IBM QRadar 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

1.1 Offerings

The Client may select from the following available offerings

1.1.1 IBM QRadar on Cloud

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 and is entitled in quantities of 100 Events per Second (EPS).

1.2 Optional Services

1.2.1 IBM QRadar on Cloud Temporary Upgrade

A service upgrade that gives an additional 1,000 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

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 event data for each 100 EPS upgrade purchase.

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.

This Cloud Service includes ninety (90) days of active, searchable storage and is entitled in quantities of 10,000 Flows per Minute (FPM).

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 Flows Add-On Data Capacity

The data capacity upgrade adds additional storage and expands the analysis period by providing Client with up to 1 full year of stored flow data for each 10,000 FPM upgrade purchase.

1.2.7 IBM QRadar on Cloud Flows Add-On Log Archival

This offering allows Clients to archive flow data from the Cloud Service during the subscribed period. IBM will work with Client to write designated flow records to object storage for archival purposes. Upon Client's request, IBM will remount up to thirty (30) days' worth of archived flow 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 10,000 FPM upgrade purchased.

1.2.8 IBM QRadar on Cloud for Non-Production Environment

The IBM QRadar on Cloud for Non-Production Environment offering delivers a dedicated test instance of the Cloud service. 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 within a dedicated test environment. 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. Client may only use this Cloud Service for non-production testing purposes.

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

1.3 Acceleration Services

1.3.1 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.

1.3.2 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.

a. **IBM QRadar on Cloud Deployment Services**

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.

b. **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. 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=FB0F42F0750011E6865BC3F213DB63F7

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:

- Engagement is a professional or training service related to the Cloud Services.
- Events Per Second is the number of occurrences of a specific event per second that is processed by or related to the use of the Cloud Services.
- Flows per Minute is the number of flows per minute managed or processed by the Cloud Services. A Flow is a record of communications between two hosts. Packets that contain the same source IP, destination IP, source port, destination port, and protocol is combined as one Flow record.
- Asset is a uniquely identified tangible resource or item of value to be accessed or managed by the Cloud Services.

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 Enabling Software

The Cloud Service contains the following Enabling Software:

Enabling Software	Applicable License Terms (if any)
Data Gateway	Client may only install and use up to ten (10) copies of the Data Gateway

6. Overriding Terms

6.1 Data Use

The following prevails over anything to the contrary in the Content and Data Protection section of the base Cloud Service terms between the parties: 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.