IBM X-Force Threat Intelligence

本“服务描述”描述云服务。适用的订单文档提供有关客户订单的定价和其他详细信息。

1. 云服务

IBM X-Force Threat Intelligence 通过 RESTful API 提供对 IBM X-Force Exchange 的编程访问，这将返回采用 JavaScript 对象表示法 (JSON) 的信息。云服务还支持 Structured Threat Information eXpression (STIX) 和 Trusted Automated eXchange of Indicator Information (TAXII) 标准。云服务旨在提供以下关键功能来帮助用户：

a. 访问有关特定安全调查的信息（称为“集合”），包括非结构化和结构化内容。

b. 访问事件类型的描述（例如，恶意软件、数据违规或漏洞）以及与此事件相关的关联可观测项。

c. 通过威胁指标（这通常是进一步调查的起点）获取最新的全面情报，并获取上下文以了解这些指标。

d. 将数据（如下面所定义）与客户服务产品相集成以利用威胁情报信息。

1.1 服务产品

客户可以从以下可用服务产品中选择：

1.1.1 IBM X-Force Exchange Commercial API

IBM X-Force Exchange Commercial Application Programming Interface (API) 允许用户自动从 IBM X-Force Exchange（IBM 的基于云的威胁情报共享平台）中使用威胁情报。该服务产品打包出售，每一万项目为一包。

1.1.2 IBM X-Force Exchange Commercial API Enterprise

IBM X-Force Exchange Commercial Application Programming Interface (API) Enterprise 允许用户自动从 IBM X-Force Exchange（IBM 的基于云的威胁情报共享平台）中使用威胁情报。该服务产品按实例出售。一个实例通过类别订阅源、IP 和 URL 报告、漏洞订阅源以及所有 TAXII 订阅源提供对 IP 和 URL 的无限制访问。对 X-Force Exchange 上未找到的指标的请求限制为每月 100,000 个项目。

1.1.3 IBM Advanced Threat Protection Feed by X-Force

IBM Advanced Threat Protection Feed by X-Force 为用户提供一组预定义的可行指标，用于直接注入到安全工具和解决方案。订阅源支持访问可行的威胁指标（IP 和 URL）、分析人员派生的威胁指标以及我们的 DNS 预警指标。订阅源以多种格式提供，包括：STIX/TAXII、JSON、文本列表和 CSV 格式。

1.1.4 Threat Intelligence Insights Standard for IBM Cloud Pak for Security

此云服务免费提供，使客户能够整合核心威胁情报，并启用 Cloud Pak for Security 上 Threat Intelligence Insights 应用程序内的功能。通过此软件包，客户可以访问 X-Force Threat Intelligence 免费层面的内容，包括 X-Force 咨询、威胁以及相关危害指标（IP、URL、漏洞、散列）。此外，客户还可以手动运行 Am-I-Affected 功能，搜索和识别其环境中的恶意威胁。IBM Security Threat Intelligence Insights 应用程序作为 IBM Cloud Pak for Security 的一部分提供，是获得此云服务的前提条件。

1.1.5 Threat Intelligence Insights Advanced for IBM Cloud Pak for Security

Threat Intelligence Insights Advanced for IBM Cloud Pak for Security 是一个高级软件包，使客户能够将 X-Force 的下一代威胁情报和功能添加到 Cloud Pak for Security 上的 Threat Intelligence Insights 应用程序中。由 IBM 的事件响应和分析团队 (IRIS) 团队创建的高级威胁情报内容包括，访问深层恶意软件、威胁分组、威胁活动和行业分析报告、补救建议、危害指标 (IOC) 等等。高级软件包还使客户能够连续自动运行 Am-I-Affected 功能，主动地对用户环境中的相关威胁进行优先级划分和识别。IBM Security Threat Intelligence Insights 应用程序作为 IBM Cloud Pak for Security 的一部分提供，是获得此云服务的前提条件。

2. 数据处理和保护数据表

位于 http://ibm.com/dpa 的 IBM 数据处理附录 (DPA) 以及下面链接中的“数据处理和保护数据表”（称为数据表或 DPA 附录）提供针对云服务及其选项的其他数据保护信息，关于可处理的内容类型、所涉及的处理活动、数据保护功能以及有关内容保留和返回的细节。如果 i) 欧盟通用数据保护条例 (EU/2016/679) (GDPR)；或 ii) http://ibm.com/dpa/dpl 上标示的其他数据保护法律适用于内容中包含的个人数据，那么 DPA 也适用于这些个人数据。

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1ECC13601F5911E69AAAC4D0C72C126B

3. 服务级别和技术支持

3.1 服务标准协议

IBM 为客户提供以下可用性服务级别协议 (SLA)。IBM 会根据累积的可用云服务应用适用的最高赔偿，如下表中所示。可用性百分比的计算方法为：“约定的月份”内总分钟数减去“约定的月份”内服务停用的总分钟数，再除以“约定的月份”内总分钟数。“服务停用”定义、索赔过程以及如何联系 IBM 反馈服务可用性问题在 IBM 的云服务支持手册 (https://www.ibm.com/software/support/saas_support_overview.html) 中进行了说明。

可用性	积分 （每月订购费用的百分比*）
小于 99.9%	2%
低于 99.0%	5%
低于 95.0%	10%

* 订购费用是当月该索赔相关的合同价格。

3.2 技术支持

通过在位于 https://www.ibm.com/support/home/pages/support-guide/ 的 IBM 支持指南中选择云服务来查找针对云服务的技术支持，包括支持联系人详细信息、严重性级别、可用性的支持小时数、响应时间以及其他支持信息和流程。

4. 费用

4.1 收费标准

云服务的收费标准在交易文档中指定。

以下收费标准适用于此云服务：

- 实例是对云服务的特定配置的每次访问。
- 项目是指出现一个通过使用云服务管理、处理或与使用云服务相关的特定项目。对于此云服务，一个“项目”表示从单个查询返回的每个结果。
- 托管虚拟服务器由处理单元、内存和输入/输出功能组成，这些功能将执行受云服务管理的所请求的过程、命令或应用程序。

5. 附加条款

对于 2019 年 1 月 1 日之前执行的云服务协议（或等效的基础云协议），可用的条款 (https://www.ibm.com/acs) 将适用。

5.1 验证

客户将 i) 按照 IBM 及其独立审计员验证客户遵守协议的情况的合理所需，保存并根据请求提供记录和系统工具输出；并且 ii) 及时订购必需的权利并按照 IBM 当时的费率支付费用以及 IBM 在发票中指定的此类验

证所确定的任何其他费用和责任。在云服务期限内以及本协议到期后的两年内，这些合规性验证义务均保持有效。

5.2 数据

5.2.1 定义

云服务涉及使用或者访问 IBM 数据和社区数据。IBM 提供通过云服务可用的数据和所有第三方内容，不做任何形式的保证，并且不对客户因访问或使用数据或第三方内容而导致的任何损失承担责任。以下定义适用：

a. **数据** – 表示任何信息、内容、文件、文本、图形、软件、代码、消息、搜索查询的输出、搜索查询的输入、论坛内容、方法或者其他可通过云服务访问的资料。

b. **IBM 数据** – 表示从 IBM 通过云服务提供给客户的数据，不包括社区数据。IBM、其许可方或者其供应商保留 IBM 数据中的全部权利、所有权和利益。

c. **社区数据** – 表示其他云服务用户通过云服务提供给客户的数据。

5.2.2 IBM 数据

IBM 将授予客户受限的、非排他的且不可转让的许可以供自行通过云服务访问和使用 IBM 数据：(i) 客户在研究和威胁调查中自己使用；或者 (ii) 将 IBM 数据集成到客户的服务产品。客户不得复制或尝试复制 IBM 数据或云服务中的大部分内容或整个内容。客户必须遵守任何 IBM 数据中包含或随附的所有版权声明、信息和限制，并且客户不得移除 IBM 数据中包含的任何文本、版权或其他专有声明。客户不得规避或尝试规避与云服务相关的任何访问限制。

如果客户将 IBM 数据纳入客户的服务产品中，客户应在其最终用户协议中：(a) 将客户及其第三方供应商的集体责任限制为合理金额的直接损害，并且不承担后续和其他间接损害以及第三方供应商的默示保证的任何和所有责任；(b) 要求客户的最终用户将最终用户协议产生的任何索赔仅针对客户；(c) 禁止独立于客户的产品或服务使用数据；(d) 禁止再许可或以其他方式进一步分发数据。

此外，如果客户将 IBM 数据并入客户服务产品，那么除了客户依据适用法律或协议条款而可能承担的损害赔偿外，针对由于以下原因导致的所有第三方索赔，客户将为 IBM 辩护、赔偿并使 IBM 免受损害：(a) 未遵守前述条款；或者 (b) 未经 IBM 授权的有关 IBM 数据的表示、声明、索赔或保证。

除非上文有明确规定，否则客户不得对 IBM 数据进行复制、修改、再制作、传输、销售、标价出售、出租、租赁、许可、再许可、再分发或提供给第三方。

5.2.3 社区数据

客户负责客户与云服务的其他用户的互动，包括访问社区数据。集合或威胁中可能会分享特定的社区数据。出于社区数据的公开可用性，数据所有者已授予云服务用户非排他的、全球范围的、已付费的权利和许可，以使用、复制、再制作、修改和/或制作衍生作品以及分发此类社区数据或其任何部分（公共许可）。如果客户依据“公共许可”复制、再制作、分发或以其他方式提供社区数据，那么客户必须提供社区数据的归属。客户只能在客户内部使用在集合或威胁中提供的数据，且仅限于非商业用途。客户可能会接触到违反 IBM 策略及本服务描述的社区数据或攻击性的社区数据。

社区数据可能包含其他云服务用户的用户概要信息。除了与其他 Cloud Service 用户沟通威胁情报信息之外，客户不得出于任何目的进行数据挖掘、复制或使用概要信息。

社区数据可包含非 IBM 运作的 Web 站点的链接。IBM 不对此类 Web 站点的内容、产品、资料或实践（包括隐私实践）负责。客户了解，访问社区数据可能会接触到某些第三方 Web 站点，客户可能会发现这些 Web 站点包含攻击性、不当或有异议的内容。

如果客户认为此数据包含不正确的或应当删除的个人信息，那么客户可以使用 X-Force IP Report 中的 Contribute 功能联系 IBM。

6. 覆盖条款

6.1 Cloudflare, Inc. 分包处理机构

以下条款优先于双方之间云服务条款的“数据安全和隐私原则”中的任何相反内容：此云服务使用 Cloudflare, Inc. 作为其内容分包处理机构之一。Cloudflare 以未加密形式处理内容，以优化云服务的交付。Cloudflare 作为 1 级服务提供商符合 PCI 标准，正在努力实现 ISO 27001 和 SOC 2 合规。（为清楚起见，云服务总体上并不符合 PCI 标准）。