IBM Resilient Security Orchestration, Automation and Response 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

IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud permite a las organizaciones gestionar y automatizar las personas, los procesos y la tecnología asociados con la respuesta a incidentes.

IBM Resilient SOAR Platform on Cloud agiliza la gestión de respuestas de privacidad y respuesta a incidentes para ofrecer una forma automatizada, más rápida y más flexible de que las organizaciones reaccionen ante eventos e incidentes. Resilient SOAR Platform on Cloud ofrece una base para la defensa correcta de la seguridad cibernética, que permite a las organizaciones:

- Crear planes de respuesta basados en estándares del sector y prácticas recomendadas.
- Integración más fácil con las herramientas de seguridad y de TI, y organización de respuestas a eventos e incidentes.
- Colaborar en toda la organización, aportando a las diversas partes interesadas herramientas para que puedan asumir su papel y tareas como parte de un esfuerzo de respuesta a incidentes.

La plataforma IBM Resilient SOAR está diseñada para organizaciones de diversos tamaños y complejidad y puede adquirirse con varios complementos opcionales. Al cliente no se le permite usar las prestaciones a menos que se especifique en la oferta o el complemento que han comprado.

1.1 Ofertas

El Cliente puede seleccionar entre las siguientes ofertas disponibles:

1.1.1 IBM Resilient SOAR Platform on Cloud

IBM Resilient SOAR Platform on Cloud Orchestration ofrece un base para la defensa de seguridad cibernética. Los Clientes pueden crear planes de respuesta basados en normas del sector y prácticas recomendadas, integrarse fácilmente con herramientas de seguridad y TI, y organizar respuestas a eventos e incidentes. El Servicio de Cloud facilita la colaboración en toda la organización, permitiendo que varias partes interesadas asuman su papel y tareas como parte de un esfuerzo de respuesta a incidentes.

Los equipos de seguridad pueden colaborar en eventos e incidentes de seguridad cibernética mediante las prestaciones de gestión de casos especialmente diseñadas de la plataforma. Las guías de referencia (Playbooks) dinámicas se adaptan a los ataques en rápida evolución, y los equipos pueden repetir rápidamente los procesos para mejorar la efectividad mediante la personalización de las guías de referencia, los campos de datos y los diseños de visualización. Las simulaciones colaboran adicionalmente en el ajuste de los procesos de respuesta. Las integraciones incorporadas e instalables proporcionan enriquecimiento de datos para recopilar el contexto para la toma de decisiones de un equipo de seguridad y permiten la organización de acciones de resolución, según la cantidad de Acciones por Mes compradas. La ingestión y el análisis del correo electrónico proporciona un método de reporting sencillo desde otras herramientas. El acceso se puede garantizar a través de la autenticación SAML. La transparencia y el análisis de riesgos reciben el soporte de análisis e informes. Esta oferta es necesaria para todos los demás complementos que se detallan a continuación.

1.2 Servicios Opcionales

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

IBM Resilient SOAR Platform on Cloud Actions activa las prestaciones organizativas de la plataforma. Las incorporaciones integradas e instalables, incluidas las integraciones con varias fuentes de inteligencia de amenazas, proporcionan un enriquecimiento automatizado para recopilar el contexto de cara a la toma de decisiones de un equipo de seguridad, así como la organización de acciones de remediación.

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

IBM Resilient SOAR Platform on Cloud Privacy permite a los Clientes evaluar y responder a infracciones de privacidad de datos. Los planes de respuesta generados por esta oferta se adaptan a los tipos de datos, las cantidades de registros y las jurisdicciones normativas aplicables. Los Clientes también pueden acceder a una base de conocimiento integrada de las regulaciones globales de notificación de infracciones de privacidad de datos que ayuda a personalizar todavía más los planes de respuesta a incidentes.

1.2.3 IBM Resilient SOAR Platform on Cloud Team Management Add-On

IBM Resilient SOAR Platform on Cloud Teams proporciona gestión de usuarios y segregación de datos entre varios equipos. La información confidencial se mantiene sobre la base de la necesidad de conocimiento, limitando el acceso con áreas de trabajo y con un control de acceso personalizable basado en roles. La gestión de usuarios y grupos puede simplificarse mediante el uso de Active Directory para la autorización de los usuarios. Los grupos independientes también se pueden configurar para que tengan su propia Organización.

1.2.4 IBM Resilient SOAR Platform on Cloud MSSP Add-On

IBM Resilient SOAR Platform on Cloud MSSP proporciona prestaciones de gestión de casos, procesos, personalización y administración de guías de referencia en múltiples Organizaciones. Los eventos e incidentes de varias Organizaciones se pueden ver en una única cola, lo cual proporciona a los analistas del proveedor de servicios de seguridad gestionada (MSSP) una visión integral de sus clientes. Las guías de referencia con configuración por Organización proporcionan una gestión simple de procesos estandarizados y personalizados.

1.2.5 IBM Resilient SOAR Platform on Cloud Non-Production Add-On

IBM Resilient SOAR Platform on Cloud Non-Production es una instancia independiente de IBM Resilient SOAR Platform que el Cliente solo podrá utilizar para actividades internas no productivas incluyendo, a título enunciativo y no limitativo, pruebas, ajuste del rendimiento, diagnóstico de errores, benchmarking interno, actividades de control de calidad de transferencia y/o desarrollo de extensiones o ampliaciones de uso interno en el Servicio de Cloud mediante interfaces de programación de aplicaciones publicadas.

1.3 Servicios de Aceleración

Las ofertas IBM Security Expert Labs (SEL) for Resilient Services son servicios prestados de forma remota que proporcionan tiempo de un experto de Resilient para orientación arquitectónica y de implementación relacionada con el despliegue de Resilient. La oferta IBM Resilient Security Orchestration, Automation and Response, ya sea como Servicio de Cloud o como software local, es un requisito previo para cualquiera de estos servicios.

1.3.1 IBM SEL for Resilient Base Starter Service

En reuniones a distancia durante 5 días, IBM proporcionará:

- ayuda en la definición de la arquitectura de IBM Security Resilient;
- instalación y configuración de IBM Security Resilient (cuando sea aplicable);
- formación de Analistas y Diseñadores para configurar y utilizar los planes de Respuesta a Incidentes actuales del Cliente, que reflejen los requisitos clave de su organización;
- guías de referencia configuradas de IBM Security Resilient basadas en los procesos únicos de las organizaciones del Cliente;
- cómo rastrear KPI y Métricas definidas según las necesidades de las organizaciones del Cliente y las prácticas recomendadas de la industria; y
- identificación de oportunidades de integración para dar soporte, automatizar y orquestar procesos de extremo a extremo.

1.3.2 IBM SEL for Resilient Premium Starter Service

En reuniones a distancia durante 3 días, IBM proporcionará:

- ayuda en la definición de la arquitectura de IBM Security Resilient;
- instalación de IBM Security Resilient (cuando sea aplicable);
- configuración inicial de IBM Security Resilient en el entorno del Cliente; y

- formación de Analistas y Diseñadores para configurar y utilizar los planes de Respuesta a Incidentes actuales del Cliente, que reflejen los requisitos clave de su organización.

1.3.3 IBM SEL for Resilient Additional Day

Además del servicio Base o Premium Starter, en una reunión a distancia de 1 día, IBM realizará cualquier actividad relacionada con IBM Security Resilient, que se acordará de antemano. Por ejemplo:

- instalación o configuración de soporte adicional de IBM Security Resilient o extensiones (cuando sea aplicable);
- formación o soporte adicional de Analistas para garantizar la disponibilidad para utilizar IBM Security Resilient como solución SOAR clave del cliente;
- orientación a los Diseñadores sobre cómo configurar y usar sus propias guías de referencia que reflejen los requisitos clave de las organizaciones del Cliente; o
- realización de un análisis rápido del entorno de IBM Security Resilient para recomendar posibles áreas de mejora.

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=A47500205B1911E6865BC3F213DB63F7

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 Usuario Autorizado es un usuario exclusivo a quien se ha concedido acceso a los Servicios de Cloud de forma directa o indirecta (por ejemplo, a través de un programa, dispositivo o servidor de aplicaciones multiplexor) mediante cualquier método.
- Usuario Simultáneo es un usuario que accede simultáneamente al Servicio de Cloud de forma directa o indirecta (por ejemplo, a través de un programa, dispositivo o servidor de aplicaciones multiplexor) en cualquier momento en particular. Una persona que accede simultáneamente al Servicio de Cloud varias veces se considera únicamente un único Usuario Simultáneo.
- Un Compromiso es un servicio profesional o de formación relacionado con 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 el objetivo de este Servicio de Cloud, un Elemento es una Acción. Una Acción es una solicitud de organización o automatización realizada por el Servicio de Cloud a otro programa de software.

5. Términos Adicionales

Para los Acuerdos de Servicio de Cloud (o acuerdos 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 Requisito de Derecho de Titularidad del Complemento

El Cliente debe adquirir un número y tipo de derechos de titularidad similares para el Servicio de Cloud básico y para cualquier Servicio de Cloud complementario.

5.3 Restricciones de Uso

Cada Cliente tiene derecho a realizar un máximo de cien mil (100.000) consultas del Servicio de Amenazas por mes. El Cliente crea una consulta del Servicio de Amenazas agregando un artefacto a un incidente cuando se ha activado su Servicio de Amenazas. Por cada dos (2) días a partir del momento en que el incidente permanece abierto y activo, se generará automáticamente una nueva consulta del Servicio de Amenazas.

Cada Cliente tiene derecho a generar un máximo de cien (100) correos electrónicos de notificación al día por Usuario Autorizado/Simultáneo. Los correos electrónicos de notificación los genera la plataforma de Resilient en base a la configuración controlada por el Cliente.

5.4 Información de Protección y Tratamiento de Datos Adicional

Para evitar dudas, IBM Resilient SOAR Platform on Cloud:

- no cifra Contenido en reposo;
- no ha sido diseñado para tratar ninguna Categoría Especial de Datos Personales; y
- no debe tener datos personales introducidos en campos de texto libre si no se solicita.

Puede encontrar información detallada sobre el cifrado y los tipos de Datos Personales procesados en la URL de la Ficha de Datos a la que se hace referencia en el apartado 2 anterior.

6. Sustitución de Condiciones

6.1 Uso de Datos

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.