IBM Resilient Incident Response Platform On Cloud

This Service Description describes the Cloud Service IBM provides to Client. Client means the company and its authorized users and recipients of the Cloud Service. The applicable Quotation and Proof of Entitlement (PoE) are provided as separate Transaction Documents

1. Cloud Service

The IBM Resilient Incident Response Platform on Cloud provides dynamic action plans (from malware to DDoS to lost devices) and best practices for responding to incidents generally. This knowledgebase leads a Client team through the response and may be configured to Client's unique operating procedures.

Incident response teams can manage and collaborate on their response directly within the IBM Resilient Incident Response Platform on Cloud. Unlike ticketing systems and other general-purpose IT tools, the IBM Resilient Incident Response Platform is fully configurable and purpose-built for incident response. Near comprehensive analysis, customizable dashboards, and robust reporting features allow senior leadership to access key information.

The IBM Resilient Incident Response Platform is designed for organizations of various sizes and complexity and is available in several, separately orderable versions:

1.1 IBM Resilient Incident Response Platform Enterprise on Cloud

IBM Resilient Incident Response Platform Enterprise on Cloud is a Cloud Service solution designed for large, varied systems of major enterprises. It offers a foundation for response planning, management, and mitigation for organizations and incident types. Users can create incident response plans based on industry standards and best practices and track incidents to resolution. The Cloud Service facilitates central collaboration across the organization, allowing various stakeholders to undertake their role and tasks as part of an incident response effort. Incident simulations may also be conducted, helping teams to test response plans, identify gaps, and refine response processes. Built-in integrations with various external threat intelligence feeds automate incident and artifact enrichment. The Cloud Service includes a knowledgebase of global data privacy breach notification regulations that helps to further tailor incident response plans. Data can also be synthesized from existing security and IT systems to provide near real-time information. Various tasks can be automated, streamlined, or fine-tuned within the Cloud Service, without the need for custom development. Client must acquire at least 1 Instance entitlement and 1 Authorized User entitlement for this service.

1.2 IBM Resilient Incident Response Platform Standard on Cloud

IBM Resilient Incident Response Platform Standard on Cloud is a Cloud Service solution designed to meet the incident response needs of medium to small enterprises. It offers much of the same functionality of IBM Resilient Incident Response Platform Enterprise on Cloud except for the following features and functions that Client is not permitted to use: privacy breach regulations, automation/orchestration, threat intelligence feeds, custom threat feeds, and LDAP integration. Client must acquire at least 1 Instance entitlement and 1 Authorized User entitlement for this service.

1.3 Optional Services

1.3.1 IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud

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

1.4 Remote Services

The following Remote Services are separately orderable, and each will expire ninety (90) days from purchase regardless of whether all hours (if applicable) have been used:

1.4.1 IBM Resilient Incident Response Platform Integration for Cloud

This offering provides integration services to connect the Cloud Service with related security and management systems using a pre-developed integration. Only one integration with one system will be set up per Engagement. Integrations available for set-up as by this Remote Service are listed below:

- **Integration with QRadar** – This integration will enable QRadar to automatically or manually push offenses to the Cloud Service as new incidents. It includes bi-directional syncing for notes, closing events, and new offense data.
- **Integration with HP Arcsight** – This integration will allow ArcSight users to manually or automatically push Arcsight event details to the Cloud Service as new incidents or add artifacts to existing incidents.
- **Integration with Splunk** – This integration will allow Splunk to automatically push alerts to the Cloud Service as incidents. Client can also run Splunk queries directly from the Cloud Service web interface.
- **Integration with ServiceNow** – This integration will enable ServiceNow users to create incidents in the Cloud Service and Cloud Service users to create tickets in ServiceNow. Updates to tickets or incidents are also replicated between the systems.
- **Integration with JIRA** – This integration will allow JIRA users to create incidents in the Cloud Service based on JIRA tickets and Cloud Service users to create tickets in JIRA. Updates to tickets or incidents are also replicated between the systems.

1.4.2 IBM Resilient Incident Response Platform Design Session for Cloud

This service provides a consultative engagement to help optimize the Cloud Service instance for Client. IBM consultants work with Client to synthesize Client's existing incident response processes for up to three (3) different incident types, refine them based on then-industry best practices and the capabilities of the Cloud Service, and advises Client on how to configure the Cloud Service to implement such processes.

2. Security Description

This Cloud Service follows IBM's data security and privacy principles for IBM SaaS which are available at http://www.ibm.com/cloud/data-security and any additional terms provided in this section. Any change to IBM's data security and privacy principals will not degrade the security of the Cloud Service.

This Cloud Service is not designed to any specific security requirements for regulated content, such as personal information or sensitive personal information. Client is responsible to determine if this Cloud Service meets Client's needs with regard to the type of content Client uses in connection with the Cloud Service.

3. Service Level Agreement

IBM provides the following availability service level agreement ("SLA") for the Cloud Service as specified in a PoE. The SLA is not a warranty. The SLA is available only to Client and applies only to use in production environments.

3.1 Availability Credits

Client must log a Severity 1 support ticket with the IBM technical support help desk within 24 hours of first becoming aware of an event that has impacted the Cloud Service availability. Client must reasonably assist IBM with any problem diagnosis and resolution.

A support ticket claim for failure to meet an SLA must be submitted within three business days after the end of the contracted month. Compensation for a valid SLA claim will be a credit against a future invoice for the Cloud Service based on the duration of time during which production system processing for the Cloud Service is not available ("Downtime"). Downtime is measured from the time Client reports the event until the time the Cloud Service is restored and does not include time related to a scheduled or announced maintenance outage; causes beyond IBM's control; problems with Client or third party content or technology, designs or instructions; unsupported system configurations and platforms or other Client errors; or Client-caused security incident or Client security testing. IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service during each contracted month, as shown in the table below. The total compensation with respect to any contracted month cannot exceed 10 percent of one twelfth (1/12th) of the annual charge for the Cloud Service.

3.2 Service Levels

Availability of the Cloud Service during a contracted month

Availability during a contracted month	Compensation (% of monthly subscription fee* for contracted month that is the subject of a claim)
99.5%	2%
98%	5%
96%	10%

* If the Cloud Service was acquired from an IBM Business Partner, the monthly subscription fee will be calculated on the then-current list price for the Cloud Service in effect for the contracted month which is the subject of a claim, discounted at a rate of 50%. IBM will make a rebate directly available to Client.

Availability, expressed as a percentage, is calculated as: the total number of minutes in a contracted month minus the total number of minutes of Downtime in a contracted month divided by the total number of minutes in the contracted month.

Example: 500 minutes total Downtime during contracted month

$$\frac{\text{43,200 total minutes in a 30 day contracted month} - \text{500 minutes Downtime} = \text{42,700 minutes}}{\text{43,200 total minutes}} = \text{2\% Availabilty credit for 98.8\% availability during the contracted month}$$

4. Technical Support

Technical support for the Cloud Service is provided via email, online forums, and an online problem reporting system. Technical support is offered with the Cloud Service and is not available as a separate offering. Technical support is available during the regular business hours of 9:00 AM to 6:00 PM Eastern Time excluding holidays.

Severity	Severity Definition	Response Time Objectives During Support Hours
1	Critical business impact/service down: Business critical functionality is inoperable or critical interface has failed. This usually applies to a production environment and indicates an inability to access services resulting in a critical impact on operations. This condition requires an immediate solution.	Within 1 hour
2	Significant business impact: A service feature or function is severely restricted in its use or Client is in jeopardy of missing business deadlines.	Within 2 business hours
3	Minor business impact: Indicates the service or functionality is usable and it is not presenting a critical impact on operations.	Within 4 business hours
4	Minimal business impact: An inquiry or non-technical request.	Within 1 business day

5. Entitlement and Billing Information

5.1 Charge Metrics

The Cloud Service is available under the charge metric specified in the Transaction Document:

a. Instance is a unit of measure by which the Cloud Service can be obtained. An Instance is access to a specific configuration of the Cloud Service. Sufficient entitlements must be obtained for each Instance of the Cloud Service made available to access and use during the measurement period specified in Client's PoE or Transaction Document.

b. Authorized User is a unit of measure by which the Cloud Service can be obtained. Client must obtain separate, dedicated entitlements for each unique Authorized User given access to the the Cloud Service in any manner directly or indirectly (for example, through a multiplexing program, device or application server) through any means. Sufficient entitlements must be obtained to cover the number of Authorized Users given access to the Cloud Service during the measurement period specified in Client's PoE or Transaction Document.

c. Engagement is a unit of measure by which the services can be obtained. An Engagement consists of professional and/or training services related to the Cloud Service. Sufficient entitlements must be obtained to cover each Engagement.

5.2 Overage Charges

If the Client's actual usage of the Cloud Service during the measurement period exceeds the entitlement specified in the PoE, Client will be charged for the overage as specified in the Transaction Document.

5.3 Remote Services Charges

Remote Services are purchased on a per Engagement metric and will be billed at the rate specified in the Transaction Document.

6. Term and Renewal Options

The term of the Cloud Service begins on the date IBM notifies Client of their access to the Cloud Service, as documented in the PoE. The PoE will specify whether the Cloud Service renews automatically, proceeds on a continuous use basis, or terminates at the end of the term.

For automatic renewal, unless Client provides written notice not to renew at least 90 days prior to the term expiration date, the Cloud Service will automatically renew for the term specified in the PoE.

For continuous use, the Cloud Service will continue to be available on a month to month basis until Client provides 90 days written notice of termination. The Cloud Service will remain available to the end of the calendar month after such 90 day period.

7. Additional Terms

7.1 General

Client agrees IBM may publicly refer to Client as a subscriber to the Cloud Services in a publicity or marketing communication.

7.2 Compliance Management Cloud Service

The Cloud Service can be used to help Client meet compliance obligations, which may be based on laws, regulations, standards or practices. Client acknowledges and agrees that any directions, suggested usage, or guidance provided by the Cloud Service does not constitute legal, accounting, or other professional advice, and Client is cautioned to obtain its own legal, accounting, or other expert counsel. Client also agrees that it is solely responsible for ensuring that Client and Client's activities, applications and systems comply with all applicable laws, regulations, standards and practices. Use of the Cloud Service does not guarantee compliance with any law, regulation, standard or practice.

7.3 Lawful Use of Cloud Service

The Cloud Service is designed to help the Client improve its security environment and data. Use of the Cloud Service may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. The Cloud Service may be used only for lawful purposes and in a lawful manner. Client agrees to use the Cloud Service pursuant to, and assumes all responsibility for complying with applicable laws, regulations and policies. Client represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of the Cloud Service.

7.4 Security Data

As part of this Cloud Service, that includes reporting activities, IBM will prepare and maintain de-identified and/or aggregate information collected from the Cloud Service ("Security Data"). The Security Data will not identify Client, or an individual except as provided in (d) below. Client herein additionally agrees that IBM may use and/or copy the Security Data only for the following purposes:

a. publishing and/or distributing the Security Data (e.g., in compilations and/or analyses related to cybersecurity);

b. developing or enhancing products or services;

c. conducting research internally or with third parties; and

d. lawful sharing of confirmed third party perpetrator information.

7.5 Cookies

Client is aware and agrees that IBM may, as part of the normal operation and support of the Cloud Service, collect personal information from Client (your employees and contractors) related to the use of the Cloud Service, through tracking and other technologies. IBM does so to gather usage statistics and information about effectiveness of our Cloud Service for the purpose of improving user experience and/or tailoring interactions with Client. Client confirms that it will obtain or have obtained consent to allow IBM to process the collected personal information for the above purpose within IBM, other IBM companies and their subcontractors, wherever we and our subcontractors do business, in compliance with applicable law. IBM will comply with requests from Client's employees and contractors to access, update, correct or delete their collected personal information.