IBM X-Force Threat Intelligence

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

1. Cloud Service

IBM X-Force Threat Intelligence provides programmatic access to IBM X-Force Exchange through a RESTful API that returns information in JavaScript Object Notation (JSON). The Cloud Service also supports the Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) standards. The Cloud Service is designed to provide the following key capabilities that help the user:

a. Access information on specific security investigations, known as 'collections', consisting of both unstructured and structured content.

b. Access descriptions of the type of incident (for example, malware, data breach, or vulnerability), and the associated observables relevant to the incident.

c. Obtain up-to-date and comprehensive intelligence across the threat indicators that are most often the starting point for further research, and the context to understand these indicators.

d. Integrate Data (as defined below) with Client's offerings to leverage threat intelligence information.

1.1 Offerings

The Client may select from the following available offerings:

1.1.1 IBM X-Force Exchange Commercial API

The IBM X-Force Exchange Commercial Application Programming Interface (API) allows users to automate the consumption of threat intelligence from IBM X-Force Exchange, the cloud-based threat intelligence sharing platform from IBM. The offering is sold in packs of Ten Thousand Items.

1.1.2 IBM X-Force Exchange Commercial API Enterprise

The IBM X-Force Exchange Commercial Application Programming Interface (API) Enterprise allows users to automate the consumption of threat intelligence from IBM X-Force Exchange, the cloud-based threat intelligence sharing platform from IBM. The offering is sold per Instance. One Instance provides unlimited access to IP and URL by category feeds, IP and URL reports, and vulnerability feeds, as well as all TAXII feeds. Requests to indicators not found on X-Force Exchange are limited to 100,000 Items per month.

1.1.3 IBM Advanced Threat Protection Feed by X-Force

The IBM Advanced Threat Protection Feed by X-Force provides users a defined set of actionable indicators for direct ingestion into security tools and solutions. The feed provides access to actionable indicators of compromise (IP's and URL's), analyst derived indicators of compromise, and our DNS Early Warning indicators. Feeds are available in multiple formats including: STIX/TAXII, JSON, Text List and CSV formats.

1.1.4 Threat Intelligence Insights Standard for IBM Cloud Pak for Security

This Cloud Service is available at no charge and offers Clients the ability to integrate core threat intelligence and enable features within the Threat Intelligence Insights application on Cloud Pak for Security. With this package Clients get access to the no charge tier of X-Force Threat Intelligence content, including X-Force Advisories, Threats and associated IOC's (IP's, URL's, Vulnerabilities, Hash's). In addition, Clients can run a manual Am-I-Affected capability to search and identify malicious threats in their environment. The IBM Security Threat Intelligence Insights application available as part of IBM Cloud Pak for Security is a prerequisite for this Cloud Service.

1.1.5 Threat Intelligence Insights Advanced for IBM Cloud Pak for Security

Threat Intelligence Insights Advanced for IBM Cloud Pak for Security is a premium package that offers Clients the ability to add X-Force's next generation of threat intelligence and capabilities to the Threat Intelligence Insights application on Cloud Pak for Security. Advanced threat intelligence content, curated by IBM's Incident Response and Analysis Team (IRIS) team, includes access to in-depth Malware, Threat

Groups, Threat Activity and Industry analyses reports, remediation recommendations, indicators of compromise (IOC's) and more. The Advanced package also enables Clients to run the Am-I-Affected capability continuously and automatically, proactively prioritizing and identifying relevant threats in a user's environment. The IBM Security Threat Intelligence Insights application available as part of IBM Cloud Pak for Security is a prerequisite for this Cloud Service.

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=1ECC13601F5911E69AAAC4D0C72C126B

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:

- Instance is each access to specific configuration of the Cloud Services.
- Item is an occurrence of a specific item that is managed by, processed by, or related to the use of the Cloud Service. For this service, an Item is each result returned from a single query.
- Managed Virtual Server (MVS) is comprised of processing units, memory and input/output capabilities that executes requested procedures, commands or applications 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 Verification

Client will i) maintain, and provide upon request, records, and system tools output, as reasonably necessary for IBM and its independent auditor to verify Client's compliance with the Agreement, and ii) promptly order and pay for required entitlements at IBM's then current rates and for other charges and liabilities determined as a result of such verification, as IBM specifies in an invoice. These compliance verification obligations remain in effect during the term of the Cloud Service and for two years thereafter.

5.2 Data

5.2.1 Definitions

The Cloud Service involves use of, or access to, IBM Data and Community Data. IBM provides the Data and all third-party content available through the Cloud Service without warranties of any kind, and shall not be liable for any losses Client incurs as a result of accessing or using the Data or the third party content. The following definitions apply:

a. **Data** – means any information, content, files, text, graphics, software, code, messages, output from search queries, input to search queries, discussion forum content, methods or other materials accessible through the Cloud Service.

b. **IBM Data** – means Data made available to Client from IBM through the Cloud Service, excluding Community Data. IBM, its licensors or its suppliers retain all right, title, and interest in the IBM Data.

c. **Community Data** – means Data made available to Client through the Cloud Service from other Cloud Service users.

5.2.2 IBM Data

IBM grants Client a limited, nonexclusive, nontransferable license to access and use the IBM Data through the Cloud Service solely – (i) for Client's personal use in support of Client's research and threat investigations, or (ii) for purposes of integrating the IBM Data into Client's offerings. Client may not duplicate or attempt to duplicate major portions or the entire contents of the IBM Data or the Cloud Service. Client must abide by all copyright notices, information, and restrictions contained in or attached to any of IBM Data, and Client may not remove any text, copyright, or other proprietary notices contained in IBM Data. Client is not permitted to circumvent or attempt to circumvent any access limitations related to the Cloud Service.

If Client incorporates IBM Data into Client's offerings, Client shall, in its end user agreement: (a) limit the collective liability of Client and its third party suppliers for direct damages to a reasonable amount and disclaim any and all liability for consequential and other indirect damages and implied warranties for third party suppliers; (b) require Client's end user to bring any claims arising out of the end user agreement solely against Client; (c) prohibit use Data separately from Client's products or services; and (d) prohibit sublicensing or otherwise further distributing the Data.

Further, if Client incorporates the IBM Data into Client's offerings, then in addition to damages for which Client may be liable under applicable law or the terms of the Agreement, Client will defend, indemnify and hold harmless IBM against and with respect to all third-party claims arising from: (a) noncompliance with the terms of the preceding paragraph; or (b) representations, statements, claims or warranties regarding the IBM Data not authorized by IBM.

Except as explicitly set forth above, Client may not copy, modify, reproduce, transmit, sell, offer for sale, rent, lease, license, sublicense, redistribute, or otherwise make available to third parties the IBM Data.

5.2.3 Community Data

Client is responsible for Client's interactions with other users of the Cloud Service, including accessing Community Data. Certain Community Data may be shared in a Collection or Threat. With respect to publicly available Community Data, the owner of the Data has granted Cloud Service users a non-exclusive, worldwide, paid-up right and license to use, copy, reproduce, modify and/or make derivative works of, and distribute such Community Data or portions thereof (the Public License). If Client copies, reproduces, distributes or otherwise makes available Community Data in accordance with the Public License, Client must provide attribution for the Community Data. Client may use Data made available in a

Collection or Threat for Client's internal, non-commercial use only. Client may be exposed to Community Data that violates IBM policies, this Service Description, or is otherwise offensive.

Community Data may include the user profile information of other Cloud Service users. Client may not data mine, copy or otherwise use profile information for any purpose other than to communicate with other Cloud Service users about threat intelligence information.

Community Data may include links to websites not operated by IBM. IBM is not responsible for the content, products, materials, or practices (including privacy practices) of such websites. Client understands that by accessing Community Data Client may be exposed to third-party websites that Client finds offensive, indecent or otherwise objectionable.

If Client believes the Data includes personal information that is incorrect or otherwise should be removed, Client can contact IBM using the Contribute feature within an X-Force IP Report.

6. Overriding Terms

6.1 Cloudflare, Inc. Subprocessor

The following prevails over anything to the contrary in the Data Security and Privacy Principles for Cloud Services terms between the parties: This Cloud Service uses Cloudflare, Inc. as one of its Subprocessors of Content. Cloudflare processes Content in unencrypted form to optimize delivery of the Cloud Service. Cloudflare is PCI compliant as a Level 1 Service Provider and is in the process of working toward ISO 27001 and SOC 2 compliance. (For clarity, the overall Cloud Service is not PCI-compliant).