Description de service
Services Cisco XDR Premier

La présente Description de service fait partie de l'Accord de services (tel que défini dans le Guide des services) et décrit les divers Services que Cisco vous fournit. Les termes commençant par une majuscule, sauf s'ils sont définis dans le présent document, ont la signification qui leur est donnée dans le Guide des services.

1. Aperçu

Le service Cisco XDR Premier inclut ce qui suit :

1.1 Le service Cisco Managed Extended Detection and Response (« Cisco MXDR »), dans le cadre duquel Cisco effectue les activités résumées à la section 2.1 et décrites plus en détail à la section 3;

1.2 Le service d'évaluation de la sécurité technique de Cisco (CTSA), dans le cadre duquel Cisco fournit des évaluations, des validations et des améliorations en matière de sécurité;

1.3 Les services de gestion des incidents Cisco Talos(Talos IR).

Le service Cisco XDR Premier utilise une combinaison de l'équipe de chercheurs de Cisco, de gestionnaires d'incidents, d'ensembles d'outils intégrés et de technologies Cisco supplémentaires pour surveiller les menaces à la sécurité et les attaques potentielles, et y répondre.

Ce document ne décrit pas les capacités de la plateforme ni de la solution Cisco XDR, qui peuvent être consultées sur le site cisco.com.

2. Caractéristiques des services (aperçu)

2.1 Caractéristiques des Services Cisco MXDR

Élément du Service	Description
Activation du service uniquement	Validation des intégrations Cisco XDR Premier : Cisco valide l'intégration des Composants du Client pris en charge par Cisco XDR Premier (tels que définis au sens de la section 2.2 ci-dessous) dans Cisco MXDR.
Détection	Surveillance des incidents de sécurité 24 heures sur 24, 7 jours sur 7, 365 jours par an : Cisco surveille les Composants pris en charge par Cisco XDR Premier pour détecter les événements et les alertes 24 heures par jour et tous les jours de l'année.
Analyse	Analyse de la plateforme Cisco XDR : Cisco effectue une analyse des données reçues par les Composants pris en charge par Cisco XDR Premier correspondants sur la plateforme XDR et, le cas échéant, transmet ces renseignements au Client en tant qu'incident de sécurité.

Investigation	Processus d'incident : l'analyste SOC de Cisco MXDR mettra en corrélation, enrichira, classera par ordre de priorité et évaluera tous les événements pour les processus SOC établis et, le cas échéant, transmettra ces renseignements au client en tant qu'incident de sécurité. Cisco déterminera la nature de l'incident de sécurité potentiel, lui attribuera une priorité et déterminera son impact potentiel, fournira des résultats d'examen détaillés et des preuves contextuelles, mettra en corrélation les renseignements relatifs au réseau, au matériel et à l'utilisateur dans les sources de produits disponibles et fournira des recommandations détaillées concernant les mesures d'atténuation à prendre pour chaque incident de sécurité.
Objectif de délai de réponse	Interventions guidées : Cisco recommande des interventions aux incidents de sécurité pour aider le Client à contenir, atténuer, corriger ou éradiquer la menace. Les interventions peuvent être menées directement à partir du Portail de service Cisco XDR Premier. 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 de sécurité grâce à la mise en œuvre de contrôles d'atténuation.

2.2 Composants pris en charge par Cisco XDR Premier

Les Services dépendent du fait que le Client a) intègre les technologies de sécurité prises en charge par Cisco XDR, qui comprennent à la fois les technologies de sécurité de Cisco (y compris les produits de sécurité de Cisco repris dans le tableau 1 ci-dessous) et certaines technologies de sécurité de tiers admissibles, comme déterminé par Cisco (ci-après collectivement appelées « **Composants pris en charge par Cisco XDR Premier** »)

3. Éléments du service Cisco XDR Premier

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.

3.1 Activation du service pour le service MXDR Premier.

L'objectif du processus d'activation du service est de collaborer avec le Client dans le but de valider l'intégration des Composants pris en charge par Cisco XDR Premier dans Cisco MXDR afin d'effectuer les activités décrites dans la présente section 3.

Remarque : bien qu'ils soient inclus dans la définition des Composants pris en charge par Cisco XDR Premier, les produits de sécurité Cisco suivants requièrent un processus d'intégration particulier pour que Cisco soit en mesure de fournir les Services :

Produit	Niveaux
Cisco Secure Endpoint	Advantage ou Premier
Cisco Secure Malware Analytics	
Cisco Secure Cloud Analytics (désormais inclus dans la licence Cisco XDR)	Télémétrie du réseau sur site
Cisco Umbrella	DNS Advantage, SIG Essentials ou SIG Advantage

Tableau 1. Les produits de sécurité Cisco qui requièrent des processus d'intégration particuliers.

Responsabilités de Cisco

- Collaborer avec le client pour s'assurer qu'il a correctement installé et mis en œuvre Cisco XDR afin que les Composants d'assistance Cisco XDR Premier puissent être contrôlés par Cisco.
- Fournir au Client la documentation technique et opérationnelle nécessaire pour l'aider à configurer les produits de sécurité Cisco indiqués dans le tableau 1 ci-dessus, y compris les exigences relatives à l'API et à l'interface de console nécessaires pour activer les Services;
- Intégrer les produits de sécurité Cisco mentionnés dans le tableau 1 à la plateforme Cisco MXDR et effectuer des tests pour vérifier qu'ils fonctionnent comme prévu et que tous les guides de Cisco ont été correctement suivis;
- Le cas échéant, collaborer avec le Client pour convenir d'une liste d'actions d'« identification » et de « confinement » que Cisco peut exécuter pour le compte du Client sur la plateforme Cisco XDR i) par événement ou ii) par type d'action (c.-à-d., quel que soit le nombre d'événements). En conséquence, Cisco documentera, dans un guide d'intervention (« Guide d'intervention »), ce qui suit :
  - la liste d'actions d'« identification » et de « confinement » que Cisco est autorisé par les présentes par le Client à exécuter en son nom et celles que le Client se réserve d'exécuter, dans chaque cas, par événement ou par type d'action;
  - la liste des Composants pris en charge par Cisco XDR Premier pour lesquels Cisco peut exécuter ces actions au nom du Client;
- Recommander des politiques de configuration initiale pour les produits de sécurité Cisco mentionnés dans le tableau 1.

Responsabilités du Client

- S'assurer que Cisco XDR a été correctement installé et mis en œuvre afin de recevoir les Services;
- Fournir les jetons API appropriés avec le niveau d'accès adéquat pour les produits Cisco du tableau 1;
- Approuver le Guide d'intervention et, le cas échéant, configurer Cisco XDR pour s'assurer que Cisco reçoit l'autorisation d'exécuter les actions disponibles pour Cisco, comme documenté dans le Guide d'intervention;
- Configurer la connectivité avec le Centre des opérations de sécurité (SOC) de Cisco et vérifier qu'elle a été correctement établie, la maintenir pendant toute la durée des Services, et assumer la responsabilité de tout problème de connectivité ultérieur;
- Apporter des changements nécessaires à la configuration et à la politique des Composants pris en charge par Cisco XDR Premier 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 l'accès aux Composants pris en charge par Cisco XDR Premier 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 Composant pris en charge par Cisco XDR Premier ni les interfaces de la console web.

Limites de la portée

- L'activation du Service n'inclut pas la licence, le déploiement, la configuration ou l'intégration de tout produit de sécurité en dehors des Composants pris en charge par Cisco XDR Premier.
- Cisco ne requiert pas d'accès direct à d'autres produits de sécurité que ceux figurant dans le tableau 1.

3.2 Détection

Cisco surveillera les alertes de sécurité et les événements des Composants pris en charge par Cisco XDR Premier pour détecter d'éventuels Incidents de sécurité. Cisco mettra en corrélation et hiérarchisera les événements et les alertes de sécurité avec les menaces connues, 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 les guides d'intervention automatisés pour déterminer si les événements observés ou les notifications sont des Incidents de sécurité potentiels. 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** »), dont les détails peuvent être consultés par le Client à partir du Portail de service Cisco XDR Premier. Tous les Incidents de sécurité seront classés par ordre de priorité et par catégorie afin de simplifier l'examen et la réponse du Client.

Responsabilités de Cisco

- Enquêter sur les incidents de sécurité liés aux Composants pris en charge par Cisco XDR Premier et les surveiller;
- Utiliser Cisco Talos Threat intelligence et Secure Malware Analytics pour trouver les menaces les plus récentes et les plus pertinentes qui peuvent être détectées par la plateforme Cisco XDR Premier grâce à des indicateurs de compromission (observables), et informer le Client des bonnes pratiques potentielles en matière d'atténuation;
- Enrichir les alertes de sécurité avec des renseignements contextuels;
- Collecter des données sur les nouvelles tactiques, techniques et procédures d'attaque pour vous aider à trouver les attaques de sécurité ou les compromissions;
- Analyser chaque Incident de sécurité pour déterminer et communiquer au Client les mesures correctives ou les interventions recommandées sur le Portail de service Cisco XDR Premier, le cas échéant;
- Signaler toutes les possibles menaces par des Incidents de sécurité détaillés disponibles sur le Portail de service Cisco XDR Premier, y compris les notifications pour tous les nouveaux Incidents de sécurité;
- Fournir des recommandations concernant l'atténuation des conséquences de tous les Incidents, y compris les interventions d'atténuation potentielles disponibles dans le cadre des Composants pris en charge par Cisco XDR Premier, 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 24/7/365 pour tous les Incidents de sécurité actifs, au besoin;
- Assurer le suivi des Incidents 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 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 des produits de sécurité Cisco dans le cadre des Composants pris en charge par Cisco XDR Premier, dès que cela est raisonnablement possible après leur mise à disposition, 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 Cisco XDR Premier;
    - les fonctionnalités de surveillance de la plateforme Cisco MXDR.

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, selon les besoins du Client;
- Approuver les mesures de correction automatisées en temps opportun, si le Client le juge nécessaire;
- Maintenir toutes les configurations requises, les déploiements, la connectivité et l'accès aux Composants pris en charge par Cisco XDR Premier, en comprenant que si les licences de produits individuels, les renseignements d'authentification d'API, la configuration ou le déploiement ne fonctionnent pas comme prévu, les services Cisco XDR Premier peuvent être défavorablement touchés.
- Assurer la connectivité entre la plateforme Cisco XDR et tous les Composants pris en charge par Cisco XDR Premier.

3.3 Analyse.

Cisco analysera les événements de sécurité, les alertes et les données détectées conformément à la section 3.2 susmentionnée dans le but de détecter les menaces à l'aide des données disponibles sur la plateforme Cisco XDR. Cisco analysera également les résultats des enquêtes de Cisco XDR Threat Hunting, les examinera et les enrichira, et fournira les résultats au Client.

Responsabilités de Cisco

- Utiliser les données de toutes les sources configurées disponibles à partir des Composants pris en charge par Cisco XDR Premier pour permettre la surveillance et la détection des menaces à la sécurité. Mettre en corrélation, analyser et étudier chaque scénario de menace présenté à l'aide de techniques et de compétences d'experts pour la menace en question. Sous réserve que le Client conserve un Composant d'assistance Cisco XDR Premier valide et des renseignements d'authentification d'API valides, comme configuré dans le cadre de l'activation du service. S'assurer que toutes les sources de données attendues transmettent bien les données à la plateforme Cisco XDR Premier, comme prévu et dans des délais acceptables, compte tenu de la configuration et de l'intégration du Client. Étudier d'autres catégories d'événements ou de trafic susceptibles de constituer une menace matérielle;
- Effectuer des analyses et utiliser des techniques d'enquête efficaces, automatisées ou manuelles, pour tout Incident, en utilisant les données disponibles et toute l'expertise pratique disponible dans le cadre des Services Cisco XDR Premier, et s'efforcer dans la mesure du possible de fournir des informations exploitables et faciles à interpréter pour le Client dans le ticket de l'Incident.

Responsabilités du Client

- Sur demande, fournir les données contextuelles demandées (p. ex., les pannes, les activités de maintenance, les retraits de composants, et plus encore);
- Examiner les incidents actifs dans le Portail de service Cisco XDR Premier dans la mesure nécessaire pour interpréter l'étendue de l'incident et élaborer un plan pour atteindre un état sûr.

3.4 Enquête.

Cisco enquêtera sur les menaces pesant sur les Composants pris en charge par Cisco XDR Premier, les applications, les points d'accès, l'identité et les éléments du réseau protégés par les Composants pris en charge par Cisco XDR Premier, lorsque les renseignements sur ces menaces sont visibles à partir des journaux, des événements, des alertes et des incidents disponibles au sein des Composants pris en charge par Cisco XDR Premier.

Responsabilités de Cisco

- Utiliser les informations sur les menaces pour rechercher des indicateurs de compromission pour confirmer les menaces, les attaques, les compromissions ou les exploits;
- Créer un dossier d'Incident de sécurité sur le Portail de service Cisco XDR Premier et aviser le Client si un Incident est identifié par Cisco ou signalé par le Client et vérifié par Cisco;
- Utiliser la méthodologie d'enquête établie pour ajouter du contexte aux sources disponibles pour aider à trouver l'incidence, la gravité et la portée de l'Incident de sécurité;
- Étudier l'Incident de sécurité pour déterminer l'incidence pour le Client, le degré de réussite de l'attaquant et ses tactiques, techniques et procédures;
- Enquêter sur les Incidents de sécurité que le Client a ouverts auprès de Cisco en utilisant le même degré d'analyse spécialisée que pour les menaces découvertes par Cisco, y compris les mêmes techniques et la même expertise disponibles pour tout autre Incident de sécurité. Cisco définira le niveau de priorité de ces Incidents de sécurité conformément à la matrice figurant à l'Annexe B et inclura les recommandations de mesures d'intervention ainsi que les renseignements disponibles qui confirment, valident ou corroborent d'une autre manière la détection d'un Incident de sécurité potentiel. Pour ces Incidents de sécurité, Cisco analysera les informations sur les menaces ou les journaux fournis par le Client, si Cisco juge que les données sont suffisamment fiables et pertinentes. Les incidents ouverts par le Client ne doivent pas nécessairement provenir de l'un des Composants pris en charge par Cisco XDR Premier.

3.5 Intervention.

Cisco informera et mettra à jour le Client de l'état de l'incident de sécurité et, en fonction de la nature de l'incident de sécurité, exécutera des actions d'« identification » et de « confinement » autorisées par le Client au sein de la plateforme Cisco XDR, fournira des recommandations guidées ou fournira des réponses générales recommandées pour aider le Client à contenir, à atténuer, à prévenir ou à éradiquer une menace à la sécurité.

Responsabilités de Cisco

- Exécuter les actions d'« identification » et de « confinement » prises en charge par Cisco XDR pour les événements détectés sur la plateforme Cisco XDR au nom du Client, comme documenté dans le Guide d'intervention approuvé par le Client lors de l'activation du service;
- Prodiguer des conseils sur la façon d'atténuer, de contenir ou de prévenir une menace à la sécurité en fonction des renseignements et des conseils fournis, selon l'environnement du Client. La réponse recommandée par Cisco à l'Incident de sécurité peut être une ou plusieurs des solutions suivantes :
    - Avec l'autorisation du Client, apporter les changements approuvés à la stratégie ou à la configuration des produits de sécurité Cisco indiqués à la section 3.1 afin d'atténuer les Incidents de sécurité ou d'y répondre (remarque : les réponses automatisées se limitent à celles documentées dans les guides d'intervention de Cisco Secure Cisco XDR Premier);
    - Lorsque l'Incident est une attaque identifiée, recommander des interventions pour atténuer les conséquences de l'attaque et prodiguer des conseils sur la façon de corriger l'Incident de sécurité en tirant parti des Composants pris en charge par Cisco XDR Premier et des solutions potentielles en dehors des Composants pris en charge par Cisco XDR Premier;
    - Lorsqu'une validation plus poussée de la menace est requise, Cisco fournira des recommandations dans les domaines d'intérêt pour l'enquête du Client. Il peut s'agir de recueillir des renseignements supplémentaires sur l'incident;
    - Lorsque les interventions ne font pas partie des Composants pris en charge par Cisco XDR Premier, Cisco fournira au client des recommandations pour une enquête plus approfondie du Client ou des mesures correctives, dans la mesure du possible.
- Créer et maintenir les guides d'intervention de Cisco XDR Premier en fonction de l'évolution des capacités et des intégrations de la plateforme Cisco XDR et des Composants pris en charge par Cisco XDR Premier, ayant une incidence sur les processus décrits ci-dessus;
- Publier des avis au fur et à mesure que de nouvelles informations sont obtenues sur des menaces nouvelles ou différentes (ces avis ne sont pas propres au Client).

Responsabilités du Client

- Exécuter toutes les actions sur la plateforme Cisco XDR autres que les actions particulières d'« identification » et de « confinement » décrites dans le Guide d'intervention (que Cisco exécutera pour le compte du Client);
- Participer aux tests de diagnostic afin d'aider à identifier la source de l'Incident;
- Effectuer les changements recommandés par Cisco aux Composants pris en charge par Cisco XDR Premier et être responsable de donner suite aux recommandations de Cisco, y compris la détermination des dépendances résultant des mesures recommandées;
- Utiliser le Portail de service Cisco XDR Premier pour configurer et approuver les interventions par l'entremise des API de Cisco;
- Utiliser les ressources du Portail de service Cisco XDR Premier pour obtenir du soutien, accéder à une base de connaissances, gérer les incidents, connaître les plus récentes informations sur les menaces et communiquer avec Cisco.

4. Talos IR et CTSA pour XDR Premier

4.1 Prestation de services Talos IR et CTSA pour XDR Premier

Les services Talos IR et CTSA pour XDR Premier fournissent aux clients XDR Premier des services d'intervention d'urgence à distance uniquement et des services proactifs à distance uniquement. Les Services peuvent inclure un ou plusieurs des services du tableau 2, sous réserve d'avoir un solde d'heures de service suffisant (consultez l'Annexe A pour en savoir plus).

Le Client peut utiliser ses heures de service pour les services suivants :

Service	Heures minimales
Renseignements sur demande	5
Atelier sur la susceptibilité aux violations	5
Évaluation de l'empreinte numérique de l'entreprise	10
Atelier de réflexion sur la conception de la sécurité	20
Intervention d'urgence en cas d'incident	40
Tests d'intrusion	40
Modélisation des menaces	40
Examen de configurations et de versions d'appareils	40
Plan d'intervention en cas d'incident	50
Guides d'intervention en cas d'incident	50
Exercice sur table	50
Évaluation de l'architecture de sécurité	80
Évaluation de l'état de préparation des IR	80
Évaluation des compromissions	80
Environnement de cyberdéfense	80
Recherche proactive de menaces	100
Simulation de menace de l'équipe rouge	160
Équipe mauve	160
Évaluation des opérations de sécurité	160

Tableau 2. Services Talos IR et CTSA pour XDR Premier disponibles

Responsabilités de Cisco

- Fournir une réponse d'urgence aux incidents en faisant remonter les incidents de sécurité du centre d'opérations de sécurité MXDR Premier vers les ressources de gestion des incidents Cisco Talos pour les clients admissibles qui ont choisi de recevoir une assistance de réponse aux incidents d'urgence de la part de Talos IR.
- Fournir au Client une estimation des heures de service en fonction de la complexité de la demande du Client et de l'étendue de la demande du Client nécessaire pour effectuer le ou les services demandés.
- Créer un document sur les exigences de service (« DES ») pour documenter les heures de service, l'étendue de la demande du client et tout produit livrable particulier à soumettre à l'approbation du Client pour tous les services proactifs demandés.
- Assurer les services Talos IR et CTSA, et fournir les produits livrables tels qu'ils sont documentés dans les DES approuvés.

Responsabilités du Client

- Assister aux réunions de prestation de services prévues pour les interventions d'urgence et les services proactifs.
- Approuver tout DES dans les dix (10) jours ouvrables suivant sa communication et au plus tard cinq (5) jours ouvrables avant toute date de début de livraison proposée.
- Solliciter des services proactifs au moins quatre-vingt-dix (90) jours avant l'expiration des heures de service.

- Lorsque le solde d'heures de service du Client est insuffisant pour couvrir les services requis de Cisco, acheter des heures de service supplémentaires pour réaliser toute intervention d'urgence en cas d'incident ou tout service proactif qui dépasse les heures de service disponibles (voir l'Annexe A pour obtenir plus de détails).

4.2 Remarques et limitations

Les remarques et les limites suivantes s'appliquent aux services Talos IR et CTSA pour XDR Premier :

- Cisco s'efforce d'attribuer uniformément les ressources tout au long de la durée de l'abonnement aux Services.
- Une fois que le nombre d'heures de service de la période d'abonnement XDR Premier, comme calculé à partir des détails de la commande, est utilisé, Cisco peut suspendre le travail jusqu'à ce que des heures supplémentaires soient achetées ou que d'autres dispositions écrites soient prises.
- La menace dépersonnalisée, l'indicateur de compromission, la vulnérabilité, l'attaque, les techniques utilisées, la faiblesse ainsi que les autres renseignements connexes que Cisco recueille auprès du Client dans le cadre des Services Talos IR et CTSA pour XDR Premier sont considérés comme des renseignements système. Nous les traitons conformément à notre programme de sécurité et de confidentialité mentionné dans le document Prestation de services par Cisco.
- En raison de la diversité des situations et des problèmes pouvant se produire, des incidents peuvent nécessiter l'utilisation de divers autres services ou fonctionnalités complémentaires au présent service. Par exemple, les incidents peuvent nécessiter l'utilisation d'outils spécialisés pour améliorer la visibilité et l'accès au réseau.
- 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.
- Cisco utilise des processus et des technologies commercialement raisonnables pour évaluer la cybersécurité du Client, mais Cisco ne garantit pas que toutes les vulnérabilités et faiblesses de l'environnement du Client seront détectées.
- Les services Talos IR et CTSA doivent être demandés et planifiés au moins quatre-vingt-dix (90) jours avant l'expiration des heures par période d'abonnement de 12 mois ou à la fin de la période d'abonnement.
- Le Client autorise expressément Cisco à effectuer des tests d'intrusion ou à simuler d'autres types de cyberattaques dans son environnement, comme indiqué dans le DES pour cette activité. Le Client fournit à Cisco une lettre d'autorisation ou des documents semblables comme preuve de cette autorisation à la demande de Cisco.
- Le Client n'est pas autorisé à signaler les activités de test, les outils ou l'infrastructure de Cisco utilisés en relation avec les Services comme malveillants à l'intention de tiers.
- Le Client indique à Cisco les conditions préalables pour chaque activité, comme il est indiqué dans le DES approuvé correspondant. Il peut s'agir de connecter des équipements Cisco à des réseaux, de configurer des dispositifs pour autoriser l'accès à Cisco ou de fournir les renseignements d'authentification demandés pour accéder aux systèmes.
- Si, au cours d'une activité, une défaillance ou un problème grave est découvert dans l'environnement du Client qui, selon Cisco, est susceptible d'affecter l'état opérationnel de l'environnement ou l'exécution de la mission, Cisco peut générer un Avis de défaillance de sécurité (« ADS »). Le cas échéant, Cisco peut suspendre ses activités jusqu'à ce que le Client ait consulté l'ADS et ait demandé à Cisco de reprendre ses activités. Dans ce cas, Cisco peut générer une Demande de modification qui peut nécessiter des Crédits supplémentaires.
- Le Client reste responsable de la sécurité de ses environnements.
- Des renseignements relatifs à la politique d'entreprise Cisco en matière de divulgation des vulnérabilités de sécurité découvertes dans le cadre des Services Cisco sont disponibles à l'adresse : https://tools.cisco.com/security/center/resources/security vulnerability policy.html#dsvdpcsd

4.3 Définitions de la Durée des services

Aux fins de la section 4. Services Talos IR et CTSA pour XDR Premier, les définitions suivantes s'appliquent :

Terme	Définition
Renseignements sur demande	Un service qui fournit des recherches par Talos IR ou Talos Intelligence pour un Client au sujet des menaces les plus récentes ou des facteurs de menace propres au contexte du Client, comme l'infrastructure, l'industrie et la propriété intellectuelle.
Atelier sur la susceptibilité aux violations	Un atelier qui évalue les contrôles existants pour une organisation afin de prévenir les violations.
Évaluation de l'empreinte numérique de l'entreprise	Un service qui, à partir d'une liste d'éléments accessibles par Internet, fournit un rapport détaillant les services offerts par ces systèmes.
Intervention d'urgence en cas d'incident	Un service d'urgence qui aide un Client à réagir aux incidents de sécurité, ce qui peut inclure le triage, la coordination, l'investigation (notamment l'analyse et les enquêtes), le confinement et les conseils pour les mesures correctives.
Atelier de réflexion sur la conception de la sécurité	Un atelier où Cisco utilisera une méthodologie de pensée conceptuelle pour aider le Client à définir les priorités en matière de sécurité et leur alignement sur les priorités de l'organisation.
Tests d'intrusion	Un service dans lequel Cisco utilise sa connaissance des vulnérabilités et des faiblesses en matière de sécurité pour évaluer celles auxquelles un Client est susceptible d'être exposé et leur incidence si elles sont exploitées par un attaquant.
Modélisation des menaces	Un service qui examine les fonctions opérationnelles, les ressources et les données clés du Client afin d'élaborer des modèles sur la manière dont elles pourraient être touchées par un incident de sécurité.
Examen de configurations et de versions	Un service qui évalue la configuration et la construction d'appareils particuliers par rapport à une norme afin de déterminer les vulnérabilités ou les faiblesses.
Plan d'intervention en cas d'incident	Un service qui révise ou crée un document pour déterminer qui est responsable de la gestion des processus et des communications en cas d'incident de sécurité.
Guides d'intervention en cas d'incident	Un service qui examine ou crée un ou plusieurs documents afin de consigner les mesures à prendre pour détecter et contenir un incident de sécurité lié à une menace particulière, et pour s'en remettre.
Exercice sur table	Un service qui facilite la mise en place de scénarios d'incidents de sécurité à différents niveaux de l'organisation du Client et qui permet de tester et de repérer les lacunes dans le plan, les processus et les procédures de réponse aux incidents d'un Client.

Terme	Définition
Évaluation de l'architecture de sécurité	Un service qui examine les contrôles de sécurité existant dans une organisation afin de détecter d'éventuelles lacunes en matière de capacités et de déterminer les domaines dans lesquels les contrôles ne fonctionnent pas comme prévu.
Évaluation des compromissions	Un service qui fournit une analyse et un examen de haut niveau de l'environnement d'un Client afin de déterminer si l'organisation du Client a été compromise ou est en train de l'être.
Environnement de cyberdéfense	Une activité de formation de plusieurs jours avec un environnement de laboratoire Cisco interactif pour les employés du Client en vue d'acquérir une expérience pratique des concepts de criminalistique numérique et de réponse aux incidents de Talos IR.
Recherche proactive de menaces :	Un service qui fournit une analyse et un examen ciblés de l'environnement d'un Client en fonction d'une hypothèse convenue afin de déterminer potentiellement si l'environnement du Client présente des signes de l'activité de cette hypothèse.
Piratage électronique	Un exercice de collaboration où Cisco émule les tactiques, techniques et procédures (TTP) de l'adversaire de manière clandestine pour simuler un adversaire du monde réel.
Équipe mauve	Un exercice de collaboration où Cisco émule les tactiques, techniques et procédures (TTP) de l'adversaire et collabore avec le Client sur les méthodes de détection des événements.
Évaluation des opérations de sécurité	Un service qui examine les opérations de sécurité existant dans une organisation afin de détecter d'éventuelles lacunes en matière de capacités et de déterminer les domaines dans lesquels les contrôles ne fonctionnent pas comme prévu.

Annexe A : Conditions

1. Conditions reliées aux Services.

1.1 **Portée des Services et exclusions.** À moins que les Services ne soient expressément mentionnés, tous les autres services Cisco sont exclus de cette Description de service. Pour plus de clarté, les éléments suivants sont exclus :

a) gestion des modifications ou mise en œuvre des modifications non couvertes par une intervention;
b) connectivité, par exemple, un circuit local;
c) fourniture, configuration, assistance et/ou gestion de tout élément ou technologie de Cisco ou de tiers.

1.2 **Production de rapports.** Cisco fournira, ou mettra à disposition par l'entremise du Portail de service Cisco XDR Premier, les rapports indiqués dans la documentation sur les rapports pour les Services de détection et de réponse. Cisco se réserve le droit d'ajouter, de modifier ou de supprimer des rapports à sa discrétion. Les rapports CTIR et CTSA ne seront pas couverts par le Portail de service Cisco XDR Premier

1.3 **Journalisation des services MXDR.** Veuillez consulter la description du produit ou du service ainsi que les données de journalisation pour les Composants de sécurité Cisco XDR Premier. Les Services conservent les données des dossiers d'Incident pendant un an, puis celles-ci sont supprimées ou remplacées sur une base continue (les données les plus anciennes en premier).

1.4 **Échange de données.** Les données relatives aux services seront échangées entre Cisco et le Client uniquement**.** Par conséquent, si le Client souhaite qu'un partenaire ou qu'un tiers reçoive des données sur l'Incident (p. ex., des dossiers sur l'Incident de sécurité) pour fournir des services complémentaires au nom du Client, le Client fournira à Cisco une lettre d'autorisation permettant cet échange de données et la coordination des Services.

1.5 **Capacités de détection et d'intervention.** Bien que Cisco ait mis en œuvre des technologies et des processus commercialement raisonnables dans le cadre du Service, Cisco ne peut pas garantir qu'il i) préviendra, détectera, arrêtera ou atténuera tous les Incidents de sécurité, ou ii) détectera toujours correctement un événement en tant qu'Incident de sécurité ou autre.

1.6 **Cisco Talos Incident Response (Talos IR) et Cisco Technical Security Assessment (CTSA) pour XDR Premier – Heures de service (« Heures de service »).** Le service de niveau Cisco XDR Premier permet au Client de bénéficier d'un nombre déterminé d'heures de service qui peuvent être imputées sur les services Talos IR ou CTSA décrits dans la section 4.1.

Les heures de service disponibles sont déterminées par Cisco en fonction de la Durée des services et du nombre d'utilisateurs du contenu de sécurité (SCU). Les heures de service sont arrondies au nombre entier supérieur et sont divisées en périodes de 12 mois pour chaque année de la Durée des services. Les heures ne sont pas reportées sur une période de 12 mois ultérieure ni sur une autre période de 12 mois.

Lorsque le Client demande un service Talos IR ou CTSA, Cisco vérifiera que le Client dispose d'un nombre suffisant d'heures de service (voir l'Annexe A: 1.6 pour la définition) pour ces services. Si le solde d'heures de service du Client n'est pas suffisant, le Client devra acheter des heures de service supplémentaires, comme documenté par Cisco. Les heures de service requises sont proportionnelles à la longueur et à la complexité du service en cours. Pour les services proactifs, Cisco documentera la portée de l'activité, les produits livrables et les heures nécessaires pour achever le service dans un DES qui devra être approuvé par le client avant le début de tout service.

1.7 **Assistance technique Cisco XDR Premier.** Les Services ne comprennent pas l'assistance technique pour les Composants pris en charge par Cisco XDR Premier ou toute autre technologie. Si le problème du Client nécessite une assistance technique pour les Composants pris en charge par Cisco XDR Premier, Cisco peut effectuer un triage initial, puis diriger le Client vers les services d'assistance technique de Cisco ou demander au Client de contacter directement l'assistance technique de Cisco. Si le Client requiert une assistance technique pour un tiers (ou des technologies qui ne sont pas de marque Cisco), il doit s'adresser aux fournisseurs tiers concernés. Le Client doit, à tout moment pendant la Durée :

1.7.1 Maintenir toutes les fonctionnalités opérationnelles (y compris l'utilisateur de Cisco et l'accès API) des Composants pris en charge par Cisco XDR Premier, comme l'exige Cisco pour permettre à Cisco de fournir les Services;
1.7.2 Informer Cisco de tout changement qui aura une incidence sur l'accès aux sources de données concernées par la prestation des Services;
1.7.3 Le cas échéant, faire appel à des fournisseurs tiers pour assurer l'assistance.

Annexe B – Niveaux de priorité pour le service Cisco XDR Premier

Cette annexe décrit la méthodologie et la terminologie associée utilisées pour définir le niveau de priorité d'un Incident.

1. Définition de l'incidence et de l'urgence

La Priorité d'un Incident est basée sur l'Incidence et l'Urgence d'un Incident.

Incidence : un Incident de sécurité est classé en fonction de l'étendue de son Incidence sur l'entreprise du Client (à savoir, l'ampleur, la portée et la complexité de l'Incident).	**Urgence :** l'Urgence d'un Incident de sécurité est classée en fonction de son incidence sur les Composants de sécurité surveillés et de son incidence sur les activités du Client.
Il existe quatre niveaux d'Incidence : **Généralisée :** l'ensemble du Service est affecté. **Grande envergure :** plusieurs emplacements sont touchés. **Localisée :** un seul emplacement ou un utilisateur individuel à plusieurs emplacements sont touchés. **Individualisée :** un seul utilisateur est touché.	Il existe quatre niveaux d'urgence : **Critique :** incident de sécurité important entraînant l'arrêt de la fonction principale ou une perte importante, une corruption ou un chiffrement non autorisé de données sensibles. Cette situation peut avoir une incidence financière immédiate et importante sur l'entreprise du Client. **Majeure :** la fonction principale est gravement endommagée en raison de la perte de fonctionnalité ou de données, de la corruption ou du chiffrement non autorisé. Il est probable que la situation ait une incidence financière importante sur l'entreprise du Client. **Mineure :** des fonctions non essentielles sont interrompues ou fortement dégradées. Il est possible que la situation ait une incidence financière sur l'entreprise du Client. **Faible/Avertissement :** des fonctions non essentielles sont dégradées. Il n'y a aucune incidence concrète. Le Client considère le problème comme faible.

1.1 Matrice des priorités

La Priorité définit le niveau d'effort qui sera fourni par Cisco et le Client pour résoudre l'Incident. Le niveau de Priorité est déterminé en se basant sur les définitions des termes « Incidence » et « Urgence » indiquées dans le tableau ci-dessous. Cisco ajustera le niveau de priorité des dossiers d'incident en fonction de la mise à jour du niveau de priorité de l'incidence ou de la résolution de l'Incident. De plus, le dossier peut rester ouvert après le confinement ou la restauration pendant une période prescrite durant l'évaluation des mesures correctives.

		INCIDENCE			
URGENCE		Généralisée	De grande envergure	Localisée	Individualisée
	Critique	P1	P1	P2	P2
	Majeure	P1	P2	P2	P3
	Mineure	P2	P3	P3	P3
	Faible / Avertissement	P4	P4	P4	P4

- P1 : Cisco et le Client engageront les ressources raisonnables, 24 heures sur 24, 7 jours sur 7 pour aider à résoudre l'Incident (comme indiqué ci-dessus).
- P2 à P4 : Cisco et le Client consacreront des ressources raisonnables à temps plein pendant les heures de travail normales pour résoudre l'Incident, fournir l'information ou fournir de l'aide (le cas échéant).

1.2 Matrice des priorités

La Priorité définit le niveau d'effort qui sera fourni par Cisco et le Client pour résoudre l'Incident. Le niveau de Priorité est déterminé en se basant sur les définitions des termes « Incidence » et « Urgence » indiquées dans le tableau ci-dessous. Cisco ajustera le niveau de priorité des dossiers d'incident en fonction de la mise à jour du niveau de priorité de l'incidence ou de la résolution de l'Incident. De plus, le dossier peut rester ouvert après le confinement ou la restauration pendant une période prescrite durant l'évaluation des mesures correctives.

	INCIDENCE				
URGENCE		Généralisée	De grande envergure	Localisée	Individualisée
	Critique	P1	P1	P2	P2
	Majeure	P1	P2	P2	P3
	Mineure	P2	P3	P3	P3
	Faible / Avertissement	P4	P4	P4	P4

- P1 : Cisco et le Client engageront les ressources raisonnables, 24 heures sur 24, 7 jours sur 7 pour aider à résoudre l'Incident (comme indiqué ci-dessus).
- P2 à P4 : Cisco et le Client consacreront des ressources raisonnables à temps plein pendant les heures de travail normales pour résoudre l'Incident, fournir l'information ou fournir de l'aide (le cas échéant).

1.3 Objectifs des niveaux de service (« ONS »)

Temps d'engagement
DÉFINITIONS Cisco communiquera avec la personne-ressource désignée par le Client dans les 30 minutes suivant la priorité d'un Incident de sécurité P1 (45 minutes pour un P2) si aucune recommandation d'atténuation, d'arrêt, de recherche, etc. n'a déjà été fournie. **Calcul** : Cisco communique avec le Client dans les délais ci-dessus pour les Incidents P1 et P2 non résolus/Nombre total d'Incidents de sécurité P1 et P2 dans le mois qui nécessitent un engagement après la hiérarchisation (c.-à-d., aucune recommandation automatique fournie).
Objectifs des niveaux de service : Remontée d'informations au client dans les délais impartis => 95 %
PÉRIODE DE MESURE : Mensuellement (un mois civil)

Si Cisco n'atteint pas l'objectif des niveaux de service susmentionné, il examinera les raisons de cet échec et déploiera des efforts commercialement raisonnables pour remédier à la cause de l'échec. Toutefois, à l'exception de l'obligation énoncée dans la phrase précédente, Cisco n'aura aucune responsabilité envers le client (qu'elle soit financière ou autre) si Cisco ne parvient pas à satisfaire à l'objectif des niveaux de service.

La période pour mesurer le rendement par rapport à l'objectif des niveaux de service se nomme la Période de mesure. La première Période de mesure commence 60 jours après l'Activation du service. Dans les trente (30) jours suivant la fin de chaque Période de mesure, Cisco fournira au Client un rapport sur les performances de Cisco par rapport à l'objectif des niveaux de service pour la Période de mesure en question (« **Rapport sur le rendement** »).

Les Rapports sur le rendement et toutes les données sous-jacentes fournies au Client pour appuyer le Rapport sur le rendement sont des Renseignements confidentiels et ne peuvent être publiés.

L'incapacité de Cisco à atteindre l'objectif des niveaux de service susmentionné sera excusée si elle est due i) à un calendrier d'activités convenu d'un commun accord, ii) à une technologie Cisco en fin de vente (EoS) ou en fin de vie (EoL) ou non couverte par la maintenance, iii) à des retards ou des défaillances causés par le Client, des équipements, des logiciels, des services, une assistance ou des fournisseurs tiers non contrôlés par Cisco, iv) à un cas de force majeure ou v) à l'incapacité du Client à mettre en œuvre les recommandations de Cisco nécessaires pour remédier aux Incidents de sécurité.