IBM QRadar Advisor with Watson

Ce Descriptif de Services détaille le Service Cloud. Les bons de commande applicables contiennent les prix et des détails supplémentaires concernant la commande du Client.

1. Service Cloud

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. 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 aux fins d'intervention et de 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.

1.1 Offres

Le Client peut faire son choix parmi les offres disponibles ci-dessous.

1.1.1 IBM QRadar Advisor with Watson

IBM QRadar Advisor with Watson exige que le Client dispose d'un déploiement IBM QRadar actif, dans un environnement sur site local ou un déploiement de cloud, et qu'il ait installé le logiciel d'activation du Service Cloud sur ce déploiement de sorte que le Client puisse accéder à ses fonctionnalités. Lorsque le Service Cloud est autorisé en fonction du nombre d'Evénements par seconde, il impose une limite au nombre de requêtes d'infraction à la sécurité que le Client peut envoyer à un débit de 1,5 requête par jour pour tous les 100 Événements par seconde (arrondi à la requête supérieure) auxquels le Client a droit. Lorsque le Service Cloud est autorisé en fonction du MVS (Managed Virtual Server), il impose une limite au nombre de requêtes d'infraction à la sécurité que le Client peut envoyer à un débit de 15 requêtes par jour pour tous les 100 MVS auxquels le Client a droit. Les requêtes envoyées au-delà de cette limite seront dépriorisées et risquent de ne pas être traitées par le Service Cloud pour le reste de la journée.

1.1.2 IBM QRadar Advisor with Watson – Enterprise

IBM QRadar Advisor with Watson – Enterprise est mieux adapté aux déploiements SOC (Security Operation Center) de grande taille qui excèdent généralement deux-cent-cinquante mille Evénements par seconde ou plus. Le Client doit installer le logiciel d'activation du Service Cloud sur le déploiement IBM QRadar qu'il a acquis séparément, afin d'accéder aux fonctionnalités du Service Cloud. QRadar Advisor with Watson – Enterprise est disponible en fonction de l'unité de mesure de redevance Instance qui ne dépend pas de la taille du déploiement IBM QRadar du Client. Le Client ne peut effectuer que 25 requêtes dans la file d'attente à un moment donné.

1.1.3 IBM QRadar Advisor with Watson – Starter Pack

IBM QRadar Advisor with Watson – Starter Pack est destiné aux nouveaux utilisateurs de QRadar Advisor with Watson. Ce Service Cloud dispose des fonctionnalités complètes de QRadar Advisor with Watson tel que décrit dans la Section 1.1.1 ci-dessus, mais il est uniquement disponible en tant que premier achat du Client de QRadar Advisor with Watson et aucun renouvellement n'est possible.

1.2 Services Optionnels

1.2.1 IBM QRadar Advisor with Watson – Test Environment

IBM QRadar Advisor with Watson – Test Environment est destiné aux Clients qui souhaitent déployer le Service Cloud dans leur environnement de test interne et ne peut être utilisé qu'à des fins de test hors

production. IBM QRadar Advisor with Watson – Test Environment doit être complété par un abonnement au Service Cloud de niveau production.

1.3 Services d'Accélération

1.3.1 IBM QRadar Advisor with Watson Advanced Services

Pour ce service d'abonnement fourni à distance, IBM fournira au Client les services de consultation suivants, jusqu'à cinq (5) jours pendant une période d'un an :

- évaluer le processus de sphère de contrôle du Client, y compris le processus d'enquête ou d'intervention en cas d'incident ;
- réévaluer la réponse des ensembles de référence ;
- ajuster l'analyse automatique pour les infractions de grande ampleur ;
- développer les cas d'utilisation ;
- fournir des recommandations pour des changements au processus de sphère de contrôle qui intègrent QRadar Advisor with Watson ;
- donner des conseils sur la façon la plus efficace de comprendre et d'intégrer les données de QRadar Advisor with Watson dans les processus existants du Client ;
- fournir un transfert de connaissances sur les sujets QRadar Advisor pertinents.

REMARQUE : Les activités suivantes peuvent être intégrées à ce service en fonction de l'état du déploiement QRadar du Client :

- effectuer un bilan de santé sur le déploiement QRadar du Client ;
- réaliser un réglage additionnel sur le déploiement QRadar existant ;
- aider à l'ajout de sources de journal additionnelles au déploiement QRadar du Client.

1.3.2 IBM QRadar Advisor with Watson Basic Setup Service

Ce service d'installation est fourni à distance et comprend quarante (40) heures de services professionnels qui expirent (90) jours après l'achat, sauf indication contraire, peu importe si toutes les heures (le cas échéant) ont été utilisées. Les services comprennent un responsable d'engagement IBM désigné qui programmera et prendra les appels.

IBM effectuera une partie ou la totalité des tâches suivantes :

- évaluer le processus de sphère de contrôle du Client, y compris le processus d'enquête ou d'intervention en cas d'incident ;
- implémenter QRadar Advisor with Watson dans l'environnement du Client :
  - installer QRadar Advisor with Watson ;
  - mapper les propriétés unifiées à QRadar Advisor with Watson ;
  - implémenter la réponse des ensembles de référence ;
  - ajuster l'analyse automatique pour les infractions de grande ampleur ;
  - donner des conseils sur les cas d'utilisation ;
  - fournir des recommandations pour des changements au processus de sphère de contrôle qui intègrent QRadar Advisor with Watson.

1.3.3 IBM QRadar Advisor with Watson Quick Setup Service

Ce service de configuration est conçu pour les Clients disposant de moins de 5 000 événements par seconde (EPS).

Pour ce service d'abonnement délivré à distance, IBM fournira au Client les services de consultation suivants (ou une combinaison des services), pour une durée maximale de seize (16) heures pendant une période de 90 jours :

- Installation de QRadar Advisor with Watson.
- Gestion des autorisations pour QRadar Advisor with Watson.

- Configuration de QRadar Advisor with Watson, qui peut inclure :
  - la configuration d'un serveur proxy sécurisé ;
  - la soumission des identifiants X-Force Exchange ;
  - la création de jetons de service autorisés ;
  - la configuration de règles de conservation pour le stockage des résultats d'analyse ;
  - le mappage des propriétés d'événement personnalisées ;
  - l'exportation des ensembles de référence ;
  - le mappage des informations sur les menaces ;
  - la configuration de l'identification des actifs ;
  - l'optimisation de l'utilisation.
- Enquête automatique sur les infractions et génération des résultats (au moins un modèle de démonstration de scénario d'utilisation).
- Exploration des analyses à l'aide du graphique relationnel.

2. Fiches Techniques sur le Traitement et la Protection des Données

L'Addendum d'IBM relatif au Traitement de Données à caractère personnel, disponible sur http://ibm.com/dpa (DPA) et la ou les Fiches Techniques (désignées par fiche(s) technique(s) ou Annexe(s) DPA) dans les liens ci-dessous contiennent des informations additionnelles sur la protection des données pour les Services Cloud et leurs options concernant les types de Contenus pouvant être traités, les activités de traitement impliquées, les dispositifs de protection des données et les détails de conservation et de retour de Contenu. Le DPA s'applique aux Données à caractère personnel du Contenu dans la mesure où i) Le Règlement Général sur la Protection des Données (UE/2016/679) (RGPD) ; ou ii) d'autres lois relatives à la protection des données identifiées sur http://ibm.com/dpa/dpl s'appliquent.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=0B439290AB5011E6BE74C84817AAB206

3. Niveaux de Service et Support Technique

3.1 Accord Relatif aux Niveaux de Service

IBM fournit au Client l'Accord relatif aux Niveaux de Service (« SLA ») de disponibilité ci-dessous. IBM appliquera le dédommagement correspondant le plus élevé, en fonction de la disponibilité cumulée du Service Cloud, comme indiqué dans le tableau ci-dessous. Le pourcentage de disponibilité est calculé comme suit : le nombre total de minutes d'un mois contractuel moins le nombre total de minutes d'indisponibilité du Service au cours du mois contractuel, divisé par le nombre total de minutes du mois contractuel. La définition de l'indisponibilité du Service, la procédure de réclamation et les moyens de contacter IBM concernant les problèmes de disponibilité de service figurent dans le guide de support de Services Cloud d'IBM à l'adresse https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilité	Avoir (% de redevance d'abonnement mensuelle*)
Inférieure à 99,9 %	2 %
Inférieure à 99,0 %	5 %
Inférieure à 95,0 %	10 %

* La redevance d'abonnement est le prix contractuel pour le mois objet de la réclamation.

3.2 Support Technique

Le support technique destiné au Service Cloud, y compris les coordonnées des personnes à contacter, les niveaux de gravité, les heures de disponibilité, les temps de réponse ainsi que d'autres informations et processus relatifs au support technique sont disponibles en sélectionnant le Service Cloud dans le guide de support IBM disponible à l'adresse https://www.ibm.com/support/home/pages/support-guide/.

4. Montant des Redevances

4.1 Unités de mesure des redevances

Les unités de mesure des redevances du Service Cloud sont indiquées dans le Document de Transaction.

Les unités de redevances suivantes s'appliquent à ce Service Cloud :

- Un Evénement Par Seconde (EPS) est une occurrence d'un EPS caractéristique, qui est traitée par ou relative à l'utilisation des Services Cloud. Dans le cadre de ce Service Cloud, les Evénements par Seconde correspondent aux événements collectés et traités par le déploiement IBM QRadar du Client.
- Une Instance représente chaque accès à une configuration spécifique des Services Cloud.
- Un Engagement est un service professionnel ou de formation relatif aux Services Cloud.
- Le serveur virtuel géré (MVS) est composé d'unités de traitement, de mémoire et de capacités d'entrée/sortie qui exécutent les procédures, commandes ou applications demandées et gérées par les Services Cloud.

5. Dispositions Additionnelles

Pour les Contrats de Services Cloud (ou des contrats Cloud de base équivalents) signés avant le 1er janvier 2019, les dispositions énoncées à l'adresse https://www.ibm.com/acs s'appliquent.

5.1 Logiciels d'Activation

Le Service Cloud contient les Logiciels d'Activation suivants :

- IBM QRadar with Watson App (https://exchange.xforce.ibmcloud.com/hub)

5.2 Utilisation Licite 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 licites et de manière licite. 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 licite du Service Cloud.

6. Dispositions dérogatoires

6.1 Utilisation de Données

La disposition suivante prévaut sur toute disposition contraire dans la clause « Contenu et protection des données » des conditions cadre de Service Cloud entre les parties : IBM n'utilisera ou ne communiquera pas les résultats découlant de l'utilisation du Service Cloud par le Client qui sont exclusivement liés au Contenu (Observations) du Client ou qui identifient le Client de quelque autre manière. IBM utilisera cependant le Contenu et d'autres informations issues du Contenu (à l'exception des analyses) dans le cadre du Service Cloud en vue d'améliorer le Service Cloud. IBM peut également partager des identificateurs de menaces et d'autres informations de sécurité intégrées au Contenu à des fins de détection des menaces et de protection.