<<Service Description: Cisco Active Threat Analytics-Premier>>

Description de service : Analyses des menaces de Cisco – Premium

Ce document décrit les services de sécurité des Analyses des menaces actives de Cisco (les « Services »).

Documents connexes : Ce document devrait être lu de pair avec les documents suivants, également publiés sur le site 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 ont le sens qui leur est attribué dans le Glossaire.

Vente directe par Cisco. Si vous vous êtes procuré ces Services directement auprès de Cisco, ce document est inclus dans votre contrat de services cadres (MSA), dans votre contrat de services avancés (ASA) ou dans votre contrat de services équivalent conclu entre vous et Cisco (le Contrat). Si vous n'avez aucun contrat établi auprès de Cisco, les modalités suivantes feront foi de contrat : http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/Advanced_Services_Click-to-Accept_Agreement_sample.pdf

Si leur contenu n'est pas déjà couvert dans votre contrat, ce document doit être lu de pair avec les documents mentionnés ci-dessus. En cas de conflit entre la présente Description de service et votre contrat MSA (ou contrat de service équivalent), cette Description de service fait foi.

Vente par un revendeur agréé Cisco. Si vous avez acquis ces services par l'intermédiaire d'un revendeur agréé de Cisco, ce document sert à titre descriptif seulement. Il ne s'agit pas d'un contrat établi entre Cisco et vous. Le contrat, le cas échéant, qui régit la prestation de ce Service est celui qui prévaut entre vous et votre Revendeur agréé. 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 http://www.cisco.com/ca/aller/descriptionsduservice/.

Cisco fournira les services de sécurité d'analyses des menaces actives (ATA) décrits ci-dessous en fonction des éléments sélectionnés et décrits dans le bon de commande pour lequel Cisco a reçu le paiement convenu. Cisco fournira une soumission, une commande de service, un énoncé des travaux ou un document similaire (la Soumission) qui établit la portée des Services et la période durant laquelle Cisco fournira ces Services. Cisco recevra un bon de commande qui renvoie à la Soumission conclue entre les parties et qui reconnaît et accepte également les modalités énoncées dans la présente. Toute autre modalité de bon de commande sera considérée comme rejetée.

Résumé du Service

Cette description de service est conçue pour fournir au client une compréhension de base des activités, des livrables et de la prestation de service que Cisco utilise pour fournir l'analyse des menaces actives.

Cisco peut recueillir des données concernant votre utilisation des services et les menaces ou menaces possibles à l'encontre de votre environnement ou votre réseau et des services (les « Données de télémesure ») afin de maintenir, d'améliorer ou de promouvoir les Services. Vous reconnaissez que Cisco peut utiliser gratuitement les données de télémesure, puisqu'elles se trouvent sous une forme qui n'identifie ni n'implique les clients ou les utilisateurs finaux clients. Quoi qu'il en soit, Cisco respectera en tout temps les lois applicables à la collecte et à l'utilisation des Données de télémesure et utilisera des moyens physiques, techniques et procéduraux raisonnables pour protéger les Données de télémesure conformément à sa politique de confidentialité disponible ici : http://www.cisco.com/c/en/us/about/trust-transparency-center/overview.html

L'ATA de Cisco peut comprendre les offres suivantes, selon les sélections et les descriptions du bon de commande.

L'offre de service de base d'ATA de Cisco peut être achetée de pair avec les coffrets complémentaires ATA indiqués ci-dessous.

Offres de service de base : ATA Premium

ATA Premium :

- Une (1) instance de dispositif de collecte et d'analyse de données (DCAP) locale qui prend en charge jusqu'à 250 000 événements par seconde (EPS) en continu (400 000 EPS en crête) et un stockage de roulement de 400 To de télémesure brute
- Une (1) instance de système de capteurs ATA sur site avec une fonction de saisie intégrale des paquets
- Une (1) option complémentaire de débit étendu pour le capteur ATA afin d'offrir la prise en charge d'un débit total de 4 Gbit/s dans les capteurs et un stockage de 60 To
- L'analyse des renseignements sur les menaces
- L'extraction des métadonnées
- Analyse avancée
- Jusqu'à 15 licences d'utilisateur pour accéder au portail client
- Directeur des enquêtes
- Recherche proactive des menaces
- Service de conservation des réponses aux incidents
- Examen trimestriel d'activité
- Exposé technique mensuel

Coffrets d'options complémentaires des offres de service de base

Les coffrets complémentaires ATA peuvent seulement être obtenus pour accompagner une des offres de service de base d'analyse des menaces actives.

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

- Déployez une instance supplémentaire de système de capteurs ATA qui prend en charge un débit allant jusqu'à 1 Gbit/s.
- Tout système de capteurs ATA supplémentaire nécessite une connexion à un déploiement de DCAP afin de recueillir et d'analyser des données sortant du système de capteurs. Il n'est pas possible de se procurer un système en tant qu'option complémentaire autonome.
- Le système de capteurs ATA comprend des fonctionnalités complètes de saisie de paquets et prend en charge une capacité de stockage allant jusqu'à 20 To.

Coffret complémentaire : **débit étendu pour le système de capteurs ATA** :

- Augmentez le débit d'une instance de système de capteurs ATA unique existante –offert en écarts de 3 Gbit/s de débit supplémentaire jusqu'à 16 Gbit/s pour l'ensemble du système de capteurs.
- Chaque coffret complémentaire de débit étendu pour le système de capteurs ATA offre 40 To de capacité de stockage supplémentaire au déploiement du système.
- On peut seulement l'ajouter à un déploiement de système de capteurs ATA existant acheté dans le cadre d'un coffret de base ATA ou en tant que coffret supplémentaire de système de capteurs ATA.

Option complémentaire ATA –**Extension de stockage**

- Augmentez la capacité de stockage du DCAP ou des capteurs afin de permettre la saisie de données d'enquête supplémentaires : offert en écarts de 400 To de télémesure brute*.

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

- Mettez en œuvre des demandes de développement concernant la solution ATA, comme des rapports adaptés ou l'intégration de télémesure supplémentaire des appareils. Ces demandes seront documentées dans la Soumission ou dans une Demande de modification ajoutée à la présente description de service

Option complémentaire ATA –**Licences supplémentaires d'accès d'utilisateur au portail client :**

- Augmentez le nombre de licences d'utilisateur d'accès au portail client au-delà de ce qui est prévu dans le Service.

L'achat de coffrets complémentaires peut exiger que Cisco envoie de l'équipement supplémentaire sous sa propriété afin que le Client effectue une installation à son emplacement.

Cisco fournira seulement le soutien relatif aux offres d'analyse des menaces actives sélectionnées dans le bon de commande.

1. Analyses des menaces actives de Cisco

Les analyses des menaces actives de Cisco offrent une surveillance de sécurité à distance à l'aide de métadonnées de paquets et de techniques de détection de comportement sur le réseau faisant appel à une grande variété de flux de renseignements sur la sécurité pendant l'ensemble de la durée afin de déceler les incidents et événements liés à la sécurité et d'intervenir rapidement.

La durée des services commence au début de la surveillance et la prestation de service (section 1.4) ou huit (8) semaines après le début du lancement (section 1.1), selon la première éventualité.

La prestation des services d'ATA se réalisera en quatre (4) étapes, selon ce qui est décrit dans le présent document.

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

1.1 Lancement

1.1.1 Gestion de projets

Cisco assignera un Gestionnaire de projet (désigne ci-dessous) dont le rôle consistera à servir d'interlocuteur unique. Cisco collaborera avec le Client pour concevoir un plan de projet complet, de gérer la main-d'œuvre et les processus de Cisco afin de fournir les Services et de veiller à ce que ces services soient fournis conformément au plan.

Responsabilités de Cisco

- Mettre à disposition un interlocuteur unique (le Gestionnaire de projet) pour traiter de toutes les questions relatives aux Services d'ATA fournis dans le cadre de la présente description de 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 avec le Client régulièrement organisées afin de discuter de l'état du service et de relever et documenter les besoins, les risques et les enjeux associés à la prestation des services.
- Agir à titre d'interlocuteur principal pour les procédures de gestion du changement.

Responsabilités du Client

- Désigner un interlocuteur de Cisco (CPOC) à qui on transmettra toutes les communications de Cisco et qui aura l'autorité d'intervenir dans tous les aspects quotidiens des Services.
- Désigner un remplaçant ou un assistant à l'interlocuteur en cas d'indisponibilité de l'interlocuteur principal.
- Participer aux réunions d'analyse du projet ou aux conférences téléphoniques régulièrement organisées.
- Réviser avec Cisco le calendrier du projet, les objectifs, les services, ainsi que les rôles et responsabilités.
- Désigner un parrain de projet ainsi que des parties prenantes majeures et définir leurs rôles dans le soutien de ce projet.
- Collaborer avec le gestionnaire de projet de Cisco afin de veiller à ce que le parrain de projet du Client, les parties prenantes majeures et tous les membres de l'équipe du projet reçoivent les communications liées au projet et participent aux séances de communication organisées régulièrement.
- Collaborer avec Cisco afin de planifier la réunion de lancement et transmettre l'ordre du jour de la réunion aux parties prenantes désignées par le Client.
- Fournir les renseignements et les documents exigés par Cisco en temps opportun afin de respecter les échéanciers du projet.
- Aviser Cisco de toute mise à niveau de matériel ou de logiciel qui pourrait être liée à la prestation de service ou de tout autre changement
- au sein du réseau du Client qui pourrait avoir une incidence sur la prestation des Services au moins dix (10) jours avant une telle mise à niveau.
- Aviser Cisco de toute autre activité de mise en œuvre qui pourrait avoir un effet sur les Services au moins dix (10) jours avant l'activité prévue.
- Aviser Cisco de toute modification au calendrier d'installation au moins 72 heures avant la date d'installation prévue à l'origine.
- Aviser Cisco de toute autre modification d'échéance liée à la présente modalité au moins dix (10) jours ouvrables avant l'activité prévue.
- Préparer les installations et les accès nécessaires en vue des réunions sur le site (comme les badges ou les accès de visiteurs, les salles de conférence, les projecteurs et les ponts de conférence).
- Effectuer toute autre tâche convenue par écrit dans le cadre du plan de projet.

1.1.2 Lancement

Le gestionnaire de projet communiquera avec le CPOC afin de planifier la réunion de lancement dans les 45 jours suivant la réception d'un bon de commande valide. La réunion de lancement a généralement lieu par conférence téléphonique où on traite des détails sur le contrat exécuté. Un partenaire de Cisco peut faire partie de l'appel. Le gestionnaire de projet, en collaboration avec les ingénieurs de Cisco affectés au compte client, participe généralement à l'étape du lancement.

Responsabilités de Cisco

- Tenir des ateliers à distance (de Cisco ou de WebEx) afin de réviser les activités liées à l'activation et les services achetés tels qu'ils sont mentionnés dans le bon de commande.

Responsabilités du Client

- Désigner des personnes-ressources clés et un personnel autorisé nécessaires pour la tenue de la réunion de lancement et communiquer avec le Gestionnaire de projet afin de faciliter et d'organiser la réunion de lancement.
- Fournir les renseignements nécessaires pour planifier les mesures d'activation.

1.2 Activation

L'activation est essentiellement une étape de collecte de renseignements qui sert de fondement à la prestation du service d'ATA. Elle comprend également la livraison et l'installation des DCAP et du système de capteurs ATA (l'équipement local) prévues dans le cadre du service d'ATA, comme l'indique le bon de commande.

1.2.1 Collecte de renseignements

Afin de gérer avec efficacité le cycle de vie d'un incident lié à la sécurité, Cisco doit comprendre entièrement l'environnement du Client et les flux de travaux de sécurité. Durant l'étape de l'activation, la collecte de renseignements se fera principalement à distance par l'intermédiaire de réunions WebEx avec les principaux membres du personnel du client et les principales parties prenantes.

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 de base
- Les documents de classification et de hiérarchisation des ressources
- Les documents et politiques actuels qui traitent du trafic réseau normal et accepté nécessaires pour configurer l'équipement local

- Des rapports de repérage des vulnérabilités qui fournissent des détails comme l'écoute des ports, les versions des services et les bases de références des vulnérabilités à moment précis qui sont associées aux ressources essentielles comme les serveurs et les applications logicielles.
- Les plans technologiques futurs

Responsabilités de Cisco :

- Planifier et coordonner des rencontres de collecte de renseignements à distance avec le Client afin de recueillir l'information nécessaire.
- Réviser les renseignements fournis par le Client en relevant les lacunes d'information et en indiquant toute mesure corrective à laquelle le Client doit prendre part.
- Examiner les situations et les emplacements dans le réseau où une saisie complète des paquets ne sera pas permise. Configurer adéquatement l'équipement sur place afin de respecter les exigences écrites et convenues avec le Client.

Responsabilités du Client

- S'assurer que les experts en la matière du Client participent aux ateliers de collecte de renseignements et fournissent les renseignements nécessaires.
- Fournir à Cisco les documents et ressources nécessaires sur demande afin de réviser les renseignements avant et pendant les ateliers.
- Fournir un recensement des réseaux IP et des schémas IP existants. Si aucun recensement n'existe, le Client a la responsabilité de collaborer avec Cisco afin de créer une carte topologique à l'aide d'outils d'investigation et de balayage.
- Fournir une liste de personnes-ressources, y compris leurs descriptions de tâches, leurs rôles et leurs responsabilités tel que nécessaire pour la gestion et la signalisation progressive des incidents.
- Fournir à Cisco des rapports trimestriels de service et de balayage des vulnérabilités pour les appareils pertinents, si ces rapports sont disponibles.
- Collaborer avec Cisco afin d'examiner les documents et les renseignements obtenus, et aider les ingénieurs-conseils réseau à documenter l'identification, la classification et la priorité des systèmes et données essentiels.
- Relever les situations et les emplacements dans le réseau où une saisie complète des paquets ne serait pas permise et fournir cette information à Cisco.
- Fournir tout renseignement complémentaire demandé par Cisco. Collaborer avec Cisco à élaborer des modèles de conception et de configuration détaillés en fournissant des renseignements et des commentaires.

1.2.2 Installation de l'équipement sur site

Cisco enverra les DCAP et les capteurs que le Client devra installer dans les 8 semaines suivant la réunion de lancement. Les détails de livraison doivent être confirmés auprès du Client au préalable.

L'équipement sur site doit être installé à un emplacement physique ou logique convenu d'un commun accord. Il restera sur le site du Client pendant toute la durée du contrat de service d'ATA acheté.

Les droits sur l'équipement sur site restent la propriété de Cisco. Cisco s'attend à ce qu'au moment de sa désinstallation, l'équipement soit dans la même condition qu'au moment de son l'installation, à l'exception de l'usure normale. Le Client devra rembourser Cisco pour tous les coûts liés à la perte, à l'endommagement ou au vol de l'équipement, sur site, à moins que Cisco en soit responsable.

Un formulaire de suivi des ressources sera fourni au client afin de valider la livraison de l'équipement sur site. Ce formulaire comprendra les détails suivants par rapport à l'équipement de Cisco installé sur le site du Client : 1) une liste détaillée des descriptions et des numéros de produit, y compris les numéros de série; 2) l'adresse physique où l'équipement sera placé; 3) le numéro de bon de commande du service correspondant acheté par le Client.

Au moment choisi par Cisco et le Gestionnaire de projet, un ingénieur-conseil réseau peut voyager sur le site afin de fournir une assistance durant l'installation et l'essai de l'équipement sur site.

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

- Routeur RPV
- Branchement/commutateur réseau passif
- Moteur(s) d'analyse de l'information
- Composants de stockage de données

Responsabilités de Cisco

- Livrer tous les dispositifs, les serveurs, les appareils et les applications de soutien sur place.
- 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 durant le soutien sur le site afin de mettre en œuvre la maintenance nécessaire au lieu physique ou logique convenu, comme la fixation, la connexion au réseau et l'alimentation.
- Permettre à Cisco ou à ses sous-traitants d'accéder au site du Client autant que Cisco le juge raisonnable afin d'inspecter ou d'effectuer l'entretien d'urgence de l'équipement sur place. L'omission de fournir un accès en temps opportun peut invalider la prestation de service et retarder la restauration et l'exécution des services.
- 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 sans NAT routée publiquement et un accès réseau d'une bande passante d'au moins 10 Mbit/s pour le routeur RPV afin d'établir une connexion sécurisée avec Cisco.
    - Remplir les exigences et les conditions liées au réseau nécessaires afin de permettre une communication bilatérale entre les unités de DCAP et les capteurs correspondants, au besoin.
- Remplir le formulaire de suivi des ressources lié à l'équipement sur site et le retourner à Cisco.
- Remplir les conditions d'espace, de connectivité et d'environnement nécessaires pour l'équipement sur site (p. ex. alimentation, climatisation, etc.) et maintenir cet équipement en état de marche. Le Client ne doit pas réaménager, débrancher, désinstaller, essayer de réparer, ou modifier de toute autre façon l'équipement sur site ni laisser d'autres le faire. S'il le fait sans avoir reçu l'approbation préalable de Cisco, le Client devra rembourser Cisco pour les coûts de réparation ou de remplacement de tout équipement endommagé. En aucun cas Cisco ne sera tenu responsable envers le Client ou envers toute autre partie pour l'interruption du service, la perte, les coûts et les dommages découlant d'une utilisation ou d'un entretien inapproprié de l'équipement sur site.
- À la fin du Contrat, retourner immédiatement l'équipement sur site à Cisco en état de marche. Une usure normale sera tolérée.

1.3 Transition

Une fois l'étape d'activation terminée, Cisco enverra un dossier de la transition au Client. Cisco indiquera un format et une méthode de livraison appropriés (selon l'ampleur et la complexité du projet), que ce soit par Internet, téléconférence, courriel, vidéoconférence ou sur le site.

Dans le dossier de la transition, on peut entre autres :

- Traiter des réussites et des difficultés au cours de l'activation afin de réviser le processus de signalisation progressive des incidents.
- Réviser les recommandations d'utilisation d'ATA relevées durant l'activation, le cas échéant.

Une fois le dossier de la transition terminé, la surveillance et la gestion des incidents seront confiées au centre des opérations de sécurité (SOC), comme le décrit la section 1.4. De plus, la facturation pour le service d'ATA commencera aussitôt que le dossier est terminé.

Responsabilités de Cisco :

- Offrir au Client une séance consacrée au dossier de la transition une fois l'étape d'activation terminée.

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 (SOC) d'ATA surveillera en amont les incidents de sécurité et leurs seuils au sein de l'infrastructure réseau du Client. La surveillance commencera après le dossier de la Transition. Le paramétrage de la télémétrie (décrit à la section 1.4.3) peut être fourni à n'importe quel moment durant la prestation des services.

Lorsque des incidents de sécurité ne sont pas détectés, le Client peut les déclarer en communiquant avec le SOC d'ATA et lui téléphoner pour relever tout incident de haute priorité (panne de système, performance dégradée, etc.). Les incidents de priorité inférieure doivent être signalés au SOC à partir du portail client (décrit à la section 1.4.3).

Lorsqu'un incident est transmis au SOC par détection automatique ou par soumission manuelle, un dossier correspondant est créé. Le SOC d'ATA aidera à la coordonner la gestion de l'incident, ce qui comprend la communication avec le Client durant le processus. Cette communication consiste également à indiquer au Client que l'incident a été résolu.

1.4.1 Dossiers de surveillance et d'incidents

Cisco a la responsabilité de surveiller l'infrastructure réseau du client couverte par la portée du Contrat conformément à ce qui a été défini durant les exercices de collecte de renseignements dans le cadre de l'étape d'activation.

Les activités de surveillance consistent à surveiller et à analyser le réseau en fonction des flux de données et de vigie des menaces afin de relever des incidents malveillants liés à la sécurité.

Responsabilités de Cisco :

- Créer des dossiers dans le portail client afin de répondre à un incident lié à la sécurité découvert ou signalé.
- Classer chaque incident de sécurité par catégorie de sécurité. Les catégories sont fondées sur une version modifiée des catégories d'incident US-CERT : http://www.us-cert.gov/government-users/reporting-requirements
- Catégoriser tous les incidents selon les priorités Élevée, Moyenne ou Faible en fonction de divers critères comme le type d'infection, la confirmation de l'incident ou le nombre de ressources touchées par l'incident. Les niveaux de priorités sont définis de la façon suivante.
    - Élevée : effet commercial critique ou perte de données importante pour le Client.
    - Moyenne : effet négatif pour le Client, perte de données possiblement importante, perte possible du service.
    - Faible : effet négatif minime pour le Client Aucune perte financière. Perte de données minimale, sinon aucune.
- 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 dossiers dans le portail et fournir des détails sur la fermeture des dossiers.
- Mettre en œuvre les techniques d'atténuation recommandées, le cas échéant.

1.4.2 Paramétrage de la télémétrie

En fonction d'un accord mutuel entre le Client et Cisco, le Client peut également envoyer une télémesure supplémentaire des DCAP afin d'offrir une plus grande visibilité du réseau et un contexte aux enquêtes d'incidents de sécurité actives.

La portée de télémesure supplémentaire se limite aux seuils de télémesure de DCAP originaux, comme ils sont décrits dans le résumé des offres de services. Lorsque la quantité de données intégrées par le DCAP atteint les seuils de stockage indiqués, la télémesure retenue est la plus ancienne à être purgée en vue du stockage de la télémesure à venir. Pour obtenir un plus grand stockage de données, il est possible d'acheter le coffret complémentaire d'extension de stockage décrit à la section 2.3.

La télémesure provenant des applications ou des appareils spécialisés du Client peut nécessiter l'achat d'un coffret complémentaire de demande de développement avant d'être intégrée au 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 télémesure en fonction de l'incidence sur la surveillance des incidents de sécurité.
- Fournir des recommandations au Client concernant toute modification nécessaire afin de permettre l'envoi de télémesure 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 modifications recommandées pour les applications ou les appareils de réseaux appropriés afin de permettre l'envoi de la télémesure au DCAP.
- Collaborer avec Cisco pour assurer la bonne réception de la télémétrie par le DCAP.

1.4.3 Portail client

Le service d'ATA comprend un portail client (le Portail) qui offrira une visibilité à la prestation du service. Durant l'étape initiale de paramétrage, les Clients recevront jusqu'à 15 comptes d'utilisateur afin que les employés autorisés puissent accéder au Portail. Les instructions d'accès au Portail et de navigation dans celui-ci seront fournies dans le cadre de l'étape d'activation par vidéo, WebEx ou visite sur le site, selon ce que Cisco a déterminé.

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

- Numéro d'identification de dossier (ou numéro de ticket) : le numéro attribué à chaque dossier par le SOC d'ATA.
- Date et heure d'ouverture de dossier : le moment où le dossier a été ouvert.
- Description du dossier : une courte description des incidents compris dans le dossier.
- État du dossier : l'état actuel dossier déterminé par la plus récente note ajoutée dans celui-ci.

Responsabilités de Cisco :

- Fournir à un maximum de 15 utilisateurs du Client un accès au portail client (et plus si le Client achète d'autres accès).
- Fournir aux membres du personnel habilités par le Client des comptes d'accès au Portail.
- Fournir des instructions pour accéder au Portail et le parcourir. Les instructions seront fournies durant l'étape d'activation par vidéo, WebEx ou visite sur le site, au choix de 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.
- Gérer et sécuriser les authentifants d'accès au Portail.

1.4.4 Directeur des enquêtes désigné

Un directeur des enquêtes désigné sera nommé. Il disposera de solides compétences en matière d'analyses et d'enquêtes sur les incidents.

Ce Directeur des enquêtes sera responsable de ce qui suit :

- Répondre aux demandes du Client et participer à la résolution des incidents de sécurité, selon les besoins du Client.
- Rester au fait de l'environnement du Client et aviser le SOC d'ATA toute modification et mise à jour.
- Étudier et suivre les tendances des sites clients.

Responsabilités de Cisco :

- Nommer un Directeur des enquêtes chargé d'accompagner le Client tout au long de la prestation de service.

Responsabilités du Client :

- Transmettre au directeur des enquêtes les renseignements, les documents et les états nécessaires en ce qui concerne les modifications à l'environnement du réseau du Client surveillé par Cisco.

1.4.5 Recherche proactive des menaces

Cisco mènera des activités qui demanderont la recherche des activités malveillantes au sein du réseau qui ne sont pas détectés par les mécanismes d'alerte traditionnels.

Responsabilités de Cisco :

- Rechercher activement des attaques en appliquant une connaissance actuelle et courante des menaces et des renseignements relatifs à ces menaces.
- Documenter et mettre à jour un plan d'action qui indique des « actions » à entreprendre pour rechercher des menaces propres à l'environnement du Client.
- Réaliser chaque action à la fréquence spécifique établie par Cisco. Créer et hiérarchiser un dossier si le résultat de l'action démontre une preuve d'incident de sécurité telle que définie par Cisco.

Responsabilités du Client :

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

1.5 Service de conservation des réponses aux incidents

Dans le cadre du service de conservation, Cisco peut fournir une partie ou la totalité des livrables de gestion des incidents suivants : a) une évaluation de la disponibilité, b) le développement du plan de gestion des incidents, c) des exercices sur table, d) la gestion proactive des menaces et e) la gestion des incidents d'urgence, notamment, le tri, la coordination, l'enquête, la retenue et la correction (pour voir lune définition de chaque livrable, consultez le glossaire), le tout pour un total de 160 heures par personne.

Limites : en raison de la diversité des situations et des problèmes que Cisco peut rencontrer, la gestion des incidents peut nécessiter l'utilisation de différents services en compléments du présent service. Par exemple, les incidents peuvent nécessiter l'utilisation d'outils spécialisés pour améliorer la visibilité et l'accès au réseau. Avant que Cisco puisse fournir un Service ou utiliser un outil supplémentaire qui nécessitera des frais additionnels, un accord écrit par l'intermédiaire d'une commande de modification devra être conclu.

Autres limitations possibles :

- Il n'est pas garanti que l'analyse de la cause première permettra de déterminer ou de confirmer la cause fondamentale d'un incident
- Des efforts raisonnables seront déployés afin de fournir des résultats concluants et un plan de résolution des problèmes.
- Les services de Gestion des incidents peuvent donner un aperçu des défaillances d'une stratégie de gestion des incidents et fournir un plan de résolution. Toutefois, l'exécution du plan peut nécessiter des services de suivi qui ne sont pas prévus dans le présent Service.
- 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 Security IR inclut :

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

Responsabilités de Cisco :

- Collaborer avec le Client pour définir comment exploiter les heures d'abonnement.
- Fournir l'accès aux services de gestion des incidents pendant la période d'abonnement.
- Mettre à disposition une ressource de gestion des incidents à distance par téléphone dans un délai de 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.

Responsabilités du client :

- Désigner l'interlocuteur ou les interlocuteurs de Cisco au sein de l'entreprise.
- Fournir des autorisations suffisantes à Cisco afin qu'elle puisse accéder aux périphériques réseau et aux périphériques de sécurité du Client et de façon électronique et physique apporter ainsi son aide.
- Garantir l'accès aux renseignements sur la stratégie de réponse aux incidents afin de mettre les processus et flux de travail à la disposition de Cisco.
- Faire le suivi et assurer la gestion des tâches demandées.

1.6 Examens du Client

On organisera des examens trimestriels ou mensuels afin de faire le point sur la collaboration et le travail accompli en matière d'ATA à ce jour.

1.6.1 Examen trimestriel d'activité

Cisco et le Client mèneront un ou plusieurs Examens trimestriels d'activité. Le QBR concerne les chefs d'affaires et de sécurité du Client afin de fournir une vue d'ensemble des résultats et de la valeur apportés par le service d'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 :

- Mener un examen trimestriel d'activité : il peut durer jusqu'à 4 heures et ne doit pas comporter de laboratoire ni de documents imprimés.
- Déterminer un format et une méthode de livraison appropriés, qui peuvent entre autres comprendre l'utilisation d'un support partagé sur Internet, par téléconférence ou sur les lieux.

Responsabilités du Client :

- S'assurer que le personnel de direction approprié est disponible pour participer à l'Examen trimestriel d'activité.
- Désigner au moins 2 représentants de la sécurité appropriés et 1 cadre responsable ou proxy approprié qui participeront à l'Examen trimestriel d'activité.
- Examiner et fournir des commentaires au cours de la réunion d'Examen trimestriel d'activité.

1.6.2 Examen technique mensuel : livraison

Un examen technique mensuel supplémentaire peut être organisé à la demande du Client. Cet examen technique peut être tenu tous les mois afin d'échanger des commentaires et des recommandations sur le programme.

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

- Un examen des Incidents de sécurité 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 :

- Mener l'Examen technique mensuel, qui sera d'une durée maximale de 1 heure sans comporter de laboratoire ni de document imprimé.
- L'examen technique mensuel sera effectué à distance par WebEx ou par téléconférence.

Responsabilités du Client :

- Si on le préfère, s'assurer que le personnel technique approprié est disponible pour participer 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 offre une visibilité d'un segment supplémentaire du réseau client. L'option de système de capteurs ATA supplémentaire ajoutera des capacités d'analyse de données de réseau de base qui prennent en charge des segments de réseau d'un débit allant jusqu'à 1 Gbit/s.

Chaque déploiement de capteur ATA supplémentaire nécessite un déploiement de DCAP afin de saisir et d'analyser les données sortant du capteur. Le système de capteurs supplémentaire offrira une saisie complète des paquets et une capacité de stockage allant jusqu'à 20 To.

Responsabilités de Cisco :

- Obtenir et livrer les composants du système de capteurs ATA supplémentaire et les expédier au Client.
- Offrir au client un soutien à distance durant l'installation des composants et valider l'accessibilité de Cisco au système de capteurs ATA supplémentaire.
- Effectuer tout l'entretien nécessaire pour le matériel ou les logiciels relatifs au système de capteurs ATA.

Responsabilités du Client :

- Voir les responsabilités du Client à la section 1.2.2.
- Fournir les éléments suivants pour le déploiement du système de capteurs ATA supplémentaire :

- Une adresse IP sans NAR routée publiquement et un accès réseau d'une bande passante d'au moins 10 Mbit/s pour le routeur RPV afin d'établir une connexion sécurisée avec Cisco.
- L'espace physique, la sécurité physique, l'alimentation, la climatisation et les conditions environnementales adéquates nécessaires pour les fonctions de calcul de l'équipement sur site.
- Maintenir le système de capteurs ATA supplémentaire en état de marche et retourner l'équipement des capteurs en état de marche à Cisco aussitôt le Contrat terminé.

2.2 Coffret complémentaire : débit étendu pour le capteur ATA

Pour les instances de chaque système de capteurs ATA (inclus dans les services de base ou acheté en option comme on le décrit à la section 2.1), le débit pris en charge du segment de réseau surveillé peut être augmenté en écarts de 3 Gbit/s à l'achat du Coffret complémentaire de débit étendu pour le capteur ATA (l'Extension de capteur). Ce coffret complémentaire comprend également une capacité de stockage supplémentaire de 40 To pour tout capteur.

Responsabilités de Cisco :

- Fournir et livrer les composants de l'Extension de capteur afin d'augmenter la prise en charge de 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 :

- Voir les responsabilités du Client à la section 1.2.2.
- Maintenir les composants de l'Extension de capteur en état de marche et retourner l'équipement des capteurs en état de marche à Cisco aussitôt le Contrat terminé.

2.3 Coffret complémentaire : extension de stockage

Le client peut acheter l'extension de stockage (le Stockage supplémentaire) afin d'accroître la capacité de stockage en lots 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 :

- Voir les responsabilités du Client à la section 1.2.2.
- Maintenir les composants de Stockage supplémentaire en état de marche et retourner l'équipement des capteurs en état de marche à Cisco aussitôt le Contrat terminé.

2.4 Coffret complémentaire : demandes de développement

Le Client peut demander le déploiement d'un ou de plusieurs efforts de développement supplémentaires, comme des rapports personnalisés ou l'intégration de télémesure d'appareils supplémentaire propre au client que Cisco peut accepter et fournir. Cisco a regroupé ces demandes de développement et leurs frais supplémentaires associés en fonction de leur niveau de complexité nécessaire pour exécuter la demande.

Catégorie	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 de ressources) • 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 appareil spécialisé (c'est-à-dire qui nécessite 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.
- Exécuter les demandes envoyées conformément aux exigences du document de demandes de développement
- Fournir une estimation ou la demande de modification proposée afin de documenter les frais associés à 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.
- Sur demande ou au besoin, fournir le bon de commande à Cisco afin d'envoyer une demande de développement.

2.5 Coffret complémentaire : Licences supplémentaires d'accès d'utilisateur au portail client

Le Client peut acheter des licences d'utilisateurs du portail client supplémentaires en plus des 15 qui sont comprises dans le service.

Responsabilités de Cisco :

- Valider et configurer des utilisateurs supplémentaires en vue de leur accès au Portail client

Responsabilités du Client :

- Acheter le nombre approprié de licences d'utilisateurs.
- Offrir des informations de connexion à la liste d'utilisateurs actifs.

ANNEXE : Glossaire

Glossaire à consulter pour lire la présente description de service. Les termes débutant par une majuscule ont la définition donnée dans le glossaire, à moins d'être définis autrement ci-dessus.

Analyse avancée : Application d'une variété de techniques exclusives ou non afin d'obtenir des sommaires de comportement normal dans des fenêtres et de lacer des alertes lorsque le comportement déroge de ces comportements normaux.
Analyse des renseignements sur les menaces : renseignements de Cisco ou d'un tiers utilisés afin de fournir une perception des dernières menaces en fonction de la situation et de l'environnement. L'ATA de Cisco utilise des renseignements de sécurité provenant de Cisco TALOS et de Cisco Collective Security Intelligence afin de fournir des analyses et un contexte complets.
ATA : analyses des menaces actives.
Client : entité qui achète les Services pour sa propre utilisation interne.
Directeur des enquêtes : Un ingénieur en sécurité désigné pour offrir au Client des compétences approfondies en gestion d'incident et en enquêtes. Il a la responsabilité de répondre aux questions du Client et de rester au fait de l'environnement de ce dernier.
Dispositif de collecte et d'analyse de données (DCAP) : l'ensemble de l'équipement de réseau de sécurité et de surveillance appartenant à Cisco restera dans les locaux physiques du Client qui sont responsables de la collecte, du rassemblement et de l'analyse de la télémesure des capteurs ou des applications et dispositifs de sécurité du client.
Dossier : un rapport numéroté qui donne des détails sur un incident de sécurité décelé par le SOC et qui nécessite l'attention du Client.
Durée : durée du service ATA acheté par le Client.
Événement de sécurité : une occurrence décelée d'un état de système, de service ou de réseau indiquant une possible atteinte à la politique de sécurité de l'information ou un d'une défaillance de commandes, ou une situation jusqu'alors inconnue qui pourrait avoir une incidence sur la sécurité (ISO 27035).
Extension de capteur : option complémentaire ATA, débit étendu pour le capteur ATA.
Extraction des métadonnées : aussi appelée l'inspection avancée des paquets, l'inspection du trafic réseau (l'en-tête et la charge utile) afin d'extraire des sommaires de trafic de protocole de niveau 7. Parmi les exemples d'extraction de métadonnées, on peut citer une extraction d'URL auquel on a accédé, les paramètres d'URL et le code de réponse du site Web (HTTP 200, 302, etc.). Elle se distingue de NetFlow et d'autres technologies semblables en ce qu'elle voit les données de charge utile et les abrège en plus des combinaisons simples d'IP et de port utilisées au cours de l'échange.
Incident de sécurité ou **Incident** : un événement ou une série d'événements indésirables ou inattendus qui ont une importante probabilité de mettre en danger les activités de l'entreprise et 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 »).
Politique d'intervention : une politique documentée qui décrit comment l'organisation du client réagira et interviendra en cas d'incidents. La politique d'intervention doit être conforme aux lois locales, provinciales et nationales et à tout règlement auquel l'organisation est soumise.
Portail client : Application Web fournie par Cisco au Client qui décrit la visibilité au sein du service d'ATA, y compris les Dossiers et les rapports.
Saisie complète des paquets : l'extraction du paquet brut (l'en-tête et la charge utile) d'un réseau et le maintien de toutes les donnes de paquet dans un disque en vue d'une récupération ultérieure. L'ATA de Cisco effectue une saisie complète des paquets à l'aide de notre composante de capteur ATA, et nos enquêteurs sont formés pour rassembler ces données de paquet comme preuves lorsqu'ils traitent de dossiers générés par un ou plusieurs de nos ensembles d'outils de détection.
SOC : centre des opérations de sécurité (« Security Operations Center »).
Système de capteurs : l'ensemble de l'équipement de Cisco hébergé dans les locaux physiques du Client qui a la responsabilité d'effectuer l'analyse des données du réseau en surveillant un segment du réseau client de façon passive. Le système de capteurs sera doté des capacités de saisie complète des paquets.
Télémesure (brute) : télémesure non compressée constituée d'environ 90 % de données texte.
Télémesure : information ou données qui offrent une perception et une visibilité de ce qui se passe sur le réseau à n'importe quel moment sur les périphériques réseau, les appareils, les applications ou les serveurs où le fonctionnement principal du dispositif ne consiste pas à générer des alertes conçues pour détecter des activités indésirables ou malveillantes des réseaux informatiques.

Descriptions de conservation de gestion des incidents :

Évaluation de la disponibilité : Cisco évalue un nombre de points de données, notamment les incidents antérieurs, les rôles et responsabilités actuels, la structure organisationnelle, les opérations de correction, les capacités de connexion et plus encore, afin d'acquérir une compréhension approfondie de l'environnement.
Pan de développement de gestion des incidents : selon les observations de l'évaluation de la disponibilité, le travail effectué avec le client afin de défini des plans d'action de gestion des incidents.
Exercices sur table : agir en tant que tiers impartial afin de concevoir, de diriger et de participer à des exercices afin d'évaluer l'efficacité du plan de gestion des incidents.
Recherche proactive des menaces : travail effectué avec le client afin de déterminer un cas (ou un ensemble de cas) d'utilisation à tester, par exemple, en trouvant des preuves d'attaque à l'aide d'une approche de mouvement latéral, d'attaque de services Web, de pirate intégré ou d'examen d'accès d'utilisateur privilégié.
Intervention d'urgence pour les incidents :
Triage : évaluer la situation actuelle afin de déterminer la meilleure façon de concevoir et d'amorcer une stratégie d'intervention.
Coordination : Suivi de l'état, mesures à prendre et compilation des mises à jour au besoin, afin de s'assurer que l'incident est correctement géré.
Enquête : analyse de la portée de l'attaque par le déploiement des outils nécessaires, en examinant les sources de journal, afin d'analyser les modèles et les problèmes, en réalisant des investigations informatiques nécessaires et des opérations d'ingénierie inverse pour les maliciels.
Retenue : Mise en quarantaine et interruption des autres mesures de l'attaquant.
Correction : suppression du maliciel ainsi que des autres outils et artéfacts laissés par les attaquants.