黑产对抗实验室基础建设项目技术需求书

一、项目背景和目标

1、项目背景

目前集团已逐步建立起风控防御体系和威胁情报系统，在事中和事后两个环节起到一定的防御效果，但是还存在一定问题，在面对黑产攻击手段和技术的动态进化，我们无法快速、自动、客观、全面地模拟真实黑产攻击，评估业务风险。因此，需要我们建设一套业务安全模拟黑产对抗平台，预判趋势，提前布控，通过平台统一调度黑产工具，更真实的模拟黑产攻击行为，快速识别业务全链路的潜在风险点，提高集团及子公司相应业务线业务安全的风险发现率。同时让业务、风控、情报有效的衔接、联动，以攻促防，大力提升业务安全的精准防护能力。

2、建设目标

黑产对抗实验室基础建设项目目标是构建一套界面可视化、评估高效的业务安全专项（蓝军）测评平台，通过模拟黑产攻击，以实现对业务的风险测评、风控能力客观评价、作弊线索复现、能力开放为关键目标，将黑产行业内主流的黑产攻击工具、环境、物料统一集成，统一调度，灵活安装部署，从而构建丰富的业务安全测评能力。具体实现三个方面的核心测评能力：

(1) 通过模拟主流互联网黑产行为，针对众多业务场景发起攻击测评，实现对公司内部应用开发流程和集团业务中存在的风险进行探测，以攻促防，推动业务提升安全防护意识；针对未接入业务风控系统的业务，可以通过直观的黑产攻击行为，引导推动业务接入风控系统，实现在线防护；

(2) 建立起与风控系统的攻防测评，对于线上风险识别策略、模型的防护效果做客观的评价，实时掌握线上防护效果；并借助风控蓝军测评能力，对于已采

购、即将采购的各类风控工具发起第三方测评，对于各类风控工具的服务效果做出客观评价，保障公司业务安全风控能力处于领先的地位；

(3) 实现对于威胁情报系统的相关能力评估，如情报数据的覆盖，并凭借蓝军平台的风险管理能力，快速实现对于情报系统收集的作弊线索进行复现，推动风控系统的策略升级，并通过将情报线索推送至各个产品线，达到情报线索的效益最大化。

二、项目采购内容

(1) 采购一套业务安全蓝军测评软件系统，可以满足集团常规业务场景的风险评测、业务安全风控工具、情报平台及攻防演练场景需求，包含软件产品的 1 年免费维保。

(2) 提供满足蓝军测评的常规硬件资源和基础对抗资源，如硬件设备资源、数据类资源、账号资源，以及常见黑产攻击工具和系统软件等。

(3) 提供若干集团业务场景攻防演练现场支持，提前发现业务漏洞，满足采购方常规场景的风险测评要求。

三、黑产对抗实验室软件产品需求

3.1 软件产品功能需求

1. 风控工具评测要求

提供业务安全风控工具的评测能力，对现有风控能力、风控工具的防护效果进行客观的有效评估，跟进线上防护效果，主要包含风险感知、设备指纹、接口防护等风控工具。针对每一项评测，需详细说明评测目标、评测要素、评测过程，并可以输出详细评测报告。

（1）支持风险感知能力测评，评测风控系统对虚假设备、虚假请求、风险应用、

风险环境、风险网络风险感知能力的准确率、实效性及覆盖率。

（2）支持设备指纹测评，针对各业务系统在应用卸载重装、跨 APP 应用打通、设备信息篡改、一键改机、一键刷机、手工重置设备、手工克隆设备、设备自动重置或克隆等不同情况下进行潜在的设备指纹稳定性和唯一性的风险评测。

（3）支持接口防护评测，需要满足在重放攻击、逻辑绕过、参数篡改和批量请求 4 个维度进行安全风险评测。

2. 业务安全评测要求

提供公司业务安全常规业务场景的评测能力，需满足但不限于对账号安全、营销业务安全、交易安全、支付安全的全方位评测，支持模拟组合攻击，针对每一项评测，均需详细说明评测目标、评测要素、评测过程，并可以输出详细评测报告。详细要求如下：

(1) 支持账号安全评测，实现对批量注册、登录保护场景等评测维度的评测：

(2) 支持营销业务安全评测，满足针对常规营销活动，如新用户奖励、签到积分、秒杀活动、拉票活动、助力活动、转盘抽奖等进行有效的风险评测，重点评测业务系统营销活动是否接入基础风控工具策略，或接入的风控策略是否有效。

3. 情报系统中情报信息评测要求

支持对威胁情报数据和线索类情报进行相关安全风险评测，威胁类情报主要是手机号、IP 和黑产工具，线索类情报主要包括业务接口漏洞，企业攻击舆情、最新作弊方法、攻击工具等。针对每一项评测，均需详细说明评测目标、评测要素、评测过程，并可以输出详细评测报告。详细要求如下：

（1） 支持对情报数据评测

1) 风险号码覆盖评测：针对情报系统对流通风险号码的覆盖情况进行评测，包括接码平台等号码来源；

2) 风险 IP 覆盖度评测：针对情报系统对流通风险 IP 的覆盖情况进行评测，包括第三方代理 IP 等风险 IP 来源；

（2） 支持对作弊线索复现

1) 复现移动端工具作弊：能够复现情报数据中的移动端黑灰产工具作弊线索，评测业务系统是否存在对应漏洞，以及是否接入了相应的风控策略，能否识别该作弊工具；

2) 复现基础接口漏洞：能够复现情报数据中的黑灰产作弊线索，评测业务接口是否存在对应漏洞，以及是否接入了相应的风控策略。包括数据泄露、可篡改参数等漏洞；

3) 复现业务逻辑漏洞：能够复现情报数据中的业务逻辑漏洞：包括重复订单、越权访问、流程绕过等逻辑漏洞。

4. 对抗引擎管理要求

平台对于业务风险测评、风控效果和风险复现，要求如下：

1) 评测任务调度：支持使用云手机、真机、模拟器进行风险环境构造，根据业务场景需要批量调度发起攻击测试。

2) 风控工具检测引擎：实现对于已经采购、建立的风控系统中所用到的各种风控工具，如风险环境检测、设备指纹、接口保护四种常见的风控工具进行客观测评，有效评估、跟进线上防护效果。

3) 场景化业务安全测评引擎：支持对各个业务场景做全方位测评，如账号安全、营销活动等关键场景，模拟其产组合攻击，可以对风控系统防护效果、风控策略做测评，检测业务中存在的安全漏洞。

4) 情报测评引擎：实现对情报数据覆盖的测评、对于收集到的作弊线索快速支持复现，并快速推广至全场景测评，确保风险快速识别防护。

5. 平台资源管理要求

(1) 设备资源：需要满足单不限于将真机、模拟器、以及云手机三种设备类型的统一集成，实现各类设备的平台实时渲染，单点/群控操作，并能统一对设备信息、应用、文件、批量操作等多种管理能力；

(2) 账号资源：需要包含接码平台、打码平台、评测账号、风险号码对接等，为测评能力提供所需的号码物料；

(3) 网络资源：需要整合通用代理 IP、VPN、海外 IP 等，为后续测评能力提供风险网络资源；

(4) 评测工具：支持包含黑产工具管理、内容检测管理及逆向工具管理，将黑产主流的作弊攻击、作弊软件等风险环境统一整合，实现众多风险环境在诸多设备上灵活安装构造。

6. 可视化控制台管理

支持一站式可视化控制台管理页面，为蓝军攻防人员、业务线 QA 等用户提供包含总览、业务安全测评、风控工具测评、威胁情报测评、平台资源管理、系统管理、权限管理等在内的丰富的平台管理能力，提高平台使用效率。

（1） 业务风险看板

提供全局概览，以及各产品业务线各业务场景的的漏洞分布和汇总情况。提供账户下创建的各类测评任务，可以统计分析出其攻击成本、攻击收入，计算黑产 ROI，同时展示该测评任务的整体攻击路径。

（2） 蓝军武器库管理

蓝军武器库管理，是建立在群控设备、云手机、真机基础上，通过平台能力统一整合各种黑产作弊工具，为后续各种蓝军攻击测评用例提供丰富的风险环境，同时可以根据威胁情报收集整理的各种黑产，实现动态快速扩展、更新、升级作弊工具、软件、脚本等攻击武器，同时要求初始武器库可以覆盖黑产作弊攻击 90%以上的攻击手段。

（3） 测评用例库管理

要求基于蓝军武器库所提供的作弊工具，结合业务场景即可快速构建各种攻击用例，并且将典型的用例进行复用，提高测评效率。

（4） 业务风险评测管理

要求支持创建风险评测任务及历史评测任务管理，支持手动攻击任务和自动攻击任务两种。根据当前移动攻击方案，在攻击完成后，系统可以自动计算此次攻击消耗的成本，并生成任务报告，并支持历史报告的切换对比功能，用户在完成测评任务后，可以针对当前测评任务中所用到的各类攻击工具的效果进行效果反馈。

（5） 风控工具评测管理

支持风险识别评测管理，可以展示当前系统已经创建的风险识别测评任务列表，可以直观看到当前任务的执行状态，可以生成测评报告。支持设备指纹评估管理，支持提供改机器工具、系统升级、参数变更、网络截取、设备注入等方式

修改设备指纹，可以实现快速对于设备指纹效果进行验证。

（6） 风控查询管理

为了有效评估测评业务对于各种风险情况是否有效识别、拦截，实验室可以支持与风控系统进行打通，以关键 key 进行关联，支持通过业务名称、攻击场景、测评类型等进行快速筛选，以列表的形式快速判断风控系统识别效果。

（7） 情报系统评估管理

支持情报测评任务列表展示，需要展示情报评测任务相关信息。支持新建情报评测任务，并在任务结束后生成评测报告，除包含基本任务信息外，提供可直接下载测评详情的功能，并直接以图表形式直观展示当前数据的覆盖率。

（8） 设备管理功能

可以实现对于实验室所使用的三种设备进行统一管理，包括云手机、模拟器和真机，同时可以实现快速设备添加，统一管理、配置、调试，为后续攻击测评提供设备支持。具体管理内容包括设备列表管理、当前账号下的可用设备情况、设备详情、设备风险管理、设备应用管理、文件管理，远程控制、设备添加等。

（9） 风险管理

要求预先内置 10-15 种风险类型，展示已添加风险列表，支持编辑/添加风险类型，支持调试风险、权限异常、改机工具、位置篡改、群控特征、风险网络等 6 大类风险，支持将风险项移除/同步至武器库。

（10） 资源管理

在测评过程中用到的号码、文件、脚本等资源均由该模块集中管理维护，为了让用户对资源类型有清晰的感知，黑产对抗实验室可以支持对文件资源、数据资源以及平台资源的管理。

（11） 系统管理

支持角色管理，可以快赋能公司内部各个业务线产品角色、QA、研发人员使用，在平台内，可以灵活创建各种用户角色、角色功能权限以及设备资源分配。支持用户管理，可以灵活为业务线人员快速开通平台权限，按照平台教程使用该对抗平台，执行基础的业务场景攻击，自助进行各种作弊能力的识别测试。

（12） 平台使用教程

需要提供各种攻击测评示例的视频教程等培训内容，从而快速赋能到各个业务线，降低安全部门人员成本、提升攻击测评效率。

3.2 产品非功能指标

1.性能指标

(1) 支持设备规模：常规企业带宽资源下，系统最高可支持数千台设备接入（含真机、模拟器、云手机）。

(2) 性能要求：一次攻防演练的周期：天级；常规企业带宽资源下，单台服务器支持 100 台设备同时发起任务。

(3) 系统响应时间：服务类接口平均响应在 200ms 以内。

2.安全性

(1) 满足系统可靠性要求，系统健壮性强，合理处理系统运行过程中出现的各种异常情况，如：人为操作错误、输入非法数据、硬件设备失败等，系统应该能正确的处理，恰当的回避。

(2) 确保源代码安全，无重大攻击漏洞。保证传输过程数据安全性、完整性、可用性。

(3) 满足审计合规要求：业务操作过程痕迹保留，可追溯、可审计，特别针对攻击实战各个环节资源、攻击行为的记录，系统能够保存操作记录，满足系统审查和事务处理。

3.技术架构

(1) 系统主要使用主流开发语言、主流开源技术框架及中间件，保证系统技术体系的先进性。

(2) 系统采用微服务方式开发，使用容器化技术使用支持 docker/k8s 进行部署发布，便于运维管理。

(3) 系统使用主流的通讯方式和报文格式提供标准且安全的系统接口，支持与已有系统进行对接。

(4) 系统支持高可用方式进行集群部署。

3.3 集成与定制化开发需求

定制化开发服务需要供应商按照采购方功能需求进行开发，主要满足如下功能点：

(1) 支持与采购方现有风控系统的打通对接。

(2) 对接统一认证平台，支持与采购方统一认证平台对接，为采购平台提供密码、用户信息、账号的管理。

(3) 支持接口定制化开发需求，软件产品的组件接口需要充分暴漏并提供拓展、更换支持，便于采购方对每个模块进行定制化开发和测试工作。

四、黑产对抗实验室硬件及对抗资源需求

提供软件系统配套的硬件和平台攻击软件资源，主要涉及到云手机、真机、路由等固定资产资源，以及接码打码、IP 等攻击软件资源。

4.1 硬件固定资产资源需求清单

序号	设备类型	设备数量	用途说明
1	云手机虚拟池	2（最低）	云手机 ARM 云服务器或者微型服务器(2*6 个云手机)
2	手机	7	常规安卓中高配手机，华为、小米等
3	手机	3	iPhone 手机
4	手机架	1（按需）	放置手机设备
5	智能电源	1（按需）	供手机使用，防止充爆
6	路由	1（按需）	企业级无线路由（供真机网络接入）
7	交换机	1（按需）	连接中控机和蓝军设备（真机、模拟器、云手机微服务器）

4.2 平台配套黑产软件及资源需求清单

序号	软件名称	用途	技术规格
1	精灵代理	代理 IP	最新版，注: 易变化，需定期购买更换
2	抹机王	改机	最新版
3	xx 改机	改机	最新版
4	雷电模拟器	虚拟设备	最新版
5	逍遥模拟器	虚拟设备	最新版
6	接码平台	风险号码 注册/登录	最新版 注：易倒闭，需定期购买新平台
7	Auto.js	自动化操作	最新版

8	Xposed	改机	最新版
9	Magisk	Hook 框架	最新版
10	按键精灵	虚拟点击	最新版
11	多开应用	虚拟设备	最新版
12	Root 工具	提取 Root 权限	稳定版
13	打码平台	完成图片验证码识别的	最新版
14	秒拨 ip	提供秒拨 IP 服务，获取 IPv4 和 IPV6 资源	最新版
15	国内和国外动态 ip	代理 IP 池	最新版

注：如上为主要资源清单，需要根据黑产最新攻击形式动态增加，需提供一年的满足重点业务线攻击测试调用的量。

五、项目实施要求

1.团队配置

(1) 要求现场开发团队有互联网黑产对抗相关系统项目工作经验，核心成员包括：项目经理、产品经理、技术架构师、开发工程师、业务安全专项测试工程师、运维工程师、黑产对抗攻击专家。

(2) 项目经理具有国内互联网黑产对抗项目开发实施 5 年以上经验。

(3) 项目组产品经理至少 1 人，且具有 5 年以上互联网黑产对抗项目产品设计经验。

(4) 项目组技术架构师至少 1 人，且具有 7 年以上互联网黑产对抗项目系统架构和设计经验。

(5) 项目组开发工程师至少 3 人，且具有 3 年以上互联网黑产对抗项目实施经验。

(6) 项目组黑产对抗攻击专家至少 2 人，且具有 5 年以上互联网黑产对抗项目建模经验。

(7) 项目组成员的资质标准，由采购方评审时对人员资质标准进行核定，要求项目组人员的稳定，如需人员变更，供应商必须提供项目组成员的完整个人材料，并经采购方的确认后才能变更。

2.实施周期

项目建设实施周期预计为 3 个月，完成产品部署及定制化开发、功能测试，UAT 测试至 Bug 修复至项目投产，以及业务技术培训，具体实施进度最终按照甲方合同约定的时间计划表推进。

3.验收要求

(1) 按适合采购方测试生产部署环境的要求完成私有化部署。

(2) 完成采购方软件需求完成功能开发和测试，并通过采购方测试。

(3) 完成采购方要求硬件需求进行部署，并与软件系统完成对接，实现软硬件功能的整合。

(4) 完成系统管理员、开发人员、运维人员、业务安全专项测试人员、风控人员等相关培训工作。

(5) 验收方式将采用甲方项目负责人以邮件确认方式完成项目验收。

4.项目管理及规范要求

实施团队应遵守《泰康项目管理制度》,监督项目进度，保证项目质量，及时汇报项目风险，确保项目按计划完成。要求投标人制定完善的项目沟通计划，包括周例会、月例会、阶段性评审会等。要求投标人做好项目进度及风险管理，及时同步项目进展及计划安排，保证项目按计划顺利完成。

六、维保服务要求

1.维保时间周期

供应商提供本项目软件产品及定制化开发部分一年期维保服务，维保服务自软件产品及定制化开发部分全部验收完毕并稳定运行一个月，双方签署《验收报告》之日起计算。

2.维保要求

(1) 提供定期更新和版本升级服务。每季度巡检一次，公司如有临时活动要求，需提供现场技术支持和保障服务。

(2) 提供 7*24 小时现场或远程技术支持服务和咨询服务，具备完善的系统应急方案，对不同级别的突发事件提供及时有效的应对措施（包括远程和现场支持）。

七、知识转移要求

1.项目交付物要求

(1) 提供业务需求、技术需求文档，包括但不限于《需求规格说明书》、《详细设计说明书》等。

(2) 提供产品测试相关文档，包括但不限于《测试方案》、《集成测试报告》、《UAT 测试报告》等。

(3) 提供项目管理类文档，包括但不限于《项目实施里程碑计划》、《关键会议纪要》、《项目总结报告》、《项目验收报告》等报告。

(4) 按照项目软件产品要求交付进行软件交付，参考第三章。

(5) 按照采购要求进行硬件固定资产资源和消耗品资源的交付，参考第四章。

2.培训方案

(1) 提供完善的系统使用和维护培训，提供项目涉及的产品、技术、运维等文档，每年至少提供 2 次现场培训，并提供相应的培训教材。

(2) 要求驻场提供完整的业务安全攻击测试指导，包括对业务安全专项测试人员的专业攻击测试指导，以及泰康内部业务侧技术人员的培训，以泰康侧实际业务为例，开展蓝军攻防实战教学，并提供相应的培训教材，培训后可执行操作简单的业务安全测评能力。

八、资质要求

1.基础资质

(1) 具有该系统软件著作权。

(2) 具有 ISO9001 质量管理体系认证、ISO 20000-信息技术服务管理体系认证、ISO 27001-信息安全管理体系认证、ISO 29151-个人身份信息保护实践指南；

(3) 具有高新技术企业认定；

(4) 具备电信与信息服务业务经营许可证。

2.行业案例

要求具备保险、银行等金融行业用户的安全产品相关的成功服务案例不少于 3 个，并提供合同等相关证明材料。