Conditions d'Utilisation IBM – Conditions Spécifiques de l'Offre SaaS

IBM Application Security on Cloud

Les Conditions d'Utilisation regroupent les présentes Conditions d'Utilisation IBM – Conditions Spécifiques de l'Offre SaaS (« Conditions Spécifiques de l'Offre SaaS ») et un document intitulé Conditions d'Utilisation IBM – Conditions Générales (« Conditions Générales ») disponibles à l'adresse URL suivante : http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

En cas de conflit, les Conditions Spécifiques de l'Offre IBM SaaS prévalent sur les Conditions Générales. En accédant à l'Offre IBM SaaS, en la commandant ou en l'utilisant, le Client de l'Offre IBM SaaS accepte les présentes Conditions d'Utilisation.

Les Conditions d'Utilisation sont régies par le Contrat International IBM Passport Advantage, le Contrat International IBM Passport Advantage Express ou le Contrat International IBM relatif à une Sélection d'Offres IBM SaaS, selon le cas (ci-après le « Contrat ») qui, avec les Conditions d'Utilisation, représentent l'intégralité de l'accord entre les parties.

1. Offres IBM SaaS

Les Conditions Spécifiques de l'Offre SaaS s'appliquent aux Offres IBM SaaS suivantes :

- IBM Application Security Analyzer

2. Unités de Mesure des Redevances

L'Offre IBM SaaS est vendue en fonction des unités de mesure de redevance suivantes indiquées dans le Document de Transaction :

a. **Instance d'Application** : unité de mesure par laquelle l'Offre IBM SaaS peut être acquise. Un droit d'utilisation d'Instance d'Application est requis pour chaque instance d'une Application connectée à l'Offre IBM SaaS. Si une Application possède plusieurs composants, chacun visant un but et/ou une base utilisateur distincts et chacun de ces termes pouvant être connecté à ou géré par l'Offre IBM SaaS, chacun desdits composants est considéré comme étant une Application distincte. En outre, les environnements de test, de développement, de transfert et de production pour une Application sont chacun considérés comme étant des instances distinctes de l'Application et chacun doit disposer d'un droit d'utilisation. Les instances d'Application multiples dans un environnement unique sont chacune considérées comme étant des instances distinctes de l'Application et chacune doit disposer d'un droit d'utilisation. L'obtention des droits d'utilisation adéquats est nécessaire pour couvrir le nombre d'Instances d'Application connectées à l'Offre IBM SaaS pendant la période de mesure indiquée dans l'Autorisation d'Utilisation ou le Document de Transaction du Client.

b. **Accès** : unité de mesure par laquelle l'Offre IBM SaaS peut être acquise. Un Accès est le droit d'utilisation de l'Offre IBM SaaS. Le Client doit se procurer une autorisation d'Accès unique pour utiliser l'Offre IBM SaaS pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (ci-après « Autorisation d'Utilisation » ou « PoE ») ou un Document de Transaction du Client.

3. Redevances et Facturation

Le montant à régler pour l'Offre IBM SaaS est indiqué dans un Document de Transaction.

3.1 Paiement à l'utilisation

Les options de paiement à l'utilisation (Pay per Use) seront facturées le mois suivant lequel le service est utilisé au tarif indiqué dans le Document de Transaction.

3.2 Redevance Mensuelle Partielle

Une Redevance Mensuelle Partielle, comme indiqué dans le Document de Transaction, peut être estimée au prorata.

4. Support Technique

Pendant la Période d'Abonnement et après notification d'IBM indiquant au Client que l'accès à l'Offre IBM SaaS est disponible, le support technique est fourni sur les forums en ligne et sous forme de support standard pendant la période des redevances de paiement à l'utilisation (Pay per Use) encourues par le Client. A partir de l'Offre IBM SaaS, les Clients peuvent soumettre un ticket de support ou ouvrir une session de discussion à des fins d'assistance. IBM mettra à disposition le manuel IBM Software as a Service Support Handbook qui contient les coordonnées des personnes à contacter ainsi que des informations et processus relatifs au support technique.

Niveau de gravité	Définition de la gravité	Objectifs de temps de réponse	Couverture de temps de réponse
1	**Impact critique sur les activités/indisponibilités 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 ne s'agit pas d'un 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

4.1 Accès aux Données du Client

IBM pourra accéder aux données du Client afin de diagnostiquer les problèmes liés au service et de faciliter les analyses de l'application du Client par le service. IBM accédera aux données uniquement pour corriger les défauts ou fournir une assistance pour les produits ou services IBM.

5. Dispositions Supplémentaires Spécifiques à l'Offre IBM SaaS

Il se peut que les scannages de sécurité n'identifient pas tous les risques de sécurité dans une application.

L'Offre IBM SaaS peut être utilisée pour aider le Client à respecter les obligations de conformité, qui peuvent être fondées sur des lois, réglementations, normes ou pratiques. Toutes instructions, toute utilisation recommandée ou tous conseils fournis par le Service ne constituent pas un avis juridique, comptable ou autre avis professionnel et le Client devra se procurer son propre conseiller juridique ou autre conseiller qualifié. Le Client 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 de ce Service ne garantit pas la conformité à toute loi, réglementation, norme ou pratique.

L'Offre IBM SaaS exécute des tests invasifs et non invasifs sur le site Web et l'application Web ou mobile que le Client choisit de scanner. Ces tests impliquent certains risques, y compris, sans s'y limiter, ce qui suit :

a. les systèmes informatiques du Client, lorsqu'ils exécutent des applications à tester, peuvent s'arrêter de façon inopinée ou tomber en panne, et ainsi être temporairement indisponibles ou donner lieu à une perte de données ;

b. les performances et le débit des systèmes du Client, ainsi que les performances et le débit des routeurs et firewalls associés, peuvent être temporairement dégradés pendant les tests ;

c. des quantités excessives de messages d'historique (log) peuvent être générées, provoquant une consommation excessive d'espace disque pour les fichiers journaux ;

d. les données peuvent être modifiées ou supprimées du fait de l'examen des vulnérabilités ;

e. des alarmes peuvent être déclenchées par les systèmes de détection d'intrusion ;

f. des e-mails peuvent être déclenchés par la fonction de messagerie électronique de l'application Web à tester ;

et

g. le service Cloud peut intercepter le trafic du réseau contrôlé afin de rechercher des événements.

Dans le cas où le Client entre dans le Service des données de connexion authentifiées pour l'application à tester, le Client ne doit saisir ces données que pour les comptes de test et non pour les utilisateurs de production. L'utilisation des données d'identification d'utilisateur de production peut donner lieu à la transmission de données personnelles via le Service.

L'Offre IBM SaaS peut être configurée pour scanner les applications Web de production. Lorsque le Client désigne le type de scannage par « production », le service est destiné à effectuer des scannages de manière à réduire les risques énumérés ci-dessus ; cependant, dans certaines situations, le Service Cloud peut entraîner la dégradation ou l'instabilité des performances dans l'infrastructure et les sites de production testés. IBM ne garantit en aucun cas que l'utilisation du Service Cloud est adaptée au scannage des sites de production.

IL INCOMBE AU CLIENT DE DÉTERMINER SI LE SERVICE EST APPROPRIE OU SÉCURISÉ POUR LE SITE WEB, L'APPLICATION WEB, L'APPLICATION MOBILE OU L'ENVIRONNEMENT TECHNIQUE DU CLIENT.

L'Offre IBM SaaS est conçue pour identifier divers problèmes de sécurité et de conformité potentiels au niveau des applications mobiles et Web et des services Web. Il ne teste pas toutes les vulnérabilités ou tous les risques de conformité et ne constitue pas une barrière aux attaques de sécurité. Les menaces, réglementations et normes en matière de sécurité changent constamment et il se peut que le Service ne reflète pas tous ces changements. Le Client est seul responsable de la sécurité et de la conformité de ses applications Web, systèmes et employés ainsi que de toutes mesures correctives. Il relève de sa seule décision d'utiliser ou non l'une quelconque des informations fournies par le Service.

Certaines lois interdisent toute tentative non autorisée d'intrusion ou d'accès aux systèmes informatiques. IL INCOMBE AU CLIENT DE VEILLER A NE PAS UTILISER LE SERVICE POUR SCANNER DES SITES WEB ET/OU DES APPLICATIONS AUTRES QUE LES SITES WEB ET/OU APPLICATIONS DONT IL EST PROPRIÉTAIRE OU CEUX POUR LESQUELS IL A LE DROIT ET L'AUTORISATION DE SCANNER.

5.2 Cookies

Le Client reconnaît et accepte qu'IBM peut, dans le cadre du fonctionnement et du support normaux de l'Offre IBM SaaS, collecter des informations personnelles auprès du Client (employés et sous-traitants du Client) liées à l'utilisation de l'Offre IBM SaaS, 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 de l'Offre IBM SaaS 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.

5.3 Sites Bénéficiaires Dérivés

Le cas échéant, les taxes sont fonction du(es) site(s) que le Client identifie comme bénéficiant de l'Offre IBM SaaS. IBM appliquera les taxes en fonction de l'adresse indiquée lors de la commande d'une Offre IBM SaaS comme étant le site bénéficiaire principal, sauf si le Client fournit des informations supplémentaires à IBM. Le Client est responsable de la mise à jour de ces informations et est tenu de fournir les éventuelles informations à IBM.

Annexe A

1. Description générale d'IBM Application Security on Cloud

IBM Application Security on Cloud offre un emplacement unique aidant le Client à identifier les vulnérabilités en matière de sécurité (par exemple, Injection SQL, XSS (Cross-Site Scripting) et Fuite de Données) pour un large éventail d'applications. Le service comprend divers types de techniques de scannage de la sécurité d'une application, chacune identifiant les problèmes de sécurité dans cette application.

IBM Application Security on Cloud permet les fonctions suivantes :

- Scannage des applications mobiles à la recherche des vulnérabilités en matière de sécurité. Ce scannage est effectué par le biais des techniques d'analyse de sécurité dynamiques (blackbox) et interactives (glassbox).
- Scannage des sites Web de production ou de pré-production à la recherche des vulnérabilités en matière de sécurité. Ce scannage est effectué par le biais des techniques d'analyse de sécurité dynamiques (blackbox).
- Scannage des flux de données dans les applications Web et bureautiques à la recherche des vulnérabilités en matière de sécurité. Ce scannage est effectué par le biais des techniques d'analyse de sécurité statiques (whitebox).
- Rapports détaillés sur les vulnérabilités en matière de sécurité, comprenant des récapitulatifs détaillés des résultats et des procédures de résolution pouvant être suivies par les développeurs.
- Intégration à diverses plateformes DevOps, telles que Maven et IBM UrbanCode