

Descriptif de Service IBM Cloud

IBM Security AppScan Mobile Analyzer

Voici la Description de Service de la Commande du Client :

1. Service Cloud

L'offre de Services Cloud est décrite ci-dessous et spécifiée dans un Bon de Commande pour les offres autorisées sélectionnées. Le Bon de Commande est constitué du Devis fourni et de l'Autorisation d'Utilisation (ci-après dénommée « PoE ») qui confirme la date de début et la durée des Services Cloud. La facturation commencera suite à la mise à disposition du Service Cloud.

1.1 IBM Security AppScan Mobile Analyzer

Ce service définit les problèmes de sécurité au niveau de code des applications mobiles Android. Il permet aux développeurs d'analyser les vulnérabilités en matière de sécurité sans avoir à fournir le code source d'application. A l'issue de l'analyse, le service génère un rapport de sécurité comprenant les détails des vulnérabilités détectées, les risques de sécurité potentiels pour l'application mobile dus à ces vulnérabilités, ainsi que des suggestions sur la façon de les résoudre.

2. Description de la sécurité

2.1 Règles de sécurité

IBM dispose d'une équipe chargée de la sécurité des informations et applique également des règles de confidentialité et de sécurité qui sont communiquées aux employés IBM. IBM exige une formation à la confidentialité et la sécurité pour le personnel qui prend en charge les centres de données IBM. Les règles et normes de sécurité IBM sont examinées et réévaluées tous les ans. Les incidents de sécurité IBM sont traités conformément à une procédure détaillée de réponse après incident.

2.2 Contrôle d'accès

L'accès aux données client, si nécessaire, n'est autorisé que par les représentants agréés du service de support IBM et le personnel des opérations de service, conformément aux principes de répartition des tâches. Le personnel IBM utilise l'authentification à deux facteurs auprès d'un hôte de gestion de « passerelle » intermédiaire. Toutes les connexions sont des canaux chiffrés lors de l'accès aux données client.

2.3 Intégrité et Disponibilité des Services

Les modifications des logiciels d'application et des systèmes d'exploitation sont régies par la procédure de gestion des modifications d'IBM. Les modifications des règles de pare-feu sont également régies par la procédure de gestion des modifications et sont examinées par le personnel de sécurité IBM avant d'être mises en œuvre. IBM surveille le centre de données 24 heures sur 24 et 7 jours sur 7. Le scannage de vulnérabilité interne et externe est régulièrement effectué par des administrateurs autorisés et des fournisseurs tiers pour aider à détecter et résoudre les risques potentiels liés à la sécurité des systèmes. Les systèmes de détection de logiciel malveillant (antivirus, détection d'intrusion, scannage de vulnérabilité et prévention contre les intrusions) sont utilisés dans tous les centres de données IBM. Les services de centre de données d'IBM prennent en charge de nombreux protocoles de distribution d'informations pour la transmission de données sur les réseaux publics. Exemples : HTTPS/SFTP/FTPS/S/MIME et VPN de site à site. Les données de sauvegarde destinées au stockage hors site sont chiffrées avant le transport.

2.4 Consignation des Activités

IBM gère des journaux de ses activités pour les systèmes, applications, référentiels de données, middleware et unités d'infrastructure de réseau qui sont capables de et configurés pour consigner l'activité. Pour minimiser la possibilité de falsification et pour permettre l'analyse centralisée, la gestion d'alertes et la génération de rapports, l'activité est consignée en temps réel dans des référentiels de journaux centralisés. Les données sont signées pour empêcher la contrefaçon. Les journaux sont analysés en temps réel et via des rapports d'analyse périodiques pour détecter les comportements anormaux. Le personnel des opérations est averti des anomalies et contacte, si nécessaire, un spécialiste de sécurité joignable 24 heures sur 24 et 7 jours sur 7.

2.5 Sécurité physique

IBM gère des normes de sécurité physique conçues pour restreindre l'accès physique non autorisé aux centres de données IBM. Seuls des points d'accès limité existent dans les centres de données ; ils sont contrôlés par l'authentification à deux facteurs et surveillés par des caméras de surveillance. L'accès n'est autorisé qu'au personnel autorisé dont l'accès est approuvé. Le personnel des opérations vérifie l'approbation et émet un badge d'accès accordant l'accès nécessaire. Les employés auxquels ces badges sont destinés doivent restituer leurs autres badges d'accès et ne peuvent être en possession du badge d'accès au centre de données que pendant la durée de leur activité. L'utilisation des badges est consignée. Les visiteurs non IBM sont enregistrés dès leur arrivée dans les locaux et sont accompagnés lorsqu'ils se trouvent dans les locaux. Les zones de livraison et les plateformes de chargement ainsi que tous les autres lieux d'entrée des personnes non autorisées sont contrôlés et isolés.

2.6 Conformité

IBM certifie que ses pratiques en matière de protection de la vie privée sont conformes à celles de l'accord Safe Harbor du Département du Commerce des États-Unis : avertissement, choix, transfert ultérieur, accès et exactitude, sécurité et mise en œuvre. IBM effectue annuellement des audits SSAE 16 (ou leur équivalent) conformes aux normes de l'industrie dans ses centres de données de production. IBM passe en revue les activités liées à la sécurité et la confidentialité quant à leur conformité aux besoins métier d'IBM. Des évaluations et des audits sont effectués régulièrement par IBM pour confirmer le respect des règles de sécurité des informations. Les employés d'IBM et les employés des fournisseurs suivent tous les ans une formation à la sensibilisation et à la sécurité de la main d'œuvre. Les membres du personnel sont informés tous les ans de leurs objectifs de travail et de leurs responsabilités quant au respect de l'éthique professionnelle, la confidentialité et les obligations de sécurité d'IBM.

3. Autorisation d'Utilisation et Informations de Facturation

3.1 Unités de Mesure des Prix

Le Service Cloud est mis à disposition en fonction de l'unité de mesure de redevance suivante indiquée dans le Bon de Commande :

- 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 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 doivent nécessairement être obtenus 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 du Logiciel ou un Document de Transaction du Client.

3.2 Redevances et Facturation

Le montant à régler pour le Service Cloud est indiqué dans un Bon de commande.

3.3 Pay as you Go

Les options Pay as you Go seront facturées le mois suivant lequel le service est utilisé au tarif indiqué dans le Document de Transaction.

4. Support Technique

Le support technique du Service Cloud est disponible pendant la période d'abonnement.

Les Horaires de Fonctionnement du Service de Support sont les suivants :

Pour plus d'informations sur les heures de disponibilité, les systèmes de notification de problème en ligne ainsi que d'autres moyens et procédures de communication de support technique, voir le manuel IBM Software as a Service Support Handbook.

Assistance après les horaires de travail :

Le service d'Assistance Après les Horaires de Travail (hors des horaires de travail normaux indiqués ci-dessus) n'est disponible que pour les problèmes de gravité 1 pendant les jours ouvrables, les week-ends et les jours fériés. Pour les problèmes de Gravité 1, le Client doit être disponible pour aider à

diagnostiquer les problèmes 24 heures sur 24 et 7 jours sur 7 ; sinon, ils sont rétrogradés au niveau de Gravité 2.

4.1 Forum de support

Un forum de support régulièrement surveillé par les représentants et les développeurs du service de support IBM est mis à la disposition de tous les clients du Service Cloud.

a. Pour poser des questions :

<https://developer.ibm.com/answers/questions/ask/?topics=appscan-mobile-analyzer>

b. Pour consulter les posts en cours :

<https://developer.ibm.com/answers/topics/appscan-mobile-analyzer/>

4.2 Support Standard

Le support standard est disponible pendant la période des redevances Pay as you Go encourues par le Client. A partir du Service Cloud, les clients peuvent soumettre un ticket de support ou ouvrir une session de discussion à des fins d'assistance. Pour plus d'informations sur les procédures de support, consultez le portail Web de support IBM à l'adresse Internet <https://support.ibmcloud.com> ou le manuel IBM SaaS Software Support Handbook à l'adresse Internet http://www.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf.

Niveau de gravité	Définition de la gravité	Objectifs de temps de réponse	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
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. Conformité Safe Harbor

IBM n'a pas déterminé la conformité de ce Service Cloud aux normes américano-européennes et américano-suisse « US-EU » et « US-Swiss » Safe Harbor Frameworks.

6. Informations supplémentaires

Le Service Cloud est conçu pour identifier divers problèmes de sécurité et de conformité potentiels au niveau des applications mobiles et des services Web mobiles. 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 mobiles, 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.

6.1 Sites Bénéficiaires Dérivés

Le cas échéant, les taxes sont fonction du(es) site(s) que le Client identifie comme bénéficiant des Services Cloud. IBM appliquera les taxes en fonction de l'adresse professionnelle indiquée lors de la commande d'un Service Cloud 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.

6.2 Cookies

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