

Descripción del Servicio

IBM QRadar Advisor with Watson

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 QRadar Advisor with Watson amplía la analítica cognitiva a QRadar Security Platform, ayuda a los Clientes y a los analistas de seguridad a investigar y a responder a las amenazas. Optimiza el corpus de conocimientos de Watson for Cyber Security, accediendo a datos no estructurados (que incluyen sitios web de seguridad, blogs, trabajos de investigación, entre otros) y correlacionándose con incidentes de seguridad locales. De este modo, puede ayudar a desvelar amenazas ocultas y a automatizar los conocimientos para una respuesta más rápida y una toma de decisiones mejorada. QRadar Advisor con Watson permite a un analista de seguridad enviar un ataque a Watson para realizar un descubrimiento de amenazas, utilizando su base de conocimientos de cientos de miles de orígenes de datos estructurados y no estructurados y correlacionándolos a las entidades de amenazas relacionadas con el ataque de seguridad original, tales como archivos maliciosos, direcciones de IP sospechosas, entidades ficticias y las relaciones entre ellas. Esto puede ser muy valioso a la hora de determinar si un ataque de seguridad está asociado o no a una campaña de malware conocido. Si es así, Watson proporciona los antecedentes del malware empleado, las vulnerabilidades explotadas y el alcance de la amenaza (incluyendo puntos finales adicionales potencialmente afectados), entre otra información.

1.1 Ofertas

El Cliente puede seleccionar entre las siguientes ofertas disponibles.

1.1.1 IBM QRadar Advisor with Watson

IBM QRadar Advisor with Watson requiere que el Cliente disponga de un despliegue activo de IBM QRadar, en un entorno local "on-premise" o en un despliegue Cloud, y tenga instalado el software de habilitación del Servicio de Cloud en dicho despliegue para que el Cliente pueda acceder a su funcionalidad. Cuando el Servicio de Cloud tiene derecho de Eventos Por Segundo, contiene un límite sobre el número de consultas de ataques de seguridad que el Cliente puede enviar al Servicio de Cloud a razón de 1,5 consultas por día por 100 Eventos Por Segundo (redondeado a la consulta más próxima) a los que el Cliente tiene derecho. Cuando el Servicio de Cloud tiene derecho de Servidor Virtual Gestionado (MVS), contiene un límite sobre el número de consultas de ataques de seguridad que el Cliente puede enviar al Servicio de Cloud a razón de 15 consultas por día por 100 MVS a los que el Cliente tiene derecho. Las consultas enviadas por encima de ese límite obtendrán un menor grado de prioridad y es posible que el Servicio de Cloud no las procese durante el resto de ese día.

1.1.2 IBM QRadar Advisor with Watson – Enterprise

IBM QRadar Advisor with Watson – Enterprise es el mejor despliegue para grandes centros de operaciones de seguridad (SOC) que generalmente superan los doscientos cincuenta mil Eventos Por Segundo o más. El Cliente debe instalar el software de habilitación del Servicio de Cloud en los despliegues adquiridos de IBM QRadar por separado para poder acceder a la funcionalidad del Servicio de Cloud. IBM QRadar Advisor with Watson – Enterprise está disponible bajo una Instancia basada en métricas de cargo que no dependen de la escala de despliegue de IBM QRadar del Cliente. El Cliente está limitado a 25 consultas en la cola en cualquier momento.

1.1.3 IBM QRadar Advisor with Watson – Starter Pack

IBM QRadar Advisor with Watson – Starter Pack está destinado a los usuarios noveles de QRadar Advisor with Watson. Este Servicio de Cloud tiene la funcionalidad completa de QRadar Advisor with Watson como se describe en el Apartado 1.1.1 anterior, pero solo está disponible con la primera compra del Cliente de QRadar Advisor with Watson, y no se renueva.

1.2 Servicios Opcionales

1.2.1 IBM QRadar Advisor with Watson – Test Environment

IBM QRadar Advisor with Watson – Test Environment es para Clientes que desean desplegar el Servicio de Cloud con su entorno de pruebas interno y pueden utilizarlo sólo para pruebas no productivas. IBM QRadar Advisor with Watson – Test Environment debe completarse con una suscripción al Servicio de Cloud a nivel productivo.

1.3 Servicios de Aceleración

1.3.1 IBM QRadar Advisor with Watson Advanced Services

Para este servicio de suscripción de entrega remota, IBM proporcionará cualquiera de los siguiente servicios de consulta al Cliente durante un máximo de cinco (5) días en el plazo de 1 año:

- Evaluar el proceso SOC del Cliente, incluyendo investigación o proceso de respuesta a incidencias;
- Reevaluar respuesta de conjuntos de referencia;
- Ajustar análisis automático para delitos de gran magnitud;
- Desarrollo de casos de uso;
- Proporcionar recomendaciones para cambios en el proceso SOC que incorporan QRadar Advisor con Watson;
- Ofrecer orientación sobre cómo comprender e incorporar más eficazmente los datos de QRadar Advisor con Watson en los procesos existentes del Cliente;
- Proporcionar transferencia de conocimientos sobre los temas adecuados de QRadar Advisor con Watson.

NOTA: Es posible que se incorporen las actividades siguientes a este servicio según el estado del desarrollo de QRadar del Cliente:

- Realizar una Revisión del Estado en el despliegue de QRadar del Cliente;
- Realizar ajustes adicionales en el despliegue de QRadar existente;
- Ayudar con orígenes de registro adicionales al despliegue de QRadar del Cliente.

1.3.2 IBM QRadar Advisor with Watson Basic Setup Service

Este servicio de configuración se proporciona de forma remota e incluye cuarenta (40) horas de servicios profesionales que caducan noventa (90) días a partir de la fecha de 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.

IBM realizará algunas o todas las tareas siguientes:

- Evaluar el proceso SOC del Cliente, incluyendo investigación o proceso de respuesta a incidencias;
- Implementar QRadar Advisor con Watson en el entorno del Cliente:
 - Instalar QRadar Advisor con Watson;
 - Correlacionar las propiedades unificadas con QRadar Advisor con Watson;
 - Implementar respuesta de conjuntos de referencia;
 - Ajustar análisis automático para delitos de gran magnitud;
 - Orientación sobre casos de uso;
 - Proporcionar recomendaciones para cambios en el proceso SOC que incorporan QRadar Advisor con Watson.

1.3.3 Servicio de Configuración Rápida de IBM QRadar Advisor with Watson

Este servicio de configuración está diseñado para Clientes con menos de 5000 eventos por segundo (EPS).

Para este servicio de entrega remota, IBM proporcionará cualquiera de los siguientes servicios de consulta (o una combinación de ellos) al Cliente durante un máximo de 16 horas en el plazo de 90 días:

- Instalación de QRadar Advisor with Watson.
- Gestión de permisos para QRadar Advisor with Watson.

- Configuración de QRadar Advisor with Watson, lo cual puede incluir lo siguiente:
 - Configuración del servidor de proxy seguro;
 - Envío de credenciales de intercambio de X-Force;
 - Creación de tokens de servicios autorizados;
 - Configuración de políticas de retención para almacenar resultados de análisis;
 - Asignación de propiedades de eventos personalizados;
 - Exportación de conjuntos de referencia;
 - Asignación de inteligencia frente a amenazas;
 - Configuración de la identificación de activos;
 - Optimización del uso.
- Investigación de delitos automáticos y resultados (al menos una muestra de casos de uso).
- Exploración de perspectivas con gráfico de relación.

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=0B439290AB5011E6BE74C84817AAB206>

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 Evento por Segundo (EPS) es una aparición de un EPS específico procesado por, o relacionado con el uso de, los Servicios de Cloud. A los efectos de este Servicio de Cloud, los Eventos por Segundo son aquellos recopilados y procesados por el despliegue de IBM QRadar del Cliente.
- Una Instancia es cada acceso a una configuración específica de los Servicios de Cloud.
- Un Compromiso es un servicio profesional o de formación relacionado con los Servicios de Cloud.
- 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 Software de Habilitación

El Servicio de Cloud contiene el Software de Habilitación siguiente:

- La aplicación IBM QRadar con Watson (<https://exchange.xforce.ibmcloud.com/hub>)

5.2 Uso Legal del Servicio de Cloud

El Servicio de Cloud se ha diseñado para ayudar al Cliente a mejorar su entorno de seguridad y los datos. El uso del Servicio de Cloud puede implicar distintas leyes o normativas, incluyendo las relativas a privacidad, protección de datos personales, empleo y almacenamiento y comunicaciones electrónicas que sean de aplicación. El Servicio de Cloud únicamente puede utilizarse con objetivos conformes a la ley y de forma legítima. El Cliente acepta utilizar el Servicio de Cloud de acuerdo con las políticas, normativas y leyes aplicables y es plenamente responsable de su cumplimiento. El Cliente declara que va a obtener o ha obtenido todos los consentimientos, permisos o licencias requeridos para el uso legítimo del Servicio de Cloud.

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.