

IBM X-Force Threat Intelligence

Esta Descripción del Servicio describe el Servicio de Cloud. Los documentos de pedidos aplicables proporcionan precios y detalles adicionales sobre el pedido del Cliente.

1. Servicio de Cloud

IBM X-Force Threat Intelligence proporciona acceso mediante programación a IBM X-Force Exchange a través de una API RESTful que devuelve información en JavaScript Object Notation (JSON). El Servicio de Cloud también da soporte a los estándares Structured Threat Information eXpression (STIX) y Trusted Automated eXchange of Indicator Information (TAXII). El Servicio de Cloud está diseñado para proporcionar las siguientes prestaciones clave que ayudan al usuario a:

- a. Acceder a información sobre investigaciones de seguridad específicas, conocidas como 'colecciones', formadas por contenido estructurado y no estructurado.
- b. Acceder a descripciones del tipo de incidencia (por ejemplo, malware, filtración de datos o vulnerabilidad) así como las actividades observables asociadas que sean relevantes para esa incidencia concreta.
- c. Obtener información actualizada y exhaustiva en los indicadores de amenazas que son con más frecuencia el punto de partida de investigaciones adicionales y el contexto para entender esos indicadores.
- d. Integrar los Datos con las ofertas del Cliente para aprovecharla información de inteligencia de amenazas.

1.1 Ofertas

El Cliente puede seleccionar entre las siguientes ofertas disponibles:

1.1.1 IBM X-Force Exchange Commercial API

IBM X-Force Exchange Commercial API permite a los usuarios automatizar el consumo de inteligencia de amenazas de IBM X-Force Exchange, la plataforma de intercambio de inteligencia de amenazas basada en cloud de IBM. La oferta se vende en paquetes de Diez Mil Elementos.

1.1.2 IBM X-Force Exchange Commercial API Enterprise

IBM X-Force Exchange Commercial Application Programming Interface (API) Enterprise permite a los usuarios automatizar el consumo de inteligencia de amenazas de IBM X-Force Exchange, la plataforma de intercambio de inteligencia de amenazas basada en cloud de IBM. La oferta se vende por Instancia. Una Instancia proporciona acceso ilimitado a IP y URL por canales de categoría, informes de IP y URL y canales de vulnerabilidad, así como a todos los canales de TAXII. Las solicitudes de indicadores que no se encuentran en X-Force Exchange están limitadas a 100.000 Elementos por mes.

1.1.3 IBM Advanced Threat Protection Feed by X-Force

IBM Advanced Threat Protection Feed by X-Force proporciona a los usuarios un conjunto definido de indicadores con capacidad de acción para el consumo directo en herramientas y soluciones de seguridad. El canal proporciona acceso a indicadores de compromiso con capacidad de acción (IPs y URLs), indicadores de compromiso derivados de analistas y nuestros indicadores de alerta anticipada de DNS. Los canales están disponibles en múltiples formatos, incluidos los siguientes: STIX/TAXII, JSON, lista de texto y formatos CSV.

1.1.4 Threat Intelligence Insights Standard for IBM Cloud Pak for Security

Este Servicio de Cloud está disponible de forma gratuita y ofrece a los Clientes la capacidad de integrar la inteligencia de amenazas básicas y habilitar características dentro de la aplicación Threat Intelligence Insights application on Cloud Pak for Security. Con este paquete, los Clientes tienen acceso al nivel gratuito de contenido de X-Force Threat Intelligence, incluyendo X-Force Advisories, las Amenazas y los IOCs asociados (IPs, URLs, Vulnerabilidades, Hash). Además, los Clientes pueden ejecutar una función manual de Am-I-Affected para buscar e identificar amenazas maliciosas en su entorno. La aplicación IBM Security Threat Intelligence Insights disponible como parte de IBM Cloud Pak for Security es un requisito previo para este Servicio de Cloud.

1.1.5 Threat Intelligence Insights Advanced for IBM Cloud Pak for Security

Threat Intelligence Insights Advanced for IBM Cloud Pak for Security es un paquete premium que ofrece a los Clientes la posibilidad de añadir la próxima generación de X-Force de inteligencia de amenaza y capacidades a Threat Intelligence Insights application on Cloud Pak for Security. El contenido avanzado de inteligencia de amenazas, supervisado por el equipo de IBM de Incident Response and Analysis Team (IRIS), incluye acceso a informes detallados sobre malware, grupos de amenazas, actividad de amenazas y análisis del sector, recomendaciones de remediación, indicadores de compromiso (IOCs), etc. El paquete Advanced también permite a los Clientes ejecutar la capacidad Am-I-Affected de forma continua y automática, priorizando e identificando proactivamente las amenazas relevantes en el entorno del usuario. La aplicación IBM Security Threat Intelligence Insights disponible como parte de IBM Cloud Pak for Security es un requisito previo para este Servicio de Cloud.

2. Fichas de Características de Protección y Tratamiento de Datos

El Anexo de Tratamiento de Datos (DPA) de IBM, en <http://ibm.com/dpa>, y las Fichas de Características de Protección y Tratamiento de Datos (referidas como fichas de datos o Suplementos del DPA) en los enlaces siguientes proporcionan información adicional de protección de datos para los Servicios de Cloud y sus opciones sobre los tipos de Contenido que pueden tratarse, las actividades de tratamiento involucradas, las características de protección de datos y detalles específicos sobre la retención y la devolución de Contenido. El DPA se aplica a los datos personales contenidos en el Contenido, siempre y cuando: i) se cumpla el Reglamento General de Protección de Datos de la Unión Europea (EU/2016/679) (GDPR); o ii) se aplique otra legislación sobre protección de datos identificada en <http://ibm.com/dpa/dpl>.
<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1ECC13601F5911E69AAAC4D0C72C126B>

3. Nivel de Servicio y Soporte Técnico

3.1 Acuerdo de Nivel de Servicio (SLA)

IBM proporciona al Cliente el siguiente contrato de nivel de servicio (SLA) de disponibilidad. IBM aplicará la compensación aplicable más alta en función de la disponibilidad acumulativa del Servicio de Cloud, como se muestra en la tabla siguiente. El porcentaje de disponibilidad se calcula como el número total de minutos en un mes contratado, menos el número total de minutos de Inactividad del Servicio en un mes contratado, dividido por el número total de minutos en un mes contratado. La definición de Inactividad del Servicio, el proceso de reclamación y la información acerca de cómo ponerse en contacto con IBM con respecto a los problemas de disponibilidad del servicio se encuentran en el manual de soporte del Servicio de Cloud de IBM, en la dirección

https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilidad	Crédito (% de la tarifa de suscripción mensual*)
Menos del 99,9%	2%
Menos del 99%	5%
Menos del 95%	10%

* La tarifa de suscripción es el precio contratado para el mes que está sujeto a la reclamación.

3.2 Soporte Técnico

El Soporte Técnico para el Servicio de Cloud, incluyendo detalles de contacto de soporte, niveles de gravedad, horas de disponibilidad de soporte, tiempos de respuesta y otros procesos e información de soporte, se encuentra seleccionando el Servicio de Cloud en la guía de soporte de IBM disponible en la dirección <https://www.ibm.com/support/home/pages/support-guide/>.

4. Cargos

4.1 Métricas de Cargo

Las métricas de cargo por el Servicio de Cloud se especifican en el Documento Transaccional.

Se aplican a este Servicio de Cloud las métricas de cargo siguientes:

- Una Instancia es cada acceso a una configuración específica de los Servicios de Cloud.
- Un Elemento es una aparición de un elemento específico tratado por, gestionado por, o relacionado con el uso del Servicio de Cloud. Para este servicio, un Elemento es cada resultado que devuelve una única consulta.
- Un Servidor Virtual Gestionado (MVS) consta de unidades de proceso, memoria y funciones de entrada/salida, y ejecuta los procedimientos, mandatos o aplicaciones gestionados por los Servicios de Cloud.

5. Términos Adicionales

Para los Contratos de Servicio de Cloud (o contratos de cloud base equivalentes) firmados antes del 1 de enero de 2019, se aplican las condiciones disponibles en <https://www.ibm.com/acs>.

5.1 Verificación

El Cliente: i) mantendrá y facilitará, cuando se le solicite, registros, y resultados generados por las herramientas del sistema, en la medida que sea razonablemente necesario para que IBM y su auditor independiente puedan verificar el cumplimiento por parte del Cliente del presente Contrato, y ii) pedirá, a la mayor brevedad, cualesquiera derechos de titularidad requeridos y pagará los cargos adicionales a los precios de IBM en vigor en ese momento y por cualquier otra responsabilidad o cargo que se determinase como resultado de dicha verificación, tal como IBM especifica en la factura. Estas obligaciones en relación con la verificación permanecerán en vigor durante la vigencia del Servicio de Cloud y los dos años siguientes.

5.2 Datos

5.2.1 Definiciones

El Servicio de Cloud implica el uso de, o el acceso a, Datos de IBM y Datos de la Comunidad. IBM proporciona los Datos y todo el contenido de terceros disponible a través del Servicio de Cloud sin garantías de ningún tipo y no será responsable por ninguna pérdida en la que el Cliente incurra como resultado del acceso o el uso de los Datos o el contenido de terceros. Se aplican las definiciones siguientes:

- Datos:** cualquier información, contenido, archivos, textos, gráficos, software, código, mensajes, salida de las consultas de búsqueda, entrada de las consultas de búsqueda, contenido de foros de discusión, métodos u otros materiales accesibles a través del Servicio de Cloud.
- Datos de IBM:** Datos puestos a disposición del Cliente por parte de IBM a través del Servicio de Cloud, excluyendo los Datos de la Comunidad. IBM, sus licenciatarios o sus proveedores conservarán todos los derechos, títulos e intereses sobre los Datos de IBM.
- Datos de la Comunidad:** datos puestos a disposición del Cliente a través del Servicio de Cloud por parte de otros usuarios del Servicio de Cloud.

5.2.2 Datos de IBM

IBM concede al Cliente una licencia no exclusiva, intransferible y limitada para acceder a los Datos de IBM y utilizarlos, exclusivamente a través del Servicio de Cloud (i) para el uso personal del Cliente como soporte a investigaciones e investigaciones de amenazas del Cliente o (ii) para integrar los Datos de IBM en las ofertas del Cliente. El Cliente no puede duplicar ni intentar duplicar partes importantes o la totalidad de los Datos de IBM o el Servicio de Cloud. El Cliente debe respetar todos los avisos de copyright, informaciones y restricciones contenidos en o adjuntados a cualesquiera Datos de IBM, y el Cliente no podrá retirar ningún texto, copyright u otros avisos de propiedad incluidos en los Datos de IBM. No se permite al Cliente eludir o intentar eludir ninguna de las limitaciones de acceso relacionadas con el Servicio de Cloud.

Si el Cliente incorpora los Datos de IBM en las ofertas del Cliente, el Cliente, en su contrato de usuario final: (a) limitará la responsabilidad colectiva del Cliente y sus proveedores terceros por daños directos a una cantidad razonable y renunciará a toda responsabilidad por daños consecuenciales y cualesquiera otros daños indirectos y garantías implícitas por proveedores terceros; (b) requerirá que el usuario final del Cliente presente cualquier reclamación que surja del contrato con el usuario final únicamente contra el Cliente; (c) prohibirá el uso de los Datos de forma separada de los productos o servicios del Cliente; y (d) prohibirá sublicenciar o distribuir de cualquier otra manera los Datos.

Asimismo, si el Cliente incorpora los Datos de IBM en las ofertas del Cliente, además de los daños por los que el Cliente puede ser responsable en virtud de la ley aplicable o de los términos del Contrato, el Cliente defenderá, indemnizará y mantendrá a IBM indemne ante aquellas reclamaciones de terceros que surjan de: (a) incumplimiento de los términos del párrafo anterior; o (b) representaciones, declaraciones, reclamaciones o garantías sobre los Datos de IBM no autorizadas por IBM.

Con excepción de lo expresamente indicado anteriormente, el Cliente no podrá copiar, modificar, reproducir, transmitir, vender, ofrecer para su venta, alquilar, arrendar, licenciar, sublicenciar, redistribuir o poner a disposición de terceros los Datos de IBM.

5.2.3 Datos de la Comunidad

El Cliente es responsable de las interacciones del Cliente con otros usuarios del Servicio de Cloud, incluyendo el acceso a los Datos de la Comunidad. Determinados Datos de la Comunidad pueden compartirse en una Colección o Amenaza. En relación con los Datos de la Comunidad disponibles públicamente, el propietario de los Datos ha concedido a los usuarios del Servicio de Cloud una licencia no exclusiva, internacional y pagada para usar, copiar, reproducir, modificar y/o realizar trabajos derivados de, y distribuir dichos Datos de la Comunidad o partes de los mismos (la Licencia Pública). Si el Cliente copia, reproduce, distribuye o pone a disposición de otros Datos de la Comunidad de contrato con la Licencia Pública, el Cliente deberá proporcionar atribución para los Datos de la Comunidad. El Cliente sólo puede utilizar los Datos disponibles en una Colección o Amenaza para el uso interno, no comercial del Cliente. El Cliente puede estar expuesto a Datos de la Comunidad que infrinjan políticas de IBM o esta Descripción del Servicio, o que sean ofensivos por cualquier motivo.

Los Datos de la Comunidad pueden incluir información de perfiles de usuario de otros usuarios del Servicio de Cloud. El Cliente no puede realizar minería de datos, copiar no utilizar la información del perfil para ninguna finalidad que no sea comunicarse con otros usuarios del Servicio de Cloud en relación con información de inteligencia de amenazas.

Los Datos de la Comunidad pueden incluir enlaces a sitios web no gestionados por IBM. IBM no se hace responsable por el contenido, los productos, los materiales o las prácticas (incluidas las prácticas de privacidad) de dichos sitios web. El Cliente comprende que al acceder a Datos de la Comunidad, el Cliente puede estar expuesto a sitios web de terceros que el Cliente considere ofensivos, indecentes o cuestionables.

Si el Cliente cree que los Datos incluyen información personal que es incorrecta o que debe ser eliminada, el Cliente puede ponerse en contacto con IBM utilizando la característica de contribución dentro de un Informe IP de X-Force.

6. Sustitución de Condiciones

6.1 Subcargado del Tratamiento: Cloudflare, Inc.

Lo siguiente prevalece sobre cualquier disposición contradictoria en las condiciones de Principios de Privacidad y Seguridad de los Datos de los Servicios de Cloud de entre las partes: este Servicio de Cloud usa Cloudflare, Inc. como Subcargado del Tratamiento del Contenido. Cloudflare trata el Contenido de forma no cifrada para optimizar la prestación del Servicio de Cloud. Cloudflare cumple los estándares PCI como Proveedor de Servicio de nivel 1 y está en proceso de obtener la homologación dentro de las normas ISO 27001 y SOC 2. (Para mayor claridad, el Servicio de Cloud, a nivel general, no cumple los estándares PCI).