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 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
- IBM Application Security on Cloud Consulting Services

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. **Job** : unité de mesure par laquelle l'Offre IBM SaaS peut être acquise. Un Job est un objet au sein de l'Offre IBM SaaS qui ne peut être divisé et qui représente un processus informatique incluant tous ses sous-processus. Des droits d'utilisation suffisants sont nécessaires pour couvrir le nombre total de Jobs traités ou gérés par l'Offre IBM SaaS pendant la période de mesure indiquée dans l'Autorisation d'Utilisation du Client ou dans un Document de Transaction.

b. **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. Des droits d'utilisation suffisants sont nécessaires 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 (PoE) ou le Document de Transaction du Client.

   Pour les besoins de cette Offre IBM SaaS :

   - Pour les tests dynamiques : un site Web adressable par le biais d'une URL publique ou privée. Chaque Instance d'Application donne droit à un site de 1000 pages maximum dans un domaine unique.
   - Pour les tests statiques : une unité de code exécutable dans un langage de programmation unique. Chaque Instance d'Application donne droit à des unités de scannage de code de 1 000 000 lignes maximum.
   - Pour les tests mobiles : une unité de code binaire pouvant être exécutée sur un appareil mobile. Chacune des plateformes mobiles (par exemple, iOS et Android) constitue des Instances d'Application différentes.

c. **Instance** : unité de mesure par laquelle l'Offre IBM SaaS peut être acquise. Une Instance est l'accès à une configuration spécifique de l'Offre IBM SaaS. Des droits d'utilisation suffisants sont

nécessaires pour chaque Instance de l'Offre IBM SaaS mise à disposition à des fins d'accès et d'utilisation pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (« PoE ») ou le Document de Transaction du Client.

Pour chaque droit d'utilisation d'Instance, le nombre de Jobs effectués ou d'Instances d'Application (Applications connectées) n'est pas limité, étant entendu toutefois qu'au maximum 30 Jobs peuvent être en cours d'exécution à un moment donné.

d. **Engagement** : unité de mesure par laquelle les services peuvent être acquis. Un Engagement comprend des services professionnels et/ou de formation relatifs à l'Offre IBM SaaS. L'obtention de droits suffisants est nécessaire pour couvrir chaque Engagement.

3. Redevances et Facturation

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

3.1 Redevances Mensuelles Partielles

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

3.2 Redevances de dépassement

Si l'utilisation réelle de l'Offre IBM SaaS 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.

3.3 Frais de Configuration

La configuration sera facturée au Client, comme indiqué dans le Document de Transaction.

4. Durée et Options de Renouvellement

La durée de l'Offre IBM SaaS commence à la date à laquelle IBM notifie au Client que ce dernier a accès à l'Offre IBM SaaS, comme décrit dans l'Autorisation d'Utilisation. L'Autorisation d'Utilisation indiquera si l'Offre IBM SaaS est renouvelée automatiquement, si elle se poursuit en continu ou si elle prend fin à l'issue de la durée.

Pour un renouvellement automatique, l'Offre IBM SaaS est automatiquement renouvelée pour la durée indiquée dans l'Autorisation d'Utilisation, sauf si le Client notifie par écrit, au moins 30 jours avant la date d'expiration de la durée, son intention de ne pas renouveler.

Pour une utilisation en continu, l'Offre IBM SaaS continuera d'être disponible mois par mois jusqu'à ce que le Client notifie la résiliation moyennant un préavis écrit de 30 jours. L'Offre IBM SaaS demeure disponible jusqu'à la fin du mois suivant ladite période de 30 jours.

5. 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	Temps de Réponse Initiaux	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

Niveau de Gravité	Définition de la Gravité	Temps de Réponse Initiaux	Couverture de Temps de Réponse
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

5.1 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.

6. Dispositions supplémentaires spécifiques à l'Offre IBM SaaS

Les scannages de la sécurité peuvent ne pas identifier tous les risques de sécurité dans une application et ils ne sont ni créés, ni conçus pour une utilisation dans des environnements à risque nécessitant des dispositifs à sûreté intégrée, par exemple et de façon non limitative, la navigation aérienne, les systèmes de contrôle du trafic aérien, les systèmes d'armement, les systèmes médicaux d'assistance respiratoire, les installations nucléaires, etc., domaines dans lesquels la non-identification des risques de sécurité peut entraîner la mort, des blessures corporelles ou des dommages matériels. Le fonctionnement ininterrompu ou sans erreur des scannages de la sécurité n'est pas garanti.

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. Certaines lois interdisent toute tentative non autorisée d'intrusion ou d'accès aux systèmes informatiques. Le Client autorise IBM à exécuter les Services, tels qu'ils sont décrits dans les présentes, et reconnaît qu'ils constituent un accès autorisé aux systèmes informatiques du Client. IBM peut dévoiler cet octroi de pouvoir à un tiers s'il le juge nécessaire pour exécuter les Services.

Les 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 ;

g. l'Offre IBM SaaS peut intercepter le trafic du réseau contrôlé afin de rechercher des événements.

Pendant les activités de test, le Client renonce à tous droits ou recours liés à tout accord relatif aux niveaux de service, qui sont fournis par IBM et relatifs aux sites Web ou applications soumis au test.

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 à caractère personnel 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, l'Offre IBM SaaS 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 de l'Offre IBM SaaS 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.

Par souci de clarté, le Contenu du Client décrit dans la clause de protection de données des Conditions d'Utilisation – Conditions Générales est également réputé inclure les données pouvant devenir accessibles à IBM pendant les Tests d'Intrusion d'Application.

6.1 Systèmes détenus par un Tiers

Pour les systèmes (ce qui, pour les besoins de la présente disposition, comprend, sans s'y limiter, les applications et les adresses IP) détenus par un tiers et qui feront l'objet de tests aux termes des présentes, le Client accepte :

a. de se procurer, avant qu'IBM ne commence les tests sur un système tiers, une lettre signée du propriétaire de chaque système, autorisant IBM à fournir les Services sur ledit système, indiquant l'acceptation par le propriétaire des conditions exposées dans la section intitulée « Autorisation d'effectuer des tests », et de fournir à IBM un exemplaire de ladite autorisation ;

b. de prendre l'entière responsabilité de communiquer au propriétaire de chaque système les éventuels risques, expositions et vulnérabilités identifiés sur ce système grâce aux tests à distance d'IBM ; et

c. si IBM le juge nécessaire, de permettre et faciliter l'échange d'informations entre le propriétaire du système et IBM.

Le Client accepte :

- d'informer immédiatement IBM chaque fois qu'il y a un changement de propriété de tout système faisant l'objet des tests stipulés par les présentes ;
- de ne pas divulguer, en dehors de son Entreprise, les livrables ou le fait qu'IBM a effectué les Services, sans l'accord préalable écrit d'IBM ; et
- d'indemniser IBM en intégralité pour toutes pertes ou responsabilités encourues par IBM en raison de réclamations de tiers découlant du non-respect par le Client des dispositions de la présente section intitulée « Systèmes détenus par un Tiers » et pour toutes assignations ou réclamations de tiers à l'encontre d'IBM ou des sous-traitants ou agents d'IBM, découlant (a) du test des risques, expositions ou vulnérabilités de la sécurité des systèmes objet des tests stipulés dans les

présentes, (b) de la remise des résultats desdits tests au Client ou (c) de l'utilisation ou la divulgation desdits résultats par le Client.

6.2 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.

Dans le cadre des Offres IBM SaaS, qui comprennent des activités de production de rapport, IBM préparera et gérera les informations anonymes et/ou cumulées extraites des Offres IBM SaaS (dénommées ci-après « 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.

6.3 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.

6.4 Informations Personnelles et Contenu et Services réglementés

Cette Offre IBM SaaS 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 cette Offre IBM SaaS répond à ses besoins quant au type du Contenu que le Client utilise en rapport avec l'Offre IBM SaaS.

IBM n'agit pas en tant que prestataire de services soumis aux réglementations de la FCC (Federal Communications Commission) ou des organismes de réglementation d'Etat, et ne vise pas à fournir de quelconques services soumis aux réglementations de la FCC ou des organismes de réglementation d'Etat. Si la FCC ou tout organisme de réglementation d'Etat impose des contraintes ou des obligations réglementaires spécifiques sur l'un quelconque des services fournis par IBM au titre des présentes, IBM peut être amenée : (a) à modifier, remplacer ou substituer des produits aux frais du Client, et/ou (b) à modifier les modalités selon lesquelles ces services sont fournis au Client afin d'éviter de se voir appliquer lesdites contraintes ou obligations (en agissant, par exemple, pour le compte du Client en qualité d'agent habilité à se procurer ces services auprès d'un opérateur indépendant).

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, accessibles au grand public ou sur un réseau privé, 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

1.1 IBM Application Analyzer

IBM Application Analyzer peut être commandé par Instance d'Application Instance, par Job (scan), ou sous la forme d'une Instance complète et permet les types de scannage suivants :

- Dynamic Analyzer – Test des sites Web de préproduction ou de production par le biais des techniques DAST
- Mobile Analyzer – Test des binaires iOS ou Android par le biais des techniques IAST
- Static Analyzer – Test de flux de données de code d'octets et de code source par le biais des techniques SAST

1.2 Service de Configuration

IBM Application Security on Cloud Consulting Services est un service de configuration productisé pour Application Analyzer. Le Service fait appel aux consultants IBM pour fournir des services de conseils et d'assistance en matière de test et de gestion des risques d'application. IBM Application Security on Cloud Consulting Services est disponible à l'achat en lots d'Engagements pouvant être dépensés dans les quantités indiquées ci-dessous pour demander et utiliser les services spécifiques suivants :

a. **Fast Start** [Utilise une (1) unité d'Engagement]

Le service Fast Start fournit l'expertise et les conseils nécessaires pour utiliser les fonctionnalités de test et de gestion des risques d'Application Security on Cloud. Une fois que le Client aura confirmé que la connexion au portail Application Security on Cloud a abouti, IBM organisera une conférence Web d'une durée maximale de deux (2) heures et pour deux (2) participants actifs afin de dispenser une formation à la sécurité d'application de base sur les configurations et fonctions d'Offre IBM SaaS, y compris les types de scannage, l'exécution des scannages, l'examen des rapports et l'installation des outils et plug-ins associés. Le service Fast Start sera terminé à l'issue (a) du cyberséminaire de formation client, (b) de l'installation des outils et plug-ins applicables et (c) de l'assistance fournie au Client pour configurer et exécuter le premier scannage du Client.

b. **Assessment Review** [utilise deux (2) unités d'Engagement]

Le service Assessment Review fournit une assistance pour l'examen d'un résultat de test, y compris la compréhension et la hiérarchisation des solutions aux vulnérabilités dans l'application. IBM organisera une conférence Web d'une durée maximale d'une (1) heure pour deux (2) participants actifs afin de présenter les vulnérabilités détectées et le risque de sécurité global de l'application,

ainsi qu'une discussion détaillée des vulnérabilités en matière de sécurité de l'application détectées, y compris (1) la façon dont la vulnérabilité a été testée, (2) la méthode de détection des vulnérabilités, (3) l'identification du risque de chaque vulnérabilité et (4) les recommandations de correction générales aidant à résoudre la vulnérabilité. L'examen sera fondé exclusivement sur le résultat du test et ne sera pas un examen du code source proprement dit. Le Client étudiera le résultat du test et le notifiera à IBM à des fins d'examen avant la conférence Web. Le service Assessment Review sera terminé à l'issue de la conférence Web.

c. **Scan for Me** [utilise quatre (4) unités d'Engagement]

Le service Scan for Me met à disposition un spécialiste IBM en matière de sécurité d'application, qui configurera et exécutera un scannage, validera les résultats et organisera une séance d'informations afin de passer en revue les résultats. Le Client autorisera un consultant IBM à accéder à son environnement ASoC pour configurer et exécuter un scannage, valider les résultats, fournir des recommandations sur la hiérarchisation des solutions et organiser une séance d'informations sur les résultats. IBM organisera une conférence Web d'une durée maximale d'une (1) heure pour deux (2) participants actifs afin de présenter les vulnérabilités détectées et le risque de sécurité global de l'application, ainsi qu'une discussion détaillée des vulnérabilités en matière de sécurité de l'application détectées, y compris (1) la façon dont la vulnérabilité a été testée, (2) la méthode de détection des vulnérabilités, (3) l'identification du risque de chaque vulnérabilité et (4) les recommandations de correction générales aidant à résoudre la vulnérabilité. A la demande et jusqu'à 30 jours après le scannage initial, IBM réalisera un nouveau scannage à l'aide de la configuration du scannage initial uniquement pour vérifier les correctifs de sécurité et non pour tester les nouvelles fonctionnalités, valider les résultats et présenter un rapport au Client. Le service Scan for Me sera terminé à l'issue de la conférence Web pour passer en revue les résultats du scannage initial ou, le cas échéant, à l'issue du nouveau scannage, à la demande du Client, et de la remise du rapport sur le nouveau scannage au Client.

d. **Advisor on Demand** [utilise sept (7) unités d'Engagement]

Le service Advisor on Demand fournit jusqu'à vingt (20) heures du temps d'un consultant IBM pouvant être utilisées pour les activités liées à l'Offre IBM SaaS. Le consultant IBM aidera à traiter les sujets spécifiques à la sécurité d'application, y compris, mais sans limitation, la gestion de programme, la hiérarchisation des tests de sécurité, les stratégies de résolution, ainsi que l'analyse et la réparation de code source. IBM collaborera avec le Client pour comprendre et élaborer un planning de projet en fonction des besoins spécifiques du Client, y compris les objectifs du projet, les technologies appropriées, les délais souhaités, les livrables attendus et le nombre prévisionnel d'engagements de service Advisor on Demand. Le Client doit autoriser l'accès aux applications, systèmes et documentations nécessaires pour la réalisation des services. Le service Advisor on Demand sera terminé à l'issue d'un maximum de 20 heures d'expertise en matière de sécurité et/ou une fois que le planning de projet et/ou les livrables définis dans le planning de projet auront été remis au Client.

e. **Test d'intrusion d'application**

Trois options :

(1) **Test d'intrusion d'application de base/conformité**, qui comprend jusqu'à quarante (40) heures du temps d'un consultant et qui porte essentiellement sur les défauts de logique à une seule étape, ainsi que les versions plus simples des failles d'injection. Utilise quinze (15) unités d'Engagement.

(2) **Test d'intrusion d'application standard**, qui comprend jusqu'à soixante (60) heures du temps d'un consultant et qui élargit la portée de manière à inclure les défauts de logique dans des workflows à plusieurs étapes, des versions complexes des failles d'injection et l'analyse des types de données complexes. Utilise vingt-et-une (21) unités d'Engagement.

(3) **Test d'intrusion d'application avancé**, qui comprend jusqu'à quatre-vingt (80) heures du temps d'un consultant et qui élargit la portée de manière à inclure l'ingénierie inverse des exécutables compilés, la dissection des protocoles de réseau personnalisés, l'analyse approfondie des bibliothèques et infrastructures accessibles au public. Utilise vingt-sept (27) unités d'Engagement.

Le service de test d'intrusion d'application met à disposition une ressource IBM pour le test et l'exploitation d'une application, la remise d'un rapport de test et l'organisation d'une séance d'informations pour expliquer les conclusions et les risques associés.

IBM organisera une réunion de lancement de projet d'une durée maximale d'une (1) heure et pour deux (2) participants actifs, afin de passer en revue l'environnement et l'organisation du Client, notamment la plateforme d'application, l'architecture, les infrastructures, l'infrastructure de support, les problèmes ou les préoccupations de sécurité connus associés à l'application, le planning de test préliminaire et le plan de contact d'urgence.

IBM organisera le test d'intrusion d'application, y compris, mais sans limitation : l'identification des vulnérabilités courantes, telles que l'injection SQL et le cross-site scripting (XSS), l'évaluation des forces et faiblesses des dispositifs de contrôle de sécurité existants, par exemple la validation, l'authentification et l'autorisation des saisies, la vérification de la mise en œuvre appropriée de la logique métier, la validation de l'utilisation correcte des protocoles sécurisés, l'identification des défauts de gestion de session, ainsi que la vérification des dispositifs de contrôle de sécurité appropriés lors de la connexion, la récupération de mot de passe, les règles de gestion de mot de passe et d'autres fonctions de gestion utilisateur. Les résultats seront consignés dans le rapport de test d'intrusion d'application. IBM organisera une conférence Web d'une durée maximale d'une (1) heure pour la présentation de rapport. Le service de test d'intrusion d'application sera terminé une fois que les heures de conseils imparties auront été utilisées, la conférence Web organisée et le rapport de test d'intrusion d'application définitif remis au Client.

1.2.1 Responsabilités relatives aux Services de Configuration

IBM :

- fournira des Services de Configuration à l'aide des unités d'Engagement achetées par le Client et conformément à l'Autorisation d'Utilisation (PoE) ; et
- a terminé un Service de Configuration une fois que les critères d'achèvement décrits dans la Clause 1.2 auront été remplis.

Le Client accepte :

- de prendre à sa charge tous les frais associés à toutes les demandes d'Engagement présentées par le Client pendant la durée du contrat ;
- et reconnaît que les unités d'Engagement achetées doivent être utilisées pendant la durée initiale du contrat et qu'elles arrivent à expiration si elles ne sont pas utilisées avant la date de fin de la période contractuelle ; et
- de présenter une demande formelle pour tous les Services de Configuration au moins 30 jours avant la date de fin de l'abonnement.

Lors de la réalisation d'un Service de Configuration, IBM peut demander au Client des informations et une coopération raisonnable. Si le Client ne fournit pas la coopération et les informations demandées dans les délais, IBM se réserve le droit de facturer les unités d'Engagement requises par les services ou le retard de réalisation du service concerné.

Pour qu'IBM puisse mener les tests avec précision, le Client s'engage à respecter les instructions d'IBM relatives à la préparation et l'entretien de l'environnement pendant la période de test.