IBM Resilient Incident Response Platform On Cloud

Ce Descriptif de Services détaille le Service Cloud qu'IBM fournit au Client. Le terme « Client » signifie la société et ses destinataires et 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

IBM Resilient Incident Response Platform on Cloud fournit des plans d'action dynamiques (programmes malveillants, attaques de déni de service distribué (Distributed Denial of Service, DDoS) et appareils perdus) ainsi que les meilleures pratiques permettant d'intervenir généralement en cas d'incident. Cette base de connaissances guide l'équipe du Client tout au long de l'intervention et peut être configurée selon les procédures d'exploitation propres au Client.

Les équipes d'intervention en cas d'incident peuvent collaborer et gérer leur intervention directement dans IBM Resilient Incident Response Platform on Cloud. Contrairement aux systèmes de demande de service de support et d'autres outils informatiques polyvalents, IBM Resilient Incident Response Platform est entièrement configurable et spécialement conçu pour les interventions en cas d'incident. Outre les analyses détaillées, des tableaux de bord personnalisables et de solides fonctionnalités de production de rapport permettent à la haute direction d'accéder aux informations clés.

IBM Resilient Incident Response Platform est conçu pour les organisations de différentes tailles et complexités et est disponible en plusieurs versions pouvant être commandées séparément :

1.1 IBM Resilient Incident Response Platform Enterprise on Cloud

L'offre IBM Resilient Incident Response Platform Enterprise on Cloud est une solution de Service Cloud destinée à une diversité de grands systèmes des grandes entreprises. Elle sert de base à la planification, la gestion et l'atténuation d'une intervention pour les organisations et les types d'incident. Les utilisateurs peuvent créer des plans d'intervention en cas d'incident en fonction des normes et meilleures pratiques du secteur d'activité et suivre les incidents jusqu'à leur résolution. Le Service Cloud facilite une collaboration centralisée dans toute l'organisation, ce qui permet aux divers intervenants d'assumer leurs rôles et tâches dans le cadre des activités d'intervention. Des simulations d'incident peuvent également être effectuées, afin d'aider les équipes de tester des plans d'intervention, de repérer les lacunes et d'affiner les processus d'intervention. Des intégrations incorporées à divers flux d'informations sur les menaces extérieures automatisent l'enrichissement des incidents et artefacts. Le Service Cloud inclut une base de connaissances en matière de réglementations globales relatives à la notification des violations de la confidentialité de données, qui aide à personnaliser davantage les plans d'intervention en cas d'incident. Les données peuvent également être synthétisées à partir des systèmes de sécurité et informatiques existants afin de fournir des informations en temps quasi réel. Diverses tâches peuvent être automatisées, simplifiées ou optimisées dans le Service Cloud, sans nécessiter de développement personnalisé. Le Client doit acquérir au moins 1 droit d'Instance et 1 droit d'Utilisateur Autorisé pour ce service.

1.2 IBM Resilient Incident Response Platform Standard on Cloud

IBM Resilient Incident Response Platform Standard on Cloud est une solution de Service Cloud conçue pour répondre aux besoins des petites et moyennes entreprises en matière d'intervention en cas d'incident. Elle offre plus ou moins les mêmes fonctionnalités d'IBM Resilient Incident Response Platform Enterprise on Cloud à l'exception des fonctions suivantes que le Client n'est pas autorisé à utiliser : réglementations relatives à la violation de la confidentialité, automatisation/orchestration, flux d'informations sur les menaces et intégration LDAP. Le Client doit acquérir au moins 1 droit d'Instance et 1 droit d'Utilisateur Autorisé pour ce service.

1.3 Services Optionnels

1.3.1 IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud

IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud est une instance distincte d'IBM Resilient Incident Response Platform que le Client peut utiliser uniquement pour des activités non destinées à la production, y compris, sans que cette liste soit limitative, pour les activités de test, d'optimisation de performances, de diagnostic d'incident, de test interne de

performances, de transfert, d'assurance qualité et/ou pour développer, à l'aide d'interfaces de programmation d'application publiées, des ajouts ou extensions du Service Cloud utilisés en interne.

1.4 Services à Distance

Les Services à Distance suivants peuvent être commandés séparément et chacun arrive à expiration quatre-vingt-dix (90) jours suivant l'acquisition, que toutes les heures (le cas échéant) aient été utilisées ou non :

1.4.1 IBM Resilient Incident Response Platform Integration for Cloud

Cette offre fournit des services d'intégration pour connecter le Service Cloud aux systèmes de sécurité et de gestion connexes, à l'aide d'une intégration pré-développée. Une seule intégration à un seul système sera configurée par Engagement. Les intégrations pouvant être configurées par ce Service à Distance sont énumérées ci-dessous :

- **Intégration à QRadar**

  Cette intégration permet à QRadar d'envoyer automatiquement ou manuellement au Service Cloud des offenses sous forme de nouveaux incidents. Elle comprend la synchronisation bidirectionnelle des notes, des événements de clôture et des nouvelles données d'offense.

- **Intégration à HP ArcSight**

  Cette intégration permet aux utilisateurs ArcSight d'envoyer manuellement ou automatiquement au Service Cloud les détails d'un événement Arcsight sous forme de nouveaux incidents ou d'ajouter des artefacts aux incidents existants.

- **Intégration à Splunk**

  Cette intégration permet à Splunk d'envoyer au Service Cloud des alertes sous forme d'incidents. Le Client peut également exécuter des requêtes Splunk directement à partir de l'interface Web du Service Cloud.

- **Intégration à ServiceNow**

  Cette intégration permet aux utilisateurs ServiceNow de créer des incidents dans le Service Cloud et aux utilisateurs de Service Cloud de créer des tickets dans ServiceNow. Les mises à jour des tickets ou incidents sont également répliquées entre les systèmes.

- **Intégration à JIRA**

  Cette intégration permet aux utilisateurs JIRA de créer des incidents dans le Service Cloud en fonction des tickets JIRA et aux utilisateurs de Service Cloud de créer des tickets dans JIRA. Les mises à jour des tickets ou incidents sont également répliquées entre les systèmes.

1.4.2 IBM Resilient Incident Response Platform Design Session for Cloud

Ce service fournit un engagement consultatif aidant à optimiser l'instance de Service Cloud pour le Client. Les consultants IBM collaboreront avec le Client pour synthétiser les processus d'intervention existants du Client pour un maximum de trois (3) types d'incident différents et les affiner en fonction des meilleures pratiques en vigueur dans le secteur d'activité et des fonctionnalités du Service Cloud, et conseillent le Client sur la façon de configurer le Service Cloud pour mettre en oeuvres ces processus.

2. Description de la Sécurité

Ce Service IBM se conforme aux principes de confidentialité et de sécurité de données d'IBM pour les Offres IBM SaaS, qui sont disponibles à l'adresse http://www.ibm.com/cloud/data-security, 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 n'a aucune exigence de sécurité spécifique au contenu réglementé, tel que les informations personnelles ou les informations personnelles sensibles. Le Client est tenu de déterminer si ce Service Cloud répond à ses besoins quant au type du Contenu qu'il utilise en rapport avec le Service Cloud.

3. Accord Relatif aux Niveaux de Service

IBM fournit l'Accord Relatif aux Niveaux de Service (ci-après dénommé « Accord Relatif aux Niveaux de Service » ou « SLA ») de disponibilité ci-dessous pour le Service Cloud, comme indiqué dans une

Autorisation d'Utilisation. Le SLA ne constitue pas une garantie. Il n'est disponible que pour le Client et ne peut être utilisé que dans les environnements de production.

3.1 Crédits de Disponibilité

Le Client doit consigner un ticket de support de Gravité 1 auprès du centre d'assistance technique IBM dans les 24 heures suivant la première fois où le Client a eu connaissance qu'un événement a eu une incidence sur la disponibilité du Service Cloud. Le Client doit raisonnablement aider IBM dans le cadre du diagnostic et de la résolution des problèmes.

Une demande de ticket de support pour non-respect d'un SLA doit être soumise dans les trois jours ouvrables suivant la fin du mois contractuel. Le dédommagement relatif à une réclamation de SLA valide sera un avoir sur une future facture du Service Cloud en fonction de la période de temps pendant laquelle le traitement du système de production pour le Service Cloud n'est pas disponible (« Durée d'Indisponibilité »). La Durée d'Indisponibilité est calculée depuis le moment où le Client signale l'événement jusqu'au moment où le Service Cloud est restauré ; elle ne comprend pas les périodes d'indisponibilité pour les raisons suivantes : indisponibilité de maintenance programmée ou annoncée, causes échappant au contrôle d'IBM, incidents liés au contenu, à la technologie, aux conceptions ou aux instructions du Client ou d'un tiers, plateformes et configurations de système non prises en charge ou autres erreurs du Client, incident de sécurité du fait du Client ou test de sécurité mené par le Client. IBM appliquera le dédommagement correspondant le plus élevé, en fonction de la disponibilité cumulée du Service Cloud pendant chaque mois contractuel, comme indiqué dans le tableau ci-dessous. Le dédommagement total relatif à tout mois contractuel ne pourra pas dépasser dix pour cent (10 %) d'un douzième (1/12ème) de la redevance annuelle du Service Cloud.

3.2 Niveaux de Service

Disponibilité du Service Cloud pendant un mois contractuel

Disponibilité pendant un mois contractuel	**Indemnisation (% de redevance d'abonnement mensuelle* pour le mois contractuel objet d'une réclamation)**
99,5 %	2 %
98 %	5 %
96 %	10 %

* Si le Service Cloud a été acquis auprès d'un Partenaire Commercial IBM, la redevance d'abonnement mensuelle sera calculée sur le prix en vigueur à ce moment-là pour le Service Cloud concerné pendant le mois contractuel qui fait l'objet d'une réclamation, avec une réduction de cinquante pour cent (50 %). IBM accordera une remise directement au Client.

La disponibilité, exprimée en pourcentage, est calculée comme suit : le nombre total de minutes d'un mois contractuel moins le nombre total de minutes de la Durée d'Indisponibilité au cours d'un mois contractuel, divisé par le nombre total de minutes d'un mois contractuel.

Exemple : 500 minutes de Durée d'Indisponibilité totale pendant un mois contractuel

Au total 43 200 minutes dans un mois contractuel de 30 jours - 500 minutes de Durée d'Indisponibilité = 42 700 minutes _____ Au total 43 200 minutes	= 2 % de crédit de Disponibilité pour 98,8 % de disponibilité pendant le mois contractuel

4. 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. Le support technique est offert avec le Service Cloud et n'est pas disponible en tant qu'offre distincte. Le support technique est disponible pendant les heures de travail normales de 9h00 à 18h00 heure normale de l'Est, excepté les jours fériés.

Niveau de Gravité	Définition de la Gravité	Objectifs de Temps de Réponse Pendant les Heures d'Assistance
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
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
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
4	**Impact minime sur les activités :** Une demande d'information ou une demande non technique	Sous 1 jour ouvrable

5. Droit d'Utilisation et Informations de Facturation

5.1 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 :

a. **Instance** : unité de mesure par laquelle le Service Cloud peut être acquis. Une Instance est l'accès à une configuration spécifique du Service Cloud. Des droits d'utilisation suffisants sont nécessaires pour chaque Instance du Service Cloud mise à disposition à des fins d'accès et d'utilisation pendant la période de mesure indiquée dans l'Autorisation d'Utilisation ou le Document de Transaction du Client.

b. **Utilisateur Autorisé** : unité de mesure par laquelle le Service Cloud peut être acquis. Le Client doit se procurer des droits d'utilisation distincts et dédiés pour chaque Utilisateur Autorisé unique ayant reçu l'accès au Service Cloud directement ou indirectement (par exemple, via un logiciel de multiplexage, un périphérique ou un serveur d'applications), par quelque moyen que ce soit. L'obtention des droits d'utilisation adéquats est nécessaire pour couvrir le nombre d'Utilisateurs Autorisés ayant accès au Service Cloud pendant la période de mesure indiquée dans l'Autorisation d'Utilisation ou le Document de Transaction du Client.

c. **Engagement** : unité de mesure par laquelle les services peuvent être acquis. Un Engagement comprend des services professionnels et/ou de formation relatifs au Service Cloud. L'obtention de droits suffisants est nécessaire pour couvrir chaque Engagement.

5.2 Redevances de dépassement

Si l'utilisation réelle du Service Cloud par le Client pendant la période de mesure dépasse les droits indiqués dans l'Autorisation d'Utilisation (« PoE »), le Client sera facturé pour l'excédent, comme indiqué dans le Document de Transaction.

5.3 Redevances des Services à Distance

Les Services à Distance sont acquis par unité de mesure d'Engagement et seront facturés au prix spécifié dans le Document de Transaction.

6. 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.

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 Service Cloud de Gestion de Conformité

Le Service Cloud peut être utilisé pour aider le Client à respecter les obligations de conformité, qui peuvent être fondées sur des lois, réglementations, normes ou pratiques. Le Client reconnaît et accepte que toutes instructions, toute utilisation recommandée ou tous conseils fournis par le Service Cloud ne constituent pas un avis juridique, comptable ou autre avis professionnel et le Client devra se procurer son propre conseiller juridique, comptable ou autre conseiller qualifié. Le Client accepte également qu'il est seul responsable de s'assurer que le Client et les activités, applications et systèmes du Client respectent les lois, réglementations, normes et pratiques en vigueur. L'utilisation du Service Cloud ne garantit pas la conformité à toute loi, réglementation, norme ou pratique.

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 Données de Sécurité

Dans le cadre du Service Cloud, qui comprend des activités de production de rapport, IBM préparera et gérera 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.

7.5 Cookies

Le Client reconnaît et accepte qu'IBM pourra, dans le cadre du fonctionnement et du support normaux du Service Cloud, collecter des informations personnelles auprès du Client (employés et sous-traitants du Client) liées à l'utilisation du Service Cloud, par le biais de processus de suivi et d'autres technologies. Cela permet à IBM de rassembler des statistiques et informations d'utilisation relatives à l'efficacité du Service Cloud pour améliorer l'acquis utilisateur et/ou personnaliser les interactions avec le Client. Le Client confirme qu'il obtiendra ou a obtenu l'accord permettant à IBM de traiter les informations personnelles collectées pour le but susmentionné chez IBM, d'autres sociétés d'IBM et leurs sous-traitants, quel que soit l'endroit où IBM et ses sous-traitants exercent leurs activités, conformément à la loi applicable. IBM se conformera aux demandes des employés et sous-traitants du Client pour l'accès, la mise à jour, la correction ou la suppression de leurs informations personnelles collectées.