**江西省水投江河信息技术有限公司**

**招标邀请文件**

**日期:2020年9月**

**目录**

[第一部分 招标邀请函 3](#_Toc15789)

[第二部分 投标须知 6](#_Toc15402)

[第三部分 评审文件 10](#_Toc11067)

[第四部分　项目内容清单及主要规格功能参数 27](#_Toc1949)

[第五部分 商务要求 33](#_Toc31267)

[第七部分 招标响应文件格式 34](#_Toc15931)

# 

# 第一部分 招标邀请函

受邀单位：

我司已中标江西省水利厅智慧水利2020年度项目，现需寻找专业网络安全支撑服务公司与我司一同完成本项目的省级网络安全监测能力建设，故邀请你单位参加本次竞标。

一、采购项目名称：智慧水利项目-省级网络安全监测能力建设

二、范围：建设水利信息化运维安全综合管理平台基础模块，本期建设包含绿盟入侵感知模块、骨干网络数据采集模块、数据分析模块、数据展示模块。功能涵盖水利骨干网络流量、威胁信息、日志信息、漏洞信息、SNMP信息、应用信息的收集、处理、分析、展示。

三、采购方式：邀请招标

四、采购控制价：210万元

五、投标单位资格及要求：

1、资格要求

（1）中华人民共和国境内注册、具有独立法人资格,具有有效的营业执照、税务登记证、组织机构代码；

（2）投标人没有正在被设区市级及以上行政或纪检、监察等主管部门责令停业、取消投标资格；财产没有被司法部门或行政执法部门接管、冻结或处于破产状态；已执行或正在执行的合同不存在欺诈行为、类似业绩没有虚假；投标文件内容真实、无弄虚作假；并且近3年投标人在投标活动中无违法行为记录。

2、本项目不允许联合体招标。

3、采购单位不接受有下列行为之一的投标单位参加招标：

（1）有违反法律、法规行为，依法被取消招投标资格且期限未满的；

（2）因招投标活动中有违法、违规和不良行为，被有关招投标行政监督部门公示且公示期未满的；

六、符合资格的投标单位应当在2020年9月7日21：00前通过电子邮件的方式将参与项目招标的回执及资格文件扫描件发送给采购单位，逾期未发送视为放弃。

七、本项目不举行集中答疑会，投标单位如有疑问请以书面函件形式向采购单位咨询。

日程安排：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 事　项 | 日期时间 | 地　点 | 备注 |
| 1 | 招标邀请文件发放 | 2020年9月4日 | 邮件发送 |  |
| 2 | 投标文件提交 | 2020年9月8日9：40 | 云中城A座39楼 |  |
| 3 | 评标 | 2020年9月8日10：00 | 云中城A座39楼 |  |
| 4 | 合同签订 | 另行通知 | 另行通知 |  |

八、投标文件递交地点：江西省南昌市高新区紫阳大道3399号云中城A座39楼大会议室，收件人：刘克立 13607097907。

九、投标响应文件递交截止时点： 2020年9月 7日9时 40分（北京时间）。评标时间：2020年9月8日10时00分至10时30分（北京时间）。

采购单位：江西省水投江河信息技术有限公司

联系人：刘克立

电话：13607097907

联系邮箱： liukeli@jxsltz.com

联系地址：江西省南昌市高新区紫阳大道3399号云中城A座39楼 邮编：330001

**回　执**

江西省水投江河信息技术有限公司：

我公司于 年 月 日接到贵公司的邀请，决定按照招标文件邀请准时响应智慧水利项目-省级网络安全监测能力建设项目的招标工作，本公司的联系人：　　　　　　，联系电话：　　　　　　　。

　　　　　　　　　　　　　　　　　公司（盖章）

**注：若在招标开始前确认不参加本次招标，请来函（加盖公章）以邮件方式及时说明，逾期视为放弃。来函通知参与招标，至招标期止却未参加的单位，公司将在今后的招标活动中不再邀请参与。**

# 第二部分 投标须知

一、说 明

1、适用范围

本竞争性招标文件适用于本次竞争性招标的采购项目。

2、定义

“采购单位”是指：江西省水投江河信息技术有限公司。

“监察员”是指：江西省水投江河信息技术有限公司纪检监察员。

“邀标单位”是指响应本文件要求，参加投标的法人或其他组织。

（1）符合《政府采购法》第二十二条规定的条件。

（2）符合招标文件规定的资格要求。

（3）符合本招标文件规定的其他要求。

“成交单位”是指经法定程序确定并授予合同的响应人。

“投标文件”是指：投标单位根据本文件要求，编制包含报价、技术和服务等所有内容的实质性响应文件。

3、服务

　“服务”是指按国家及行业规范要求，投标单位承诺的技术服务以及招标文件规定的其它服务。

4、招标费用及响应：

投标单位承担所有与本次投标有关的全部费用。

二、投标文件

1、投标文件的构成

招标文件由下列文件以及在招标过程中发出的修正和补充文件组成：

（1）投标邀请函；

（2）投标须知；

（3）评审；

（4）项目内容；

（5）商务要求；

（6）技术要求；

（7）投标响应文件格式；

（8）在招标过程中由采购单位发出的修正和补充文件等

2、投标单位应认真阅读、并充分理解招标文件的全部内容（包括所有的补充、修改内容、重要事项、格式、条款和技术服务规范、参数及要求等），投标单位没有按照招标文件要求提交全部资料，或者投标响应文件没有对招标文件在各方面都做出实质性响应是投标单位的风险，有可能导致其投标响应被拒绝，或被认定为无效响应或被确定为响应无效。

三、投标响应文件的编制

1、投标单位对响应文件的编制应按要求装订。

2、投标单位提交的响应文件及其与采购单位就有关招标的所有来往函电均应使用中文。

3、投标响应文件必须按本文件的全部内容，包括所有补充通知及附件进行编制。

4、如因投标单位只填写和提供了本文件要求的部分内容和附件，而给招标造成困难的，其可能导致的结果和责任由响应自行承担。

四、招标报价要求

对于本文件中未列明，而投标单位认为必需的费用也需列入报价。在合同实施时，采购单位将不予支付投标单位没有列入的项目费用，并认为此项目的费用已包括在报价中。

五、招标保证金

无。

六、投标响应文件的份数和递交

1、投标单位应将响应文件的正本和所有的副本分别密封包装，并在外包装上清晰标明“正本”、“副本”字样。响应文件数量正本壹本、副本壹本，封口处应加盖投标单位印章。

2、投标响应文件的封装袋正面应当标明：

（1）招标项目名称；

（2）投标单位名全称；

（3）日期。

3、所有响应文件应于第一部分《招标邀请函》中规定的地点和截止时点前递交给采购单位。

4、迟交的响应文件，按《政府采购法》及《江西省水利投资集团有限公司采购管理暂行办法》的规定，采购单位将拒收在规定的递交响应文件截止时点之后收到的任何投标响应文件。

七、注意事项

1、任何要求对招标文件进行澄清的投标单位，均应以书面形式在招标文件规定的招标响应文件递交截止日以前通知采购单位。采购单位对投标单位所要求澄清的内容以书面形式予以答复。

2、投标单位在规定的时间内未要求对招标文件澄清或提出疑问的采购单位将视其为无异议。对招标文件中描述有歧意或前后不一致的地方，招标小组有权进行评判，但对同一条款的评判应适用于每个投标单位。

3、招标：（按本招标文件的第三部分评审文件执行）

八、确定成交办法

1、合理最低价法。按本竞争性招标文件第三部分评审文件规定的评审办法进行评审，以报价合理最低的投标单位作为成交候选单位。

2、成交人确定后，采购单位向成交人发出《成交通知书》。《成交通知书》对成交人和采购单位具有同等法律效力。

九、质疑

如果投标单位对此次采购活动有疑问，可依法向采购单位提出质疑。采购单位应当依法给与答复，并将结果告知有关当事人。

九、签订合同

成交单位在收到成交通知书后，按规定与采购单位签订合同。

十、成交通知书格式：

**成交通知书**

公司：

你方于 年 月 日所递交的 项目招标响应文件已被我方接收，被确定为成交人。

成交价：金额为人民币 元；（大写： ）。

请你方在收到通知后尽快到我方签订合同。

特此通知！

采购单位：（盖章）

日期：年 月 日

# 第三部分 评审文件

一、招标小组

本次招标由采购单位依据《江西省水利投资集团有限公司管理暂行办法》组建招标小组，招标小组成员5名，监督小组成员1-2人，记录1人。

二、招标步骤

（1）招标小组对投标单位响应文件进行现场审查；

（2）招标小组可根据实际情况现场确定是否需进行二次招标，如需进行二次招标，应明确招标顺序、招标主要内容，并详细做好招标记录，主要工作如下：

①招标小组确定招标顺序、招标主要内容，并做好详细记录。

②各有效投标响应人根据二次招标情况给出最终报价；

（3）招标小组根据响应文件（如有二次招标，以最低报价为准）进行评选，按投标价格由低至高排出各有效投标单位的名次，以投标价格最低的投标单位作为成交候选单位。

三、现场审查

分为资格性检查和符合性检查。审查响应文件是否对竞争性招标文件作出实质性的响应，对未作出实质性响应的投标单位现场告知其投标无效（废标）。

四、评标方式

价格最低者中标。

五、技术参数及要求

（一）技术部分

|  |  |  |  |
| --- | --- | --- | --- |
| **采购品目** | **技术参数及要求** | **数量** | **单位** |
| 态势感知系统 | 1. 平台应基于大数据基础构架，具备海量数据接入、存储、访问、计算能力 2. 平台应支持分布式部署方式，支持首次部署结束后根据负载要求灵活扩展，提高存储、计算能力，且不影响业务运行，部署模式支持集群部署且集群规模不低于100台 3. 数据存储应支持Redis内存缓存、Kafka分布式消息系统、关系型数据库、Elasticsearch搜索引擎，支持Hadoop生态存储系统（HDFS分布式文件系统、HBase分布式键值存储、Hive数据仓库），支持不低于百TB级别数据存储与访问 4. 平台应支持多种协议的数据接入，包括但不限于FTP、SFTP、UDP、TCP、Netflow、本地文件系统 5. 平台应支持单向光闸场景数据接入，支持利用转发模块完成数据不同网络间的数据摆渡 6. 平台应支持多维度资产管理，进行多维度资产视图分析，系统至少内置五种视图：资产组视图、业务系统视图、组织结构视图、地理位置视图、行业视图。 7. 平台应支持对接入数据直接以文件形式进行存储或者解析规范化后存储至数据仓库或者搜索引擎中，数据保存时间应提供配置项且满足合规要求 8. 平台应支持灵活的配置选取接入协议、解析规范化规则完成数据接入，支持对数据接收、数据解析、数据存储速率进行监控并界面展示，支持配置允许接入日志的ip地址白名单，支持查看最近解析失败的原始日志 9. 平台应支持对至少10000个网络资产进行发现探测，对暴露在互联网上的网络资产设施进行检查，包括但不限于资产核查、脆弱性检测、完整性检测、可用性检测和认证检测 10. 平台应支持按照不同视图对资产信息进行统计包括各视图下节点数、各节点下资产数、各类型资产数等统计； 11. 平台应支持对重点单位或重点网站的漏洞扫描能力，平台支持向安全采集探针下发系统漏洞扫描任务、网站安全漏洞扫描任务、口令猜测扫描任务，通过平台进行统一扫描任务监控、管理，对扫描结果可以进行可视化呈现 12. 平台应支持在线下发漏洞扫描任务的能力，应支持灵活的任务策略配置，包括但不限于：调度策略（立即、定时、周期）、扫描设备选择（支持自动/手动指定扫描设备进行漏洞扫描）、漏洞模板策略、登录扫描参数、扫描引擎参数等。 13. 平台应支持离线漏洞结果数据导入平台进行进一步分析的能力，至少支持绿盟RSAS的离线导入； 14. 平台应支持对扫描任务进行灵活多样管理的能力，支持扫描任务过程中的进度及状态查看，支持对任务的删除，重扫、查询等操作； 15. 平台应支持多源异构安全设备告警日志数据的接入并分析能力，并根据日志分析出可疑的威胁事件，支持统计过滤、时序关联、机器学习等分析模型。 16. 平台应支持规则分析能力，应支持不少于200种内置分析识别规则并支持内置规则的升级，支持用户自定义规则，用户自定义规则可以支持导入导出。 17. 平台应支持复杂模型的分析能力，应支持DGA、决策树机器学习算法，提供僵尸网络场景、隐蔽信道场景、WebShell场景的检测，并输出相关的可疑事件。 18. 平台应支持一定时间窗口内多种规则组合的分析场景，并输出相关的可疑事件。 19. 为保障产品安全能力，产品厂商应具有微软漏洞通告能力，是微软MAPP成员，能够及时响应微软系统漏洞通告，及时进行系统加固。 20. 平台应支持可疑安全事件的自动化生成能力，为方便后续研判，安全事件属性应至少包括：事件名称、事件类型、事件开始、事件结束时间、威胁等级、置信度、攻击结果、攻击链阶段、攻击者、受害者、来源设备、处置建议等。 21. 平台应支持接入并分析流量数据，接入的数据类型包括但不限于会话日志、http日志、dns日志、文件还原日志、FTP日志、邮件日志、Telnet日志、认证记录日志、数据库操作日志、登录日志、SSL/TLS日志、社会账号日志、ICMP日志、接口流量日志、Flow日志等。 22. 平台支持可疑行为查询分析能力，可以对不同场景下的可疑行为进行预览和详细信息查看操作。 23. 平台应支持不少于25种内置可疑行为分析场景，内置场景支持升级；支持用户自定义的场景，且用户自定义的场景支持导入导出。分析场景支持在线和离线分析，离线分析支持定时和周期执行。 24. 平台应支持多种类型的情报接入，至少包含：ip、url、域名、样本、漏洞、热点事件情报 25. 平台应支持接入ip情报，IP情报至少包含：ip地址、地理位置信息、信誉等级、攻击类型、脆弱性指数、威胁指数、反向域名、提供商、操作系统及版本、运行的服务及版本、ip历史恶意行为、情报更新时间、关联的其他情报信息 26. 平台应支持界面查看漏洞情报预警列表以及详情，支持对界面对预警情报设置处置标记，并统计展示已处置、未处置预警数量 27. 平台应支持界面查看漏洞情报、热点事件情报预警趋势图 28. 平台应支持以地图形式展示各个单位安全状况信息。支持大屏投放要求及分辨率兼容要求，且易于操作，展现形式多样，画面丰富，并且能够以地图、趋势图、饼状图等多种图形化方式展现网络安全态势情况，动态提醒当前网络最新的安全威胁； 29. 平台应支持展示资产情况的统计，包括资产、网站资产、未识别的资产、失陷资产、新增资产统计总数。同时支持资产拓扑图的展示，并提供拓扑图的配置功能。 30. 平台应支持所监测网络安全情况的态势呈现能力，态势呈现包括但不限于综合态势、威胁态势、脆弱性态势、环境感知态势、运维响应态势。 31. 平台应支持对导致资产失陷的攻击意图、资产数量、以及已处置的数量进行统计，并以列表的形式进行展示。 32. 平台应支持展示APT威胁态势，并记录APT组织的名称和攻击次数。 33. 平台应支持提供漏洞运维状态统计，按总体漏洞和高危漏洞两个维度，展示漏洞总数以及漏洞关联的资产总数，并以柱状图的形式展示不同状态的漏洞处置单的统计情况。 34. 平台应支持安全治理能力，能够结合环境数据自动化评估安全治理等级和评分，安全治理等级应包括优、良、待改进三级，总评分应充分结合建设情况指标、运行能力指标、安全态势指标、合规指标等加权计算得到。 35. 为保障产品安全能力，产品厂商应具备漏洞挖掘能力，是国家信息安全漏洞库（CNNVD）的一级技术支撑单位。 36. 平台应支持评估安全目标的达成情况，根据安全治理评分得到结论，区分安全治理成果是否达标。 37. 平台应支持权限管理能力，支持对界面菜单功能访问以及平台数据访问进行权限控制 38. 平台权限控制应支持分权分域，通过权限域划分可访问的界面菜单功能和访问资产、设备数据，权限域包含可访问的界面菜单功能列表和有权访问的资产、设备列表，权限域下用户只能对域内包含界面菜单功能进行访问，只能管理对应资产、设备列表相关业务数据。权限域支持组织成树状结构，下级权限域界面菜单功能列表和有权访问的资产、设备列表只能分配为上级权限域子集。 39. 为保证不同角色人员对平台的友好使用，平台应支持通过角色分离实现三权分立，且至少应包含三类内置角色：系统管理员：负责除日志审计管理外的所有功能；用户：由系统管理员生成，管理其相应业务；审计管理员：负责审计系统管理员和用户的工作 40. 平台应支持多级部署，上下级平台支持在界面中通过配置方式进行对接，并查看联通状态，支持配置多个下级平台或上级平台 41. 多级平台部署时，下级平台应支持上报数据到上级平台，下级平台支持从界面选择外发的数据库表或者索引，通过配置过滤条件执行外发。上级平台应支持从界面选择接收下级平台存储数据的库表、索引，并将接收到的数据根据数据类型自动路由到目的库表、索引 42. 平台应支持运维人员通过web方式登录平台进行运维管理 43. 平台应支持通过操作界面对系统的各项配置进行管理，包含但不限于：用户账号管理、权限管理、组件管理、数据接入配置、级联配置、存储管理、任务管理、集群主机管理、大数据存储计算设施管理、系统升级等 44. 为保障产品安全能力，产品厂商需为中国反钓鱼网站联盟成员，具备对各类钓鱼邮件中钓鱼网站的快速上报和关停能力。 45. 平台应支持通过操作界面配置平台进行集群部署，支持选择部署节点并检查节点是否满足平台部署要求，支持选择部署的大数据存储计算设施以及设施各角色实例部署节点，支持配置大数据存储计算设施重要部署配置参数。支持自动化集群部署能力，能够自动完成节点、大数据存储计算设施部署并且界面打印部署日志 46. 平台应支持从漏洞管理、威胁管理、流量分析等模块推送需要运维的安全事件进行处置，推送内容包括优先级别、事件ID、事件名称、运维对象、事件类型、分类、事件分级、来源、发生时间、次数、状态、处理建议等相关信息，并且支持自定义 47. 平台应支持对威胁、失陷主机、网站安全事件、脆弱性等事件进行统一运维处理，提供统一入口 48. 平台支持对安全运维事件选择进行一键封堵，可设置封堵类型、封堵对象、封堵设备、封堵原因、封堵时间等信息； 49. 平台应支持工单数据的权限管理，所有的运维人员都可查看平台所有工单，可通过责任人是自己来查看自己的工单；仅支持对责任人是自己账号的工单进行操作。 50. 平台应支持一键封堵的权限管理能力，支持分账号、分权限的封堵策略管理，一键封堵角色需至少区分操作员、审批员、管理员，且支持多角色共存 51. 平台应支持一键封堵审批流程配置与管理，支持操作员新建封堵输入、申请解封堵、选择封堵设备等操作，支持审批员审批封堵申请、解封堵申请，审批环节支持本地审批与第三方审批插件审批 | 1 | 套 |
| 流量探针系统 | 1. 要求采用多核架构，专用安全操作系统，系统硬件为全内置封闭式结构，稳定可靠，标准2U机架尺寸，交流冗余双电源，配置不少于6个千兆GE接口，1个接口扩展插槽（4GE/4SFP/8GE/8SFP/2SPF+/4SPF+），1个GE管理口，1个RJ45串口，2个USB接口，吞吐量≥2Gbps，最大并发会话数≥180万，每秒新增会话数≥25000； 2. 支持导入HTTPS证书，对流量进行解密还原 3. 支持对http、smtp、imap、pop3、ftp、telnet、dns、icmp、ssl、ldap、mssql、oracle等常见协议的深度解析和还原。 4. 支持对工控和物联网协议的深度解析和还原，常见协议包coap,goose,Modbus,mqtt 5. 支持流量灰名单，关注重点资产流量，对命中灰名单的流量进行还原和威胁检测。灰名单类型包括IP、端口、IP+端口、域名 6. 支持覆盖多种攻击特征，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测，攻击特征库数量至少为9000种以上。 7. 支持对流量中出现的文件进行发现和还原，支持还原的协议包括：http、smtp、pop3、imap、ftp、webmail、samba 8. 支持还原的可执行类型：bat、dll、sys、exe、com、src、pif。 9. 支持还原的文档类型：doc/docx、xls/xlsx、ppt/pptx、pdf、rtf、 wpt、pot、wps、pps、mpp、et、dpt、dps、ett、dot。 10. 支持还原的压缩包类型：zip、7z、rar、gzip、tar、bz。 11. 支持还原的网页脚本类型：asp、js、jsp、html、phtml、xhtml、php 、htm、mhtml、 htx、 plg 12. 支持对常见应用服务和常见数据库协议的口令暴力破解检测。 13. 支持多种抗逃逸攻击检测，检测类至少包含TCP标志位规避攻击、URL斜线分隔符规避攻击、TCP校验和规避攻击、URL NULL字符分割规避攻击、HTTP长URL规避攻击、HTTP请求伪造参数规避攻击。在告警信息中至少显示规避攻击的类型和规避攻击的事件名称 14. 支持基于SCADA等工控协议的相关漏洞攻击检测 15. 支持网络层/应用层DDOS检测和告警 16. 支持自定义TCP端口和UDP端口扫描检测模型，支持配置参数包括检测阈值、检测周期、复位时间，提供默认配置。检测产生的告警信息至少包括扫描类型和扫描事件名称。 17. 支持自定义pingFlood、sysflood、udpflood、Pingsweep、arpspoof、Dnsreqflood、Dnsreplyflood、httpgetflood和httppostflood检测模型，支持配置的参数包括检测阈值、检测周期、复位时间，提供默认配置。 18. 支持针对主流Web服务器及插件的已知漏洞攻击检测。 19. 支持爬虫检测，具备对100种以上的爬虫特征进行识别和检测的能力 20. 支持sql注入、XSS、SSI指令、Webshell、目录遍历、远程文件包含等攻击检测。 21. 支持对WEB服务器上的文件下载进行检测。 22. 支持对WEB服务器的慢速攻击检测，能够检测低频的HTTP请求。 23. 支持对敏感信息进行检测。 24. 内置WEB应用机器学习检测模型，支持对sqli，xss，exec，phprce，ptravel和jeli攻击类型进行分类检测和告警，告警信息至少包括机器学习告警类型和威胁事件名称 25. WEB类告警详情包含请求和响应信息，在请求和响应信息中能标记规则匹配中的字段信息，便于运维人员快速进行确认攻击事件 26. 支持WEB类的攻击结果进行判定 27. 内置恶意文件检测引擎，支持对可执行文件、文档、压缩包和网页脚本进行恶意代码检测和告警，告警信息中至少包含恶意文件类型、恶意文件家族信息和恶意文件变种信息， 28. 内置基于统计学特征和操作码序列训练的检测模型，支持对asp、jsp、php文件类型进行检测和告警 29. 内置基于webshell通信特点以及流量特征构建决策模型，支持对asp文件、php文件、jsp文件和图片马进行检测和告警 30. 告警信息至少包括机器学习告警类型和威胁事件名称 31. 支持自定义TCP/UDP行为检测模型，通过自定义内部资产对流量中的异常行为（包括内部向外部发起、内部对内部发起）进行检测和告警，告警信息包含检测类型和威胁事件名称 32. 支持自定义TCP、UDP行为模型，配置参数至少包括检测阈值、检测周期、复位时间、IP对象 33. 应具备元数据提取、存储和检索的能力。 34. 支持对入侵检测告警、WEB应用告警、威胁情报告警和恶意文件告警中的攻击IP和受害IP发送阻断报文，进行旁路阻断 35. 支持自定义一键封堵，配置策略包括IP类型（配置选项包括源ip/源端口/目的ip/ 目的端口）、域名类型、生效时间和失效时间 36. 支持自定义规则抓取和留存可疑原始流量，自定义规则支持对原始流量的payload进行匹配。自定义规则内容至少包括：源IP/源端口、目的IP/目的端口、匹配类型（二进制、字符串、正则表达式）、匹配特征、会话数量、过期时间 37. 提供原始pcap包查询API接口，大数据平台可通过该接口下发查询条件、获取指定pcap包 38. 为保证厂商Web信誉库的可靠性，能够阻止过滤含有恶意代码的高风险网站，实现对终端用户的安全保护，厂商为StopBadware合作伙伴。 39. 支持从流量中识别资产信息和展示，识别的信息至少包括资产IP、资产MAC、服务端口号、服务协议、设备类型、地理位置、操作系统、资产状态、资产描述、资产关联账号 40. 系统应具备系统运行状态监控功能，能够实时查看CPU使用率、内存使用率、磁盘剩余空间、系统运行时间、接口状态、流量等信息。 41. 支持配置策略的备份，备份数据至少包括全部配置、引擎参数、接口参数和白名单 42. 支持备份策略恢复，恢复的类型包括全部配置、引擎参数配置，接口参数配置和白名单配置 ； 43. 支持对采集的全部流量进行存储、检索和下载，检索条件包括源IP、目的IP、源端口、目的端口、起止时间。 44. 支持对入侵检测告警、WEB应用告警、威胁情报告警和恶意文件告警中的攻击IP和受害IP发送阻断报文，进行旁路阻断。 | 1 | 套 |
| Web应用防火墙 | 1. 产品为专业WEB应用防火墙，而非安全网关或NGFW的防护模块； 2. 2U,含交流冗余电源模块,2\*USB接口,1\*RJ45串口,2\*GE管理口。1个2万兆SFPP插槽（不含光纤接口模块），3个可选扩展插槽位，可购买千兆（光、电）、万兆光链路扩展板卡，网络吞吐6G，应用吞吐3G，1T硬盘。 3. 支持透明部署，旁路部署，反向代理模式以及镜像部署模式，支持HA的A/S部署模式，支持配置同步； 4. 支持针对主流Web服务器及插件的已知漏洞防护。Web服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS等；插件应覆盖：dedecms、phpmuadmin、PHPWind、shopex、discuz、echsop、vbulletin、wordpress等； 5. 支持快速模式和向导模式，其中向导模式可以根据用户配置的操作系统、web服务器、数据库、开发语言信息，自动生成一套安全解决方案； 6. 支持非法文件上传防护，有效识别文件上传行为，并对上传行为的内容做安全检测，可以根据需要，禁止上传以下文件类型：PE(windows Executable File)、ELF(linux Executable File)、PHP web shell、Linux shell、Power shell(windows Script File)、Java shell、Asp shell、Perl shell、Python shell及Ruby shell； 7. 支持基于专业技术实现的Web扫描防护，支持规则库匹配、请求量统计（最小样本数、离散率、最大请求量）、应答分布统计（成功/失败应答比例、最小统计量）设置。**提供功能截图进行佐证，并加盖原厂公章。** 8. 支持对注入、XSS、SSI指令、Webshell防护、路径穿越及远程文件包含的攻击防护。，支持CSRF（跨站请求伪造）防护。提供盗链防护，支持Referer和Cookie算法； 9. 支持与异常流量清洗设备联动，对流量进行按需清洗； 10. 支持基于五元组（源IP地址、目的IP地址、源端口、目的端口、协议类型）及接口的网络层访问控制功能； 11. 系统提供可配置的内置规则；且支持自定义规则，规则属性要求支持“检测方向（请求或响应）”、“检测对象（URI/URI-path/Host/参数名/参数/Header-name/Header/Cookie名/Version/请求方法/Request-Body）”、匹配操作、特征签名等丰富要素； 12. 支持爬虫防护，实现对100种以上的爬虫特征进行识别和阻断，防止页面因爬虫而引起信息泄露等问题； 13. 支持敏感信息过滤，对用户的个人隐私信息（信用卡卡号、手机号、身份证号码）泄露进行检测、阻断或替换； 14. 支持暴力破解防护，可针对指定URL进行暴力破解防护，可设置GET、POST登陆阀值、检测周期； 15. 可以与SaaS扫描服务或者Web漏洞扫描器产品联动，在WAF上定期自动获取专家级、个性化的《WEB漏洞扫描报告》，并转化为WAF可执行的、有针对性的WEB安全防护策略。支持手动导入扫描结果，也支持在WAF上自动下发扫描任务，扫描完成后扫描结果自动上传WAF； 16. 支持利用威胁情报建立IP风险画像，提供6类信誉数据：DDos攻击、安全漏洞、垃圾邮件、Web攻击、扫描源、Botnet客户端； 17. 支持PCI-DSS V3.0符合性报表； 18. 支持XML基础校验，包括最大树深度、元素名长度、元素个数、子节点个数、属性值长度、文档大小等参数配置；支持Schema、SOAP校验，可根据会话标识、浏览器标识、用户名、服务器IP及端口、协议、时间进行会话跟踪，还原攻击场景。**提供功能截图进行佐证，并加盖原厂公章。** 19. 可根据已知自身业务地理分布的客户，对特定区域访问进行控制，有效拦截地域性的攻击 20. 基于机器学习和语义分析的智能检测引擎，提升SQL和XSS检测精度 21. 支持信息泄露防护，提供针对服务器状态码进行过滤和伪装的安全策略，可对响应码及响应文件进行设置； 22. 支持URL ACL。对多种HTTP方法执行访问控制，包括：GET、POST、HEAD、PUT、DELETE等； 23. 支持对攻击源地址的智能阻断，支持永久封禁或者自定义IP封禁时间（秒/分钟/小时），并且可以手工解除解禁。 | 2 | 套 |
| 下一代防火墙 | 1. 系统采用多核架构，专用安全操作系统，系统硬件为全内置封闭式结构，稳定可靠，标准机架尺寸，2U机型，含交流双电源，1个RJ45串口、2个GE管理口、2个USB接口、2个SFP+万兆光口、12个千兆电口，1个接口扩展槽位，每个槽位支持（4GE/4SFP/8GE/8SFP/2SFP+）,最高支持24个网络接口，电口均支持内置Bypass,三层吞吐不少于10Gbps，应用层吞吐量不小于6Gbps，最大并发不少于400万，每秒新建不少于10万。支持WEB界面设置静态路由及OSPF、RIP、BGP动态路由协议；支持基于源/目的地址、接口的、基于服务的策略路由 2. 支持虚拟线、二层透明、路由、混合、旁路监听、PPPoE等接入方式，适应各种网络环境需求。 3. 支持内置/自定义ISP路由库，支持SSL VPN、L2TP VPN 4. 支持基于策略的双向NAT、动态/静态NAT、端口PAT 5. 可通过移动端实现设备安全运维监控，APP支持安全设备运行状态监控，监控指标包括CPU使用率、内存使用率、设备IP地址，设备HASH，设备类型，设备状态，系统版本，规则库版本，证书终止时间。**提供以上原厂盖章功能界面截图及原厂官网APP下载截图进行佐证，并加盖原厂公章**。 6. 支持链路探测，能够在每接口上以ICMP/TCP/UDP协议探测目标主机可达性，探测链路是否有效 7. 支持对不少于2200种应用的识别和控制，至少支持5大类，比如：商业系统、协作应用、一般网络应用、媒体等及28子类，比如：认证服务、数据库、ERP-CRM、软件更新、电子邮件、VOIP视频、游戏等；支持自定义应用 8. 支持无线热点发现，发现内网私接无线热点，对无线热点进行管理,防止非法热点的接入 9. 支持设置应用超时时间，支持反向路由 10. 支持识别控制多种途径的文件传输及该途径传输的文件格式：比如能够识别控制腾讯QQ、MSN、新浪UC、网易PoPo等传输途径，并且能够识别控制腾讯QQ、MSN、新浪UC、网易PoPo中bmp、jif、jpeg、chm、exe、avi等文件格式的传输 11. 支持网页浏览、论坛发帖、电子邮件、即时通讯、文件传输、服务器操作等信息关键字的实时检测和过滤 12. 支持事件关联分析功能。管理员可以通过不同的数据分析模块，数据分析模块包括：源IP、目的IP、应用、用户、防火墙策略、入侵防护事件、URL事件、内容过滤事件、防病毒事件。对相关日志中包含的信息进行深入挖掘，获取自身需要的统计数据 13. 支持泛洪类攻击防护：UDP/DNS/SYN/PING 泛洪；支持ARP欺骗类攻击 14. 支持对多次身份验证失败的用户进行帐号、IP锁定或禁用及加验图形验证码 15. 可不通过主机扫描等技术，也不需要在主机上安装任何插件，即可识别内网主机的操作系统、杀毒软件、浏览器等信息，可自定义操作系统、浏览器、杀毒软件的风险等级，并支持预置风险等级。**提供功能截图进行佐证，并加盖原厂公章。** 16. 可生成内网资产风险报表，提供高风险资产top10，提供操作系统等相关资产信息的数据统计和报表展示 17. 支持对本地账户密码进行安全强制，包括最小长度，安全级别限制 18. 支持云端接入，可在云端监控设备的CPU、内存等信息，并可查看设备的安全等级及评分，能够在云端支持子账号授权，提供子账号接入云端管理安全事件 19. 支持配置向导功能，可针对常见组网配置提供指导以帮助管理员快速部署上线设备 | 1 | 套 |
| 数据库审计系统 | 1. 2U机架式（专用硬件平台），冗余交流电源，2GE板载管理口4GE板载接口，1×接口板卡插槽。32GB内存，1×6TB硬盘。标50个数据库(IP+Port)授权。标配20个RMAgent探针授权。纯数据库流量200Mbit，每秒入库量12000条/秒，峰值SQL吞吐量20000条/秒，在线会话6000个。 2. 旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计（不需要提供DBA账号和任何数据库账户，不需要创建任何数据库账户）。 3. 支持Oracle、SQL Server、Db2、Informix、PostgreSQL、Sybase ASE、Sybase IQ、MySQL、MongoDB、SAP HANA、MariaDB、Percona等主流数据库。 4. 支持Teradata、Cache、人大金仓、达梦、神通、南大通用、华为Guass等数据库审计。 5. 支持SSH或者KVM登录Oracle、MySQL、SQL Server数据库服务器后，直接执行的SQL操作的审计，不依赖于数据库自身审计功能。**提供功能截图进行佐证，并加盖原厂公章。** 6. 支持华为Guass DB 100、Guass DB 200数据库。 7. 支持跨语句、跨多包的绑定变量名及绑定变量值的审计；支持对超长SQL操作语句审计，可以正常记录单条长度小于等于2M字节的SQL语句内容。 8. 支持访问来源信息：客户端IP、端口、数据库名称、数据库用户、OS用户、访问工具、主机名称、MAC地址。 9. 支持应用身份信息：应用客户端IP、端口、应用用户名、应用URL标识、应用URL模板、URL、URL地址参数、URL消息体参数；支持数据库主机信息：数据库IP、端口、数据库名、服务名（实例）。 10. 支持SQL语句信息：SQL标识、操作类型（DDL、DML、DCL等）、影响行数、响应时间、语句捕获时间、执行结果（DB应答码、应答错误信息）、受影响对象、SQL语句、SQL语句模板、SQL参数、结果集；支持数据库单向\双向审计。 11. 支持数据库告警功能，支持对根据IP、账号、客户端工具名、时间等定制规则进行告警。 12. 所投产品的生产厂商具备挖掘国产品牌数据库漏洞能力，所挖漏洞被CNNVD或CNVD承认且具有编号，必须提供至少3个国外数据库漏洞编号，5个国内数据库漏洞编号。 13. 支持按照策略进行结果集审计，可以指定敏感表审计结果集。 14. 支持通过返回行数和内容大小控制返回结果集大小，降低系统开销。 15. 支持基于结果集的关键字检索。 16. 非时间戳的解析方式，采用应用端轻量级插件部署，在并发1000个连接的情况下，实现100%准确关联；以精确方式审计到应用端相关信息，支持应用用户和源IP的关联审计；支持Weblogic、Tomcat、Websphere、Jboss等主流的应用服务器；支持对F5等负载均衡模式下虚拟IP的识别，深入挖掘原始应用IP。 17. 内置安全特征库规则，如SQL注入、缓冲区溢出、权限提升、数据泄露、拒绝服务、访问操作系统、改密码、Bypass FGAC、修改FGAC、审计、游标注入、访问敏感组件、创建外部JOB、恶意代码、非系统用户执行命令等常规漏洞。 18. 具备公安部数据库安全审计类（增强级）检验报告。 19. 支持识别口令猜解攻击，以及在同一个会话里，相同IP、数据库用户的频次攻击告警。 20. 可自定义审计策略。审计策略至少支持20个条件，规则各条件之间支持与或非逻辑关系。 21. 结果集审计支持全局开启，也支持按照具体策略进行结果集审计开启的功能。 22. 告警数量需支持最大告警数量限制，超过告警阈值之后便不告警。 23. 支持基于时间、IP地址、数据库服务器IP地址、用户名、数据库操作命令、数据库表名，执行结果，应用用户、数据库服务（实例）名、报文关键字等多种丰富的查询检索条件；支持应用层关联审计查询和关联分析。 24. 支持不同审计账户，各自查看不同的数据库审计内容，要求：A账户不能看到B账户的数据库审计记录，B账户不能看到A账户的数据库审计记录，安全管理员可以看到所有的审计记录； 25. 支持将常用的查询条件保存成固定查询模板，方便后续快速查询。 26. 支持对查询结果中可能存在的敏感数据进行掩码处理，防止敏感数据泄露。 27. 支持对查询结果以CSV文件格式导出到本地。 28. 在同一套审计系统内可创建子账号，并对不同的子账号授予不同的数据库审计记录的查询检索权限，确保子账号之间彼此数据不可见，避免数据交叉泄露。 29. 支持SQL语句自定义业务化语言翻译。 30. 系统提供不少于40个报表模型，分别基于全库、数据库组和单库维度进行展现。 31. 支持合规性报表，如PCI、等级保护、SOX法案等专项报表展现。 32. 支持专项报表展现，针对风险、性能、访问源、账户等信息做专项报表展现。 33. 支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种统计图展现形式，基于总体概况、性能、会话、语句、风险多层面展现报表。 34. 支持按日、周、月等时间周期生成报表。 35. 支持报表数据后台定期预生成，保障报表数据展现速度。 36. 支持将报表按指定的时间推送至指定管理员的邮箱。 37. 报表支持以Word、PDF、HTML等格保存到本地。 38. 支持会话级检索和详情展现：包括在线的并发会话、活跃会话、失败登录会话等提供专项的分析界面。 39. 支持失败登录会话查询和统计：包括客户IP、数据库用户、操作系统用户、工具或应用、数据库应答码、失败原因和失败次数等信息。 40. 访问源分析：可展现不同数据库节点的访问源统计、分析状态。 41. 以操作类型为维度，统计表级别对象被访问次数，可生成行为轨迹图； 42. 并可通过对象的访问次数，下钻追溯到该表对象下所有的访问语句详情，以及该表对象访问来源。 43. 获取同一数据库不同时间段及不同数据库同一时间段的SQL语句量和会话量的对比统计数据以及变化趋势。 44. 可基于单个数据库建立学习期，默认学习期内行为可信认，学习期结束后，产生的数据标记为新型对象、新型语句模板。 45. 日志备份与恢复管理，支持审计日志数据的备份与恢复，支持自动备份，备份数据可以选择高性能或高压缩比，支持的备份服务器类型至少包含FTP、SFTP、NFS方式，备份记录可以查询。 46. 支持KAFKA、SYSLOG方式进行审计数据外送； 47. KAFKA外送审计数据内容包括：客户端IP、客户端端口、客户端MAC、数据库用户名、数据库实例名等会话信息，SQL语句参数、SQL捕获时间、结果集、语句模板、SQL语句等语句详细信息。 48. 支持客户端IP别名设置，针对不同客户端IP自定义别名展现。 49. 支持IP地址、数据库用户、时间、对象、应用用户分组，并且分组对象可以直接在规则中引用。 50. 审计设备WEB界面提供自动诊断功能，可以自动收集实例级参数、策略中心参数、操作系统参数、应用中间件参数。 51. 系统告警内容支持网卡异常、分区超限、异常关机、CPU超限、内存超限、会话超限、包数超限、SQL数超限、agent异常等。 52. 风险告警内容支持触发规则风险内容，并支持根据风险等级高、中、低进行告警通知。 53. 告警方式包括：邮件、短信、SYSLOG、SNMP、企业微信、审计系统前台界面；支持短信平台对接，发起告警操作。 54. 支持三权分立，系统默认设定系统管理员、规则配置员、审计查看员、操作日志查看员等角色，并且可以新建不同用户，分配不同数据库权限和不同的菜单管理权限。 55. 系统支持LDAP/AD域对接，支持AD域用户关联审计系统用户，通过AD域账户统一登录审计系统。 56. 支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址等信息，并且自动添加到审计范围，无需用户提供网段、数据库地址等信息。 57. 具有自身安全审计功能，可以对审计系统的所有用户操作进行审计记录。 58. 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》，数据库安全审计国标-增强级。 59. 产品支持IPv6，具有IPv6 Ready Logo认证。 | 1 | 套 |
| 安全培训服务 | 提供CISP认证培训 |  |  |

（二）商务部分

|  |  |
| --- | --- |
| **商务条款** | **商务要求** |
| 业绩合同 | 投标人投标供应商提供近三年（2017年5月1日至今，以  合同签订时间为准）类似项目业绩。  **投标文件中附清晰的合同复印件，加盖投标供应商公章** |

第四部分　项目内容清单及主要规格功能参数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 规格 | 功能 | 数量 |
| 1 | 态势感知平台 | 具备海量数据接入、存储、访问、计算能力，平台支持分布式部署方式，支持首次部署结束后根据负载要求灵活扩展，提高存储、计算能力，且不影响业务运行，部署模式支持集群部署且集群规模不低于100台  平台应支持多种协议的数据接入，包括但不限于FTP、SFTP、UDP、TCP、Netflow、本地文件系统  平台应支持配置灵活的解析规范化规则采集第三方安全设备日志，并实现异构日志格式归一化。  平台应支持灵活的配置选取接入协议、解析规范化规则完成数据接入，支持对数据接收、数据解析、数据存储速率进行监控并界面展示，支持配置允许接入日志的ip地址白名单，支持查看最近解析失败的原始日志  平台应支持多维度资产管理，进行多维度资产视图分析，系统至少内置五种视图：资产组视图、业务系统视图、组织结构视图、地理位置视图、行业视图  平台应支持对至少10000个网络资产进行发现探测，对暴露在互联网上的网络资产设施进行检查，包括但不限于资产核查、脆弱性检测、完整性检测、可用性检测和认证检测  平台应支持按照不同视图对资产信息进行统计包括各视图下节点数、各节点下资产数、各类型资产数等统计；  平台应支持资产稽查比对，对于实时发现资产和已有资产库资产比对分析资产新增、变更、减少的情况，变更分析需要细致到资产属性粒度，即可查看具体端口、服务的变化情况；并支持对资产发现结果进行处理，可选择入库或者丢弃  平台应支持对失陷资产进行判定，并提供失陷资产的统计和展示 | 基础平台节点（含一年威胁情报服务，自授权导入之日起开始计算）  日志威胁分析管理，收集安全设备等日志进行标准化处理与存储，针对收集日志数据进行威胁分析、汇总、展示，及时发现网络安全事件线索。  全流量威胁管理，针对流量探针上报的告警和流量元数据信息，利用规则检测和机器学习引擎能力，及时发现网络安全事件线索，及时检测病毒木马、网络攻击等安全事件情况。  异常行为分析管理，针对收集的日志数据进行基线检测，及时发现网络安全事件。  脆弱性管理，可向漏洞扫描探针、网站安全检测探针下发任务，并针对扫描产生的系统漏洞进行分析、汇总、展示。  网站安全检测，对网站安全监测系统、网站脆弱性监测系统、网站安全管理系统产生的监测日志进行汇总、分析。  安全编排自动化响应，提供案例管理、可视化编排、剧本管理、响应设备配置和运维自动化展示，可联动安全设备进行封堵或隔离，且支持封堵审批  基础服务包,包含平台系统升级授权、平台界面操作远程指导、模块功能使用咨询、平台升级指导,简单问题远程咨询和排查。 | 1套 |
| 2 | 流量探针系统 | 2U含交流冗余电源模块,8GCF卡,CPU\*1 Intel i7-2600 3.4GHz,16G内存,1T SATA硬盘,USB\*2,管理口RJ45\*1,RJ45串口\*1,板载1000M电口\*6(3组BYPASS),一个扩展插槽，网络吞吐2G。 | 支持导入HTTPS证书，对流量进行解密还原  支持对http、smtp、imap、pop3、ftp、telnet、dns、icmp、ssl、ldap、mssql、oracle等常见协议的深度解析和还原。  支持对工控和物联网协议的深度解析和还原，常见协议包coap,goose,Modbus,mqtt  支持流量灰名单，关注重点资产流量，对命中灰名单的流量进行还原和威胁检测。灰名单类型包括IP、端口、IP+端口、域名  支持对流量中出现的文件进行发现和还原，支持还原的协议包括：http、smtp、pop3、imap、ftp、webmail、samba  支持还原的可执行类型：bat、dll、sys、exe、com、src、pif。  支持还原的文档类型：doc/docx、xls/xlsx、ppt/pptx、pdf、rtf、 wpt、pot、wps、pps、mpp、et、dpt、dps、ett、dot。  支持还原的压缩包类型：zip、7z、rar、gzip、tar、bz。  支持还原的网页脚本类型：asp、js、jsp、html、phtml、xhtml、php 、htm、mhtml、 htx、 plg  支持对入侵检测告警、WEB应用告警、威胁情报告警和恶意文件告警中的攻击IP和受害IP发送阻断报文，进行旁路阻断  支持自定义一键封堵，配置策略包括IP类型（配置选项包括源ip/源端口/目的ip/ 目的端口）、域名类型、生效时间和失效时间 |  |
| 3 | Web防火墙 | 2U,含交流冗余电源模块,2\*USB接口,1\*RJ45串口,2\*GE管理口。1个2万兆SFPP插槽（不含光纤接口模块），3个可选扩展插槽位，可购买千兆（光、电）、万兆光链路扩展板卡，网络吞吐6G，应用吞吐3G，1T硬盘。 | 支持透明部署，旁路部署，反向代理模式以及镜像部署模式，支持HA的A/S部署模式，支持配置同步；  支持针对主流Web服务器及插件的已知漏洞防护。Web服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS等；插件应覆盖：dedecms、phpmuadmin、PHPWind、shopex、discuz、echsop、vbulletin、wordpress等；  支持非法文件上传防护，有效识别文件上传行为，并对上传行为的内容做安全检测，可以根据需要，禁止上传；  支持对注入、XSS、SSI指令、Webshell防护、路径穿越及远程文件包含的攻击防护。支持CSRF（跨站请求伪造）防护。提供盗链防护，支持Referer和Cookie算法；  支持基于五元组（源IP地址、目的IP地址、源端口、目的端口、协议类型）及接口的网络层访问控制功能；  支持爬虫防护，实现对100种以上的爬虫特征进行识别和阻断，防止页面因爬虫而引起信息泄露等问题；  支持敏感信息过滤，对用户的个人隐私信息（信用卡卡号、手机号、身份证号码）泄露进行检测、阻断或替换；  支持暴力破解防护，可针对指定URL进行暴力破解防护，可设置GET、POST登陆阀值、检测周期 | 2套 |
| 4 | 下一代防火墙 | 标准机架尺寸，2U机型，含交流双电源，1个RJ45串口、2个GE管理口、2个USB接口、2个SFP+万兆光口、12个千兆电口，1个接口扩展槽位，每个槽位支持（4GE/4SFP/8GE/8SFP/2SFP+）,最高支持24个网络接口，电口均支持内置Bypass,三层吞吐不少于10Gbps，应用层吞吐量不小于6Gbps，最大并发不少于400万，每秒新建不少于10万。 | 支持WEB界面设置静态路由及OSPF、RIP、BGP动态路由协议；支持基于源/目的地址、接口的、基于服务的策略路由  支持虚拟线、二层透明、路由、混合、旁路监听、PPPoE等接入方式，适应各种网络环境需求  支持内置/自定义ISP路由库，支持SSL VPN、L2TP VPN  支持基于策略的双向NAT、动态/静态NAT、端口PAT  支持泛洪类攻击防护：UDP/DNS/SYN/PING 泛洪；支持ARP欺骗类攻击 | 1套 |
| 5 | 数据库审计 | 2U机架式（专用硬件平台），冗余交流电源，2GE板载管理口，4GE板载接口，1×接口板卡插槽。  32GB内存，1×6TB硬盘。  标配50个数据库(IP+Port)授权。  标配20个RMAgent探针授权。纯数据库流量200Mbit，  每秒入库量12000条/秒，  峰值SQL吞吐量20000条/秒，  在线会话6000个, | 支持Oracle、SQL Server、Db2、Informix、PostgreSQL、Sybase ASE、Sybase IQ、MySQL、MongoDB、SAP HANA、MariaDB、Percona等主流数据库。  支持Teradata、Cache、人大金仓、达梦、神通、南大通用、华为Guass等数据库审计。  支持跨语句、跨多包的绑定变量名及绑定变量值的审计；支持对超长SQL操作语句审计，可以正常记录单条长度小于等于2M字节的SQL语句内容。  支持访问来源信息：客户端IP、端口、数据库名称、数据库用户、OS用户、访问工具、主机名称、MAC地址。  支持应用身份信息：应用客户端IP、端口、应用用户名、应用URL标识、应用URL模板、URL、URL地址参数、URL消息体参数；支持数据库主机信息：数据库IP、端口、数据库名、服务名（实例）。  支持SQL语句信息：SQL标识、操作类型（DDL、DML、DCL等）、影响行数、响应时间、语句捕获时间、执行结果（DB应答码、应答错误信息）、受影响对象、SQL语句、SQL语句模板、SQL参数、结果集；支持数据库单向\双向审计。  支持数据库告警功能，支持对根据IP、账号、客户端工具名、时间等定制规则进行告警。 | 1套 |
| 6 | 安全培训服务 | 无 | CISP认证培训 | 3人 |

# 第五部分 商务要求

1、响应人商务资信应按本招标文件第一部分所列的资格要求提供真实的证明文件，并加盖单位公章。

2、相应报价应按本竞争性招标文件第七部分招标响应文件格式中报价函的要求填写，并加盖单位公章。

报价注意事项如下：

（1）投标单位须按招标文件中响应文件格式要求填写固定总价。

（2）如投标单位响应报价严重偏离市场行情，或出现严重不平衡报价的，经招标小组评定，有权作废标处理。

（3）投标单位的报价应是承接本项目承包范围内的全部费用。

（4）本合同服务需交纳的一切税费包含在所报的固定总价中，不单独报价。

（5）投标单位的报价还应包括：管理人员和技术人员各项费用、现场费用、公司管理费、法定税金、利润及风险补偿等为完成本项目的全部费用。

（6）报价为一轮报价。

3、项目期限：合同签订后，首付款到账后开始采购设备以及软件开发，其中硬件设备到货周期：45天，软件开发周期：150天。

# 第七部分 招标响应文件格式

招标响应文件

项目名称：

单位（公章）

年 月 日

注：本封面格式仅做参考，不做强制要求。

一、自查表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 评审内容 | | 采购文件要求 | **自查结论** | **备注** |
| 资格性检查 | 投标/响应文件 | 按对应格式文件填写、签署、盖章(原件) | □通过  □不通过 |  |
| 法定代表人/负责人资格证明书及授权委托书 | 按对应格式文件签署、盖章(原件) | □通过  □不通过 |  |
| 回　执 | 在时间内回邮件（加盖公盖） | □通过  □不通过 |  |
| 准入条件  (关于资格的声明函) | 1．应具备《政府采购法》第二十二条规定的条件。  2．投标单位必须是在中华人民共和国境内注册并合法运作的组织机构，须具备提供采购货物的经营资格，并有能力提供完善的售后服务。  3. 投标单位须提供通过年检的营业执照副本复印件加盖单位公章。 | □通过  □不通过 |  |
| 其他要求 | 按响应资料清单中规定提供“必须提交”的文件资料 | □通过  □不通过 |  |

注：以上材料将作为投标单位合格性和有效性审核的重要内容之一，投标单位必须严格按照其内容及序列要求在招标文件中对应如实提供，对缺漏和不符合项将会直接导致无效！在对应的□打“√”。

投标单位法定代表人（或法定代表人授权代表）签字：

投标单位名称（签章）：

日期： 年 月 日

## 二、招标响应书

致：(采购单位)

依据贵方（采购项目名称）招标采购服务的招标邀请，我方将招标文件要求提交下述文件正本壹份，副本壹份。

1、自查表

2、报价函

3、资格证明等相关文件

4、满足质量保证要求承诺函

5、满足售后服务及技术支持要求承诺函

6、投标产品技术要求

7、其他材料

在此，我方声明如下：

1.同意并接受招标文件的各项要求，遵守招标文件中的各项规定，按招标文件的要求提供报价。

2.我方承诺在本次响应文件中提供的一切文件，无论是原件还是复印件均为真实和准确的，绝无任何虚假、伪造和夸大的成份，否则，愿承担相应的后果和法律责任。

3.我方完全服从和尊重评委会所作的评定结果。

投标单位名称(公章)：

投标单位（法定代表人授权代表）代表签字：

地址：

电话：

电子邮件：

**法定代表人/负责人资格证明书及授权委托书**

**（1）法定代表人资格证明书**

投标单位名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

单位性质：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

地址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

成立时间：\_\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日

经营期限：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

姓名：\_\_\_\_\_\_\_性别：\_\_\_年龄：\_\_\_职务：\_\_\_\_\_\_\_\_

系\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（投标单位名称）的法定代表人。

特此证明。

投标单位： (盖章)

年月日

**(为避免废标，请务必提供本附件)**

法人代表身份证

法定代表人身份证复印件

**（2）法定代表人授权委托书**

本人\_\_\_\_\_\_\_\_（姓名）系\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（投标单位名称）的法定代表人，现委托\_\_\_\_\_\_\_\_（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清、说明、补正、递交、撤回、修改\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（项目名称）响应文件、签订合同和处理有关事宜，其法律后果由我方承担。

委托期限：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

代理人无转委托权。

附：法定代表人身份证明

投标单位：（盖单位章）

法定代表人：（签字）

身份证号码：

委托代理人：（签字）

身份证号码：

年月日

说明：1.法定代表人为企业事业单位、国家机关、社会团体的主要行政负责人。

2.内容必须填写真实、清楚、涂改无效，不得转让、买卖。

3.将此证明书提交对方作为合同附件**。**

4.授权权限：全权代表本公司参与上述采购项目的投标/招标响应，负责提供与签署确认一切文书资料，以及向贵方递交的任何补充承诺。

5.投标/招标签字代表为法定代表人，则本表不适用。

代理人身份证复印件

代理人身份证复印件

**三、报价函**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 数量 | 单位 | 单价 | 总价 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 投标总价 | | | | | |

注：1、投标人所报单价应为包含采购、安装、调试、税金、验收、质保期服务、与货物有关的运输和保险及其他伴随服务的全费用单价；

2、以上表中各项可进一步细分，栏数不够可自加或附表；

3、投标人应按招标文件中采购货物技术参数一览表中所列货物填写本表；

4、投标人应根据采购货物技术参数一览表在本表后附相关技术证明文件并加盖投标单位公章。

投标人：

年 月 日

## 四、资格、资质证等相关资料

## 包括但不限于：

## 1、营业执照副本复印件

## 2、招标文件要求的其它资格证明文件

**注：以上文件都须加盖单位公章**