IBM QRadar on Cloud

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

1.1 Ofertas

El Cliente puede seleccionar entre las siguientes ofertas disponibles:

1.1.1 IBM QRadar on Cloud

La oferta IBM QRadar on Cloud proporciona una solución de inteligencia de seguridad avanzada del Cloud de IBM, basada en el producto IBM Security QRadar SIEM. Permite a los Clientes recopilar, correlacionar y almacenar eventos generados en entornos de tipo cloud locales y remotos, así como realiza gestión de seguridad y amenazas como lo harían con un producto QRadar SIEM desplegado localmente. Como parte de esta oferta, IBM también proporciona monitorización de infraestructura ininterrumpida (24x7) y aplica los parches críticos o el nivel de software más reciente siempre que estén disponibles.

Este Servicio de Cloud incluye noventa (90) días de almacenamiento activo, con posibilidad de búsqueda, y tiene autorización en cantidades de 100 Eventos por Segundo (EPS).

1.2 Servicios Opcionales

1.2.1 IBM QRadar on Cloud Temporary Upgrade

Una actualización de servicio que aporta una capacidad adicional de 1.000 EPS para la recopilación y el procesamiento de eventos de registro, pero únicamente para un número de meses temporal. El Cliente puede comprar varias unidades de esta actualización, hasta el nivel de EPS máximo que la oferta pueda soportar. La intención de esta parte es permitir a un Cliente que necesita cobertura durante momentos "pico" durante el año satisfacer estas necesidades a través de una actualización de la capacidad temporal. Al final del plazo de vigencia, estas cantidades aumentadas de capacidad temporal se eliminarán del entorno del Cliente.

1.2.2 IBM QRadar on Cloud Data Capacity

La actualización de capacidad de datos agrega almacenamiento adicional y amplía el período de análisis. La actualización de capacidad proporciona a los Clientes hasta un año completo de datos de eventos almacenados por cada compra de actualización de 100 EPS.

1.2.3 IBM QRadar on Cloud Flows Add-On

Se integra con IBM QRadar SIEM y procesadores de flujo para proporcionar análisis de flujo y visibilidad de red de Capa 3 para ayudar al Cliente a percibir, detectar y responder a las actividades a través de la red del Cliente.

Este Servicio de Cloud incluye noventa (90) días de almacenamiento activo, con posibilidad de búsqueda, y tiene autorización en cantidades de 10.000 Flujos por Minuto (FPM).

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

Percibe y descubre proactivamente las vulnerabilidades de seguridad de las aplicaciones y los dispositivos de red, al agregar contexto y dar soporte a la priorización de las actividades de remediación y mitigación.

1.2.5 IBM QRadar on Cloud Log Archival

Permite al Cliente archivar datos de eventos del Servicio de Cloud durante el período suscrito. IBM trabajará con el Cliente para registrar eventos designados en el almacenamiento de objetos con fines de archivado. A petición del Cliente, IBM volverá a reunir hasta treinta (30) días de datos de eventos archivados en la instancia del Cliente del Servicio de Cloud en el plazo de tres (3) días laborables a partir de dicha petición. Dichos datos permanecerán disponibles para el Cliente durante 48 horas antes de volver al almacenamiento de objetos de archivado. El Cliente puede realizar dos peticiones en un

período de tres meses. La actualización de capacidad proporciona a los Clientes hasta un año completo de datos almacenados por cada actualización de 100 EPS adquirida.

1.2.6 IBM QRadar on Cloud Flows Add-On Data Capacity

La actualización de capacidad de datos agrega almacenamiento adicional y amplía el período de análisis al proporcionar al Cliente hasta un año completo de datos de flujo almacenados por cada compra de actualización de 10.000 FPM.

1.2.7 IBM QRadar on Cloud Flows Add-On Log Archival

Esta oferta permite a los Clientes archivar datos de flujo del Servicio de Cloud durante el período suscrito. IBM trabajará con el Cliente para grabar registros de flujo designados en el almacenamiento de objetos con fines de archivado. A petición del Cliente, IBM volverá a reunir hasta treinta (30) días de datos de flujo archivados en la instancia del Cliente del Servicio de Cloud en el plazo de tres (3) días laborables a partir de dicha petición. Dichos datos permanecerán disponibles para el Cliente durante 48 horas antes de volver al almacenamiento de objetos de archivado. El Cliente puede realizar dos peticiones en un período de tres meses. La actualización de capacidad proporciona a los Clientes hasta un año completo de datos almacenados por cada actualización de 10.000 FPM adquirida.

1.2.8 IBM QRadar on Cloud for Non-Production Environment

La oferta IBM QRadar on Cloud for Non-Production Environment ofrece una instancia de prueba dedicada del Servicio de Cloud. Permite a los Clientes recopilar, correlacionar y almacenar eventos generados en entornos locales y de cloud, así como realiza gestión de seguridad y amenazas como lo harían con un producto QRadar SIEM desplegado localmente en un entorno de prueba dedicado. Como parte de esta oferta, IBM también proporciona monitorización de infraestructura ininterrumpida (24x7) y aplica los parches críticos o el nivel de software más reciente siempre que estén disponibles. El Cliente solo puede utilizar este Servicio de Cloud para pruebas no productivas.

Este Servicio de Cloud incluye noventa (90) días de almacenamiento activo, con posibilidad de búsqueda.

1.3 Servicios de Aceleración

1.3.1 IBM QRadar on Cloud Optimization Service

Para este servicio de suscripción prestado de forma remota, IBM llevará a cabo una reunión de revisión con el Cliente para evaluar la salud actual de la instancia del Servicio de Cloud del Cliente y ofrecerá los resultados al Cliente a través de un informe sobre el estado de salud de QRadar on Cloud que identificará áreas de mejora, de existir.

Adicionalmente, IBM ofrecerá al Cliente cualquiera de los siguientes servicios de consultoría, a petición del Cliente, durante un máximo de ocho (8) días en el plazo de 1 año:

- Ayuda para añadir orígenes de registro adicionales al Servicio de Cloud;
- Configuración de búsquedas, informes y dashboards adicionales;
- Ajuste adicional en el despliegue existente de QRadar;
- Transferencia de conocimientos sobre temas específicos de QRadar.

1.3.2 Servicios de Configuración

Los siguientes servicios de configuración se prestan de forma remota y se solicitan por separado. Cada servicio solicitado vencerá a los noventa (90) días desde la compra, a menos que se indique de otro modo, independientemente de si se han utilizado todas las horas (si procede). Los servicios incluirán un IBM Engagement Manager designado que planificará las llamadas de puesta en marcha.

a. **IBM QRadar on Cloud Deployment Services**

Este servicio ofrece cuarenta (40) horas de servicios profesionales durante los cuales IBM realizará algunos o todos los puntos siguientes:

IBM llevará a cabo una revisión de la arquitectura SIEM de hasta dieciséis horas de duración para definir los requisitos de creación de informes del Cliente y ofrecerá sus resultados al Cliente en un informe de arquitectura de la solución que contribuirá a definir y capturar los requisitos del Cliente.

Este informe incluirá lo siguiente:

- Los requisitos de creación de informes definidos por el Cliente para cumplir los requisitos de inteligencia de seguridad, auditoría y conformidad del Cliente.
- Los requisitos de inteligencia de seguridad, casos de uso y aplicaciones en cuya implementación IBM puede ayudar (hasta diez (10) casos de uso y hasta dos (2) aplicaciones).
- Información de alto nivel sobre los orígenes del flujo y registro del Cliente necesaria para dar soporte a los casos de uso.
- Consideraciones sobre la infraestructura de red, como firewalls y puertos.

Según el informe de arquitectura de la solución, IBM llevará a cabo las siguientes tareas que permita el tiempo restante:

- Configuración de la recopilación de eventos de hasta tres (3) instancias de un máximo de diez (10) tipos de origen de registro en el Servicio de Cloud. Esta actividad incluirá la transferencia de conocimientos al personal relevante del Cliente, para que puedan añadir más orígenes de registro como necesiten. Solo se incluirán como parte de este servicio los orígenes de registro compatibles con los módulos estándar de soporte de dispositivo (DSM) de QRadar.
- Ajuste inicial, que incluye a) activación de reglas listas para usar, búsquedas guardadas, informes y gráficos de series temporales acumulados; b) identificación y eliminación de orígenes de ruido; y c) configuración de almacenamiento offline a través de NFS, CIFS o iSCSI.
- Implementación de diez (10) casos de uso y dos (2) aplicaciones de IBM QRadar App Exchange descritos en el documento de arquitectura de la solución.

b. **IBM QRadar on Cloud Custom Parser Service**

Este servicio proporcionará el desarrollo de un único analizador personalizado/uDSM para dar soporte a los tipos de origen de registro no estándar del Cliente que se van a enviar al Servicio de Cloud e incluye las siguientes tareas:

- Creación de un analizador personalizado para un tipo de origen de registro no estándar (trabajo realizado de forma remota);
- Creación, configuración y correlación de uDSM;
- Despliegue y prueba de uDSM personalizado;
- Análisis de hasta veinticinco tipos de mensaje del origen de registro.

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://www.ibm.com/dpa/dpl.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=FB0F42F0750011E6865BC3F213DB63F7

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:

- Un Compromiso es un servicio profesional o de formación relacionado con los Servicios de Cloud.
- Eventos por Segundo es el número de apariciones de un evento específico por segundo procesado por, o relacionado con, el uso de los Servicios de Cloud.
- Flujos por Minuto es el número de flujos por minuto gestionados o procesados por los Servicios de Cloud. Un Flujo es un registro de comunicaciones entre dos hosts. Los paquetes que contienen la misma IP de origen, IP de destino, puerto de origen, puerto de destino y protocolo se combinan como un registro de Flujo.
- Un Activo es un recurso tangible o elemento de valor identificado de manera única para su acceso o gestión por parte de 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 Software de Habilitación

El Servicio de Cloud contiene el Software de Habilitación siguiente:

Software de Habilitación	Condiciones de Licencia Aplicables (si existen)
Data Gateway	El Cliente solo puede instalar y utilizar hasta diez (10) copias de Data Gateway

6. Sustitución de Condiciones

6.1 Uso de Datos

Lo siguiente prevalece sobre cualquier disposición contradictoria el apartado Contenido y Protección de Datos de las condiciones básicas del Servicio de Cloud entre las partes: IBM no utilizará ni revelará los resultados que surjan del uso del Servicio de Cloud por parte del Cliente que sean exclusivos del Contenido (Insights) del Cliente o que de otro modo identifiquen al Cliente. IBM, no obstante, puede utilizar Contenido y otras informaciones derivadas del Contenido (excepto Insights) como parte del Servicio de Cloud, con la finalidad de mejorar el Servicio de Cloud. IBM también puede compartir identificadores de amenazas y otra información de seguridad incluida en el Contenido para la protección y la detección de amenazas.