IBM QRadar Advisor with Watson

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

1. Cloud Service

IBM QRadar Advisor with Watson extends cognitive analytics to the QRadar Security Platform, helping Clients and security analysts to investigate and respond to threats. It leverages Watson for Cyber Security's corpus of knowledge, tapping into unstructured data (including security websites, blogs, and research papers, among others) and correlating with local security incidents. By doing so, it can help to uncover hidden threats and automate insights for responses and decision making. QRadar Advisor with Watson enables a security analyst to send a security offense to Watson to perform a threat discovery, using its knowledge base of hundreds of thousands of unstructured and structured data sources and mapping that back to threat entities related to the original security offense, such as malicious files, suspicious IP addresses, rogue entities, and the relationships between them. This can be particularly valuable in determining whether or not a security offense is associated with a known malware campaign. If so, Watson provides background on the malware employed, vulnerabilities exploited, and scope of the threat (including additional potentially impacted endpoints), among other insights.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM QRadar Advisor with Watson

IBM QRadar Advisor with Watson requires that Client have an active IBM QRadar deployment, either in a local on-premise environment or cloud deployment, and have installed the Cloud Service's enabling software on that deployment in order for Client to access its functionality. The Cloud Service contains a 'soft limit' on the number of security offense queries that Client may send to the Cloud Service at a rate of 1.5 requests per day per 100 Events Per Second (rounded up to the nearest request) that Client is entitled to. Queries sent beyond that limit will not be processed by the Cloud Service for the remainder of that day.

1.1.2 IBM QRadar Advisor with Watson – Enterprise

IBM QRadar Advisor with Watson – Enterprise is best suited for large security operations center (SOC) deployments that generally exceed two hundred fifty thousand Events Per Second or greater. Client must install the Cloud Service's enabling software on their separately acquired IBM QRadar deployment to access the Cloud Service's functionality. IBM QRadar Advisor with Watson – Enterprise is available under an Instance based charge metric that is not dependent on the scale of Client's IBM QRadar deployment. Client is limited to 25 submissions in the queue at any given time.

1.1.3 IBM QRadar Advisor with Watson – Starter Pack

IBM QRadar Advisor with Watson – Starter Pack is for first time users of QRadar Advisor with Watson. This Cloud Service has the full functionality of QRadar Advisor with Watson as described in section 1.1.1 above, but is only available as the Client's first purchase of QRadar Advisor with Watson, and does not renew.

1.2 Optional Services

1.2.1 IBM QRadar Advisor with Watson – Test Environment

IBM QRadar Advisor with Watson – Test Environment is for Clients who wish to deploy the Cloud Service with their internal test environment and can be used only for non-production testing purposes. IBM QRadar Advisor with Watson – Test Environment must be complemented by a subscription to the production-level Cloud Service.

1.3 Acceleration Services

1.3.1 IBM QRadar Advisor with Watson Advanced Services

For this remotely delivered subscription service, IBM will provide any of the following consulting services to the Client for up to 5 days in the period of 1 year:

- Evaluate Client SOC process, including investigation and/or incident response process;
- Re-evaluate reference-sets response;
- Adjust auto-analysis for high-magnitude offenses;
- Use case development;
- Provide recommendations for SOC process changes that incorporate QRadar Advisor with Watson;
- Give guidance on how to most efficiently understand and incorporate the data from QRadar Advisor with Watson into the Client's existing processes;
- Provide knowledge transfer on pertinent QRadar Advisor with Watson subjects.

NOTE: The following activities may be incorporated into this service based on the status of Client's QRadar deployment:

- Perform a Health Check on the Client's QRadar deployment;
- Perform additional tuning on the existing QRadar deployment;
- Assist with adding additional log sources to the Client's QRadar deployment.

1.3.2 IBM QRadar Advisor with Watson Basic Setup Service

This setup service is remotely delivered and includes forty (40) hours of professional services which 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.

IBM will perform some or all of the following:

- Evaluate Client SOC process, including investigation and/or incident response process;
- Implement QRadar Advisor with Watson in the Client's environment:
    - Install QRadar Advisor with Watson;
    - Map unified properties to QRadar Advisor with Watson;
    - Implement reference-sets response;
    - Adjust auto-analysis for high-magnitude offenses;
    - Use case guidance;
    - Provide recommendations for SOC process changes that incorporate QRadar Advisor with Watson.

1.3.3 IBM QRadar Advisor with Watson Quick Setup Service

This setup service is designed for Clients with less than 5,000 events per second (EPS).

For this remotely delivered service, IBM will provide any of the following consulting services (or combination thereof) to the Client for up to 16 hours within a 90-day period:

- QRadar Advisor with Watson installation.
- Permissions management for QRadar Advisor with Watson.
- Configuration of QRadar Advisor with Watson, which can include:
    - Configuration of secure proxy server;
    - Submission of X-Force exchange credentials;
    - Creation of authorized service tokens;
    - Configuration of retention policies for storing analysis results;
    - Custom event properties mapping;
    - Export of reference sets;

- Threat intelligence mapping;
- Configuration of asset identification;
- Usage optimization;

- Automatic offense investigation and results (at least one use case showcase).
- Insights exploration with the relationship graph.

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://ibm.com/dpa/dpl apply.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=0B439290AB5011E6BE74C84817AAB206

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:

- Event Per Second (EPS) is an occurrence of a specific EPS that is processed by or related to the use of the Cloud Services. For the purpose of this Cloud Service, the Events per Second are those collected and processed by the Client's IBM QRadar deployment.
- Instance is each access to specific configuration of the Cloud Services.
- Engagement is a professional or training service related to 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:

- IBM QRadar with Watson App (https://exchange.xforce.ibmcloud.com/hub)

5.2 Lawful Use of the 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.

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 may however use Content and other information (except for Insights) that results from Content in the course of providing the Cloud Service subject to removing personal identifiers; so that any personal data can no longer be attributed to a specific individual without the use of additional information. IBM will use such data only for research, testing, and offering development.