

Description de l'offre : Cisco Security Analytics and Logging

La présente description de l'offre (la « **Description de l'offre** ») décrit le logiciel-service Cisco Security Analytics and Logging (« **Logiciel-service SAL** » ou les « **Services en nuage** ») et le logiciel Cisco Security Analytics and Logging sur site (« **Logiciel SAL sur site** » ou le « **Logiciel** »). Votre droit d'utilisation du Logiciel et des Services en nuage est régi par la présente Description de l'offre et par le Contrat de licence d'utilisateur final de Cisco, accessible au www.cisco.com/go/eula (ou toute autre condition similaire existant entre Vous et Cisco) (le « **Contrat** »). Les termes commençant par une majuscule utilisés dans cette Description de l'offre qui ne sont pas autrement définis aux présentes ont le sens qui leur est donné dans le Contrat.

1. Description

1.1. Cisco Security Analytics and Logging

Cisco Security Analytics and Logging (« SAL ») offre une gestion centralisée des journaux (CLM) pour simplifier les opérations informatiques, avec une capacité supplémentaire d'analyse des journaux pour offrir une visibilité améliorée et une détection des menaces sophistiquées. Au début, SAL prenait en charge les journaux de pare-feu Cisco (FTD et ASA). Les journaux de trafic du réseau et d'autres sources de journaux ont été progressivement inclus. Les différents types de journaux sont couverts par la même structure d'offre, qui adopte un modèle de licence imbriqué (c.-à-d. avec des licences secondaires imbriquées dans des capacités de licence principales). Les licences sont les suivantes :

- (a) **Essentials**, anciennement Logging and Troubleshooting (LT) : service de journalisation centralisé et évolutif avec options de rétention à long terme, avec accès au détails activé par le biais de contrôles de visualisation avancés comme la recherche, le filtre, le téléchargement, etc.
- (b) **Avantage**, anciennement Log Analytics (LA) : capacité facultative d'analyse des journaux pour détecter des menaces sophistiquées à l'aide de techniques de modélisation comportementale. Ces algorithmes de détection des menaces tirent parti des analyses Cisco Stealthwatch existantes et déclenchent de nouvelles alertes personnalisées pour les journaux de SAL.
- (c) **Premier**, anciennement Total Network Analytics (TA) : analyse des journaux agrégés avec les journaux natifs de Cisco Stealthwatch, pour une analyse de bout en bout.

Les licences de Logiciel-service SAL comprennent le droit d'utilisation de Cisco Defense Orchestrator (CDO) pour afficher les journaux du pare-feu. En outre, les licences Avantage (Log Analytics) et Premier (Total Network Analytics) comprennent le droit d'utilisation de Stealthwatch Cloud (SWC) pour la détection des menaces sophistiquées. Veuillez noter que le Logiciel-service SAL ne nécessite pas d'abonnement distinct pour CDO ou SWC, et n'est pas non plus obligatoire pour la journalisation de SAL pour les dispositifs pare-feu soient gérés par CDO.

De même, les licences de Logiciel SAL sur site tirent parti des dispositifs virtuels et physiques Stealthwatch Enterprise (SWE), sans avoir besoin de licences de débit de flux SWE distinctes pour les besoins du Logiciel SAL sur site. Des licences de débit de flux continuent d'être nécessaires pour les besoins de SWE.

1.2. Cisco SecureX

Votre abonnement SAL comprend l'accès à Cisco SecureX, la plateforme de sécurité intégrée de Cisco qui regroupe les informations sur les menaces (grâce à la solution de protection contre les menaces SecureX, également connue sous le nom de Cisco Threat Response), unifie la visibilité sur divers produits de sécurité de Cisco et de tiers, permet des flux de travail automatisés, etc. Puisque les données de SAL déclenchent des alertes dans SWC ou SWE, de telles alertes seront visualisées dans SecureX en tirant parti de l'intégration native de Stealthwatch avec SecureX. Pour en savoir plus sur SecureX, consultez la Description de l'offre de SecureX à l'adresse https://www.cisco.com/c/fr_ca/about/legal/cloud-and-software/cloud-terms.html.

2. Conditions générales supplémentaires

2.1. Facturation excédentaire

Les licences Security Analytics and Logging sont facturées en fonction du volume du journal en gigaoctets (Go) par jour. Pour l'offre de Logiciel-service SAL seulement, Cisco peut facturer des excédents mensuellement en arriérés. À la fin de chaque mois civil, Cisco calcule le volume quotidien moyen réel du journal des événements du pare-feu pour le mois et facture automatiquement les excédents au client, le cas échéant. Par exemple, si un client achète un abonnement de 10 Go/jour, il a droit à 300 Go de volume de journaux d'événements du pare-feu pour un mois civil de 30 jours. Si, à la fin de ce mois civil, le client a utilisé 330 Go, l'utilisation quotidienne moyenne est de $330/30 = 11$, et Cisco a le droit de facturer au client un excédent d'abonnement de 1 Go/jour pour ce mois.

2.2. Avis de non-responsabilité

CISCO NE FAIT AUCUNE REPRÉSENTATION ET N'ÉMET AUCUNE GARANTIE VOULANT QUE LES SERVICES EN NUAGE OU LE LOGICIEL PROCURENT UNE SÉCURITÉ ABSOLUE, CAR LES TECHNOLOGIES UTILISÉES POUR EFFECTUER DES ATTAQUES ET DES INTRUSIONS MALVEILLANTES ENVERS LES FICHIERS, LES RÉSEAUX ET LES POINTS TERMINAUX ÉVOLUENT CONTINUUELLEMENT. CISCO NE FAIT AUCUNE REPRÉSENTATION ET N'ÉMET AUCUNE GARANTIE VOULANT QUE LES SERVICES EN NUAGE OU LE LOGICIEL PROTÈGENT TOUS VOS FICHIERS, VOS RÉSEAUX ET VOS POINTS D'EXTRÉMITÉ CONTRE TOUS LES PROGRAMMES MALVEILLANTS, LES VIRUS ET LES ATTAQUES MALVEILLANTES DE TIERS. CISCO NE FAIT AUCUNE REPRÉSENTATION ET N'ÉMET AUCUNE GARANTIE RELATIVE AUX SYSTÈMES ET AUX SERVICES DE FOURNISSEURS TIERS AUXQUELS S'INTÈGRE UN SERVICE EN NUAGE OU UN LOGICIEL, OU CONCERNANT UNE ASSISTANCE PERMANENTE POUR L'INTÉGRATION. LES INTÉGRATIONS MISES À VOTRE DISPOSITION NE SONT PAS GÉNÉRALEMENT DES PRODUITS MIS EN MARCHÉ INCLUS DANS VOTRE COMMANDE SONT FOURNIS « TELS QUELS ».

3. Protection des données

Les fiches techniques sur la confidentialité de SAL, CDO, SWE, SWC et SecureX (accessibles [ici](#)) précisent les Données personnelles que Cisco recueille et traite dans le cadre de la prestation des Services en nuage. Pour plus de détails sur comment Cisco traite, utilise et protège toutes les catégories de données, consultez le [Centre de sécurité et de confiance de Cisco](#).

4. Assistance et maintenance

Un abonnement **Security Analytics and Logging (logiciel-service)** inclut un soutien de base comprenant l'assistance en ligne uniquement. L'assistance en ligne permet un accès aux services d'assistance et de dépannage grâce à des outils en ligne, à la messagerie électronique et à l'ouverture de demande en ligne uniquement. Aucun soutien téléphonique n'est offert. Les directives en matière de gravité et de signalisation progressive ne s'appliquent pas. Cisco répondra aux demandes d'assistance soumises au plus tard le jour ouvrable suivant, pendant les heures de travail normales.

Vous aurez également accès au site Cisco.com, qui fournit des informations générales et techniques utiles à propos des produits Cisco, ainsi qu'à la base de connaissances en ligne et aux forums de Cisco. Notez que des restrictions d'accès déterminées par Cisco peuvent s'appliquer occasionnellement.

Le tableau ci-dessous décrit les objectifs de temps de réponse de Cisco en fonction de la gravité des cas. Cisco peut ajuster la gravité des cas pour s'aligner avec les définitions de gravité ci-dessous.

Service d'assistance logicielle	Couverture de l'assistance technique	Objectif de temps de réponse aux demandes de gravité 1 ou 2.	Objectif de temps de réponse aux demandes de gravité 3 ou 4.
De base avec assistance en ligne	Web	Réponse à toutes les demandes au plus tard le jour ouvrable suivant, pendant les heures de travail normales	

Un abonnement **Security Analytics and Logging (sur site)** inclut un service d'assistance logicielle de base intégré comprenant l'assistance par téléphone et en ligne.

Le tableau ci-dessous décrit les objectifs de temps de réponse de Cisco en fonction de la gravité des cas. Cisco peut ajuster la gravité des cas pour s'aligner avec les définitions de gravité ci-dessous.

Service d'assistance logicielle	Couverture de l'assistance technique	Objectif de temps de réponse aux demandes de gravité 1 ou 2.	Objectif de temps de réponse aux demandes de gravité 3 ou 4.
Service d'assistance logicielle de base	Accès en tout temps au centre d'assistance technique de Cisco (par téléphone et en ligne)	Réponse en une heure	Réponse durant le Jour ouvrable suivant

Les définitions suivantes s'appliquent à la présente section :

Temps de réponse : le délai entre le moment où la demande est soumise dans le système de gestion des demandes et celui où l'ingénieur en assistance communique avec vous.

Gravité 1 : les Services en nuage ne sont pas disponibles, ne fonctionnent plus ou ont une incidence critique ou importante sur les opérations commerciales de la personne ayant soumis la demande. La personne ayant soumis la demande et Cisco mobiliseront des ressources à temps plein pour résoudre la situation.

Gravité 2 : le fonctionnement des Services en nuage est défaillant ou des aspects importants des opérations commerciales de la personne ayant soumis la demande sont touchés par une performance logicielle inacceptable. La personne ayant soumis la demande et Cisco mobiliseront des ressources à plein temps pendant les heures de travail normales pour résoudre la situation.

Gravité 3 : le fonctionnement des Services en nuage est altéré, bien que la plupart des opérations commerciales restent fonctionnelles. Le client et Cisco sont prêts à mobiliser des ressources pendant les heures de travail normales pour résoudre la situation.

Gravité 4 : il y a un problème mineur intermittent de fonctionnalité ou de rendement, ou de l'information sur les Services en nuage est requise. Il y a peu ou pas d'incidence sur les opérations commerciales de la personne ayant soumis la demande. La personne ayant soumis la demande et Cisco sont tous deux disposés à mobiliser des ressources pendant les heures de travail normales afin de fournir de l'information ou de l'assistance, selon les besoins.

Jours ouvrables : jours de travail généralement acceptés pour le travail hebdomadaire au sein de la région concernée, durant lesquels les Services en nuage sont offerts, hormis les jours fériés observés par Cisco.

Heure locale : heure de l'Europe centrale pour l'assistance offerte en Europe, au Moyen-Orient et en Afrique; heure normale de l'Est australienne pour l'assistance offerte en Australie; heure normale du Japon pour l'assistance offerte au Japon; et heure normale du Pacifique pour l'assistance offerte dans tous les autres pays.

Heures de travail normales : de 8 h à 17 h, heure locale, en fonction de l'adresse des bureaux du centre d'assistance technique (CAT) de Cisco, les jours ouvrables, pour le traitement des appels de demande d'assistance.