**终端高级威胁防护系统采购书**

一、项目情况

1. 项目名称：终端高级威胁防护系统采购。
2. 采购需求：详见附件二。
3. 投标金额：小于人民币98万元（含税）,其中,终端威胁检测响应系统小于38万元,网络流量沙箱系统小于60万元。投标金额包含投标人为提供本合同项下所有产品及服务所涉及到的所有费用，如税费等。
4. 投标保证金：人民币19600元。
5. 中标方式：根据本采购书“评分标准”对各投标文件进行评分，总分最高的投标人为第一中标候选人；总分相同的，投标价格较低者中标候选排序在先，价格也相同的，以随机抽取方式确定中标人。

二、商务要求

1. 投标人必须是在国内注册的独立法人或其他组织，提供营业执照（或事业单位、社会团体相关证书）的复印件（并加盖公章）。
2. 投标人必须能够提供上海本地化技术支持和服务。
3. 本项目最高投标限价98万元（投标价格为含税报价，包括提供本项目所有税费。本项目需开具增值税专用发票，如所提供的服务税率不同，须按照相应税率分别开具发票（合同金额不变）。其中，终端威胁检测响应系统低于人民币38万元；网络流量沙箱系统低于人民币60万元。 投标人除提交投标总价外，须提供两套系统分项报价（不得赠送）。
4. 付款方式：中标人需须开具增值税专用发票，并接受以下付款方式：

（1）合同签订后，支付合同总金额的30%；

（2）设备到货后，安装清点并加电无故障，支付合同总金额的40%，

（3）设备验收合格后上线，原厂服务生效（提供原厂服务生效证明）并验收无误后，支付合同总金额的20%；

（4）服务满一年，支付合同总金额的5%；

（5）方式A：中标人开具为期2年，金额为合同总金额5%的银行保函后（保函受益人为上海黄金交易所，且不可撤销），支付合同总金额的5%；方式B：三年维保到期后，支付合同总金额剩余的5%（A,B二选一）。

1. 投标人须提交投标保证金，投标文件中应附有投标保证金的付款有效凭证复印件。
2. 开标后投标人在投标有效期内撤回投标；或因投标人的原因对本次招标工作造成较严重后果的；或投标人在中标通知书发放后10天内不与招标人签订合同的，招标人有权不予退还投标保证金，且取消相关投标人的中标资格。
3. 本项目不支持联合体投标，本项目不得转包或分包。
4. 投标人在招标过程中参与围标、串标或陪标等舞弊或作假行为的，一经核实，招标人有权要求其2年内不得参与招标人系统内任何招标采购工作。同时，对已中标的上述作假行为投标人，应取消其中标资格并不予返还投标保证金；对已签订合同的，则视为违约，违约金比例为合同金额的20%，守约方有权终止合同，违约方须返还已经收到的全部合同款项。若因上述情况造成招标人或守约方其他损失的，须进行赔偿。
5. 投标有效期：从提交投标文件的截止之日起算不少于90天。
6. 投标人未被“信用中国”网站（www.creditchina.gov.cn）列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单。投标人需提供递交投标文件截止日期前一个月内通过“信用中国”网站（www.creditchina.gov.cn）“信用服务”栏对投标人“失信被执行人”、“重大税收违法失信主体”、“政府采购严重违法失信行为记录名单”情况的查询记录截图，截图要求显示查询时间。如未提供有效截图，投标文件将被否决。如查询期间跳转非“信用中国网站”，以最终跳转的网页查询记录截图为准。提供内容如下:

①“失信被执行人”情况查询记录截图（须包含投标人全称、查询结果及查询时间）

②“重大税收违法失信主体”情况查询记录截图（须包含投标人全称、查询结果及查询时间）

③“政府采购严重违法失信行为记录名单”情况查询记录截图（须包含投标人全称、查询结果及查询时间）

1. 投标人参与投标表示同意上述所有条款。

三、响应文件

响应文件应由：商务报价文件，商务响应文件（证明其为合格服务商的有关资格证明文件，采购文件要求提供的其他资料），技术响应文件（针对本项目的技术或服务偏离说明表，采购文件要求提供的其他资料）。

1. **响应人的商务报价文件至少应包括以下内容（均需加盖公章）**
2. 报价单**（可单独密封）**。
3. **响应人的商务文件**

响应人提交的证明其有资格进行投标且有能力履行合同的资格证明文件应包括下列文件（未提供相应材料或材料无效者以废标计）：

1. 法定代表人（投资人/负责人）授权书（格式见附件一），法定代表人及授权委托人的身份证；
2. 提供有效的营业执照、税务登记证、组织机构代码证；或上述证件的三证合一件，以上均为加盖公章后的原件复印件。
3. 投标保证金的付款有效凭证复印件。

投标保证金应当从投标人的基本账户转出，并写明账户信息，如开户行以及账号等，并在银行付款备注栏中注明该投标保证金所对应的项目名称。

**上金所账户信息：**

**单位名称：上海黄金交易所**

**开户银行：中国工商银行浦东分行**

**账号：1001280909000000163**

1. 提交针对商务要求的响应。

针对商务条款响应表参考格式如下：

**商务条款响应/偏离表**

响应人名称：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 商务条款 | 响应 | 是否偏离 | 说明 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

响应人代表签字：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（盖章）

1. 其他响应人认为有必要提供的资料。
2. **响应人的技术文件**
3. 投标人本次服务方案。
4. 响应人提交的针对招标需求的响应。参考格式见下表：

**规格、技术参数响应/偏离表**

响应人名称：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 招标要求 | 投标规格 | 响应/偏离 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

响应人代表签字：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（盖章）

1. 其他响应人认为有必要提供的资料。
2. **响应文件要求**

响应人的响应文件必须按照采购书要求制作。

四、评分标准

评分标准详见附件三

五、采购程序安排

1. 递交投标文件截止时间

2024年8月22日16：00前，响应单位将响应文件加盖公章并密封后(一式3份，正本1份，副本2份)并附联系人名片，**送至上海黄金交易所采购办**（上海市黄浦区中山南路699号912），接收人：陈佳士，021-33128863。请附上联系人名片。

1. 投标人须根据招标人要求提交投标文件的电子版本。

上海黄金交易所

2024年8月14日

六、附件

## 附件一：授权书

**法定代表人（投资人/负责人）授权书**

本授权书声明：注册于*国家或地区的名称*的*公司名称*的*法定代表人姓名（投资人/负责人）* 代表本公司授权 *单位名称*的*被授权人的姓名* 为本公司的合法代理人，参加“*项目名称*”项目的投标及合同签订执行，以本公司名义处理一切与之有关的事务。

本授权书经法定代表人（投资人/负责人）及代理人签字(或盖章)并加盖单位公章后生效。

法定代表人（投资人/负责人）签字或盖章：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

代理人（被授权人）签字或盖章：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

单位名称（盖章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

注：授权书空格项均为必填项，未满足上述要求的授权书视为无效授权，所投标书以废标计；**另附上提供法定代表人（投资人/负责人）和被授权人身份证正反面的复印件。**

## 附件二：采购需求

**一、需求概述**

根据上海黄金交易所终端高级威胁防护系统项目需求，需要采购如下设备:

|  |  |
| --- | --- |
| **设备** | **数量** |
| 终端威胁检测响应系统 | 3套 |
| 网络流量沙箱系统 | 1套 |

**二、技术需求**

1. 基本需求：

1）投标商品须为原厂全新产品，无任何翻新、返修等情况；

2）投标商品须使用符合国内自主可控技术的CPU和操作系统；

3）投标商品须带3年原厂现场支持服务，3年原厂硬件维保24\*7\*4服务，3年原厂软件更新和技术支持服务；除原厂服务外投标商还需提供供应商服务，服务期与原厂一致；

4）所购设备需配置C13-C14接口电源线；

5）投标商提供设备的安装，调试工作；

6）投标商需协调原厂商完成交易所要求的测试内容，测试设备由投标商提供，测试设备的硬件型号、软件版本及功能许可等须与后续交货设备完全一致，测试须按照交易所要求的测试内容进行，测试结果由交易所、投标商及原厂商三方确认。如测试不通过，视为投标商违约，交易所有权解除合同并不承担任何责任。（测试内容见附录1）

7）投标商须确保本次投标设备相关的配置和数据等信息仅用于解决交易所的设备问题，且不得将相关信息传到境外。

8）服务地点：上海。

1. 设备性能和功能需求：

**（1）终端威胁检测响应系统**

|  |  |
| --- | --- |
| **功能** | **技术规格要求** |
| 设备硬件规格 | 1G电口数量≥4个；万兆光接口（包含多模光模块）≥2个； |
| 内存≥64G;600G\*2以上的SSD固态raid阵列，4\*1T以上的SATA机械硬盘阵列； |
| 支持电源可热插拔； |
| 设备硬件尺寸≤2U； |
| 设备电源冗余； |
| 硬件数量及终端许可数量（含国产终端） | 每套终端威胁检测响应系统需要至少1台硬件服务器，3套系统总终端许可数不低于1000个（许可有效期3年）； |
| 设备要求 | 基于B/S的管理架构，Web界面支持主流浏览器； |
| 具备网页接口账号管理机制，并提供个别用户可自行设定操作接口； |
| 允许多位用户同时登入系统； |
| 支持本地认证与第三方外部认证（如RADIUS、TACACS）； |
| 本地集成能力 | 可提供开放的Web API接口对接网络流量沙箱系统，并根据沙箱反馈的结果进行全网威胁信息更新； |
| 操作系统适配 | 客户端至少支持操作系统类型：银河麒麟，Windows； |
| 基础功能 | 可以通过管理控制台识别客户端的操作系统、体系架构、IP地址、MAC地址等信息，并进行管理； |
| 控制中心支持对客户端多级分组管理，支持多级分组的创建、删除、移动至新分组； |
| 提供灵活的策略管理能力，支持下发全局策略以及分组策略； |
| 支持客户端的防卸载功能，避免用户自行卸载，管理员可设置卸载密码； |
| 支持在线、离线两种更新方式； |
| 平台保留扩展能力，可根据需求开放接口与第三方平台联动对接； |
| 防病毒模块 | 产品能够实时监控并清除来自各种途径的病毒、木马、蠕虫、恶意软件、勒索软件、黑客工具等恶意威胁； |
| 产品需具有防病毒引擎，且提供更新； |
| 支持检测全局可疑站点（C&C)识别，监控可疑站点的连接，并提供记录或者阻止的处理措施； |
| 具备将可疑文件提交沙箱设备的联动能力，可自动提交可疑恶意文件，并可接收沙箱返回的分析情报； |
| 检测与响应模块 | 基于需求，可配置探针记录内容（进程，网络，注册表和系统事件等）；对“勒索事件”和“挖矿事件”进行热点事件的专项统计； |
| 支持对用户普遍关心和危害程度高的威胁，提供专项检测和结果呈现，包括“暴力破解、Shell反弹、WebShell、PowerShell、本地提权、文档漏洞利用”； |
| 提供远程遏制终端给管理员，仅保留终端与服务器的连接，有效避免威胁蔓延； |
| 支持网络封停自动化响应动作：支持配置自动响应的时间段，即生效周期和生效时间，支持设置封停时长。自动封停后的IP记录在封停列表，封停时长过后自动解封； |
| 系统管理 | 支持SNMP等多种组合报警方式； |
| 采用Syslog日志格式，支持分级和按类型输出以及日志加密传输； |
| 自动提供经过分析后的图形化日/周/月报表； |

**（2）网络流量沙箱系统**

|  |  |
| --- | --- |
| **功能** | **技术规格要求** |
| 设备硬件规格 | 不少于2台硬件设备组成的硬件集群（该集群需具备业务高可用性）； |
| 1G电口数量≥2个，万兆光接口（包含多模光模块）≥2个； |
| 内存≥64G，硬盘≥4T； |
| 支持电源可热插拔； |
| 设备硬件尺寸≤2U； |
| 设备电源冗余； |
| 设备要求 | 支持并发处理文件≥20个； |
| 基于B/S的管理架构，Web界面支持主流浏览器； |
| 具备网页接口账号管理机制，并提供个别用户可自行设定操作接口； |
| 允许多位用户同时登入系统； |
| 支持本地认证与第三方外部认证（如RADIUS、TACACS）； |
| 文件分析能力 | 支持文档、URL、IP、Domain 4种可疑威胁对象的分析； |
| 通过可视化中心或报表可以查看详细样本活动及外联通讯等全部分析结果； |
| 沙箱能够对未知漏洞利用代码和恶意程序的行为进行动态分析； |
| 对提交的可疑URL利用沙箱执行页面扫描、动态链接分析、动态脚本及控件分析，并针对URL指向的可疑文件进行沙箱分析； |
| 本地集成能力 | 可提供开放的Web API接口给终端威胁检测响应系统提交可疑威胁样本，分析完成后将结果及时反馈至终端威胁检测响应系统；可根据需求提供接口给其他第三方产品或授权人员提交样本进行检测； |
| 设备可与交易所在用邮件安全网关（亚信DDEI）进行对接，将沙箱分析后的特征库和威胁情报等实时输入至邮件安全网关，允许邮件安全网关将可疑文件发送至设备进行检测； |
| 系统管理 | 支持SNMP等多种组合报警方式； |
| 采用Syslog日志格式，支持分级和按类型输出以及日志加密传输； |
| 自动提供经过分析后的图形化日/周/月报表； |
| 可支持自定义定制监控大屏模板； |

**三、服务需求（SLA）（原厂+第三方服务）**

| 一、服务频率 | | | |
| --- | --- | --- | --- |
| 序号 | 服务内容 | 频率 | 备注 |
| 1 | 巡检频率和次数 | 每季度1次，全年4次。 | 供应商。 |
| 2 | 故障处理 | 故障发生时处理。 | 不限次数；按招标方要求，由供应商或原厂提供服务。 |
| 3 | 系统变更、项目上线技术保障 | 系统变更或项目上线时，派遣技术保障人员，进行技术保障工作，保障起止时间根据甲方的要求。 | 按招标方要求，由供应商或原厂提供服务。 |
| 4 | 高危病毒爆发期、国家重大会议期和重大任务期间的保障 | 在高危病毒爆发期、国家重大会议期和重大任务期间进行保障，技术保障人员(A\B角)进行技术保障工作，提供应急响应电话，当客户出现技术问题时，及时到达现场解决问题，保障起止时间根据甲方的要求。 | 按招标方要求，由供应商或原厂提供服务。 |

|  |  |  |  |
| --- | --- | --- | --- |
| 二、响应时间 | | | |
| 序号 | 服务内容 | 响应时间 | 备注 |
| 1 | 故障处理响应时间 | 接招标方通知后2小时内到达现场，1个自然日内排除故障，故障排除后3个自然日内提交《故障应急处理和分析报告》。 | 按招标方要求，由供应商或原厂提供服务。 |
| 2 | 技术咨询响应时间 | 接招标方咨询请求后1个工作日内答复。 | 按招标方要求，由供应商或原厂提供服务。 |
| 3 | 巡检报告 | 巡检结束3个工作日内提供。 | 按招标方要求，由供应商或原厂提供服务。 |
| 4 | 技术变更的评估响应时间 | 接招标方请求后2个工作日内答复。 | 按招标方要求，由供应商或原厂提供服务。 |
| 5 | 硬件替换送达招标方的时间节点 | 购买24\*7\*4服务，确认设备硬件故障后供应商半小时内向厂商报障，在厂商受理申请并生成故障处理单号后如需进行替换处理的，替换件需在4小时内到场。 | 按招标方要求，由供应商和原厂共同提供服务。 |

|  |  |  |  |
| --- | --- | --- | --- |
| 三、服务日历 | | | |
| 序号 | 服务内容 | 服务时间 | 备注 |
| 1 | 电话支持 | 7\*24 | 按招标方要求，由供应商或原厂提供服务。 |
| 2 | 邮件支持 | 7\*24 | 按招标方要求，由供应商或原厂提供服务。 |
| 3 | 现场服务 | 非故障时5\*9（工作日）；故障时根据招标方要求。 | 按招标方要求，由供应商或原厂提供服务。 |

附录1

1. **测试目的**

为了确保中标设备在性能和功能性等方面符合交易所的预期要求，待合同签订后，需对中标设备进行验证测试。

1. **测试环境**
2. 硬件设备

交易所可提供测试所需要的交换机及PC，中标方提供中标设备。

1. 测试拓扑

按测试案例拓扑进行测试。

1. 测试工具

中标方提供通用性测试工具。

1. 测试时间

测试时间为2周。

1. **功能测试**

**终端威胁检测响应系统**

|  |  |
| --- | --- |
| **测试目的** | 验证终端威胁检测响应系统客户端操作系统适配性。 |
| **测试说明** | 验证终端客户端是否适配交易所在用的麒麟、windows终端，能否识别终端的操作系统、体系架构、IP地址、MAC地址等基础信息。 |
| **测试环境** | 测试拓扑如下：    预制条件：  1.我所提供测试麒麟、windows终端；  2.配置IP地址，PC能与测试设备正常通信，测试设备间能够正常通信。 |
| **测试步骤** | 1.分别在麒麟、windows终端安装终端客户端；  2.验证服务端能否管理测试客户端并识别终端相关基础信息。 |
| **实测结果** |  |
| **测试结果** | □通过 □部分通过 □失败 □未测试或不支持 |
| **备 注** |  |

|  |  |
| --- | --- |
| **测试目的** | 验证终端威胁检测响应系统的病毒防护能力。 |
| **测试说明** | 由交易所提供恶意文件样本，验证终端威胁检测响应系统的病毒防护能力。 |
| **测试环境** | 测试拓扑如下：    预制条件：  1.我所提供测试麒麟、windows终端；  2.配置IP地址，PC能与测试设备正常通信，测试设备间能够正常通信。 |
| **测试步骤** | 1.分别在麒麟、windows终端提交恶意文件；  2.验证终端威胁检测响应系统能否识别并处置相关恶意文件。 |
| **实测结果** |  |
| **测试结果** | □通过 □部分通过 □失败 □未测试或不支持 |
| **备 注** |  |

|  |  |
| --- | --- |
| **测试目的** | 验证终端威胁检测响应系统的检测响应能力。 |
| **测试说明** | 验证终端威胁检测响应系统的检测响应能力。 |
| **测试环境** | 测试拓扑如下：    预制条件：  1.我所提供测试麒麟一台、windows终端两台（攻击机和靶机）；  2.配置IP地址，PC能与测试设备正常通信，测试设备间能够正常通信。 |
| **测试步骤** | 1.使用攻击机分别针对麒麟和windows终端进行漏洞扫描攻击；  2.威胁检测响应系统服务端查看攻击日志；  3.通过响应模块开启响应能力（封锁攻击机攻击）。 |
| **实测结果** |  |
| **测试结果** | □通过 □部分通过 □失败 □未测试或不支持 |
| **备 注** |  |

**网络流量沙箱系统**

|  |  |
| --- | --- |
| **测试目的** | 验证网络流量沙箱文件分析能力。 |
| **测试说明** | 验证沙箱支持文档、URL、IP、Domain 4种可疑威胁对象的分析，通过可视化中心或报表可以查看详细样本活动及外联通讯等全部分析结果，能够对未知漏洞利用代码和恶意程序的行为进行动态分析，对提交的可疑URL利用沙箱执行页面扫描、动态链接分析、动态脚本及控件分析，并针对URL指向的可疑文件进行沙箱分析。 |
| **测试环境** | 测试拓扑如下：    预制条件：  1.我所提供文档、URL、IP和Domain4类可疑威胁对象实体。 |
| **测试步骤** | 1.登录服务端，分别提交验证文档、URL、IP和Domain4类可疑威胁对象实体；  2.访问可视化中心，查看各类可疑威胁对象的分析统计结果。 |
| **实测结果** |  |
| **测试结果** | □通过 □部分通过 □失败 □未测试或不支持 |
| **备 注** |  |

|  |  |
| --- | --- |
| **测试目的** | 验证网络流量沙箱设备性能。 |
| **测试说明** | 验证沙箱能否达到并行至少20个文件的处理性能。 |
| **测试环境** | 测试拓扑如下：    预制条件：  1.我所提供可疑威胁对象实体。 |
| **测试步骤** | 1.登录服务端，同步提交20个可疑威胁对象实体；  2.访问可视化中心，查看各类可疑威胁对象的分析统计结果。 |
| **实测结果** |  |
| **测试结果** | □通过 □部分通过 □失败 □未测试或不支持 |
| **备 注** |  |

|  |  |
| --- | --- |
| **测试目的** | 验证网络流量沙箱特征库、情报共享能力。 |
| **测试说明** | 验证沙箱特征库、情报共享能力，要求将沙箱特征库、情报共享至交易所邮件安全网关。 |
| **测试环境** | 测试拓扑如下：    预置条件：  1.所有测试设备正常启动；  2.配置IP地址，PC能与测试设备正常通信，测试设备间能够正常通信。 |
| **测试步骤** | 1.登录服务端，配置邮件安全网关与沙箱联动策略，并开启威胁情报共享；  2.手动往沙箱系统上传恶意样本；  3.发送具有相同威胁情报特征的附件邮件；  4.登录邮件网关服务端，查看威胁情报生效情况。 |
| **实测结果** |  |
| **测试结果** | □通过 □部分通过 □失败 □未测试或不支持 |
| **备 注** |  |

**威胁检测响应系统与网络流量沙箱系统联动**

|  |  |
| --- | --- |
| **测试目的** | 验证威胁检测响应系统与网络流量沙箱系统联动能力。 |
| **测试说明** | 验证终端威胁检测响应系统具备与沙箱系统联动，针对终端恶意文件通过沙箱进行动态分析，并获取分析后的结果。 |
| **测试环境** | 测试拓扑如下：    预制条件：  1.所有测试设备正常启动；  2.威胁检测响应系统服务端与沙箱系统正常通信。 |
| **测试步骤** | 1.登录威胁检测响应系统管理后台；  2.启用威胁检测响应系统中沙箱系统虚拟平台提交可疑文件；  3.终端制定目录放置可疑文件；  4.分别登录沙箱系统和威胁检测响应系统管理后台查看分析结果和获取IOC后处置可疑文件结果。 |
| **实测结果** |  |
| **测试结果** | □通过 □部分通过 □失败 □未测试或不支持 |
| **备 注** |  |

## 附件三：评分标准

**项目评分标准**

**一、评标原则：**

1. 采用“百分制评标法”，分别对技术需求与商务需求进行评分，其中价格评分为30分，商务技术评分为70分。
2. 对所有投标人的投标评估，评委都采用相同的程序和标准。
3. 所有投标产品为同品牌且同型号的两个以上投标人，先对该品牌投标人进行评分，得分最高的同品牌(及型号)投标人获得中标候选人推荐资格继续参加评审,其他同品牌(及型号)投标按无效处理；评审得分相同的，以投标价格较低的投标人获得继续评审资格，价格相同的则以随机方式抽取,合并投标后有效标书数量少于3家，项目按流标处理。
4. 对采购书及评分标准的理解出现争议时，其最终解释权在招标人。
5. 若所有的有效投标经评分后,商务技术得分大于等于42分的投标少于1家，本次招标做流标处理。
6. 综合得分按照由高到低排序并作为中标候选人选用顺序，评标委员会推荐排名第一的投标人为中标候选人，出现得分并列时，以投标价格较低的投标人为第一中标候选人，价格相同的则由评标委员会随机抽取中标人推荐资格。

**二、符合性检查：**

凡出现下列情况之一者，予以废标：

投标书不符合本招标文件规定的要求或者未按照本招标文件规定提供各类文件、资质证书者；

投标人未提交投标保证金或金额不足；

投标材料未按照招标要求加盖公章，或法定代表人（法定代表授权的代理人）未签字；

代理人无法定代表人出具的授权委托书；或没有出具法定代表人和代理人身份证复印件者（要求清晰可辨）；

超出经营范围投标的；

投标有效期不满足采购书要求的；

投标文件未能满足本采购书“**商务要求”**及本采购书附件2 **“采购需求”**要求全部条款者；

投标总价格大于或等于小于人民币98万元（含税）的,或终端威胁检测响应系统大于或等于38万元的,或网络流量沙箱系统大于或等于60万元的；

递交两份或多份内容不同的投标文件，或在一份投标文件中对同一招标内容报有两个或多个报价，且未声明哪一个为最终报价的（按采购书规定提交备选投标方案的除外）；

附加条件的报价（除采购书中有规定外）；

投标人虚假投标，提供的投标文件与事实不符；或在澄清过程中虚假澄清，提供的澄清文件与事实不符；

开标后，投标人提出降价或进行抬价或利用澄清机会实质性变更投标价的；

投标人复制采购书的技术规格相关部分内容作为其投标文件的一部分的；

招标过程中投标人存在作假或舞弊行为的；

有其他违法违规情形的或符合采购书规定的其他废标条件的。

**三、评标标准**

* + - 1. 以各有效投标的含税投标总价作为评标价。
      2. 以各评标价的最低价作为评标基准价。
      3. 如某投标人的评标价低于所有评标价平均值的比例超过25.11%（含），需在评标委员会要求的时间内提供书面说明，证明其能够诚信履约并承诺中标后提供采购文件规定以外的履约担保，否则评标委员会应当将其作为无效投标处理。
      4. 价格评分=(评标基准价/评标价)×30
      5. 价格评分保留小数点后两位，第三位四舍五入。

**四、商务技术评分**

评委对各份投标书根据以下内容进行分析评定后各自打分。为使评分时能体现量化，评委按以下内容进行评定后打分，各项得分合计后计算算术平均值后为各投标人的最终得分。

具体评分方式见下表：

|  |  |  |
| --- | --- | --- |
| **评标要素** | **评分项** | **分值** |
| 厂商要求 | 1、投标人所投的终端威胁检测响应系统提供国家机构颁发的计算机软件著作权登记证书的2分；  2、投标人所投的网络流量沙箱系统提供国家机构颁发的计算机软件著作权登记证书的2分。  **(须提供证书复印件)** | 4 |
| 1、投标人所投的终端威胁检测响应系统设备厂商具备CCRC信息安全服务信息系统安全运维服务一级资质得3分，二级得2分，三级得1分；  2、投标人所投的网络流量沙箱系统设备厂商具备CCRC信息安全服务信息系统安全运维服务一级资质得3分，二级得2分，三级得1分。  **(须提供证书复印件)** | 6 |
| 设备要求 | 根据所投的终端威胁检测响应系统支持的除银河麒麟、windows以外的操作系统种类丰富度进行评分，每类操作系统得1分，满分3分。**（需提供承诺函）** | 3 |
| 根据所投的网络流量沙箱系统能够识别的漏洞利用代码和恶意程序的行为（进程操作行为、文件操作行为、系统配置操作行为、网络通信行为等）丰富程度进行评分，每种行为得1分，满分4分。**（需提供证明材料）** | 4 |
| 根据所投的网络流量沙箱系统支持监测的文件类型（如压缩文件、可执行文件、办公文档、脚本、Web页面等）丰富度进行评分，每个类型得1分，满分5分。  **（需提供证明材料）** | 5 |
| 根据所投的网络流量沙箱系统支持的操作系统镜像种类（如银河麒麟、windows、UOS、Ubuntu等）丰富度进行评分，每个种类得1分，满分4分。  **（需提供证明材料）** | 4 |
| 资质要求 | 1、投标人具备ISO20000信息技术服务管理体系认证证书的得2分；  2、投标人具备ISO27001信息安全管理体系认证证书的得2分；  3、投标人具备信息系统建设和服务能力评估CS认证证书(三级及以上）的得2分。**（需提供认证证书复印件）** | 6 |
| 业绩要求 | 1、投标人提供自2021年1月1日起,所投终端威胁检测响应系统同系列设备销售案例，每个合同案例得1分，满分5分。  2、投标人提供自2021年1月1日起,所投流量沙箱分析系统同系列设备销售案例，每个合同案例得1分，满分5分。  **（合同可不为投标人签署；投标人须提供合同案例销售设备与本次投标设备属同一系列的说明;合同无签署日期不得分；合同标的不与投标产品相关，不得分）** | 10 |
| 实施方案 | 项目方案中，具备详实有效的安装实施方案，方案技术路线明确合理，操作步骤详细具体，可执行性强的，得0-5分。 | 5 |
| 项目方案中，有根据项目特点定制的资源管理计划的，计划中包含细化的人员调配方案，包含合理、步骤清晰的设备调试配置方案的，得0-5分。 | 5 |
| 项目方案中，具备有效且根据项目特点定制的验收方案，验收方案中详细描述验收条件、验收时间及验收步骤等要素的，得0-5分。 | 5 |
| 项目方案中，包含详细的售后保障方案，售后保障全面，处理流程清晰、贴合需求，得0-5分。 | 5 |
| 实施团队资质 | 投标人投入到本项目的项目经理至少1人，视相关工作年限、履历及是否具备PMP证书，得0-3分，满分3分。（提供履历、PMP证书复印件并加盖投标人公章）。  注：投标人须提交人员流动承诺，承诺所提交本项目团队人员在未得到招标人同意的前提下不做更换。无承诺不得分。（须提供承诺函并加盖公章） | 3 |
| 投标人投入到本项目进行集成工作的工程师视相关工作年限及履历得0-3分，满分3分。**注：本项须配合提交人员流动承诺，承诺所提交本项目工程师在未得到招标人同意的前提下不做更换。无承诺不得分（须提供承诺函）。** | 3 |
| 投标人和原厂投入到本项目的工程师持有网络安全方面认证证书，视证书与本项目相关度进行综合评判，每份证书得1分，满分2分。（需提供相应证书复印件） | 2 |

注：

1. 评分标准中涉及证明材料的，均需提交有效期内的清晰复印件，否则不得分。

2. 请投标人注明投标文件中响应评分细则的位置和页码数。

## 附件四：合同

**上海黄金交易所**

**终端高级威胁防护系统**

**采购合同**

**项目： 终端高级威胁防护系统采购项目**

**终端高级威胁防护系统采购合同**

**甲方（买方）： 上海黄金交易所**

地址： 上海中山南路699号

电话： 021-33189588

**乙方（卖方）：**

地址：

电话：

1. **为保护本合同各方的合法权益，根据《中华人民共和国民法典》等国家法律法规及规范性文件的规定，并严格遵循招标文件的相关要求，甲方和乙方订立本合同，以兹信守。**
2. **合同总金额与货物明细**
   1. 合同总金额（含税）：**¥元（大写：人民币元整）**
   2. 上述合同总金额包括了为实施本项目所需的所有硬件和服务（如有）费用，乙方须按照硬件和服务类别，及其适用税率，分别开具发票，不得额外追加费用。
   3. 货物明细（见附件一，乙方承诺所提供的货物和服务能够满足甲方招标要求和乙方投标书承诺的全部内容，如有不符构成违约、按照本合同的违约条款处理）
   4. 货物到货验收（见附件二）
   5. 货物安装验收（见附件三）
   6. 其他要求（见附件四）

**三、付款方式**

1、甲方按照以下付款方式在收到乙方每一笔款项的合法增值税专用发票后30个工作日内向乙方转账支付相应金额款项。

2、付款方式：

（1）合同签订后，甲方支付合同总金额的30%；

（2）设备到货后，安装清点并加电无故障，甲方支付合同总金额的40%，

（3）设备验收合格后上线，原厂服务生效（提供原厂服务生效证明）并验收无误后，甲方支付合同总金额的20%；

（4）服务满一年，甲方支付合同总金额的5%；

（5）方式A：乙方开具为期2年，金额为合同总金额5%的银行保函后（保函受益人为上海黄金交易所，且不可撤销），甲方支付合同总金额的5%；方式B：三年维保到期后，甲方支付合同总金额剩余的5%（A,B二选一）。

甲方账户信息：

单位名称：上海黄金交易所

开户银行：工行浦东分行

开户账号：1001280909000000163

税号：91310000736228569K

乙方账户信息：

单位名称：

开户银行：

开户账号：

乙方于此承诺，在本合同履行期间保证上述所载之乙方银行账户不变。如对前述银行账户信息确需变更的，乙方应当提前7个工作日书面通知甲方且经甲方确认知悉后，方可视为该银行账户变更成功。如因乙方提供的账户信息错误或未经前述约定之有效变更程序，导致甲方不能按照本合同约定付款或付款未成功的，甲方将不承担任何责任。

**四、交货及安装事宜**

1、交货时间：合同签订后的 30 个自然日内完成供货

2、交货信息：

（1）甲方指定本合同项下货物的收货单位（人）全称为： 上海黄金交易所 ；货物收货地址为：

（2）甲方指定的联系人的姓名及联系方式为：

（3）乙方指定的联系人的姓名及联系方式为：

3、运输方式以及运费承担：乙方负责货物到合同指定的交货地点的运输，并承担货物的运输风险。

4、非甲方原因延宕，产品交付、清点并加电验收通过后的15个工作日内，乙方须按需协调原厂共同按照甲方要求完成所有产品的集成安装工作。

**五、包装标准、品质保证**

1、乙方提供的货物为原厂商包装，包装按原厂商的有关规定执行，解释权归原厂商，安装集成服务由乙方协调原厂共同执行，甲方提供必要的安装条件支持。

2、乙方交付甲方的本合同项下的货物均须符合原厂商的相关技术规范。

3、乙方向甲方承诺：本方向甲方承诺的产品及服务均为原厂正品，乙方确保甲方可以享受原厂保修服务，在规定的质量保证期内，乙方确保原厂对设计、工艺和材料等缺陷而造成的任何问题或故障负责。一旦发生上述质量问题或故障等情况，由乙方负责协调原厂处理，并确保原厂及时、免费更换有问题的整机，如原厂无法按上述约定进行保修及更换，由乙方向甲方承担责任。除合同另有规定外，在质保期内如出现上述情况，乙方应在收到甲方通知后5个工作日内，协调原厂免费负责更换有缺陷的整机。

4.乙方承诺，准许甲方在履行本合同过程中，出于合同目的的使用乙方权利框架内的知识产权及各项关联权利。

**六**、**验收**

1. 验货标准：货物在品牌、规格、型号、数量和包装上符合原厂商的标准以及本合同第二款与第五款的约定。
2. 乙方向甲方提供验收单（见附件二），甲方在货物到达交货地点后 15 个工作日内进行货物验收。验收时，须由甲乙双方共同对货物进行清点并加电试运行，清点无误，加电无故障，则视为本项验收通过；若由于非乙方原因导致逾期10个工作日仍未验收，视为此项验收通过。甲方在验收过程中发现问题，乙方又未能在 3 个工作日内予以解决的且令甲方满意的，视为乙方违约，按照本合同第七款第一条“乙方违约责任”第（1）项约定处罚。
3. 本次采购的所有货物安装工作由原厂完成，乙方负责（甲方提供必要的协助），乙方协调原厂需在货物验收完成后 20 个工作日内完成设备的安装集成工作，安装集成工作完成后须经甲方验收通过。甲方在安装集成工作完毕并提交验收申请（见附件三）10个工作日内必须展开验收，若由于甲方原因导致逾期10个工作日仍未验收，视为验收通过。甲方须对验收过程中发现的问题向乙方进行详细说明，存在异议的，双方协商解决；乙方须对甲方所有验收过程中发现的问题及时进行处理， 应在发现问题后3个工作日内解决且令甲方满意的。
4. 甲方须对验收过程中发现的问题向乙方进行详细说明，存在异议的，双方协商解决；乙方须对甲方所有验收过程中发现的问题及时响应（3个工作日内响应）并解决且令甲方满意的。非甲方原因，所有上线前的安装工作须按照合同要求完成，否则视为乙方违约，按照本合同第七款第一条“乙方违约责任”第（1）项约定处罚。
5. 甲方不得无故拖延验收过程，或者对设备及其安装过程提出超出本合同之外的其他要求，若因此造成逾期付款，视为甲方违约，按照本合同第七款第二条“甲方违约责任”第（1）项约定处罚。
6. 甲方的验收签字人应为甲方指定的联系人，若为其他人签字视为无效。

**七**、**违约责任**

1、乙方违约责任

（1）乙方逾期交货或者逾期完成安装集成工作的（所供货物与需求不符或者不能满足本合同第二款、第五款所规定的要求且在合同约定的期限内未能纠正且令甲方满意的；或者在合同执行过程中，附件中的其他要求未能满足且在 3 个工作日内未能解决且令甲方满意的），甲方有权要求乙方每日按合同总金额的百分之一向甲方支付违约金。所有违约金最高不超过合同总金额的 20% 。乙方逾期 20 个工作日仍未能交付全部货物并验收通过的，或者乙方逾期 20 个工作日仍未能按照合同约定完成安装集成工作的，甲方有权解除合同，并按照 1.2 倍金额收回已交付乙方的款项，由此给甲方造成其他损失的，乙方应承担赔偿责任。

（2）乙方所交货物的品牌、规格、数量、质量、外包装经确认不符合合同规定的，若甲方同意接受则双方可重新协商合同价款；如果甲方不同意接受，则按照本条第（1）项约定执行合同。

（3）因可归咎于乙方的原因（如乙方未能将货物送至甲方指定的交货地点），未能按时将货物交付甲方指定地点的，乙方应承担赔偿责任，赔偿方式按照本条第（1）项约定执行。

（4）乙方无故拒绝交付约定货物的，视为乙方单方违约，乙方应向甲方支付其无故拒绝交付部分的货物金额的 20% 赔偿甲方，由此给甲方造成其他损失的，乙方应承担赔偿责任。

（5）合同执行期间，原厂服务过程中出现不符合SLA条款的情况，甲方书面通知原厂并要求乙方进行督促，在3个工作日内整改，整改后仍不符合相关条款的视为乙方违约。每违约1次，需支付合同金额1%的违约金。

（6）乙方在本项目招标过程中如有参与围标、串标或陪标等舞弊或作假行为的，一经甲方核实则构成违约，乙方应承担本合同总额20%的违约金并返还甲方已支付的全部合同款项。同时，甲方有权终止本合同。若造成甲方其他损失，乙方须进行赔付。

(7) 乙方需协调原厂商完成甲方要求的测试内容，测试设备由乙方提供，测试设备的硬件型号、软件版本及功能许可等须与后续交货设备完全一致，测试须按照甲方要求的测试内容进行，测试结果由甲方、乙方及原厂商三方确认。如测试不通过，视为乙方违约，甲方有权解除合同并不承担任何责任。

2、甲方违约责任

（1）甲方无正当理由逾期付款的，每逾期一日须按合同总金额的万分之三的标准向乙方支付违约金。此项违约金最高不超过合同总金额的 20% 。甲方逾期付款且经乙方书面催讨后30日仍未能支付合同规定款项的，乙方有权解除合同，并有权不返还甲方已支付款项。

（2）甲方无故拒绝接受符合合同约定货物的（包括甲方中途退货），视为甲方单方违约，乙方有权要求甲方向乙方支付其无故拒绝接受部分（或中途退货部分）货物金额的 20% 赔偿乙方。

（3）因可归咎于甲方的原因（如因甲方错误告知交货地点和接货人，致使乙方无法按时送达），由此给乙方造成损失，甲方应承担赔偿责任。

3、违约金支付：所有一方向另一方支付的违约金须在违约发生后10个工作日内支付，每延迟一日按照合同金额的1%支付违约。乙方违约后甲方收回已支付款项的支付方式及利息照此办理。

**八、货物保管风险的转移**

货物到达本合同约定的交货地点之前，货物保管风险由乙方承担；货物到达本合同约定的交货地点之后，货物保管风险由甲方承担，乙方不再承担任何保管责任。

**九、服务条款**

本合同附件所列货物，乙方根据需求情况进行服务，本合同另有其他约定的以其他约定为准。

**十、不可抗力**

如果由于战争、火灾、水灾、台风、地震、传染病疫情和政府行为等依法视为不可抗力之因素而造成无法按合同约定履行义务时，双方可以免责任，互不承担违约责任。但任何一方应在不可抗力发生后2个工作日内善意、及时地以书面形式通知不知情的另一方，并应于不可抗力发生后20日内向对方出具国家有关机关签署的不可抗力事故证明书。

**十一、争议解决方式**

因本合同引起的或与本合同有关的任何争议，双方首先协商解决，协商不成时，任意一方可在甲方所在地人民法院提起诉讼，通过法律途径解决。

**十二、保密**

在本合同生效后，任何一方向另一方提供的、该另一方不能从公共渠道取得的信息均构成提供方的保密信息，接受信息的一方除非为履行本合同之目的，不得向任何第三方披露或许可任何第三方使用该等保密信息，但接受信息的一方根据中国有关法律的规定有义务进行披露的情形除外，在此情形发生前，接受信息的一方应当首先通知提供信息的一方该等法定披露的范围及所依据的有关法律规定。

就本合同的目的而言，“保密信息”指一方因本合同而向另一方披露的所有业务及技术信息，除非这些信息目前或其后并非因违反对披露方的任何保密责任而变为公开的信息，或者这些信息己经或其后由另一方所开发或从不须承担任何保密责任的独立来源取得。本款规定不因本合同的期满、无效、终止而失效。

**十三、合同效力及变更**

1. 本合同经双方加盖公章或合同专用章后生效，并以最后签订盖章日期为生效日期，仅一方填写日期，则该日期为合同生效日期，若双方均未填写日期，本合同不生效。
2. 合同未尽事宜双方应协商解决，必要时可签订补充协议，补充协议作为合同附件与合同正本有同等法律效力。
3. 特别约定：合同及其附件构成全部合同，合同签订之日起，双方以前或执行本合同过程中所做的任何口头交流、声明或协议等相关文件均告无效。本合同任何一方均可提出对本合同内容的补充和修订，但是任何补充和修订仅能以合同各方盖章的书面文件形式进行，该类文件是本合同的有效组成部分。
4. 本合同一式肆份，甲乙双方各执贰份，具有同等法律效力。
5. 甲方公告的招标文件及乙方的投标文件作为本合同的一部分，具有同等法律效力，如有不一致，以乙方的投标文件为准。

**甲方：上海黄金交易所（章） 乙方： （章）**

**日期：2024年 月 日 日期：2024年 月 日**

附件一：货物明细

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 品牌 | 型号和规格 | 数量 | 金额（元） |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 合计（税率13%） | | | | |  |

详细配置

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 数量 | 配置明细 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

附件二：

货物到货验收单

经验收，以下货物的品牌规格、配置、数量等均与合同约定相符，安装清点并加电无故障，安装验收通过。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 数量 | 配置明细 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

甲方验收人： 日期： 年 月 日

乙方验收人： 日期： 年 月 日

甲方采购办： 日期： 年 月 日

附件三：

货物安装验收单

经验收，以下货物已按照甲方及相关设备安装要求安装（集成），运行无故障，安装验收通过。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 数量 | 配置明细 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

甲方验收人： 日期： 年 月 日

乙方验收人： 日期： 年 月 日

甲方采购办： 日期： 年 月 日

附件四：其他要求

一、服务要求

1. 基本需求：

1）商品须为原厂全新产品，无任何翻新、返修等情况；

2）商品须使用符合国内自主可控技术的CPU和操作系统；

3）商品须带3年原厂现场支持服务，3年原厂硬件维保24\*7\*4服务，3年原厂软件更新和技术支持服务；除原厂服务外投标商还需提供供应商服务，服务期与原厂一致；

4）所购设备需配置C13-C14接口电源线；

5）乙方提供设备的安装，调试工作；

6）乙方需协调原厂商完成甲方要求的测试内容，测试设备由乙方提供，测试设备的硬件型号、软件版本及功能许可等须与后续交货设备完全一致，测试须按照甲方要求的测试内容进行，测试结果由甲方、乙方及原厂商三方确认。（测试内容见本项目招标文件）

7）乙方须确保本次投标设备相关的配置和数据等信息仅用于解决甲方的设备问题，且不得将相关信息传到境外。

8）服务地点：上海。

1. 设备性能和功能需求：

**（1）终端威胁检测响应系统**

|  |  |
| --- | --- |
| **功能** | **技术规格要求** |
| 设备硬件规格 | 1G电口数量≥4个；万兆光接口（包含多模光模块）≥2个； |
| 内存≥64G;600G\*2以上的SSD固态raid阵列，4\*1T以上的SATA机械硬盘阵列； |
| 支持电源可热插拔； |
| 设备硬件尺寸≤2U； |
| 设备电源冗余； |
| 硬件数量及终端许可数量（含国产终端） | 每套终端威胁检测响应系统需要至少1台硬件服务器，3套系统总终端许可数不低于1000个（许可有效期3年）； |
| 设备要求 | 基于B/S的管理架构，Web界面支持主流浏览器； |
| 具备网页接口账号管理机制，并提供个别用户可自行设定操作接口； |
| 允许多位用户同时登入系统； |
| 支持本地认证与第三方外部认证（如RADIUS、TACACS） |
| 本地集成能力 | 可提供开放的Web API接口对接网络流量沙箱系统，并根据沙箱反馈的结果进行全网威胁信息更新； |
| 操作系统适配 | 客户端至少支持操作系统类型：银河麒麟，Windows； |
| 基础功能 | 可以通过管理控制台识别客户端的操作系统、体系架构、IP地址、MAC地址等信息，并进行管理； |
| 控制中心支持对客户端多级分组管理，支持多级分组的创建、删除、移动至新分组； |
| 提供灵活的策略管理能力，支持下发全局策略以及分组策略； |
| 支持客户端的防卸载功能，避免用户自行卸载，管理员可设置卸载密码； |
| 支持在线、离线两种更新方式； |
| 平台保留扩展能力，可根据需求开放接口与第三方平台联动对接； |
| 防病毒模块 | 产品能够实时监控并清除来自各种途径的病毒、木马、蠕虫、恶意软件、勒索软件、黑客工具等恶意威胁； |
| 产品需具有防病毒引擎，且提供更新； |
| 支持检测全局可疑站点（C&C)识别，监控可疑站点的连接，并提供记录或者阻止的处理措施； |
| 具备将可疑文件提交沙盒设备的联动能力，可自动提交可疑恶意文件，并可接收沙箱返回的分析情报； |
| 检测与响应模块 | 基于需求，可配置探针记录内容（进程，网络，注册表和系统事件等）；对“勒索事件”和“挖矿事件”进行热点事件的专项统计； |
| 支持对用户普遍关心和危害程度高的威胁，提供专项检测和结果呈现，包括“暴力破解、Shell反弹、WebShell、PowerShell、本地提权、文档漏洞利用”； |
| 提供远程遏制终端给管理员，仅保留终端与服务器的连接，有效避免威胁蔓延； |
| 支持网络封停自动化响应动作：支持配置自动响应的时间段，即生效周期和生效时间，支持设置封停时长。自动封停后的IP记录在封停列表，封停时长过后自动解封； |
| 系统管理 | 支持SNMP等多种组合报警方式； |
| 采用Syslog日志格式，支持分级和按类型输出以及日志加密传输； |
| 自动提供经过分析后的图形化日/周/月报表； |

**（2）网络流量沙箱系统**

|  |  |
| --- | --- |
| **功能** | **技术规格要求** |
| 设备硬件规格 | 不少于2台硬件设备组成的硬件集群（该集群需具备业务高可用性）； |
| 1G电口数量≥2个，万兆光接口（包含多模光模块）≥2个； |
| 内存≥64G，硬盘≥4T； |
| 支持电源可热插拔； |
| 设备硬件尺寸≤2U； |
| 设备电源冗余； |
| 设备要求 | 支持并发处理文件≥20个； |
| 基于B/S的管理架构，Web界面支持主流浏览器； |
| 具备网页接口账号管理机制，并提供个别用户可自行设定操作接口； |
| 允许多位用户同时登入系统； |
| 支持本地认证与第三方外部认证（如RADIUS、TACACS）； |
| 文件分析能力 | 支持文档、URL、IP、Domain 4种可疑威胁对象的分析； |
| 通过可视化中心或报表可以查看详细样本活动及外联通讯等全部分析结果； |
| 沙箱能够对未知漏洞利用代码和恶意程序的行为进行动态分析； |
| 对提交的可疑URL利用沙箱执行页面扫描、动态链接分析、动态脚本及控件分析，并针对URL指向的可疑文件进行沙箱分析； |
| 本地集成能力 | 可提供开放的Web API接口给终端威胁检测响应系统提交可疑威胁样本，分析完成后将结果及时反馈至终端威胁检测响应系统；可根据需求提供接口给其他第三方产品或授权人员提交样本进行检测； |
| 设备可与交易所在用邮件安全网关（亚信DDEI）进行对接，将沙箱分析后的特征库和威胁情报等实时输入至邮件安全网关，允许邮件安全网关将可疑文件发送至设备进行检测； |
| 系统管理 | 支持SNMP等多种组合报警方式； |
| 采用Syslog日志格式，支持分级和按类型输出以及日志加密传输； |
| 自动提供经过分析后的图形化日/周/月报表； |
| 可支持自定义定制监控大屏模板； |

**三、服务需求（SLA）（原厂+第三方服务）**

| 一、服务频率 | | | |
| --- | --- | --- | --- |
| 序号 | 服务内容 | 频率 | 备注 |
| 1 | 巡检频率和次数 | 每季度1次，全年4次。 | 供应商。 |
| 2 | 故障处理 | 故障发生时处理。 | 不限次数；按甲方要求，由乙方或原厂提供服务。 |
| 3 | 系统变更、项目上线技术保障 | 系统变更或项目上线时，派遣技术保障人员，进行技术保障工作，保障起止时间根据甲方的要求。 | 按甲方要求，由乙方或原厂提供服务。 |
| 4 | 高危病毒爆发期、国家重大会议期和重大任务期间的保障 | 在高危病毒爆发期、国家重大会议期和重大任务期间进行保障，技术保障人员(A\B角)进行技术保障工作，提供应急响应电话，当客户出现技术问题时，及时到达现场解决问题，保障起止时间根据甲方的要求。 | 按甲方要求，由乙方或原厂提供服务。 |

|  |  |  |  |
| --- | --- | --- | --- |
| 二、响应时间 | | | |
| 序号 | 服务内容 | 响应时间 | 备注 |
| 1 | 故障处理响应时间 | 接甲方通知后2小时内到达现场，1个自然日内排除故障，故障排除后3个自然日内提交《故障应急处理和分析报告》。 | 按甲方要求，由乙方或原厂提供服务。 |
| 2 | 技术咨询响应时间 | 接甲方咨询请求后1个工作日内答复。 | 按甲方要求，由乙方或原厂提供服务。 |
| 3 | 巡检报告 | 巡检结束3个工作日内提供。 | 按甲方要求，由乙方或原厂提供服务。 |
| 4 | 技术变更的评估响应时间 | 接甲方请求后2个工作日内答复。 | 按甲方要求，由乙方或原厂提供服务。 |
| 5 | 硬件替换送达甲方的时间节点 | 购买24\*7\*4服务，确认设备硬件故障后乙方半小时内向厂商报障，在厂商受理申请并生成故障处理单号后如需进行替换处理的，替换件需在4小时内到场。 | 按甲方要求，由乙方和原厂共同提供服务。 |

|  |  |  |  |
| --- | --- | --- | --- |
| 三、服务日历 | | | |
| 序号 | 服务内容 | 服务时间 | 备注 |
| 1 | 电话支持 | 7\*24 | 按甲方要求，由乙方或原厂提供服务。 |
| 2 | 邮件支持 | 7\*24 | 按甲方要求，由乙方或原厂提供服务。 |
| 3 | 现场服务 | 非故障时5\*9（工作日）；故障时根据甲方要求。 | 按甲方要求，由乙方或原厂提供服务。 |

四、服务团队人员

承诺

乙方承诺，未经甲方同意，不得变更项目经理及其他团队人员。如需变更，应签署以下项目人员变更单：

1、 变更原因：

2、 变更人员名单：

乙方代表签字：

甲方需求部门签字：

甲方采购办签字：

签字日期：