnaire de projet » ou « PM ») pour tous les problèmes liés aux prestations ATA fournies dans le cadre de ce Service. Cette personne sera identifiée et sera disponible durant les heures normales de bureau.
- Désigner un suppléant en cas d'indisponibilité du Gestionnaire de projet.
- Définir le flux de communication avec le commanditaire et les parties prenantes majeures du Client.
- Participer aux réunions périodiques prévues avec le Client pour évaluer l'avancement du service, identifier et consigner les dépendances, les risques et les problèmes en rapport avec la prestation réussie du service.
- Agir à titre d'interlocuteur principal pour les procédures de gestion du changement.

Responsabilités du Client :

- Désigner un interlocuteur unique auquel toutes les communications de Cisco peuvent être adressées et qui est habilité à agir en ce qui concerne tous les aspects des services ATA.
- Désigner un suppléant ou interlocuteur secondaire, cette personne ayant le pouvoir d'agir sur tous les aspects des services en l'absence de l'interlocuteur principal.
- Participation aux réunions d'analyse du projet ou aux conférences téléphoniques régulièrement organisées.
- Révision avec Cisco du calendrier du projet, des objectifs, des services, ainsi que des rôles et responsabilités.

- Désigner un commanditaire du projet et des parties prenantes majeures et définir leur rôle dans le cadre de ce projet.
- Travailler avec le chef de projet Cisco pour s'assurer que le commanditaire du projet chez le Client, les parties prenantes majeures et tous les membres de l'équipe de projet reçoivent les communications relatives au projet et sont inclus dans les sessions de communication programmées régulièrement.
- Collaborer avec Cisco pour planifier la réunion de lancement et communiquer le calendrier de la réunion aux parties prenantes désignées du Client.
- Fournir les renseignements et la documentation demandés par Cisco de manière opportune afin de respecter les calendriers du projet.
- Informer Cisco de toute mise à niveau matérielle ou logicielle ayant trait à la prestation des Services ou de tout autre changement au niveau du réseau actuel du Client ayant trait à la prestation des Services au moins dix (10) jours ouvrables avant la mise à niveau.
- Informer Cisco de toute activité de mise en œuvre planifiée dans les dix (10) jours ouvrables précédant l'activité planifiée.
- Informer Cisco de toute modification relative à la planification d'une installation au moins soixante-douze (72) heures avant la date d'installation planifiée initiale.
- Informer Cisco de toute modification de planification relative à ce Terme au moins dix (10) jours ouvrables avant l'activité planifiée.
- Organiser la disponibilité des installations nécessaires et l'accès pour les réunions sur site (p. ex. badges d'accès et badges visiteurs, salles de conférence, projecteurs et ponts de conférence).

1.1.2 Réunion de lancement

Le Gestionnaire de projet communiquera avec l'interlocuteur du Client afin d'organiser la réunion de lancement dans un délai de quarante-cinq (45) jours suivant la réception d'un Bon de commande valide. La réunion de lancement se déroule en général sous forme de conférence téléphonique abordant les détails du contrat souscrit. Un partenaire Cisco peut être sollicité. Le Gestionnaire de projet, assisté des ingénieurs Cisco affectés au compte du Client, anime généralement la réunion de lancement.

Responsabilités de Cisco

- Organiser un ou plusieurs ateliers de lancement à distance (Cisco WebEx) pour examiner les mesures d'activation et les services achetés, conformément aux indications du Bon de commande.

Responsabilités du Client :

- Identifier les principales personnes-ressources et les membres habilités du personnel devant assister à la réunion de lancement, et collaborer avec le Gestionnaire de projet pour organiser et animer la réunion de lancement.
- Fournir les renseignements nécessaires pour planifier les mesures d'activation.

1.2 Activation

L'activation est principalement une phase de collecte de renseignements qui constituera la base de la prestation du service ATA. Elle comprendra également la livraison et l'installation des unités de DCAP et des capteurs ATA (l'« équipement sur site ») inclus dans le service ATA, conformément aux indications du Bon de commande.

1.2.1 Collecte des renseignements

Pour gérer efficacement le déroulement d'un incident de sécurité, Cisco a besoin d'assimiler l'ensemble des processus relatifs à l'environnement et à la sécurité du Client. La collecte des renseignements lors de la phase d'activation sera principalement effectuée à distance au moyen d'une série de réunions WebEx avec le personnel et les parties prenantes majeures du Client.

Les renseignements recueillis lors de cette phase peuvent inclure :

- La structure organisationnelle et les présentations
- Les objectifs de la solution, ainsi que les exigences commerciales, techniques et opérationnelles
- La politique de sécurité actuelle, l'environnement existant de gestion des incidents relatifs à la sécurité et les procédures de gestion des incidents
- Les schémas des réseaux et les cartes de topologie
- Le recensement des réseaux IP et des schémas IP existants
- L'étude de la conception de l'emplacement physique et logique des unités de DCAP et des capteurs ATA
- Les documents de classification et de hiérarchisation des ressources
- Les politiques ou renseignements existants qui font référence au trafic réseau normal et acceptable requis pour procéder correctement à la configuration des équipements sur site
- Les rapports trimestriels d'analyses de vulnérabilité qui fournissent des détails tels que les ports d'écoute, la version des services et les références ponctuelles des vulnérabilités concernant des ressources essentielles telles que les serveurs ou les applications logicielles
- Les plans technologiques futurs

Responsabilités de Cisco :

- Planifier et coordonner les réunions de collecte à distance de renseignements avec le Client pour recueillir les renseignements pertinents en fonction des besoins.
- Examiner les renseignements tels qu'ils ont été fournis par le Client, en déterminant les écarts éventuels et en relevant toutes les mesures correctives éventuelles qui nécessitent des mesures de la part du Client.
- Examiner les situations et les emplacements du réseau où la technologie de capture intégrale de paquets peut ne pas convenir. Configurer correctement l'équipement sur site afin de respecter les exigences du Client.

Responsabilités du Client :

- S'assurer que les experts du Client participent aux ateliers de collecte de renseignements et qu'ils fournissent les renseignements nécessaires, en fonction des besoins.
- Fournir à Cisco la documentation et les ressources pertinentes pour examiner les renseignements requis avant ou pendant les ateliers, en fonction des besoins.
- Fournir un recensement des réseaux IP et des schémas IP existants. S'il n'en existe pas, le Client est chargé de collaborer avec Cisco pour créer une carte topologique à l'aide des outils de recherche et d'analyse.
- Fournir une liste complète des personnes-ressources (incluant la description de leur poste, leur fonction et leurs responsabilités) avec lesquelles communiquer lors de la gestion et de la signalisation d'un incident.
- Fournir à Cisco des rapports trimestriels faisant état de l'analyse de vulnérabilité et des services pour les appareils concernés, le cas échéant.
- Collaborer avec Cisco afin d'examiner les documents et les renseignements collectés et aider les spécialistes en ingénierie-conseils réseau Cisco dans le cadre de la documentation de l'identification, de la classification et de la hiérarchisation des systèmes et des données les plus importants.
- Définir les situations et les emplacements du réseau où la technologie de capture intégrale des paquets peut ne pas convenir et indiquer ces renseignements à Cisco.
- Fournir tout renseignement complémentaire demandé par Cisco. Collaborer avec Cisco pour développer des modèles détaillés de configuration et de conception en apportant des renseignements et une rétroaction.

1.2.2 Installation de l'équipement sur site

Cisco expédiera les unités de DCAP et les capteurs, que le Client devra installer sur son site, huit (8) semaines suivant la première réunion de lancement. Les détails de l'expédition doivent être confirmés avec le Client avant l'expédition. L'équipement sur site comporte l'équipement de sécurité des réseaux nécessaire à l'exécution du service ATA, conformément aux offres de service choisies sur le Bon de commande.

L'équipement sur site doit être installé au niveau d'un emplacement physique/logique dont il sera mutuellement convenu et demeurera dans les locaux du Client pour la durée du service ATA acheté.

Les droits sur l'équipement sur site restent la propriété de Cisco. Au moment du retrait, Cisco entend récupérer l'équipement sur site dans le même état que lors de son installation, en tenant compte de l'usure normale. Le Client remboursera à Cisco les frais relatifs à l'équipement sur site qui sont considérés comme dépassant le cadre d'une usure normale.

Un formulaire de suivi des ressources sera remis au Client en vue de sa validation après l'expédition de l'équipement sur site. Ce formulaire comprendra les renseignements suivants concernant l'équipement Cisco placé dans les locaux du Client : 1) descriptions détaillées, références des produits et numéros de série; 2) adresse physique à laquelle l'équipement se trouvera; 3) numéro de Bon de commande correspondant au service acheté par le Client.

Comme prévu entre Cisco et le Gestionnaire de projet, un ingénieur-conseil réseau Cisco peut se rendre sur le site pour y apporter une assistance à l'installation et au test de l'équipement.

Les éléments suivants peuvent être fournis en tant qu'équipement sur site :

- Routeur RPV
- Branchement/commutateur réseau passif
- Moteurs d'analyse de renseignements
- Composants de stockage des données

Responsabilités de Cisco :

- Expédier tous les appareils, serveurs ou périphériques prenant en charge des applications sur l'équipement sur site.
- Assister le Client lors de l'installation de l'équipement sur site.
- Assister dans l'instauration de la connectivité entre les unités de DCAP et les capteurs et la confirmer.
- Établir la connectivité entre le site du Client et l'équipement sur site de Cisco.
- Réaliser toute la maintenance matérielle ou logicielle requise relative à l'équipement sur site.

Responsabilités du Client :

- Installer l'équipement sur site selon les directives fournies par Cisco.
- Collaborer avec Cisco pour assurer l'assistance sur site afin de mettre en œuvre la maintenance nécessaire à l'emplacement physique et logique convenu (empilement, connexion réseau, alimentation, etc.).
- Permettre à Cisco ou à ses fournisseurs d'accéder aux sites du Client dans la mesure établie de manière raisonnable par Cisco en vue de l'inspection ou de la maintenance d'urgence de l'équipement sur site. L'absence d'accès permis en temps opportun peut infirmer la prestation des services et retarder leur rétablissement et leur exécution.
- Fournir à Cisco un accès au site ou une assistance pour la maintenance matérielle requise.
- Fournir les éléments suivants pour chaque unité de DCAP ou capteur :
  - Une adresse IP non NAT acheminée publiquement et un accès réseau avec bande passante Internet d'au moins 10 Mbit/s pour le routeur RPV afin d'établir une connexion sécurisée à Cisco.
  - Satisfaire les exigences en matière de réseau et les conditions nécessaires pour autoriser les communications bidirectionnelles entre les unités de DCAP et les capteurs correspondants, selon les besoins.
  - Un espace physique, une sûreté physique, une alimentation électrique, un système de refroidissement et des conditions environnementales convenables nécessaires pour l'exploitation informatique des équipements sur site.

- Remplir et retourner à Cisco le formulaire de suivi des ressources relatif aux équipements sur site.
- Maintenir les équipements sur site en bon état de fonctionnement. Le Client s'engage à ne pas réorganiser, déconnecter, retirer, tenter de réparer ou altérer de toute autre manière les équipements sur site, et à ne laisser aucune autre personne faire de même. Si cela venait à se produire sans la réception préalable du consentement écrit de Cisco, le Client serait chargé de rembourser Cisco du coût de la réparation ou du remplacement de tout équipement endommagé. Le Client ou toute autre partie ne pourront en aucun cas tenir Cisco responsable des interruptions de service ou des pertes, coûts ou dommages de toute nature résultant d'une utilisation ou d'une maintenance incorrecte des équipements sur site.
- Retourner à Cisco les équipements sur site en état de fonctionnement immédiatement après la résiliation ou l'expiration de la Durée.

1.3 Transition

Au terme de la phase d'activation, Cisco fournira au Client un dossier de présentation de la Transition. Cisco déterminera un format adéquat et un procédé de livraison pouvant notamment comprendre, mais sans s'y limiter, l'utilisation d'un support partagé par Internet, par téléconférence ou sur site.

Les éléments couverts dans le dossier de présentation de la Transition peuvent inclure :

- une analyse des activations réussies et des défis;
- une évaluation du processus de signalisation progressive des incidents;
- une évaluation des recommandations ATA établies lors de la phase d'activation, le cas échéant.

Lorsque le dossier de présentation de la Transition sera terminé, la surveillance et la gestion des incidents seront transférées au centre des opérations de sécurité ATA (SOC ATA) de Cisco, comme décrit dans la section 1.4. De plus, la préparation et l'envoi des factures pour le service ATA commenceront également à l'issue de la remise du dossier de présentation de la Transition.

Responsabilités de Cisco :

- Au terme de la phase d'activation, assurer une séance de présentation du dossier de la Transition au Client.

Responsabilités du Client :

- Désigner au moins deux (2) représentants de la sécurité pour participer à la présentation du dossier de la Transition.

1.4 Surveillance et Prestation de service

Le centre des opérations de sécurité ATA de Cisco (le SOC, ou SOC ATA) surveillera de manière proactive les principaux seuils et incidents liés à la sécurité au sein de l'infrastructure réseau du Client. La surveillance commencera à la suite de la présentation du dossier de la Transition; un paramétrage de la télémétrie (comme décrit dans la section 1.4.2) peut être envoyé à tout moment pendant la prestation de services.

En cas d'incidents de sécurité non détectés, le Client peut déclarer un Incident de sécurité en communiquant avec le SOC ATA et communiquer par téléphone tout incident de priorité élevée (panne du système, diminution des performances, etc.). Les incidents de faible priorité doivent être signalés au SOC via le Portail client (décrit à la section 1.4.2).

Lors de la détection automatique ou de la soumission manuelle d'un incident au SOC, un Billet d'incident est créé. Le SOC ATA est responsable en dernier ressort de la coordination de la gestion de l'incident, ce qui comprend la communication avec le Client tout au long du processus de gestion d'Incident. Cette communication comprend également la notification au Client du traitement ou de la résolution de l'incident.

1.4.1 Dossiers de surveillance et d'incidents

Cisco est responsable de la supervision de l'environnement, des systèmes et des données du Client, comme défini lors de la phase d'activation dans la classification des ressources et dans les définitions des priorités.

Les activités consistent principalement à surveiller et à analyser les données en provenance du réseau en corrélation avec les flux de données relatives aux menaces afin d'identifier les incidents de sécurité potentiels liés à la malveillance.

Responsabilités de Cisco :

- Créer des billets d'incident sur le Portail client.
- Classer chaque incident de sécurité par catégorie de sécurité. Les catégories sont basées sur une version modifiée des catégories d'incident US-CERT : http://www.us-cert.gov/government-users/reporting-requirements
- Attribuer à tous les incidents un niveau de priorité Élevé, Moyen ou Faible en fonction de critères multiples comme le type d'infection, la confirmation de l'incident ou la quantité de ressources concernées par l'incident. Les niveaux de priorités sont définis de la façon suivante.
  - Élevé : grave impact sur l'entreprise ou perte des données du Client
  - Moyen : effet négatif pour le Client, perte potentielle de données, perte potentielle de service
  - Faible : effet négatif minime pour le Client Pas de perte financière. Pas de perte de données.
- Aviser par voie électronique les interlocuteurs désignés par le Client au sujet des nouveaux incidents par le biais du Portail client.
- Fournir des recommandations d'atténuation selon leur disponibilité pour l'incident de sécurité associé.

Responsabilités du Client :

- Examiner les billets d'incidents sur le Portail client et fournir des détails pour la clôture des billets.
- Mettre en œuvre les techniques d'atténuation recommandées, le cas échéant.

1.4.2 Paramétrage de la télémétrie

Le Client peut également transmettre une télémétrie supplémentaire, convenue mutuellement par le Client et Cisco, vers le DCAP pour offrir une visibilité et un contexte réseau plus importants et avoir des enquêtes sur les incidents actifs plus efficaces.

La quantité de la télémétrie supplémentaire est limitée par les seuils originaux de télémétrie DCAP, comme définie dans l'aperçu des offres de service de base. Lorsque la quantité de données transmise au DCAP atteint les seuils de stockage indiqués, la télémétrie est redirigée avec la plus ancienne en cours de purge, permettant ainsi l'ouverture du stockage pour la télémétrie entrante. Le coffret complémentaire de stockage, comme décrit dans la section 2.3, peut être acheté si la conservation des renseignements supplémentaires est souhaitée.

La télémétrie provenant d'applications ou d'appareils spécialisés propres au Client peut nécessiter l'achat d'une option complémentaire de Demandes de développement avant d'être transmis par DCAP.

Responsabilités de Cisco :

- Collaborer avec le Client sur la découverte de périphérique réseau pour comprendre les rôles et les fonctions de ces derniers.
- Établir les priorités de la télémétrie en fonction de la valeur et de la surveillance des incidents de sécurité.
- Fournir des recommandations au Client sur tous les changements nécessaires afin de permettre l'envoi de télémétrie au DCAP.
- Valider la réception de la télémétrie approuvée au DCAP.

Responsabilités du Client :

- Fournir les renseignements nécessaires pour la découverte des périphériques réseau.
- Collaborer avec Cisco pour hiérarchiser les sources de télémétrie.
- Mettre en œuvre les changements recommandés sur les applications ou les appareils réseau applicables afin de permettre l'envoi de la télémétrie au DCAP.
- Collaborer avec Cisco pour assurer la bonne réception de la télémétrie par le DCAP.

1.4.3 Portail des clients

Le service ATA comprend un Portail client (le « Portail ») destiné à donner une visibilité à la prestation des services.

Durant la phase initiale de paramétrage, les Clients recevront des comptes permettant aux employés habilités d'accéder au Portail. Les consignes d'accès au Portail et les instructions de navigation seront fournies dans le cadre de la phase d'activation sous forme de vidéo, par le biais de WebEx ou sur site conformément à ce qui sera établi par Cisco.

Les renseignements contenus dans le Portail peuvent inclure les éléments suivants.

- Numéro identifiant le Billet d'incident : numéro de suivi attribué à chaque billet par le SOC ATA.
- Date et heure d'ouverture du Billet d'incident : moment auquel le billet a été ouvert.
- Description de Billet d'incident : résumé du ou des incidents décrits en détail dans le billet.
- Statut du Billet d'incident : statut actuel du billet selon la note la plus récente saisie dans le billet.

Responsabilités de Cisco :

- Fournir un accès au Client au Portail client dédié.
- Fournir des comptes pour le personnel autorisé du Client pour accéder au Portail.
- Fournir des instructions pour accéder au Portail et le parcourir. Les instructions seront fournies pendant la phase d'activation par vidéo, WebEx ou sur place tel que déterminé par Cisco.

Responsabilités du Client :

- Définir et mettre à jour la liste des utilisateurs autorisés avec le privilège de consulter le Portail client.
- Examiner les renseignements présentés dans le Portail.

1.4.4 Directeur des enquêtes désigné

Un Directeur des enquêtes avec des compétences approfondies en analyse et enquête sur les incidents sera nommé.

Ce Directeur des enquêtes sera responsable de ce qui suit :

- Répondre aux demandes du Client et aider à la résolution des incidents selon les besoins du Client
- Rester au fait de l'environnement du Client et faire part de tout changement ou de toute mise à jour au SOC ATA
- Étudier et suivre les tendances des sites clients

Responsabilités de Cisco :

- Nommer un Directeur des enquêtes pour assister le Client tout au long de la prestation des services

Responsabilités du Client :

- Fournir au Directeur des enquêtes les renseignements, la documentation ou les données de statut nécessaires, dans la mesure où ces éléments concernent les changements apportés à l'environnement réseau du Client dont Cisco assure la surveillance.

1.4.5 Recherche proactive des menaces (coffret Premier)

Pour les Clients ayant acquis le coffret Premier : Cisco effectuera des activités consistant à rechercher les activités malveillantes qui ne sont pas identifiées par les mécanismes d'alerte traditionnels.

Responsabilités de Cisco :

- Rechercher activement les attaques en mettant en pratique la connaissance des menaces actuelles et les renseignements associés à ces dernières.
- Documenter et mettre à jour un plan d'action permanent contenant une simulation de recherche des menaces propres à l'environnement du Client.
- Réaliser chaque simulation à la fréquence spécifique établie par Cisco. Créer un Billet d'incident et en établir la priorité si les résultats de la simulation mettent en évidence un Incident de sécurité tel que déterminé par Cisco.

Responsabilités du Client :

- Examiner les Billets d'incident créés par Cisco suite à une simulation menée de manière proactive.
- Mettre en œuvre les recommandations de correction ou d'atténuation, le cas échéant.

1.5 Examens du Client

Des examens trimestriels ou mensuels auront lieu pour établir un résumé de la collaboration et du travail déjà réalisé en matière d'ATA.

1.5.1 Examen trimestriel d'activité

Cisco et le Client mèneront un ou plusieurs Examens trimestriels d'activité. L'Examen trimestriel d'activité s'adresse aux dirigeants du Client dans les domaines des affaires et de la sécurité et offre une vue globale des résultats et de la valeur apportée par le service ATA.

Les activités et les éléments couverts par cet examen incluent :

- Un examen des Incidents signalés
- Une discussion sur les programmes potentiels d'atténuation ou de correction
- Un examen des principaux changements prévus ou effectués sur le réseau du Client

Responsabilités de Cisco :

- Fournir un Examen trimestriel d'activité : il peut durer jusqu'à quatre (4) heures sans documents imprimés ou exercices pratiques.
- Déterminer un format adéquat et un procédé de livraison pouvant inclure, notamment, l'utilisation d'un support partagé par Internet, par téléconférence ou sur site.

Responsabilités du Client :

- S'assurer que le personnel de direction concerné du Client pourra être présent à l'Examen trimestriel d'activité.
- Désigner au moins deux (2) représentants techniques de la sécurité et un (1) cadre commanditaire ou représentant approprié pour participer à l'Examen trimestriel d'activité.
- Examiner et fournir des commentaires au cours de la réunion d'Examen trimestriel d'activité.

1.5.2 Livraison de l'Examen technique mensuel (coffret Premier)

Pour les Clients du service Premier, un Examen technique mensuel facultatif peut être fourni. Cet examen technique peut avoir lieu tous les mois afin d'apporter une rétroaction réciproque et proposer des recommandations de programmes.

Les activités et les éléments couverts par l'Examen technique mensuel incluent :

- Un examen des Incidents signalés
- Une discussion sur les programmes potentiels d'atténuation ou de correction
- Un examen des principaux changements prévus ou effectués sur le réseau du Client

Responsabilités de Cisco :

- Fournir l'Examen technique mensuel : il peut durer jusqu'à une (1) heure sans documents imprimés ou exercices pratiques.
- Le procédé de livraison de l'Examen technique mensuel est distant (WebEx ou téléconférence).

Responsabilités du Client :

- Au besoin, s'assurer que l'équipe technique compétente du Client pourra être présente à l'Examen technique mensuel.
- Désigner un (1) représentant technique de la sécurité pour participer à l'Examen technique mensuel.
- Examiner et fournir des commentaires au cours de la réunion d'Examen technique mensuel.

2. Coffrets complémentaires ATA

2.1 Coffret complémentaire : système de capteurs ATA supplémentaire

Le coffret complémentaire de système de capteurs ATA supplémentaire donne une visibilité sur un segment supplémentaire du réseau du Client. Le système de capteurs ATA supplémentaire fournira des fonctions d'analyse de données réseau basique, prenant en charge les segments réseau à un débit allant jusqu'à 1 Gbps.

Chaque déploiement de système de capteurs ATA supplémentaire nécessite une unité DCAP déployée afin d'identifier et d'analyser la sortie des données venant du capteur. Pour le volet ATA Premier, le capteur inclut les fonctionnalités de capture intégrale de paquets et prend en charge jusqu'à 20 To de stockage. Pour le volet ATA Optimisé, le capteur ATA n'inclut pas les fonctionnalités de capture intégrale de paquets et prend en charge jusqu'à 10 To de stockage.

Responsabilités de Cisco :

- Obtenir et livrer les composants du système de capteurs ATA supplémentaire et les expédier au Client.
- Assister le Client lors de l'installation des composants et valider l'accessibilité de Cisco au système de capteurs ATA supplémentaire.
- Effectuer la maintenance entière requise pour le matériel ou le logiciel du système de capteurs ATA supplémentaire.

Responsabilités du Client :

- Installer les composants du système de capteurs ATA supplémentaire conformément aux indications de Cisco.
- Collaborer avec Cisco pour assurer l'assistance sur site afin de mettre en œuvre la maintenance nécessaire à l'emplacement physique et logique convenu (empilement, connexion réseau, alimentation, etc.).
- Permettre à Cisco ou à ses fournisseurs d'accéder aux sites du Client dans la mesure établie de manière raisonnable par Cisco en vue de l'inspection ou de la maintenance d'urgence de l'équipement sur site. L'absence d'accès permis en temps opportun peut infirmer la prestation des services et retarder leur rétablissement et leur exécution.
- Fournir à Cisco un accès au site ou une assistance pour la maintenance matérielle requise.
- Fournir les éléments suivants pour le déploiement du système de capteurs ATA supplémentaire :
  - Une adresse IP non NAT acheminée publiquement et un accès réseau avec bande passante Internet d'au moins 10 Mbit/s pour le routeur RPV afin d'établir une connexion sécurisée à Cisco.
  - Un espace physique, une sûreté physique, une alimentation électrique, un système de refroidissement et des conditions environnementales convenables nécessaires pour l'exploitation informatique des équipements sur site.
- Maintenir le système de capteurs ATA supplémentaire en bon état de fonctionnement et retourner à Cisco les équipements en état de fonctionnement immédiatement après la résiliation ou l'expiration de la Durée.

2.2 Coffret complémentaire : débit étendu pour le capteur ATA

Pour les cas de chaque système de capteurs ATA (inclus dans l'offre du service de base ou acheté en tant qu'option complémentaire comme décrit dans la section 2.1), le débit pris en charge par le segment de réseau suivi peut être augmenté par incréments de 3 Gbps, avec l'achat de l'option supplémentaire de débit étendu pour capteur ATA (« extension de capteur »). L'extension de capteur permet également d'obtenir 40 To de stockage supplémentaire sur un capteur.

Responsabilités de Cisco :

- Obtenir et livrer les composants d'extension de capteur pour augmenter la prise en charge du débit du système de capteurs ATA.
- Aider à l'installation des composants d'extension de capteur.
- Effectuer la maintenance entière requise pour le matériel ou le logiciel de l'extension de capteur.

Responsabilités du Client :

- Installer les composants d'extension conformément aux indications de Cisco.
- Collaborer avec Cisco pour assurer l'assistance sur site afin de mettre en œuvre la maintenance nécessaire à l'emplacement physique et logique convenu (empilement, connexion réseau, alimentation, etc.).
- Permettre à Cisco ou à ses fournisseurs d'accéder aux sites du Client dans la mesure établie de manière raisonnable par Cisco en vue de l'inspection ou de la maintenance d'urgence de l'équipement sur site. L'absence d'accès permis en temps opportun peut infirmer la prestation des services et retarder leur rétablissement et leur exécution.
- Fournir à Cisco un accès au site ou une assistance pour la maintenance matérielle requise.
- Maintenir les composants d'extension en bon état de fonctionnement et retourner à Cisco les équipements en état de fonctionnement immédiatement après la résiliation ou l'expiration de la Durée.

2.3 Coffret complémentaire : extension de stockage

Le Client a la possibilité d'acheter une extension de stockage (« stockage supplémentaire ») pour augmenter la capacité de stockage du DCAP, par incréments de 400 To.

Responsabilités de Cisco :

- Obtenir et livrer l'équipement supplémentaire pour augmenter le support de stockage.
- Aider à l'installation des composants du stockage supplémentaire.
- Effectuer la maintenance entière requise pour le matériel ou le logiciel pour le stockage supplémentaire.

Responsabilités du Client :

- Installer les composants du stockage supplémentaire conformément aux indications de Cisco.
- Collaborer avec Cisco pour assurer l'assistance sur site afin de mettre en œuvre la maintenance nécessaire à l'emplacement physique et logique convenu (empilement, connexion réseau, alimentation, etc.).
- Permettre à Cisco ou à ses fournisseurs d'accéder aux sites du Client dans la mesure établie de manière raisonnable par Cisco en vue de l'inspection ou de la maintenance d'urgence de l'équipement sur site.
- Fournir à Cisco un accès au site ou une assistance pour la maintenance matérielle requise.
- Maintenir les composants du stockage supplémentaire en bon état de fonctionnement et retourner à Cisco les équipements en état de fonctionnement immédiatement après la résiliation ou l'expiration de la Durée.

2.4 Coffret complémentaire : demandes de développement

Le Client peut demander un ou plusieurs efforts de développement de la solution, comme les rapports personnalisés et l'ingestion de ressources, la télémétrie de périphériques propres au Client, qui peuvent être approuvés et fournis par Cisco. Cisco a classé ces demandes de développement en fonction du niveau de complexité requis pour mettre en œuvre la demande.

Type	Complexité	Items (articles)
Type 1	Faible	• Intégration d'un flux unique de télémétrie syslog depuis un périphérique spécifique du Client • Rapport automatisé statique unique • Détection d'une anomalie statistique pour une source unique de données
Type 2	Moyen	• Ingestion de données de renseignement appartenant au Client (par exemple, la base de données d'actifs) • Rapport automatisé enrichi et unique
Type 3	Élevé	• Détection d'une anomalie statistique sur les données corrélées (plusieurs sources de données) • Intégration avancée pour un périphérique spécialisé (nécessite par exemple un agent personnalisé pour extraire les données)

Responsabilités de Cisco :

- Confirmer et approuver la capacité à fournir les demandes de développement reçues du Client.
- Recueillir et documenter les exigences du Client pour chaque demande de développement.
- Mettre en œuvre et fournir la personnalisation conformément au document relatif aux exigences sur la demande de développement.

Responsabilités du Client :

- Fournir à Cisco les conditions de la demande de développement.
- Examiner et valider la documentation sur les exigences de Cisco avant la mise en œuvre de la demande personnalisée.

ANNEXE : Glossaire

Glossaire à consulter pour lire la présente description de service. Les termes en lettres capitales non définis autrement ci-dessus et utilisés dans ce document revêtent la signification présentée dans le Glossaire.

ATA : analyses des menaces actives.

Billets d'incidents : rapport énuméré contenant les détails d'un Incident de sécurité détecté par le SOC et nécessitant l'attention du Client.

Capteur : ensemble de l'équipement de sécurité appartenant à Cisco, situé sur le site physique du Client, qui est chargé de l'analyse des données du réseau en surveillant passivement un segment défini du réseau Client. Pour le volet ATA Premier, le capteur inclut les fonctionnalités de capture intégrale de paquets.

Client : entité qui achète les Services pour sa propre utilisation interne.

Directeur des enquêtes : spécialiste en ingénierie de la sécurité affecté au Client et disposant de solides compétences en matière d'analyses et d'enquêtes; il est chargé de répondre aux requêtes du Client et de rester au fait de l'environnement du Client.

Durée : durée du service ATA acheté par le Client.

Extension de capteur : option complémentaire ATA, débit étendu pour le capteur ATA.

Événement de sécurité : cas identifié d'un état d'un système, d'un service ou d'un réseau indiquant une faille possible de la politique de sécurité de l'information ou une défaillance des contrôles, ou une situation précédemment inconnue et susceptible de concerner la sécurité (ISO 27035).

Incident de sécurité ou **Incident :** événement unique ou série d'événements indésirables ou inattendus en matière de sécurité de l'information, présentant une probabilité importante de compromettre les opérations commerciales et de menacer la sécurité de l'information (ISO 27035).

ISO : Organisation internationale de normalisation.

Locaux du Client : emplacement physique du Client où se trouve l'unité DCAP.

NCE : spécialiste en ingénierie conseil réseau (« Network Consulting Engineer »).

NetFlow : protocole réseau utilisé par des périphériques réseau pour caractériser le fonctionnement du réseau et surveiller le trafic IP.

Portail client : application Web fournie au Client par Cisco qui détaille la visibilité sur le service ATA, en incluant notamment des rapports et des billets d'incidents.

Posture de réaction : politique documentée qui décrit comment la structure du Client réagit et fait face aux incidents. La posture de réaction devrait s'aligner avec la législation du pays, de l'état ou de la région et avec toutes les réglementations auxquelles l'organisation est astreinte.

SOC : centre des opérations de sécurité (« Security Operations Center »).

Télémétrie : renseignements ou données qui permettent une prise de conscience et une visibilité sur ce qui se produit sur le réseau à un moment donné sur des périphériques réseau, des dispositifs, des applications et des serveurs, dans lesquels la principale fonction du dispositif ne consiste pas à générer des alertes de sécurité conçues pour détecter une activité malveillante ou indésirable sur les réseaux informatiques.

Télémétrie (brute) : télémétrie non compressée constituée d'environ 90 % de données texte.

Terminal de collecte et d'analyse de données ou DCAP : ensemble de l'équipement de réseau de sécurité et de surveillance appartenant à Cisco, situé sur le site physique du Client, qui est chargé de la collecte, du regroupement et de l'analyse de la télémétrie à partir des capteurs et/ou des dispositifs de sécurité et des applications du Client.