第六章 服务需求及服务验收要求

一、采购内容

校园网络安全运营中心建设

标的名称	数量	单位	最高单价限价（万元）	小计（万元）	要求/备注	服务/货物/工程	所属行业
态势感知平台	1	台	35	35	核心产品	货物	软件和信息技术服务业
潜伏威胁探针	1	台	15	15	核心产品	货物	软件和信息技术服务业
安全托管模块服务	3（10 资产*3 年）	年	5	15		服务	软件和信息技术服务业
合计				65			

注：投标单价不得超过最高单价限价，否则作废标处理。

二、技术要求

（一）态势感知平台

态势感知平台			
名称	**重要性**	**技术参数及要求**	**证明材料要求**
性能参数	★	存储容量≥14.4T，在带宽性能 1Gbps 时存储时长≥900 天/1Gbps。（提供证明材料并加盖公章）	是
硬件参数	★	规格：需为 2U 标准机架式设备，内存≥3*32GB DDR4 3200，系统盘≥1*480GB SATA SSD，数据盘≥4*4TB，标配盘位数≥12，电源：需为冗余电源，接口：至少 4 个千兆电口，2 个万兆光口。	是
功能参数		1、支持综合安全风险、主机安全风险、脆弱性感知、外部感知、工单、摘要、处置报告多种方式呈现，也支持自定义时间导出 PPT 报告。（提供截图证明和第三方权威检测报告并加盖公章）	是
		2、支持大屏展示业务外连态势，包括外连风险总览、外连威胁 TOP10、外连态势、外连地区 TOP5、实时威胁监控；支持国际、国内地图自主切换（需提供产品功能	是

		截图证明并加盖公章）；	
	▲	3、支持不同视角展示全网安全态势，包括综合安全态势、分支安全态势、安全事件态势、网络攻击态势、外连风险态势、横向威胁态势、脆弱性态势、资产态势、正常横向访问监控态势、正常外连监控态势、设备运行态势等 13 个独立的大屏展示功能；支持大屏轮播，可自定义播放顺序（需提供产品功能截图证明并加盖公章）；	是
		4、支持检测 15 类以上常见协议的弱密码，包括 HTTP、FTP、LDAP、VMWARE、ORACLE、VNC 等协议，检测信息包含账号、密码、服务器、所属分支和业务、类型、最近发现时间等；支持筛选管理员账号与是否登录成功，并支持导出弱密码报告（需提供产品功能截图证明并加盖公章）；	是
		5、支持检测业务服务器的配置不当，检测内容包括服务器、所属业务、所属分支、配置不当类型、风险等级、发现时间等；支持配置不当类型下钻，展示配置不当详情，提供解决方案和数据包举证，并支持导出配置不当报告（需提供产品功能截图证明并加盖公章）；	是
	▲	6、支持挖矿专项检测页面，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息（需提供截图证明并加盖公章，且所投产品必须提供第三方权威机构功能项的产品检测报告）	是
		7、支持不同场景下数据库异常模型的算法编辑，可选择稀有值检测算法、ZScore 异常检测算法、箱线图异常检测算法；可将不同类型的算法应用到不同的资产（需提供产品功能截图证明并加盖公章）；	是
		8、支持邮件威胁分析，可展示收件人 TOP5、发件人账号 TOP5、恶意邮件类型分布、危害和处置建议；支持对恶意邮件详情分析，包含收件人账号、恶意邮件数量、发件人账号、附件名称、病毒名称、恶意链接名称等，并支持导出分析结果（需提供产品功能截图证明并加盖公章）；	是
	▲	9、支持横向访问服务器流量分析，包括 TOP5 应用流量趋势、TOP5 协议趋势；支持服务器视角和来访分支视角，其中服务器视角可展示服务器 IP、总流量、源 IP 数量、应用 TOP10、协议端口 TOP10、连接失败数、最大并发，并支持以表格形式导出数据（需提供产品功能截图证明并加盖公章）；	是

		10、支持网站攻击、漏洞利用、C&C 通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等关联分析规则，规则数量达到 200 条以上；支持自定义统计与序列关联分析规则（需提供产品功能截图证明并加盖公章）；	是
	▲	11、支持服务器行为分析建模，具备独立页面展示行为引擎学习的天数、异常行为与异常服务器数量，并对异常行为进行举证描述；支持对业务服务器内网横向被访问、横向主动访问、外连等建立行为基线，包括访问流量趋势、访问次数趋势、自定义非正常时间段、常见访问源网段、访问源主机、应用 TOP5、目的端口 TOP5 等，提前发现未知异常行为（需提供产品功能截图证明并加盖公章）；	是
		12、支持对数据库登录地点、登陆时间、访问表、访问数据量、访问数据库频率等进行持续学习和监控，判断是否存在数据异常行为，发现非常见用户登录、非常见地址访问、非常见时间段访问、非常见数据库表访问、数据库频繁访问、数据库表访问量过大等异常行为。（需提供截图证明并加盖公章）；	是
	▲	13、支持不同场景下数据库异常模型的算法编辑，可选择稀有值检测算法、ZScore 异常检测算法、箱线图异常检测算法；可将不同类型的算法应用到不同的资产（需提供产品功能截图证明并加盖公章）；	是
配套能力	▲	提供 IPS 防护能力组件设备，设备要求网络层吞吐量≥50G， IPS 吞吐量≥6G，并发连接数≥1000 万。（提供证明材料并加盖公章）	是
	▲	规格：2U 标准机架式设备，内存≥32G，硬盘容量≥128G SSD+480G SSD，电源：需为冗余电源，接口：至少 6 个千兆电口，至少 6 个万兆光口 SFP+。（提供证明材料并加盖公章）	是
	▲	产品内置 IPS 检测引擎，支持超过 11000 种攻击监测规则库。规则库支持按照攻击类型、操作系统、风险等级、应用类型、流行程度等方式分类。（需提供产品功能截图证明并加盖公章）	是
	▲	产品支持对 SMIP、POP3、IMAP、FTP、TELNET、LDAP、RDP、MSSQL、DB2、REDIS、POSTGRESQL、HTTP 等服务的弱口令登录行为检测防御，采用弱口令字典和口令强度两种方式检测，弱口令字典支持导入、导出、重置。可自定义口令强度规则，如密码长度、密码字符类型等。支持对发生的弱口令事件进行取证。（需提供产品功能截图证明并加盖公章）	是
其他要求	▲	1、产品需具备网络安全专用产品安全检测/认证证书，提供相关证书和检测报告。	是

	▲	2、要求具备国家版权局颁发的软件著作权登记证书，提供相关证明材料。	是
服务要求		要求提供上门安装调试及工程师3年7×24小时免费上门服务，提供原厂出具的针对本项目的授权书、服务承诺函，提供3年免费软硬件质保及3年规则库升级；	
		招标人保留测试权力，在签订项目合同时要求提供样机进行上述功能要求的逐一测试验证，无法满足招标人有权进行废标处理。	

（二）潜伏威胁探针

潜伏威胁探针			
名称	**重要性**	**技术参数及要求**	**证明材料要求**
性能参数	★	网络层吞吐量≥2Gbp，应用层吞吐量≥650Mbps。（提供证明材料并加盖公章）	是
硬件参数	★	规格：需为2U标准机架式设备，内存≥8G，硬盘≥480G SSD，电源：需为冗余电源，接口：至少6个千兆电口，至少2个万兆光口SFP+。（提供证明材料并加盖公章）	是
功能参数		1、具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等；	
		2、具备报文检测引擎，可实现IP碎片重组、TCP流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意UR监测模式，可完成模式匹配并生成事件，可提取URL记录和域名记录；	
		3、支持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整站系统漏洞等网站攻击检测（需提供产品功能截图证明并加盖公章）；	是
	▲	4、支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤（需提供产品功能截图证明并加盖公章）；	是
		5、支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Network Device、Scan漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击等服务漏洞攻击检测（需提供产品功能截图证明并加盖公章）；	是
		6、支持FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、VNC等协议暴力破解检测（需提供产品功能截图证明并加盖公章）；	是

	▲	7、支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等（需提供产品功能截图证明并加盖公章）；	是
		8、支持 5 种类型日志传输模式，包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求（需提供产品功能截图证明并加盖公章）；	是
		9、支持传输访问检测日志，包括正常访问、风险访问、违规访问（需提供产品功能截图证明并加盖公章）；	是
		10、支持 IP，IP 组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式（需提供产品功能截图证明并加盖公章）；	是
		11、内置 URL 库、IPS 漏洞特征识别库、应用识别库、WEB 应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库（需提供产品功能截图证明并加盖公章）；	是
	▲	12、支持流量抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式（需提供产品功能截图证明并加盖公章）；	是
		13、支持设备内置简单命令行管理窗口，便于基础运维调试；	
服务要求		1、要求提供上门安装调试，提供原厂出具的针对本项目的授权书、服务承诺函，提供 3 年免费软硬件质保；	
		2、招标人保留测试权力，在签订项目合同时要求提供样机进行上述功能要求的逐一测试验证，无法满足招标人有权进行废标处理。	

（三）安全托管模块服务

安全托管模块服务			
名称	**重要性**	**技术参数及要求**	**证明材料要求**
服务要求	★	针对学校 10 个核心资产进行 3 年的安全托管服务，服务要求围绕威胁、事件两个要素，通过云端安全运营中心和安全专家团队有效协同的“人机共智”模式 7*24H 持续性开展网络安全保障工作，构建主动、闭环的安全运营体系。要求提供承诺书。	是
服务内容		1、资产识别与梳理 资产发现与识别：借助安全工具对用户资产进行全面发现和深度识别，并在后续服务过程中触发资产变更等相关服务流程，确保安全运营中心中资产信息	

		的准确性和全面性。——一季度配合梳理一次。	
功能参数		2、支持挖矿专项检测，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息（需提供截图证明并加盖公章，且所投产品必须提供第三方权威机构功能项的产品检测报告）	
		3、每年配合学校进行一次攻防/应急演练。	
		4、应急处置： 建立安全事件的进度监控机制。 普通事件从安全日志分析研判到通告，用时小于 1 小时；遏制影响时间小于 4 小时。 重大事故启用应急响应机制，工作时间 15 分钟，非工作时间 30 分钟之内云端专家进行响应，默认由专家团队进行远程协助解决，如远程无法解决的则采用最快的交通工具，省会 2 小时内上门处置，省内 8 小时内上门处置。	
		5、安全加固——漏洞分析与管理： 通过漏洞扫描工具识别系统安全漏洞，结合多种信息对识别的漏洞进行优先级排序，最后提出切实可行的漏洞修复指导。同时，借助漏洞跟踪管理平台，可以有效地追踪资产漏洞生命周期，清楚地掌握资产的脆弱性状况，实现漏洞全生命周期的可视、可控和可管。（提供证明材料并加盖公章）	
		6、安全加固——弱口令分析与管理： 实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat 等。 针对不同行业提供行业密码字典，有针对性的进行内网弱口令检测，并将检测发现的问题通过工单系统跟踪修复状态。	
		7、威胁分析与通告： 实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、高级黑客攻击事件、持续攻击事件。实时监测网络安全状态，对病毒事件自动化生成工单，及时进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发 DOS 型、C&C 访问型、文件感	

		染型、木马型。	
		8、每年配合学校组织一次钓鱼邮件演练。	
		9、主动分析与响应： 每月主动分析病毒类、攻击类、漏洞利用类、失陷类的安全事件，并提供相应解决方案。	
		10、策略管理： 安全专家每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。	
		11、持续攻击对抗： 通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗。	
		12、事件分析与处置： 实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。	
		13、针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助用户快速恢复业务，消除或减轻影响。	
	▲	14、要求云端安全运营服务平台可对接项目中本地态势感知平台，需出具对接承诺函并加盖公章；	是
其他要求		1、投标方应当具备云端检测和分析平台，为招标方提供 7*24 小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示；提供云端服务平台告警审核功能界面截图，举证一个告警聚合分析的例子和一个告警详情展示具备上述能力	是
		2、投标方所投服务供应商具备国家信息安全测评信息安全服务资质证书（安全运营类一级），符合信息安全服务资质安全运营类一类（基本执行级）（A 类）要求。	是
配套能力		3、提供一套日志审计软件（3 年有效期）； 4、日志审计软件审计许可证书数量不少于 20 个； 5、日志审计软件平均每秒处理日志数（eps）最大性能不低于 800；（配套虚拟化资源 4C，8G，系统盘 80G，磁盘按照学校要求存储天数部署即可）	

备注：“★”号条款是实质性条款， 不满足该指标项作废标处理。

三、其他要求

1、合同履行期限：合同签订后 30 日内完成供货、安装调试完毕并交付使

用

2、质保期： 3 年。

3、报价内容：

投标人投标报价包含所需全部的设备价、运输费、安装调试费、保险费、报检、技术培训费、验收、售后服务、利润等完成本次采购所需的一切费用和税金。对于采购文件中未列明，而投标人认为必需的费用也需列入总报价，在合同实施时，采购人将不予支付投标人没有列入的项目费用，并认为此项目的费用已包括在总报价中。）

4、验收标准：

（1）产品到达指定地点后，由投标人与采购人共同清点，无误后签字确定；如有差异由投标人承担一切责任。

（2）投标人须保证所提供产品为全新的、未使用过的，且为制造商原厂原装，相关技术白皮书证明文件。

（3）在产品安装调试过程中，如涉及设备生产厂家的工作，需由厂家提供必要的技术支持，最终调试完成后，确认无误，采购人签署最终验收合格书。