Description de service Détection et intervention gérées de Cisco Secure

Le présent document (cette « **Description de service** ») décrit les fonctionnalités, les composants et les conditions du service Détection et intervention gérées de Cisco Secure (les **« Services** ») que Cisco fournira au Client 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. Cette Description du service doit être lue conjointement avec Prestation de services par Cisco, situé à : Prestation de services par Cisco. L'annexe A de cette Description du service comporte les conditions supplémentaires régissant les Services.

1. Description

1.1 Aperçu

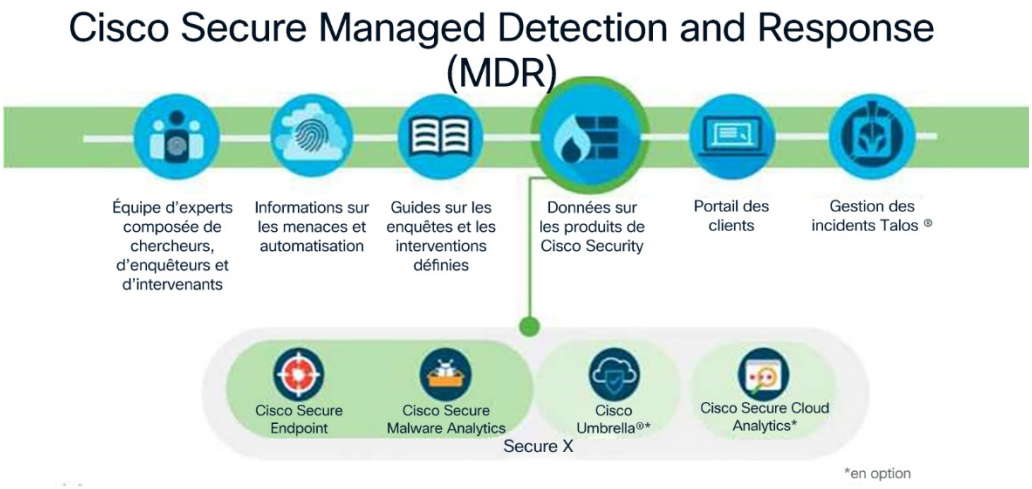
Le service Détection et intervention gérées de Cisco Secure fait appel à différentes ressources qualifiées, à des ensembles d'outils intégrés et à des technologies Cisco Secure pour surveiller les possibles menaces et les violations de sécurité et intervenir. Il comprend les services suivants :

a) Aide à la configuration des produits Cisco Secure admissibles, dont Cisco Secure Endpoint, Cisco Umbrella, Cisco Secure Malware Analytics et Cisco Secure Cloud Analytics, conformément aux pratiques exemplaires recommandées par Cisco.

b) Surveillance des menaces à la recherche d'indicateurs de compromission ou d'alertes.

c) Surveillance 24/7 par le biais des Centres des opérations de sécurité de Cisco à l'aide d'un modèle « ajusté aux fuseaux horaires ».

d) L'équipe de chercheurs, d'enquêteurs et d'intervenants de Cisco utilise à la fois les informations sur les menaces ainsi que les guides sur les enquêtes et les interventions définies de Talos pour détecter les menaces et les alertes, et intervenir. Les interventions de Cisco peuvent être de l'ordre de renseignements, de recommandations ou de changements en fonction du type de menace ou du signe de compromission. Les Services reposent sur les Composants de sécurité couverts et les fonctionnalités suivantes :



1.2 Caractéristiques des Services Détection et intervention gérées de Cisco Secure

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 : le service de gestion des incidents Cisco Talos organise des réunions d'examen à distance sur une base trimestrielle, auxquels peuvent assister tous les Clients du service Détection et intervention gérées. Cette séance d'information trimestrielle fournira des mises à jour sur les modèles actuels de menaces, les volumes de détection 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.
Analyse	Guides des enquêtes et d'intervention : Cisco utilise ses guides 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. 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. Vous trouverez une description de ces Services ici : https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/cisco-talos-incident-response-retainer-service.pdf

* Service facultatif – sous réserve de conditions et de frais supplémentaires

1.3 Technologies Cisco Secure prises en charge

Les Services dépendent du fait que le Client (a) dispose de certains services infonuagiques et logiciels de sécurité Cisco (indiqués ci-dessous) et que (b) la configuration de ceux-ci soit effectuée comme défini dans la documentation fournie par Cisco. Collectivement, ces services infonuagiques et ces logiciels Cisco seront désignés comme étant les « **technologies Cisco Secure admissibles** ». Le Client doit également obtenir et maintenir tous les contrats d'assistance et de maintenance Cisco applicables ainsi que toute infrastructure requise (c.-à-d. les types d'appareils compatibles) pour répondre aux besoins typiques du Client. Les frais des services Détection et intervention gérées ne comprennent pas