

IBM QRadar Advisor with Watson

Ce Descriptif de Services décrit le service qu'IBM fournit au Client. Le terme « Client » signifie et inclut la société et ses destinataires ou utilisateurs autorisés du Service Cloud. Le Devis et l'Autorisation d'Utilisation sont fournis séparément sous la forme de Documents de Transaction.

1. Service Cloud

1.1 IBM QRadar Advisor with Watson Service

IBM QRadar Advisor with Watson étend les analyses cognitives à la Plateforme de Sécurité QRadar, afin d'aider les clients et les analystes de sécurité à étudier les menaces et y réagir rapidement. Il tire parti du corpus de connaissances de Watson for Cyber Security afin d'exploiter les données non structurées (notamment les sites Web de sécurité, les blogs et les documents de recherche) et d'établir une corrélation avec les incidents de sécurité locaux. Ainsi, il peut aider à détecter les menaces dissimulées et à automatiser les analyses en vue d'accélérer l'intervention et d'améliorer la prise de décision. QRadar Advisor with Watson permet à un analyste de sécurité d'envoyer une infraction à la sécurité à Watson afin de détecter les menaces, en utilisant sa base de connaissances de centaines de milliers de sources de données non structurées et structurées et en les re-mappant aux entités de menace liées à l'infraction d'origine, par exemple les fichiers malveillants, les adresses IP suspectes, les entités agressives et les relations entre elles. Cette approche peut être particulièrement utile pour déterminer si une infraction à la sécurité est ou non associée à une campagne malveillante connue. Si c'est le cas, Watson fournit des informations de fond sur les logiciels malveillants employés, les vulnérabilités exploitées et la portée de la menace (y compris les points d'extrémité additionnels potentiellement impactés), ainsi que d'autres analyses.

Le Service Cloud exige que le Client dispose d'un déploiement IBM Security QRadar actif et qu'il ait installé le code d'activation du Service Cloud sur ce déploiement de sorte que le Client puisse accéder à ses fonctionnalités. Le Service Cloud impose une 'limite souple' au nombre de requêtes d'infraction à la sécurité que le Client peut envoyer à un débit de quinze (15) requêtes par jour pour tous les 1000 Événements par seconde auxquels le Client a droit. Les requêtes envoyées au-delà de cette limite seront traitées par le Service Cloud, mais elles seront dépriorisées et renvoyées à un débit moins élevé.

1.2 IBM QRadar Advisor with Watson Trial

IBM QRadar Advisor with Watson Trial (le « Service Cloud d'essai ») fournit les fonctionnalités d'IBM QRadar Advisor with Watson à titre d'essai. Le Client pourra accéder au Service Cloud d'essai pendant la période indiquée dans un document de transaction ou toute autre documentation, à l'issue de laquelle l'accès du Client prend fin. Le Client ne pourra envoyer qu'un maximum de 5 requêtes d'infraction à la sécurité par jour pendant la période d'essai. Le Service Cloud d'essai est fourni en l'état et sans garantie et le Client ne pourra l'utiliser que pour des tests en interne et à des fins non destinées à la production. Les temps de réponse aux requêtes peuvent varier pendant la période d'essai en fonction des niveaux de trafic en cours.

2. Description de la Sécurité

Ce Service Cloud se conforme aux principes de confidentialité et de sécurité de données d'IBM pour l'Offre IBM SaaS, qui sont disponibles à l'adresse <http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp>, ainsi qu'à toutes dispositions additionnelles stipulées dans la présente Clause. Les éventuelles modifications des principes de sécurité et de confidentialité de données d'IBM ne dégraderont pas la sécurité du Service Cloud.

Ce Service Cloud peut être utilisé pour traiter certains contenus comportant des données personnelles si le Client, en tant que responsable du traitement des données, détermine que les mesures de sécurité techniques ou organisationnelles sont appropriées pour les risques présentés par le traitement et la nature des données à protéger. Le Client reconnaît que ce Service Cloud ne propose pas de fonctions permettant la protection des données personnelles sensibles ou des données soumises à des obligations réglementaires supplémentaires. Le Client reconnaît qu'IBM n'a pas connaissance des types de données inclus dans le contenu et ne peut pas évaluer la conformité des Services Cloud ou des mesures de sécurité en place.

Le Service Cloud permet au Client d'entrer et de gérer uniquement les informations suivantes dont certaines peuvent être considérées comme informations personnelles (« PII ») en vertu des lois applicables aux données personnelles :

- Adresses IP de destination/source
- Adresses URL
- Domaines
- Hachages de fichier

2.1 Dispositifs de Sécurité et Responsabilités

Le Service Cloud implémente les dispositifs de sécurité suivants :

Le Service Cloud chiffre le contenu pendant la transmission de données entre le réseau IBM et le déploiement IBM Security QRadar du Client. Le Service Cloud ne chiffre pas le contenu stocké attendant la transmission de données.

Le Service Cloud ne conserve pas le contenu entré une fois qu'il a accompli sa fonction au niveau de ces données.

3. Support Technique

Le support technique destiné au Service Cloud est fourni par e-mail, sur les forums en ligne et par le biais d'un système de notification de problème en ligne, comme décrit ci-dessous. Le support technique est offert avec le Service Cloud et n'est pas disponible en tant qu'offre distincte.

Niveau de Gravité	Définition de la Gravité	Objectifs de Temps de Réponse	Couverture de Temps de Réponse
1	Impact critique sur les activités/indisponibilité du service : Une fonctionnalité critique est inutilisable ou une interface critique est défaillante. Cela s'applique généralement à un environnement de production et indique l'impossibilité d'accès aux services, ce qui donne lieu à un impact critique sur les opérations. Cette condition nécessite une solution immédiate.	Sous 1 heure	24 heures sur 24 et 7 jours sur 7
2	Impact significatif sur les activités : L'utilisation d'un dispositif ou d'une fonction du service est gravement restreinte ou le Client risque de ne pas respecter des délais.	Sous 2 heures ouvrables	Heures ouvrables du lundi au vendredi
3	Impact mineur sur les activités : Indique que le service ou la fonctionnalité est utilisable et qu'il n'a pas d'impact critique sur les opérations.	Sous quatre heures ouvrables	Heures ouvrables du lundi au vendredi
4	Impact minime sur les activités : Une demande d'information ou une demande non technique	Sous 1 jour ouvrable	Heures ouvrables du lundi au vendredi

Pour les Clients qui ont participé au programme bêta du Service Cloud et qui utilisent encore la version 7.2.7 de la Plateforme QRadar, il se peut que certains problèmes de support techniques ne puissent pas être résolus, de sorte que ces Clients devront passer à la version 7.2.8 et installer le dernier correctif afin de recevoir le support technique complet.

4. Droit d'Utilisation et Informations de Facturation

4.1 Unités de mesure des redevances

Le Service Cloud est disponible en fonction de l'unité de mesure de redevance indiquée dans le Document de Transaction :

- 100 Événements par seconde** : unité de mesure par laquelle le Service Cloud peut être acquis. Un Événement est une occurrence d'un événement caractéristique, qui est traitée par ou relative à

l'utilisation du Service Cloud. Des droits d'utilisation suffisants sont nécessaires pour couvrir le nombre total d'Événements par seconde, arrondi à la centaine suivante, qui se produisent pendant la période de mesure indiquée dans une Autorisation d'Utilisation (« PoE ») ou un Document de Transaction.

5. Durée et Options de Renouvellement

La durée du Service Cloud commence à la date à laquelle IBM notifie au Client que ce dernier a accès au Service Cloud, comme décrit dans l'Autorisation d'Utilisation. L'Autorisation d'Utilisation indiquera si le Service Cloud est renouvelé automatiquement, s'il se poursuit en continu ou s'il prend fin à l'issue de la durée.

Pour un renouvellement automatique, le Service Cloud est automatiquement renouvelé pour la durée indiquée dans l'Autorisation d'Utilisation, sauf si le Client notifie par écrit, au moins 90 jours avant la date d'expiration de la durée, son intention de ne pas renouveler.

Pour une utilisation en continu, le Service Cloud continuera d'être disponible mois par mois jusqu'à ce que le Client notifie la résiliation moyennant un préavis écrit de 90 jours. Le Service Cloud demeure disponible jusqu'à la fin du mois suivant ladite période de 90 jours.

6. Logiciels d'Activation

Le Service Cloud nécessite des logiciels d'activation que le Client télécharge vers ses systèmes pour faciliter l'utilisation du Service Cloud. Le Client est autorisé à utiliser les logiciels d'activation uniquement en association avec son utilisation du Service Cloud. Les logiciels d'activation sont fournis « EN L'ÉTAT ».

Les logiciels d'activation destinés au Service Cloud sont disponibles pour téléchargement par le Client sur le portail IBM Security App Exchange à l'adresse <https://exchange.xforce.ibmcloud.com/hub>.

7. Dispositions Additionnelles

7.1 Dispositions Générales

Le Client accepte qu'IBM pourra désigner publiquement le Client en tant qu'abonné aux Services Cloud dans les communications publicitaires ou marketing.

7.2 Logiciels d'Activation

Le Service Cloud nécessite des logiciels d'activation que le Client télécharge vers ses systèmes pour faciliter l'utilisation du Service Cloud. Le Client est autorisé à utiliser les logiciels d'activation uniquement en association avec son utilisation du Service Cloud. Les logiciels d'activation sont fournis « EN L'ÉTAT ».

Les logiciels d'activation destinés au Service Cloud sont disponibles pour téléchargement par le Client sur le portail IBM Security App Exchange à l'adresse <https://exchange.xforce.ibmcloud.com/hub>.

7.3 Utilisation Légale du Service Cloud

Le Service Cloud est conçu pour aider le Client à améliorer son environnement et ses données de sécurité. L'utilisation du Service Cloud peut être soumise à diverses lois et réglementations, notamment celles relatives à la confidentialité, la protection des données, l'emploi et le stockage et les communications électroniques. Le Service Cloud ne peut être utilisé qu'à des fins légales et de manière légale. Le Client s'engage à utiliser le Service Cloud conformément aux lois, règlements et réglementations applicables et assume toutes les responsabilités relatives au respect desdites lois, règlements et réglementations. Le Client convient qu'il a obtenu ou qu'il obtiendra tous les consentements, autorisations ou licences nécessaires pour permettre l'utilisation légale du Service Cloud.

7.4 Expiration du Service Cloud

Avant l'expiration ou la résiliation du Service Cloud, le Client peut utiliser l'une quelconque des fonctions de génération de rapports ou d'exportation fournies du Service Cloud pour extraire des données.

7.5 Données de Sécurité

Dans le cadre du Service Cloud, qui comprend des activités de production de rapport, IBM préparera et gèrera les informations anonymes et/ou cumulées extraites du Service Cloud (« Données de Sécurité »). Sauf disposition contraire stipulée dans le paragraphe (d) ci-dessous, les Données de Sécurité n'identifieront pas le Client ou un individu. En outre, le Client accepte par les présentes qu'IBM puisse utiliser et/ou copier les Données de Sécurité uniquement aux fins suivantes :

- a. publication et/ou distribution des Données de Sécurité (par exemple, dans les compilations et/ou analyses liées à la cybersécurité) ;
- b. développement ou amélioration des produits ou services ;
- c. réalisation d'étude en interne ou auprès de tiers ; et
- d. partage légal des informations confirmées relatives à un contrevenant tiers.