一、项目概况

为落实上级关于加强网络安全工作，提升系统安全防护能力，加强各类信息系统安全防护和数据安全保护，优化调整服务器策略配置，加强管理终端管控，以应对当下复杂的网络环境，有效防范勒索病毒、挖矿病毒等，净化校园网络环境，保障校园和师生信息资产的安全。

本项目为成都航空职业技术学院网络安全防御系统升级项目，拟通过招标方式择优选取 1 家供应商为采购人供货，本项目采购预算为 85.00 万元。

二、采购清单及技术参数要求

（一）采购清单★

序号	产品名称	产品描述	数量
1	态势感知平台	校园网安全态势感知分析平台硬件及系统软件，对校园网络进行安全威胁检测、风险分析、安全运营等。	1 套
		校园网总出口流量探针（网络吞吐流量≥10G），采集校园网络总出口流量、威胁数据，上报日志给态势感知平台。	1 套
		校园数据中心流量探针（网络吞吐流量≥3G），采集校园数据中心出口流量、威胁数据，上报日志给态势感知平台。	1 套
		态势感知平台远程运营分析服务（托管安全服务，提供一年 50 个重要资产的综合分析服务），通过云端关联分析和研判平台收集态势感知平台的威胁告警，为我校提供综合分析服务，远程协助威胁事件的闭环处置。	1 套
2	服务器安全管理系统	服务器安全管理系统（提供 20 个节点的安全防护授权），对我校服务器或主机进行统一运维管理、安全策略维护及安全日志分析、威胁溯源等。	1 套
3	出口防火墙系统	下一代防火墙（网络层处理≥80G），在我校校园网络总出口部署高性能防火墙，结合防火墙应用层网络安全防护和威胁情报能力，对全校网络流量进行整体监测和清洗，避免网络安全事件（包括但不仅限于勒索、挖矿等恶意事件）的发生。	1 台
4	网站云监测	为我校官方网站提供 1 年 7*24 小时的安全事件云端远程监测服务。	1 套

（二）技术参数要求

(1) 态势感知平台

1. ▲校园网态势感知平台配置要求：CPU≥2路12核，主频≥2.2 GHZ ；内存容量≥256G，内存规格DDR4 ，固态硬盘容量≥2块960G SSD（支持Raid 1）；企业级SATA硬盘容量≥12块4TB硬盘，（SATA 3.5寸），电源≥2，电口（含Console接口）≥4*GE，万兆SPF+插槽≥2（配置≥2个万兆多模光模块），含三年硬件维保服务，三年软件升级服务，三年威胁情报升级服务。

2. ▲学校网络总出口流量探针配置要求：同时开启网络流量采集、威胁数据采集和日志上报功能情况下网络吞吐量≥10Gbps，HTTP并发连接数≥800万，HTTP新建连接速率≥30万/秒；≥8个接口扩展插槽（本次配置千兆SFP光口≥4，含4个千兆SFP多模光模块，万兆SFP+光口≥2，含2个SFP+万多模光模块），提供SSL流量解密功能永久使用授权，实现对SSL协议的加密流量进行卸载和解密。含三年应用识别库、三年入侵检测特征库（含漏洞利用特征、WEB入侵特征）、三年病毒检测特征库等升级服务。含三年硬件维修服务。

3. ▲学校数据中心流量探针配置要求：同时开启网络流量采集、威胁数据采集和日志上报功能情况下网络吞吐量≥3Gbps，HTTP并发连接数≥350万，HTTP新建连接速率≥12万/秒；≥2个接口扩展插槽（本次配置千兆电口≥6，万兆SFP+光口≥4，含4个SFP+万多模光模块），提供SSL流量解密功能永久使用授权，实现对SSL协议的加密流量进行卸载和解密。含三年应用识别库、三年入侵检测特征库（含漏洞利用特征、WEB入侵特征）、三年病毒检测特征库等升级服务。含三年硬件维修服务。

4. ▲为保障态势感知平台有效使用，本次项目需提供数据中心重点资产≥50个（资产数量以IP地址为基准），提供7*24远程运营分析服务（托管安全服务），通过云端关联分析和研判平台收集态势感知平台的威胁告警，包括流量设备告警、安全设备的告警、系统告警等数据，进行关联分析和研判，为学校提供资产、威胁、脆弱性等方面的综合分析服务，帮助学校精准识别和监测网络中的安全威胁，并对确认的威胁事件及时通知学校安全管理人员、主动进

行响应，远程协助学校安全管理人员完成威胁事件的闭环处置工作，提供专业的运营指导及改进建议。

5. 平台需要具备全网安全资产梳理功能，需支持管理资产主机设备、网络设备、安全设备、应用系统等资产类型管理；支持DHCP场景下的资产管理，支持对DHCP网段范围、DHCP租期等属性进行配置。

6. 平台需要支持统计潜在风险资产数、受攻击资产数、失陷资产数以支持对重大网络安全事件进行威胁预警，支持通过预警包导入完成网络安全事件的影响面评估，并持续地跟进事态的发展，快速完成重大网络安全事件的预警及处置。

7. 支持导入第三方漏洞扫描报告，系统支持主流扫描器厂家（例如绿盟、启明、网神、天融信等）漏扫报告的解析识别和导入管理，支持人工漏洞报告导入，支持使用模板进行漏洞信息的导入。

8. 支持接入各种类型数据包括但不限于：设备日志、网络流量、失陷类威胁情报数据、资产数据、漏洞数据等数据进行关联分析，支持对IPV6日志进行关联分析。

9. 支持从攻击者视角对至少最近30天时间范围的告警进行归纳分析，列表展示包括：攻击者IP、IP归属地、IP来源、攻击手段、攻击链阶段、最高危害等级、受害者IP数、威胁告警数、首次攻击时间、最新一次攻击时间，方便安全管理人员进行溯源。

10. 支持与本次项目中的防火墙产品进行联动处置，当发现失陷主机、恶意域名等威胁事件后，可以及时给联动设备下发阻断或告警的安全防护策略动作且防护策略支持对生效时长的配置，支持的联动处置消息类型包括IPv4地址、IPv6地址、URL、域名。

11. ▲支持对服务器安全管理系统联动设备下发的联动处置命令，命令包含：禁止失陷主机访问其他主机；禁止其他服务器访问失陷主机；隔离主机及恶意文件；同步资产及漏洞数据。（提供相关截图证明材料并加盖投标人公章）

12. ▲支持将网站云监测告警解析成告警日志，通过关联规则产生告警；支持同步网站资产数据及WEB漏洞数据（提供相关截图证明材料并加盖投标人公章）。

13. ▲支持利用语境关联分析技术，将网络流量日志、安全设备告警日志、操作系统告警日志、重要应用系统日志，结合威胁情报，进行多维关联分析，帮助学校发现更深层次的网络安全风险（提供由国家版权局、国家知识产权局、公安部上述任何一家国家权威机构颁发的语境关联分析引擎软件证书复印件加以佐证，提供证书复印件并加盖投标人公章）。

(2) 服务器安全管理系统

1. ▲产品形态要求：产品为软件化产品，具有统一控制端对全网主机统一集中管理、策略下发、数据分析等。

2. ▲操作系统兼容性：支持windows/linux主流操作系统及国产化操作系统，包括但不限于以下的操作系统：Windows Server；RedHat；CentOS；Ubuntu；Suse；中标麒麟、红旗等。

3. ▲授权数量：本次项目授权≥20个客户端授权。

4. 支持对校园网内的服务器进行扫描，并自动获取服务器相关信息，包括服务器名、在线状态、别名、主机IP、AgentID、分组标签、操作系统、IPv4、IPv6、负责人、所属部门等信息，可通过自动或手动方式进行资产发现的任务设置。

5. ▲支持梳理学习主机上的应用运行情况，并进行白名单管理，针对白名单外的应用告警；支持自动学习并梳理出对互联网暴露的服务器端口信息，并提供端口处置（提供产品功能配置截图证明并加盖投标人公章）。

6. 可支持等级保护2.0的二级、三级检查、测评、整改的业务检查，系统内置官方等保2.0的二级、三级基线模板，满足等保二级及等保三级要求，同时支持自定义基线检查任务。

7. 支持主动的自动化病毒查杀，可支持多引擎技术识别并查杀最新病毒；可支持病毒文件自动隔离、自动删除、不处理等方式。

8. ▲支持应用高级防护的设置，可有效拦截未知WebShell，及时发现网站程序中存在的漏洞并支持Web防护（提供产品功能配置截图证明并加盖投标人公章）。

9. ▲支持RASP（Runtime Application Self Protection）运行时应用自我保护技术，可对ASP、Net、PHP、Java等语言进行RASP防护；（提供产品功能配置截图证明并加盖投标人公章）。

10. ▲支持通过对我校主机资产进行整体管理，结合防病毒、微隔离、漏洞检测防护和入侵监测防护能力，有效防止恶意事件（例如勒索、挖矿等）的发生。

11. ▲支持与本次项目中的态势感知平台联动，接收联动处置命令，命令包含：禁止失陷主机访问其他主机；禁止其他服务器访问失陷主机；隔离主机及恶意文件；同步资产及漏洞数据。（提供相关截图证明材料并加盖投标人公章）

12. 支持利用语境关联分析技术，将服务器告警日志、行为基线日志、系统操作日志，结合威胁情报，进行多维关联分析，提升服务主机网络安全风险发现能力和防护能力。（提供由国家版权局、国家知识产权局、公安部上述任何一家国家权威机构颁发的语境关联分析引擎软件证书复印件加以佐证，提供证书复印件并加盖投标人公章）

13. 产品资质要求：产品拥有自主知识产权，非OEM、代理销售产品，具有国家版权局颁发的“计算机软件著作权登记证书”；拥有公安部颁发的“主机文件监测”类产品安全专用销售许可证。（提供以上2项资质复印件，并加盖投标人公章）

(3) 出口防火墙系统

1. ▲网络处理能力≥80G；并发连接≥800万；每秒新建连接≥100万/秒，电源≥2，≥8个扩展板卡插槽（配置≥4口万兆SFP+板卡，含4个万兆多模光模块），提供三年硬件维保服务。

2. ▲产品必须具备应用层网络安全防护能力，本次配置应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测全功能三年授权升级服务，功能模块全开处理能力不低于12G。

3. 支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。

4. 支持MPLS流量透传；支持针对MPLS流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能（提供相关截图证明材料并加盖投标人公章）。

5. 支持对HTTP/FTP/POP3/SMTP/IMAP/SMB等协议流量的病毒查杀；本地病毒库规模大于3000万。

6. ▲支持利用语境关联分析技术，将漏洞防护告警日志、病毒防护告警日志、URL过滤日志，结合威胁情报，进行多维关联分析，提升防火墙网络安全风险发现能力和防护能力。（提供由国家版权局、国家知识产权局、公安部上述任何一家国家权威机构颁发的语境关联分析引擎软件证书复印件加以佐证，提供证书复印件并加盖投标人公章）

7. 支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等。

8. 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量；并对威胁情报发现的恶意主机执行自动阻断。

9. 支持与本方案中配置的态势感知与安全运营平台联动，上报网络活动产生的数据至态势感知与安全运营平台；并支持接收来自态势感知与安全运营平台推送的处置策略，及时拦截绕过防御措施产生的高级威胁。（提供相关截图证明材料并加盖投标人公章）

10. 产品资质要求：公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（级别为增强级）；《中国国家信息安全产品认证证书》（级别为增强级）。（提供以上证书复印件并加盖投标人公章）

(4) 网站云监测

1. ▲提供至少1个域名一年网站云监测服务，包括漏洞扫描、违规内容监测、网页挂马监测、内容变更监测、黑链监测、网站可用性监测、FGHK监测、未知资产发现以及标准的报表管理和通报管理模块。
2. ▲提供至少1个域名一年的基础人工运维服务，服务内容包括7*24小时的安全事件监测验证和安全事件通告下发，定期远程漏洞扫描及高危漏洞人工验证，7*24小时电话技术支持服务。
3. 支持以树形模式展示网站目录结构；支持以列表展示网站存在的外链及坏链，并提供指定连接检索能力。
4. 支持针对行业漏洞情报进行同步预警，并短信或邮件及时通知给学校安全管理人员。
5. 识别并定位网站外部链接位置，对目标网站进行监测、查看是否被植入后门。
6. 对目标网站进行监测、查看主机是否被渗透，并作为矿机使用，植入挖矿脚本。
7. DNS监测，支持华北、华东、华南、海外机房超过40个监测节点，确保电信、联通和移动都具备监测点；支持A记录更改监测，网站A记录解析变更时可进行告警，告警支持短信/邮件方式（提供证明材料并加盖投标人公章）。
8. ▲支持与态势感知与安全运营平台进行联动，支持将网站告警同步给态势感知与安全运营平台；支持同步网站资产数据及WEB漏洞数据。（提供相关截图证明材料并加盖投标人公章）

（三）培训及售后服务

(1) 培训

针对本次项目实施内容，组织对学校相关技术人员、管理人员的现场培训。投标人需提供培训相关设备设施（如需搭建培训环境）、培训计划、培训资料和培训讲师。

(2) 售后服务

1. 服务和支持的范围

在设备和软件质保期内，学校可要求投标人在下述领域提供服务和支持，并提出方案：

- 当建成的系统进行升级、更换时，投标人都必须配合，并提供相关技术、软件升级包和人员支持（含原厂）。
- 针对本次项目实施内容、产品进行每季度一次的巡检服务及重要时期的深度巡检（重要时期深度巡检是否开展由学校根据具体情况确定），巡检内容需完全覆盖设备/系统正常运行所需检查点。
- 在与本次项目实施内容有关的周边外围设备/系统改造时，投标人必须提供必要的配合，包括现场支持。

2. 服务和支持的组织结构

投标人需对本次项目服务和支持的组织结构进行详细描述，包括但不限于：

- 服务体系
- 组织结构
- 人员组成，包括数量和相关能力

3. 故障处理

投标人须对本次项目涉及的软件类（bug）故障、硬件类故障的处理流程、时效进行详细描述。

4. 响应时间要求

在设备和软件质保期内，投标人自接到报修电话后 0.5 小时电话响应，2 小时内到达现场，并在到达现场后 4 个小时内解决问题。

如投标人在接到学校提出的技术服务要求或维修通知后 0.5 小时内没有响应、拒绝或没有能力在到达现场后 4 小时内解决故障，学校有权委托第三方对合同范围内软件系统及/或所购产品进行维修或提供技术服务，由此产生的一切费用由投标人承担。

5. 备品备件

投标人需结合厂商及自身实际，对本次项目涉及硬件在成都的备件情况进行详细描述。

三、★商务要求

1. 服务期限：合同签订后 60 日历天内。

2. 服务地点：成都航空职业技术学院成都市龙泉驿区车城东七路 699 号。

3. 资金支付方式、时间、条件：合同签订生效后，采购人向投标人支付合同总金额的 30%预付款，在完成全部工作并验收合格后支付合同剩余金额。（投标人须向采购人出具合法有效完整的完税发票及凭证资料后进行支付结算，付款方式均采用公对公的银行转账，投标人接受转账的开户信息以采购合同载明的为准。）

4. 验收：

应严格按照政府采购相关法律法规以及《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）相关要求、采购合同、本项目招标文件的要求、中标人的投标文件及承诺等进行验收。

5. 其他要求：由于新冠疫情，确保人员的健康，在项目实施过程中须严格遵行采购人单位疫情防控相关规定配合采购人实行疫情防控相关工作。**（须在其他响应性文件中单独提供承诺函，格式自拟，否则视为无效投标。）**

6. 投标人根据情况自行踏勘现场及前期相关配套设施设备，如中标，不可因未了解项目现场情况而放弃中标不履行中标人义务。如因中标人不能正常履约给采购人造成任何损失的，采购人将保留进一步追溯的权利，并由中标人赔偿所有损失；如放弃中标，按照政府采购相关法律法规执行，所产生的后果由中标人承担。**（须在其他响应文件中单独提供承诺函进行响应，由投标人法定代表人签字并加盖投标人公章。）**

7. 保密要求：在项目开始前，须与采购人签订保密协议，严格遵守法律法规，对相关敏感、系统风险信息、项目实施内容等信息进行严格保密。未经同意，严禁将上述内容与任何第三方透露或用于其他商业用途，并承担由此产生的一切损失。**（须在其他响应性文件中单独提供承诺函，格式自拟，否则视为无效投标。）**

8. 投标人应保证：如中标，所提供的服务或其任何一部分均不会侵犯任何第三方的专利权、商标权或著作权。**（须在其他响应文件中单独提供承诺函进行响应，由投标人法定代表人签字并加盖投标人公章。）**

9. 投标人在实施过程中应不影响现有办公网络使用，保证教务教学正常进行，特殊情况需中断网络的应书面申请，征得学校同意后方可实施，否则造成损失的应由投标人全额承担，如长时间严重影响学校正常办公教学使用且通知整改后无明显改善的，采购人有权终止合同， 并依法追究相关责任。**（须在其他响应**

文件中单独提供承诺函进行响应，由投标人法定代表人签字并加盖投标人公章。）

四、其他要求

1. 投标人有完成本项目的能力，有类似相关业绩作为经验。

2. 针对本项目提供项目实施方案，内容包括：①项目需求分析、②现场服务支持团队、③备品备件、④日常运行维护服务方案、⑤项目进度保障方案、⑥服务保障措施、⑦质量保障措施、⑧故障及应急处置服务方案。

3. 针对本项目提供售后服务方案，内容包括：①售后服务承诺、②售后服务电话、③售后服务人员配置、④售后服务响应时间、⑤售后巡检、⑥培训方案。

4. ★要求单独提供承诺函的条款，投标人必须就该条款内容逐项单独出具一份承诺函进行承诺，并由投标人法定代表人签字并加盖投标人公章。

5. 其他有利于项目实施的承诺或相关证书或证明。

说明：1、本章节带“★”号条款为实质性要求，投标人若未满足的，将被视为无效投标。

2、本章中实质性要求未明确要求证明材料的以投标人在商务应答表或服务应答表中对应的应答为准。

3、如投标人提供虚假材料谋取中标，一经核实，按相关法律法规处理。