Descripción de Servicios de Cloud de IBM

IBM Security AppScan Mobile Analyzer

Lo siguiente es la Descripción de Servicio de su Pedido:

1. Servicio de Cloud

La oferta del Servicio de Cloud se describe a continuación y se especifica en un Documento de Pedido para las ofertas bajo derechos de titularidad seleccionadas. El Documento de Pedido consistirá en el Presupuesto que se presenta y el Documento de Titularidad (POE) que confirma la fecha de inicio y final de los Servicios de Cloud. La facturación empezará tras la provisión del Servicio de Cloud.

1.1 IBM Security AppScan Mobile Analyzer

Este servicio identifica problemas de seguridad a nivel de código de aplicaciones móviles Android. Permite a los desarrolladores buscar vulnerabilidades de seguridad sin necesidad de proporcionar el código fuente de la aplicación. Al final de la exploración, el servicio genera un informe de seguridad que incluye detalles de las vulnerabilidades detectadas y los potenciales riesgos de seguridad para la aplicación móvil causados por el uso de estas vulnerabilidades, con sugerencias de cómo solucionarlos.

2. Descripción de las Medidas de Seguridad

2.1 Políticas de Seguridad

IBM dispone de un equipo de seguridad de la información y también mantiene políticas de privacidad y seguridad, que se comunican a los empleados de IBM. IBM requiere una formación en privacidad y seguridad al personal que ofrece soporte en los centros de datos de IBM. Las políticas de seguridad y los estándares de IBM se revisan y se evalúan anualmente. Las incidencias de seguridad de IBM se gestionan de acuerdo con un procedimiento completo de respuestas ante incidencias.

2.2 Control de Acceso

El acceso a los datos del Cliente, si se requiere, sólo está permitido a personal de operaciones de servicio o representantes de soporte de IBM autorizados de acuerdo con los principios de segregación de tareas. El personal de IBM utiliza una autenticación de dos factores a un host de gestión intermedio "gateway". Todas las conexiones son canales cifrados al acceder a los datos del Cliente.

2.3 Integridad y Disponibilidad del Servicio

Las modificaciones del sistema operativo y el software de aplicaciones se rigen por el proceso de gestión de cambios de IBM. Los cambios de las reglas de firewall también se rigen por el proceso de gestión de cambios y los revisa el personal de seguridad de IBM antes de la implementación. IBM monitoriza el centro de datos 24x7. El escaneo de vulnerabilidades internas y externas lo realizan normalmente los administradores autorizados y los proveedores de terceros para ayudar a detectar y resolver posibles vulnerabilidades de seguridad del sistema. Se utilizan sistemas de detección de Malware (antivirus, detección de intrusiones, escaneo de vulnerabilidades y prevención de intrusiones) en todos los centros de datos de IBM. Los servicios de los centros de datos de IBM dan soporte a una gran cantidad de protocolos de entrega de información para la transmisión de datos en redes públicas. Algunos ejemplos son HTTPS/SFTP/FTPS/S/MIME y VPN de sitio a sitio. Los datos de copia de seguridad pensados para el almacenamiento fuera del sitio se cifran antes del transporte.

2.4 Registros de Actividad

IBM mantiene los registros de su actividad para sistemas, aplicaciones, repositorios de datos, dispositivos de middleware y de infraestructura de red que están configurados para registrar la actividad. Para minimizar la posibilidad de manipulación indebida y permitir un análisis central, alertas e informes, el registro de actividad se realiza en tiempo real en repositorios de registros centrales. Los datos se firman para prevenir la manipulación indebida. Los registros se analizan en tiempo real y a través de unos informes de análisis periódicos para poder detectar comportamientos anómalos. Se avisa al personal de operaciones de las anomalías y éstos se ponen en contacto con un especialista en seguridad disponible 24x7, si es necesario.

2.5 Seguridad Física

IBM mantiene los estándares de seguridad física diseñados para restringir el acceso físico no autorizado a los centros de datos de IBM. Existen puntos de acceso limitado en los centros de datos, que están controlados por una autenticación de dos factores y están monitorizados por las cámaras de vigilancia. El acceso está permitido sólo al personal autorizado que dispone de acceso aprobado. El personal de operaciones verifica la aprobación y emite un identificador de acceso que otorga el acceso necesario. Los empleados con dichos identificadores no deben utilizar otros identificadores de acceso y sólo pueden disponer del identificador de acceso al centro de datos durante su período de actividad. La utilización de identificadores está registrada. Los visitantes que no sean de IBM se registrarán al entrar en las instalaciones y serán escoltados mientras estén en las instalaciones. Las áreas de entrega y de descarga y otros puntos donde puedan entrar personas no autorizadas están controladas y aisladas.

2.6 Cumplimiento

IBM certifica sus prácticas de privacidad anualmente de acuerdo con los principios Safe Harbor del Departamento de Comercio de los EE.UU.: aviso, selección, transferencia de salida, acceso y precisión, seguridad y monitorización/ejecución. IBM realiza auditorías bajo la norma SSAE 16 del sector (o alguna norma equivalente) anualmente en los centros de datos de producción. IBM revisa las actividades relacionadas con seguridad y la privacidad para que cumplan con los requisitos de negocio de IBM. IBM realiza evaluaciones y auditorías regularmente para confirmar el cumplimiento con las políticas de seguridad de la información. Los empleados de IBM y de los proveedores completan la formación de conocimiento y seguridad del personal, anualmente. Se recuerda al personal los objetivos de su trabajo y sus responsabilidades para cumplir con la conducta ética comercial, confidencialidad y obligaciones de seguridad de IBM, anualmente.

3. Información de Derechos de Titularidad y Facturación

3.1 Métricas de Cargo

El Servicio de Cloud se pone a disposición bajo la siguiente métrica de cargo, según se especifica en el Documento de Pedido:

- Instancia de Aplicación es una unidad de medida con la que se puede adquirir SaaS IBM. Se requiere un derecho de titularidad de Instancia de Aplicación por cada instancia de una Aplicación que esté conectada a SaaS IBM. Si una Aplicación tiene varios componentes, cada uno de los cuales con un objetivo y/o un usuario destinatario distinto, y cada uno de ellos puede ser conectado a o gestionado por SaaS IBM, cada componente se considera una Aplicación independiente. Además, los entornos de pruebas, desarrollo, puesta en escena, transferencia y producción para una Aplicación son considerados como instancias independientes de la Aplicación y cada uno debe tener un derecho de titularidad. Varias instancias de Aplicación en un único entorno son consideradas como instancias independientes de la Aplicación y cada una debe tener un derecho de titularidad. Deben adquirirse Derechos de Titularidad suficientes para cubrir el número Instancias de Aplicación conectadas a SaaS IBM durante el período de medida especificado en el Documento de Titularidad (POE) o Documento Transaccional del Cliente.

3.2 Cargos y Facturación

El importe que se debe abonar para el Servicio de Cloud se especifica en un Documento de Pedido.

3.3 Pago por Uso

Las opciones de Pago por Uso se facturarán el mes siguiente al uso del servicio, según la tarifa establecida en el Documento Transaccional.

4. Soporte Técnico

El Soporte Técnico para Servicio de Cloud está disponible durante el Período de Suscripción.

El horario de atención de soporte es el siguiente:

La información sobre las horas de disponibilidad, sistemas de informes de problemas en línea, así como otros procesos y vehículos de comunicación de soporte técnico, se describe en el manual IBM Software as a Service Support Handbook.

Soporte fuera del horario laboral:

El Soporte fuera del horario laboral (fuera del horario normal de funcionamiento establecido anteriormente) sólo está disponible para los problemas de Severidad 1 en días laborables, fines de semana y durante las vacaciones. Los problemas de Severidad 1 requieren que el Cliente esté

disponible para ayudar a diagnosticar los problemas durante el período de soporte ininterrumpido 24X7; de lo contrario, pasan a ser de Severidad 2.

4.1 Soporte de foro

Todos los clientes del Servicio de Cloud proporcionan soporte de foro monitorizado regularmente por parte de los desarrolladores y representantes de soporte de IBM.

a. Realizar preguntas:

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

b. Ver las publicaciones actuales:

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

4.2 Soporte Estándar

El Soporte Estándar está disponible durante el periodo de tiempo en el cual el Cliente incluye en cargos de Pago por Uso. Desde dentro del Servicio de Cloud, los clientes pueden enviar un ticket de soporte o abrir una sesión de chat para obtener ayuda. Para obtener más información acerca de los procedimientos de soporte, consulte el portal web de soporte en el sitio: https://support.ibmcloud.com o en el manual IBM SaaS Software Support Handbook: http://www.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf.

Severidad	Definición de Severidad	Objetivos de Tiempo de Respuesta	Cobertura de Tiempo de respuesta
1	**Impacto de negocio crítico / caída del servicio:** La función de impacto de negocio no está operativa o la interfaz crítica ha fallado. Esto se aplica normalmente a un entorno de producción e indica una incapacidad de acceso a los servicios, que causa un impacto crítico en las operaciones. Esta condición requiere una solución inmediata.	En el plazo de una hora	24x7
2	**Impacto de negocio significativo:** El uso de una característica de negocio del servicio o una función del servicio está muy restringido o el Cliente corre el riesgo de pasarse las fechas límite.	En el plazo de dos horas laborales	L-V horas laborales
3	**Impacto de negocio menor:** Indica que el servicio o la función no se pueden utilizar y no significa un impacto de negocio crítico en las operaciones.	En el plazo de cuatro horas laborales	L-V horas laborales
4	**Impacto de negocio mínimo:** Una consulta o una solicitud no técnica	En el plazo de 1 día laborable	L-V horas laborales

5. Conformidad con Safe Harbor

IBM no ha determinado la conformidad de este Servicio de Cloud con los Acuerdos de Safe Harbor de EE.UU. / Suiza.

6. Información Adicional

El Servicio de Cloud está diseñado para identificar una variedad de posibles problemas de seguridad y conformidad en aplicaciones móviles y servicios de web móvil. No prueba todas las vulnerabilidades o riesgos de conformidad, ni actúa como barrera frente a los ataques de seguridad. Las amenazas, legislaciones y normas de seguridad cambian continuamente, y el Servicio puede que no siempre refleje estos cambios. La seguridad y la conformidad de las aplicaciones móviles, los sistemas y los empleados del Cliente, así como todas las medidas correctivas, son responsabilidad exclusiva del Cliente. La utilización o no utilización de la información proporcionada por el Servicio depende única y exclusivamente del Cliente.

6.1 Ubicaciones con Ventajas Derivadas

Cuando sea aplicable, los tributos se realizan en las ubicaciones que el Cliente identifica como receptoras de los Servicios de Cloud. IBM aplicará los tributos en base a las direcciones de facturación enumeradas a la hora de solicitar un Servicio de Cloud como ubicación del beneficiario principal, a menos que el Cliente proporcione información adicional a IBM. El Cliente es responsable de mantener esta información actualizada y de comunicar cualquier cambio a IBM.

6.2 Cookies

El Cliente reconoce y acepta que IBM puede, como parte de la operativa normal y el soporte del Servicio de Cloud, recopilar información personal del Cliente (empleados y contratistas) en relación con el uso del Servicio de Cloud, a través de seguimiento y de otras tecnologías. IBM lo hace para recopilar estadísticas de uso e información acerca de la eficacia del Servicio de Cloud de IBM, con la finalidad de mejorar la experiencia de usuario y/o personalizar las interacciones con el Cliente. El Cliente confirma que va a obtener o ha obtenido el consentimiento para permitir a IBM procesar los Datos Personales recopilados con la finalidad mencionada dentro de IBM, de otras empresas de IBM y sus subcontratistas, allí donde IBM y los subcontratistas de IBM ejecuten actividades profesionales, de acuerdo con la ley aplicable. IBM cursará adecuadamente cualquier petición de los empleados y subcontratistas del Cliente para acceder, actualizar, corregir o eliminar su información personal de contacto.