**广东碧桂园职业学院网上办事大厅系统采购需求书**

**一、采购范围**

1.数量清单如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备（货物）名称** | **单位** | **数量** |
| 1 | 网上办事大厅系统 | 套 | 1 |

2.供应商需完成如下事项：

供应商报价需包括设备及相关附件的采购、包装、送货、安装、验收、培训、税费、技术服务（包括技术资料的提供）、保修期保障、其它费用等一切支出。

**二、商务需求**

1.对供应商的资格要求：

（1）对供应商的资格要求：国内（指按国家有关规定要求注册）注册资金500万元（含500万元）以上，具备独立法人资格；具有信息技术服务管理体系、信息安全管理体系和质量管理体系认证证书，在广东省具备20人以上的软件开发实施团队，近三年至少具备1项同类型项目实施经验，具有履行合同所必须的设备和专业技术能力。

（2）投标人的证明文件不符合标“★”的任一项的，则视为未实质响应招标要求，取消其投标资格。

2.软件产品必须拥有软件著作权登记证书。

3.实施要求：实施团队必须有丰富的实施经验，实施负责人具备项目管理相关证书。

4.合同签字生效后，以甲方发出书面通知之日起，90个工作日内实施完毕。

5.付款方式：

（1）项目实施环境（含服务器、数据库、软件系统基准版等）部署完成后，经甲方确认后，于10个工作日内支付结算款的30%。

（2）项目实施完成后，甲乙双方办理正式竣工验收及结算手续后，甲方于10个工作日内支付结算款的65%。

（2）余款5%作为质量保证金，甲方在3年产品质量保证期满后10个工作日内无息向乙方结清余下货款。

**三、系统功能要求：**

| **序号** | **功能模块** | | **功能描述** |
| --- | --- | --- | --- |
| 1 | 服务中心平台 | 事务大厅 （搜索中心） | 1.为用户提供私人搜索引擎，一键搜索个人数据，包括用户在办事大厅的办事记录、日程记录及办事大厅为用户提供的服务信息等。 2.通过智能化搜索与规范化数据分类，帮助用户快速定位查询内容。支持关键字智能推荐，包括：关联推荐、热门搜索及历史搜索，让查询更加智能化、人性化。 3.支持事务热度分享与推荐，有助于用户定位热门事务。用户可一键发起事务办理。 4.要求支持场景事务导航，可通过智能咨询，提供关键字、所属部门、事务分类、事务标签等开展智能事务推荐。通过人工智能分析用户个人需求，形成目标事务组合，对用户进行针对性事务推荐。 5.要求具备事务常用操作问答知识库，减少管理人员对于常见问题常见的重复问答工作。 6.要求具备智能操作引导。智能操作引导应具备简单引导和详细引导模式，并支持用户在查看引导操作过程中随时终止引导。 |
| 个人事务管理 | 1.个人事务主页 根据用户个人需求而自定义的个人事务主页，通过事务卡片封装各类个人事务相关事务信息，如日程日历事务、事务状态信息、事务统计等。支持在一张卡片中集中展示待办、申请、关注、待阅、草稿等事项，能够看到申请事项的当前步骤与进度，时间点与状态等信息，点击相关事务可直接跳转。要求提供现场演示。 2.应根据用户角色提供默认桌面卡片模板；用户也可以自定义卡片布局，进行个人主页卡片管理，也可以恢复默认。 3.个人信息 支持个人事务统计，提升个人效率，可通过年、月、周的统计维度，统计事务完成率，分析个人审批事务总数与个人事务耗时情况，分析个人效率排名； 支持用户设置委托人，便于在特殊情况由他人代理权限继续处理事务； 支持个人常用审批意见设置，可一次性设置单条或多条常用审批意见； 4.个人密保与安全 支持用户修改个人密码，并且跟踪个人账号登录日志，登录信息须包括登录时间、登录IP、访问端、浏览器类型。 5.任务托办 支持用户双方点对点的任务转交办理，任务发起方可通过任务状态了解任务完成进度。 支持任务接收方可以通过日程的形式及消息的形式接收任务通知。 支持任务接收方在确认完成托办的任务后，任务发起方可以通过消息形式即时了解任务完成情况。 6.个人页面主题设置 支持对个人页面皮肤色调，字体大小进行设置。 7.个人关注事务 能够实现个人关注事务台账展示。对所关注事务的分析状态进行全面跟进。 8.个人阅办 支持对用户集中呈现个人阅办信息，支持阅读情况分类。 9.个人日程日历管理 要求可汇聚各业务系统日程，实现日程数据统一管理 （为此需要提供第三方应用可调用的外部接口及数据视图结构 ）。 应提供完善的日程服务功能，包括：群发日程管理、自定义个人日程、待办日程安排、受托任务提醒。 通过与用户手机日历的对接，向用户发送离线日程信息，帮助用户随时随地查看日程。应支持用户开通日程信息的消息提醒（微信、站内消息等渠道）。 |
| 事务综合管控 | 1、图标管理 应为事务中心的事务服务提供图标维护管理，提供基础的增删改操作。要求支持将图片托拖拽至网页即可完成事务图标上传。 2、事务管理 事务分类管理，应为事务提供分类维护管理功能，实现学校业务域在事务上划分，提供基础的增删改查、停用/禁用等功能。 要求为事务中心的服务事务提供维护管理功能，统一维护用户端事务大厅中展示的所有事务。 要求根据事务的属性提供类型划分，根据事务类型，划分为“流程性事务”及“非流程性事务”，“非流程事务”可作为信息类事务及指南说明类事务；根据事务跳转方式，划分为“新窗口”“内嵌”“路由”，新窗口与内嵌的打开方式针对外部跳转页面，分新窗口和本窗口打开，支持集成外部应用集成路径，路由仅针对事务中心内部的页面，跳转方式与卡片跳转至二级页一致，此方式可快速跳转事务中心内其他服务。 要求支持事务发起权限设置，基于角色分配事务发起事务。支持事务管理负责人权限配置，使每一个事务均有对应负责人，做到事事负责。 要求支持事务发布终端配置，每条事务均能够兼容PC端与移动端。 要求支持事务时间发布策略配置，针对非常态化事务，应支持事务发布时间段配置，有助于事务有针对性触达；支持配置日程提醒策略，如周期性提醒日程提醒、自定义时间提醒。 要求支持事务催办策略配置，便于有效提升事务结办效率。支持自定义配置自动催办时间点、手动催办时间点。 要求支持事务标签绑定，便于事务分类、事务智能推荐。要求支持事务绑定多个标签。 演示事务管理功能。可在同一界面对PC端和移动端进行统一管理，自由设置事务开通办理的时间段，并且开启日程提醒用户申请事务（包括周期性提醒和自定义提醒），自由设置事务自动和手动两种催办方式的时间 3、模块及卡片管理 办事页面管理，应为用户端的一级菜单页面提供维护管理功能，在提供固定的“首页”和“事务大厅”页面的基础上向用户提供自定义菜单页的功能，用户可设置自定义页面的用户使用权限、跳转方式等。 要求按照页面的自定义程度，分类为默认页面、自定义页面。 首页卡片排列模板管理，应为不同角色的用户提供初始化个人首页卡片排版风格与卡片内容，能够为不同角色预定义个性化角色页面。 要求支持卡片管理，应为用户端首页的展示卡片提供维护与管理功能，提供卡片各类参数的配置功能及基础的增删改查操作。支持卡片化的整体布局，可随意添加已有卡片，要求不少于30个，添加的卡片可自行排列顺序，以体现个性化服务。 要求支持配置流程卡片，应提供专为流程服务的流程卡片配置功能，从申请者、审批者及监控者的角色为对应的用户提供某项事务的流程实例汇总卡片及二级页。 要求支持卡片分类管理，应为卡片提供分类维护管理 4、事务中心站内新闻管理 应为用户端的系统新闻数据提供维护管理，提供基础的增删改查操作。 5、登录页管理 要求支持事务中心登录页内容发布，应为登录页底部的文章数据提供维护管理，提供基础的增删改查操作。 要求支持banner设置，应为登录页的banner图片及内容提供维护管理功能，限制登录页banner至多显示三张，提供基础的修改、排序、停用/禁用等功能。 应为移动端首页的banner图片及内容提供维护管理功能，提供基础的修改、排序、停用/禁用等功能。 6、帮助管理 操作问答，应为用户端的操作问答数据提供维护管理，提供基础的增删改查操作。 用户反馈，应为用户端用户反馈的问题提供维护管理，提供基础的删查操作。 7、评价管理 应为流程性事务提供评价维护管理，维护申请者对结办流程的评价，提供停用/开通评价、公开评价信息等功能。支持按照分类进行应用的查看，也可就满意度、评论人数对应用进行排名查看，支持一键设置是否开通评价、是否匿名、是否显示满意度，对评价详情进行查看，支持批量处理。 8、客户端管理 应为维护人员提供客户端的基础配置参数及主题设置参数进行维护管理。 9、网站管理 应为维护人员提供事务网站的基础配置参数，包括图片上传、页脚信息以及外部网站链接等。 要求支持事务部门管理，提供基础的新增、修改、排序、停用/禁用等功能。 要求支持网站新闻管理，提供基础的发布、撤回以及查看详情等功能。 要求支持服务对象管理，提供基础的新增、修改、是否显示、关联事务等功能。 10、百科管理 要求支持百科词条管理，提供基础的新增、修改、排序、停用/禁用等功能。 要求支持百科知识管理，提供基础的增删改查操作。 要求支持知识分类管理，提供基础的新增、修改、排序、停用/禁用等功能。 要求支持访客咨询管理，提供发布、答复以及删除等基础功能。 |
|
| 2 | 移动服务 | | 基于校园H5页面的服务大厅，让用户随时随地都能查看到我的相关事务。微信事务大厅分为消息界面、个人中心和服务大厅。 1、信息界面 移动事务中心基于学校的微信企业号发布，应实现通用事务中心对微信的信息推送。当用户有事务中心任务需要办理时，微信需要以信息发送的方式实现信息提醒。用户点击提醒信息中的地址应跳转至事务办理界面办理事务。 2、个人中心 个人中心应支持用户快速查看自己相关的事务办理信息，包括：我的待办、我的待阅、我的申请、我要办事、我的已办、我的已阅、我的结办、我的草稿、我的收藏、我的关注、我的积分。 系统应支持用户点击相应的模块进行事务办理以及对事务办理情况进行查看。 用户点击我的待办阅览自己的待办事务，所有的待办事务按照时间进行排序，应支持根据事务的紧急状况进行提示。点击具体待办事项进入事务办理界面，可以查看事务办理表单进行事务办理。并且系统应支持用户查看之前所有节点的办理情况和办理意见，同时系统应支持将事务转交给他人处理以及对事务进行抄送，并且支持用户一键配置转交他人处理时事务完成后是否返回给自己。 3、服务大厅 应提供事务查询和办理支持。系统需支持事务检索和分类展示事务类型，供用户进行分类事务查询办理。在具体的事务详情中，系统应支持用户查看事务的流转记录和流程图，展示效果必须与移动端实现良好的适配。 |
| 3 | 事务流程工具 | 流程工具 | 一、流程管理 包括基于web的流程绘制、新增流程、删除流程、打包流程、下载流程、导入流程、拷贝流程、发布流程、停止流程。 要求引擎提供基于WEB的可视化建模工具，业务人员通过拖、拉、拽的方式即可以进行流程设计。应具备以下特点： 1.集成多达几百项的流程运行参数，基本达到流程建模的零代码化； 2.领先的全Web化的流程建模工具，只需要IE即可以进行流程的设计； 3.支持复制功能，有相同或类似的业务流程时只需要点击复制即可以复制一个流程； 4.支持一键打包下载和在线安装流程功能； 5.支持严格的流程版本控制功能； 6.支持错误检查功能，设计流程时系统会自动判断业务流程的语法错误； 7.单个流程可以支持多达6000个节点以上的大型流程； 8.支持分级权限控制，各部门只能设计自己的业务流程； 9.支持复杂的子流程嵌套功能； 10.支持共用子流程功能。 二、规则管理 智能规则组件要求能对运行在系统中的业务流程进行统一监控和管理，并把所有与业务流程有关的业务规则进行统一管理和授权，当业务流程运行中出现违反“规则”的情况，智能规则组件就会发出警报，实现实时的风险控制。 主要实现包括业务规则设定、系统规则设定、外部规则设定、异常事件、超时事件、路由事件、表单事件、新增规则、删除规则、打包规则、下载规则、导入规则、复制规则。 可以为工作流引擎内的规则引擎提供规则程序，系统分为流程规则和系统规则。通过定义这些规则后在流程建模的过程中或者在系统的全局引用中就可以使用这些规则来控制环节之间的路由及事件的触发和相应的系统配置。要求提供国家级软件测评中心开具的测评报告中关键页复印件并加盖原厂公章，报告测评内容包括以上内容。 三、岗位管理 包括新增岗位、删除岗位、岗位成员管理、岗位参与流程管理。 四、监控管理 流程监控是对正在流转的流程提供实时的跟踪功能，主要表现在已流转的实例数据，流程拥有者可以很方便的通过监控功能列出有权监控的业务流程和实例数据，并对正在运行的流程进行在线修改，如： 启动环节、停止环节、更换处理人、结束流程、暂停实例、恢复流程等操作，这些操作会被安全引擎进行记录。 |
| 表单工具 | 主要功能包括基于web的表单绘制、主表单定义、子表单定义、共享表单定义、表单模板、数据字典、新增表单、删除表单、打包表单、下载表单、导入表单、拷贝表单、表单检索。 表单建模工具可以非常快速的设计出学校所需要的复杂业务数据表单，如报修申请单、请假单、打印审批单等，而不需要特别专业的技术要求。设计器可以智能的根据数据库设计自动生成表单样式和字段控件，并且包含常用的业务规则，如：字段验证、不允许为空、字段事件、人员选择控件、日期选择控件、部门选择控件、级联下拉框、动态明细表、数据源绑定、卡片表单等。能够快速实现在线表单建模。 工具需以下特点： 要求表单建模完全基于Web方式设计即见即所得，无需安装任何客户端软件和插件； 用户无需关心数据库结构，系统智能存储数据； 要求一个流程可以绑定一个主表单多个子表单，无需为每个环节设计表单视图； 应支持第三方工具进行表单设计，如FrontPage、Dreamweaver、EditPlus等； 应支持大表单设计单表可包含多达10000个以上的字段； 表单设计时，设计人员无需关心数据库结构； 应支持表单的打包、复制功能，支持一键安装到生产机中； 应支持表单模板功能，企业可以把常用的表单格式做成表单模板； 应支持Word/Excel表单，表单建模中可以使用Word或Excel的形式存在； 应支持字段级的权限控制； 应支持表单更换功能，即同一个流程的不同环节可以使用不同的表单样式； 应支持分级表单设计，各部门可以设计自己的表单互不干扰； 应支持多张子表单，即用户可以在各个环节中使用不同的子表单，在各环节填写完成后，再由指定环节进行聚合成一张总表单，数据也将全部被继承； 应支持不同的附件上载到表单的不同位置，以实现多个附件按要求上传和进行权限控制； 应支持表单打开和存盘时分别触发业务逻辑代码，在打开时可以对表单字段的数据进行初始化，存盘时可以对相应的字段进行逻辑运算。 可以用于工作流引擎所能解析的表单模型的建立，通过本模块用户HTML编辑框对流程的数据表单进行绘制，在对表单的建模过程中用户可以对表单中的字段进行定义包括权限、初始值、检验规则、是否为空。要求提供国家级软件测评中心开具的测评报告中关键页复印件并加盖原厂公章，报告测评内容包括以上内容。 |
| 4 | 流程定制服务 | | 完成学校指定的20项办事大厅师生服务的实施和上线，包括但不限于以下工作：业务流程需求调研和整理，流程及表单的配置和开发，流程相关业务数据整理及初始化导入，流程上线准备，流程调优和培训服务。 |
| 5 | 效能服务 | | 1、事务统计 为事务管理人员提供多维度的事务统计分析，包括事务总数、在办事务数等不少于20项事务运行分析指标。 要求重点统计并下钻查看所有事务、所有结办事务、所有在办事务、今日办理几类核心事务统计指标。支持统计时间段自定义，支持一键导出统计结果，用excel报表方式统计各条分析事务对象的事务基础信息，申请人，当前节点、最后更新时间、总耗时。能够便于事务管理人员实现对事务科学分析。 2、事务效能监控大屏 要求采用2.5D方式，对事务统计及监控数据结果实现动态大屏分析。要求大屏页面中对统计结果形式包括且不限于滚动列表、波动图、饼状图、条形图。支持在大屏中直接获取到关键数据，包括PC和移动端的办理总量、各时段办理占比、事务建设总数、各事务结办总数、事务热度榜，以及及滚动播出实时事务动态。要求提供现场演示。 3、效能大厅 支持划分全校性数据统计及各单位部门办事统计，支持统计层级下钻查询至流程实例。 支持用户自定义统计时间范围，查看各阶段统计数据。 支持区分部门主管服务及参办服务，帮助了解部门在日常事务审批过程中，参与其他部门的事务审批情况。 支持对部门人员进行服务效率的监控，帮助部门评定审批人员办事效率。 支持细化服务事项的办理详情，对某项具体事项业务服务情况进行统计概述及办理清单汇总，支持办理清单多条件查询及导出。 提供数据大屏的换肤功能，满足学校的对大屏主题的切换需求。 |
| 6 | 事务百科服务 | | 能够提供学校事务中心总体建设情况对外展示与宣传的入口，学校师生及游客都可通过事务网站了解学校事务中心当前总体建设情况，获取可办理的服务信息、服务指南及相关服务部门等信息。 1、 网站首页 提供热门事务及推荐事务展示，帮助用户快速获取当前学校重点办理事务； 支持查看事务服务提供部门，能够查看部门相关简介及服务清单； 支持查看事务百科总的词条数和知识量、热门词条搜索及今日办事动态中申请量、办理量和结办量的统计。 支持查看关于学校事务中心建设相关新闻，及时传递事务中心建设通知。 2、 服务清单 支持统一汇总展示学校提供的办事服务清单，支持游客无需登录即可直接办理事务，师生需要先登录事务中心再进行事务办理。 搜索区域提供关键字查询及服务对象、负责部门、事务分类和事务标签的筛选查询。支持清单列表按字母排序和按热度多少排序，用户可直接在网站上查看事务的办事指南或通过网站的指引登录事务中心平台进行事务办理。 支持为用户提供办事指南、办事流程、注意事项及附件下载的详细说明。 支持用户查看事务的服务部门、所属分类、所属标签、办事满意度、热度、收藏量、服务福相及办理时段信息。支持用户下载办事指南及分享到微信。 3、 办事动态 支持统计学校事务办理情况，包括办理量、明星事务、分类办事统计及部门办事统计。 提供明星事务功能，展示近一周办理量前五的事务，支持办理情况从事务分类、所属部门结合周月年提供条形图和环形图统计。 4、 网站新闻 提供事务中心系统新闻对外发布展示。 5、 事务百科 百科首页为用户提供知识查询、展示最新知识、热门知识及最新咨询，帮助用户快速获取当前热门咨询。 支持以轮播的形式展示最新的15条知识，支持查看知识详情。热门知识展示浏览量TOP5的知识信息，支持查看知识详情。 支持学校师生就学校服务事件发起网上咨询，百科后台可以收集咨询并选择回复咨询。 支持游客在提交咨询时，系统启动检索功能，若存在类似的知识或者咨询则会提示游客，支持游客选择查看推荐，也可直接提交问题。 支持词条库收录学校专有名词及其相关知识，例如:服务事项、部门机构名称、组织协会名称等；支持帮助学校逐步建立校园专有名称词条库。 词条详情页面支持查看该词条的解释及与该词条相关联的知识。 支持咨询榜集中展示用户的所有咨询，通过收集有同样问题的用户数量，帮助学校了解学校师生普遍遇到的服务问题。 支持知识库根据分类收录学校相关知识点，包括：办事指南、学校名词解析、操作问答等。为学校师生提供规范有序的资讯信息查询库。 6、三张清单： 支持展示各单位部门基本信息，包括部门简介、办公地点、联系方式等信息。 支持提供学校各单位部门责任清单，明确各部门的职责范围。 支持汇总各单位部门在办事大厅平台提供的服务清单，明确服务对象及服务类型。 支持汇总各单位部门在办事大厅平台需参与审批办理的审批清单，明确部门审批范围。 |
| 7 | 权限服务 | | 要求首页展示部门、用户、角色、岗位、用户组总数，并以条状图、饼状图展示部门数据分布情况。 要求对部门类型进行管理，支持编号、类型名称、级别三种字段快速查询；对已有的部门类型进行统一管理，增加或者删除操作；同时支持修改部门类型信息，手动选择是否启用部门类型。  要求对用户类型进行管理，支持编号、类型名称、级别三种字段快速查询；对已有的用户类型进行统一管理，增加或者删除操作；同时支持修改用户类型信息，手动选择是否启用用户类型。  要求对机构进行管理，支持机构编号、机构名称两种字段进行快速查询；对已有的机构类型进行统一管理，增加或者删除操作；同时支持修改机构信息，手动选择是否激活该机构以及手动选择是否为默认状态，对处于默认状态的机构可以选择其授权范围。  要求对部门进行管理，能够对用户的部门信息进行编辑管理，包括对部门信息的新增、修改、删除、导入、导出、模糊查询（能够通过部门编号、名称、类型），同时能够对部门信息的状态、分配用户、分配角色进行编辑，并对分配用户编辑操作包括新增、移除、查询、禁/启用。  要求对用户进行管理，包括重置密码、导出、新增、删除、查看修改、及更多操作（分配角色、分配用户组、分配用户、修改密码）；同时能够查看用户编号、姓名、昵称、性别、类型、部门、状态、移动电话、邮箱、操作的界面。  要求对角色进行管理，能够对编号、名称、角色类型进行查询，同时支持对角色信息新增、删除、修改、分配权限，并对权限分配用户提供更多操作包括分配用户、分配岗位、分配用户组、分配部门，同时对用户分配权限范围内对应用细粒度授权，平台能够精细到功能模块的权限分配。  要求对岗位进行管理，包括对用户岗位进行模糊查询、新增、删除的操作，同时能够查看岗位名称、岗位编号、备注、所属应用、机构及操作信息，同时操作能够对岗位信息进行修改、删除、分配用户、分配角色。  要求对用户组进行管理，能够通过用户组名称、所属应用进行查询，支持对用户组信息进行新增、删除的操作，同时能够查看用户组名称、编号、所属应用、所属机构、状态及操作信息，同时操作能够对用户组信息进行修改、删除、分配用户、分配角色。  要求对服务进行管理，服务管理包括对应用服务的新增、删除、导入、导出、查询，同时能够编辑服务名称、编号、镜像地址、状态级操作，操作包括对服务的修改、删除。  要求对应用进行管理。包括对应用的新增、删除、导入、导出、编号/名称的查询，同时能够在界面展示应用名称、编号、描述、状态、操作，其中操作包括对应用信息的修改、删除、分配服务、菜单管理，而菜单管理能够对应用所属服务，编号、名称、权限类型进行查询，并且能够对应用的关联关系进行操作，包括编号、名称、类型的查询、选取。  要求对权限进行管理。包括对应用模块的新增、删除、编号/名称/所属服务的查询，同时能够在界面展示模块名称、编号、所属服务、类型及操作，其中操作包括对应用模块信息的修改、删除、功能管理，而功能管理能够对应用所属服务，编号、名称进行查询，并且能够对应用功能模块新增、移除并以界面的形式展现包括功能名称、编号、操作（修改、删除、分配资源）。  要求对资源进行管理，包括对服务的新增、删除、编号/url/请求类型/状态的查询，同时能够在界面展示服务编号、请求类型、状态、服务及操作，其中操作包括对服务信息的修改、删除、分配权限。 要求对通用配置进行管理，包括对配置编号、配置名称、配置值、缓存状态等进行增加、删除、修改、查询操作。  要求对系统信息配置进行管理，包括对编号、系统名称、所属机构等信息进行增加、删除、修改、查询操作  要求安全设置服务。支持对登录验证码进行启用，包括密码容错次数以及密码锁定时间进行具体设置。  要求在线用户管理。包括对在线用户进行清空所有认证权限缓存、清空资源缓存以及支持重置密码重试次数等操作；并支持对在线用户进行踢出操作，保障系统的安全性。  要求调度管理。包括对任务组、任务名、cron表达式、URL等进行任务添加  要求缓存管理。包括对不同类似的缓存key进行删除、清空操作。  要求访问日志管理。管理员可对不同访问用户进行数据统计，支持对用户、部门、登录时间以及浏览器类型进行查询操作，支持删除操作  要求操作日志管理。对操作用户进行查看详情操作。可查看操作用户信息、请求详情以及请求返回结果内容。支持对用户、用户类型、部门、请求时间进行操作 |
| 8 | 数据对接服务 | | 1、提供与学院统一信息门户平台、数据中心平台、统一身份认证平台集成，以及其他应用软件系统接口的解决方案，并公开数据字典； 2、提供与学院统一通信平台对接服务，提供基于微信、短信、邮件的各类项目管理的信息通知服务。 |

**四、服务需求**

1.乙方交付的产品质量保证期为3年，自该产品经甲方验收合格签字之日起算。

2.在质量保证期内，由供应商提供免费升级及维护服务（另有特别说明的，按其要求执行），质量保证期届满后，如甲方需要乙方继续提供升级及维护服务，由甲乙双方另行协商。

**附表：技术参数表**

**1、安全态势感知平台技术参数**

| **序号** | **功能及技术指标** | | **详细参数** |
| --- | --- | --- | --- |
| 1 | 硬件要求 | | 国产品牌 标准2U机架式设备，双冗余电源，CPU数量≥2，内存≥192GB,具备独立的系统盘和数据盘，系统盘要求为固态硬盘，容量≥128GB，数据盘≥48TB，支持RAID5，接口≥4个千兆电口+4个万兆光口，数据吞吐量≥8Gbps。支持多节点设备组成HA集群，实现存储空间、处理性能弹性扩充；保证业务运行的连续性、可靠性 |
| 2 | 数据采集 | | 支持从威胁探针、终端、安全设备（如防火墙、IDPS、WAF等）和第三方网络设备（通过标准syslog协议输出）处收集流量和日志数据。  支持syslog、winlogbeat、wmi、jdbc、webservice、ftp、snmptrap格式的数据 |
| 3 | 全网安全态势大屏 | | 支持不同安全视角展示16个独立的大屏展示功能 ，包括全网安全态势感知大屏、重点时期防护、安全事件态势、通报预警态势、资产态势大屏等。  支持对安全事件、外部攻击者等维度进行自定义设置实现实时告警展示，支持大屏轮播，可在一个屏幕上自动切换轮播不同的大屏，所有大屏可自定义播放顺序。 |
| 4 | 资产  管理 | 资产发现 | 支持通过主动发送微量包的扫描方式探测潜在的服务器（影子资产）以及学习服务器的基础信息，资产指纹信息包括资产类型、端口、操作系统、mac地址、主机名等。  支持跨三层取mac地址，识别资产mac地址，并能够解决不同资产IP冲突问题，以及DHCP场景IP变更的问题。 |
| 资产全生命周期管理 | 支持资产多级分支管理，最多可至15级分支，支持资产全生命周期自动管理，包括资产自动发现、多级资产、资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等。 |
| 5 | 脆弱性管理 | 弱密码检测 | 弱密码识别支持主动扫描，支持加密协议的弱口令登录检测，支持SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL等协议。  弱密码检测规则支持高度自定义，包括规则名称、生效域名、长度规则、字符规则、字典序、web空密码、账号白名单、密码白名单、txt文件格式导入。 |
| 威胁分析 | 支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、OpenLDAP等操作系统、数据库、Web应用等 ，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告。 |
| 6 | 威  胁  检  测 | Webshell检测 | 具备基于AI的webshell通信流量检测，可检出加密（如冰蝎）的通信流量。，具备650+webshell规则检测，且覆盖webshell整个攻击阶段检测，包括webshell上传点探测、webshell上传下载、webshell通信。 |
| 事后异常行为检测 | 具备元数据行为分析引擎：httpflow、dnsflow、adflow、icmpflow、maillflow等, 通过异常行为分析，结合各类机器学习算法完成未知威胁检测。包括：内网穿透、代理、远控、隧道、反弹shell等事后检测场景。 |
| 挖矿专项检测 | 支持挖矿专项检测页面，具备挖矿攻击事前、事中和事后全链路的检测分析能力。  平台内置挖矿安全知识库，对常见挖矿行为和病毒木马等提供详细的背景介绍、感染现象、详细分析、相关IOC（MD5、C2、URL）、解决方案。 |
| 文件威胁分析 | 文件威胁分析支持平台内置的静态文件检测引擎、AI智能引擎、SAVE查杀引擎、webshellkiller引擎，利用LSA, AutoEncoder, LogicRegression, SVM, 随机森林，XGBoost等多种机器学习算法组合进行综合研判。支持采用AI技术针对无文件落地的恶意脚本进行检测。 |
| 邮件威胁分析 | 支持针对政企邮件混淆宏病毒威胁检测，可通过不断下钻的特征向量提取和聚类算法有效检出邮件威胁。支持对smtp、imap、pop3、webmail等邮件协议审计，提取邮件正文和附件中的流量，并对邮件附件、正文链接、邮件行为、发件人等多维度进行规则和机器学习检测，从而识别出钓鱼邮件、病毒邮件、垃圾邮件、鱼叉式钓鱼等恶意邮件。 |
| 第三方日志关联分析可视 | 支持SIEM日志关联分析结果的可视化展示。包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供每一台设备专项分析的页面。如防火墙外部攻击场景分析、VPN账号异常场景分析、Windows服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析。 |
| 日志检索 | 支持安全检测日志、审计日志、第三方日志存储；日志类型包括漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS攻击、邮件安全、文件安全、网络流量、DNS、HTTP、用户、数据库、文件审计、POP3、SMTP、IMAP、LDAP、FTP、Telnet等。 |
| 主机行为EBA分析 | 支持利用EBA技术进行资产的行为分析，对这些对象进行持续的学习和行为画像构建，以基线画像的形式检测异于基线的异常行为作为入口点，结合以降维、聚类、决策树为主的计算处理模型发现异常用户/资产行为。内建异常行为学习模型，并支持用户对EBA基线进行自定义调整，优化模型。 |
| 7 | 事件  处置 | 告警消减 | 支持多维度模糊聚类算法将大量外部攻击日志聚合成少量攻击事件，聚合维度包括攻击IP、攻击地址、攻击目标和目标手法。 |
| 联动处置 | 安全事件支持与深信服防火墙、终端安全响应系统、超融合联动封锁、访问控制，安全事件支持与终端安全响应系统联动一键查杀、进程取证，支持关闭深信服超融合上的中毒虚拟主机，支持对深信服超融合上中毒的虚拟主机进行快照。 |
| 8 | 外网态势感知 | | 提供不少于5个域名的网站的云端漏洞主动扫描和持续监测服务。  支持和SIP联动，定期对互联网业务系统进行漏洞扫描，将主动漏洞扫描和被动流量检测结合，实时发现内外网存在的安全风险，并通过邮件、微信公众号等方式进行主动告警通知；  支持7\*24h的监测，及时发现网页篡改、敏感内容、挂马、黑链、断网等安全事件； |
| 9 | 攻防  处置 | 实战攻防中心 | 具备实战化攻防中心，支持备战阶段的对外服务器外网暴露面分析、内网服务器暴露面梳理暴。实战阶段的实时攻击分析，实时展受害者IP、攻击者IP、XFF、攻击结果、攻击次数、事件类型、威胁等级、联动响应、状态码、确定性等级等20个以上类型。实战阶段的全过程可视溯源分析、总结阶段的值守报告等全过程流程。 |
| 威胁情报  共享 | 支持云端与本地威胁情报共享，实时收集同步攻击者IP，并详细展示情报列表，包括IOC、区域、来源、更新时间、剩余封锁时间、状态、操作等，并可对本地威胁情报及云端威胁情报联动同品牌防火墙实现自动封锁。 |
| 溯源中心 | 支持自动化溯源，可自动化复现受害者从最开始的遭受攻击到权限维持各个阶段的黑客行为，包括攻击入口溯源。支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息。  支持攻击溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息。 |
| 10 | 报表中心 | 全网安全态势报告 | 可快速生成月度、季度、年度PPT报表，包含网络安全整体解读、网络安全风险详情、告警及事件响应盘点等，帮助用户高效汇报，体现安全工作价值。 |
| 告警推送 | 告警方式支持邮件告警、短信、微信告警方式。 |
| 11 | 应用中心 | 合规自检工具 | 支持同品牌防火墙、终端安全响应系统、上网行为管理等设备的配置核查并上报结果，提供自动化监测和配置引导。  支持已合规基线管控业务安全，实时监测等保差距项和高风险项，避免策略变更导致不合规，有效应对网监不定期抽查和复测场景。 |
| 12 | 设备管理 | 基础特征库升级 | 具备IPS漏洞特征识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、URL库、应用识别库、恶意链接库、白名单库；支持定期自动升级或离线手动升级。 |
| 平台快捷控件 | 支持快捷菜单悬浮控件，平台全部功能可根据使用习惯自定义添加到快捷控件，方便使用，提高运维工作效率。 |
| 接入设备管理 | 支持流量探针统一升级管理，支持监控流量探针与安全组件的运行状态，包含日志传输模式、日志传输量、最近同步信息等。 |
| 管理员角色 | 支持管理员账号的新增、删除、启用、禁用等，支持免登陆及单点登录设置，支持可信IP设置。支持角色的管理范围及页面权限的收敛设置。支持系统管理员、安全保密管理员和安全审计员三个管理员角色。 |
| 13 | 产品资质 | | 为保证厂家具备在用户核心业务在紧急情况下的应急响应能力，厂商为网络安全应急服务支撑单位证书（国家级） |
| 要求具备公安颁发的安全管理平台销售许可证  要求具备ISCCC IT产品信息安全认证证书  要求具备国家版权局颁发的软件著作权登记证书 |
| 14 | 售后服务 | | 必须在省内有厂家直属的服务办事机构，提供7\*24小时快速上门服务和2小时内快速响应服务 |

**2、探针设备技术参数**

| **序号** | **功能及技术指标** | **详细参数** |
| --- | --- | --- |
| 1 | 硬件要求 | 和SIP同品牌，标准2U机架式设备，接口数量≥6个千兆电口、2个万兆光口；硬盘容量≥1T；数据处理性能≥2Gbps，冗余电源 |
| 2 | 部署模式 | 旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响 |
| 3 | 资产发现 | 具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。 |
| 4 | 基础检测功能 | 具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意UR监测模式，可完成模式匹配并生成事件，可提取URL记录和域名记录。 |
| 5 | 网站攻击检测 | 支持SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞等网站攻击检测。 |
| 6 | 敏感信息检测 | 支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤。 |
| 7 | 漏洞利用攻击检测 | 支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Network Device、Scan漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击等服务漏洞攻击检测。 |
| 支持Application漏洞攻击、File漏洞攻击、Scan漏洞攻击、Shellcode漏洞攻击、System漏洞利用攻击、Web Activex等客户端漏洞攻击检测。 |
| 支持FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、等协议暴力破解检测。 |
| 8 | 异常流量检测 | 支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括3389、53、80/8080、21、69、443、25、110、143、22等（需提。 |
| 支持ICMP、UDP、SYN、DNS等协议外发异常流量检测，支持自定义阀值。 |
| 9 | 僵尸网络行为检测 | 支持HTTP未知站点下载可执行文件、浏览最近30天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC通信等僵尸网络行为检测。 |
| 10 | 高级检测 | 支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。 |
| 支持传输安全检测日志，包括网络攻击检测日志、漏洞利用攻击检测日志、僵尸网络检测日志、业务弱点发现日志。 |
| 支持传输访问检测日志，包括正常访问、风险访问、违规访问。 |
| 支持传输协议审计日志，包括https协议日志、http协议审计日志、DNS协议审计日志、邮件协议审计日志、SMB协议审计日志、AD域协议审计日志、WEB登录审计日志、FTP协议审计日志、Telnet协议审计日志、ICMP协议审计日志、LLMNR协议审计日志。 |
| 11 | 违规访问检测 | 支持IP，IP组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式。 |
| 12 | 沙盒对接 | 支持将流量还原的文件发送至沙盒分析；可支持第三方沙盒对接。 |
| 13 | 特征库 | 内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库。 |
| 14 | 抓包分析 | 支持流量抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式。 |
| 15 | 管理功能 | 支持设备内置简单命令行管理窗口，便于基础运维调试（需提供截图证明）；  可实时监控设备的CPU、内存、存储空间使用情况；  能够监控监听接口的实时流量情况。 |
| 16 | 产品资质 | 要求具备公安颁发的网络入侵检测系统销售许可证 |
| 17 | 厂商资质 | 厂商具备软件开发成熟度CMMI 5级认证，提供证书复印件并加盖厂商公章；  厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位；  厂商需是中国反网络病毒联盟ANVA成员单位；  厂商是微软安全响应中心的MAPP计划成员；  厂商为国家信息安全漏洞共享平台CNVD用户组成员，提供CNVD官网截图证明并加盖厂商公章；  厂商具备云安全成熟度成熟度模型CSA-CMMI 5认证，提供证书复印件并加盖厂商公章； |
| 18 | 售后服务 | 必须在省内有厂家直属的服务办事机构，提供7\*24小时快速上门服务和2小时内快速响应服务 |

**3、安全服务技术要求**

| **序号** | **服务类型** | **内容及要求** |
| --- | --- | --- |
| **1** | 资产识别与梳理 | 投标方需借助安全工具对招标方资产进行识别和梳理，并在后续服务过程中根据识别的资产变化情况触发资产变更等相关服务流程，确保资产信息的准确性和全面性 |
| 投标方需结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理；当资产发生变更时，安全专家对变更信息进行确认与更新 |
| **2** | 安全现状评估 | 系统与Web漏洞扫描：对操作系统、数据库、常见应用/协议、Web通用漏洞与常规漏洞进行漏洞扫描 |
| 弱口令扫描：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等 |
| 基线配置核查：检查支撑信息化业务的主机操作系统、数据库、中间件的基线配置情况，确保达到相应的安全防护要求。检查项包含但不限于帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制等配置情况 |
| 勒索病毒事件分析：投标方需分析判断主机是否感染了勒索病毒；是否已感染勒索病毒文件；根据已发生的漏洞攻击行为分析判断否存在勒索病毒攻击等 |
| 挖矿病毒事件分析：投标方需分析是否感染了挖矿病毒/木马；是否处于挖矿状态；根据已发生的漏洞攻击行为分析判断是否存在以植入挖矿木马为目的的漏洞攻击等 |
| 蠕虫病毒事件：投标方需确认文件是否被感染，定位失陷的代码并进行修复 |
| 针对漏洞利用攻击行为、Webshell上传行为、Web系统目录遍历攻击行为、SQL注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务风险点 |
| 失陷主机分析：投标方需对失陷主机进行分析研判（如后门脚本类事件），并给出修复建议 |
| 潜伏威胁分析：投标方需分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出解决建议。含：对外攻击、APT C&C通道、隐藏外联通道等外联威胁行为 |
| **3** | 问题处置 | 投标方需对发现的问题进行处置，包含内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等 |
| **4** | 漏洞管理 | 漏洞扫描与验证：投标方需提供不少于每月一次针对服务范围内的资产的系统漏洞和Web漏洞进行全量扫描，并针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害 |
| 漏洞优先级排序：投标方需提供客观的漏洞修复优先级指导，不能以漏洞危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度 |
| 漏洞验证：提供漏洞验证服务，针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的漏洞，自动生成漏洞工单，安全专家跟进漏洞状态，各个处理进度透明，方便招标方清晰了解当前漏洞的处置状态，将漏洞处理工作可视化 |
| 漏洞修复建议：针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案 |
| 服务催单：针对服务平台生成的工单，招标方可按需催单，用户可在服务平台上采用邮件等方式提醒安全专家加快协助处置，督促投标方第一时间处理 |
| 漏洞复测：需提供漏洞复测措施，及时检验漏洞真实修复情况。投标方要支持招标方可按需针对指定漏洞，指定资产等小范围进行，降低漏洞复测时的潜在影响范围 |
| 漏洞状态总览：对发现的漏洞建立状态总览机制，自动化持续跟踪漏洞情况，清晰直观地展示漏洞的修复情况，遗留情况以及漏洞对比情况，使得招标方可做到漏洞的可视、可管、可控 |
| 最新漏洞预警与排查：投标方需实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。 |
| 最新漏洞处置指导：一旦确认漏洞影响范围后，安全专家提供专业的处置建议，处置建议包含两部分，补丁方案以及临时规避措施。 |
| 最新漏洞复测与状态跟踪：由投标方对该最新漏洞建立状态追踪机制；跟踪修复状态，遗留情况。 |
| **5** | 威胁管理 | 结合大数据分析、人工智能、云端专家提供安全事件发现服务：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态,发现各类安全事件，并自动生成工单 |
| 实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件 |
| 实时监测网络安全状态，对病毒事件自动化生成工单,及时进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发DOS型、C&C访问型、文件感染型、木马型 |
| 投标方需针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机，将深度关联分析的结果通过邮件、微信等方式告知用户 |
| 结合威胁情报，投标方需排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固 |
| 投标方需每月主动分析病毒类的安全事件：提供病毒处置工具，并针对服务范围内的业务资产使用病毒处置工具进行病毒查杀，对于服务范围外的业务资产，安全专家协助用户查杀病毒 |
| 投标方需每月主动分析攻击类的安全事件：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗，当用户无防御措施时，提供攻击类安全事件的处置建议 |
| 投标方需每月主动分析漏洞利用类的安全事件并验证该漏洞是否利用成功，提供工具协助处置 |
| 投标方需每月主动分析失陷类的安全事件并协助用户处置，并提供溯源服务 |
| 策略调配：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新 |
| 策略定期管理：投标方需每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到有效的防护效果 |
| 通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗 |
| 通过全网大数据分析，发现有境外黑客或高级黑客正在攻击，立即采取行动封锁黑客行为 |
| 实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。 |
| 针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助招标方快速恢复业务，消除或减轻影响 |
| 入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务 |
| 入侵威胁清除：排查攻击路径，恶意文件清除 |
| 入侵原因分析：还原攻击路径，分析入侵事件原因 |
| 加固建议指导：结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵 |
| **6** | 服务水平协议 | 对安全事件服务水平作出承诺：  1）从安全日志产生到事件通告给招标方的时间方面，按照国际标准对安全事件的分类分级指南，重大安全事件和较大安全事件的通告时间小于30分钟，一般事件的通告时间少于1小时。  2）在未配备投标方的边界防护服务组件和终端防护服务组件的情况下，运营服务对于重大安全事件和较大安全事件的遏制影响和处置完成时间小于4小时，对于一般事件的遏制影响和处置完成时间小于24小时。  3）安全事件经过服务人员的确认后，各类安全事件的判断准确率不低于99%。  4）在配备了投标方的边界防护服务组件和终端防护服务组件的情况下，安全事件的闭环处置比例达到100%。  5）以上要求未达标的惩罚措施为：每不达标一次，服务时间延长一周。  6）对于特别重大安全事件应启动应急响应机制，10分钟之内云端专家进行响应，同城2小时上门处置，同省4小时上门处置。  7）服务期内若发生一次特别重大安全事件，投标方将扣除服务合同金额3%作为赔偿金。 |
| 安全威胁服务水平作出承诺：  1）从安全日志产生到威胁通告给招标方的时间方面，高级威胁的通告时间少于30分钟，一般威胁的通告时间少于1小时。  2）在未配备投标方的边界防护服务组件和终端防护服务组件的情况下，高级威胁和一般威胁的处置完成时间少于24小时。  3）安全威胁经过服务人员的确认后，高级威胁和一般威胁的判断准确率不低于99%。  4）在配备了投标方的边界防护服务组件和终端防护服务组件的情况下，高级威胁和一般威胁的闭环处置比例达到100%。  5）以上要求未达标的惩罚措施为：每不达标一次，服务时间延长一周。 |
| 对安全漏洞服务水平作出承诺：  1）在配备投标方的漏洞定期扫描服务组件的情况下，漏洞扫描的频率不低于每30天扫描一次。  2）高危可利用漏洞从发现到完成闭环处置的时间少于7个工作日。  3）高危可利用漏洞经服务人员确认后的准确率不低于99%。  4）高危可利用漏洞的闭环处置比例达到100%。  5）对于0day和最新漏洞，从发现漏洞到通告给招标方的时间少于8小时。  6）在配备投标方的边界防护服务组件和终端防护服务组件的情况下，对于0day和最新漏洞，在发布相应的攻击POC之后，运营服务将在24小时内遏制漏洞的影响。  7）0day漏洞经过服务人员确认后的准确率不低于99%。  8）在配备了投标方的边界防护服务组件和终端防护服务组件的情况下，0day漏洞的闭环处置比例达到100%。  9）以上要求未达标的惩罚措施为：每不达标一次，服务时间延长一周。 |
| **7** | 服务交付物 | 交付物名称：《安全服务运营报告》，报告频率：每周一次  交付物名称：《首次威胁分析与处置报告》，报告频率：一次  交付物名称：《事件分析与处置报告》，报告频率：按需触发，不限次数  交付物名称：《安全报告》，报告频率：按需触发，不限次数  交付物名称：《综合分析报告/运营月报》，报告频率：每月一次  交付物名称：《勒索风险排查报告》，报告频率：每季度一次  交付物名称：《季度汇报PPT》，报告频率：每季度一次  交付物名称：《年度汇报PPT》，报告频率：每年一次  中标后招标方有权要求中标方严格按照上述频率要求提供服务交付物，确保满足招标方安全需求。如中标方未能按时提供，招标方有权终止服务合同，中间产生任何费用由中标方自行承担 |
| **8** | 服务频率 | 7\*24小时持续专家服务，威胁发现及时响应 |