IBM Resilient Security Orchestration, Automation and Response on Cloud

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order.

1. Cloud Service

IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud enables organizations to orchestrate and automate the people, processes, and technology that are associated with incident response.

IBM Resilient SOAR Platform on Cloud streamlines incident response and privacy response management to deliver an automated, faster, and more flexible way for organizations to react to events and incidents. The Resilient SOAR Platform on Cloud delivers a foundation for successful cybersecurity defense that enables organizations to:

- Create response plans that are based on industry standards and best practices.
- Integrate more easily with security and IT tools, and orchestrate responses to events and incidents.
- Collaborate across the organization, equipping various stakeholders with the tools to fulfill their roles and tasks as part of an incident response effort.

The IBM Resilient SOAR Platform is designed for organizations of various sizes and complexity and can be purchased with several optional add-ons. Client is not permitted to use capabilities unless specified in the offering or add-on they have purchased.

1.1 Offerings

The Client may select from the following available offerings:

1.1.1 IBM Resilient SOAR Platform on Cloud

IBM Resilient SOAR Platform on Cloud Orchestration offers a foundation for cybersecurity defense. Clients can create response plans based on industry standards and best practices, easily integrate with security and IT tools, and orchestrate responses to events and incidents. The Cloud Service facilitates collaboration across the organization, allowing various stakeholders to undertake their role and tasks as part of an incident response effort.

Security teams can collaborate on cybersecurity events and incidents using the platform's purpose-built case management capabilities. Dynamic Playbooks adapt to rapidly evolving attacks, and teams can quickly iterate on processes to improve effectiveness by customizing playbooks, data fields, and display layouts. Simulations further aid in refinement of response processes. Built-in and installable integrations provide data enrichment to gather context for a security team's decision-making and enable orchestration of remediation actions, pursuant to the quantity of Actions per Month purchased. Email ingestion and parsing provides a lightweight method to escalate from other tools. Access can be secured via SAML authentication. Transparency and risk analysis are aided by analytics and reporting. This offering is required for all other add-ons below.

1.2 Optional Services

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

IBM Resilient SOAR Platform on Cloud Actions enable the platform's orchestration capabilities. Built-in and installable integrations, including integrations with various threat intelligence feeds, provide automated enrichment to gather context for a security team's decision-making as well as orchestration of remediation actions.

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

IBM Resilient SOAR Platform on Cloud Privacy enables Clients to assess and respond to privacy data breaches. The response plans generated by this offering adapt to the data types, record quantities, and applicable regulatory jurisdictions. Clients can also access a built-in knowledgebase of global data privacy breach notification regulations that helps to further tailor their incident response plans.

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

IBM Resilient SOAR Platform on Cloud Teams provides user management and data segregation across multiple teams. Sensitive information is kept on a need-to-know basis by limiting access with Workspaces and with customizable role-based access control. User and group management can be simplified by leveraging Active Directory for user authorization. Separate groups can also be configured to have their own Organization.

1.2.4 IBM Resilient SOAR Platform on Cloud MSSP Add-On

IBM Resilient SOAR Platform on Cloud MSSP provides case management, process, customization, and playbook management capabilities across multiple Organizations. Events and incidents from multiple Organizations can be viewed in a single queue, providing managed security service provider (MSSP) analysts with a comprehensive view of their customers. Playbooks with per-Organization configuration provide simple management of both standardized and customized processes.

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

IBM Resilient SOAR Platform on Cloud Non-Production is a separate instance of the IBM Resilient SOAR Platform that Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, stating quality assurance activity and/or developing internally used additions or extension to the Cloud Service using published application programming interfaces.

1.3 Acceleration Services

IBM Security Expert Labs (SEL) for Resilient Services offerings are remotely delivered services that provide a Resilient expert's time for architectural and implementation guidance related to the Resilient deployment. The IBM Resilient Security, Orchestration and Response offering – either as a Cloud Service or as on-premise software – is a prerequisite for any of these Services.

1.3.1 IBM SEL for Resilient Base Starter Service

In a 5-day remote engagement, IBM will provide:

- help defining the IBM Security Resilient architecture;
- installed & configured IBM Security Resilient (where applicable);
- training for Analysts and Designers to configure and use Client's current Incident Response plans, reflecting Client's organizations' key requirements;
- IBM Security Resilient configured Playbooks based on Client's organizations' unique processes;
- how to track defined KPIs and Metrics according Client's organizations' need and industry best practices; and
- identify integration opportunities to support, automate and orchestrate end-to-end process.

1.3.2 IBM SEL for Resilient Premium Starter Service

In a 3-day remote engagement, IBM will:

- help define the IBM Security Resilient architecture;
- install IBM Security Resilient (where applicable);
- initially configure IBM Security Resilient in Client's environment; and
- train Analysts and Designers to configure and use Client's current Incident Response plans, reflecting its organizations' key requirements.

1.3.3 IBM SEL for Resilient Additional Day

In addition to the Base or Premium Starter service, in a 1-day remote engagement, IBM will perform any IBM Security Resilient related activity, to be agreed upon beforehand. For instance:

- further support installation or configuration of IBM Security Resilient or extensions (where applicable);
- further train or support Analysts to ensure readiness to use IBM Security Resilient as Client's key SOAR solution;
- guide Designers on how to configure and use their own 'Playbooks' that reflect Client's organizations' key requirements; or

- perform a quick scan of the IBM Security Resilient environment to recommend potential improvement areas.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below provide additional data protection information for the Cloud Services and its options regarding the types of Content that may be processed, the processing activities involved, the data protection features, and specifics on retention and return of Content. The DPA applies to personal data contained in Content, if and to the extent i) the European General Data Protection Regulation (EU/2016/679) (GDPR); or ii) other data protection laws identified at http://www.ibm.com/dpa/dpl apply.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=A47500205B1911E6865BC3F213DB63F7

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at https://www.ibm.com/support/home/pages/support-guide/.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Authorized User is a unique user authorized to access the Cloud Services in any manner directly or indirectly (for example, through a multiplexing program, device or application server) through any means.
- Concurrent User is a user simultaneously accessing the Cloud Service in any manner directly or indirectly (for example, through a multiplexing program, device, or application server) at any particular point in time. A person who is simultaneously accessing the Cloud Service multiple times counts only as a single Concurrent User.
- Engagement is a professional or training service related to the Cloud Services.
- Item is an occurrence of a specific item that is managed by, processed by, or related to the use of the Cloud Service. For the purpose of this Cloud Service, an Item is an Action. An Action is an orchestration or automation request made by the Cloud Service to another software program.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at https://www.ibm.com/acs apply.

5.1 Verification

Client will i) maintain, and provide upon request, records, and system tools output, as reasonably necessary for IBM and its independent auditor to verify Client's compliance with the Agreement, and ii) promptly order and pay for required entitlements at IBM's then current rates and for other charges and liabilities determined as a result of such verification, as IBM specifies in an invoice. These compliance verification obligations remain in effect during the term of the Cloud Service and for two years thereafter.

5.2 Add-On Entitlement Requirement

Client must acquire an equal number and type of entitlements to both the base and any Add-On Cloud Service.

5.3 Restrictions on Use

Each Client is entitled to make a maximum of one hundred thousand (100,000) Threat Service queries per month. Client creates a Threat Service query by adding an artifact to an incident when their Threat Service has been activated. For each two (2) days thereafter that the incident remains open and active, a new Threat Service query will automatically generate.

Each Client is entitled to generate a maximum of one hundred (100) notification emails per day per Authorized/Concurrent User. Notification emails are generated by the Resilient platform based on Client-controlled configuration.

5.4 Additional Data Processing and Protection Information

For the avoidance of doubt, IBM Resilient SOAR Platform on Cloud:

- does not encrypt Content at rest;
- is not designed to process any Special Categories of Personal Data; and
- should not have personal data entered into free text fields if not requested.

Detailed information regarding encryption and types of Personal Data processed can be found at the url for the Data Sheet referenced in Section 2 above.

6. Overriding Terms

6.1 Data Use

IBM will not use or disclose the results arising from Client's use of the Cloud Service that are unique to Client's Content (Insights) or that otherwise identify Client. IBM will however use Content and other information that result from Content (except for Insights) as part of the Cloud Service for the purpose of improving the Cloud Service. IBM may also share threat identifiers and other security information embedded in Content for threat detection and protection purposes.