IBM QRadar on Cloud

This Service Description describes the Cloud Service IBM provides to Client. Client means the contracting party 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

1.1 IBM QRadar on Cloud 100 EPS

The IBM QRadar on Cloud offering delivers an advanced security intelligence solution from the IBM Cloud based on the IBM Security QRadar SIEM product. It allows Clients to collect, correlate, and store events generated from both on premise and cloud environments and perform security and threat management as they would do with a QRadar SIEM product deployed on premise. As part of the offering, IBM also provides infrastructure monitoring on a 24x7 basis and applies the latest software level or critical patches whenever they are available.

This Cloud Service includes ninety (90) days of active, searchable storage.

1.2 Optional Features or Services

1.2.1 IBM QRadar on Cloud 1K EPS Temporary Upgrade

A service upgrade that gives an additional 1000 EPS capacity for collecting and processing log events, but only for a temporary number of months. Client can purchase multiple units of this upgrade, up to the maximum EPS level that the offering can support. The intention of this part is to enable a Client who requires coverage during "spike" occasions during the year to meet those requirements via a temporary capacity upgrade. At the end of the term length, these temporary capacity increase amounts will be removed from the Client's environment.

1.2.2 IBM QRadar on Cloud Data Capacity 100 EPS

The data capacity upgrade adds additional storage and expands the analysis period. The capacity upgrade provides clients with up to 1 full year of stored data for each 100 EPS upgrade purchased.

1.2.3 IBM QRadar on Cloud Flows Add-On

Integrates with IBM QRadar SIEM and flow processors to provide Layer 3 network visibility and flow analysis to help Client's sense, detect and respond to activities throughout Client's network.

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

Proactively senses and discovers network device and application security vulnerabilities, adding context and supporting the prioritization of remediation and mitigation activities.

1.2.5 IBM QRadar on Cloud Log Archival

Allows Client to archive event data from the Cloud Service during the subscribed period. IBM will work with Client to write designated events to object storage for archival purposes. Upon Client's request, IBM will remount up to thirty (30) days' worth of archived event data to Client's instance of the Cloud Service within three (3) business days of such request. Such data will remain available to Client for 48 hours before being returned to archival object storage. Client may make up to two requests per three month period. The capacity upgrade provides Clients with up to 1 full year of stored data for each 100 EPS upgrade purchased

1.2.6 IBM QRadar on Cloud Optimization Service

For this remotely delivered subscription service, IBM will conduct a review meeting with Client to assess the current health of the Client's Cloud Service instance and deliver the results to Client via a QRadar on Cloud Health Status report which will identify areas for improvement, if any.

Additionally, IBM will provide any of the following consulting services to the Client, on Client's request, for up to eight (8) days within the period of 1 year:

- Assist with adding additional log sources to the Cloud Service;
- Configure additional searches, reports and dashboards;

- Perform additional tuning on the existing QRadar deployment; and
- Provide knowledge transfer on pertinent QRadar subjects.

1.3 Setup Services

The following setup services are remotely delivered and separately orderable. Each service ordered will expire (90) days from purchase, unless otherwise noted, regardless of whether all hours (if applicable) have been used. Services will include a designated IBM Engagement Manager who will schedule any kick-off calls.

1.3.1 IBM QRadar on Cloud Deployment Service

This service provides forty (40) hours of professional services during which IBM will perform some or all of the following:

IBM will conduct a SIEM architecture review of up to sixteen hours in duration to define the Client's reporting requirements and will deliver its findings to the Client in a solution architecture report that will help define and capture the Client's requirements.

This report will include:

- The Client-defined reporting requirements to help meet Client's compliance, auditing and security intelligence requirements.
- The security intelligence requirements, use cases, and apps that IBM may assist with implementing (up to ten (10) use cases and up to two (2) apps).
- High level information on Client's log and flow sources that will be required to support the use cases.
- Network infrastructure considerations, such as firewalls and ports.

Based on the solution architecture report, IBM will perform the following tasks as remaining time allows:

- Configure the collection of events for up to three (3) instances of up to ten (10) log source types into the Cloud Service. This activity will include knowledge transfer to Client's relevant personnel so they may add more log sources as required. Only log sources supported by standard QRadar Device Support Modules (DSMs) will be included as part of this service.
- Initial tuning, which includes a) activating out-of-the-box rules, saved searches, accumulated time series graphs and reports; b) Identifying and removing sources of noise; and c) configuring offline storage via NFS, CIFS, or iSCSI.
- Implement the ten (10) use cases and two (2) apps from the IBM QRadar App Exchange documented in the solution architecture document.

1.3.2 IBM QRadar on Cloud Custom Parser Service

This service will provide the development of a single custom parser/uDSM for supporting Client's non-standard log source types that are to be sent to the Cloud Service and includes the following tasks:

- Create a custom parser for one non-standard log source type (work performed remotely);
- Create, configure, and mapping of uDSM;
- Deploy and test the custom uDSM; and
- Parse up to twenty-five message types for the log source.

2. Content and Data Protection

The Data Processing and Protection data sheet (Data Sheet) provides information specific to the Cloud Service regarding the type of Content enabled to be processed, the processing activities involved, the data protection features, and specifics on retention and return of Content. Any details or clarifications and terms, including Client responsibilities, around use of the Cloud Service and data protection features, if any, are set forth in this section. There may be more than one Data Sheet applicable to Client's use of the Cloud Service based upon options selected by Client. The Data Sheet may only be available in English and not available in local language. Despite any practices of local law or custom, the parties agree that they understand English and it is an appropriate language regarding acquisition and use of the Cloud Services. The following Data Sheet(s) apply to the Cloud Service and its available options. Client acknowledges that i) IBM may modify Data Sheet(s) from time to time at IBM's sole discretion and ii) such

modifications will supersede prior versions. The intent of any modification to Data Sheet(s) will be to i) improve or clarify existing commitments, ii) maintain alignment to current adopted standards and applicable laws, or iii) provide additional commitments. No modification to Data Sheet(s) will materially degrade the data protection of a Cloud Service.

Link(s) to the applicable Data Sheet(s):

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

Client is responsible to take necessary actions to order, enable, or use available data protection features for a Cloud Service and accepts responsibility for use of the Cloud Services if Client fails to take such actions, including meeting any data protection or other legal requirements regarding Content.

IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and DPA Exhibit(s) apply and are referenced in as part of the Agreement, if and to the extent the European General Data Protection Regulation (EU/2016/679) (GDPR) applies to personal data contained in Content. The applicable Data Sheet(s) for this Cloud Service will serve as the DPA Exhibit(s). If the DPA applies, IBM's obligation to provide notice of changes to Subprocessors and Client's right to object to such changes will apply as set out in DPA.

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 that there is a critical business impact and the Cloud Service is not available. 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 3 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)
Less than 99.9%	2%
Less than 99%	5%
Less than 95%	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.

4. Technical Support

Technical support for the Cloud Service is provided via email, online forums, and an online problem reporting system. IBM's software as a service support guide available at https://www-01.ibm.com/software/support/saas_support_guide.html provides technical support contact and other information and processes. Technical support is offered with the Cloud Service and is not available as a separate offering.

5. Entitlement and Billing Information

5.1 Charge Metrics

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

- 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.
- Events Per Second (EPS) is a unit of measure by which the Cloud Service can be obtained. An Event is an occurrence of a specific event that is processed by or related to the use of the Cloud Service. Sufficient entitlements must be obtained to cover the number of Events per second to be collected and processed by the Cloud Service during the measurement period specified in Client's PoE or Transaction Document.
- Ten Thousand Flows per Minute is a unit of measure by which the Cloud Service can be obtained. A Flow is a record of communications between two hosts. All of the packets that contain the same source IP, destination IP, source port, destination port, and protocol is combined to become one Flow record. Sufficient entitlements must be obtained to cover the highest number of Flows within a one minute interval, rounded up to the nearest Ten Thousand, managed or processed by the Cloud Service during the measurement period specified in Client's PoE or Transaction Document.
- 256 Assets is a unit of measure by which the Cloud Service can be obtained. An Asset is any tangible resource or item of value to be managed, including production equipment, facilities, transportation, IT hardware and software. Any resource or item with a unique identifier in the Cloud Service is separate Asset. Sufficient entitlements must be obtained to cover the Assets, rounded up to the nearest 256, accessed or managed by the Cloud Service during the measurement period specified in Client's Proof of Entitlement or Transaction Document. Each 256 Asset entitlement represents 256 Assets.

5.2 Set-Up Charges

A one-time setup fee will be billed at the rate specified in the Transaction Document for each setup service ordered.

5.3 Billing Frequency

Based on selected billing frequency, IBM will invoice Client the charges due at the beginning of the billing frequency term, except for overage and usage type of charges which will be invoiced in arrears.

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. Renewals are subject to an annual price increase as specified in a quote. In the event the automatic renewal is after receipt of an IBM notice of a withdrawal of the Cloud Service, the renewal term will end the earlier of the end of the current renewal term or the announced withdrawal date.

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 may not use Cloud Services, alone or in combination with other services or products, in support of any of the following high risk activities: design, construction, control, or maintenance of nuclear facilities, mass transit systems, air traffic control systems, automotive control systems, weapons systems, or aircraft navigation or communications, or any other activity where failure of the Cloud Service could give rise to a material threat of death or serious personal injury.

7.2 Enabling Software

This Cloud Service includes enabling software, which may be used only in connection with Client's use of the Cloud Service and only for the Cloud Service term. If enabling software is accompanied by a separate license agreement, the term of such license agreement(s) also applies, as limited by this section. In the event of conflict, the terms of this Service Description prevail over any such accompanying license agreement. Enabling software is provided "AS-IS". Client may only install and use up to 10 copies of the Enabling Software.

7.3 Secure Data

IBM may collect indicators of potential malicious activity from Client's Content for use in cyberthreat intelligence contexts, specifically URLs, IP addresses, domains, and file hashes. IBM may, in turn, notify Client if these indicators suggest that Client's cyberthreat risk is elevated.