IBM QRadar Advisor with Watson

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 QRadar Advisor with Watson 将认知分析功能扩展到 QRadar Security Platform，帮助客户和安全分析师调查和应对威胁。它利用 Watson for Cyber Security 的知识语料库，深入挖掘非结构化数据（包括安全网站、博客和研究报告等），并与本地安全事件关联。因此，它有助于揭示隐藏的威胁，自动获取洞察，从而进行响应和决策。QRadar Advisor with Watson 使安全分析师能够向 Watson 发送安全攻击信息，让 Watson 利用其包含成千上万个结构化和非结构化数据源的知识库，执行威胁发现操作，从而追溯到与原始安全攻击相关的威胁实体，例如恶意文件、可疑 IP 地址、恶意实体以及它们之间的关系。这在确定安全攻击是否与已知的恶意活动相关方面特别有效。如果事实果真如此，Watson 会提供与恶意软件有关的背景资料、被攻击的漏洞、威胁的范围（包括可能影响的其他端点）以及其他洞察。

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 QRadar Advisor with Watson

IBM QRadar Advisor with Watson 要求客户在本地内部部署环境或云环境中部署一个活动的 IBM QRadar，并在该部署上安装此云服务的支持软件，以便客户使用它的功能。当云服务按每秒事件数授权时，它包含对安全攻击查询数量的限制，也就是在客户授权范围内，客户可以按每天每秒每 100 个事件向云服务发送 1.5 个查询（向上取整为最接近的查询）。当云服务按托管虚拟服务器 (MVS) 授权时，它包含对安全攻击查询数量的限制，也就是在客户授权范围内，客户可以按照每天每 100 个 MVS 向云服务发送 15 个查询。在当天剩余时间内，对于发送的超出此限制的查询，优先级将会降低，且此云服务将不会进行处理。

1.1.2 IBM QRadar Advisor with Watson – Enterprise

IBM QRadar Advisor with Watson - Enterprise 最适用于大型安全运营中心 (SOC) 的部署，这类部署通常每秒处理超过二十五万个事件。客户必须在其单独购买的 IBM QRadar 部署中安装此云服务的支持软件，以访问此云服务的功能。IBM QRadar Advisor with Watson – 根据不依赖于客户的 IBM QRadar 部署规模的基于实例的计费标准提供。限制客户在任何给定时间在队列中最多进行 25 次查询。

1.1.3 IBM QRadar Advisor with Watson – Starter Pack

IBM QRadar Advisor with Watson – Starter Pack 面向 QRadar Advisor with Watson 的初次使用者。此云服务具有 QRadar Advisor with Watson 的完整功能，如以上第 1.1.1 节中所述，但是仅适用于客户第一次购买 QRadar Advisor with Watson，而不适用于续订。

1.2 可选服务

1.2.1 IBM QRadar Advisor with Watson – Test Environment

IBM QRadar Advisor with Watson – Test Environment 适用于希望为其内部测试环境部署云服务客户，并且仅可用于非生产测试目的。IBM QRadar Advisor with Watson – Test Environment 必须通过订购生产级云服务进行补充。

1.3 加速服务

1.3.1 IBM QRadar Advisor with Watson Advanced Services

对于此远程交付的订阅服务，IBM 将在一年时间内向客户提供最多五 (5) 天的以下任何咨询服务：

- 评估客户 SOC 流程，包括调查和/或事件响应流程；
- 重新评估参考集合响应；
- 调整高量级攻击的自动分析；

- 用例开发；
- 为 SOC 流程变更提供有关整合 QRadar Advisor with Watson 的建议；
- 提供有关如何最有效理解来自 QRadar Advisor with Watson 的数据并将其整合到客户现有流程中的指导意见；
- 提供相关 QRadar Advisor with Watson 主题的知识传授。

注：以下活动可根据客户 QRadar 部署状态整合到此服务中：

- 对客户 QRadar 部署执行运行状况检查；
- 对现有 QRadar 部署执行其他调优；
- 协助将其他日志源添加到客户 QRadar 部署中。

1.3.2 IBM QRadar Advisor with Watson 基本设置服务

此设置服务采用远程交付并包含四十 (40) 小时的专业服务，无论是否用尽了小时数（如果适用），这些服务都将自订购之日起 90 天后到期，除非另有说明。服务将包含一名指定的 IBM 服务项目经理，负责安排任何启动电话会议。

IBM 将执行以下部分或全部操作：

- 评估客户 SOC 流程，包括调查和/或事件响应流程；
- 在客户环境内实施 QRadar Advisor with Watson：
  - 安装 QRadar Advisor with Watson；
  - 将统一的属性映射到 QRadar Advisor with Watson；
  - 实施参考集合响应；
  - 调整高量级攻击的自动分析；
  - 用例指南；
  - 为 SOC 流程变更提供有关整合 QRadar Advisor with Watson 的建议。

1.3.3 IBM QRadar Advisor with Watson 快速设置服务

此设置服务适用于每秒事件数 (EPS) 小于 5,000 的客户。

对于此远程交付的服务，IBM 将在 90 天内向客户提供最多 16 小时的以下任何咨询服务（或服务组合）：

- QRadar Advisor with Watson 安装。
- QRadar Advisor with Watson 权限管理。
- QRadar Advisor with Watson 配置，可以包括：
  - 配置安全代理服务器；
  - 提交 X-Force Exchange 凭证；
  - 创建授权服务令牌；
  - 配置保留时间策略以存储分析结果；
  - 定制事件属性映射；
  - 导出参考集合；
  - 威胁情报映射；
  - 配置资产标识；
  - 使用情况优化。
- 自动攻击调查和结果（至少一个用例展示）。
- 使用关系图的洞察探究。

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=0B439290AB5011E6BE74C84817AAB206

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：

- 每秒事件 (EPS) 是指出现一次通过使用云服务处理或与使用云服务相关的特定 EPS。对于此云服务，每秒事件数量是指由客户的 IBM QRadar 部署收集和处理的每秒事件数量。
- 实例是对云服务的特定配置的每次访问。
- 互动是与云服务相关的专业或培训服务。
- 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 支持软件

云服务包含以下支持软件：

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

5.2 云服务的合法使用

云服务旨在帮助客户改进其安全环境和数据。对云服务的使用可能涉及不同的法律或法规，包括与隐私、数据保护、雇佣、电子通信和存储相关的法律法规。云服务只可出于合法目的、采用合法方式使用。客户同意按照规定使用云服务，并承担所有责任，遵守适用的法律、法规和政策。客户声明，自己将获取或已经获取合法使用云服务所需的任何同意书、权限或许可。

6. 覆盖条款

6.1 数据使用

以下条款优先于双方之间基本云服务条款的“内容和数据保护”部分中的任何相反内容：IBM 不会使用或披露客户使用云服务而产生的专属于客户的内容的结果（洞察）或以其他方式表明客户身份的结果。但是，IBM 将在提供云服务的过程中使用这些内容以及由这些内容生成的其他信息（洞察除外）来改进云服务。IBM 可能还会共享威胁标识和嵌入在内容中的其他安全信息，以进行威胁检测和实施保护。