网络安全态势感知及运营平台

(技术及服务部分)

# 采购需求

## 项目概述

在信息化时代，网络已经深刻地融入了经济社会生活的各个方面，网络安全威胁也随之向经济社会的各个层面渗透，网络安全的重要性随之不断提高。党的十八大以来，以习近平同志为核心的党中央从总体国家安全观出发对加强国家网络安全工作做出了重要的部署，对加强网络安全及网络安全法制建设提出了明确的要求。党的十八大以来，国家制定和出台了一系列政策及法律法规，《网络安全法》也于2017年6月正式实施，这些法律法规对各行业信息安全工作提出了具体要求。

经过多年的信息化建设，江苏师范大学信息化应用水平正不断提高，信息化建设成效显著。但是，作为信息化发展的重要组成部分，网络安全的状态直接制约着信息化发展的程度。根据网络安全法的详细内容规定，校园的网络安全建设目前还存在缺少最新的安全技术防御措施，缺少有效的安全管理规程，缺少基于大数据的智能运维管理平台，缺少安全管理体系、安全评估手段和应急措施等问题。为促进江苏师范大学的网络安全发展，全面贯彻国家网络安全及信息化工作相关要求，落实《网络安全法》等法律法规，江苏师范大学计划开展网络安全态势感知及运营系统建设，通过增补安全设备与安全态势感知平台，落实安全服务，开展等级保护等相关工作，建立体系化的网络安全感知及运营系统，切实提高学校的网络安全防护水平，推动学校信息化进一步发展。

## 项目采购说明

本次项目所采购设备主要包括：网络安全态势感知及运营平台、下一代防火墙、入侵防护系统、WEB应用防护系统、漏洞扫描系统、网络安全审计系统、数据库审计系统、Bypass交换机、以及专业的安全服务等。

投标公司需提供满足项目要求的软、硬件产品以及安全服务。投标单位中标后，招标人保留按照招标文件技术参数功能要求逐条验证的权利，如有任何功能项不满足则视为虚假应标，中标人须赔偿招标人因此造成的损失，并承担相关法律责任。

## 产品技术要求

所投产品提供三年硬件质保服务和软件升级服务。供应商所投所有安全产品必须同时适用于IPv4和IPv6环境。

### 网络安全态势感知及运营平台(含日志审计模块)(1套)

|  |  |
| --- | --- |
| **分类** | **具体要求** |
| **★**产品架构及性能 | 基于大数据平台构架。具备海量数据收集与快速检索能力。 |
| 日志平均处理能力（每秒日志解析能力EPS）：40000EPS，峰值处理能力（每秒日志解析能力EPS）：50000EPS；具备功能模块：日志审计、入侵态势感知、闭环脆弱性管理、威胁情报以及攻击链分析等；三年软件升级（包含软件更新服务、远程支持服务）。 |
| 数据采集引擎具备数据压缩能力。 |
| 基于B/S架构，采用最新的HTML5标准，通过web方式对本系统实现管理。 |
| 支持BYOD设备远程管理。 |
| 平台自身具备可扩展性、开放性，能够平滑扩展平台功能；支持平台系统集群部署，能够平滑扩展平台处理能力。 |
| 监测范围 | 监测范围包括但不限于网络安全设备、网络设备、数据库、中间件、操作系统、应用系统等。 |
| 数据采集 | 支持的数据采集方式包括但不限于：SYSLOG、SNMP/SNMP TRAP、FTP/SFTP、HTTP、API接口、WebService、专用Agent等方式，采集日志等。 |
| 日志管理 | 能够采集、保存原始日志数据，保存时间至少半年。能够实现海量日志数据快速查询。根据日志量增长情况，能够灵活扩展日志处理能力。系统必须具备日志范式化功能，实现对异构日志格式的统一化。内置管理设备授权许可≥500 |
| 工作台和仪表盘 | 支持定义小场景入口的快捷菜单项、面对当前用户的风险、流程、告警、资产、待办、预警、安全通告等的数据呈现。支持工单和风险预警提示。通过可视化图形展示当前网内安全概况，提供基于风险、脆弱性、威胁、资产、工单、情报预警、运维监控等仪表盘展示。 |
| **★**资产管理 | 支持多维度资产管理，支持多维度资产分析视图，系统至少内置三种视图：地理视图、业务视图、组织架构视图**（提供功能截图并加盖原厂公章）。**支持资产发现，结合同品牌漏洞扫描设备进行新资产发现。支持多维度资产视图，安全组织，地域，安全域随意切换。支持资产标签，且至少6种标签以上，根据标签可快速查询资产。支持平台支持手工注册资产，支持对资产进行修改/删除、批量导入/导出/添加/修改/删除等多种方式的管理。支持多维度资产分析，支持资产攻击链分析包括七级攻击链步骤图。 |
| 安全事件管理 | 支持针对日志或事件类型生产新的事件关联规则配置，规则包括对日志或事件的统计，属性值比较的配置，支持配置时间窗口。支持面向日志类型的规则配置，支持通过插件方式实现日志类型的扩展。支持日志包括：入侵防护日志、应用管理日志、认证日志、防病毒日志、数据防泄漏日志、Web安全日志、运行日志、高级威胁日志、url过滤日志、VPN日志、waf日志、内容审计日志、数据库审计日志、无线热点发现日志等。支持日志下钻，通过可视化界面展示原始日志。 |
| **★**安全态势展现 | 支持大屏投放要求及分辨率兼容要求，且易于操作，展现形式多样，画面丰富，并且能够以地图、柱状图、饼状图等多种图形化方式展现网络安全态势情况，动态提醒当前网络最新的安全威胁。 支持系统漏洞管理，结合漏扫设备，进行漏洞大数据分析整合，对网内资产漏洞提供闭环漏洞管理，无缝连接，且通讯加密。支持扩展至少5种安全维度的态势感知，入侵态势，异常流量态势，僵木蠕态势，系统漏洞态势，网站安全态势**（提供功能截图并加盖原厂公章）。**支持单一资产及根据地域划分的资产组合安全态势的监控、查询和展示，提供对资产的风险评分、脆弱性评分、威胁评分、关联漏洞信息、事件信息等。直观地展示攻击的情况。可以对地图进行下钻，查看对应地域的攻击和被攻击top5 ip的情况，支持地图动态联动。 |
| 脆弱性管理 | 支持脆弱性闭环管理，遵循扫描、评估、处置等管理维度。支持资产、漏洞、任务策略维度的数据源筛选，对脆弱性、漏洞、网站安全事件、资产等数据进行统计分析汇总，以各类统计图表方式，围绕资产，呈现风险、漏洞及网站安全事件数量及变化趋势等。支持漏洞状态信息列表呈现，并基于漏洞分值、漏洞热度、防护措施、资产重要性、忽略比等的优先级排序。 |
| **★**情报及预警管理 | 厂商具备情报收集能力，拥有自研威胁情报中心**（提供功能截图并加盖原厂公章）**。支持用户通过平台接口针对URL、IP、未知文件信息进行云端情报查询，获取URL、IP、可疑文件的威胁情报，帮助用户判断威胁程度；支持定时从云端获取情报和手工获取的方式。支持情报等级划分；支持人工发布漏洞情报和威胁情报；支持通过情报预警及情报的归档。支持漏洞情报从情报名称、漏洞类型、漏洞ID、漏洞热度（漏洞被引用次数）展示；支持漏洞情报和资产的关联分析，展示情报受影响的TOPN资产信息和漏洞详情。情报能够与平台本地事件进行关联管理，并进行特殊警示，突出告警。平台内置信誉库、地理信息库、漏洞库，并可持续更新。支持通过情报进行预警和触发工单，形成有效警示作用。支持预警的手工录入；支持情报和资产的关联分析生成威胁预警、漏洞预警；支持预警发布时的邮件通知/短信通知；支持通过工单进行预警响应处理。支持通过手工方式输入安全通告实现安全信息的上传下达。支持安全通告发布时的邮件通知/短信通知。 |
| ★攻击链条分析 | 支持收集同品牌入侵防护系统的日志分析为攻击的7个阶段;展示七级攻击链模型及每级事件关联的目标ＩＰ数;攻击链事件的时间范围随地图的时间控件变化。**（提供功能截图并加盖原厂公章）** |
| 运维响应 | 采用模块化管理，具备告警管理平台、工单管理平台、报表管理平台，设备管理平台。 |
| 系统自身安全性管理 | 支持系统自身日志记录并可查询；支持实时监控平台自身的CPU、内存和磁盘使用率，并以图形化方式动态显示。支持实时监控所有数据采集引擎和中心平台的工作状态，一旦发现故障，及时告警；支持实时统计平台数据处理能力，系统基本参数管理、基本配置管理。 |
| 服务器配置要求 | CPU: 2\*E5-2630V2 （6核心12线程、2.6GHz）；内存：128GB DDR 3 1333MHz；硬盘：8\*1TB（ext4文件系统格式、7200转），Raid5；Raid卡：带缓存raid卡；内置光驱；电源：热插拔冗余电源（1+1）1100瓦。 |
| 产品资质 | 必须具备安全管理平台类《计算机信息系统安全专用产品销售许可证》，需提供证书复印件。 |
| 《计算机软件著作权登记证书》，需提供证书复印件。 |
| 必须具备IT产品信息安全认证证书，需提供证书复印件。 |
| 厂商资质 | 获得国家信息安全测评中心颁发的信息安全服务资质证书，包括：（1）安全工程类二级（2）安全开发类一级；须提供以上两个证书的复印件。 |
| 获得中国信息安全认证中心颁发的ISCCC信息安全服务资质认证证书，包括：（1）应急处理一级服务资质（2）信息系统安全集成一级服务资质（3）风险评估一级服务资质；须提供以上三个证书的复印件。 |
| 国家计算机网络应急技术处理协调中心CNCERT颁发的网络安全应急服务支撑单位证书（国家级），提供复印件 |

### 下一代防火墙（1台）

|  |  |
| --- | --- |
| **分类** | **具体要求** |
| 配置要求 | 标准2U机型，含交流冗余电源模块，2\*USB接口，1\*RJ45串口，2\*RJ45管理口，≥8个 SFP口，≥4个万兆SFP+口，2个接口扩展槽位（可扩展≥16个 SFP口或者≥8个万兆SFP+口）；开通功能：流量管理、应用管理、IPSec VPN、资产识别功能、防病毒模块；三年质保和软件升级（包含软件更新服务、产品保修服务、远程支持服务）。 |
| 网络层吞吐量≥40G；应用吞吐量 ≥20G；最大并发会话量不少于800W。 |
| 联动能力 | 考虑项目整体联动效果，需要和网络安全态势感知及运营平台统一品牌。 |
| 防火墙功能 | 支持虚拟线、二层透明、三层、混合、旁路监听接入方式，适应各种网络环境需求。 |
| 支持策略路由，策略路由可基于应用进行流量控制。 |
| 支持源IP联动封锁。在入侵防御事件中发现源IP存在攻击行为时，可以一键封禁该IP，并设置封禁的时间。 |
| ★资产风险识别 | 支持资产风险识别。可根据用户指定的网络范围，通过自动、手动识别等多种方式，识别资产类型，如PC、移动设备、服务器等等资源类型。 |
| 支持对易受攻击的系统及应用软件进行打分告警、报表分析，如操作系统版本漏洞威胁度、上网浏览器客户端漏洞威胁度等，让用户实时了解当前网络资产资源中的脆弱度。 |
| 支持安全加固指导及实施。针对识别出的资产风险，为用户提供一键安全策略生成的功能，并可实时告警和记录入侵安全事件，形成安全事件报表和趋势图，指导用户及时做出加固防护，**提供截图厂商盖章证明**。 |
| 漏洞发现 | 支持联动外部扫描器，外部扫描器定期将漏洞推送至防火墙，通过防火墙可查看扫描器上报的内部资产漏洞的拦截情况。  |
| 信誉防护 | 支持信誉、僵尸网络防护。云端定期下发Web信誉、僵尸网络服务器、恶意站点信息到防火墙上，由防火墙对匹配相关特征的恶意攻击进行拦截。 |
| ★移动端安全运维 | 可通过移动端实现设备安全运维监控，APP支持安全设备运行状态监控，监控指标包括CPU使用率、内存使用率、设备IP地址，设备状态，查看安全告警等功能，**提供APP下载网页和相关链接以及包括APP相关功能界面的厂商盖章截图证明。** |
| 产品资质 | 获得公安部颁发的《计算机信息系统安全专用产品销售许可证》,产品类型须为第二代防火墙产品(增强级-支持IPV6)，提供复印件。 |
| 提供由中国信息安全测评中心颁发的《自主原创产品测评证书》，提供复印件。 |
| 获得国家信息安全测评信息技术产品安全测评证书（EAL3+以上等级），提供复印件。 |
| 厂商资质 | 获得中国信息安全认证中心颁发的ISCCC信息安全服务资质认证证书，包括：（1）应急处理一级服务资质（2）信息系统安全集成一级服务资质（3）风险评估一级服务资质；须提供以上三个证书的复印件。 |
| 获得国家信息安全测评中心颁发的信息安全服务资质证书，包括：（1）安全工程类二级（2）安全开发类一级；须提供以上两个证书的复印件。 |
| 国家计算机网络应急技术处理协调中心CNCERT颁发的网络安全应急服务支撑单位证书（国家级），提供复印件。 |

### 入侵防护系统（2台）

|  |  |  |
| --- | --- | --- |
| **类别** | **参数** | **具体要求** |
| 设备要求 | 联动要求 | 考虑项目整体联动效果，需要和网络安全态势感知及运营平台统一品牌。 |
| 配置要求 | 2U机型，含交流冗余电源模块，2\*USB接口，1\*RJ45串口，2\*GE管理口，≥8个 SFP口，≥4个万兆SFP+口，2个接口扩展槽位（可扩展为≥16个 SFP口或者≥8个万兆SFP+口）；开通防毒墙模块；三年质保和软件升级（包含软件更新服务、产品保修服务、远程支持服务）。 |
| 吞吐量 | 三层吞吐量≥30G,应用层吞吐不少于20G。 |
| ★攻击防护 | 攻击特征库 | 1. 系统应提供覆盖广泛的攻击特征库，能够针对7800种以上的攻击行为、异常事件，以及网络资源滥用流量，进行检测和防御。系统携带的攻击特征库须获得CVE-Compatible兼容性认证。
2. 系统应提供敏感数据外发的防护功能，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）。

**以上两个提供界面截图盖章证明。** |
| 攻击防护类型 | 支持基于SCADA等工控协议的相关漏洞攻击检测。 |
| 沙箱联动 | 未知威胁防护 | 支持提供恶意软件分析服务。 |
| 支持对未知可疑文件统计。 |
| ★应用识别能力 | 资产识别 | 系统应提供基于资产的保护，具备资产识别功能，包括操作系统、浏览器、应用类型等客户资产相关信息的识别能力，**提供界面截图盖章证明。** |
| ★管理能力 | 一键巡检 | 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，**提供界面截图盖章证明**。 |
| 误报处置 | 支持对用户所认为的误报事件进行一键关联反馈，由厂家确认分析。 |
| ★移动端安全运维 | 可通过移动端实现设备安全运维监控，APP支持安全设备运行状态监控，监控指标包括CPU使用率、内存使用率、设备IP地址，设备状态，查看安全告警等功能，**提供APP下载网页和相关链接以及包括APP相关功能界面的厂商盖章截图证明。** |
| 产品成熟度证明 | 市场占有率 | 投标产品应该是经过市场考验的成熟产品，在国内市场具有较高的市场份额。在CCID或IDC有排名，且排名为前三的品牌，提供证明复印件。 |
| 产品资质 | 投标IPS产品应具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，提供复印件。 |
| 投标IPS产品应具有中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》，并获得EAL3+以上级别，提供复印件。 |
| 厂商资质以及安全能力 | 获得中国信息安全认证中心颁发的ISCCC信息安全服务资质认证证书，包括：（1）应急处理一级服务资质（2）信息系统安全集成一级服务资质（3）风险评估一级服务资质。须提供以上三个证书的复印件。 |
| 获得国家信息安全测评中心颁发的信息安全服务资质证书，包括：（1）安全工程类二级（2）安全开发类一级；须提供以上两个证书的复印件。 |
| 国家计算机网络应急技术处理协调中心CNCERT颁发的网络安全应急服务支撑单位证书（国家级），提供复印件。 |
| Bypass交换机（2台） | 需要提供与设备相互兼容的bypass交换机；4个单模光纤接口（LC）；每个bypass交换机提供1路万兆Bypass交换能力，提供Fail-Safe保护功能；三年质保和软件升级（包含软件更新服务、产品保修服务、远程支持服务） |

### WEB应用防护系统（1台）

| **分类** | **具体要求** |
| --- | --- |
| 联动要求 | 考虑项目整体联动效果，需要和网络安全态势感知及运营平台统一品牌 |
| 设备要求 | 配置要求 | 2U机型,含交流冗余电源模块,2\*USB接口,1\*RJ45串口,2\*GE管理口,默认带50G SSL加速卡，≥4个 SFP口，≥4个万兆SFP+口，1个接口扩展槽位（可扩展≥4个 SFP口或者≥2个万兆SFP+口）；具备网页防篡改功能；三年质保和软件升级（包含软件更新服务、产品保修服务、远程支持服务）。 |
| 硬盘容量 | 设备自带硬盘容量≥1TB，无需依赖于独立的服务器或管理设备进行安全日志搜集。  |
| 性能要求 | 网络吞吐量不少于30G，应用吞吐量不少于15G。 |
| 部署能力 | 支持串联部署、旁路部署、反向代理以及镜像监听等部署模式。 |
| ★紧急模式 | 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成为瓶颈。当连接数恢复正常时，自动退出紧急模式，**提供界面截图并盖章证明**。 |
| 例外策略 | 支持对安全策略的一键式例外配置。 |
| WEB基础架构防护 | 支持防护：蠕虫、缓冲区溢出、CGI信息扫描、目录遍历等攻击。 |
| 暴力破解防护 | 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。 |
| 会话跟踪 | 支持会话追踪能力，能够关联用户的web请求及所有操作，达到攻击链还原，用户行为研究及攻击动机挖掘的目的。 |
| XML防护 | 支持XML防护，包括XML基础校验、Schema校验以及SOAP校验。 |
| ★智能补丁联动 | 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，**提供配置界面截图及厂商盖章证明。** |
| ★流量清洗 | 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，检测算法支持5种，包括：etag、http cookies、url cookies、ascii-image、bmp-image。支持对慢速攻击的防护，**提供界面截图盖章证明**。 |
| 支持与抗拒绝服务系统联动，对流量按需清洗。 |
| 产品资质 | 产品应获得至少为EAL3+级别的《国家信息安全测评信息技术产品安全测评证书》，提供证书复印件。 |
| ★移动端安全运维 | 可通过移动端实现设备安全运维监控，APP支持安全设备运行状态监控，监控指标包括CPU使用率、内存使用率、设备IP地址，设备状态，查看安全告警等功能，提供APP下载网页和相关链接以及包括APP相关功能界面的厂商盖章截图证明。 |
| 厂商资质 | 获得国家信息安全测评中心颁发的信息安全服务资质证书，包括：（1）安全工程类二级（2）安全开发类一级；须提供以上两个证书的复印件。 |
| 国家计算机网络应急技术处理协调中心CNCERT颁发的网络安全应急服务支撑单位证书（国家级），提供复印件。 |
| 获得中国信息安全认证中心颁发的ISCCC信息安全服务资质认证证书，包括：（1）应急处理一级服务资质（2）信息系统安全集成一级服务资质（3）风险评估一级服务资质。须提供以上三个证书的复印件。 |
| Bypass交换机（1台） | 需要提供与设备相互兼容的bypass交换机；4个单模光纤接口（LC）；每个bypass交换机提供1路万兆Bypass交换能力，提供Fail-Safe保护功能；三年质保和软件升级（包含软件更新服务、产品保修服务、远程支持服务） |

### 漏洞扫描系统（1台）

|  |  |
| --- | --- |
| **分类** | **具体要求** |
| 系统平台 | 系统使用专门的硬件，基于嵌入式安全操作系统，系统采用B/S架构设计，保证系统的工作效率和自身安全性。 |
| 联动要求 | 用于实现脆弱性管理，需要和网络安全态势感知及运营平台统一品牌。 |
| 配置要求 | 标准机1U架设备，含交流冗余电源，1\*RJ45串口，1\*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（可扩展8个千兆电口或者8个千兆SFP口）；可扫描IP总数（或域名数）：无限制, 提供≥2授权扫描端口，最大配置支持≥13路授权扫描端口,具备安全配置核查以及WEB应用漏洞扫描模块；三年质保和软件升级（包含软件更新服务、产品保修服务、远程支持服务）。 |
| 漏洞数 | 漏洞知识库漏洞信息大于22000条。 |
| 提供详细的漏洞描述和对应的解决方案描述。 |
| ★安全配置核查 | 设备可通过扩展支持安全配置核查功能，支持对以下组件进行检查：操作系统：WindowsXP/2003/2008/Vista/7/8、linux、Unix数据库: Mysql、Sybase、DB2、Oracle、Informix、MSSQL应用服务：Apache、Weblogic、TOMCAT、Websphere、IIS路由器：Cisco、Juniper、华为、H3C、中兴防火墙: CISCO、华为、Netscreen、Fortinet、安氏领信、CheckPoint虚拟化设备：VMware ESXi、Xen、XenServer、Hyper-V Wlan设备Wlan设备：中兴、华为、思科、国人、邦讯、大唐、H3C**（提供截图证明并加盖公章）**。 |
| ★高级扫描能力 | 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300条相关漏洞，并**提供功能截图和支持的漏洞列表并加盖公章**。 |
| 漏洞扫描时可以在扫描过程中人工指定包括SNMP、SMB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。 |
| 支持断点续扫，可对已完成的扫描任务中没有被覆盖到的目标重新下发扫描任务。 |
| 支持扫描国产操作系统、应用及软件的安全漏洞，如红旗、麒麟、起点操作系统。 |
| 扫描通知 | 允许管理员配置扫描通知，在扫描任务运行开始时向被扫描的资产发送扫描通知。 |
| ★自定义风险值标准 | 支持自定义风险值计算标准配置，可对主机风险等级评定标准和网络风险等级评定标准进行自定义，，**提供截图证明并加盖公章**。 |
| 产品成熟度 | 投标产品应该是经过市场考验的成熟产品，在国内市场具有较高的市场份额。在CCID或IDC有排名，且排名为前三的品牌，提供证明复印件。 |
| 产品资质 | 产品获得中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》 |
| 中国信息安全认证中心颁发的中国国家信息安全产品认证证书,提供复印件 |
| 产品要求取得中国信息安全测评中心信息技术产品安全测评证书（EAL3+以上级别）,提供复印件 |
| 厂商资质 | 获得国家信息安全测评中心颁发的信息安全服务资质证书，包括：（1）安全工程类二级（2）安全开发类一级；须提供以上两个证书的复印件。 |
| 获得中国信息安全认证中心颁发的ISCCC信息安全服务资质认证证书，包括：（1）应急处理一级服务资质（2）信息系统安全集成一级服务资质（3）风险评估一级服务资质；须提供以上三个证书的复印件。 |
| 安全厂商应具备主动发现主流操作系统或应用系统新漏洞的能力，被CVE收录并**公开发布**的漏洞数量不少于80个。需提供详细的CVE漏洞列表、安全厂商官网公开链接证明。 |
| 国家计算机网络应急技术处理协调中心CNCERT颁发的网络安全应急服务支撑单位证书（国家级），提供复印件。 |

### 网络安全审计系统（1台）

|  |  |
| --- | --- |
| **分类** | **具体要求** |
| 配置要求 | 系统采用专用硬件架构与专用安全操作系统；标准机2U架设备，含交流冗余电源模块，2\*USB接口，1\*RJ45串口，2\*GE管理口，≥8个 SFP口，≥4个万兆SFP+口；最大检测能力不少于30G；具备应用分析、流量分析功能模块；三年质保和软件升级（包含软件更新服务、产品保修服务、远程支持服务）。 |
| 考虑项目整体联动效果，需要和网络安全态势感知及运营平台统一品牌。 |
| 部署方式 | 采用B/S管理方式， 无需在被审计系统上安装任何代理，支持单点、多点、多级部署。 |
| 采用旁路部署方式对原有网络不造成影响，网络审计产品的故障不影响被审计系统的正常运行。 |
| 审计内容支持 | 系统应支持对常用的HTTP、SMTP/POP3、WEBMAIL、论坛、IM、音视频、P2P、网络游戏等网络行为进行审计并记录相关日志信息。可对基于明文传输的应用进行关键字内容审计，如邮件主题、论坛主题、发帖关键字、即时通讯关键字等，可进行网页还原。 |
| 支持审计ORALCE、SQL SERVER、MY SQL、DB2、Sybase、Infomix、Postgresql等各类主流数据库系统，并具备灵活的审计策略：支持基于IP地址、时间、用户/用户组、数据库用户名、数据库类型、数据库表名、字段名、关键字等组合审计策略，并实时告警响应。 |
| ★高级扩展审计能力 | WEB威胁分析能力：应能通过对互联网资源（域名、IP地址、URL等）进行威胁分析和信誉评级，将含有恶意代码的网站例入Web信誉库，达到阻止过滤含有恶意代码的高风险网站，实现对终端用户的安全保护，并且支持网页还原功能。 |
| WEB威胁分析能力：支持超过1000万条的庞大中英文URL数据库，超过十种分类，如不良言论、色情暴力等；根据用户设定规则，可过滤非法不良网站并实时告警。 |
| 无线审计能力：为满足使用要求，安全审计需支持网络无线热点审计功能，能发现非法的无线热点，记录无线热点访问网络时所使用的IP地址、认证用户等信息。支持扩展数据库审计能力：支持ORALCE、SQL SERVER、MY SQL、DB2、Sybase、Infomix、Postgresql等各类主流数据库系统审计：基于IP地址、时间、用户/用户组、数据库用户名、数据库类型、数据库表名、字段名、关键字等组合审计策略，并实时告警响应，**以上提供截图证明加盖原厂公章**。 |
| 网站挂马主动扫描：支持基于IP地址/域名、深度、并发数等多种组合扫描策略，记录符合扫描策略的网站IP地址等。 |
| 支持移动应用审计，能够识别通过移动热点所访问的移动类应用，例如IM类、社交类、网购类、影音类、资讯类等应用，并记录IP地址、应用名称、访问时间等信息；能够对主流的移动应用进行内容层面的详细审计，主要是对微博、网页言论、网页访问详细记录IP地址、URL地址、访问时间、访问或发布的具体内容等信息。 |
| 关联能力 | 支持用户身份信息智能关联技术，可将用户各种身份信息与其终端IP地址进行智能关联形成用户身份信息库，从而提高事件定位的精确度。 |
| 产品资质 | 信息系统安全专用产品销售许可证，请提供复印件。 |
| 中国信息安全测评中心《信息技术产品安全测评证书》（EAL3以上级别），请提供复印件。 |
| 国家版权局《计算机软件著作权等级证书》，请提供复印件。 |
| 厂商资质 | 获得国家信息安全测评中心颁发的信息安全服务资质证书，包括：（1）安全工程类二级（2）安全开发类一级；须提供以上两个证书的复印件。 |
| 获得中国信息安全认证中心颁发的ISCCC信息安全服务资质认证证书，包括：（1）应急处理一级服务资质（2）信息系统安全集成一级服务资质（3）风险评估一级服务资质。须提供以上三个证书的复印件。 |
| 国家计算机网络应急技术处理协调中心CNCERT颁发的网络安全应急服务支撑单位证书（国家级），提供复印件。 |

### 数据库审计系统（1台）

|  |  |
| --- | --- |
| **分类** | **具体要求** |
| 配置要求 | 硬件设备 | 标准机2U架设备，含交流冗余电源模块，2\*USB接口，1\*RJ45串口，1\*GE管理口，6\*GE电口，1个接口扩展槽位（可扩展为4个千兆SFP插槽）；支持审计的数据库实例不少于15个；三年质保和软件升级（包含软件更新服务、产品保修服务、远程支持服务）。 |
| 部署方式 | 设备支持旁路模式部署，通过端口镜像方式对数据库流量进行审计和告警 |
| 数据存储 | 系统自带内部存储，存储空间不低于4TB；  |
| 数据库类型 | 支持类型 | 支持以下数据库类型：Oracle、SQL Server、MySQL、DB2、GBase、DM |
| 审计能力和策略 | 审计内容 | 系统可记录以下会话终端信息：IP、MAC、Port、工具名(程序名)；  |
| 系统可记录会话登录时间、会话时长； |
| 系统可记录以下数据库操作信息：操作类型（DDL、DML、DCL等）、操作时间、执行时长、操作成功与失败、操作对象（表、列、存储过程名称）、SQL语句； |
| 系统可记录数据库操作影响的范围信息：如查询、修改、删除操作的影响行数,以及返回行数；  |
| 应用管理审计 | 支持应用关联审计，可在中间件平台环境下部署jWrapper精确还原应用用户，以满足GB/T 22239-2008信息系统安全等级保护在安全审计领域的基本要求，jWrapper需支持以下中间件平台:WebLogic, WebSphere, Tomcat  |
| ★入侵检测能力 | 漏洞攻击 | 可扩展支持数据库漏洞检测功能，提供对CVE上已公开的数据库漏洞攻击行为的监测与告警；提供200个以上漏洞攻击特征库；**提供厂商盖章的功能截图。** |
| SQL注入 | 可扩展支持SQL注入检测功能，通过模式匹配的方式对SQL访问进行监测与告警,判断是否为可疑SQL注入；提供SQL注入特征库；**提供厂商盖章的功能截图。** |
| 告警 | 告警策略 | 系统支持黑白名单告警策略：白名单对象不告警、黑名单对象告警。 |
| 响应方式 | 系统可根据不同的安全级别采用不同的响应方式，包括记录、告警。 |
| 系统支持的告警方式包括：邮件、短信、SYSLOG、SNMP。 |
| 产品资质 | 中国国家信息安全产品认证证书，请提供复印件。 |
| 公安销售许可证，请提供复印件。 |
| 厂商资质以及安全能力 | 获得中国信息安全认证中心颁发的ISCCC信息安全服务资质认证证书，包括：（1）应急处理一级服务资质（2）信息系统安全集成一级服务资质（3）风险评估一级服务资质。须提供以上三个证书的复印件。 |
| 获得国家信息安全测评中心颁发的信息安全服务资质证书，包括：（1）安全工程类二级（2）安全开发类一级；须提供以上两个证书的复印件。 |

## 安全服务技术要求

以下所有服务周期为一年。

###  7\*24小时网站监控服务

|  |  |  |  |
| --- | --- | --- | --- |
| **执行内容** | **执行细节** | **执行周期、频率** | **响应方式** |
| 页面篡改监测 | 监控站点及要求：对江苏师范大学对外网站进行主页监测，其中重要站点需要全域名监测。对保护站点的约定数量（数量支持自定义）关键页面进行实时篡改监测。 | 对每个关键页面监测次数每天不低于96次，每次监测间隔不高于15分钟 | 1、发现异常情况30分钟以内通知，发现网页被恶意篡改第一时间告警。2、在监测周报体现监测结果。3、通过邮件即时响应，同时在监测周报中体现监测结果。 |
| 网站访问平稳度监测（针对10个重要站点） | 实时监测目标站点的访问速度、页面加载时间等网站性能参数。 | 对每个目标站点监测次数每天不低于96次，每次监测间隔不高于15分钟 | 1、发现异常情况30分钟以内通知，发现无法访问第一时间告警。2、在监测周报体现监测结果，出示监测报告。 |
| 支持多协议平稳度监测，监测协议包括HTTP，HTTPS，TCP。 |
| 支持多点平稳度监测，并列举不少于三个监测点。 |
| 支持多种报警事件通告，通告内容包括通断，延迟，波动，异常返回码。 |
| 支持平稳度响应图片按时间定制展示。 |
| DNS解析监测（针对10个重要站点） | 实时监测多省主要运营商的DNS缓存服务器及被监测域名的授权服务器对被监测域名的解析结果是否正确。包括A记录、CNAME记录、NS记录、MX记录、SOA记录、PTR记录。 | 对每个目标域名监测次数每天不低于96次，每次监测间隔不高于15分钟 | 1、发现异常情况30分钟以内通知，发现无法访问第一时间告警。2、在监测周报体现监测结果 |
| 要求支持多省主流ISP的递归查询服务器，在全国各地部署多个监测节点，用以监控各地ISP的缓存服务器对目标站点的解析结果，确保各地用户都能正常访问用户站点，列举不少于三个监测点，需提供截图证明。 |
| 挂马监测 | 监控站点及要求：江苏师范大学对外网站进行主页监测，其中重要站点需要全域名监测。对目标站点的约定数量关键页面进行实时挂马监测。 | 支持进行分级监测，对于首页5分钟一次监测，二级页面15分钟监测一次，根据所选服务包不同会有所限制 | 1、发现异常情况，30分钟以内以邮件、短信、电话方式进行通知。2、在监测周报体现监测结果 |
| 各网站挂马情况的全面展示。 | 每周 | 通过邮件即时响应，同时在监测周报中体现监测结果 |
| 被挂马页面URL。 | 每周 | 通过邮件即时响应，同时在监测周报中体现监测结果 |
| 详细感染路径，需提供截图证明。 | 每周 | 通过邮件即时响应，同时在监测周报中体现监测结果 |
| 攻击类型及其次数统计等。 | 每周 | 通过邮件即时响应，同时在监测周报中体现监测结果 |
| Web应用漏洞（针对重要站点） | 支持扫描漏洞类型：SQL注入、XPATH注入、LDAP注入、SSI注入、系统命令执行、缓冲区溢出、格式化字符串攻击；客户端攻击类型：跨站脚本攻击、内容欺骗。 | 每周一次 | 发现异常第一时间通知用户，并形成漏洞说明文档。 |
| 授权类型：凭据/会话预测、授权不充分、会话期限不足、会话固定。 |
| 认证类型：弱口令验证、暴力猜测、认证不充分。 |
| 信息泄露：目录遍历、目录索引信息泄露。 |
| 漏洞通报平台里进行展示用户漏洞扫描所处的状态，待扫描、待验证、待修复、已修复，以及漏洞详情和解决方案 | 实时 | 在漏洞通报平台里进行展示 |
| 远程系统漏洞（针对重要站点） | 支持扫描漏洞类型：本地权限提升、远程执行命令、远程数据修改、远程拒绝服务、远程信息泄露、不必要的服务。 | 每周一次 | 发现异常第一时间通知用户，并形成漏洞说明文档。 |

服务交付成果：《江苏师范大学网站监测报告》

### 业务系统漏洞扫描与加固服务

|  |  |  |  |
| --- | --- | --- | --- |
| **执行内容** | **执行细节** | **执行周期、频率** | **响应方式** |
| 业务系统脆弱性扫描 | 系统层：包含UNIX系列、Linux系列以及专用操作系统等。通过脆弱性扫描需发现操作系统本身的不安全因素，主要包括身份认证、访问控制、系统漏洞等及操作系统的安全配置问题。 | ≥4次  | 针对扫描服务发现的漏洞，要求能够提供专业有效的解决建议，同时需派驻原厂人员进行驻场，对漏洞进行修复，对系统安全进行加固。 |
| 网络层：通过脆弱性扫描需发现网络信息的安全性问题，包括网络层身份认证，网络资源的访问控制，数据传输的保密与完整性、远程接入、域名系统、路由系统的安全等。 |
| 应用层：通过脆弱性扫描需发现所采用的应用软件和数据的安全性，包括：数据库软件、Web服务、电子邮件系统、域名系统、交换与路由系统、防火墙及应用网管系统、业务应用软件以及其它网络服务系统等。 |
| 对评估范围内的主机、服务器、信息系统等进行安全扫描，需提供资产与漏洞的对应及分布情况，需提供可操作的安全建议或临时解决办法。 |
| 可采用的扫描方式不仅限于硬件设备扫描，也可采用SaaS服务“零部署”的方式，收集资产并对资产进行漏洞扫描。 |
| 可支持SaaS漏洞扫描服务，可用于日常对各类IT资产操作系统或交换路由设备及系统上运行的数据库、Web网站等服务上存在的安全漏洞进行定期自助扫描。 |
| 扫描内容包含漏洞扫描、配置核查、WEB应用扫描等，对于扫描出的漏洞风险、配置核查风险、WEB应用风险需进行综合分析，给出总体综合评估结论，扫描报告可包含主机漏洞、配置核查等多项结果。  |
| 扫描器内置漏洞知识库漏洞信息大于22000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准，并提供CVE Compatible证书证明。 |
| 设备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。 |
| 设备可按IP范围、起止时间、任务名称、任务状态、漏洞模板、配置模板、用户账号筛选所有扫描任务并进行汇总，支持在线查看汇总的风险详情和输出离线汇总报表。 |
| 设备具备系统快照功能，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。 |
| 设备支持虚拟化设备配置核查，包括Hyper-V、VMWare ESXi、VMWare vCenter、XEN、XenServer配置核查。 |
| 设备支持Web应用扫描能力，提供多种Web应用漏洞的安全检测，如SQL注入、跨站脚本、网站挂马、网页木马、CGI漏洞等。 |
| 设备配置核查支持本地检查，可以利用ActiveX控件进行本地检查，仅需要IE访问配置核查设备即可进行本机配置核查 |
| 产品应该是被广泛应用的成熟产品，在国内市场具有较高的市场份额，在CCID或IDC有排名，且排名为前三的品牌。 |
| 外网远程扫描需针对信息系统层面，通过扫描器发现信息系统常见的SQL注入、跨站等漏洞。 |

服务交付成果：《江苏师范大学业务系统安全评估扫描结果》

前期部分交付成果和报告包括：

《江苏师范大学信息安全保障服务项目安全加固建议方案》

实施过程交付成果和报告包括：

《江苏师范大学信息安全保障服务项目安全加固结果报告》

《江苏师范大学信息安全保障服务项目安全加固实施分析》

《江苏师范大学信息安全保障服务项目安全加固复检报告》

《江苏师范大学信息安全保障服务项目安全加固分析报告》

### 渗透测试服务

|  |  |  |  |
| --- | --- | --- | --- |
| **执行内容** | **执行细节** | **执行周期、频率** | **响应方式** |
| 网站漏洞渗透测项目 | 在服务期内对学校指定的2个系统进行渗透测试。 | ≥1次 | 需派驻原厂人员进行驻场，通过渗透测试，发现业务系统存在的安全漏洞，并为客户提供修复建议，包括配置、认证、会话、授权、数据验证等测试内容，以及安全建议整理及测试报告编写等工作。 |
| 厂商服务人员提供的渗透测试报告，必须包含漏洞从发现到最终利用的整个过程记录，通过校方对系统进行加固完之后，需要进行二次测试已确认漏洞是否合理修复。 |
| 数据存储区：SQL 注入、二次注入、NoSQL注入、XPath注入、LDAP注入。 |
| 验证机制：设计缺陷、暴力破解登陆、可预测性、注册用户、记住密码、 密码修改、忘记密码缺陷、万能密码登录绕过。 |
| 会话管理：可预测性、泄露令牌、劫持令牌。 |
| 访问控制：水平权限、垂直权限、未授权访问。 |
| 后端组件：注入操作系统命令、操作文件路径、注入 XML 后端 HTTP 请求。 |
| 应用程序逻辑缺陷： 无限制操作、 绕过、 验证码问题、 修改任意密码、与机制竞争。 |
| 跨站攻击：反射型 XSS、存储型 XSS、DOM 型 XSS、请求伪造、UI 伪装、数据劫持。 |
| 信息泄露：错误信息、调试信息、公共信息、提示信息、敏感信息。上传漏洞：任意上传文件、截断上传。 |
| 服务器漏洞渗透测试项目 | 在服务期内对学校指定的2个系统进行渗透测试。 | ≥1次 | 需派驻原厂人员进行驻场，通过渗透测试，发现业务系统存在的安全漏洞，并为客户提供修复建议，包括配置、认证、会话、授权、数据验证等测试内容，以及安全建议整理及测试报告编写等工作。 |
| 厂商服务人员提供的渗透测试报告，必须包含漏洞从发现到最终利用的整个过程记录，通过校方对系统进行加固完之后，需要进行二次测试已确认漏洞是否合理修复。 |
| Web 服务器配置缺陷：默认证书、默认内容、目录列表、WebDAV 方法、Web服务器作为代理服务器、虚拟主机配置缺陷、保障 Web 服务器配置的安全。 |
| 易受攻击的服务器软件： 应用程序框架缺陷、 内存管理漏洞、 编码与规范化漏洞、查找 Web 服务器漏洞。 |

服务交付成果：《江苏师范大学渗透测试报告》

### 应急响应服务

|  |  |
| --- | --- |
| **执行内容** | **执行细节** |
| 应急服务 | 要求在服务期内需提供至少2次应急服务。 |
| 接到应急响应请求时迅速启动响应预案。 |
| 接到远程紧急响应请求发出 30 分钟内指派工程师进行远程支持。 |
| 在远程紧急响应2小时后未能解决问题，则立即执行本地紧急响应流程，在本地紧急响应请求发出后，工程师需要在2小时内到达事故现场，协助客户人员进行问题处理； 若有需要，必须提供厂商自主研发的web应用防火墙、配置核查系统、入侵防御系统、远程安全评估系统、抗拒绝服务系统等硬件设备进行防护；为能随着入侵事件的变化动态调整设备，保证处于设备最佳防护状态，要求设备可与同品牌云对接，提供设备可管理服务，包括策略调优、日志分析、设备维护等；响应服务完成后，服务人员需要整理详细的事故处理报告，内容包括事故原因分析、已造成的影响、解决方案等。 |
| 如遇到重大的攻击事件，为保障系统安全，确保问题已得到实质性解决，用户可提要求，需要派原厂服务人员在安全加固后，继续现场值守3天。 |
| 远程紧急响应和本地紧急响应提供 7×24 小时服务。 |

服务交付成果

评估部分交付成果和报告包括：

《江苏师范大学信息安全保障服务项目应急响应级别对应表》

《江苏师范大学信息安全保障服务项目应急响应事件记录单》

《江苏师范大学信息安全保障服务项目安全事件分析》

事后总结交付成果和报告包括：

《江苏师范大学信息安全保障服务项目安全事件处理总结报告》

### 安全制度梳理

|  |  |  |  |
| --- | --- | --- | --- |
| **执行内容** | **执行细节** | **执行周期、频率** | **响应方式** |
| 安全制度梳理 | 梳理和核查包括不限于以下各项信息安全管理制度及制度执行情况:信息安全组织架构设置、信息安全人员配备和岗位职责制定优化、信息系统的规划、建设、运维、废弃等环节的信息安全制度制定、信息安全制度执行情况记录。 | ≥1次 | 厂家安排专业的工程师编写规范制度。 |
| 协助江苏师范大学完成信息安全管理体系落地，其中包含：建立适合学校实际的信息安全管理体系框架、评估和识别关键的业务处理流程、资产和岗位设置等、实现安全体系文档化，管理流程化、绩效控制可量化和安全意识普及。 |
| 协助学校对外包或购置的开发软件在投入使用前提出相关安全开发制度。 |

服务交付成果：

《江苏师范大学日常工作安全管理制度》

《江苏师范大学安全运维管理制度》

《江苏师范大学第三方技术人员管理制度》

### 安全培训服务

|  |  |  |  |
| --- | --- | --- | --- |
| **执行内容** | **执行细节** | **执行周期、频率** | **响应方式** |
| 安全服务培训 | 根据江苏师范大学信息系统和人员的情况，提供不少于3次的信息安全专业系列培训课程，培训课程和培训计划江苏师范大学自行选择。 | 至少3次（每次培训时间不少于2小时） | 厂家安排专业的安全培训工程师进行培训，并提供安全培训PPT课件。 |
| 安全意识培训内容主要讲办公电脑、平板、智能设备、移动存储设备等终端设备在使用互联网、内网网络的安全、保密意识和安全常识。 |
| 安全技术培训内容主要讲解当前最新的安全技术、黑客攻击技术和手段，以及如何做好日常的各项防范工作。 |
| 安全等级保护培训内容主要讲国家等级保护工作政策、行业标准、监管要求、最佳实践等方面的发展情况。 |

服务交付成果：

《江苏师范大学培训大纲》

《江苏师范大学培训内容PPT》

### 等保咨询服务

|  |  |  |  |
| --- | --- | --- | --- |
| **执行内容** | **执行细节** | **执行周期** | **响应方式** |
| 完成应用系统等级保护 | 完成两个指定系统的三级等级保护测评和六个指定系统的二级等级保护测评 | / | 需要帮助用户通过指定应用系统的等保测评：两个三级系统，六个二级系统，**报价应包含测评费用** |
| 定级备案服务 | 对学校信息系统进行摸底调查，全面掌握系统的网络分布、业务类型、应用或服务范围、管理架构、系统结构等基本情况，按照《信息安全等级保护管理办法》和《信息系统安全等级保护定级指南》的要求，确定定级对象。 | 不限次数 | 厂家基于不同的需求，提供相应专业的咨询服务以及相应输出文件。 |
| 差距分析服务 | 协助招标人完成业务系统的等保评估（风险评估，差距报告）并提供详细的整改方案。 |
| 协助预测评服务 | 对学校等保安全整改和信息系统完成自测工作并给出相应参考分数。 |
| 协助备案服务 | 协助招标人完成等级保护测评及备案： （1）根据国家评测标准进行提交前的内部预测评自测报告工作。（2）协助招标人通过国家推荐的等保测评机构的测评及获得公安机关颁发的《信息系统安全等级保护备案证明》，并在测评期间的意见对现有系统进行进一步的整改和加固，直至最终通过测评。（3）协助招标人向公安机关有关部门申请相关应用系统的《信息系统安全等级保护备案证明》，包括准备资料和完成手续相关材。 |

服务交付成果：《江苏师范大学安全咨询指导建议书》

### 安全驻场服务（原厂工程师1人）

|  |  |  |  |
| --- | --- | --- | --- |
| **执行内容** | **执行细节** | **执行周期、频率** | **响应方式** |
| 重要活动安全驻场服务 | 提供一名原厂专业安全工程师进行安全驻场服务；在重要活动期间增派1名以上专业安全工程师现场值守，协助监测学校网络设施和信息系统安全运行状况，内容主要包括安全设备监控、安全巡检、安全日志分析、 应急处置四项主要内容：安全设备监控：对安全设备运行进行监控和维护；安全巡检：对安全设备进行健康状态检查，包括系统引擎、CPU占用率、内存占用率、接口状态、证书授权状态等内容；安全日志分析：对安全设备产生的高、中风险告警事件进行分析，包括事件类型分布、事件发展趋势、事件频率、源地址、目的地址等内容；应急处置：对突发安全事件进行应急响应，阻止安全事件影响扩大，查找安全事件产生原因。 | ≥12次 | 厂家人员根据活动重要性定好值守级别和值守时间；现场值守实施工作完成后，值守人员对当日值守情况形成日报，一个周期的值守工作完成后三个工作日内，值守人员将出示一份现场值守整体报告。 |

服务交付成果：《江苏师范大学巡检报告》

### 服务厂商资质要求

|  |  |
| --- | --- |
| **分类** | **具体要求** |
| 提供原厂服务的厂商资质 | 获得中国信息安全认证中心颁发的ISCCC信息安全服务资质认证证书，包括：（1）应急处理一级服务资质（2）信息系统安全集成一级服务资质（3）风险评估一级服务资质。须提供以上三个证书的复印件。 |
| 获得国家信息安全测评中心颁发的信息安全服务资质证书，包括：（1）安全工程类二级（2）安全开发类一级；须提供以上两个证书的复印件。 |
| 国家计算机网络应急技术处理协调中心CNCERT颁发的网络安全应急服务支撑单位证书（国家级），提供复印件 |

# 服务能力及工作要求

## 产品质保及售后服务

（1）该项目中所有硬件产品以及软件平台类产品免费质保叁年，设备均为原厂生产（**投标时需提供原厂商授权及叁年质保函原件）**；设备安装、调试等须由设备供应商工程师上门免费服务。在质量保证期内更换的任何配件，须为原设备厂家生产并且保证替代的零配件是新的未使用过和未经修复的。

（2）设备所有的软件系统、相关数据库等均须提供叁年免费升级。供货时提供完备的软件、技术资料和用户维护手册。

（3）产品质保期从货物安装调试、验收合格之日起计算。在质保期内中标供应商应自行处理保修凭证问题，采购人不负责提供产品的保修卡、发票等保修凭证。

（4）质保期内中标供应商须提供7×24小时免费服务，1小时内做出响应，24小时内应派专业技术人员到达现场提供免费咨询、维修服务。如属硬件故障原因而且24小时无法排除故障的，则应免费提供同等配置的备用设备以保证用户设备的正常运行。若未能在规定的时间内进行现场响应和解决设备问题的，用户采取一切措施所产生的费用和风险由中标供应商承担。

## 安全服务实施要求

（1）项目周期及计划要求

项目应严格按照国家信息安全等级保护相关要求以及满足江苏师范大学信息安全保护需求等按期、按质执行，确保在规定的时间内完成各项检查及信息安全工作。

（2）项目交付要求

项目中各项安全服务结果必须真实、可靠、全面，满足各级主管部门网络与信息安全检查相关要求、国家信息安全等级保护标准要求；

项目实施过程产生的所有过程文档、检查记录、人员访谈纪要、检测原始数据、服务结果报告等必须进行电子和纸制双重归档，根据要求，整理成册，并及时交付江苏师范大学相关部门及责任人。

（3）项目资源要求

为确保信息安全服务项目的有效落实，合作方需具备全面的项目管理能力，对于项目各项服务内容要求、实施计划与质量控制、风险评估与分析、专项问题分析与咨询等方面，提出完整的管控方案。

应当按计划合理配置人员进行安全服务实施；

应当由专人进行项目管理与跟踪。

## 安全服务管理要求

（1）服务方必须严格遵守学校的各项规章制度和劳动纪律。

（2）服务方必须遵守保密制度，做好对学校网络资料和资源的保密工作。

（3）服务方在工作中能服从学校的统一安排和管理。

## 安全服务保密要求

没有学校事先书面同意，服务方不得将由学校提供的有关合同或任何合同条文、规格、计划、图纸、师生信息或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

## 安全服务考核办法

采用中期考核和终期考核的方式，对安全服务单位服务质量进行考核。考核内容主要依据以下条款：

（1）按采购文件及合同要求提供相关服务成果报告，所有报告以及协助甲方完成的安全制度梳理文档应按照规定的内容、格式要求，规定的时间、频率要求提供，每发生一次服务报告事故（内容明显错误、数据格式错误、迟于规定时间提交等）扣1分。

（2）月度高危安全漏洞误报率（含漏报率）超过5%，出现一次扣5分。月度高危安全漏洞误报率=（月度误报数量+漏报数量）/月度高危事件通报总数。其中误报数量是指被通报用户单位反馈通报信息有误且经证实的数量，漏报数量是指对相同被扫描主体的安全漏洞，服务服务单位未发现、未验证，但由其他渠道（教育部、公安、网信、省通管局等）被通报的事件数量。

（3）保障安全服务连续性，因乙方原因造成服务中断，影响业务正常运行的情况，每出现一次扣1分，2小时内无法恢复的，修复每延长2小时扣1分。

（4）安全服务期间不服从甲方统一安排管理，由于乙方态度问题与甲方运维人员发生冲突，每出现一次扣2分。

（5）安全服务期间未能及时响应甲方服务需求，提供相关服务支撑，每出现一次扣1分。

（6）考核满分为100分，当乙方出现扣分情节，甲方会以书面方式告知（允许乙方进行申诉，申诉失败开始扣分）。总计分低于90分甲方将以书面文件对乙方进行一次警告，总计分低于80分视为不合格，甲方有权进行追责（包括要求限期整改，严重直至终止服务合同等）。

（7）出现违反安全保密要求和信息泄露事件的，甲方可直接终止服务合同、扣除指定比例服务费并追责。