IBM Security Intelligence on Cloud

This Service Description describes the Cloud Service IBM provides to Client. Client means and includes the company, its authorized users or recipients of the Cloud Service.

1. Cloud Service

The Cloud Service offering provided by IBM is described below. The applicable Quotation and Proof of Entitlement (PoE) are provided as separate Transaction Documents.

1.1 IBM Security Intelligence on Cloud Basic Service

The IBM Security Intelligence 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.

1.2 Optional Features

a. IBM Security Intelligence on Cloud 1K EPS Upgrade

A service upgrade that gives additional 1000 EPS capacity for collecting and processing log events. Client can purchase multiple units of this upgrade, up to the maximum EPS level that the offering can support.

b. IBM Security Intelligence on Cloud 1K EPS Temporary Upgrade

A service upgrade that gives 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.

2. Security Description

2.1 Security Policies

IBM has an information security team and maintains privacy and security policies that are communicated to IBM employees. IBM requires annual privacy and security training for personnel. IBM security policies are revalidated annually based on industry practices and IBM business requirements. Security incidents are handled based on comprehensive incident response procedures. IBM maintains physical security standards designed to limit access to authorized personnel at IBM data centers, including limited and monitored access points. Visitors register upon entering and are escorted while on the premises.

2.2 Access Control

IBM authorized staff use two–factor authentication to an intermediate “gateway” management host. IP Blocking may be utilized to prevent access by known compromised Internet sites and users in U.S. embargoed countries. Access to Client data and transfer of data in or out of the hosting environment is logged. WIFI use is prohibited within the IBM data centers that support this Cloud Service.

2.3 Service Integrity and Availability

Modifications to operating systems, application software, and firewall rules are handled under IBM’s change management process. Changes to firewall rules are reviewed by the IBM security staff before implementation. IBM monitors the data center 24x7. Internal and external vulnerability scanning is conducted regularly by authorized administrators and third party vendors to help detect and resolve potential system security exposures. Malware detection systems (antivirus, intrusion detection, vulnerability scanning, and intrusion prevention) are used in all IBM data centers. IBM’s data center services support a variety of information delivery protocols for transmission of data over public networks. Examples include HTTPS/SFTP/FTPS/S/MIME and site-to-site VPN. Backup data intended for off-site storage is encrypted prior to transport.

2.4 Activity Logging

IBM maintains logs of its activity for systems, applications, data repositories, middleware and network infrastructure devices that are capable of and configured for logging activity. To minimize the possibility of tampering and to enable central analysis, alerting and reporting, activity logging is done in real-time at central log repositories. Data is signed to prevent tampering. Logs are analyzed in real-time and via periodic analysis reports to detect anomalous behavior. Operations staff is alerted to anomalies and contacts a 24x7 on-call security specialist when needed.

2.5 Compliance

This Cloud Service is not US-EU Safe Harbor certified.

IBM performs industry standard SSAE 16 audits (or their equivalent) annually in production data centers for compliance with IBM information security policies. IBM maintains annual SOC II certification for specific SoftLayer data center location(s) used to provide the Cloud Service. IBM's SOC II review audits the security, availability and process integrity of how SoftLayer data centers operate its physical facilities. The audit report is available to Client and its auditors upon request.

3. Service Level Agreement

IBM provides the following availability service level agreement ("SLA") for the Cloud Service as specified in the Transaction Document. The SLA is not a warranty.

3.1 Definitions

a. "Availability Credit" means the compensation IBM will provide for a validated Claim. The Availability Credit will be applied in the form of a credit against a future invoice for the Cloud Service if acquired directly from IBM. If the Cloud Service is acquired from an IBM Business Partner, then IBM will make a rebate directly available to Client.

b. "Claim" means a claim Client submits to IBM that a service level has not been met during a Contracted Month.

c. "Contracted Month" means each full calendar month during the Cloud Service term measured from 12:00 a.m. Eastern US time on the first day of the month through 11:59 p.m. Eastern US time on the last day of the month.

d. "Downtime" means a period of time during which production system processing for the Cloud Service for which Client is entitled to use is not available. Downtime does not include the period of time when the Cloud Service is not available because of:

   (1) a scheduled or announced maintenance outage;

   (2) Events or causes beyond IBM's control (e.g., natural disaster, internet outages, emergency maintenance, etc.);

   (3) problems with content, equipment, or applications Client uses with the Cloud Service or any third party software, hardware, or other technology;

   (4) Client's failure to adhere to required system configurations and supported platforms or Client system administration, commands, or programming errors;

   (5) Client's caused security breach or any security testing performed by Client; or

   (6) IBM's compliance with any designs, specifications, or instructions that Client provides to IBM or a third party provides to IBM on Client's behalf.

e. "Event" means a circumstance or set of circumstances taken together, resulting in a failure to meet a service level.

3.2 Availability Credits

To submit a Claim, Client must log a Severity 1 support ticket (as defined below in the Technical Support section) for each Event with the IBM technical support help desk within 24 hours of first becoming aware that the Event has impacted use of the Cloud Service. Client must provide all necessary information about the Event and reasonably assist IBM with the diagnosis and resolution.

A Claim for Availability Credit must be submitted within three business days after the end of the Contracted Month in which the Claim arose.

a. Availability Credits are based on the duration of Downtime measured from the time Client reports the Downtime. For each valid Claim, IBM will apply the highest applicable Availability Credit based

on the cumulative availability of the Cloud Service during each Contracted Month, as shown in the table below.

b. For bundled Cloud Services (individual Cloud Service offerings packaged and sold together as a single offering for a single combined price), the Availability Credit will be calculated based on the single combined monthly price for the bundled Cloud Service, and not the monthly subscription fee for each individual Cloud Service. Client may only submit Claims relating to one individual Cloud Service in a bundle at a given time.

The total Availability Credits awarded with respect to any Contracted Month cannot exceed 10 percent of one twelfth (1/12th) of the annual charge for the Cloud Service.

3.3 Service Levels

Availability of the Cloud Service during a Contracted Month is as follows:

Achieved Service Level (Availability) during a Contracted Month	Availability Credit (% of Monthly Subscription Fee* for Contracted Month which 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%.

Achieved Service Level (Availability), expressed as a percentage, is calculated as: (a) the total number of minutes in a Contracted Month, minus (b) the total number of minutes of Downtime in a Contracted Month, divided by (c) the total number of minutes in a Contracted Month.

Example: 250 (50) minutes total Downtime during Contracted Month

43,200 total minutes in a 30 day Contracted Month -- 250 (50) minutes Downtime = 42,950 (43,200) minutes _____ 43,200 total minutes	= 2% Availability Credit for 99.4% Achieved Service Level during the Contracted Month

3.4 Other Information about this SLA

This SLA is available to the Client company and does not apply to claims made by a user of the Cloud Service or for any beta or trial services. The SLA only applies to the Cloud Services in productive use. It does not apply to non-production environments, including but not limited to test, disaster recovery, quality assurance, or development.

4. 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.

More information about hours of availability, email addresses, online problem reporting systems, and other technical support communication vehicles and processes are described in the IBM Software as a Service Support Handbook.

Severity	Severity Definition	Response Time Objectives	Response Time Coverage
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	Within 1 hour	24x7

	inability to access services resulting in a critical impact on operations. This condition requires an immediate solution.		
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	M-F 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	M-F business hours}
4	Minimal business impact: An inquiry or non-technical request.	Within 1 business day	M-F business hours

5. Entitlement and Billing Information

5.1 Charge Metrics

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

a. Events Per Second (EPS) is a unit of measure by which the Cloud Service can be obtained. An event is a log event generated from a server, application or device that can be processed for a specific purpose. 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 a Proof of Entitlement (PoE) or Transaction Document.

b. 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 Proof of Entitlement (PoE) or Transaction Document.

6. Term and Renewal Options

6.1 Term

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. Client may increase their level of use of the Cloud Service during the term by contacting IBM or their IBM Business Partner, and the increase will be confirmed in a Transaction Document.

6.2 Term Renewal Options

The Transaction Document will specify which of the following applies to renewal of the Cloud Service term.

6.2.1 Automatic Renewal

Where renewal is automatic, the Cloud Service will automatically renew for a term specified in the Transaction Document (either a one year term or the same duration as the expiring term) unless Client has provided written termination at least 90 days prior to the term expiration date.

6.2.2 Continuous Billing

Where billing is continuous, Client will continue to have access to the Cloud Service following the end of the term and will be billed for usage on a continuous basis. To discontinue use of the Cloud Service and stop the continuous billing process, Client must provide 90 days written notice of cancellation. Client will be billed for any outstanding access charges through the end of the month of cancellation.

6.2.3 Renewal Required

Where the renewal type is specified as "terminate", the Cloud Service will terminate at the end of the term and Client access will end. To continue use of the Cloud Service beyond the term end date, Client must order a new subscription term.

7. Enabling Software

This Cloud Service includes enabling software, which should be used only in connection with Client's use of the Cloud Service for the Cloud Service term. If the enabling software contains sample code, Client

may make derivative works of the sample code for use with the Cloud Service. 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. Client is responsible to remove enabling software upon expiration or termination of the Cloud Service.

8. General

8.1 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.