

IBM Application Security on Cloud

Les Conditions d'utilisation se composent du présent document intitulé «Conditions d'utilisation IBM – Modalités relatives aux offres de Logiciel-service» (les «Modalités des offres de Logiciel-service») et d'un document intitulé «Conditions d'utilisation IBM – Modalités générales» (les «Modalités générales»), qui est disponible à l'adresse <http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/>.

Advenant une incompatibilité entre les Modalités générales et les présentes Modalités des offres de Logiciel-service, ces dernières prévaudront. Le Client accepte les présentes Conditions d'utilisation en commandant le Logiciel-service IBM, en y accédant ou en l'utilisant.

Ces Conditions d'utilisation sont régies par le Contrat Passport Advantage international IBM, le Contrat Passport Advantage Express international IBM ou le Contrat international régissant les offres désignées relatives aux Logiciels-services IBM (aussi appelés Logiciels sous forme de services), selon le cas (le «Contrat»), et celui-ci, de pair avec les Conditions d'utilisation, constitue l'entente intégrale.

1. Logiciel-service IBM

Les offres de Logiciel-service IBM suivantes sont régies par les présentes Modalités des offres de Logiciel-service :

- IBM Application Security on Cloud
- IBM Application Security on Cloud Consulting Services

2. Paramètres de calcul des frais

Le Logiciel-service IBM est vendu en fonction d'un des paramètres de calcul des frais suivants, comme spécifié dans le Document transactionnel :

- a. Un **Travail** est une unité de mesure servant de base pour obtenir le Logiciel-service IBM. Un Travail est un objet dans le Logiciel-service IBM qui ne peut pas être subdivisé et correspond à un processus informatique qui inclut tous ses sous-processus. Il faut obtenir un nombre suffisant d'autorisations pour couvrir le nombre total de Travaux qui sont traités ou gérés par le Logiciel-service IBM pendant la période de mesure indiquée dans l'Autorisation d'utilisation ou le Document transactionnel du Client.
- b. Une **Instance d'application** est une unité de mesure servant de base pour obtenir le Logiciel-service IBM. Une autorisation d'utilisation d'une Instance d'application est requise pour chaque instance d'une Application connectée au Logiciel-service IBM. Si une Application comprend de multiples composants, et que chaque composant sert à une fin distincte ou à des utilisateurs distincts et peut être connecté au Logiciel-service IBM ou être géré par ce dernier, chacun de ces composants est alors considéré comme une Application distincte. De plus, les environnements de test, de développement, de bac à sable et de production pour une Application sont tous considérés comme des instances séparées de l'Application, de sorte que chacun d'eux nécessite une autorisation d'utilisation. De multiples Instances d'application dans un seul environnement sont considérées chacune comme étant des instances distinctes de l'Application et chacune d'elles nécessite une autorisation d'utilisation. Il faut obtenir un nombre suffisant d'autorisations pour couvrir le nombre d'Instances d'application connectées au Logiciel-service IBM pendant la période de mesure indiquée dans l'Autorisation d'utilisation ou le Document transactionnel du Client.

Pour les besoins du présent Logiciel-service IBM :

- Pour les tests dynamiques : site Web accessible par le biais d'une adresse URL publique ou privée. Chaque Instance d'application donne droit à un site d'un maximum de mille (1 000) pages dans un seul domaine.
- Pour les tests statiques : unité de code exécutable dans un seul langage de programmation. Chaque Instance d'application autorise l'analyse d'unités de code d'un maximum d'un million (1 000 000) de lignes.

- Pour les tests mobiles : unité de code binaire pouvant être exécutée sur un appareil mobile. Chaque plateforme mobile différente (p. ex., iOS et Android) constitue une Instance d'application distincte.
- c. Une **Instance** est une unité de mesure servant de base pour obtenir le Logiciel-service IBM. Une Instance correspond à un accès à une configuration spécifique du Logiciel-service IBM. Il faut obtenir un nombre suffisant d'autorisations pour couvrir chaque Instance du Logiciel-service IBM mise en disponibilité aux fins d'accès et d'utilisation pendant la période de mesure indiquée dans l'Autorisation d'utilisation ou le Document transactionnel du Client.
Chaque Instance autorisée donne la possibilité de traiter un nombre illimité de Travaux ou d'utiliser un nombre illimité d'Instances d'application (Applications connectées). Il n'est toutefois pas possible de traiter plus de trente (30) Travaux simultanément.
- d. Un **Mandat** est une unité de mesure servant de base pour obtenir les services. Un Mandat correspond à des services professionnels ou de formation liés au Logiciel-service IBM. Il faut obtenir un nombre suffisant d'autorisations pour couvrir chaque Mandat.

3. Frais et facturation

Le montant exigible pour le Logiciel-service IBM est indiqué dans un Document transactionnel.

3.1 Frais mensuels partiels

IBM peut imposer des frais mensuels partiels, calculés au prorata, comme spécifié dans le Document transactionnel.

3.2 Frais d'utilisation excédentaire

Si l'utilisation réelle que fait le Client du Logiciel-service IBM au cours de la période de mesure excède l'utilisation autorisée spécifiée dans l'Autorisation d'utilisation, le Client devra payer des frais d'utilisation excédentaire, au tarif indiqué dans le Document transactionnel.

3.3 Frais de mise en place

Des frais de mise en place seront facturés au Client selon le tarif indiqué dans le Document transactionnel.

4. Période d'abonnement et options de renouvellement

La Période d'abonnement au Logiciel-service IBM commence à la date à laquelle IBM avise le Client qu'il a accès au Logiciel-service IBM, comme indiqué dans l'Autorisation d'utilisation. Ce dernier document spécifiera si l'abonnement au Logiciel-service IBM se renouvelle automatiquement, s'il se poursuit sur une base continue ou s'il se termine à la fin de la Période d'abonnement.

Dans le cas d'un renouvellement automatique, l'abonnement au Logiciel-service IBM se renouvellera automatiquement pour la Période d'abonnement spécifiée dans l'Autorisation d'utilisation, à moins que le Client n'avise IBM par écrit de sa décision de ne pas renouveler l'abonnement, au moins trente (30) jours avant la fin de la Période d'abonnement.

S'il s'agit d'une utilisation continue, le Logiciel-service IBM continuera d'être disponible pour le Client, sur une base mensuelle, jusqu'à ce que ce dernier transmette à IBM un préavis écrit de trente (30) jours indiquant sa décision de cesser l'abonnement. Le Logiciel-service IBM demeurera disponible jusqu'à la fin du mois civil qui suit cette période de trente (30) jours.

5. Assistance technique

Au cours de la Période d'abonnement et une fois qu'IBM a avisé le Client qu'il a accès au Logiciel-service IBM, l'assistance technique est fournie par le biais de forums en ligne et en tant qu'assistance standard pendant la période au cours de laquelle le Client engage des frais payables à l'utilisation. À partir du Logiciel-service IBM, le Client peut soumettre un dossier d'incident ou ouvrir une séance de clavardage afin d'obtenir de l'assistance. IBM mettra en disponibilité le guide d'assistance pour les Logiciels-services IBM («IBM Software as a Service Support Handbook») qui fournit les coordonnées pour obtenir de l'assistance technique ainsi que d'autres informations et processus à cet égard.

Gravité	Définition	Objectifs de temps de réponse	Période de couverture
1	Incidence critique sur l'entreprise ou interruption d'un service crucial Une fonction critique pour l'entreprise est hors d'usage ou une interface cruciale ne fonctionne plus. Cette situation s'applique habituellement dans un environnement de production et indique une incapacité d'accéder aux services, ce qui a une incidence critique sur les activités de l'entreprise. Cette situation exige une solution immédiate.	Au plus une (1) heure	24 heures sur 24, 7 jours sur 7
2	Incidence importante sur l'entreprise L'utilisation d'une option ou d'une fonction du service est grandement limitée ou le Client risque de manquer une échéance commerciale.	Au plus deux (2) heures ouvrables	Heures ouvrables, du lundi au vendredi
3	Incidence mineure sur l'entreprise Le service ou la fonctionnalité du service est utilisable et cela n'a aucune incidence critique sur les activités de l'entreprise.	Au plus quatre (4) heures ouvrables	Heures ouvrables, du lundi au vendredi
4	Incidence minimale sur l'entreprise Demande de renseignements ou demande non technique	Au plus un (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 des problèmes avec le service et de faciliter l'analyse de l'application du Client par le service. IBM accédera aux données uniquement pour réparer des défauts ou pour fournir de l'assistance concernant des produits ou des services IBM.

6. Modalités supplémentaires relatives aux offres de Logiciel-service IBM

Les analyses de sécurité peuvent ne pas identifier tous les risques de sécurité dans une application et ne sont pas conçues ou prévues pour être utilisées dans des environnements dangereux nécessitant un fonctionnement à sécurité intégrée, y compris, notamment, les systèmes de navigation aérienne et de contrôle de la circulation aérienne, les systèmes d'armement, les systèmes de maintien des fonctions vitales, les installations nucléaires ou toute autre application où le défaut d'identifier les risques de sécurité pourrait entraîner un décès, des lésions corporelles ou des dommages matériels. IBM ne garantit pas que les analyses de sécurité fonctionneront sans interruption ou sans erreur.

Le Logiciel-service IBM peut être utilisé pour aider le Client à respecter les obligations de conformité, qui peuvent être fondées sur des lois, réglementations, normes ou pratiques. Les indications, utilisations suggérées ou directives fournies par le Service ne constituent pas des conseils juridiques, comptables ou autres conseils professionnels. Il est fortement recommandé au Client d'obtenir lui-même des conseils d'un avocat ou autre expert. Le Client assume seul la responsabilité de s'assurer que ses activités, ses applications et ses systèmes respectent toutes les lois, réglementations, normes et pratiques applicables. L'utilisation de ce Service ne garantit pas la conformité avec toute loi, réglementation, norme ou pratique.

Le Logiciel-service IBM effectue des tests invasifs et non invasifs sur le site Web et dans l'application Web ou mobile que le Client choisit d'analyser. Certaines lois interdisent toute tentative non autorisée de pénétrer les systèmes informatiques ou d'y accéder. Le Client autorise IBM à exécuter les Services décrits aux présentes et reconnaît que les Services constituent un accès autorisé aux systèmes informatiques du Client. IBM peut divulguer la présente autorisation à un tiers si cela s'avère nécessaire pour fournir les Services.

Ces tests comportent certains risques, y compris, notamment, ce qui suit :

- a. lorsque les systèmes informatiques du Client exécutent des applications soumises à des tests, ils peuvent figer ou planter, ce qui les rend temporairement indisponibles ou entraîne la perte de données;
- b. les performances et le débit des systèmes du Client, ainsi que les performances et le débit des routeurs et des pare-feu associés peuvent être temporairement dégradés pendant les tests;

- c. des quantités excessives de messages du journal peuvent être générées, ce qui entraîne une consommation excessive d'espace disque pour le fichier journal;
- d. des données peuvent être modifiées ou supprimées en raison de la recherche de vulnérabilités;
- e. des alarmes peuvent être déclenchées par des systèmes de détection des intrusions;
- f. des courriels peuvent être déclenchés par la fonction de messagerie de l'application Web soumise à des tests;
- g. le Logiciel-service IBM peut intercepter le trafic du réseau surveillé aux fins de recherche d'événements.

Tous les droits ou recours prévus par IBM aux termes d'une entente de niveau de service relativement à des applications ou à des sites Web soumis à des tests seront suspendus pendant toute activité de test.

Dans le cas où le Client entre des justificatifs d'accès authentifiés pour l'application en cours de test dans le Service, il doit les entrer uniquement pour les comptes de test et non pour les utilisateurs en environnement de production. L'utilisation de justificatifs d'identité des utilisateurs en environnement de production pourrait entraîner la transmission de données personnelles par l'intermédiaire du Service.

Le Logiciel-service IBM peut être configuré pour analyser des applications Web en environnement de production. Lorsque le Client définit le type d'analyse à «production», le service est conçu pour effectuer des analyses de manière à réduire les risques énumérés ci-dessus. Toutefois, dans certaines situations, le Logiciel-service IBM peut mener à une dégradation des performances ou à l'instabilité dans l'infrastructure et les sites de production testés. IBM n'offre aucune garantie et ne fait aucune déclaration concernant la pertinence d'utiliser le Logiciel-service IBM pour analyser les sites de production.

IL INCOMBE AU CLIENT DE DÉTERMINER SI LE SERVICE EST PERTINENT ET SÉCURITAIRE POUR SON SITE WEB, SON APPLICATION WEB, SON APPLICATION MOBILE OU SON ENVIRONNEMENT TECHNIQUE.

Le Logiciel-service IBM est conçu pour identifier une variété de problèmes potentiels de sécurité et de conformité dans les applications mobiles et Web et les services Web. Il ne teste pas toutes les vulnérabilités ou les risques touchant la conformité et n'agit pas non plus comme une barrière contre les attaques visant la sécurité. Étant donné que les menaces à la sécurité et les règlements et les normes de sécurité changent continuellement, il se pourrait que le Service ne reflète pas tous ces changements. Le Client assume seul la responsabilité de la sécurité et de la conformité de son application Web, de ses systèmes et de ses employés, de même que des mesures correctives qui sont appliquées. Le Client décide, à sa seule discrétion, d'utiliser ou non l'information fournie par le Service.

Certaines lois interdisent toute tentative non autorisée de pénétrer les systèmes informatiques ou d'y accéder. **LE CLIENT A LA RESPONSABILITÉ DE S'ASSURER DE NE PAS UTILISER LE SERVICE POUR ANALYSER LES APPLICATIONS OU SITES WEB AUTRES QUE CEUX QUI LUI APPARTIENNENT OU CEUX QU'IL A LE DROIT ET L'AUTORITÉ D'ANALYSER.**

Par souci de clarté, le contenu du Client décrit dans la section qui porte sur la protection des données dans les Conditions d'utilisation d'IBM – Modalités générales est également réputé inclure les données qui peuvent devenir accessibles à IBM pendant les Tests de pénétration d'applications.

6.1 Systèmes appartenant à un tiers

Pour les systèmes (qui, aux fins de la présente disposition, comprennent, notamment, les applications et les adresses IP) appartenant à un tiers, qui seront soumis à des tests aux termes des présentes, le Client convient :

- a. d'obtenir une lettre signée par le propriétaire de chaque système, autorisant IBM à fournir les Services sur le système en question et indiquant que le propriétaire accepte les modalités énoncées dans la section intitulée «Permission pour effectuer des tests», et fournir à IBM une copie de cette autorisation, et ce, avant qu'IBM fasse des tests sur un système d'un tiers;
- b. d'assumer seul la responsabilité de communiquer au propriétaire du système les risques, les expositions et les vulnérabilités qui y sont identifiés à la suite des tests à distance faits par IBM; et
- c. d'organiser et de faciliter l'échange d'informations entre le propriétaire du système et IBM, tel qu'IBM le juge nécessaire.

Le Client convient :

- d'aviser IBM immédiatement lors d'un changement de propriété de tout système soumis aux termes des présentes;
- de ne pas divulguer les articles livrables ou le fait qu'IBM a fourni les Services, à l'extérieur de l'Entreprise du Client sans le consentement écrit préalable d'IBM; et
- d'indemniser IBM en totalité pour les pertes ou les responsabilités engagées par IBM en raison de réclamations de tiers découlant du défaut du Client de se conformer aux exigences de la présente section intitulée «Systèmes appartenant à un tiers» et pour tous les brevets d'assignation ou réclamations de tiers déposés contre IBM ou ses sous-traitants ou mandataires découlant (a) de tests sur les risques, les expositions ou les vulnérabilités de sécurité des systèmes soumis à des tests aux termes des présentes, (b) de la remise des résultats de tels tests au Client, ou (c) de l'utilisation ou de la divulgation de tels résultats par le Client.

6.2 Témoins

Le Client sait et convient qu'IBM peut, dans le cadre de ses activités normales d'exploitation et de soutien du Logiciel-service, recueillir des renseignements personnels du Client (de ses employés et entrepreneurs) en lien avec l'utilisation du Logiciel-service IBM, en utilisant des technologies de surveillance ou d'autres technologies. IBM recueille de telles données afin d'obtenir des statistiques d'utilisation et de l'information sur l'efficacité de son Logiciel-service, en vue d'améliorer l'expérience des utilisateurs ou de personnaliser les interactions avec le Client. Le Client confirme qu'il obtiendra ou qu'il a obtenu le consentement pour permettre à IBM de traiter les renseignements personnels recueillis, aux fins énoncées plus haut, au sein d'IBM, dans d'autres entreprises d'IBM et dans l'entreprise de leurs sous-traitants, partout où ils font affaire, et conformément à ce que permettent les lois applicables. IBM acquiescera aux demandes des employés et des entrepreneurs du Client concernant leur accès aux renseignements personnels qui ont été recueillis sur eux, ainsi qu'à leurs demandes de mise à jour, de correction ou de suppression de ces mêmes renseignements.

Dans le cadre du Logiciel-service IBM, qui inclut des activités de production de rapports, IBM préparera et gèrera de l'information anonymisée ou regroupée recueillie à partir du Logiciel-service IBM (appelée «Données de sécurité»). Ces Données de sécurité n'identifieront pas le Client ni toute autre personne, sauf comme prévu au point (d) ci-dessous. Le Client convient également par les présentes qu'IBM peut utiliser ou copier les Données de sécurité uniquement aux fins suivantes :

- a. la publication et/ou la distribution des Données de sécurité (p. ex., dans des compilations et/ou des analyses liées à la cybersécurité);
- b. le développement ou l'amélioration de produits ou de services;
- c. les activités de recherche à l'interne ou avec des tiers; et
- d. le partage licite d'information confirmée sur un tiers intrus.

6.3 Emplacements bénéficiaires

Les taxes applicables, s'il y a lieu, sont basées sur le ou les emplacements que le Client identifie comme étant ceux qui bénéficient du Logiciel-service IBM. Ainsi, IBM appliquera les taxes en se basant sur l'adresse professionnelle que le Client désigne comme l'emplacement qui est le principal bénéficiaire au moment de commander le Logiciel-service IBM, à moins que le Client ne fournisse à IBM de l'information supplémentaire à ce sujet. Le Client a la responsabilité de maintenir cette information à jour et d'informer IBM de tout changement.

6.4 Renseignements personnels et contenu et services réglementés

Ce Logiciel-service IBM n'est pas conçu pour répondre à des exigences de sécurité spécifiques relativement au contenu réglementé, comme les renseignements personnels ou les renseignements personnels sensibles. Il incombe au Client de déterminer si ce Logiciel-service IBM répond à ses besoins en ce qui a trait au type de contenu qu'il utilise en lien avec le Logiciel-service IBM.

IBM n'est pas un fournisseur de services qui sont réglementés par la Federal Communications Commission («FCC») ou des organismes de réglementation d'État («Organismes de réglementation»), et n'a pas l'intention de fournir des services qui sont réglementés par la FCC ou des Organismes de réglementation. Si la FCC ou tout Organisme de réglementation impose des exigences ou des obligations à l'égard de l'un des services fournis par IBM aux termes des présentes, IBM peut : (a) modifier, remplacer ou substituer les produits aux frais du Client, et/ou (b) modifier la façon dont ces services sont

fournis au Client afin d'éviter que de telles exigences ou obligations soient imposées à IBM (par exemple, en agissant à titre de mandataire du Client pour acquérir ces services auprès d'une tierce entreprise de télécommunications).

Appendice A

1. Description générale de l'offre IBM Application Security on Cloud

Le Logiciel-service IBM Application Security on Cloud offre au Client un endroit unique pour identifier des vulnérabilités en matière de sécurité (comme une injection SQL, les scripts intersites et le vol de données) pour une variété d'applications. Le Logiciel-service fait appel à divers types de techniques d'analyse de la sécurité des applications permettant d'identifier des problèmes de sécurité dans une application.

Le Logiciel-service IBM Application Security on Cloud offre les capacités suivantes :

- Analyse des applications mobiles à la recherche de vulnérabilités en matière de sécurité. Cette analyse se fait à l'aide de techniques d'analyse de sécurité dynamique (boîte noire) et interactive (boîte transparente).
- Analyse de sites Web de production ou de préproduction, accessibles sur un réseau public ou privé, à la recherche de vulnérabilités en matière de sécurité. Cette analyse se fait à l'aide de techniques d'analyse de sécurité dynamique (boîte noire).
- Analyse des flux de données dans les applications Web et bureautiques à la recherche de vulnérabilités en matière de sécurité. Cette analyse se fait à l'aide de techniques d'analyse de sécurité statique (boîte blanche).
- Production de rapports détaillés sur les vulnérabilités en matière de sécurité, comprenant à la fois des sommaires détaillés des résultats d'analyse et les étapes que peuvent suivre les développeurs pour corriger la situation.
- Intégration à diverses plateformes de développement et d'exploitation.

1.1 IBM Application Analyzer

Le Logiciel-service IBM Application Analyzer peut être commandé par Instance d'application ou par Travail (analyse), ou en tant qu'Instance intégrale, et permet de faire les types d'analyses ci-dessous :

- Dynamic Analyzer – Tester des sites Web de préproduction ou de production au moyen de techniques DAST (Dynamic Application Security Testing)
- Mobile Analyzer – Tester des fichiers binaires iOS ou Android au moyen de techniques IAST (Interactive Application Security Testing)
- Static Analyzer – Tester des flux de données de code à octets ou de code source au moyen de techniques SAST (Static Application Security Testing)

1.2 Services de mise en place

L'offre IBM Application Security on Cloud Consulting Services est un service de mise en place productisé pour le module Application Analyzer. Le Service fait appel à des consultants IBM pour fournir des conseils et de l'assistance sur les tests et la gestion des risques liés aux applications. L'offre IBM Application Security on Cloud Consulting Services s'achète sous forme de blocs de Mandats qui peuvent être appliqués selon les quantités indiquées ci-dessous afin de demander et d'utiliser les services spécifiques suivants :

a. **Service Fast Start** [Utilise une (1) unité «Mandat»]

Le service Fast Start offre une expertise et des conseils pour l'utilisation des fonctions de test et de gestion des risques du Logiciel-service IBM Application Security on Cloud. Une fois que le Client a confirmé sa connexion au portail Application Security on Cloud, IBM organisera une cyberconférence d'un maximum de deux (2) heures pour deux (2) participants actifs afin d'offrir une formation sur les configurations et les fonctions de base du Logiciel-service Application Security on Cloud, y compris les types d'analyse, l'exécution d'analyses, l'examen de rapports et l'installation d'outils et de plugiciels connexes. Le service Fast Start se terminera après (a) la tenue du cyberséminaire de formation du Client, (b) l'installation des outils et des plugiciels applicables, et (c) l'assistance apportée au Client pour configurer et exécuter la première analyse.

b. **Service Assessment Review** [Utilise deux (2) unités «Mandat»]

Le service Assessment Review offre de l'assistance pour passer en revue un résultat de test, notamment pour comprendre les corrections des vulnérabilités dans l'application et les classer par ordre de priorité. IBM organisera une cyberconférence d'un maximum d'une (1) heure pour deux (2) participants actifs afin de donner un aperçu des vulnérabilités trouvées et du risque de sécurité global de l'application, et d'animer une discussion détaillée sur les vulnérabilités en matière de sécurité trouvées dans l'application, y compris (1) comment la vulnérabilité a été testée, (2) comment les vulnérabilités ont été détectées, (3) quel est le risque de chaque vulnérabilité, et (4) comment aider à remédier à la vulnérabilité. L'examen portera exclusivement sur le résultat du test et ne sera pas un examen du code source lui-même. Le Client passera en revue les résultats du test et les communiquera à IBM pour examen avant la cyberconférence. Le service Assessment Review se terminera après la tenue de la cyberconférence.

c. **Service Scan for Me** [Utilise quatre (4) unités «Mandat»]

Le service Scan for Me fournit un expert IBM de la sécurité des applications, qui configurera et lancera une analyse, validera les résultats et tiendra une séance d'information pour passer en revue les constatations. Le Client permettra à un consultant IBM d'accéder à son environnement Application Security on Cloud pour configurer et lancer une analyse, valider les résultats, faire des recommandations sur la priorisation des corrections et tenir une séance d'information sur les résultats. IBM organisera une cyberconférence d'un maximum d'une (1) heure pour deux (2) participants actifs afin de donner un aperçu des vulnérabilités trouvées et du risque de sécurité global de l'application, et d'animer une discussion détaillée sur les vulnérabilités en matière de sécurité trouvées dans l'application, y compris (1) comment la vulnérabilité a été testée, (2) comment les vulnérabilités ont été détectées, (3) quel est le risque de chaque vulnérabilité, et (4) comment aider à remédier à la vulnérabilité. À la demande du Client, jusqu'à trente (30) jours après l'analyse initiale, IBM fera une nouvelle analyse en utilisant la configuration d'origine pour vérifier les correctifs de sécurité seulement (et non pour tester de nouvelles fonctionnalités), valider les résultats et remettre un rapport au Client. Le service Scan for Me se terminera après la tenue de la cyberconférence pour passer en revue les résultats de l'analyse initiale ou, s'il y a lieu, après l'exécution de la nouvelle analyse demandée par le Client et la remise du rapport de réanalyse au Client.

d. **Service Advisor on Demand** [Utilise sept (7) unités «Mandat»]

Le service Advisor on Demand permet d'obtenir jusqu'à vingt (20) heures de services d'un consultant IBM, qui peuvent être utilisées pour des activités liées au Logiciel-service IBM. Le consultant IBM aidera le Client avec des sujets spécifiques en matière de sécurité des applications, y compris, notamment, la gestion des programmes, la priorisation des tests de sécurité, les stratégies de correction, l'analyse et la réparation de code source. IBM travaillera avec le Client pour comprendre et créer un calendrier de projet avec les exigences spécifiques du Client, y compris les objectifs du projet, les technologies pertinentes, les délais souhaités, les résultats attendus et le nombre estimé de Mandats du service Advisor on Demand. Le Client doit accorder un accès aux applications, aux systèmes et à la documentation nécessaires à la prestation des services. Le service Advisor on Demand se terminera lorsque le Client aura épuisé un maximum de vingt (20) heures d'expertise en matière de sécurité ou que les articles livrables définis dans le calendrier de projet lui auront été livrés.

e. **Tests de pénétration d'applications**

Ce service comprend trois (3) options :

- (1) Le **test de pénétration d'applications d'entrée de gamme/de conformité**, qui comprend jusqu'à quarante (40) heures de services d'un Consultant, porte sur des failles logiques à étape unique et sur des versions simples de failles d'injection. Utilise quinze (15) unités «Mandat».
- (2) Le **test de pénétration d'applications standard**, qui comprend jusqu'à soixante (60) heures de services d'un Consultant, étend la portée pour inclure des failles logiques dans des flux de travail à étapes multiples, des versions complexes de failles d'injection et l'analyse de types de données complexes. Utilise vingt-et-un (21) unités «Mandat».

- (3) Le **test de pénétration d'applications évolué**, qui comprend jusqu'à quatre-vingts (80) heures de services d'un Consultant, étend la portée pour inclure l'ingénierie inverse d'exécutables compilés, la dissection de protocoles de réseaux personnalisés, l'analyse approfondie de bibliothèques et de cadres de référence accessibles au public. Utilise vingt-sept (27) unités «Mandat».

Le service de tests de pénétration d'applications fournit une ressource IBM pour tester et exploiter une application, livrer un rapport de test et tenir une séance d'information pour expliquer les constatations et les risques connexes.

IBM organisera un appel de lancement du projet d'un maximum d'une (1) heure pour deux (2) participants actifs afin de passer en revue l'environnement et l'entreprise du Client, y compris la plateforme d'application, l'architecture, les cadres de référence, l'infrastructure de soutien, les problèmes de sécurité connus ou les préoccupations liées à l'application, le calendrier des tests préliminaires et le plan de communication en cas d'urgence.

IBM effectuera les tests de pénétration d'applications, y compris, notamment, l'identification de vulnérabilités courantes telles que l'injection SQL et les scripts intersites, l'évaluation des forces et des faiblesses des contrôles de sécurité existants, tels que la validation, l'authentification et l'autorisation des entrées, la vérification de la bonne application de la logique applicative, la validation de la bonne utilisation de protocoles sécurisés, l'identification des défauts de manipulation de session et la vérification des contrôles de sécurité appropriés lors de la connexion, la récupération de mots de passe, la politique régissant les mots de passe et d'autres fonctions de gestion des utilisateurs. Les résultats seront consignés dans le rapport de test de pénétration d'applications. IBM organisera une cyberconférence d'un maximum d'une (1) heure pour la présentation du rapport. Le service de test de pénétration d'applications sera terminé lorsque le temps de consultation alloué aura été épuisé, que la cyberconférence aura eu lieu et que le rapport final du test de pénétration d'applications aura été remis au Client.

1.2.1 Responsabilités relatives aux Services de mise en place

IBM s'engage à :

- fournir des Services de mise en place en utilisant des unités «Mandat» achetées par le Client et conformément à l'Autorisation d'utilisation; et
- avoir terminé un Service de mise en place lorsque les critères d'achèvement décrits à la section 1.2 auront été satisfaits.

Le Client convient :

- d'assumer la responsabilité de tous les frais associés à toutes les demandes de Mandat faites par le Client au cours de la période contractuelle;
- et reconnaît que les unités «Mandat» achetées doivent être utilisées au cours de la période contractuelle initiale et qu'elles expirent si elles n'ont pas servi à la date de fin de la période contractuelle; et
- d'initier une demande formelle pour tous les Services de mise en place au moins trente (30) jours avant la date de fin de l'abonnement.

Lors de la prestation de tout Service de mise en place, IBM peut demander au Client de lui fournir des renseignements et de coopérer avec elle de façon raisonnable. Si le Client ne fournit pas les renseignements demandés ou s'il ne coopère pas dans les délais prescrits, il pourrait, à la discrétion d'IBM, engager des frais liés aux unités «Mandat» tel que requis par les services ou subir des retards dans la prestation du service applicable.

Pour permettre à IBM d'effectuer les tests avec précision, le Client convient de suivre les instructions d'IBM relativement à la préparation et au maintien de l'environnement au cours de la période de test.