



## Service Description

---

### IBM QRadar Advisor with Watson

This Service Description describes the service IBM provides to Client. Client means and includes the company, its authorized users or 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 Advisor with Watson Service

IBM QRadar Advisor with Watson extends cognitive analytics to the QRadar Security Platform, helping clients and security analysts to rapidly 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 faster response and improved 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.

The Cloud Service requires that Client have an active IBM Security QRadar deployment and have installed the Cloud Service's enabling code 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 fifteen (15) request per day per 1000 Events Per Second that Client is entitled to. Queries sent beyond that limit will be processed by the Cloud Service, but will be de-prioritized and returned at a slower rate.

##### 1.2 IBM QRadar Advisor with Watson Trial

IBM QRadar Advisor with Watson Trial ("Trial Cloud Service") provides the functionality of IBM QRadar Advisor with Watson on a trial basis. Client's access to the Trial Cloud Service will be up to a period of time that is specified in a transaction document or other documentation, at the end of which Client's access will end. Client may also only send a maximum of 5 security offense queries per day during the trial. The Trial Cloud Service is provided on a non-warranted, 'as is' basis and Client may only use it for internal test and non-productive use. Response times to queries may vary during the trial based on current traffic levels.

#### 2. Security Description

This Cloud Service follows IBM's data security and privacy principles for IBM SaaS which are available at <http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp> 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 may be used to process select content that contains personal data if Client, as the data controller, determines that the technical and organizational security measures are appropriate to the risks presented by the processing and the nature of the data to be protected. Client recognizes that this Cloud Service does not offer features for the protection of sensitive personal data or data subject to additional regulatory requirements. Client acknowledges that IBM has no knowledge of the types of data that have been included in the content, and cannot make an assessment as to the suitability of the Cloud Services or the security protections which are in place.

The Cloud Service will enable Client to input and manage only the following content, some of which may be considered personal information ("PI") under applicable privacy laws:

- Destination/Source IP Addresses
- URLs
- Domains
- File Hashes

## 2.1 Security Features and Responsibilities

The Cloud Service implements the following security features:

The Cloud Service does encrypt content during data transmission between the IBM network and the Client's IBM Security QRadar deployment. The Cloud Service does not encrypt content when at rest awaiting data transmission.

The Cloud Service does not maintain or persist the input content after it has performed its function on that data.

## 3. Technical Support

Technical support for the Cloud Service is provided via email, online forums, and an online problem reporting system as described below. Technical support is offered with the Cloud Service and is not available as a separate offering.

Severity	Severity Definition	Response Time Objectives	Response Time Coverage
1	<b>Critical business impact/service down:</b> 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	24x7
2	<b>Significant business impact:</b> A service feature or function is severely restricted in its use or Client is in jeopardy of missing business deadlines.	Within 2 business hours	M-F business hours
3	<b>Minor business impact:</b> Indicates the service or functionality is usable and it is not presenting a critical impact on operations.	Within 4 business hours	M-F business hours}
4	<b>Minimal business impact:</b> An inquiry or non-technical request.	Within 1 business day	M-F business hours

For Clients that participated in the beta of the Cloud Service and who are still on version 7.2.7 of the QRadar Platform, some technical support issues may not be capable of being resolved and such Clients will need to upgrade to version 7.2.8 and install the latest patch in order to receive full technical support.

## 4. Entitlement and Billing Information

### 4.1 Charge Metrics

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

- a. **100 Events Per Second** – 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, rounded up to the nearest one hundred, that occurs during the measurement period specified in a Proof of Entitlement (PoE) or Transaction Document.

## 5. 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.

## **6. Enabling Software**

The Cloud Service requires the use of enabling software that Client downloads to Client systems to facilitate use of the Cloud Service. Client may use enabling software only in connection with use of the Cloud Service. Enabling software is provided "AS-IS".

The enabling software for the Cloud Service is made available for download by Client from the IBM Security App Exchange at <https://exchange.xforce.ibmcloud.com/hub>.

## **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 Enabling Software**

The Cloud Service requires the use of enabling software that Client downloads to Client systems to facilitate use of the Cloud Service. Client may use enabling software only in connection with use of the Cloud Service. Enabling software is provided "AS-IS".

The enabling software for the Cloud Service is made available for download by Client from the IBM Security App Exchange at <https://exchange.xforce.ibmcloud.com/hub>.

### **7.3 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.

### **7.4 Cloud Service Expiration**

Before expiration or termination of the Cloud Service, Client can use any of the provided reporting or export features of the Cloud Service to extract data.

### **7.5 Security Data**

As part of the 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.