招标项目技术、服务、政府采购合同内容条款及其他商务要求

一、项目概况（本项目作为项目介绍，不作为评定项）

为应对随着网络大环境不断变化带来的网络安全威胁，提高四川体育职业学院网络安全防护设备的网络风险防控能力，拟采购一批网络安全态势感知平台设备来实时检测系统的网络安全风险和威胁。

二、★项目清单

序号	采购标的	采购数量	单位	备注
1	态势感知平台（核心产品）	1	台	不允许进口产品参与
2	探针	1	台	
3	数据中心防火墙	2	台	
4	安全运营服务平台	1	项	

三、项目技术参数

序号	名称	技术参数要求
1	态势感知平台	1、★内存≥96GB DDR4 2933，系统盘≥240GB SATA SSD，数据盘≥32TB，冗余电源，接口≥4千兆电口。授权及售后要求：配置≥3年特征库升级，≥3年软件升级、硬件维保。 2、▲具备威胁定性引擎，支持通过告警的上下文关联、时序关系结合威胁情报与专家经验对安全告警进行目的性确认以及优

		先级顺序。告警分类纬度包括人工渗透、程序自动化、业务相关风险和其它。**（提供具有 CMA 或 CNAS 资质的检测机构出具的检测报告复印件并加盖投标人公章）** 3、支持一键下发对探针进行监控检查，快速判断当前设备运行是否存在风险，并针对风险点给出具体处置建议，检查结果支持通过邮件推送给管理员。 4、支持通过流量检测出网络设备，并进行可视化绘制。 5、支持等保合规性检查，实时监测等保差距项和高风险项防止由于策略变化导致不合规。 6、▲具备挖矿检测能力，支持规则库的本地检测和主动探测的云端检测。挖矿事件展示纬度包括：事件发生时间、挖矿阶段、威胁等级/描述/定性/情报、攻击次数。**（提供具有 CMA 或 CNAS 资质的检测机构出具的检测报告复印件并加盖投标人公章）** 7、▲支持订阅推送，推送的形式包括短信、邮件、微信，推送的内容包括安全事件、脆弱性以及外部攻击，其中推送的频率可自定义。**（提供具有 CMA 或 CNAS 资质的检测机构出具的检测报告复印件并加盖投标人公章）** 8、▲支持导出 PPT 格式的风险报告，报告内容至少包含脆弱性感知、外部威胁感知、主机安全风险、工单以及综合安全风险，并且支持快速生成月报、季度报、年报。**（提供具有 CMA 或 CNAS 资质的检测机构出具的检测报告复印件并加盖投标人公章）** 9、支持各类大屏展示，3D 地球大屏展示网络攻击态势，包括攻击次数、遭受攻击资产组、攻击源地址、攻击源 IP、攻击手段排行、遭受攻击服务器排行，支持境外、境内切换。 10、具有资产管理功能，能够新增资产、编辑资产、查看资产，能够新增资产组、编辑资产组、删除资产组，能够批量导入资产。 11、提供云端威胁情报查询，查询结果需包含：IP 主机信息、IP 位置信息、域名流行度、情报 IOC 详情、相关样本、可视化

		分析、域名解析记录、域名注册信息、关联域名、数字证书等信息。
2	探针	1、★性能参数：网络层吞吐量≥2Gbps，应用层吞吐量≥600Mbps，内存大小≥8G，硬盘容量≥480GB SSD，冗余电源，千兆电口≥6个，万兆光模块≥2个，≥3年软件升级、硬件维保。 2、支持流量抓包分析，定义配置源IP、源端口、目的IP和目的端口、传输层协议以及标签类型。 3、支持旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响。 4、支持根据数据包方向、协议、端口、IP地址等信息自定义应用规则来识别应用类型。 5、支持流量白名单，过滤掉不关注资产流量，白名单类型应包括IP、端口、域名。 6、支持自定义内网服务器IP组、客户端IP组，用于识别资产信息。定义的时间段内不能访问或能访问某服务器。 7、支持对HTTP未知站点下载可执行文件、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。 8、支持传输协议审计日志、DNS协议审计日志、邮件协议审计日志、SMB协议审计日志、AD域日志、WEB登录日志、FTP日志等。 9、▲支持敏感信息检测，检测内容至少包括身份证、手机号码、银行卡号、邮箱；支持基于IP和域名的旁路阻断。**（提供对应功能截图加盖投标人公章）**

3	数据中心防火墙	1、★标准机架式 2U 设备，网络层吞吐量≥20G，应用层吞吐量≥9G，IPS 吞吐量≥1G，并发连接数≥200 万，接口要求：≥8 千兆电口，≥2 万兆光口。配置≥3 年入侵防御特征库升级，≥3 年病毒过滤升级，3 年实时漏洞分析，≥3 年 Web 应用防护规则库升级，≥3 年威胁情报。 2、同时支持 IPV4 及 IPV6 协议。 3、支持自定义安全策略，安全策略组功能；可针对源、目的、协议、用户、时间等进行访问控制策略配置。 4、路由协议：支持动态地址转换、静态地址转换以及端口地址转换功能，支持 OSPFv2/v3 等路由协议。 5、▲具备未知威胁防护能力，支持评估现网风险业务总数、开放勒索病毒常用端口、弱口令、感染勒索病毒业务数量。**（提供对应功能截图和具有 CMA 或 CNAS 资质的检测机构出具的检测报告复印件并加盖投标人公章）** 6、支持通过 TCP 代理及 SSL 代理等方式对 https 进行解密。 7、支持 ftp 协议命令控制功能，避免互联网服务遭受篡改等攻击。 8、▲具备云威胁情报能力，通过主动探测和威胁情报，对危险流量进行拦截和实时检测，并且支持分布式节点加速。支持拦截的威胁类型至少包括挖矿、黑客工具、木马远控、恶意 URL、僵尸网络。**（提供对应功能截图和具有 CMA 或 CNAS 资质的检测机构出具的检测报告复印件并加盖投标人公章）** 9、支持三权分立功能，具备安全管理员、审计员、系统管理员三种角色。 10、产品支持基于 IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL 等应用协议进行深度检测与防护。

		11、▲支持服务器漏洞防护、Cookie 攻击防护、压缩病毒文件防护，针对漏洞的扫描攻击可进行 IP 记录和封锁。**（提供对应功能截图加盖投标人公章）** 12、▲漏洞攻击特征识别库内置数量不少于 17000 项，WEB 应用攻击特征内置数量不少于 4800 项，僵尸网络与病毒防护库内置数量不少于 160 万项。**（提供对应功能截图并加盖投标人公章）** 13、防火墙本地日志存储空间不足时支持日志服务器存储，支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间。 14、支持多对一、一对多和一对一等多种地址转换方式。支持 NAT44、NAT64、NAT66 地址转换方式。支持 NAT 穿透技术 ALG，支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 15、支持手机微信端接收防火墙告警和事件并且支持一键封锁 IP。
4	安全运营服务平台	1、★支持数据中心资产（IP）数量≥50 个、服务期限：3 年；支持安全组件可接入≥6 个；组件日志留存时间≥6 个月，40G；日志处理能力≥500Mbps；监测报告 1 月≥4 份。 2、支持人工实时监控与管理，提供 7*24 的安全事件监控、分析与响应服务，确保对安全威胁的即时发现与处理。 3、支持 IDS、IPS、资产管理系统、资产扫描系统、漏洞扫描系统、漏洞管理系统、防火墙、EDR 等安全组件的信息汇聚。 4、支持在安全事件发生时，初步研判、事件分析、根因分析、修复建议和后续改进措施。 5、▲支持自定义日志清洗规则设置，可根据源 IP、目的 IP、威胁名称、告警组件、威胁等级、攻击结果、周期性重复告警频率等条件对安全组件日志进行清洗。**（提供产品功能截图并加盖投标人公章）** 6、支持统一汇聚显示多安全组件来源的安全告警，显示字段包

		括告警时间、源 IP、目的 IP，威胁等级、报告来源、攻击链阶段、协议、威胁名称。 7、▲支持手动录入漏洞，包括受影响 url、漏洞名称、漏洞库编号、漏洞描述、漏洞载荷信息、修复建议、漏洞等级、关联资产等信息。**（提供产品页功能截图并加盖投标人公章）** 8、▲支持对资产测绘引擎进行汇聚管理，能够在 MSS 向资产探测引擎下发任务。能够对扫描任务指定任务名称、探测目标、端口范围、扫描速度、并发数、协议、重复次数等信息。**（提供产品功能截图并加盖投标人公章）** 9、▲可支持高兼容零代码接入 IDS、防火墙等威胁监测组件，可通过 WEB 界面完成威胁组件接入。**（提供产品功能截图并加盖投标人公章）** 10、支持呈现内网整体安全运营情况，包含发现资产数、资产探测任务状态、安全态势趋势，服务水平监测，事件的已完成、正在处理、等待查看状态的统计。实时掌握内网运营情况。 11、▲能够根据 IP 汇聚搜索出 IP 的关联工单、关联资产信息、关联漏洞信息、关联告警信息。**（提供产品功能截图并加盖原投标人公章）** 12、▲安全运营服务所使用的云防御平台支持无限制带宽，不单独收费，可支持超大量访问请求。支持无限制 QPS，不单独收费，多节点负载，有效提高访问效率。**（提供产品功能截图并加盖投标人公章）** 13、安全运营服务所使用的云防御平台支持重保模式，在重大活动或高风险时期进行防护配置，提高业务系统整体防御等级。 14、▲安全运营服务所使用的云防御平台支持拟态防御，支持模拟不同的动态请求访问交互模式实现拟态防御效果，进而迷惑攻击者使其无法形成实质有效攻击。**（提供产品功能截图并加盖投标人公章）** 15、▲安全运营服务所使用的云防御平台支持全网协同防御，当平台中部分网站遭受攻击时，能够屏蔽攻击者对其他网站的攻击。支撑基于行业的协同防御场景，支持政府组织、金融理财、教育文化、新闻媒体、医疗健康等不少于五种常见行业的协同防御；支持基于网络机器流量数据分类的协同防御场景，支持恶意代理、恶意 IDC 设备、洋葱路由、星链 IP、撒旦 IP、APT 攻击 IP 等不少于五种以上类别的协同防御，支持设置 IP 白名单；相关 IP 数据库提供动态更新能力。**（提供产品功能截**

		图并加盖投标人公章） 16、▲安全运营服务所使用的云防御平台支持特定攻击行为清洗协同防御，支持漏洞扫描器攻击屏蔽、网络爆破屏蔽；支持重保专项攻击协同防御；支持基于 IDC 的协同防御，支持阿里云 IDC、腾讯云 IDC、百度云 IDC、亚马逊 IDC、微软 IDC、谷歌 IDC 等不少于五种以上 IDC 的协同防御。**（提供产品功能截图并加盖投标人公章）** 17、能够识别 Web 攻击者的 IP 所在地区，如是境外 IP，可限制境外 IP 访问，并支持设定限制时间。 18、支持超过上千个网站攻击数据进行地图展示，并且可以查看每一个网站基于时间、攻击分类、攻击趋势等态势展示。 19、支持 IPv6 解析，能将 IPv6 流量转化为 IPv4 后再转发给源网站，制造商通过 IPv6 认证。 20、支持网站缓存功能，即使网站源站内容被篡改，访客访问到的内容也是网站原来缓存的内容 21、支持锁定页面关键资源（如 Banner 图片、LOGO 图片），避免关键资源受篡改而影响页面。 22、★中标后招标方有权要求中标方严格按照频率要求提供服务交付物，确保满足招标方安全需求，交付物如下： 交付物名称:《安全运营日报》，报告频率：每天一次 交付物名称:《安全运营周报》，报告频率：每周一次 交付物名称:《安全运营月报》，报告频率：每月一次 交付物名称:《脆弱性识别报告》，报告频率：每季度一次 交付物名称:《脆弱性处置报告》，报告频率：每季度一次 交付物名称:《成熟度评估报告》，报告频率：每季度一次 交付物名称:《威胁情报报告》，报告频率：每季度一次 交付物名称:《巡检报告》，报告频率：每季度一次 交付物名称:《安全事件实时通知》，报告频率：按需触发，不

		限次数 交付物名称:《安全事件处置报告》，报告频率：按需触发，不限次数 交付物名称:《重点保障值守方案》，报告频率：按需触发，不限次数 交付物名称:《重点保障值守报告》，报告频率：按需触发，不限次数

四、履约标准（本项为评审依据，未完全满足仅按要求进行扣分，不影响其响应文件有效性）

1、投标人需针对本项目提供技术方案，方案内容包括但不限于：①建设背景和建设目标；②建设思路和建设内容；③安全运营服务方案。售后服务方案包括但不限于①应急服务响应方案②备品配件措施（包括涉及维修或配件更换等情况）③系统培训方案④售后服务计划安排方案

2、投标人需具有类似服务案例（业绩）；

3、投标人需为本项目配置服务团队人员。

注：以上产品凡涉及 3C 认证，入网许可证等，供应商应承诺在成交后签订合同前提供相关证书（提供承诺函原件加盖公章）。

注：标注“★”号的参数为本项目实质性要求，若是有负偏离，视为未实质性响应招标文件要求；标注“▲”号的参数为重要参数，若有负偏离按照评审标准进行扣分。

四、商务要求：

（一）服务类项目：服务期限、服务地点、付款方式、验收标准等：

1、★交货时间：在接到采购人交货通知后30个日历内完成供货。

2、★交货地点：四川省成都市武侯区太平寺路9号四川体育职业学院。

3、★付款方法和条件：合同签订后10个工作日内支付合同金额的40%，完成供货并安装调试完毕，达到上线运行标准，经验收合格后20个工作日内付合同金额的60%。

乙方应按照甲方要求和流程办理款项支付手续，并出具正式票据和相关承诺书等文件。在办理过程中，因乙方未提供符合要求的资料，甲方不予支付，由此产生的全部责任由乙方承担。甲方每次付款前，乙方应当向甲方开具合法有效的票据，否则甲方有权拒绝付款，且不承担任何责任。满足合同约定支付条件的，采购人应自收到供应商发票后15日内将资金支付到合同约定的供应商账户。中标、成交供应商为中小企业的，采购人原则上应当自收到供应商发票后10个工作日内将资金支付到合同约定的供应商账户。

4、★履约验收标准、时间及方式：

（1）履约验收时间：供应商提出验收申请之日起30日内组织验收；验收组织方式：自行验收；履约验收程序：一次性验收；验收主体：四川体育职业学院。

（2）技术履约验收内容及商务履约验收内容：以招标文件、供应商投标文件和双方签订的合同为验收依据。

（3）验收标准：严格按照政府采购相关法律法规和《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》(财库〔2016〕205号)以及《政府采购需求管理办法》(财库〔2021〕22号)的要求进行验收，以招标文件、供应商投标文件和双方签订的合同为验收依据。

5、★质保期：验收合格后进入质保期，产品质保期3年，在质保期内属产品质量问题所发生的一切费用由投标人负担。

6、售后服务要求**（本项不作为技术参数条数计数，未完全满足仅按综合评分明细表的评审标准详细要求进行扣分，不影响其响应文件有效性）**

（1）培训要求：需向采购人提供不少于1次使用操作培训，达到采购人不少于1名工作人员熟练使用，并在培训后提供使用咨询。

（2）由供应商或生产商负责到校安装调试，定期维护。

（3）提供7×24小时的技术支持服务。接到采购人故障电话时应1小时内响应，4小时内到达现场，12小时内不能排除设备故障的，应提供备用机，以保证设备的正常使用。

（4）涉及维修或配件更换等情况，在48小时维修完毕投入正常使用（不可抗因素除外）；若未在规定期限内修复而造成采购人的直接和间接经济损失，由投标供应商承担。

注：

1.其他未尽事宜在合同中约定。

2.以上打★号的为本次采购项目的实质性要求，不允许有负偏离,否则符合性审查不予以通过。