安全特征采集-招标需求公示

各潜在供应商：

依照《深圳经济特区政府采购条例》相关规定，我公司计划对安全特征采集项目进行公开招标，现将有关情况向潜在供应商公示，征求意见：

1.采购人名称：鹏城实验室

2.采购项目名称：安全特征采集

3.采购项目描述：(内容、用途、数量、简要技术需求等)：详见附件链接。

4.采购方式：公开招标

5.评审标准：综合评标，详见附件链接。

6.征求意见期限：从2019年11月26日起至2019年11月28日止

7.招标代理机构：

联系人：吴小姐 陈先生

地址：深圳市福田区天安数码城创新科技广场一期B座408B室

联系电话：0755-83232102 88602731

办公邮箱：szrnxzb@163.com

8.备注：潜在供应商对公示内容有异议的，请于公示之日内以实名书面（包括联系人、地址、联系电话）形式（加盖公章）将意见反馈至深圳市瑞凝信招标咨询有限公司办公邮箱。

深圳市瑞凝信招标咨询有限公司

2019年11月26日

第一部分　投标人资格要求

符合《政府采购法》第二十二条规定的供应商条件并同时满足以下要求：

（1）具有独立法人资格或具有独立承担民事责任的能力的其它组织（提供营业执照或事业单位法人证等法人证明扫描件，原件备查）；

（2）参与本项目投标前三年内，在经营活动中没有重大违法记录（由供应商在《投标人具备投标资格的证明文件》中作出声明）；

（3）参与本项目政府采购活动时不存在被有关部门禁止参与政府采购活动且在有效期内的情况（由供应商在《投标人具备投标资格的证明文件》中作出声明）；

（4）参与政府采购项目投标的供应商未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单（由供应商在《投标人具备投标资格的证明文件》中作出声明）。

（5）本项目不接受联合体投标，不得分包、转包。

第二部分　项目基本情况

货物清单明细

序号	货物名称	单位	数量	项目预算	备注
1	入侵检测系统 1	1	套		不接受进口
2	入侵检测系统 2	1	套		不接受进口
3	僵木蠕检测系统	1	套		不接受进口
4	入侵检测系统 3	1	套		不接受进口
5	新一代威胁感知系统	1	套		不接受进口
6	入侵检测系统 4	1	套		不接受进口
7	入侵检测系统 5	1	套		不接受进口
8	入侵检测系统 6	1	套		不接受进口
9	Web 应用防火墙 1	1	套		不接受进口
10	web 应用防火墙 2	1	套		不接受进口
11	web 应用防火墙 3	1	套		不接受进口
12	Web 应用防火墙 4	1	套		不接受进口
13	Web 应用防火墙 5	1	套		不接受进口
14	网络审计系统 V3	1	套		不接受进口
15	上网行为管理系统	1	套		不接受进口
16	沙箱	1	套		不接受进口
17	漏洞扫描系统 1	2	套		不接受进口
18	漏洞扫描系统 2	2	套		不接受进口
19	漏洞扫描系统 3	2	套		不接受进口
20	漏洞扫描系统 4	2	套		不接受进口
合计（单位;元）				11,705,000.00	

备注：1.备注栏注明“拒绝进口”的产品不接受投标人选用进口产品参与投标；注明“接受进口”的产品允许投标人选用进口产品参与投标，但不排斥国内产品。

2、进口产品是指通过海关验放进入中国境内且产自关境外的产品。即所谓进口产品是指制造过程均在国外，如果产品在国内组装，其中的零部件（包括核心部件）是进口产品，则应当视为非进口产品。采用“接受进口”的产品优先采购向我国企业转让技术、与我国企业签订消化吸收再创新方案的供应商的进口产品，相关内容以财库〔2007〕119 号文和财办库〔2008〕248 号文的相关规定为准。

3、本项目核心产品为：沙箱（如涉及）

第三部分　需求书

（带★号为必须满足的技术指标项,不满足则投标无效。带▲号为重要技术指标项，不满足重点扣分）

1、技术性能指标

入侵检测系统1

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；
		1.2 基于专业多核硬件平台，非 X86 硬件平台；
		1.3 ▲千兆电口≥8 个，千兆光口≥4 个，万兆光口≥8 个（含 8 个万兆多模光模块），设备扩展槽位≥5；（需提供截图证明材料）
		1.4 配置 2 块 480GB SSD 硬盘，模块化双电源，模块化双风扇，配置 3 年 IPS/AV/ACG 功能授权函；配置 3 年安全威胁情报升级服务授权函；
		1.5 开启防护策略后整机应用层吞吐量≥25Gbps，并发连接数≥1500 万，新建连接数≥40 万/秒，支持虚拟 IPS，数量≥16，配置 14 路防护授权；
		1.6 为非 UTM 架构产品，支持路由、NAT 等网关类产品功能，可以三层部署
		1.7 攻击特征库数量≥3000、病毒特征库数量≥8000、支持的协议识别数量≥3000，
		1.8 检测到攻击报文或攻击流量后，支持 Web 重定向、黑名单等响应方式，以实现第一时间隔离有安全威胁的主机；
		1.9 支持专业防病毒功能，集成第三方专业防病毒厂商的专业病毒库，提供产品与专业防病毒厂商的合作证明；
		1.10具有中国信息安全测评中心的《信息技术产品安全测评证书 EAL3+》；
		1.11具备 IPv6 Ready Phase2 认证证书；

		1.12提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新
		1.13提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新
		1.14提供流量安全事件的可理解描述
		1.15★流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.16流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

入侵检测系统2

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；最大配置为 62 个接口， 默认包括 7 个可插拔的扩展槽和 2 个 10/100/1000BASE-T 接口，默认包括 4 个 SFP+插槽；1 个 CONSOLE;2 个 USB.标配模块化双冗余电源，默认含 WEBFILTER 功能。
		1.2 支持多操作系统引导，出于安全性考虑，多系统需在设备启动过程中进行选择，不得在 WEB 维护界面中设置系统切换选项。
		1.3 支持多端口链路聚合，支持 11 种链路负载均衡算法。
		1.4 系统应具备：融合模式匹配、协议分析、异常检测、会话关联分析，逃逸等多种技术，准确识别入侵攻击行为，为用户提供 2~7 层深度入侵防御。
		1.5 支持攻击报文取证功能，检测到攻击事件后将原始报文完整记录下来，作为电子证据。
		1.6 涵盖广泛的攻击特征库、能够针对 5900 种以上攻击的攻击行为、异常事件，以及网络资源滥用流量，进行检测和防御。
		1.7 支持自定义规则，并且自定义规则库可以导入导出
		1.8 具备独立的 URL 检测过滤引擎。
		1.9 支持 URL 地址分类库，超过 1000 万种。
		1.10支持对设备接口流量的阀值进行设置及报警
		1.11支持独立的 DDOS 检测、阻断及防御基线自学习的能力。
		1.12支持 DDOS 机器人自学习功能，学习时间可设置。
		1.13系统能够根据数据内容而非端口智能识别包括 P2P、即时通讯、电子商务、股票交易、网络游戏、网络电视、移动应用等在内的 23 大类超过 2300 种应用。
		1.14系统应支持多种形式的日志存储,本地存储、发送至日志服务器、

		本地日志服务器双存储、自动方式判断日志服务器状态自动决定日志的记录方式。
		1.15设备生产厂商应具备《TL9000 电讯业质量管理体系认证》
		1.16提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新
		1.17提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新
		1.18提供流量安全事件的可理解描述
		1.19流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.20流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

僵木蠕检测系统

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；最大配置为 66 个接口， 默认包括 6 个可插拔的扩展槽和 2 个 10/100/1000BASE-T 接口,默认包括 2 块 2 个 SFP+插槽万兆接口扩展卡标配模块化双冗余电源.默认含：1 年木马文件检测特征库及 1 年 TOPSEC 僵尸主机特征库升级,木马检测能力：>10Gbps
		1.2 支持自定义僵尸主机检测规则，支持自定义规则配置向导功能，帮助用户进行配置指引，可以设置自定义规则的基本参数包括规则 ID、规则描述、风险等级、协议、协议名称、源地址、源端口、目的地址、目的端口及方向。还可以进行高级参数设置如阈值设置、IP 选项、负载选项。
		1.3 支持记录报文功能，检测到僵尸主机行为后将原始报文完整记录下来，作为电子证据。
		1.4 应涵盖广泛的僵尸主机特征库、能够针对 3500 种以上僵尸主机行为、进行监测。
		1.5 能够检测包括僵尸网络、蠕虫病毒、发包程序、网页木马、WIN 平台木马、Android 木马、IOS/MAC 木马等在内至少 10 种僵尸主机攻击类型。
		1.6 支持 430 万以上木马文件传播监测规则。
		1.7 能够自定义木马文件传播特征，至少包括文件 MD5 校验和、文件内容特征串自定义方式，并支持自定义特征的导入或导出。

		1.8 支持对除已知木马攻击的监测分析外，还可以实现对疑似木马进行捕获和筛选分析。
		1.9 支持疑似样本捕获，针对常见可执行的文件进行检验，将其定义为疑似样本并进行还原。
		1.10支持在线抓包，支持自定义数据包的属性参数，包括抓包数量、协议类型、源 IP、源端口、目的 IP、目的端口、源或目的 IP、源或目的端口、采样比、接口等，并抓取数据流量中相应的数据报文。可通过提取分析抓包数据来了解当前网络受攻击情况。
		1.11支持手动添加 URL 黑白名单。支持当数据报文匹配到监测策略中的策略动作为阻断时自动添加 URL 动态黑名单，并可以配置 URL 动态黑名单的超时时间和检测周期。
		1.12支持手动添加 IP 黑白名单。支持当数据报文匹配到监测策略中的策略动作为阻断时自动添加 IP 动态黑名单，并可以配置 URL 动态黑名单的超时时间和检测周期。
		1.13支持旁路阻断功能，通过发送 TCP reset 报文阻断攻击连接 。
		1.14支持多种形式的日志存储,如本地存储、发送至日志服务器、发送到控制台等方式。
		1.15应提供全方位的包含管理、系统、策略、通讯、硬件、容错、测试等告警。
		1.16支持声音报警、NetBios、控制台、SNMP、邮件等方式的报警。
		1.17支持攻击趋势展示功能，对僵尸主机攻击趋势进行，并以图形化的形式展示一天、一周、一个月时间内的僵尸主机攻击数量。
		1.18设备生产厂商应具备《TL9000 电讯业质量管理体系认证》
		1.19提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新
		1.20提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新
		1.21提供流量安全事件的可理解描述
		1.22★流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.23流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

入侵检测系统 3

编号	招标技术指标名称	招标技术指标值

1	性能指标	1.1 标准机架式设备；冗余电源，千兆电口≥4 个，千兆光口≥4 个，万兆光口≥8 个，并含 2 个 USB2.0 接口和 1 个 RJ45 串口；支持 bypass；
		1.2 网络层吞吐量 80Gbps，IPS 吞吐量 30Gbps，并发连结数 1600W，新建连接数（CPS）60W；
		1.3 支持路由部署、透明网桥部署、旁路部署、虚拟网线以及混合部署等多种方式；支持 802.1Q VLAN Trunk、access 接口类型，VLAN 三层接口和子接口；支持链路聚合功能，可将多条物理链路聚合成一条带宽更高的逻辑链路使用；支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路；
		1.4 支持静态路由和 ECMP 等价路由协议；支持 OSPF 动态路由协议；
		1.5 支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、地域、认证用户、子接口和 VLAN 等因素实现对象的流量控制；
		1.6 支持 URL 过滤和文件过滤功能，URL 过滤支持 GET，POST 请求过滤和 HTTPS 网站过滤，文件过滤支持文件上传和下载过滤；
		1.7 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；
		1.8 支持连接会话展示，可针对具体的 IP 地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体 IP 的会话记录；支持根据国家/地区来进行地域访问控制，保障业务访问安全性；
		1.9 支持细致的服务器敏感数据识别，识别维度包含服务器 IP、业务重要性、识别方式、开放的服务与端口、敏感数据页面数以及更新时间等，并且可以进行详细的页面 URL 以及页面信息举证；
		1.10支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别；
		1.11支持关键文件保护功能，能够过滤文件的上传和下载行为，以防止非法外传和下载行为。能识别的文件类型应包含至少以下几类：音频视频类文件、图片类文件、文本类文件、压缩文件、应用程序类文件等；
		1.12支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志实时上报与展示等功能；
		1.13支持 SYSLOG 标准日志协议；安全日志根据日志类型可存储在产品内置数据中心、Syslog 日志服务器多种方式；
		1.14双机支持 A/S，A/A 方式部署；提供完善的双机热备处理机制，支持配置同步，会话同步和用户状态同步，保证主机发生故障时，业务可以自动平滑切换到备机上运行；
		1.15提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新

		1.16提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新
		1.17提供流量安全事件的可理解描述
		1.18流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.19流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

新一代威胁感知系统

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 平台设备： 标准机架式设备；配置 4*GE 管理电口，3*USB3.0 接口，1*DB9 Console 接口，冗余电源，960G SSD + 12*4TB SATA 存储硬盘。含 36 个月产品标准维保服务，自发货之日起开始计算。含三年威胁情报更新授权，自授权导入之日起开始计算。
		1.2 支持以受害资产维度进行分析，分析内容包括失陷状态、受到的攻击类型、威胁级别、处于的攻击阶段、所属的资产分组
		1.3 ▲支持与云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索，查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（需提供截图证明材料）
		1.4 支持基于威胁情报的威胁检测，检测类型包含 APT 事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件，并可自定义威胁情报
		1.5 支持对威胁告警事件进行调查分析，结合大数据分析技术以攻击链视角进行呈现
		1.6 支持对业务资产主动外连行为检测，包含：外连 IP、外连 IP 归属、服务商、外连流量大小
		1.7 ▲通过机器学习技术发现动态恶意域名，检测准确率≥99%（需提供截图证明材料）
		1.8 支持 HTTP 代理行为发现，检测内容包含：代理 IP、代理端口、代理次数
		1.9 支持暴力破解行为检测，检测内容包含：登录 IP 归属、使用协议、爆破次数、爆破成功与否
		1.10支持弱口令检测，检测内容包含：弱口令、弱口令对应账号

		1.11▲支持检索异常报文、域名解析、文件传输、FTP 控制通道、LDAP 行为、登录动作、邮件行为、MQ 流量、网络阻断、数据库操作、SSL 加密协商、TCP 流量、Telnet 行为、UDP 流量、WEB 访问等网络流量日志，并可基于时间、IP、端口、协议、上下行负载等多重字段组合进行日志检索（需提供截图证明材料）
		1.12支持告警日志检索，可基于时间、告警类型、文件 MD5、文件名、文件传输方向、攻击方式、攻击结果、来源/目的所属国、IP 地址、上下行负载等多字段混合搜索
		1.13支持与云端安全运营中心联动。设备能连接互联网时，安全专家在云端分析并撰写威胁分析报告下发到设备上共用户查阅；设备离线时，可将关键数据离线导出上传到云端安全运营中心，安全专家进行分析撰写威胁分析报告。
		1.14探针设备： 2U 标准上架设备，含滑轨。配置 2*GE 流量监听电口，2*10GE 流量监听光口，2*GE 管理电口，3*USB3.0 接口，1*DB9 Console 接口，冗余电源;4TB SATA 存储硬盘。
		1.15支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs 等
		1.16支持基于工具特征的 WEBSHELL 检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：冰蝎、中国菜刀、小马上传工具、小马生成器等。
		1.17支持对流量中出现文件传输行为进行发现和还原，并记录文件 MD5 发送至分析设备，如可执行文件（EXE、DLL、OCX、SYS、COM、apk 等）、压缩格式文件（RAR、ZIP、GZ、7Z 等）、文档类型文件（word、excel、pdf、rtf、ppt 等）
		1.18支持常见数据库协议的识别或还原：DB2、Oracle、SQL Server、MySQL、PostgreSQL 等协议
		1.19支持自定义协议和端口，满足特殊场景下的流量抓取
		1.20支持基于流量实时 IOC 匹配功能，设备具备主流的 IOC，情报总量 50+万条
		1.21支持基于 webshell 函数的攻击检测，如文件包含漏洞、任意文件写入、任意目录读取、任意文件包含、preg_replace 代码执行等
		1.22支持基于代理程序的攻击检测，如 TCP 代理程序、HTTP 代理程序等
		1.23支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力支持基于 IP 地址的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断
		1.24支持基于 URL 的旁路阻断，并能将 URL 请求进行重定向
		1.25支持 AES256、SM4 数据传输加密，确保数据传输的安全性

		1.26支持威胁告警信息发送给 syslog 服务器，支持将威胁告警、威胁等级、网络日志、攻击结果、威胁类型等日志传输给 KAFKA、威胁分析平台。
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

入侵检测系统 4

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；网络层吞吐 20Gbps，10Gbps 入侵检测吞吐，并发链接≥900 万；2U 机箱，配备 4 个千兆电口、4 个万兆光口，冗余电源，自带 1 个液晶屏，1 个 HA 电口及 1 个管理口（非业务口），两个扩展槽。含三年硬件维修，三年 IPS 特征库升级服务，可选包含 APP、AV 特征库升级服务 ：
		1.2 支持显示系统最近 1 小时、24 小时、1 周、1 个月的入侵攻击事件趋势图
		1.3 支持实时显示系统 CPU 使用率、流量内存使用率、系统内存使用率、硬件存储使用率、CPU 温度
		1.4 提供初次使用设备配置向导，包括主机名称配置、密码配置、系统时间、登录超时时间、网络配置、IDS 配置等
		1.5 支持从 web 页面登录命令行进行系统配置
		1.6 支持基于策略的管理 IP 限制和入接口限制
		1.7 支持物理监听接口
		1.8 支持自定义 HA 心跳口和管理接口
		1.9 支持配置 DNS 服务器
		1.10支持双机热备、负载均衡、主动共享三种模式
		1.11支持对 ACL 策略进行冲突检测和冗余检测
		1.12支持黑名单，根据报文的源 IP 地址、掩码进行报文过滤
		1.13支持白名单，根据报文的源 IP 地址、掩码让报文通过，支持 IPS 业务、防垃圾邮件、防病毒、应用安全和流量控制五个业务
		1.14支持应用识别、入侵防护、关键字过滤、URL 过滤、AV 等安全模块一次性扫描，系统整体性能几乎不受功能的增加而降低
		1.15支持源 IP、目的 IP、源域、目的域、时间、用户、应用
		1.16支持 2000 多种应用特征库，可准确识别各种 IM、P2P、网络游戏、流媒体、股票等应用
		1.17支持基于 5 元组自定义协议特征，支持正则表达式自定义内容特征

		1.18支持基于 IP 碎片重组、TCP 流重组、会话状态跟踪、应用层协议解码等数据流处理方式的攻击识别
		1.19支持模式匹配、异常检测、统计分析，以及抗 IDS/IPS 逃逸等多种检测技术
		1.20▲支持对单个攻击事件保存其原始报文以供取证分析 提供 IDS 事件日志和报表，报表支持 PDF、TXT、HTML、CSV、DOCX 格式，并提供导出功能（需提供截图证明材料）
		1.21实时流量统计，支持最近 10 分钟、1 小时、24 小时跨度的流量趋势图、连接趋势图，支持 top10 应用、top10 用户统计
		1.22提供多种业务报表，可依据五元组、应用协议、时间点/时间段等元素自定义报表内容并显示
		1.23可对接口流量/应用/协议的异常状态进行告警，并以 Email/SNMP Trap/声音等方式通知管理员
		1.24支持 ping、tracert 等网络测试工具
		1.25提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新
		1.26提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新
		1.27提供流量安全事件的可理解描述
		1.28流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.29流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

入侵检测系统 5

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；1 个 RJ-45 Console 口，2 个 10/100/1000 Base-T 带外管理口，4 个扩展槽位，可选配千兆、万兆扩展板卡，2 个 USB 口，含嵌入式软件、控制中心软件，含 36 个月软硬件维保与特征库升级。
		1.2 具备弱口令检测能力，并提供自定义弱口令规则的能力，使用户可以灵活定义网络内的弱口令条件，
		1.3 威胁告警需提供设置用户关注事件的能力，通过设置，可以明确地将事件设置为需要关注或不需要关注，用户的设置结果将取代用户自动分析的结果，即：用户设置为需要关注的报警事

		件，直接在告警界面进行显示，用户设置为不需要关注的报警事件，不再在用户的事件报警展示界面进行展示；
		1.4 操作系统资产配置与报警自动关联，根据配置的目的地址、影响系统与影响设备进行上报事件的过滤；
		1.5 可针对达到识别策略的事件进行优化处理，包括对日志的处理和策略的处理；
		1.6 提供根据用户的组织结构定义“组织/部门”的能力，并且“组织/部门”之间可以嵌套，“组织/部门”可以通过：IP、IP 段、引擎（加网口）、子控进行定义；
		1.7 可以针对组织目录来查看历史事件与生成报表；
		1.8 支持从威胁发现到威胁展示、威胁说明、分析帮助、处理过程帮助、处理过程记录、后继续自动处理的威胁全过程处理流程，帮助用户发现威胁、分析威胁、处理威胁，完成威胁管理工作的全流程闭环，
		1.9 提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新
		1.10提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新
		1.11提供流量安全事件的可理解描述
		1.12流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.13流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

入侵检测系统 6

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；需提供 1 个 RJ45 串口，2 个 1000M 管理口，2 个 USB 接口，4 个 1000M 以太网电口，4 个 SFP 接口,2 个网络接口插槽
		1.2 吞吐量≥12Gbps，最大并发会话数：300 万，每秒新增会话数：10 万，时延<40μs
		1.3 系统应提供覆盖广泛的攻击特征库，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和阻断。系统须提供对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解等恶意流量的检测。

		1.4 系统应提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为。系统应提供敏感数据外发的检测功能，能够识别通过自身的敏感数据信息（身份证号、银行卡、手机号等）系统应提供关键文件外发检测功能，能够识别通过自身的关键文件，检测非法外传行为。能识别的关键文件类型应包含至少以下几类：文档类如 Excel、PDF、PowerPoint、Word 等，压缩文件类如 CAB、GZIP、RAR、ZIP、JAR 等，图像类如 BMP、GIF、JPEG 等，音频视频类如 MP3、AVI、MKV、MP4、MPEG、WMV 等，脚本类如 BAT、CMD、WSF 等，程序类如 APK、DLL、EXE、JAVA_CLASS 等；系统应提供基于信誉的僵尸网络检测能力，具备可以持续升级的信誉库，IDS 通过信誉库内的恶意网站 IP、C&C 服务器地址的信誉值执行相应的检测动作；系统应提供 URL 分类库，提供中英文网页过滤数据库，实现高风险、不良网站过滤；系统应提供在线病毒检测能力；支持文件信誉功能;系统应能识别主流的应用程序，识别种类不少于 1000 种。系统应支持“一键巡检”功能，可根据设备运行过程中反馈的数据进行全面分析，并生成图表相结合的安全报告。定时进行巡检可发现异常漏洞与受攻击情况;系统应提供丰富的响应方式，包括：会话阻断、IP 隔离、邮件通知等功能，满足用户各种响应需求；系统应具备攻击快照功能，详细记录触发告警的数据特征，以便做进一步的事件分析；系统应具备地址簿功能，在报表中直观显示 IP 地址所处国家、地区或某个部门。支持自定义私有 IP 地址库和导入外部公网 IP 地址库
		1.5 提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新
		1.6 提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新
		1.7 提供流量安全事件的可理解描述
		1.8 流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.9 流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

Web 应用防火墙 1

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；双交流电源，8G 内存，1T 硬盘，2 个以太网千兆管理接口，≥6 个以太网千兆电口，≥8 个以太网千兆光口，≥4 万兆以太网 SFP+光接口（含万兆多模光模块），≥1 个接口扩展槽位；

		1.2 HTTP 吞吐量不低于 1Gbps，HTTP 并发连接数不低于 60 万、HTTP 每秒新建连接数不低于 4 万，保护网站站点数量无限制，含 3 年特征库升级许可。；
		1.3 系统采用 B/S 设计架构，并采用 SSL 加密通信方式，通过浏览器方便对产品进行远程管理；
		1.4 支持透明流模式、透明代理模式、反向代理模式、路由牵引模式、镜像检测模式及镜像阻断模式；
		1.5 支持旁路镜像模式下，对检测到的攻击进行旁路阻断；
		1.6 支持通过 BGP 方式对流量进行牵引，并在清洗攻击后回注，回注过程支持设置 SNAT 策略；
		1.7 提供 DNS 服务器功能，支持服务器泛域名和普通域名服务；
		1.8 支持 HTTP 协议校验，可根据实际网络状况自定义协议参数合规标准，过滤非法数据；
		1.9 支持设置扫描陷阱，防止恶意扫描；提供功能截图作为证明；
		1.10支持爬虫防护和文件上传、下载过滤；
		1.11支持 cookie 加固及加密保护；
		1.12具备 CCRC 网络关键设备和网络安全专用产品安全认证证书-增强级；
		1.13具备工业和信息化部颁发的电信设备进网许可证；
		1.14 提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新
		1.15提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新
		1.16提供流量安全事件的可理解描述
		1.17流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.18流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

web 应用防火墙 2

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；最大配置为 26 个接口；默认包括 2 个可插拔的扩展槽和 4 个 10/100/1000BASE-T 接口和 4 个 SFP 插槽，2 个 10/100/1000BASE-T 接口（作为 HA 口和管理口）；双电源；含 3 年特征库升级服务。内含 SQL 注入、XSS、CSRF 等 WEB 攻击防

		护功能、URL 访问控制功能、防盗链功能、WEB 漏洞扫描功能、DDOS 攻击防护功能、网页防篡改功能。
		1.2 支持 VLAN 划分，支持多 VLAN 环境下 trunk 的部署
		1.3 支持虚拟线无论任何网络环境可强制数据从一个接口转发到另一个接口
		1.4 支持链路聚合(Channel)部署，提高链路带宽；支持 Trunk 链路防护
		1.5 支持 900+条以上的应用层规则
		1.6 支持暴力登录防护
		1.7 支持对身份证、信用卡、手机电话号码、座机电话号码、邮箱地址等敏感信息做检查，当检查到此类数据后可通过配置特殊字符予以替换隐藏，防止信息泄露
		1.8 支持对 URL 编码、多次编码等方式绕过 WAF 的编码方式进行识别，防止绕过
		1.9 可对文件做下载控制，包括最大下载文件大小、禁止下载文件的扩展名、MIME 类型等
		1.10支持自学习建模功能，可以通过学习正常 URL 参数的长度、参数类型、请求方法等数据特点创建白名单模型，如果参数违反白名单模型则认为是非法流量直接阻断，开启自学习建模功能后可生成自学习网站参数的自学习结果报告
		1.11支持虚拟补丁功能，支持导入 appscan、w3af 等第三方扫描器的扫描结果生成 WAF 的规则，对此类网站漏洞直接防护
		1.12支持基线学习，可以自动学习用户 http 正常流量阈值模型，并给出推荐阈值配置项
		1.13对 ddos 流量支持检测清洗和强制防御两种模式，检测清洗根据是否到达阈值对流量进行清洗，强制清洗对所有流量直接进行流量清洗判断
		1.14支持针对每秒包数、每秒新建连接数、每秒并发连接数对 HTTP/HTTPS Flood 攻击做控制配置
		1.15网关型网页防篡改，无需在服务器中安装任何插件，可以对动态网站及静态网站文件内容进行防篡改，当检测到篡改后可以实时恢复篡改内容
		1.16支持多种 WEB 应用漏洞的安全扫描检测，如 SQL 注入、跨站脚本、目录遍历等
		1.17支持自定义 WEB 漏洞扫描任务，支持对需要认证登录的 web 系统进行漏洞扫描，支持自定义每日、每周、每月等扫描周期设置
		1.18支持同一台 WAF 上下接口状态联动(一个接口 down 另外一个接口也同步 down)
		1.19设备生产厂商应具备《TL9000 电讯业质量管理体系认证》
		1.20提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新
		1.21提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新

		1.22提供流量安全事件的可理解描述
		1.23流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.24流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

web 应用防火墙 3

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；有液晶面板，1TB 硬盘，冗余电源，2 个扩展插槽。标准配置 2 个万兆 SFP+插槽，4 个千兆电口，1 个 Console 口，2 个 USB 口.Web 安全保护 512 个站点。包含三年 WAF 软件特征库服务，三年硬件维修服务。
		1.2 网络吞吐量为 10Gbps，应用层处理能力为 6Gbps，网络并发连接数 400 万，HTTP 并发为 150 万，HTTP 新建连接数大于等于 60000/s。
		1.3 产品具备支持透明在线部署，不更改网络或网站配置，即插即用，无需配置 IP 地址即可防护
		1.4 产品具备支持镜像分析数据并实现旁路阻断功能，产品具备专门的阻断接口设置
		1.5 产品具备支持链路聚合(Channel)部署，接口支持自定义划分，支持多进多出模式，显著提高设备间的吞吐能力
		1.6 产品具备支持静态路由、策略路由等路由配置
		1.7 产品具备支持对负载均衡服务器任意数量网站进行防护，内置有负载均衡算法，包含轮询、Hash 算法
		1.8 产品具备支持代理服务器模式，支持 HTTP、HTTPS 代理模式，提供针对后端服务器的代理模式
		1.9 产品具备自学习系统，无需人工干预，自动获取网站相关信息
		1.10产品具备自学习网站与防护功自动匹配并启动防御效果
		1.11产品具备根据网站流量自动生成网站文件和 URL 地址的树形结构展示拓扑图
		1.12产品具备对 URL 地址的请求次数、响应时间、参数信息等数据进行统计分析展示
		1.13产品具备支持 SQL 注入、跨站脚本、防爬虫、扫描器、信息泄露、溢出、协议完整性等至少 7 种知识库展示说明

		1.14产品具备支持 HTTP 协议校验细粒度规则检测，至少提供 20 种 HTTP 协议校验策略参数，其中要包括 Cookies、Host、Range 等策略参数
		1.15产品具备弱密码检测功能，提供用户名、密码字典检测机制
		1.16产品具备支持威胁情报中心联动功能，具备 FTP、API、key 联动方式
		1.17产品具备提供威胁情报中心的安全情报 IP 数量统计，并提供分析数据模型、IP 数量、百分比等详细信息
		1.18产品具备提供威胁情报中心的安全情报风险值统计，并提供分析数据模型、危险程度、百分比等详细信息
		1.19产品具备提供威胁情报中心的安全情报活跃度统计，并提供分析数据模型、活跃程度、百分比等详细信息
		1.20产品具备双机运行保障机制，支持主/主模式、主/备防护工作模式
		1.21产品具备专用接口进行双主机的配置同步功能 产品具备冗余系统备份机制，升级或运行中出现软件异常，可自动切换至备份系统保障设备正常运行
		1.22产品具备软件 bypass 功能，当发现系统运行异常时，可手动切换 bypass 功能，保障网站正常访问
		1.23提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新
		1.24提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新
		1.25提供流量安全事件的可理解描述
		1.26★流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.27流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

Web 应用防火墙 4

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；含交流双电源，2*USB 接口，1*RJ45 串口，2*GE 管理口，至少具备 4 个 GE 业务电口带 BYPASS，4 个 SFP 光口，2 个网络接口插槽，并且所有业务接口均无需授权全部可用，网络吞吐量不少于 10Gbps，时延<50us。

		1.2 旁路部署支持流量牵引、二层回注、跨接回注及 PBR 回注方式。支持 A/S 部署模式（链路切换、配置同步）；支持 VRRP 协议。支持非对称路由下的部署
		1.3 支持紧急模式，当并发连接数超过阀值时，WAF 自动进入紧急模式，已经代理的连接正常代理，对新增的请求不进行代理，直接转发，防止 WAF 成为访问瓶颈。当连接数恢复正常时，自动退出紧急模式
		1.4 支持对安全策略的一键式例外配置。
		1.5 支持对 HTTP 协议合法性进行验证，提供 HTTP 协议防护功能。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。支持对 SSL（HTTPS）加密会话进行分析。支持防护：蠕虫、缓冲区溢出、CGI 信息扫描、目录遍历等攻击。
		1.6 支持暴力破解防护，支持基于 GET 或 POST 分别设置触发阈值。能够识别 Form、Ajax、Jsonp 等多种登录验证方式。
		1.7 对流出数据内容进行安全审查，对敏感关键字实施过滤，防止身份证等隐私信息非法泄露；支持 XML 基础校验，包括最大树深度、元素名长度、元素个数、子节点个数等参数配置。支持基于五元组（源 IP 地址、目的 IP 地址、源端口、目的源口、协议类型）及接口的网络层访问控制功能
		1.8 为防止 web 攻击手段采用 base64 编码混淆真实攻击意图，WAF 应支持 Base64 编码攻击防护；支持 HTTPS 国密算法；支持镜像监听模式下 HTTPS 流量的解析；HTTPS 支持配置 HSTS 功能
		1.9 支持国内广泛使用的本土化自产 web 框架及组件，如：织梦 dedecms、ECShop 等系统及其衍生模版的漏洞，应具备防护规则库。
		1.10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；
		1.11可以与同品牌 SaaS 扫描服务或者 Web 漏洞扫描器联动，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
		1.12提供本地清洗服务，能够对用户侧流量型及精细型 DDOS 攻击进行防护，防护能力应具备如下要求：支持 TCP Flood 防护，支持 HTTP Flood 防护，支持多种检测算法，支持对慢速攻击的防护；支持与抗拒绝服务系统联动，对流量进行按需清洗
		1.13提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新
		1.14提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新
		1.15提供流量安全事件的可理解描述
		1.16流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号

		1.17流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

Web 应用防火墙 5

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；三层吞吐量≥80G，应用层吞吐量≥20G，http 并发连结数≥16000W，http 新建连接数（CPS）≥300,000 个；
		1.2 硬件参数：标准 2U 架构，冗余电源，千兆电口≥4 个，千兆光口≥4 个,并含 2 个 USB2.0 接口和 1 个 RJ45 串口;支持 bypass；
		1.3 支持路由模式部署；支持透明网桥部署，实现应用层透明部署；支持镜像部署，镜像服务器流量即可实现安全审计和告警；
		1.4 支持 802.1Q VLAN Trunk、access 接口，VLAN 三层接口，子接口；支持链路聚合功能，可将多条物理链路聚合成一条带宽更高的逻辑链路使用，提升网络带宽和增加容错性；支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路；
		1.5 支持静态路由，ECMP 等价路由协议；支持 OSPFv2/v3 动态路由协议；
		1.6 访问控制规则支持基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组的细化控制方式；访问控制规则支持失效规则识别，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况；支持针对源 IP、目的 IP 和双向 IP 连接数控制,可设置每个 IP 最大并发连接数；
		1.7 支持 URL 过滤和文件过滤功能，URL 过滤支持 HTTP（get），HTTP（post）请求过滤和 HTTPS 过滤，文件过滤支持文件上传和下载过滤；支持针对 SMTP、POP3、IMAP 邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件异常账号检测等，支持根据邮件附件类型进行文件过滤；支持针对 HTTP、FTP 协议内容检测与病毒查杀；
		1.8 支持抵御 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 整站系统漏洞等攻击；支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；支持 HTTP 协议异常检测，包括 HTTP 请求异常检测、HTTP 头部字段 SQL 注入检测、URL 溢出检测、

		Post 实体溢出检测、HTTP 头部溢出检测；支持 FTP 弱口令检测、WEB 登陆弱口令检测、WEB 登陆明文检测；支持 CC 攻击、CSRF 攻击、COOKIE 攻击等攻击防护功能；支持针对网站的漏洞恶意扫描进行防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测，支持基于目录访问频率和敏感文件扫描等恶意扫描行为进行防护；支持 Web 漏洞扫描功能，可扫描检测网站是否存在 SQL 注入、CSRF、XSS、远程文件包含、DOM 跨站脚本攻击等漏洞；
		1.9 双机支持 A/S，A/A 方式部署；提供完善的双机热备处理机制，支持配置同步，会话同步和用户状态同步，保证主机发生故障时，业务可以自动平滑切换到备机上运行；
		1.10提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新
		1.11提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新
		1.12提供流量安全事件的可理解描述 流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.13流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

网络审计系统

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；2 个 10/100/1000BASE-TX 管理口，4 个 SFP 插槽，4 个 1000BASE 电口采集口，2T 存储空间； 配置双电源；默认含 1 年的 URL 库、攻击库和应用识别库； 冗余 2 个扩展槽位，扩展板卡尾字母-A； 支持扩展双硬盘；
		1.2 支持实名审计，支持 802.1x,PPPoE,AD 等环境下终端 IP 地址和用户实名信息或主机信息绑定显示，可显示在线用户的 PPPoE 账号和 AD 域用户等信息。
		1.3 支持对 HTTP 协议进行审计，审计内容包括：访问域，URL 引用页、URL 分类、http 请求类型、http 响应类型、请求文件、请求参数、访问行为、发布内容、请求结果、浏览器、服务器、Cookie、返回长度、代理客户端地址、代理上网服务、HTTP 响应时间、源目的地址、MAC 地址等。
		1.4 支持应用协议行为识别，最少分为 12 大类，可以把应用协议分组进行审计，用户可以根据需求自行选择审计内容。

		1.5 支持 FTP、Radius、Telnet、即时通讯等协议以及 SMTP、POP3、IMAP 的邮件审计功能；
		1.6 支持 330 种以上国内常见应用协议行为的自动识别与审计记录。
		1.7 支持共享协议（SMB 文件共享、NFS 共享）审计。系统内置高危 SQL 查询和注入、远程命令执行、跨站脚本攻击等高危指令告警规则。
		1.8 支持流量趋势分析、IP 分组流量统计，可以对传输协议、应用协议、应用协议组、源目的地址、源目的端口进行统计分析，可以多条件组合分析。
		1.9 支持基于流的流量分析功能，可对其他设备发送的 Netflow 进行分析，支持对 Netflow v5/v9 版本的流量分析。
		1.10支持 WEB 登录锁定配置，可自定义用户名/密码尝试次数和登录锁定时间。
		1.11支持双操作系统，当常用系统出现故障可以使用备用系统恢复。
		1.12支持单点、多点、多级管理模式 ；采用 B/S 管理方式，不需要单独的管理设备。
		1.13一体化设备，审计、解析、管理、报警、存储均在一台物理设备上实现。
		1.14通过扩展软件授权许可即可在同一硬件平台上实现数据库审计系统的所有功能。
		1.15支持 IPV6 环境部署和 IPV6 环境下网络审计系统全部功能的审计。
		1.16设备生产厂商应具备《TL9000 电讯业质量管理体系认证》
		1.17提供流量安全事件的可理解描述
		1.18流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.19流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

上网行为管理系统

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；系统硬件为全内置封闭式结构，稳定可靠，加电即可运行，启动过程无须人工干预；
		1.2 多核架构设计，非 X86 架构，双交流电源；

		1.3 10M/100M/1000M 自适应电接口数量≥12，支持千兆 SFP 光接口数量≥12，万兆接口总数≥2； 配置 2 个万兆多模光模块，3 年特征库升级许可授权；
		1.4 支持路由模式、透明（网桥）模式、混合模式，支持镜像接口，部署模式切换无需重启设备；
		1.5 支持以太网接口、VLAN、桥接口、聚合接口、隧道接口、4G 无线接口、安全域、IPv6 隧道接口、Ipsec 隧道接口；支持端口镜像；
		1.6 支持虚拟线配置，虚拟线的两个接口支持状态联动。数据传输支持 vlan tag 过滤，提供 web 界面截图；
		1.7 支持 DDNS 功能，花生壳 DDNS 客户端以及域名 IP 绑定功能，并提供 web 配置界面截图；
		1.8 支持 VRF 功能、IPv6 功能；
		1.9 支持 IPSec VPN 支持第三方对接和快速配置、GRE OVER ipsec、IPSec 冷备份；
		1.10针对特定无应用指纹的应用：迅雷、P2P 下载支持行为模式的智能识别，并提供截图；
		1.11支持 SSL 加密内容审计、用户行为审计、流量管理、防私接路由、用户认证等功能；
		1.12支持针对特定域名的 APP 缓存，只要是该域名传输的 APP 全部缓存，支持自学习性缓存，设备可自动缓存特定服务器的所有终端应用提供配置截图；
		1.13支持一个公网 IP 映射到内网多台服务器，服务器间支持连接和源地址 hash，支持服务器健康检查，提供 web 配置界面截图；
		1.14支持非对称路由和地址代理功能；
		1.15提供流量安全事件的可理解描述
		1.16流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.17流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件
		4.4 三年特征库免费升级

沙箱

编号	招标技术指标名称	招标技术指标值

1	性能指标	1.1 标准机架式设备；产品采用 B/S 架构，软硬件一体化设计，系统硬件为全内置封闭式结构，稳定可靠，加电即可运行，启动过程无须人工干预。
		1.2 8 核 2.1G 主频，128G 内存，4T 硬盘，双交流电源，4 千兆电，2 千兆光（含万兆多模光模块）；
		1.3 吞吐量≥1Gbps，文件动态检测能力≥3 万/天，文件静态检测能力≥600 万/天，WEB 文件动态检测能力≥150 万/天；
		1.4 采用创新的应用级沙箱和数据关联分析技术，集成 AV 和 IDS 辅助检测模块，具备威胁情报体系。
		1.5 支持 Ipv4、IPv6、VxLAN 流量解析，协议识别和文件还原检测；
		1.6 支持从 HTTP、FTP、POP3、SMTP、IMAP、SMB、CIFS 协议中还原出指定格式文件；
		1.7 支持对样本内容进行静态检测，发现已知漏洞、木马、蠕虫、病毒、黑客工具等恶意代码；支持动态沙箱检测技术来检测已知和未知的漏洞，以及木马、蠕虫、病毒、黑客工具等恶意代码；
		1.8 支持集成多个 AV 检测引擎，支持白名单功能，能够对已知的正常样本进行过滤和筛选；
		1.9 支持多种网络协议仿真，如 ICMP、WEB、DNS、HTTP 等；
		1.10采用隔离技术，支持单沙箱同时检测多个样本，提高检测性能；
		1.11支持网页分片检测、HTML 网页检测、JS 文件检测、缓冲区溢出攻击检测、通过匹配行为检测等多种 WEB 沙箱检测方式；
		1.12提供流量安全事件与漏洞（CVE/BID/MSB）的对应关系，并支持对应关系的更新
		1.13提供流量安全事件与弱点（CWE）的对应关系，并支持对应关系的更新
		1.14提供流量安全事件的可理解描述
		1.15★流量安全事件标识源 MAC 地址、目的 MAC 地址、源 VLAN 号、目的 VLAN 号
		1.16流量检测性能不小于 10Gpbs
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

漏洞扫描系统 1

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；双交流电源，8G 内存，1T 硬盘，≥8 个以太网千兆电口，≥8 个以太网千兆光口，支持 2 个接口扩展槽位，配置≥4 个万兆光口（含万兆多模光模块）；

		1.2 系统包含主机漏洞扫描、数据库漏洞扫描、WEB 漏洞扫描功能授权；
		1.3 主机及数据库扫描目标并发数量不少于 80 个，扫描进程并发数量不少于 150 个，WEB 漏扫目标并发数量不少于 5 个，扫描进程并发数量不少于 10 个；无限 IP 地址或域名授权函，3 年特征库升级许可授权；
		1.4 支持多级管理（3 级及 3 级以上），可以分布式大规模部署，可通过统一平台进行集中化管理；
		1.5 持资产自动发现功能，发现存活的目标自动添加到资产列表中，便于管理员对资产的管理；
		1.6 支持添加数据库资产时提供帐户口令连接测试，保证扫描正确性；
		1.7 支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等;
		1.8 主机漏洞知识库可检测漏洞数量 50000+,其中可检测 CVE 漏洞数不低于 48000+个，非 CVE 漏洞数不低于 3000+个,漏洞信息全中文支持，提供漏洞名称、威胁类型、风险级别等漏洞信息详细描述及其对应的解决方案；
		1.9 支持主机漏洞知识库与 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等国内外主流标准兼容；
		1.10支持在扫描过程中人工指定包括 SMB、SSH、Telnet、SNMP 等常见协议的登陆口令，登陆到相应的系统中对特定应用进行深入扫描；
		1.11支持 IPV4、IPV6 双协议栈地址扫描；
		1.12支持对数据库进行帐户口令认证登陆，登陆到相应的数据库中对特定应用进行深入扫描，其中主流数据库类型支持包括不局限于 Oracle、Mysql、MSSQL、DB2、Informix、Sybase、达梦等 7 种数据库类型；
		1.13WEB 漏洞知识库漏洞信息 1000+，提供漏洞名称、威胁类型、风险级别等漏洞信息详细描述及其对应的解决方案；（提供界面截图）；
		1.14支持渗透测试功能，对发现的 SQL 注入或 SQL 盲注等漏洞，通过渗透测试功能可以获取数据库相关信息；
		1.15漏洞探测类型包括：操作系统漏洞、应用程序漏洞、Web 漏洞、弱口令漏洞、配置漏洞、数据库漏洞、服务器漏洞、网络设备漏洞、安全设备漏洞
		1.16漏洞探测模块能同时连接试验网络与分析网络，连接试验网进行漏洞探测，连接分析网进行探测数据传输
		1.17漏洞探测模块探测完毕后将探测数据发送到漏洞探测管理模块，支持探测数据动态增量更新
		1.18漏洞探测模块支持接收漏洞探测管理模块的控制命令与配置信息（开始、停止、探测试验网络 ID、探测 IP 范围）连接相应的试验网络进行漏洞探测

		1.19漏洞探测数据符合统一格式
		1.20支持同时对 1000 个试验网络进行漏洞探测
		1.21可探测有 CVE 编号漏洞数不低于 30000 个
		1.22已公开高危漏洞探测覆盖率和准确率超过 90%
		1.23探测单个节点时间小于 5 分钟
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

漏洞扫描系统 2

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；含 1 个 RJ45 串口，1 个 GE 管理口，6 个 10M/100M/1000M 自适应以太网电口扫描口，1 个接口扩展槽位（支持 4 电、4 光、8 电、8 光），支持 IPv4 和 IPv6 环境的部署和扫描，允许最大并发扫描 60 个 IP 地址，允许最大并发任务≥10 个任务，支持无限个 IP 授权扫描。
		1.2 支持检测的漏洞数大于 10000 条，兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准，并提供 CVE Compatible 证书。产品应支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息。提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。内置不同的漏洞模板针对 Unix、Windows 操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略；支持自动模板匹配技术。支持扫描主流虚拟机管理系统的安全漏洞，如：VMWareESX/ESXi，要求能够扫描大于 100 条相关漏洞。
		1.3 具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用 SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP 等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。支持立即执行、定时执行、周期执行扫描任务，自定义的周期时间可精确至每*月第*个星期*的*点*分。提供通过资产树对资产进行分级管理，支持设备权重设置和可信设备登记，支持将资产信息批量导入到资产树，可在资产树上直接指定主机开展扫描任务。可以通过多种维度搜索定位资产和查看资产风险，包括并不限于：节点或设备名称、资产 IP 范围、资产管理员、

		资产操作系统类型、资产风险等级、漏洞名称、开放的端口、资产 banner 信息等；支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态。
		1.4 内置加固知识库，覆盖常见的 window 和 linux 等系统，内置丰富的加固点击加固操作步骤，并对加固点配置风险值；加固知识库按照高中低分类。
		1.5 支持通过仪表盘直观展示资产风险值、主机风险等级分布、资产风险趋势、资产风险分布趋势等内容，并可查看详情。支持将按 IP 范围、起止时间、任务名称、任务状态、漏洞模板、用户等筛选扫描任务,并对筛选结果进行汇总,和生成在线及离线报表。
		1.6 提供备份恢复机制，能够对扫描结果、扫描模板、参数集等配置文件进行导出和导入操作；能够对系统创建还原点对系统进行备份和还原。提供系统快照功能，当系统出现问题时，可以通过恢复快照，一次性将系统恢复到快照时的版本，并将用户数据一同恢复。
		1.7 漏洞探测类型包括：操作系统漏洞、应用程序漏洞、Web 漏洞、弱口令漏洞、配置漏洞、数据库漏洞、服务器漏洞、网络设备漏洞、安全设备漏洞
		1.8 漏洞探测模块能同时连接试验网络与分析网络，连接试验网进行漏洞探测，连接分析网进行探测数据传输
		1.9 漏洞探测模块探测完毕后将探测数据发送到漏洞探测管理模块，支持探测数据动态增量更新;漏洞探测模块支持接收漏洞探测管理模块的控制命令与配置信息（开始、停止、探测试验网络 ID、探测 IP 范围）连接相应的试验网络进行漏洞探测）漏洞探测数据符合统一格式;支持同时对 1000 个试验网络进行漏洞探测;可探测有 CVE 编号漏洞数不低于 30000 个;已公开高危漏洞探测覆盖率和准确率超过 90%;探测单个节点时间小于 5 分钟
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

漏洞扫描系统 3

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；1TB 硬盘，标准配置 6 个 10/100/1000M 自适应电口，4 个 SFP 插槽,2 个扩展插槽，液晶面板显示，2 个 USB

		口，1 个 Console 口，冗余电源。包含三年漏洞特征库升级，三年硬件维修服务。
		1.2 模块化漏洞扫描系统，Web 扫描域名无限制，Web 扫描任务并发数大于等于 35 个域名。系统扫描 IP 地址无限制，支持扫描 A 类、B 类、C 类地址，系统扫描支持大于等于 200 个 IP 地址并行扫描。
		1.3 产品具备 B/S 架构设计，并采用 SSL 加密通信方式，用户可以通过浏览器远程方便的对产品进行管理。
		1.4 产品具备 DNS 配置，本地可以对互联网远端的 Web 网站进行漏洞扫描
		1.5 产品具备分布式部署需支持自定义管理中心端口号、策略端口号、远端扫描引擎名称等信息
		1.6 产品具备分布式部署提供远端扫描引擎列表，列表需对设备状态、策略同步、规则同步、引擎类型等状态提供最直观的展示效果
		1.7 产品具备以树形结构方式管理，针对树形结构的资产呈现资质风险
		1.8 产品需支持多种扫描方式，提供对 IP、域名、安全域、批量检测等目标扫描方式
		1.9 产品具备支持未知资产探测发现功能，提供基于对 IP、端口的探测功能
		1.10产品具备对未知资产的探测点数、检测耗时、起始/结束时间、检测耗时等详细信息提供实时在线状态查询
		1.11产品应具备操作系统、数据库、网络设备等主流系统的漏洞库列表，并提供至少 20 种以上的漏洞库分类
		1.12产品漏洞库列表数量必须大于 20000 条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准兼容
		1.13产品具备对主流的数据库软件的漏洞检查，支持 Oracle、MySQL、SQL server、DB2 等数据库的安全漏洞检查，并提供至少 3000 种相关漏洞库
		1.14产品具备对 iOS、Android、Blackberry、windowsphone 等操作系统，并提供至少 50 种以上的相关漏洞库
		1.15产品具备对后门检测的安全漏洞检查，包括对 Microsoft IIS 特洛伊木马检测、MacOS X 恶意程序等常见后门漏洞的安全检测，并提供至少 100 种以上的相关漏洞库
		1.16产品具备对网站目录进行扫描识别，并用树形结构展示网站架构
		1.17产品需支持对 Web 网站漏洞扫描的同时，查看网站漏洞情况和 Web 目录结构，数据进行实时同步呈现
		1.18产品具备字典上传功能，基于协议、口令类型的字典自定义设置
		1.19产品具备口令猜解的速率设置，避免因频繁破解导致账户锁定的安全事件

		1.20产品具备中国移动管理信息系统安全的配置核查
		1.21产品具备中国电信的 528 号安全配置核查标准
		1.22产品具备漏洞在线查询功能，可以根据漏洞严重级别进行区别展示，并以颜色对漏洞级别进行区分
		1.23产品具备对检测任务、安全域、资产等类型进行漏洞情况查询
		1.24产品具备以漏洞为中心为查询对象，查询存在漏洞的相关资产，并可以查询深入的详细漏洞明细
		1.25产品具备自定义报表功能，提供对标题、信息、LOGO 等数据的自定义
		1.26产品具备漏洞库升级服务，支持手动、自动升级方式
		1.27产品具备时间、日期管理功能，通过时间服务器调整设备日期与时间
		1.28产品具备告警功能，支持邮件、短信、SNMP、Syslog、FTP、日志存储阈值等多种告警机制
		1.29漏洞探测类型包括：操作系统漏洞、应用程序漏洞、Web 漏洞、弱口令漏洞、配置漏洞、数据库漏洞、服务器漏洞、网络设备漏洞、安全设备漏洞
		1.30漏洞探测模块能同时连接试验网络与分析网络，连接试验网进行漏洞探测，连接分析网进行探测数据传输
		1.31漏洞探测模块探测完毕后将探测数据发送到漏洞探测管理模块，支持探测数据动态增量更新
		1.32★漏洞探测模块支持接收漏洞探测管理模块的控制命令与配置信息（开始、停止、探测试验网络 ID、探测 IP 范围）连接相应的试验网络进行漏洞探测）
		1.33漏洞探测数据符合统一格式
		1.34支持同时对 1000 个试验网络进行漏洞探测
		1.35可探测有 CVE 编号漏洞数不低于 30000 个
		1.36已公开高危漏洞探测覆盖率和准确率超过 90%
		1.37探测单个节点时间小于 5 分钟
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

漏洞扫描系统 4

编号	招标技术指标名称	招标技术指标值
1	性能指标	1.1 标准机架式设备；支持系统扫描、数据库检测、口令猜解，更可扩展 web 扫描，涵盖市面绝大部分设备的漏洞扫描

		1.2 采用验证分析方法，融合最新的操作系统指纹识别、智能端口服务识别等技术，能够准确识别被扫描对象的各种信息
		1.3 运用预探测、多线程的扫描技术，能够快速发现网络中的存活主机
		1.4 产品漏洞库涵盖目前的安全漏洞和攻击特征，漏洞库具备至少 CVE、CNNVD、CNCVE、CNVD、BUGTRAQ 编号；
		1.5 产品扫描信息包括主机信息、用户信息、服务信息、漏洞信息等内容。需给出各类扫描信息的详细列表，支持 60000 种以上漏洞，其中数据库漏洞库为 500 种以上；
		1.6 支持 Windows 域环境扫描，可针对目标主机的系统配置缺陷及漏洞进行扫描；
		1.7 产品支持对扫描对象安全脆弱性的全面检查，如安全补丁、口令、服务配置等。请详细描述针对主机和网络的扫描类别及项目；
		1.8 支持数据库登录扫描，至少应包括数据库账号，密码，SYSDBA、SYSOPER、NORMAL 认证，SID、数据库名称、实例名称及实例号等登录选项的设置；
		1.9 支持 SNMP 等协议的漏洞检测；
		1.10产品要求提供多种缺省扫描策略，并可按照特定的需求，灵活制定目标对象或目标群组，可以同时应用不同扫描策略，并允许自定义扫描策略和扫描参数；
		1.11支持自动定时扫描和多种计划扫描任务管理功能，可按照指定的时间、对象自动扫描，并自动生成报告
		1.12可以并行地检查多个被评估的系统，能够提供扫描策略定制，可以保证扫描的安全性，不影响应用系统和网络业务的正常运行；
		1.13支持口令猜解功能；
		1.14支持扫描范围自定义、资产导入扫描范围、从文件导入扫描范围；
		1.15支持主机存活探测，支持 ARP、ICMP ping、TCP ping 及 UDP ping 四种类型；
		1.16支持 connect、SYN 两种端口扫描方式；
		1.17支持每台主机最大并发检测数设置，支持单个任务并发扫描数设置；
		1.18支持登录扫描，支持 ssh/smb/telnet/pop/pop3/imap/ftp/rsh/rexec/wsus/RDP 多种登录方式；
		1.19设备生产厂商应具备《TL9000 电讯业质量管理体系认证》
		1.20漏洞探测类型包括：操作系统漏洞、应用程序漏洞、Web 漏洞、弱口令漏洞、配置漏洞、数据库漏洞、服务器漏洞、网络设备漏洞、安全设备漏洞
		1.21漏洞探测模块能同时连接试验网络与分析网络，连接试验网进行漏洞探测，连接分析网进行探测数据传输

		1.22漏洞探测模块探测完毕后将探测数据发送到漏洞探测管理模块，支持探测数据动态增量更新
		1.23漏洞探测模块支持接收漏洞探测管理模块的控制命令与配置信息（开始、停止、探测试验网络 ID、探测 IP 范围）连接相应的试验网络进行漏洞探测
		1.24漏洞探测数据符合统一格式
		1.25支持同时对 1000 个试验网络进行漏洞探测
		1.26可探测有 CVE 编号漏洞数不低于 30000 个
		1.27已公开高危漏洞探测覆盖率和准确率超过 90%
		1.28探测单个节点时间小于 5 分钟
2	软件	2.1 设备自带软件，标准版本
3	调试培训服务	3.1 至少一次现场免费培训
		3.2 满足 24 小时热线服务
4	其他要求	4.1 系统组建和实现测试功能等的必备附件
		4.2 系统使用说明书及培训文档
		4.3 订单确认后 2 个月内需要提供设备的安装条件

2、商务需求

序号	目录	商务需求
1	★交货	1.1 交货地点：鹏城实验室指定地点
		1.2 交货期：合同签订后 60 日内（自然日）交付并通过采购人验收。
2	★报价方式及要求	2.1 投标报价必须是人民币含税价（投标价包含所有费用，包含但不限于货物价格、税费、包装、运输、装卸、安装、调试、技术指导、培训、咨询、服务、保险、检测、验收合格交付使用之前以及技术和售后服务、质保期退运返修等其他所有费用）。
3	★付款方式	3.1① 签订合同后支付 50%货款；②设备到货安装验收合格后支付 50%货款。
4	★质保和售后服务	4.1 投标人需为本项目配备足够的售后服务力量。
		4.2 投标人售后服务响应时间：电话响应时间要求 1 小时内，到场响应时间要求 24 个小时内（指从接到报障至到达故障现场的时间）。
		4.3 投标人必须能够随时提供全新备品，一旦设备出现问题必须保证全新备品能在 24 小时内到现场，48 小时内解决相关问题。
		4.4 投标人免费提供技术支持热线电话。
		4.5 投标人免费提供 email 技术支持，并且在 24 小时内回复。
		4.6 投标人提供仪器设备的免费保修期 3 年（保修期内免费维修并更换除消耗品以外的零部件，维修人员的路费、食宿等自理）。
		4.7 投标人提供该设备的技术使用说明书及外购配件仪器说明书，并指导在使用该设备时的操作注意事项等。
		4.8 投标人提供三年特征库/漏洞库免费升级，其中漏洞库更新周期：一周

5	★培训要求	5.1 满足 24 小时热线服务。
		5.2 为保证投标人所提供的仪器设备安全、可靠运行，便于采购人的运行维护，必须对采购人培训合格的维护和管理人员。
		5.3 投标人负责对采购人提供至少一次现场技术培训，以便工作人员在培训后能熟练地掌握系统的维护工作，并能及时排除大部分的系统障碍。
6	运输及包装方式的要求	6.1 设备的包装、运输由投标人负责，应使用崭新坚固的木质包装（标准包装），适合于空运、或陆运等长途运输方式；适合气候变化；投标人应对任何由于不当包装或防护措施不利而导致的商品损坏、损失、费用增长等后果负责。
7	★安装、调试和验收	7.1 投标人货物经过双方检验认可后，签署验收报告，产品保修期自验收合格之日起算，由投标人提供产品保修文件。
		7.2 当满足以下条件时，采购人才向投标人签发货物验收报告： a、投标人已按照合同规定提供了全部产品及完整的技术资料。 b、货物符合招标文件技术规格书的要求，性能满足要求。 c、货物具备产品合格证。
		7.3 投标人技术工程师负责现场的免费安装、调试。
		7.4 仪器设备运抵安装现场后，采购人将与投标人共同开箱验收，如投标人届时不派人来,则验收结果应以采购人和当地商检人员的验收报告为最终验收结果。验收时发现短缺、破损，采购人有权要求投标人立即补发和负责更换。
		7.5 投标人应提出仪器设备测试的内容、项目、指标和方法,投标人有责任对采购人的技术人员提出的问题作出解答。测试应进行详细记录，仪器设备测试结束后，由投标人技术人员签字后交给采购人验收。
		7.6 保修期自最终安装验收合格后开始，保修期内卖方要保修除消耗品以外的所有部件。在保修期内，如果仪器设备发生故障，投标人要调查故障原因并修复直至满足最终验收指标和性能的要求，或者更换整个或部分有缺陷的材料。以上都应是免费的。
8	质量及知识产权要求	8.1 投标人提供完好、全新的原包装产品（包括零配件），随机技术资料齐全。产品符合国家质量检测标准，必须具有生产日期、厂名、厂址、产品合格证等。进口产品须提供海关进货单（复印件备查）。 8.2 采购人在中国使用该货物或货物的任何一部分时，免受第三方提出的侵犯其专利权、商标权或工业设计权等知识产权的起诉或司法干预。如果发生上述起诉或干预，则其法律责任均由投标人负责。

第四部　评审标准

评审项目	评议内容	分值	评分细则
技术标（J）（40分）	对技术条款的响应程度	32	投标人应如实填写《技术条款响应表》，评审委员会根据技术需求参数响应情况进行打分，各项技术参数指标及要求全部满足的得32分，标“▲”指标参数为重要技术指标项，每负偏离一项扣5分；其他一般参数每负偏离一项扣3分，扣完为止。 标“▲”指标参数要求提供相应的截图等有效证明材料，否则做负偏离评审。
	技术保障措施	3	1、实施项目经理具有信息系统项目管理师资格证，得0.5分，否则不得分； 2、实施项目经理具有服务项目管理人员高级项目经理资格证，得0.5分，否则不得分； 3、项目团队人员（不少于10人，项目经理除外）情况： (1) 信息安全保障人员认证证书不少于4人； (2) IT服务工程师或IT服务经理不少于2人； (3) 通信专业中级或以上工程师不少于 2人； (4) 计算机高级工程师不少于1人； (5) 网络工程师不少于1人 人员不满10人不得分。人员超过10人，且完全满足5项得2分，满足4项得1分，不足4项不得分。同一人员满足不同条件只计为一人。要求提供相关人员2019年8月-10月社保证明及相关证书扫描件，原件备查。
	产品的质量可靠性和先进性	5	投标产品技术先进性： 优：最新型的产品，代表该设备最先进水平；技术成熟、设备可靠，综合优，得5分。 良：该产品类似项目经验丰富，同类产品应用广泛，且用户反应良好，得3分。 中：技术成熟、设备可靠，类似项目经验一般，同类产品应用较少，得1分。 差：不得分。
价格标（G）（40分）	投标总价	40	得分按以下公式计算：得分=Z/Sn×40 其中：Z--通过资格性审查和符合性审查且报价不超过预算控制金额的最低评标报价。 Sn--通过资格性审查和符合性审查且报价不超过预算控制金额的评标报价。 根据财政部、工业和信息化部关于《政府采购促进中小企业发展暂行办法》第五条的规定，评委按照投标人提供的《中小企业声明函》中的相关内容，对同时符合以下条件的投标价格给予6%的扣除，扣除后的价格作为投标人的评审报价进行价格评比： ① 投标人为小型或微型企业； ② 所投全部投标产品、承担的项目全部工程或者全部服务

			均由小型或微型企业制造或提供。 评标价计算公式：若投标人适用《政府采购促进中小企业发展暂行办法》：投标人评标报价=投标报价*（1－6%）若投标人不适用《政府采购促进中小企业发展暂行办法》：投标人评标报价=投标报价
商务标（S）（20分）	对商务条款的响应程度	2	全部满足得 2 分，每负偏离一项减 1 分，扣完为止。
	同类业绩	3	投标人近三年(2016 年 1 月至今）完成的同类业绩，每提供一个得 1 分，最高得 3 分，未提供的不得分。投标人必须在投标文件中提供每一个项目的合同关键页和加盖公章的验收报告复印件，否则不得分。
	施工安全保障措施	8	1、具有信息安全管理体系认证证书（认证范围必须包含计算机软件开发的信息安全管理）得 1 分； 2、具有 IT 服务管理体系认证证书（认证范围必须包含系统集成的硬件及软件维护）得 1 分； 3、具有 ITSS 信息技术服务运行维护资质得 2 分； 4、具有省级或以上企业技术中心得 2 分； 5、具有省级或以上工程中心得 2 分。 要求提供以上所有相关认证（资质）文件扫描件，（原件备查）作为得分依据。评分中出现无证明资料或专家无法凭所提供资料判断是否得分的情况，一律作不得分处理。
	售后服务	2	投标人在深圳市内设售后服务网点得 2 分，在广东省内设售后服务网点得 1 分，其它不得分。 需提供工商注册证明或房屋租赁合同复印件，并加盖公章。
	诚信	5	根据《深圳市财政委员会关于印发〈深圳市政府采购供应商诚信管理暂行办法操作细则〉的通知》(深财购[2017]42 号）的要求，投标人在参与政府采购活动中存在诚信相关问题且在主管部门相关处理措施实施期限内的，本项不得分，否则得满分。投标人无需提供任何证明材料，由工作人员向评审委员会提供相关信息
总得分（N）		100	N= J+G+S