IBM Resilient Security Orchestration, Automation and Response on Cloud

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 Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud permet aux organisations d'orchestrer et d'automatiser les personnes, processus et technologies associés à une intervention en cas d'incident.

IBM Resilient SOAR Platform on Cloud simplifie la gestion des interventions en cas d'incident et d'atteinte à la vie privée pour fournir un moyen automatique, plus rapide et plus flexible permettant aux organisations de réagir aux événements et incidents. Resilient SOAR Platform on Cloud sert de base pour assurer la protection de la cybersécurité, permettant aux organisations :

- de créer des plans d'intervention en fonction des normes et meilleures pratiques du secteur d'activité ;
- de s'intégrer plus facilement aux outils de sécurité et informatiques et d'orchestrer les réponses aux événements et incidents ;
- de collaborer dans toute l'organisation, en équipant les divers intervenants des outils permettant d'assumer leurs rôles et tâches dans le cadre des activités d'intervention.

IBM Resilient SOAR Platform est conçu pour les organisations de différentes tailles et complexités et est disponible à l'achat avec plusieurs modules complémentaires en option. Le Client n'est pas autorisé à utiliser les fonctionnalités sauf mention contraire dans l'offre ou le module complémentaire qu'il a acheté.

1.1 Offres

Le Client peut faire son choix parmi les offres disponibles suivantes :

1.1.1 IBM Resilient SOAR Platform on Cloud

IBM Resilient SOAR Platform on Cloud Orchestration sert de base à la protection de la cybersécurité. Les Clients peuvent créer des plans d'intervention en fonction des normes et meilleurs pratiques du secteur d'activité, s'intégrer aisément aux outils de sécurité et informatiques et orchestrer des réponses aux événements et aux incidents. Le Service Cloud facilite une collaboration dans toute l'organisation, ce qui permet aux divers intervenants d'assumer leurs rôles et tâches dans le cadre des activités d'intervention.

Les équipes de sécurité peuvent collaborer sur des événements et incidents de cybersécurité en utilisant les fonctionnalités de gestion de cas spécialement conçues de la plateforme. Les protocoles dynamiques s'adaptent aux attaques en évolution rapide, de sorte que les équipes peuvent reproduire les processus pour améliorer l'efficacité en personnalisant les protocoles, les zones de données et les formats d'affichage. Les simulations facilitent davantage l'amélioration des processus d'intervention. Des intégrations incorporées et installables permettent l'enrichissement des données en vue d'établir un cadre pour le processus de prise de décision d'une équipe de sécurité, ainsi que l'orchestration des actions correctives, conformément à la quantité d'Actions par mois achetées. L'intégration et l'analyse syntaxique des e-mails fournissent une méthode légère permettant l'escalade à partir d'autres outils. L'accès peut être sécurisé par le biais de l'authentification SAML. La transparence et l'analyse des risques sont facilitées à l'aide d'analyses et de rapports. Cette offre est requise pour tous les autres modules complémentaires ci-dessous.

1.2 Services Optionnels

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

IBM Resilient SOAR Platform on Cloud Actions active les fonctionnalités d'orchestration de la plateforme. Des intégrations incorporées et installables, y compris les intégrations aux divers flux de partage de renseignements sur les menaces, automatisent l'enrichissement en vue d'établir un cadre pour le processus de prise de décision d'une équipe de sécurité et permettent l'orchestration des actions correctives.

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

IBM Resilient SOAR Platform on Cloud Privacy permet aux Clients d'évaluer les atteintes à la protection des données et d'y réagir. Les plans d'intervention générés par cette offre s'adaptent aux types de données, aux quantités de dossiers et aux juridictions de régulation compétentes. Les Clients peuvent également accéder à une base de connaissances intégrée en matière de réglementations globales relatives à la notification des atteintes à la protection des données, qui aide à personnaliser davantage leurs plans d'intervention en cas d'incident.

1.2.3 IBM Resilient SOAR Platform on Cloud Team Management Add-On

IBM Resilient SOAR Platform on Cloud Teams permet la gestion des utilisateurs et la séparation des données entre plusieurs équipes. Les informations sensibles sont conservées selon les besoins, en limitant l'accès à l'aide d'Espaces de travail et du contrôle d'accès personnalisable basé sur des rôles. La gestion des utilisateurs et des groupes peut être simplifiée en optimisant Active Directory pour l'autorisation d'utilisateur. Des groupes distincts peuvent également être configurés pour qu'ils disposent de leur propre Organisation.

1.2.4 IBM Resilient SOAR Platform on Cloud MSSP Add-On

IBM Resilient SOAR Platform on Cloud MSSP fournit des fonctionnalités de gestion de cas, de processus, de protocole et de personnalisation pour plusieurs Organisations. Les événements et incidents de plusieurs Organisations peuvent être consultés dans une file d'attente unique, afin de donner aux analystes MSSP (Managed Security Service Provider) une vue globale de leurs clients. Les protocoles configurés par Organisation permettent la gestion simplifiée des processus normalisés et personnalisés.

1.2.5 IBM Resilient SOAR Platform on Cloud Non-Production Add-On

IBM Resilient SOAR Platform on Cloud Non-Production est une instance distincte d'IBM Resilient SOAR Platform que le Client peut utiliser uniquement pour des activités internes 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 pré-production, d'assurance qualité et/ou pour développer, à l'aide d'interfaces de programmation d'application publiées, des ajouts ou extension du Service Cloud utilisés en interne.

1.3 Services d'Accélération

Les offres IBM Security Expert Labs (SEL) for Resilient Services sont des services délivrés à distance qui fournissent des compétences d'expert Resilient en vue de conseils sur l'architecture et l'implémentation en lien avec le déploiement de Resilient. L'offre IBM Resilient Security, Orchestration and Response, sous la forme d'un Service Cloud ou d'un logiciel sur site, est une condition préalable à l'un quelconque de ces Services.

1.3.1 IBM SEL for Resilient Base Starter Service

Dans le cadre d'un engagement à distance de 5 jours, IBM :

- aidera à définir l'architecture d'IBM Security Resilient ;
- installera et configurera IBM Security Resilient (à l'endroit applicable) ;
- formera les Analystes et les Concepteurs à la configuration et l'utilisation des actuels plans d'intervention en cas d'incident du Client, afin de refléter les principales exigences des organisations du Client ;
- fournira des protocoles configurés d'IBM Security Resilient en fonction des processus uniques des organisations du Client ;
- fournira les procédures de suivi des métriques et indicateurs KPI définis, en fonction des besoins et des pratiques exemplaires du secteur d'activité des organisations du Client ; et
- identifiera les opportunités d'intégration permettant de prendre en charge, d'automatiser et d'orchestrer les processus de bout en bout.

1.3.2 IBM SEL for Resilient Premium Starter Service

Dans le cadre d'un engagement à distance de 3 jours, IBM :

- aidera à définir l'architecture d'IBM Security Resilient ;
- installera IBM Security Resilient (à l'endroit applicable) ;
- configurera initialement IBM Security Resilient dans l'environnement du Client ; et
- formera les Analystes et les Concepteurs à la configuration et l'utilisation des actuels plans d'intervention en cas d'incident du Client, afin de refléter les principales exigences des organisations du Client.

1.3.3 IBM SEL for Resilient Additional Day

Outre le service Base ou Premium Starter, IBM effectuera, au cours d'un engagement à distance d'un jour, toutes les activités liées à IBM Security Resilient qui doivent être convenues au préalable. Par exemple :

- fournir une assistance supplémentaire dans le cadre de l'installation ou la configuration d'IBM Security Resilient ou des extensions (à l'endroit applicable) ;
- fournir des formations ou aides supplémentaires aux Analystes pour qu'ils soient prêts à utiliser IBM Security Resilient en tant que solution SOAR clé du client ;
- guider les Concepteurs dans la configuration et l'utilisation de leurs propres 'Protocoles' reflétant les principales exigences des organisations du Client ; ou
- effectuer une analyse rapide de l'environnement IBM Security Resilient pour recommander les points susceptibles d'être améliorés.

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 Européen sur la Protection des Données (UE/2016/679) (RGPD) ; ou ii) d'autres lois relatives à la protection des données identifiées sur http://www.ibm.com/dpa/dpl s'appliquent.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=A47500205B1911E6865BC3F213DB63F7

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 Utilisateur Autorisé est un utilisateur unique autorisé à accéder aux Services Cloud directement ou indirectement (par exemple, via un logiciel de multiplexage, un périphérique ou un serveur d'applications), par quelque moyen que ce soit.
- Un Utilisateur Simultané est un utilisateur qui accède au Service Cloud directement ou indirectement (par exemple, par le biais d'un logiciel de multiplexage, d'un périphérique ou d'un serveur d'applications), à un moment donné. Une personne qui accède simultanément au Service Cloud à plusieurs reprises n'est considérée que comme un Utilisateur Simultané unique.
- Un Engagement est un service professionnel ou de formation relatif aux Services Cloud.
- Un Elément est une occurrence d'un élément caractéristique, qui est gérée par, traitée par ou relative à l'utilisation du Service Cloud. Pour les besoins de ce Service Cloud, un Elément est une Action. Une Action est une demande d'orchestration ou d'automatisation soumise par le Service Cloud à un autre logiciel.

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 Vérification

Le Client i) conservera, et fournira sur demande, des enregistrements et des sorties d'outils système, comme cela s'avère raisonnablement nécessaire pour permettre à IBM et son auditeur indépendant de vérifier le respect du Contrat par le Client, et ii) commandera et paiera dans les plus brefs délais tout droit d'utilisation requis aux prix en vigueur d'IBM, ainsi que toutes autres dépenses ou obligations déterminées par suite de ladite vérification, comme indiqué par IBM dans une facture. Ces obligations de vérification de la conformité demeurent en vigueur pendant toute la durée du Service Cloud et pendant les deux années suivantes.

5.2 Obligation d'autorisation de module complémentaire

Le Client doit acquérir un nombre et un type d'autorisation équivalents pour le Service Cloud de base et tout Service Cloud complémentaire (Add-On).

5.3 Restrictions d'utilisation

Chaque Client est autorisé à effectuer un maximum de cent milliers (100 000) de requêtes de Service de Menace par mois. Le Client crée une requête de Service de Menace en ajoutant un artefact à un incident lorsque son Service de Menace a été activé. Tous les deux (2) jours suivants où l'incident reste ouvert et actif, une nouvelle requête de Service de Menace sera automatiquement générée.

Chaque Client est autorisé à générer un maximum de cent (100) e-mails de notification par jour par Utilisateur Autorisé/Simultané. Les e-mails de notification sont générés par la plateforme Resilient basée sur une configuration contrôlée par le Client.

5.4 Autres informations relatives au traitement et à la protection des données

Pour éviter toute confusion, IBM Resilient SOAR Platform on Cloud :

- ne chiffre pas le Contenu qui est stocké ;
- n'est pas conçu pour traiter une quelconque Catégorie Particulière de Données à caractère personnel ; et
- ne doit pas permettre la saisie de données à caractère personnel dans les zones de texte libre, en l'absence d'une demande.

Des informations détaillées relatives au chiffrement et aux types de Données à caractère personnel traitées sont disponibles à l'adresse URL des Fiches Techniques référencées dans la Clause 2 ci-dessus.

6. Dispositions dérogatoires

6.1 Utilisation de Données

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 du Client (Observations) 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.