## 核心产品：主动探测引擎

## 是否有强制节能产品（具体哪些产品）：无

## 交货地点：营口市公安局指定地点

## 交货时间：合同签订后10个工作日内

## 付款方式及条件：验收合格后先支付95%，剩余5%一年后付清

## 技术要求

### 平台通用硬件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 配置要求 | 单位 | 数量 |
| 1 | 业务服务器 | ★1.2U标准式机架设备、★2.至少提供4个千兆电口+2个万兆光口、★3.cpu≥12核24线程\*2、★4.内存≥256G、★5.≥4TB\*12硬盘、双电源；服务器用于部署等级保护子系统实时监测子系统威胁感知子系统通报预警子系统快速处置子系统内外网各一台 | 台 | 2 |
| 2 | 业务服务器 | ★1.2U标准式机架设备、★2.至少提供4个千兆电口+2个万兆光口、★3.cpu≥12核24线程\*2、★4.内存≥256G、★5.≥4TB\*12硬盘、双电源；服务器用于部署数据支撑子系统内外网各一台 | 台 | 2 |
| 3 | 千兆交换机 | ★1.不少于2个万兆光口2.48个千兆电口；1. 包转发率≥240Mpps，
2. 交换机容量≥480Gbps，
3. 支持LACP，支持端口镜像；
4. 至少提供2个万兆多模光模块。
 | 台 | 2 |
| 4 | 防火墙 | ★1.吞吐量>8Gbps,最大并发连≥300万；1. 每秒新建连接数≥10万，
2. 3.2U标准机架设备，
3. 4.标配不少于12\*GE电口，12\*SFP光口。

功能要求：1.支持应用识别，内置5000种以上应用特征库，并可识别iOS、安卓等移动互联网软件如微博、微信等特征，并可智能识别P2P和迅雷行为，并支持在线升级和手动升级2.支持自定义应用，可基于协议、端口、IP、域名等维度定义未知应用支持IP准入、MAC准入、IP+MAC准入、本地WEB认证、Portal认证、短信认证、免认证、微信认证、混合认证、AD域单点登录和访客二维码认证3.支持IPv4、IPv6双协议栈异常包攻击防御，攻击类型至少包含：PingofDeath、Land-Base、TearDrop、TCPflag、Winnuke、Smurf、IP选项、IPSpoof、Jolt2等4.支持扫描攻击防御，可基于设定的阈值识别扫描，并自动对发起扫描的主机进行限制5.支持基于目的IP和接口的SYN、UDP、ICMP、DNS等flood攻击防御6.内置不少于8000条IPS规则库，包含安全漏洞、CGI攻击、缓存溢出、木马后门、网络数据库攻击、蠕虫病毒、间谍软件、欺骗劫持等安全类型；并支持在线升级和手动升级7.支持对最多20级的压缩文件进行解压查杀8.提供在设备端上的全网威胁情报的搜索查询，包括IP、域名、文件（MD5/SHA1等）情报的查询9.提供最新的威胁情报信息，能够对新爆发的0day、高危漏洞等进行预警，并提供配置向导协助管理员生成安全防护策略10.支持实时获取威胁情报，并应用威胁情报对本地资产进行威胁检测，并可对检测到的威胁情报11.支持基于资产的安全分析，支持展示网络中存在安全风险的资产以及对应的风险级别，至少可查看资产基本信息、攻击态势、攻击日志统计、攻击的具体事件类型、攻击时间等 | 台 | 2 |
| 5 | 单向光闸 | ★1.发送端至少提供2个10/100/1000MRJ45接口，2.接收端至少提供2个10/100/1000MRJ45接口，★3.不少于2个USB口，1个Console口；★4.单向传输速率≥1000Mbps；系统整体时延：<5毫秒；支持HA模式。 | 台 | 1 |
| 6 | 机柜 | 42U标准服务器机柜 | 台 | 2 |
| 7 | PDU电源 | 防雷PDU机柜插座不低于8位总控全长大于1.8米 | 件 | 2 |
| 8 | 平台PC控制端 | 1. 不低于i7处理器，（同类产品即可，不低于其主频及参数）
2. ≥32G内存，
3. ≥1T存储空间
 | 台 | 3 |

### 可视化展示通用硬件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 配置要求 | 单位 | 数量 |
| 1 | 拼缝标亮LCD拼接显示单元 | ★1.面板尺寸不小于55寸，拼缝不大于2.5mm，分辨率不低于1920\*1080；2.亮度不低于500cd/m2，对比度不低于1200:1；3.提供多种视频输入接口：至少包含1个DVI接口，1个HDMI接口，1个VGA接口；4.内置图像拼接显示功能，支持拼缝补偿5.支持屏幕防灼，图像翻转6.支持白平衡调整，调整范围不小于视角：178°(水平)/178°(垂直)7.支持面板工作时长记录及显示8.支持快速设置拼接单元ID，现场调试更方便9.支持倍帧功能10.支持通电后延时启动功能 | 台 | 6 |
| 2 | 拼接屏直立式支架底座 | 55寸拼接屏直立式支架底座-3.5-H60(模块化落地式) | 套 | 3 |
| 3 | 拼接屏直立式支架单元 | 55寸拼接屏直立式支架单元-3.5(模块化落地式) | 套 | 6 |
| 4 | DVI-D线缆 | 10米DVI-D线缆-拼接屏专用 | 条 | 6 |
| 5 | 综合显控单元8路输出 | ★1.不少于2个标准RJ45（10/100/1000Base-T）接口，2个USB3.0接口；★2.最少支持输入8路；最少支持输出8路，每路输出支持1/3/4/6/7/8分屏；3.支持高清，标清混合解码上墙；4.可解码显示12\*1200W@20/12\*4K@30/48\*1080P@30/108\*720P@30；5.拥有自主知识产权的解码算法，解码效率高，图像清晰6.支持G.711A、G.711U、AAC-LC的音频格式的解码；7.支持开窗、漫游、画中画功能；8.支持接受中心服务器对设备业务进行配置和管理；9.支持单路视频输出的分屏处理，最大16分屏；10.支持IP协议的组播传输方式；11.支持本地升级和远程升级； | 台 | 1 |
| 6 | 可视化展示控制台PC | 1.不低于i7处理器，（同类产品即可不低于其主频及参数）2.1T以上存储空间，3.不低于RTX3070显卡（相同功能即可，不限于该型号） | 台 | 2 |
| 7 | 22U网络机柜 | 600\*600\*1200；19英寸标准；冷轧钢材； | 台 | 1 |
| 8 | PDU机柜插座 | 机柜开关电源；不少于8位10A新国标孔；输入电流16A；承载功率400W | 台 | 1 |
| 9 | 电源控制顺序管理器 | 最大支持30A大电流继电器；承载不小于8台设备转换； | 台 | 1 |
| 10 | 数字效果器混响器 | 输入通道；单声道；立体声；输出通道；输入通道功能PADDSPPEAKLED；usb输出电平；幻象电源电压+48V； | 台 | 1 |
| 11 | 声频功率放大器 | 频率相应40Hz-18KHZ（正负0.5dB）；总谐波失真40HZ-18KHZ(大于或等于0.2%)；信噪比小于76dB | 台 | 1 |
| 12 | 室内外防水扩音器 | 内置扬声功能；4.5高保真单元；全铝合金外壳；铝合金网罩 | 台 | 4 |
| 13 | 鹅颈式远程通话器 | 金属鹅颈360°；发射功率300mW；调制方式FM；高次谐波>40db；防干扰； | 套 | 1 |
| 14 | 室内铺设-电源线 | 国标；铜芯RVV护套线；三芯；平方2.5户外电缆电源电线 | 米 | 250 |
| 15 | 室内铺设-网线 | 国标；高速超六类；纯无氧铜POE；内外非屏蔽千兆网线UTP-CAT6 | 米 | 250 |
| 16 | 室内铺设-HDMI高清线 | 国标；2.0高清线；4k数据线；笔记本音视频线； | 条 | 3 |
| 17 | 室内铺设-扬声线 | 国标；紫外线；纯铜工程线；无氧铜； | 米 | 150 |
| 18 | 室内铺设-音频线 | 国标；aux音频线；3.5mm公对公； | 米 | 17 |
| 19 | 室内铺设-插排 | 开关电源；5位10A新国标孔；输入电流16A；承载功率300W | 个 | 4 |
| 20 | 铝合金防踩踏地槽 | 铝合金材质；国标； | 米 | 10 |
| 21 | 背景墙 | 背景墙颜色定制；形象标识和上级部门统一标准； | 平方米 | 20 |
| 22 | 电视墙 | 电视墙颜色定制；形象标识和上级部门统一标准； | 平方米 | 20 |
| 23 | 条形屏 | 国标；定制 | 米 | 12 |
| 24 | 射灯 | 超亮轨道灯30瓦；导轨灯； | 个 | 5 |
| 25 | 背景墙电源线 | 国标；铜芯RVV护套线；二芯；平方1.0户外电缆电源电线 | 米 | 30 |

### 3平台专用硬件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 配置要求 | 单位 | 数量 |
| 1 | 主动探测引擎 | 在互联网上部署探测，对辖区网络资产和系统进行主动探测，监测重要信息系统遭攻击情况、安全隐患和安全运行情况。包括安全漏洞、木马、可用性等监测数据。★硬件规格：2U★内存：≥32G★硬盘：≥1T\*1★网口：至少提供千兆RJ45网口\*2个电源：1+1冗余电源★每台至少150个监测资产能力功能要求：1.提供日志自动审计功能，根据指定的审计标准自动、定时审计；并将审计结果发送到指定邮箱当中。2.厂商漏洞策略库提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与国际CVE、国内CNNVD漏洞库标准兼容。3.存在误报漏洞可通过产品在扫描结果处一键反馈给厂商协助修改；4.支持识别被扫描目标对象的网站响应状态，能根据不同的响应状态直观呈现不同颜色标识；5.管理人员可根据系统给出的漏洞参数、HTTP请求/响应数据，快速验证，一键验证漏洞6.支持对网站的应用可用性监测，访问延时监测，能及时识别网站的应用异常；7.支持按分、小时、天的时间设置监测频率8.支持首页变更监测，支持网站黑页监测，支持对网站源码比较。9.产品具备国家信息安全漏洞库《兼容性资质证书》10.产品具备公安部的《计算机信息系统安全专用产品销售许可证》（增强级） | 台 | 2 |
| 2 | 流量监测引擎 | ★在重点单位网络出口、我市网络出口、骨干节点、城域或运营商主干链路进行流量分光，流量监测设备进流量还原与检测，含特征匹配、异常检测，检测内容包括病毒、木马、蠕虫等恶意流量、恶意攻击流量，可针对重点关注的应用或协议进行分析。默认单台引擎支持≥10Gbps网络层吞吐量功能要求：1.支持审计http、ftp、smtp、pop3、smb、imap、dns等协议报文，并提供审计协议类型的端口号配置，可根据需要变更端口号2.支持解析Mysql/MSSQL/DB2/Oracle等协议报文3.支持LDAP登录行为的识别4.具备VXLAN镜像流量的检测功能5.具备对HTTPS流量解析能力6.支持检测WEB攻击、异常访问、恶意文件攻击、C&CIP/URL、WEB后门访问、发件人欺骗、邮件头欺骗、邮件钓鱼欺骗、邮件恶意链接、DGA域名请求、SMB远程溢出攻击、暗链、WEB行为分析等风险7.可自动对内网主机进行威胁指数分析，详细展示具体的威胁指数、威胁活动、历史威胁指数、遭受的攻击类型、攻击次数、攻击状态等8.自动关联行为分析的详细展现，包含SQL注入取数据、表单破解、XSS测试、目录穿越读取文件、多人访问Webshell、APT攻击等9.对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接10.通过分析文件中的二进制代码，找到文件溢出攻击的代码，并能找到APT攻击中的0day攻击 | 台 | 1 |
| 3 | 网络资产普查系统 | ★软硬一体化2U标准机架式设备；1+1冗余电源；可用磁盘空间不小于1T，可用内存不小于32G；至少标配4电口，可扩展4电4光或8电或8光或2万兆光。功能要求：1.提供审计功能，能够对登陆日志、操作日常进行记录和查询，并可以将日志导入导出操作。2.提供日志自动审计功能，根据指定的审计标准自动、定时审计；并将审计结果发送到指定邮箱当中。3.厂商漏洞策略库大于35000条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与国际CVE、国内CNNVD漏洞库标准兼容。4.系统内置不同的策略模板如针对Linux、Windows操作系统等模板，同时允许用户定制扫描策略；用户可定义扫描范围、定义扫描端口、扫描使用的参数集等具体扫描选项。5.支持Windows系列操作系统，支持Linux主流操作系统（Centos、Redhat、Debian、Fedora、Ubuntu、Suse等），支持Unix主流操作系统（AIX、HPUX、Solaris等）；6.支持对Web、FTP、电子邮件等应用系统、Apache等web中间件服务器以及Office等常用软件进行漏洞扫描；7.可以自定义扫描端口范围、端口扫描策略提供采用SMB、SSH等协议对Windows、Linux系统进行登录授权扫描。8.具备弱口令扫描功能，提供多种弱口令扫描协议，包括SMB、RDP、SSH、TELNET、FTP、SMTP、IMAP、POP3、MySQL、MSSQL、REDIS、RTSP]等协议进行弱口令扫描，允许用户自定义用户、密码字典。9.支持发现非默认端口启动的服务，支持务的协议识别、版本10.可根据端口识别出的软件版本提供可能存在的相关漏洞列表 | 套 | 1 |

### 4平台软件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 系统名称 | 内容及功能要求 | 单位 | 数量 |
| 1 | 实时监测系统 | 实时监测系统主要用于管理平台数据采集引擎设备的各类安全监测设备及策略和任务，能及时发现、识别网络攻击威胁，监测恐怖组织、黑客组织、不法份子等的攻击活动、攻击行为、攻击方法手段；监测重点保护对象所受的攻击威胁、破坏、窃密、渗透等情况，以及重点保护对象的网络、系统、大数据等安全状况、存在的漏洞、隐患等，为快速处置、通报预警等系统提供基础支撑。功能要求：1.支持查看平台监测的系统数、安全事件数、安全隐患数、设备告警数；2.支持查看安全事件和安全隐患的区域分布；3.支持查看安全事件、安全隐患和设备告警的趋势统计。4.支持安全事件分类统计和事件及隐患的行业排名。5.建立全维度实时监测体系，监测方式至少包括：网站监测、流量检测、资产探测、后门检测。6.支持任务详情查看，包括历史监测记录，单次监测任务详情，任务状态等；7.支持按照事件告警级别、数据类型、风险类别、客户端IP、响应码、时间范围等查询告警信息，并支持导出。支持隐患录入和查看、导出网站累计隐患列表及列表报告下载。8.支持对针对扫描出的隐患做通报，包括对公安、单位发布提醒或者发布限期整改。9.提供日志自动审计功能，根据指定的审计标准自动、定时审计；并将审计结果发送到指定邮箱当中。10.支持识别被扫描目标对象的网站响应状态，能根据不同的响应状态直观呈现不同颜色标识；11.管理人员可根据系统给出的漏洞参数、HTTP请求/响应数据，快速验证，一键验证漏洞12.支持对网站的应用可用性监测，访问延时监测，能及时识别网站的应用异常； | 套 | 1 |
| 2 | 等级保护系统 | 系统的主要功能包括等级保护概况一览、重要信息系统所属单位管理、重要信息系统管理、等级保护测评报告管理、等级保护测评机构管理、等级保护测评项目管理、等级保护数据统计分析和等级保护政策法律法规管理等，并能实现与等级保护检查工具箱进行对接。功能要求：1.支持直观展示当前账号的等保待处理信息，包括备案待审批、测评待审批、已申请发证待审批、备案变更待审批、备案撤销待审批、复测评待审批等统计数量。支持直接跳转到相应的待审批页面。2.支持单个录入、单个导入、批量导入的方式录入备案系统信息；支持第三级以上信息系统提交附件。并支持预览导入的备案系统信息。3.支持按等级保护级别、备案状态、测评状态、时间、关键字等条件快速查询筛选出系统，支持组合查询。并支持按系统所属的状态快速筛选。4.支持查看备案单位信息、系统信息、系统定级情况、第三级以上信息系统提交材料情况。5.支持对全国的测评机构进行管理，包括查看、新增等操作，并支持计算机构信誉度。6.支持对待测评、已测评系统进行列表、查询，可按照测评时间、区域、行业、测评机构、等保级别、关键字等综合查询；7.支持对测评师进行管理，包括查看测评师编号、所属机构，并支持计算测评师信誉度。8.支持按任务名称、类型、被检查的系统，进行检查任务创建。支持多个系统批量检查任务下发。9.支持对辖区内备案单位、备案系统、已测评系统、已发证系统进行汇总统计。10.支持按区域、按行业、按单位、按系统统计系统定级情况和等保状态情况。11.支持查询系统全部的备案单位，备案系统，支持导出支持批量导出系统信息。12.支持等保相关的各类文件资料的上传、下载、删除。 | 套 | 1 |
| 3 | 态势感知系统 | 基于多维态势可视化技术，对网络空间安全相关信息进行汇聚融合，形成针对人、物、地、事、关系的多维视图，从不同视角出发感知网络安全态势。系统主要包括总体态势、资产态势、隐患态势、攻击态势、事件态势和通报态势六大视角。功能要求：1.支持网络安全总体态势分析，包括当前监管对象统计、实时监测隐患数统计、通报预警统计、风险趋势、高危系统排名、高危地区排名、监测对象分布统计、事件与隐患统计、通报预警统计等内容。2.监管对象分类至少包含IDC单位数、备案单位数、备案系统数、等保单位数、等保系统数和政府网站数等几类。实时监测隐患事件分类至少包含服务器后门、DDOS攻击、僵木蠕病毒、非法系统、入侵事件等类型。3.支持按时间、监管对象或行业对隐患区域位置统计、行业隐患分布和高危系统排名等内容进行筛选统计展示。4.支持对struts2、webshell等专项隐患进行消息推送。5.隐患区域位置统计、行业隐患分布、高危系统等内容需支持详情展示,展示隐患排行TOP5的系统6.支持按时间、攻击类型分布、攻击区域（境内攻击源/境外攻击源）、攻击IP/受攻击IP排名等内容进行筛选统计和展示。7.支持安全事件分析，内容需包含重点监测系统数、安全事件数、安全事件分类统计、事件趋势、最新事件概览、事件类型分布、事件区域排名、事件取证展示等。8.支持按时间、监管对象或行业对安全事件分类统计、事件趋势、最新事件概览、事件类型分布、事件区域排名、事件取证等内容进行筛选统计和展示。9.支持通报预警分析，内容需包含区域通报处置总体概览、通报统计、反馈情况统计、通报处置效率统计、通报预警趋势、隐患通报概览、事件通报概览、区域处置统计、行业分类统计等。10.支持对预警、处置的效率进行可视化呈现，可对某辖区工作量进行直观考核和评价。11.支持对区域通报统计、反馈情况统计、通报效率统计、通报预警趋势、区域处置统计、行业类型统计、处置效率统计等内容需支持详情展示。12.支持多种统计方式实现及可视化展现当前通报、处置状态，并且支持多层交互。 | 套 | 1 |
| 4 | 通报预警子系统 | 通报预警系统是根据获取的态势、趋势、攻击、威胁、风险、隐患、问题等情况，利用通报预警系统汇总、分析、研判，并及时将情况上报、通报、下达，进行预警及快速处置。功能要求：1.支持接入第三方数据源上报的网络安全事件2.支持对安全事件进行管理，并可通过区域、发现时间、事件等级、事件类型、发现厂商、通报状态、关键字等进行高级查询3.支持WEB端通报、APP通报多种通报方式；4.支持隐患录入和查看、导出网站累计隐患列表及列表报告下载。5.支持对针对扫描出的隐患做通报，包括对公安、单位发布提醒或者发布限期整改。6.支持对选择的公安和单位发布通知，可以快速切换我发出的通知和我收到的通知。7.支持将我发送的通报、我收到的通报和抄送我的安全事件通报进行统一汇总，可查看通报的事件信息，包括通报的详情（包括发布人、接收人、通报状态等）、事件详情、该次通报的通报记录等信息，实现对整个通报过程进行跟踪记录。8.支持通报的签收、处置和反馈；9.支持Web端通报和手机APP通报的同步发布、接收、和处置反馈；10. 支持对通报过程进行跟踪记录，完整记录预警任务发起、查阅、处理和审核等各阶段的时间点、处理人员和操作内容等详情，查看网站详情、通报记录、隐患详情；11.将我发送的通报、我收到的通报和抄送我的安全隐患进行统一汇总，包括隐患提醒管理和整改管理两项内容12.支持提醒管理，对发现的最新隐患发布提醒或下载报告，支持指定通知接收人、通报类型、隐患详情描述及上传附件。13对发现的最新隐患下发限期整改通知或下载报告，支持指定通知接收人、整改类型、整改限期日期、隐患详情描述及上传附件。 | 套 | 1 |
| 5 | 快速处置子系统 | 对网络安全事件、案件进行处置的管理平台，支持与应急处置工具箱对接功能要求：1.首页统计展示该地转递线索数、任务总数、处置中的事件数、已办结的事件数2.支持系统的数据同步3.支持线索生成任务4.安全事件发生时，支持将安全事件转为快速处置任务，新增任务、批量上传任务，新建任务时支持新建处置策略，处置策略可自定义，如：简易处理、常规处理、全面处理。5.支持下载任务、办结任务及批量办结任务6.支持对任务的复核，可下载具体任务处理过程的相关文件，可填写复核意见7.支持对整改建议的管理，包括上传、下载、删除资料8.支持新增策略，可选择加入现有的策略组9.支持查询、编辑、删除及批量删除策略10.支持新增策略组，可自定义选择具体的策略组合 | 套 | 1 |
| 6 | 数据支撑子系统 | 提供标准的接口，可采集各种外部数据，并进行格式泛化和预处理，可通过光闸同步到数据支撑子系统；功能要求：支持Syslog、FTP、https协议日志收集；支持安全事件标准协议的数据；支持多文件类型的复合数据；支持动态配置模板来支持新的数据源；支持对CPU，内存，硬盘，网络等硬件资源的监控；支持对各种数据源的入库速度监控；支持对平台本身关键运营参数监控；支持对监控对象某些指标超过阈值的告警；支持识别监管对象异常的变化识别和告警；支持通过光闸从互联网把数据传输到专网；支持通过光码从专网把数据传输到互联网；支持传输过程中包括文本流和文件流；支持传输过程中根据设备要求自动拆分，组包和校验；支持传输的数据包括灵活形式的web请求转发；支持对各种来源日志进行归一化处理；支持对各种来源日志进行IP详细信息，域名详细信息，单位信息等信息的补充完善；支持对地面的不同形式描述进行标准化处理；支持识别质量低下的数据并且归档记录；支持对各种来源日志合并到最终统一数据流进行基础和高级分析；支持多租户的数据空间隔离；支持对各种来源安全事件自动智能转换到标准分类；支持对相似日志的多种去重合并算法；支持对全库数据的复杂条件查询；支持对各种数据源多种维度的分布统计；支持对各种数据源多种维度的时间轴统计；支持对各种数据源多种维度的重要性聚合； | 套 | 1 |

### 5平台服务

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 名称 | 服务要求 | 服务时间 |
| 1 | 漏洞验证服务 | 对网站监测发现的漏洞隐患提供人工验证服务。提供100个网站的验证，每年不超过500个问题记录。提供对恶意IP、恶意URL、恶意程序、漏洞隐患、攻击事件等多种来源的网络安全威胁情报。 | 1年 |
| 2 | 驻场服务 | 提供1人1年驻场服务,对威胁情报提供人工验证、威胁手段分析、威胁追踪溯源等技术支撑。 | 1年 |