Description de service pour Cisco Secure Endpoint-Complete

Le présent document (cette « **Description de service** ») décrit les fonctionnalités, les composants et les conditions du service Cisco Secure Endpoint-Complete que Cisco fournira au Client (les « **Services** ») répertorié dans la commande (« **Client** »). La quantité et le type précis des Services achetés par le Client (directement ou par l'intermédiaire d'un Revendeur autorisé) seront consignés dans une commande de service, un devis ou une commande web signée ou acceptée, ou par tout autre moyen de consentement (par exemple, l'émission d'un bon de commande) (« **Commande** ») entre les parties. La présente Description de service doit être lue conjointement avec le document Prestation de services par Cisco et la Description de l'offre Cisco Secure Endpoint pour le Contrat de l'offre propre à la licence Endpoint. L'annexe A de cette Description de service comporte les conditions supplémentaires régissant les Services.

1. Aperçu de la solution

Cisco Secure Endpoint-Complete est une combinaison de la technologie Cisco Secure Endpoint, de la capacité Cisco Talos Threat Hunting, du service Cisco Talos Incident Response et du service Cisco Secure Managed Detection and Response (MDR) qui fournit au client i) une surveillance des menaces 24 heures sur 24 et 7 jours sur 7 grâce à une combinaison du service Détection et intervention gérées de Cisco Secure et de la capacité de recherche de menaces de Cisco Talos, et ii) le service Cisco Talos Incident Response, qui permet de préparer le Client à répondre à des violations de sécurité ou à des compromissions et qui apporte une aide au Client lors de tels incidents.

2. Détails de la solution

2.1. Caractéristiques des Services Cisco Secure Endpoint-Complete

Élément du Service	Description
Activation	Validation de la configuration de la technologie de Cisco Secure : Cisco configure sa plateforme Détection et intervention gérées, harmonise les dossiers d'exploitation et travaille avec le Client pour configurer et déployer les Composants de sécurité couverts (définis ci-dessous dans la section 2 afin que Cisco puisse surveiller activement l'environnement du Client de la manière décrite dans la présente Description des Services.
Détection	Surveillance des Incidents et des alertes de sécurité 24/7/365 : Cisco offre une surveillance 24/7/365 des Composants de sécurité couverts par des analystes de menaces, des enquêteurs et des intervenants en cas d'incident expérimentés. Séance d'information trimestrielle sur les menaces : réunions d'examen à distance sur une base trimestrielle, auxquels peuvent assister tous les Clients du service Détection et intervention gérées de Cisco Secure. Cette séance d'information trimestrielle fournira des mises à jour sur les modèles actuels de menaces et les tendances en matière d'événements. Recherche de menaces : Pour les Clients ayant activé la recherche de menaces de Cisco, Cisco recevra les alertes de menaces, les étudiera et fournira les résultats au Client. Pour en savoir plus sur la recherche de menaces, cliquez ici : https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/secure-endpoint-offer-description.pdf.
Analyse	Plans d'exécution des enquêtes et des interventions : Cisco utilise ses plans d'exécution de détection, d'investigation et d'intervention.
Investigation	Service d'informations sur les menaces de Talos intégré : Cisco mettra en corrélation et hiérarchisera les alertes de sécurité avec les menaces courantes, les informations sur les menaces de Talos et les informations sur les menaces de tiers en utilisant des analyses, l'orchestration de la sécurité et l'automatisation des interventions pour déterminer si les événements observés ou les notifications sont des failles de sécurité ou des compromissions.
Objectif de délai de réponse	Interventions guidées : Cisco recommande des interventions pour contenir, atténuer, corriger ou éradiquer la menace. Conseils sur les menaces : Cisco donne des conseils sur les menaces nouvellement découvertes afin d'aider les Clients à prévenir de manière proactive les incidents ou les compromissions grâce à la mise en œuvre de contrôles d'atténuation.
Gestion des incidents	Service de gestion des incidents Cisco Talos intégré : Ce service offre une assistance en cas d'urgence et des services proactifs pour évaluer, renforcer et améliorer le programme de préparation aux incidents des Clients.

2.2. Technologies Cisco Secure

Les Services dépendent de la configuration par le Client des services en nuage et des produits logiciels de Cisco définis dans la documentation fournie par Cisco dans le cadre du Service complet Cisco Secure Endpoint. Collectivement, ces services en nuage et ces logiciels Cisco seront désignés comme étant les « **technologies Cisco Secure** ».

Voici les technologies Cisco Secure :

a) Cisco Secure Endpoint Premier
b) Cisco Secure Malware Analytics
c) Cisco SecureX Orchestrator

Le Client doit acheter le service Cisco Secure Endpoint-Complete et les technologies Cisco Secure conjointement dans le cadre de la même UGS de commande, selon les quantités définies par Cisco dans le devis de Cisco. Le Client est également tenu d'obtenir et de maintenir tous les contrats d'assistance et de maintenance Cisco applicables ainsi que toute infrastructure requise (c.-à-d., les types d'appareils compatibles) en rapport avec le service Cisco Secure Endpoint-Complete et pour répondre aux besoins du Client.

3. Modèle de prestation de service pour Cisco Secure Endpoint-Complete

Cisco utilise un cadre opérationnel normalisé de l'Institut national des normes et de la technologie (NIST) pour la prestation des Services, comme décrit plus en détail dans la section 3. Aux fins de la présente Description de service, la technologie Cisco Secure indiquée dans la commande comme faisant partie de la portée des Services est définie comme un « **composant de sécurité couvert** ».

3.1 Activation du service.

Le but de l'Activation du service est de configurer la plateforme du service Détection et intervention gérées de Cisco et de travailler avec le Client pour configurer les Composants de sécurité couverts afin d'effectuer les autres activités décrites dans la section 3.

Responsabilités de Cisco

- Cisco fournira au Client la documentation technique et opérationnelle pour l'aider à configurer les Composants de sécurité couverts, y compris les exigences d'interface API nécessaires pour activer les Services;
- Sous réserve que le Client ait effectué correctement les étapes requises décrites ci-dessous, Cisco intégrera les Composants de sécurité couverts à la plateforme Détection et intervention gérées de Cisco et effectuer des tests pour vérifier qu'ils fonctionnent comme prévu et que tous les guides de Cisco ont été correctement suivis;
- Cisco recommandera des politiques de configuration initiale pour les Composants de sécurité couverts.

Responsabilités du Client

Le Client devra :

- Fournir les jetons API appropriés avec le bon niveau d'accès pour les Composants de sécurité couverts;
- Configurer et vérifier que la connexion au Centre des opérations de sécurité de Cisco a bien été établie et fournir du soutien en cas de futurs problèmes de connectivité;
- Apporter des changements nécessaires à la configuration et à la politique des Composants de sécurité couverts afin qu'ils respectent les recommandations de Cisco nécessaires à la prestation des Services;
- Fournir et tenir à jour les coordonnées des personnes-ressources techniques et opérationnelles désignées, ainsi que la hiérarchie du personnel de l'entreprise;

- Fournir et maintenir un accès administrateur complet aux Composants de sécurité couverts pour Cisco, selon les besoins de Cisco pour la prestation des Services. Par exemple, le Client ne supprimera ni ne limitera l'accès de l'API pour chaque technologie ni des interfaces Web.

3.2. Détection

Cisco surveillera les alertes et les notifications de sécurité des Composants de sécurité couverts pour détecter d'éventuels Incidents. Cisco mettra en corrélation et hiérarchisera les alertes de sécurité avec les menaces courantes, les informations sur les menaces de Talos et les informations sur les menaces de tiers en utilisant des analyses, l'orchestration de la sécurité et l'automatisation des interventions pour déterminer si les événements observés ou les notifications sont des failles de sécurité ou de compromission. Les événements de sécurité détectés qui, selon Cisco, peuvent constituer une possible menace à la sécurité seront consignés en tant qu'incident pour le Client (« **Incident de sécurité** »), disponibles dans le Portail de service Détection et intervention gérées de Cisco Secure. Tous les Incidents seront classés par ordre de priorité et par catégorie afin de simplifier la réponse du Client.

Responsabilités de Cisco

- Surveiller les événements et les alertes de sécurité des Composants de sécurité couverts et enquêter sur ceux-ci par l'intermédiaire de la plateforme Détection et intervention gérées de Cisco Secure, en tirant parti des informations sur les menaces de Talos, de SecureX Orchestrator et des fonctionnalités du service Cisco Secure Endpoint :
    - Utiliser les fonctionnalités des Composants de sécurité couverts, conformément à la configuration et aux politiques recommandées par Cisco. Cela comprend les contrôles de sécurité, les interventions, la fonctionnalité de requête et les techniques de détection;
    - Utiliser les informations sur les menaces de Cisco Talos et l'analyse sécurisée des programmes malveillants pour trouver les menaces les plus récentes et les plus pertinentes, les indicateurs d'attaque ou de compromission et les pratiques exemplaires d'atténuation;
    - Tirer parti des informations sur les menaces de Cisco Talos et des outils de la plateforme Détection et intervention de Cisco pour améliorer les alertes avec des informations complémentaires;
    - Utiliser la recherche de menaces et les outils pour recueillir des données sur les nouvelles tactiques, techniques et procédures d'attaque pour vous aider à trouver les failles de sécurité ou les compromissions;
    - Analyser chaque Incident pour déterminer et communiquer au Client les mesures correctives ou les interventions recommandées;
    - Collaborer avec le Client sur tous les Incidents à haut risque (P1 ou P2) (alerte vraie positive vérifiée) en communiquant directement avec lui du Centre des opérations de sécurité de Cisco à l'aide des coordonnées fournies par le Client. Cisco fournira le contexte sur la gravité des menaces et signalera l'Incident conformément au plan d'intervention en cas d'Incident convenu. Cisco fournit les mesures correctives recommandées au Client pour qu'il effectue les correctifs afin de résoudre l'Incident.
    - Signaler rapidement au Client toutes les possibles menaces détectées au moyen de rapports détaillés sur les Incidents disponibles dans le Portail de service Détection et intervention gérées de Cisco Secure, y compris envoyer des notifications concernant tous les nouveaux Incidents de sécurité;
    - Fournir des recommandations concernant l'atténuation des conséquences de tous les Incidents, y compris les interventions d'atténuation disponibles dans le cadre des Composants de sécurité couverts, ainsi que les pratiques exemplaires, les contrôles et les configurations qui s'appliquent concernant les conséquences d'un Incident de sécurité;

- Fournir une communication experte du Centre des opérations de sécurité 24/7/365 pour tous les Incidents de sécurité actifs, au besoin;
- Assurer le suivi des Incidents de sécurité à mesure qu'ils évoluent au fil du temps, en ajoutant un contexte ou des détections supplémentaires aux Incidents existants, au besoin et dans la mesure du possible;
- Répondre aux demandes de renseignements du Client concernant les Incidents de sécurité actifs et les informations contextuelles, telles que les informations sur les menaces ou les conséquences générales sur l'environnement ou les activités du Client;
- Informer le Client de tout changement important ou de toute nouvelle fonctionnalité dans les Composants de sécurité couverts, au fur et à mesure qu'ils sont disponibles, en temps opportun, y compris de tout changement de configuration ou de politique recommandée;
- Informer le client de toute panne planifiée ou imprévue en ce qui concerne : le Portail de service Détection et intervention gérées de Cisco Secure, les fonctionnalités de surveillance de la plateforme Détection et intervention gérées de Cisco ou la fonctionnalité liée à la capacité de Cisco à surveiller ou intervenir aux événements provenant des Composants de sécurité couverts.

Responsabilités du client

- Aviser Cisco des activités ou des pannes prévues (p. ex. des mises à jour logicielles) ou s'il détecte un possible Incident;
- Effectuer les mesures correctives recommandées par les analystes de la sécurité de Cisco;
- Approuver les mesures de correction automatisées en temps opportun;
- Maintenir une configuration de déploiement acceptable et un déploiement des Composants de sécurité couverts, au besoin, afin de permettre à Cisco d'exécuter les Services conformément à la présente Description de services.