IBM Application Security 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 Application Security on Cloud 提供单个场所以帮助客户发现各个应用程序的安全漏洞（例如，SQL 注入、跨站点脚本编制和数据泄漏）。服务包括各种类型的应用程序安全扫描技术，其中每个都用于识别此应用程序中的安全问题。

IBM Application Security on Cloud 提供以下功能：

- 扫描移动应用程序以查找安全漏洞。通过交互式（白盒）安全分析技术来完成。
- 扫描生产或预生产面向公众或专用网络上的 Web 站点以查找安全漏洞。通过动态（黑盒）安全分析技术来完成。
- 扫描 Web 和桌面应用程序中的数据流以查找安全漏洞。通过静态（白盒）安全分析技术来完成。
- 详细的安全漏洞报告，其中包含发现以及开发人员可采用的补救步骤的高级摘要。
- 集成各种 DevOps 平台。

1.1 IBM Application Analyzer

IBM Application Analyzer 可根据应用实例或工作量（扫描量）进行订购，或作为完整的实例允许以下类型的扫描：

- Dynamic Analyzer – 通过 DAST 技术测试预生产或生产网站
- Mobile Analyzer – 通过 IAST 技术测试 iOS 或 Android 二进制文件
- Static Analyzer – 通过 SAST 技术测试字节或源代码的数据流

1.2 设置服务

IBM Application Security on Cloud Consulting Services 是用于 Application Analyzer 的产品化设置服务。该服务通过 IBM 顾问在测试和管理应用风险方面提供指导和帮助。IBM Application Security on Cloud Consulting Services 可作为服务项目块进行购买，并根据以下规定的数量进行消耗，以便请求并使用以下特定服务：

a. **快速启动** [使用一个 (1) 服务项目单元]

“快速启动”服务为使用 Application Security on Cloud 测试和风险管理功能提供专业知识和指导。 客户确认成功登录到 Application Security on Cloud 门户网站后，IBM 将开 展一场最长两 (2) 小时的网络会议，并且两位 (2) 积极参与者将提供有关基础 AppSec on Cloud 服务配置和功能的指导，包括扫描类型、运行扫描、审查报告和安装相关的工具和插件。完成 (a) 客户教育研讨会、(b) 适用的工具和插件的安装并 (c) 帮助客户设置并运行客户的第一次扫描后，“快速启动”服务便已完成。

b. **评估审查** [使用两个 (2) 服务项目单元]

“评估审查”服务可为审查测试结果提供帮助，包括了解和优先考虑应用中的漏洞修复。IBM 将开展一场最长一 (1) 小时的会议，并且两位 (2) 积极参与者将提供有关发现的漏洞、应用的整体安全风险以及针对发现的应用安全漏洞进行的详细讨论的概述，其中包括 (1) 如何测试漏洞、(2) 如何检测漏洞、(3) 每个漏洞的风险是什么，并 (4) 提供一般的修复建议，以帮助修复该漏洞。该审查将完全基于测试结果，并且并非审查源代码自身。客户将审查测试结果，并在网络会议之前，将与 IBM 确认测试结果的审查。完成网络会议后，“评估审查”服务便已完成。

c. **为我扫描**[使用四个 (4) 服务项目单元]

“为我扫描”服务将提供一位 IBM 应用安全专家，帮助您配置并运行扫描、验证结果并进行简报以审查结果。客户将允许一位 IBM 顾问访问其 ASoC 环境，来配置并运行扫描、验证结果、提供有关修复优先次序的建议并对结果进行简报。IBM 将开展一场最长一 (1) 小时的会议，并且两位 (2) 积极参与

者将提供有关发现的漏洞、应用的整体安全风险以及针对发现的应用安全漏洞进行的详细讨论的概述，其中包括 (1) 如何测试漏洞、(2) 如何检测漏洞、(3) 每个漏洞的风险是什么，并 (4) 提供一般的修复建议，以帮助修复该漏洞。如果客户要求，那么初始扫描的 30 天后，IBM 将使用原先的扫描配置重新进行扫描，来验证安全修补程序，而不是测试新的功能、验证结果并向客户提供报告。完成网络会议并审查初始的扫描结果后，或（如适用）完成客户要求的重新扫描并将重新扫描报告传递给客户后，“为我扫描”服务便会完成。

d. **按需顾问** [使用七个 (7) 服务项目单元]

“按需顾问”服务提供多达二十 (20) 小时的 IBM 顾问时间，可用于与 Cloud Service 相关的活动。IBM 顾问将协助应用安全特定主题，包括但不限于，程序管理、安全性测试优先级划分、补救策略、源代码分析和源代码修复。IBM 将与客户合作，来了解并创建符合特定客户要求的项目时间表，包括项目目标、相关技术、所需的时间线、预期的可交付成果以及 “按需顾问”服务项目的预计数量。客户必须提供对执行服务所需的必要应用、系统和文档的访问。在最长 20 个小时的安全专业知识已经执行后和/或项目时间表和/或其中定义的记录的可交付成果提供给客户后，“按需顾问”服务便已完成。

e. **应用渗透测试**

三个选项：

(1) **合规性/入门级应用渗透测试**，其中包括最长四十 (40) 小时的咨询时间，专注于单步逻辑缺陷以及注入缺陷的简化版本。使用十五个 (15) 服务项目单元。

(2) **标准应用渗透测试**，其中包括最长六十 (60) 小时的咨询时间，并扩展了关注领域，包括多步骤工作流程中的逻辑缺陷、注入缺陷的复杂版本和复杂数据类型的分析。使用二十一个 (21) 服务项目单元。

(3) **高级应用渗透测试**

提供最长八十 (80) 小时的咨询时间，并扩展了关注领域，包括编译后可执行文件的反向工程、定制网络协议的剖析、对公开可用的库和框架的深入分析。使用二十七个 (27) 服务项目单元。

应用渗透测试服务提供 IBM 资源来测试并开发应用、交付测试报告并执行简要报告，以解释测试结果和相关的风险。

IBM 将开始一 (1) 小时的项目启动会，两位 (2) 活动参与者将审查客户的环境和组织，包括应用平台、体系架构、框架、支持基础架构、与应用相关的已知安全问题或顾虑、初步测试时间表和紧急联络计划。

IBM 将进行应用渗透测试，包括但不限于：识别常见漏洞（如 SQL 注入和跨站点脚本）、评估现有安全控件的优点和缺点（如输入验证、身份验证和授权）、检查业务逻辑是否正确执行、验证安全协议的正确使用、识别会话处理缺陷并验证有关登录、密码恢复、密码策略以及其他用户管理功能的适当安全控件。测试结果将在应用渗透测试报告中记录。IBM 将开展一场一 (1) 小时的简要报告网络会议。在用完分配的咨询时间、开展网络会议并将最终的应用渗透测试报告提供给客户后，应用渗透测试服务便已完成。

1.2.1 设置服务责任

IBM 应：

- 通过客户购买的服务项目单元并根据客户订单条款提供设置服务；并且
- 当 1.2 节中描述的完成标准完成时，客户便完成了设置服务。

客户同意：

- 负责承担与客户在合同期内提出的所有服务项目请求相关的所有费用；
- 并承认，购买的服务项目单元必须在初始的合同期限内使用，如果合同到期时还未使用，那么将会过期；
- 在订购结束日期之前至少 30 天内，为所有设置服务发出正式请求。

在执行任何设置服务时，IBM 可向客户要求信息及合理的合作。如果客户未能及时地提供所需的信息或合作，那么可能导致根据服务来对服务项目单元收费，或导致适用服务的性能延迟，这一切都由 IBM 决定。

为了让 IBM 精确地进行测试，客户同意遵照 IBM 的指示，为测试阶段准备并维护环境。

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。

IBM 不作为受联邦通信委员会 ("FCC") 或国家监管机构 ("State Regulators") 管控的服务的提供商经营业务，也不打算提供任何受 FCC 或 State Regulator 管控的服务。如果 FCC 或任何 State Regulator 对 IBM 在本协议中提供的任何服务强加监管要求或义务，IBM 可以：(a) 由客户付费对产品进行修改、替换或使用代替产品，和/或 (b) 更改为客户提供此类服务的方式，以避免适用此类需求或义务（例如，通过作为客户的代理来从第三方承运商获得此类服务）。

3. 技术支持

在订购周期内，当 IBM 通知客户可以访问 Cloud Service 之后，将通过在线论坛提供技术支持，并作为客户产生“按使用付费”费用期间的标准支持。在此 Cloud Service 中，客户可以提交支持凭单或打开交谈会话以获取支持。IBM 将提供《IBM 软件即服务支持手册》，其中提供了技术支持联系信息以及其他信息和流程。

严重性	严重性定义	响应时间目标	响应时间覆盖
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	24x7 方式
2	**严重业务影响：** 服务的一项业务功能或特性的使用严重受限，或您正面临不能按时完成业务任务的危险。	2 个工作小时内	周一到周五的工作时间
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	周一到周五的工作时间
4	**最小业务影响：** 咨询或非技术请求	1 个工作日内	周一到周五的工作时间

3.1 访问客户数据

IBM 将出于诊断服务问题和便于服务扫描客户的应用程序的目的而访问客户数据。IBM 将仅出于纠正缺陷或为 IBM 产品或服务提供支持之目的访问数据。

4. 权利和计费信息

4.1 收费标准

Cloud Service 根据交易文档中指定的收费标准提供：

a. **作业** - 获取 Cloud Service 时所采用的一种计量单位。“作业”是 Cloud Service 内部不能进一步分割的对象，表示包含其所有子过程的计算过程。客户必须获得足够的权利，以涵盖客户的 PoE 或交易文档中指定的评估期间 Cloud Service 所处理或管理的作业总数。

b. **应用程序实例** - 获取 Cloud Service 时所采用的一种计量单位。连接到 Cloud Service 的应用程序的每一个实例都需要一份应用程序实例授权。如果应用程序包含多个组件，每个组件都为不同的目的和/或用户群提供服务，并且每个组件都可连接到 Cloud Service 或由 Cloud Service 进行管理，那么每个此类组件都被视为一个单独的应用程序。此外，应用程序的测试、开发、登台和生产环境均被认为是应用程序的单独实例，每个实例都必须获得一份权利。单一环境中的多个应用程序实例中的每一个均被认为是应用程序的单独实例，每个实例都必须获得一份权利。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连接到 Cloud Service 的应用程序实例数。

对于此 Cloud Service，应用程序实例是指单个应用程序的连续扫描，进一步定义如下所示：

- 针对动态测试：可通过公共或专有的 URL 进行访问的网站。每个应用实例在单个域中有权使用包含多达 5,000 个页面的站点。
- 针对静态测试：为单个可执行环境构建的代码单元。每个应用实例可以扫描高达 1,000,000 行的代码单元。
- 针对移动测试：可在移动设备上执行的二进制代码单元。每个不同的移动平台（如 iOS 和 Android）构成不同的应用实例。

c. **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，以涵盖权利证明 (PoE) 或交易文档中指定的评估期间可访问和使用的每个 Cloud Service 实例。

对于每份实例权利，执行的作业或应用程序实例（连接的应用程序）的数量并没有限制，但是，在任意给定时间内，同时运行的作业不得超过 30 个。

d. **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。

4.2 未满一个月的收费标准

根据交易文档的规定，使用未满一个月将按比例收取费用。

4.3 盘盈费用

如果评估期间 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。

4.4 设置费用

按照交易文档中的规定向客户收取设置费用。

5. 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。

对于自动续约，除非客户在期限到期日期之前，至少提前 30 天发出不再续约的书面通知，否则将按照 PoE 中指定的期限对 Cloud Service 自动续约。

对于持续使用，在客户提前 30 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 30 天期限过后的日历月末终止。

6. 附加条款

安全扫描可能无法识别应用中的所有安全隐患，并且它们也并不是被设计用于需要故障安全操作的危险环境，包括但不限于，飞机导航、空中交通管制系统、武器系统、生命支持系统、核设施或者由于无法识别安全隐患而可能导致死亡、人身伤害或财产损失的任何其他应用。安全扫描不保证运行过程中不会出现中断或错误。

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。Cloud Service 提供的任何指示、建议用法或指南并未包含法律、财务或其他专业建议，提醒客户获取自己的法律顾问或其他专家顾问。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。使用此 Cloud Service 并不保证遵守任何法律、法规、标准或实践。

Cloud Service 在 Web 站点上执行入侵性和非入侵性测试，Web 或移动应用程序客户选择进行扫描。某些法律禁止在未经授权的情况下尝试进入或访问计算机系统。客户授权 IBM 执行此处所述的服务，并承认服务有权访问客户的计算机系统。 如果认为对执行服务有必要， IBM 可向第三方进行授权。

测试会带来某些固有风险，包括但不限于以下：

a. 客户的计算机系统在测试状态下运行应用程序时可能暂挂或崩溃，导致系统暂时不可用或数据丢失；

b. 客户系统的性能和吞吐量以及相关联的路由器和防火墙的性能和吞吐量可能在测试期间暂时降级；

c. 可能生成过多日志消息，导致耗费过多的日志文件磁盘空间；

d. 探测漏洞可能导致数据被更改或删除；

e. 入侵检测系统可能触发警报；

f. 所测试 Web 应用程序的电子邮件功能可能触发电子邮件；并且

g. Cloud Service 可能在查找事件时阻断受监控网络的流量。

由 IBM 提供且与接受测试的网站或应用相关的任何服务级别协议的权利或补救措施将在任何测试活动中被放弃。

为防止客户将所测试应用程序的已认证登录凭证输入 Cloud Service 中，客户只能针对测试帐户（而不是生产用户）输入此类凭证。使用生产用户凭证可能导致个人数据通过 Cloud Service 传输。

可以配置 Cloud Service 以扫描生产 Web 应用程序。当客户将扫描类型设置为“生产”时，服务旨在以降低上述风险的方式执行扫描；但是，在特定情况下，Cloud Service 可能会导致测试的生产站点和基础架构性能下降或不稳定。对于使用 Cloud Service 扫描时生产站点的适用性，IBM 不作任何声明或保证。

客户需自行承担责任，决定 Cloud Service 是否适用于客户的 Web 站点、Web 应用程序、移动应用程序或技术环境及其安全性。

Cloud Service 旨在识别移动和 Web 应用程序以及 Web 服务中的各种潜在安全和合规性问题。它不会测试所有漏洞或合规性风险，也不能阻止安全攻击。安全威胁、法规和标准不断变化，Cloud Service 可能不会反应所有此类变化。客户需自行承担其 Web 应用程序、系统和员工的安全性和合规性责任，并采取任何补救措施。客户自行决定是否使用 Cloud Service 提供的任何信息。

某些法律禁止在未经授权的情况下尝试进入或访问计算机系统。客户需负责确保客户不使用 Cloud Service 扫描任何客户所有及客户有权扫描的 Web 站点和/或应用程序之外的 Web 站点和/或应用程序。

为明确起见，Cloud Service 协议的“数据保护”部分中描述的客户内容也被认为包含 IBM 在应用渗透测试期间可访问的数据。

6.1 第三方拥有的系统

针对第三方拥有的且将成为测试对象的系统（该规定的目的包括但不限于应用和 IP 地址），客户同意：

a. 在 IBM 对第三方系统进行测试之前，客户将获得来自每个系统的所有者的签名信件，该信件授权 IBM 在该系统上提供服务并表明所有者接受“Permission to Perform Testing”部分中规定的条件，并且客户将为 IBM 提供此授权的副本；

b. 全权负责 IBM 对系统拥有者进行远程测试时传达在这些系统上识别的任何风险、攻击和漏洞；并

c. 在 IBM 认为必要时，安排并促进系统所有者与 IBM 之间的信息交流。

客户同意：

- 只要作为测试对象的任何系统的所有权有所改变，都将立即通知 IBM。
- 未经 IBM 事先书面同意，不会对外披露交付件，也不会披露 IBM 为客户执行服务的事实；并且
- 全额赔偿 IBM 由于客户未能遵守“第三方拥有的系统”部分的要求所引起的第三方索赔而为 IBM 带来的任何损失或责任；以及任何由于以下原因针对 IBM 或 IBM 的分包商或代理的第三方传票或索赔 (a) 对作为测试对象的系统测试安全风险、敞口和漏洞，(b) 为客户提供此测试的结果或(c) 客户对此结果的使用或披露。

6.2 Cookies

客户了解并同意，作为 Cloud Service 正常运行和支持的一部分，IBM 可向客户（客户的员工和承包商）通过跟踪等技术收集有关 Cloud Service 使用的个人信息。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。

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（称为“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。

6.3 支持软件

此 Cloud Service 包括支持软件，只能在 Cloud Service 期限内与客户对 Cloud Service 的使用相关联的情况下使用该软件。