IBM Resilient Incident Response Platform On Cloud

本“服务描述”描述 IBM 向客户提供的 Cloud Service。客户表示公司、公司授权用户和 Cloud Service 接收方。提供适用的“报价”和“权利证明”(PoE) 作为独立的交易文档。

1. Cloud Service

IBM Resilient Incident Response Platform on Cloud 提供动态行动计划（从恶意软件到 DDoS，以及丢失的设备）和通常应对事件的最佳实践。此知识库引导客户团队进行响应，可以为客户的独特操作流程配置。

事件响应团队可以直接在 IBM Resilient Incident Response Platform on Cloud 中进行响应管理和协作。与凭单系统和其他通用 IT 工具不同，IBM Resilient Incident Response Platform 完全可配置，并且专门针对事件响应而构建。近乎全面的分析、可定制仪表板以及强大的报告功能支持高管层访问重要信息。

IBM Resilient Incident Response Platform 专门针对各类规模以及复杂程度不同的组织而设计，并提供几种可单独订购的版本：

1.1 IBM Resilient Incident Response Platform Enterprise on Cloud

IBM Resilient Incident Response Platform Enterprise on Cloud 是 Cloud Service 解决方案，为主要组织的各类大型系统而设计。它为针对组织和事件类型的响应计划、管理和缓解奠定了基础。用户可以根据行业标准和最佳实践创建事件响应计划，并跟踪事件直至解决。Cloud Service 促进整个组织的中心协作，并且作为事件响应工作的一部分允许不同项目干系人承担他们的角色和任务。还可以进行事件模拟，帮助团队测试响应计划、识别间隔并优化响应进程。与各种外部威胁情报订阅源的内置集成可以自动执行事件和工件改进。Cloud Service 包含全局数据隐私违规通知法规知识库，帮助进一步制定事件响应计划。数据还可以从现有安全和 IT 系统中合成，以提供近乎实时的信息。无需定制开发，即可以在 Cloud Service 内自动执行、精简或调整各种任务。对于此服务，客户必须至少获取 1 份实例权利和 1 份授权用户权利。

1.2 IBM Resilient Incident Response Platform Standard on Cloud

IBM Resilient Incident Response Platform Standard on Cloud 是 Cloud Service 解决方案，旨在满足中小型组织的事件响应需求。它所提供的功能与 IBM Resilient Incident Response Platform Enterprise on Cloud 大致相同，但客户不得使用以下功能：隐私违规、自动化/编排、威胁情报订阅源、定制威胁订阅源和 LDAP 集成。对于此服务，客户必须至少获取 1 份实例权利和 1 份授权用户权利。

1.3 可选服务

1.3.1 IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud

IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud 是一个单独的 IBM Resilient Incident Response Platform 实例，客户仅可将其用于内部非生产活动，包括但不限于测试、性能调优、故障诊断、内部基准评测、登台质量评估活动和/或使用发布的应用程序编程接口开发内部使用的 Cloud Service 插件或扩展。

1.4 远程服务

以下远程服务可单独订购，并且无论是否用尽了小时数（如果适用），每项服务都将在购买九十 (90) 天后到期：

1.4.1 IBM Resilient Incident Response Platform Integration for Cloud

此服务产品提供集成服务，以使用预先开发的集成将 Cloud Service 连接到相关的安全与管理系统。每个服务项目将仅设置与一个系统的一个集成。此远程服务支持的集成设置列示如下：

- **与 QRadar 的集成**

  此集成将支持 QRadar 将违规行为作为新事件自动或手动推送到 Cloud Service。还包括说明、关闭事件与新违规事件数据的双向同步。

- **与 HP Arcsight 的集成**

  此集成允许 ArcSight 用户将 Arcsight 事件详细信息作为新事件手动或自动推送至 Cloud Service，或者为现有事件添加工件。

- **与 Splunk 的集成**

  此集成允许 Splunk 将警报作为事件自动推送至 Cloud Service。客户还可以在 Cloud Service Web 界面中门直接运行 Splunk 查询。

- **与 ServiceNow 的集成**

  此集成将允许 ServiceNow 用户在 Cloud Service 中创建事件，允许 Cloud Service 用户在 ServiceNow 中创建凭单。还可以在系统之间复制凭单或事件的更新。

- **与 JIRA 的集成**

  此集成支持 JIRA 用户基于 JIRA 凭单在 Cloud Service 中创建事件，支持 Cloud Service 用户在 JIRA 中创建凭单。还可以在系统之间复制凭单或事件的更新。

1.4.2 IBM Resilient Incident Response Platform Design Session for Cloud

此服务提供咨询性的服务项目，帮助优化客户的 Cloud Service 实例。IBM 顾问将与客户合作，针对最多三 (3) 种不同事件类型对客户的现有事件响应进程进行综合，根据当时行业最佳实践和 Cloud Service 功能对其进行优化，并就如何配置 Cloud Service 以实施此类进程向客户提供建议。

2. 安全描述

此 Cloud Service 遵循 http://www.ibm.com/cloud/data-security 中提供的针对 IBM SaaS 的 IBM 数据安全和隐私原则，以及本部分中提供的任何其他条款。对于 IBM 数据安全和隐私原则的任何更改都不会降低 Cloud Service 的安全性。

此 Cloud Service 并非旨在满足任何受管控内容（例如，个人信息或敏感的个人信息）的特定安全要求。客户负责确定在客户使用的与 Cloud Service 有关的内容类型方面，此 Cloud Service 是否符合客户需求。

3. 服务标准协议

IBM 按照 PoE 中的规定为 Cloud Service 提供了以下可用性服务级别协议 (SLA)。本 SLA 不构成保证。本 SLA 仅提供给客户，且只能应用于生产环境。

3.1 可用性积分

客户必须在首次发现事件影响 Cloud Service 可用性的 24 小时内，通过 IBM 技术支持帮助中心记录 1 级严重性支持凭单。客户必须为 IBM 的任何问题诊断和解决提供合理帮助。

必须在约定的月份结束后的三个工作日内提交支持凭单，对未能满足 SLA 提出索赔。针对有效 SLA 索赔的赔偿将基于 Cloud Service 的生产系统处理不可用的时间段（“停机时间”），以针对 Cloud Service 的将来发票的贷记金额的形式支付。停机时间从客户报告停机事件开始计算，到 Cloud Service 复原为止，其中不包括有关以下方面的时间：计划或宣布的维护停运；IBM 可控范围之外的停机原因；客户或第三方的内容或技术、设计或指令问题；不受支持的系统配置和平台或其他由客户引起的错误；或客户导致的安全事件或客户安全测试。IBM 会根据每个约定的月份内累积的可用 Cloud Service 适用最高的赔偿，如下表中所示。对任何“约定的月份”给与的赔偿总额不应超过年度 Cloud Service 费用的十二分之一 (1/12) 的百分之十。

3.2 服务级别

约定的月份内的 Cloud Service 的可用性

一个合同月期间的可用性	补偿 （受索赔的“约定的月份”的每月订购费用* 的百分比）
99.5%	2%
98%	5%
96%	10%

* 如果 Cloud Service 是从 IBM 业务合作伙伴处购买的，那么每月订购费用将基于受索赔的“约定的月份”期间有效的 Cloud Service 当时目录价格进行计算，适用折扣费率为 50%。IBM 将直接向客户应用折扣。

可用性以百分比表示，计算如下：一个合同月中的总分钟数减合同月总停机时间，除以该合同月的总分钟数。

示例：约定的月份内停机时间总计 500 分钟

30 天的“约定的月份”内总计 43,200 分钟 - 500 分钟停机时间 = 42700 分钟 ——————————————— 总时间 43,200 分钟	= 2% 可用性积分，在约定的月份内可用性 98.8%

4. 技术支持

通过电子邮件、在线论坛和在线问题报告系统提供 Cloud Service 技术支持。技术支持随附于 Cloud Service，不作为独立产品提供。技术支持于正常工作日美国东部标准时间早 9:00 点至晚 6:00 点（节假日除外）提供。

严重性	严重性定义	支持期间的响应时间目标
1	**关键业务影响/服务停止：** 业务关键功能无法运行或关键接口已故障。这通常适用于生产环境，并且表示无法访问服务对运营产生重大影响。这一情况需要立刻解决。	1 小时内
2	**严重业务影响：** 服务特性或服务功能在使用中受到严重限制，或者客户可能错过业务截止期限。	2 个工作小时内
3	**轻微业务影响：** 表明服务或功能还可使用，不会对运营产生关键影响。	4 个工作小时内
4	**最小业务影响：** 咨询或非技术请求。	1 个工作日内

5. 权利和计费信息

5.1 收费标准

Cloud Service 根据交易文档中指定的收费标准提供：

a. **实例** - 获取 Cloud Service 时所采用的一种计量单位。实例是对 Cloud Service 特定配置的访问。客户必须获取足够的权利，以涵盖客户的 PoE 或交易文档中所指定的评估期间可访问和使用的每个 Cloud Service 实例。

b. **授权用户** - 获取 Cloud Service 时所采用的一种计量单位。客户必须为每位唯一的“授权用户”取得单独且专有的权利，使其能够以任何方式，通过任何途径直接或间接地（例如，通过多路复用程序、设备或应用程序服务器）访问 Cloud Service。必须获取足够的权利，以涵盖客户 PoE 或交易文档中所指定的评估周期内有权访问 Cloud Service 的“授权用户”的数量。

c. **服务项目** - 获取服务时所采用的一种计量单位。服务项目包含与 Cloud Service 相关的专业服务和/或培训服务。必须获取足够的权利以涵盖每项服务项目。

5.2 盘盈费用

如果评估期间客户对 Cloud Service 的实际使用超出了 PoE 中指定的权利，那么将按照交易文档中的规定向客户收取盘盈费用。

5.3 远程服务费用

远程服务按服务项目购买，并且按交易文档中指定的价格收费。

6. 期限和续约选项

Cloud Service 期限自 IBM 通知客户可访问 PoE 中记录的 Cloud Service 之日算起。PoE 将指定 Cloud Service 是自动续订、在持续使用基础上继续，还是在期限结束时终止。

对于自动续订，除非客户在期限到期日期之前，至少提前 90 天发出不再续订的书面通知，否则将按照 PoE 中指定的期限对 Cloud Service 自动续订。

对于持续使用，在客户提前 90 天发出终止书面通知之前，Cloud Service 将以月为单位继续有效。Cloud Service 的有效期将于 90 天期限过后的日历月末终止。

7. 附加条款

7.1 一般条款

客户同意 IBM 可在宣传或市场营销中将客户公开为 Cloud Services 的订户。

7.2 合规性管理 Cloud Service

Cloud Service 可用于帮助客户满足合规性义务的要求，该义务可能基于法律、法规、标准或实践。客户承认并同意 Cloud Service 提供的任何指示、建议用法或指南并不构成法律、会计或其他专业意见，客户需要获取自己的法律顾问、会计或其他专家顾问建议。客户也同意客户自行负责确保客户及其活动、应用程序和系统遵守所有适用的法律、法规、标准和实践。使用 Cloud Service 并不保证遵守任何法律、法规、标准或实践。

7.3 Cloud Service 的合法使用

Cloud Service 旨在帮助客户改进其安全环境和数据。对 Cloud Service 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。Cloud Service 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 Cloud Service，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 Cloud Service 所需的任何同意书、权限或许可。

7.4 安全性数据

作为 Cloud Service（包括报告活动）的一部分，IBM 将准备并维护从 Cloud Service 收集的去标识化的信息和/或汇总信息（“安全性数据”）。“安全性数据”将不会识别客户或个人，以下 (d) 中提供内容除外。客户在此同意 IBM 只能出于以下目的使用和/或复制“安全性数据”：

a. 发布和/或分发“安全性数据”（例如，与网络安全相关的编译和/或分析中）；

b. 开发或增强产品或服务；

c. 开展内部研究或与第三方一起开展研究；以及

d. 合法共享已确认的第三方罪犯信息。

7.5 Cookies

客户了解并同意，在 Cloud Service 正常运行和支持过程中，IBM 可向客户（您的员工和承包商）通过跟踪和其他技术收集有关 Cloud Service 的使用情况的个人信息。IBM 公司以此收集 Cloud Service 的使用统计信息和有效性信息，旨在改善用户体验和/或定制与客户的交互。客户确认其将取得或已取得同意，允许 IBM 在遵守适用的法律的情况下，在 IBM、其他 IBM 公司及其分包商内部处理收集到的个人信息用于上述目的，无论我们和我们的分包商在何处开展业务。IBM 将履行客户的员工和承包商访问、更新、纠正或删除所收集的个人信息的请求。