**浙江金融职业学院**

**数据中心高级威胁监测与安全管理项目**

**磋商文件**

**（线上电子交易）**

**项目名称：数据中心高级威胁监测与安全管理项目**

**项目编号：QSZB-Z(H)-B22216(CS)**

**采 购 人：浙江金融职业学院**

**采购代理机构：浙江求是招标代理有限公司**

**采购计划文号：[2022]31352号**

**目 录**

**第一章 采购邀请**

**第二章 采购需求**

**第三章 供应商须知**

**第四章 评审方法和评审标准**

**第五章 拟签订的合同文本**

**第六章 响应文件格式**

**第一章 采购邀请**

**项目概况**

 **数据中心高级威胁监测与安全管理项目 采购项目的潜在供应商应在 政府采购云平台（https://www.zcygov.cn） 获取（下载）采购文件，并于 2022年7月8日13:30:00 （北京时间）前提交（上传）响应文件。**

**一、项目基本情况**

1.项目编号：QSZB-Z(H)-B22216(CS)

2.项目名称：数据中心高级威胁监测与安全管理项目

3.采购方式：竞争性磋商

4.预算金额（元）：750000

5.最高限价（元）：750000

6.合同履约期限：合同签订后60天内完成所有硬件设备的安装、调试并交付使用

7.本项目（是）接受联合体响应。

8.采购需求：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **标项****序号** | **名称** | **数量** | **单位** | **简要技术需求或服务要求** | **是否允许采购进口产品** |
| 1 | 数据中心高级威胁监测与安全管理项目  | 1 | 批 | 详见采购需求 | 不允许 |

**二、申请人的资格要求：**

1.满足《中华人民共和国政府采购法》第二十二条规定，未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

2.落实政府采购政策需满足的资格要求：无

3.本项目的特定资格要求：无。

**三、获取（下载）采购文件**

时间：2022年6月27日至2022年7月8日，每天上午00:00至12:00，下午12:00至23:59（北京时间，线上获取法定节假日均可，线下获取文件法定节假日除外）

地点（网址）：政府采购云平台（https://www.zcygov.cn）

方式：供应商登录政采云平台（https://www.zcygov.cn）在线申请获取采购文件（进入“项目采购”应用，在获取采购文件菜单中选择项目，申请获取采购文件）

售价（元）：0

**四、响应文件提交（上传）**

截止时间：2022年7月8日13:30:00（北京时间）

地点（网址）：政府采购云平台（https://www.zcygov.cn）

**五、响应文件开启**

开启时间：2022年7月8日13:30:00（北京时间）

地点（网址）：政府采购云平台（https://www.zcygov.cn）/杭州市西湖区玉古路173号中田大厦16楼（求是招标会议室6）

**六、公告期限**

自本公告发布之日起3个工作日。

**七、其他补充事宜**

1.《浙江省财政厅关于进一步发挥政府采购政策功能全力推动经济稳进提质的通知》 （浙财采监（2022）3号）、《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号）已分别于2022年1月29日和2022年2月1日开始实施，此前有关规定与上述文件内容不一致的，按上述文件要求执行。

2.根据《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号）文件关于“健全行政裁决机制”要求，鼓励供应商在线提起询问，路径为：政采云-项目采购-询问质疑投诉-询问列表:鼓励供应商在线提起质疑，路径为：政采云-项目采购-询问质疑投诉-质疑列表。质疑供应商对在线质疑答复不满意的，可在线提起投诉，路径为：浙江政府服务网-政府采购投诉处理-在线办理。

3.供应商认为采购文件使自己的权益受到损害的，可以自获取采购文件之日或者采购公告期限届满之日（公告期限届满后获取采购文件的，以公告期限届满之日为准）起7个工作日内，对采购文件需求的以书面形式向采购人提出质疑，对其他内容的以书面形式向采购人和采购代理机构提出质疑。质疑供应商对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。

4.其他事项：

（1）需要落实的政府采购政策：包括节约资源、保护环境、促进中小企业发展等。详见磋商文件的第三章-采购项目需要落实的政府采购政策。

▲（2）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动；为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后不得再参加该采购项目的其他采购活动。

**八、凡对本次采购提出询问、质疑、投诉请按以下方式联系**

1.采购人信息

名称：浙江金融职业学院

地址：杭州市下沙高教园区学源街118号

联系方式： 陈老师 0571-86766955

项目联系人（询问）：徐老师

项目联系方式（询问）:18958092458

质疑联系人： 潘老师

质疑联系方式： 0571-86739399

2.采购代理机构信息

名称：浙江求是招标代理有限公司

地址：杭州市西湖区玉古路173号中田大厦11楼

传真：/

项目联系人（询问）：陈应俭、杨立凯

项目联系方式（询问）：0571-87670301

质疑联系人：余水星

质疑联系方式：0571-81110356

质疑邮箱：jdkh@qszb.net

3.同级政府采购监督管理部门

名称：浙江省财政厅政府采购监管处

地址：杭州市环城西路37号

传真：/

联系人：倪文良、吴聪瑜

监督投诉电话：0571-87057615、87058489

若对项目采购电子交易系统操作有疑问，可登录政采云（https://www.zcygov.cn/），点击右侧咨询小采，获取采小蜜智能服务管家帮助，或拨打政采云服务热线400-881-7190获取热线服务帮助。

CA问题联系电话（人工）：汇信CA 400-888-4636；天谷CA 400-087-8198。

**第二章 采购需求**

**一、为落实政府采购政策需满足的要求：**

|  |  |  |
| --- | --- | --- |
| **序号** | **政策名称** | **内容** |
| 1 | 政府采购进口产品 | 不允许采购进口产品 |
| 2 | 政府强制采购节能产品 | 不适用 |
| 3 | 政府优先采购节能、环保产品 | 提供材料详见磋商文件第六章“商务和技术文件” |
| 4 | 政府采购促进中小企业发展 | 提供材料详见磋商文件第六章“报价文件”**本项目采购标的为：货物，采购标的对应的中小企业划分标准所属行业：软件和信息技术服务业****中小企业划型标准：软件和信息技术服务业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员10人及以上，且营业收入50万元及以上的为小型企业；从业人员10人以下或营业收入50万元以下的为微型企业。** |
| 5 | 政府采购支持监狱企业发展 | 提供材料详见磋商文件第六章“报价文件” |
| 6 | 政府采购促进残疾人就业 | 提供材料详见磋商文件第六章“报价文件” |

**二、采购资金的支付方式、时间、条件：**

|  |  |
| --- | --- |
| **▲履约保证金** | 无 |
| **▲付款方式** | 1.预付款：1.1.支付条件：供应商提交银行、保险公司等金融机构出具的预付款保函；1.2.支付时间、数额：合同生效并具备实施条件后七个工作日内，采购人向成交供应商支付合同金额40%的预付款。备注：签订合同时，供应商明确表示无需预付款或者主动要求降低预付款比例的，采购单位可不适用前述规定。2.项目完成后，经采购人验收合格后，采购人自收到发票后7个工作日内，支付至合同金额的100%。 |

**三、服务要求（技术要求里另有注明的以技术要求为准）：**

|  |  |
| --- | --- |
| **交付时间** | 合同签订后60天内完成所有硬件设备的安装、调试并交付使用 |
| **交付地点** | 采购人指定地点 |
| **质保期** |

|  |  |  |
| --- | --- | --- |
| 高级威胁监测安全系统及配套服务 | 高级威胁监测安全系统 | 5年 |
| 安全配套服务（安全运营分析） | 5年 |
| 安全配套服务（其它） | 2年 |
| 应急响应服务 | 现场安全应急响应 | 2年 |
| 重保服务 | 现场重保值守服务 | 2年 |
| 网站云防护 | 网站云防护服务 | 1年 |
| 网站云监测 | 网站云监测服务 | 1年 |

▲质保期不满足磋商文件要求的响应无效。 |
| **服务标准、期限、效率** | 1.在质保期内，供应商应对货物出现的质量及安全问题负责处理解决并承担一切费用，每年安排不少于四次原厂工程师上门巡检设备、查看分析日志、升级固件软件、优化设备、调整不合理配置。2.质保期内出现无法排除的故障，供应商需无条件更换同型号产品。3.质保期满后，供应商继续为采购人服务，仅收取零配件成本费。4.因人为因素出现的故障不在免费保修范围内。5.如在使用过程中发生质量问题，响应供应商须提供7\*24小时技术支持，出现系统故障30分钟内响应，需要现场服务时2小时赶到现场，24小时解决故障，出现重大故障时，负责用户与厂商之间的技术协调工作。 6.培训：供应商应对采购人的操作人员、维修人员免费进行培训；供应商应提供相应的培训计划；上述内容的实现方式、时间、地点、人数应在响应文件中详细说明。 |
| **其他技术、服务要求** | 1.供应商应按磋商文件规定的货物性能、技术要求、质量标准向采购人提供未经使用的全新产品，符合国家法律规定和技术规格、质量标准的出厂原装合格产品。2.技术支持：供应商应及时免费提供合同货物软件的升级，免费提供合同货物新功能和应用的资料。3.安装调试： 3.1安装地点：采购人指定地点；3.2安装完成时间：接到采购人通知后在规定时间内完成安装和调试，如在规定的时间内由于供应商的原因不能完成安装和调试，供应商应承担由此给采购人造成的损失；3.3如供应商委托国内代理（或其他机构）负责安装或配合安装应在签约时指明，但供应商仍要对合同货物及其安装质量负全部责任；3.4安装标准：符合我国国家有关技术规范要求和技术标准，所有的软件和硬件必须保证同时安装到位；3.5供应商免费提供合同货物的安装服务；3.6供应商在响应文件中应提供安装调试计划、对安装场地和环境的要求。4.供应商应提供质保期满后主要零部件报价单、质保期满后维护费、软件升级及其相关服务内容；5.供货时提供有关的全套技术文件。6.供应商应保证所提供的货物或其中任何一部分均不会侵犯第三方的知识产权。 |
| **验收标准** | 1.验收由采购人负责实施；2.验收依据：2.1合同、磋商文件、响应文件；2.2供应商提供的技术规格、经采购人认可的合同货物的有效检验文件；2.3供应商响应文件中提供的经采购人认可的合同货物的验收标准（符合中国有关的国家、地方、行业标准）和检测办法及相应检测手段。3.供应商应派员在所供货物到采购人处时进行到货验收，有需要时能联系产品制造商到场共同验收，若发现任何损坏及质量问题，供应商负责妥善处理直至采购人满意，由此产生的费用由供应商承担。4.验收合格的条件：4.1所供货物符合产品标准和合同的要求；4.2在进行测试和验收过程中发现的问题已被解决并得到采购人的认可；4.3合同中规定的所有货物和材料均已交付；4.4所供货物已通过使用单位组织的验收；4.5所有相关的技术文件及资料均已提交并得到接受。 |

**四、技术要求：**

**（一）需执行的国家相关标准、行业标准、地方标准或者其他标准、规范：**如技术要求中未注明需执行的国家相关标准、行业标准、地方标准或者其他标准、规范的，执行最新标准、规范。

**（二）采购标的项目概况：**

1.1.建设背景

2014年2月，中央网络安全和信息化领导小组成立，习近平总书记作为领导小组组长，指出“没有网络安全就没有国家安全”、“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施”，确定了国家网络安全和信息化发展的方向。2017年6月1日起正式施行的《中华人民共和国网络安全法》，指出“国家实行网络安全等级保护制度”， 2019年5月，《网络安全等级保护制度2.0》发布，网络安全等级保护制度体系已经发生了巨大的变化。随着高校信息化建设的逐步深入，学校教务工作、招生工作、科研管理工作、学生校内的学习和生活等对信息系统的依赖程度越来越高；教育信息化建设中大量的信息资源，成为学校成熟的业务展示和应用平台，在未来的教育信息化规划中占有非常重要的地位。从安全性上分析，高校业务应用和网络系统日益复杂，外部攻击、内部资源滥用、木马和病毒等不安全因素越来越显著，信息化安全是业务应用发展需要关注的核心和重点。为贯彻落实国家信息安全等级保护制度和《网络安全法》，规范和指导全国教育信息化建设工作，国家发布了一系列关于教育行业信息化工作的通知，并且随着我国网络安全法的正式实行，保障信息系统安全已经成为学校应承担的法律义务。

浙江金融职业学院作为全国双高校建设标杆，在网络信息安全建设过程中，一方面要规划部署网络信息安全设备提升安全防护能力，另一方面需要加强学校网络信息安全的日常运维、管理，确保学校网络信息安全在关键时间节点不出事故，守住网络信息安全红线。

学校网络信息安全防护目前采用传统模式，以出口下一代防火墙（带IPS、WAF模块）为主，通过防火墙访问策略配置、IPS入侵检测、WAF防护，以及加上联动处置模块，有效提升了学校安全防护能力，保护了学校信息化资产。但随着国家，以及教育主管部门对网络安全越来越重视，同时黑客攻击手段不断的更新，学校网络信息安全面临更大的挑战，在每年内部攻防演练过程中，很多高校被成功入侵。为此，我们需不断明确网络安全在信息化过程中的重要性，并根据网络安全技术的迭代更新，不断优化我们学校整体安全防护方案。

1.2.建设目标

在面临越来越严峻的网络安全形势下，通过本项目的实施，有效梳理学校网络信息安全防护体系、层次，完善各类安全设备的防护策略；通过漏洞扫描、渗透测试等途径，发现问题，解决问题。特别在重大时间节点，专业人员安全值守，基于情报的高级威胁监测，可以快速的帮助安全运营人员发现、研判重大安全事件（如：永恒之蓝、APT事件、挖矿病毒等），确保不发生重大网络安全事件，持续提升学校网络信息安全防护能力。

具体目标为：

1、学校整体网络流量高，分析数据庞大，需要对网络流量进行监测，同时出具对应的威胁分析报告；

2、对学校的网络流量数据进行存储和还原，对已经发生网络攻击行为，攻击路径、受感染面和信息泄露状况，结合业务场景从多个维度对攻击事件进行分析，提高对威胁的认知；

3、对学校各类信息系统、核心资产进行定期的漏洞扫描、弱口令检查、渗透测试检查等，并及时、有效、专业的解决发现的问题；

4、对学校服务器、网络设备、安全设备等IT设备自身存在的安全配置缺陷和薄弱环节进行分析、修补、检验，消除、降低IT设备的高、中风险隐患，防范安全事件发生，避免信息系统脆弱性被非法利用，增强信息系统安全防范能力，保障业务的可持续性；

5、提供应急响应演练、应急响应服务，学校一旦发生网络安全事故，安全运维服务人员做到第一时间响应，第一时间解决；

6、在重大事件时期，通过多方管理进行现场安全保障，维护持续安全防护能力。

（三**）采购标的需满足的质量、安全、技术规格、物理特性等要求**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 采购项 | 采购内容 | 数量 | 计量单位 | 备注 |
| 1 | 高级威胁监测安全系统及配套服务 | 高级威胁监测安全系统 | 1 | 套 |  |
| 安全配套服务 | 1 | 项 |  |
| 2 | 应急响应服务 | 现场安全应急响应 | 10 | 次 |  |
| 3 | 重保服务 | 现场重保值守服务 | 50 | 人/天 |  |
| 4 | 网站云防护 | 网站云防护服务 | 1 | 年 | 20域名 |
| 5 | 网站云监测 | 网站云监测服务 | 1 | 年 | 20域名 |

**（四）总体要求**

4.1高级威胁监测安全系统及配套服务

|  |  |
| --- | --- |
| 名称 | 技术需求 |
| 高级威胁监测安全系统组成 | 包含2台独立设备，由威胁分析模块、全流量威胁发现模块（分析探针）两个节点组成。其中两个独立设备为同一品牌。 |
| 威胁分析模块 | 标准2U设备；≥4\*GE管理电口；≥3\*USB3.0接口；≥2\*10GE业务光口；冗余电源；内存≥128G；≥960G SSD + 8\*4TB SATA 存储硬盘；处理性能≥10000eps。系统软件1套。不少于5年原厂标准维保服务。不少于5年威胁情报更新授权与规则升级授权。不少于2个SOAR流程授权。 |
| 全流量威胁发现模块（分析探针） | 标准2U设备；≥2\*GE流量监听电口；≥2\*10GE流量监听光口；≥2\*GE管理电口；≥2\*USB接口；≥2\*GE千兆接口；冗余电源；≥4TB SATA存储硬盘。吞吐≥8Gbps。系统软件1套。不少于5年原厂标准维保服务；不少于5年威胁情报更新授权与规则升级授权。 |

4.1.1威胁分析模块功能参数

|  |  |
| --- | --- |
| 功能类别 | 招标要求 |
| 硬件规格 | 标准2U设备，≥4\*GE管理电口；≥3\*USB3.0接口；≥2\*10GE业务光口；冗余电源；内存≥128G； |
| 存储容量：≥960G SSD系统盘 + 8\*4TB SATA 数据盘； |
| 处理性能≥10000eps |
| 威胁感知 | 告警分析 | 支持告警的深度行为分析，行为包括DNS解析行为、TCP/UDP交互行为、WEB访问行为、传输文件行为 |
| 受害资产分析 | 支持以受害资产维度进行分析，分析内容包括失陷状态、受到的攻击类型、威胁级别、处于的攻击阶段、所属的资产分组 |
| 攻击者分析 | 以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产。 |
| 威胁分析 | 支持平台内置的静态文件检测引擎、AI智能引擎、SAVE查杀引擎、webshellkiller引擎，利用LSA, AutoEncoder, LogicRegression, SVM, 随机森林，XGBoost等多种机器学习算法组合进行综合研判。支持采用AI技术针对无文件落地的恶意脚本进行检测。 |
| 威胁情报维度分析包括：情报详情、影响资产列表、资产的行为（行为包含：DNS解析、TCP流量、UDP流量、WEB访问、文件传输）； |
| 系统安全的细分维度包括：漏洞、弱口令、勒索病毒设备安全、挖矿行为设备安全； |
| 云端联动 | 支持云端与本地威胁情报共享，实时收集同步攻击者IP，并详细展示情报列表，包括IOC、区域、来源、更新时间、剩余封锁时间、状态、操作等。 |
| 威胁情报 | 支持基于威胁情报的威胁检测，检测类型包含APT事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件，并可自定义威胁情报 |
| 白名单 | 支持对告警进行加白，加白参数包括受害IP、攻击IP、威胁情报、规则、XFF、URL、威胁名称； |
| 行为分析 | DNS访问分析 | 支持DNS服务器日志导入，可以接入DNS服务器的日志，安全分析引擎将结合DNS服务器的日志，定位出DNS服务器代理风险外连场景下真实源IP，从而有效地进行风险处置闭环。 |
| 支持DNS重绑定分析：能够展示受害IP、攻击IP、域名、DNS解析记录、访问时间等详细信息； |
| 非常规访问分析 | 支持可疑代理分析：能够发现socks、http、reDuh、Regeory Tunnel、Tunna等代理类型； |
| 支持远程工具分析：能够发现pc\_anywhere、ultra\_vnc、chrome\_remote\_desktop、oray、teamviewer等远程工具类型； |
| 支持反弹shell分析：能够展示受害IP、攻击IP、端口、受害地域/资产组、攻击地域/资产组、最近访问时间等详细信息； |
| 邮件行为分析 | 支持针对政企邮件混淆宏病毒威胁检测，可通过不断下钻的特征向量提取和聚类算法有效检出邮件威胁。支持对smtp、imap、pop3、webmail等邮件协议审计，提取邮件正文和附件中的流量，并对邮件附件、正文链接、邮件行为、发件人等多维度进行规则和机器学习检测，从而识别出钓鱼邮件、病毒邮件、垃圾邮件、鱼叉式钓鱼等恶意邮件。 |
| 登录行为分析 | 支持暴力破解行为检测，检测内容包含：源ip、目的ip、使用协议、爆破次数、爆破成功与否等； |
| 为了解决校园网存在大量弱密码的问题，提高弱密码检测精准度，弱密码检测弱密码检测逻辑分为登录入口、弱密码定义、登陆结果三个步骤，登陆结果检测技术基于UEBA学习技术（无监督自我学习）提取登陆成功的特征，通过UEBA技术对响应体内容和登录跳转路径进行持续学习训练登录成功特征，并支持安全导出弱密码日志和脆弱性感知报告。 |
| 弱密码识别支持主动扫描，支持加密协议的弱口令登录检测，支持SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL等协议。 |
| 支持明文密码泄露行为检测，检测内容包含：登录账号IP、账号、密码、使用协议； |
| WEB服务器行为分析 | 支持非常用请求方法分析，展示源ip、目的ip、域名、访问链接、请求方法、状态码、最近访问时间等信息； |
| 支持可疑爬虫或扫描分析，能自定义web访问频率，且能设置源IP白名单。 |
| 支持后门上传利用分析，能展示受害ip、攻击ip、上传页面、后门链接、利用次数、最近发生时间等详细信息 |
| 数据库行为分析 | 支持对mysql、mssql、oracle、sybase等常见数据库高危操作行为分析，其能自定义规则 |
| 访问行为分析 | 支持外部访问分析，能展示源ip、资产ip、端口、协议、时间等详细信息，且能自定义源ip白名单 |
| 支持资产横向访问分析，能展示源资产ip、目的资产ip、端口、协议、时间等详细信息，需拥有国家互联网应急中心的应急服务支撑单位材料依据，且能自定义源ip白名单。 |
| 支持内部资产主机外联分析，能展示资产ip、外联ip、外联地域、端口、协议、时间等详细信息，且能自定义源ip白名单 |
| 支持风险端口访问分析，能自定义风险端口，且能自定义白名单 |
| 为保证我校行为分析的举证效果和准确性，实现挖矿、木马等用户风险行为快速定位，需要与我校本地专业上网行为审计设备进行对接，实现用户账号信息同步，支持上网提醒、冻结账号、查询账号，提升管理及溯源查询效率，以基于用户身份进行威胁管控 |
| 黑IP行为分析 | 支持通过云端威胁情报获取黑IP列表，与告警和日志进行匹配并生成告警，支持黑IP规则导入 |
| 响应处置狩猎 | 威胁狩猎分析 | 支持自动化溯源，可自动化复现受害者从最开始的遭受攻击到权限维持各个阶段的黑客行为，包括攻击入口溯源。支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息。 |
| 处置编排 | 支持工作流程自定义编排 |
| 支持全流量处置编排的联动服务管理，响应处置模块结合各类告警和日志进行攻防场景的深度分析，进行高价值告警和威胁溯源分析拓线，并将分析结果回注系统生成新的告警通过接口与安全组件处置联动，支持自动/手动方式的响应指令下发，实现对威胁事件的处置动作 |
| 威胁溯源 | 联动处置 | 处置中心的多个模块的安全事件内置多个处置策略模板，为保障我校安全处置效果及效率须对接学校校园安全基础设施（包括防火墙、终端安全响应系统、超融合内建安全）实现联动封锁、访问控制，完成终端安全响应系统联动一键查杀、进程取证，完成关闭超融合上的中毒虚拟主机，完成对超融合上中毒的虚拟主机进行快照，保证核心业务数据不丢失等功能。 |
| 处置记录策略管理 | 支持策略定义，可根据工作流进行处置动作定义，且能根据告警类型、攻击结果、威胁类别进行联动策略定义 |
| 支持编排处置日志记录，记录处置时间、受害ip、攻击ip、告警类型、威胁名称、域名、处置策略、告警来源等信息 |
| 网络日志检索 | 支持安全检测日志、审计日志、第三方日志存储；日志类型包括漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS攻击、邮件安全、文件安全、网络流量、DNS、HTTP、用户、数据库、文件审计、POP3、SMTP、IMAP、LDAP、FTP、Telnet等。 |
| 溯源举证 | 支持自动化溯源，可自动化复现校内受害者从最开始的遭受攻击到权限维持各个阶段的黑客行为，包括攻击入口溯源。支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息。支持攻击溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息 |
| 可视化展示 | 告警日志检索 | 支持告警日志检索，可基于时间、告警类型、文件MD5、文件名、文件传输方向、攻击方式、攻击结果、来源/目的所属国、IP地址、上下行负载等多字段混合搜索 |
| 终端日志检索 | 支持检索进程等动作的日志；可以及时发现终端上存在的异常现象，并可结合网络日志及告警日志深挖威胁的攻击全过程 |
| SIME检索 | 支持SIEM日志关联分析结果的可视化展示。并且内置关联规则对日志进行二次分析，分析结果可视化展示。包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等。 |
| 外部威胁态势 | 支持大屏展示网络攻击态势，包括整体网络风险指数、告警总数、攻击次数、攻击IP数、攻击源国家/地区TOP5、攻击态势，并支持自动翻转的攻击全景地图展示 |
| 大屏可视 | 为帮助我校充分展示安全建设效果，支持不同安全视角展示设备内置不少于16个独立的大屏展示功能，包括全网安全态势感知大屏、分支安全态势、安全事件态势、通报预警态势、资产态势大屏等，同时能满足多种场景的监控，比如日常运维、护网场景。支持对安全事件、外部攻击者、ATTCK能力图谱等维度进行自定义设置实现实时告警展示，支持大屏轮播，可在一个屏幕上自动切换轮播不同的大屏，所有大屏可自定义播放顺序。 |
| 威胁事件态势 | 支持大屏展示整体威胁事件态势，包括威胁类型分布、威胁类型TOP5、受害主机TOP5、威胁事件趋势、最新告警事件 |
| 资产风险态势 | 支持大屏展示整体资产风险态势，包含资产树结构、资产分类、开放服务统计、网段管理、资产风险趋势、资产风险状态 |
| 访问态势 | 支持大屏展示资产包括外部访问、横向访问、内网外联态势 |
| 安全服务 | 专家分析服务 | 支持与云端安全运营中心联动。设备能连接互联网时，安全专家在云端分析威胁；设备离线时，可将关键数据离线导出上传到云端安全运营中心，且需满足运行维护符合性ITSS二级的能力并要求材料依据支撑 |
| 响应工具 | 安全工具 | 为了全方位响应客户的需求，可通过威胁维基库、僵尸网络查杀工具、安全服务器分析等协助用户快速发现和解决安全问题。 |
| 资产管理 | 自动发现 | 支持自动从流量中识别资产信息包含：IP、端口、服务、操作系统、MAC  |
| 资产分组 | 支持对资产进行分组管理及对应内网网段的录入，系统自动根据用户录入的网段发现资产信息，同时支持根据分组过滤资产列表 |
| 资产标签 | 支持对资产打标签，同时支持根据标签过滤资产列表 |
| 资产列表 | 支持资产属性重新识别，当发现资产数据不准确时，可清空该资产属性，如主机名、备注、操作系统、标签、地理位置、硬件信息、应用软件信息、账号信息、责任人信息、端口信息等，重新发起识别后，平台会自动补齐资产属性，可批量操作。 |
| 资产探测 | 为了帮助我校便捷管理信息化资产及发现影子资产，提升资产风险管理能力，支持通过主动发送微量包的扫描方式探测潜在的服务器（影子资产）以及学习服务器的基础信息，资产指纹信息包括资产类型、端口、操作系统、MAC地址、主机名等。 |
| 资产互访 | 支持展示资产及资产分组之间互访信息，信息包括：互访协议、目的端口、互访次数 |
| 报表管理 | 报表导出 | 为了帮助管理员高效汇报，体现安全工作价值，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报告。并且可快速生成月度、季度、年度PPT报表，摘要报告支持PPT格式导出；包含网络安全整体解读、网络安全风险详情、告警及事件响应盘点等。 |
| 系统管理 | 配置核查 | 支持安全基线配置监测，可监测到开放了禁用端口、协议、属性变更等，已IP地址、MAC地址、所属租户和检测到时间来判断是否处置。 |
| 与威胁情报平台对接 | 支持230+情报源，DNS信誉库总量超过2000万，其中黑名单100万，URL信誉库总量超过1亿，其中URL分类库3000万，文件样本库总量超过10亿，每日新增200万。拥有国内领先的企业级域名信誉库，拥有丰富而准确的国内的URL分类库。支持威胁情报关联分析，内置威胁情报数量不少于170W。 |
| 集群部署 | 支持分析平台横向扩展至多台设备集群 |
| 学校化管理 | 支持自定义产品名称、产品logo |
| 运营管理 | 提供告警展示场景，支持展示场景的切换。每个告警展示场景中支持自定义页面数据展示的范围，方便管理人员的日常运维工作 |
| 联动管理 | 支持系统日志、告警日志、原始告警、行为分析信息发送给syslog服务器，支持系统日志、告警日志、行为分析信息发送给邮件服务器，支持将系统日志、告警日志、原始告警、资产配置、行为分析配置信息传输给KA\*\*A， |
| 安全组件联动 | 支持与安全组件进行联动，发现威胁事件后支持对攻击IP、恶意域名和受害资产的流量进行封禁 |
| 安全专项告警联动处置 | 支持文件、邮件、勒索、挖矿相关安全事件专项页面展示，且所有专项告警支持直接进行联动处置，联动处置支持自动调用内置处置策略模板，也支持自动化编排的自定义处置流程策略。支持根据自身业务和安全运维经验自定义告警/事件，以便提高告警的精确度，减少运维成本。 |
| 远程接入联动 | 与我校现网VPN系统进行对接，防止学校远程接入平台的用户账号及密码泄露导致恶意访问对我校业务造成连续性影响，及时准确定位出恶意访问账号，现网VPN对接协议由我校提供API接口文档，需提供详细对接方案 |
| 安全性管理 | 支持多次登录失败锁定账号和超时登陆配置 |
| 支持数据传输加密，确保数据传输的安全性 |
| 级联管理邮件告警 | 支持自定义WEB访问端口 |
| 支持邮件告警功能，可以定时向指定邮箱发送安全事件、攻击利用、恶意软件、拒绝服务等类型的告警信息 |
| 支持二级级联部署，下级分析平台向上级分析平台发送告警和相关信息，在上级分析平台上进行汇总展示 |
| 日志备份 | 支持对日志进行导出备份以及导入恢复 |
| 用户管理 | 可根据用户角色对用户进行区分，赋予不同角色用户不同的操作权限（系统管理员、操作员、审计员） |
| 访问白名单 | 支持配置平台访问白名单 |
| 规则管理 | 支持威胁情报、白名单、弱口令字典、暴力破解规则、漏洞知识库，支持用户新建规则信息 |
| 设备监控 | 支持查看本级设备及连接设备的状态信息 |
| 重保模式 | 重保任务 | 因校方有重保任务，为确保校方有效完成重保任务，所以该设备必须支持重保模式，在设备模式上有重保模式模块，模块可开启，具备实战化攻防中心，支持备战阶段的对外服务器外网暴露面分析、内网服务器暴露面梳理。实战阶段的实时攻击分析，实时展受害者IP、攻击者IP、XFF、攻击结果、攻击次数、威胁类型、威胁等级、状态码等20个以上类型。实战阶段的全过程可视溯源分析可以查看攻击者画像，包括攻击概览、攻击统计趋势、攻击详情等信息。 |
| 产品销售许可 | 要求计算机信息系统安全专用产品的销售许可 |
| 服务 | 承诺签订合同时提供五年原厂商质保服务承诺函及授权书。 |

4.1.2全流量威胁发现模块（分析探针）功能参数

|  |  |
| --- | --- |
| 功能类别 | 招标要求 |
| 硬件规格 | 标准2U设备；≥2\*GE流量监听电口；≥2\*10GE流量监听光口；≥2\*GE管理电口；≥2\*USB接口；≥2\*GE千兆接口；冗余电源； |
| 存储容量：≥4TB SATA数据硬盘； |
| 流量吞吐：≥8Gbps |
| 流量采集 | 网络协议 | 支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs等 |
| 文件协议 | 支持对流量中出现文件传输行为进行发现和还原，并记录文件MD5发送至分析设备，如可执行文件（EXE、DLL、OCX、SYS、COM、apk等）、压缩格式文件（RAR、ZIP、GZ、7Z等）、文档类型文件（word、excel、pdf、rtf、ppt等） |
| 数据库协议 | 支持常见数据库协议的识别或还原：DB2、Oracle、SQL Server、MySQL、PostgreSQL等协议 |
| 会话流量 | 支持双向会话检测机制、语义分析检测技术、智能分析引擎。 |
| 自定义协议 | 支持自定义协议和端口，满足特殊场景下的流量抓取 |
| 日志传输 | 为适应我校不同时期带宽占用和安全级别的场景需求，须至少支持5种类型日志传输模式,包含标准模式（占用带宽中等、安全等级中等）、精简模式（占用带宽小、安全等级低）、高级模式（占用带宽大、安全等级高）、局域网模式（横向访问检测）、自定义模式 |
| 威胁检测 | 威胁情报 | 1、安全规则库：支持WEB应用防护识别库、IPS漏洞利用检测识别库、实时漏洞分析识别库、黑客工具检测识别库，且具备自定义的web防护识别库、漏洞利用检测检测引擎。2、具备安全检测特征识别库、安全知识库、IOC威胁情报库、热点事件库、文件智能分析模型库检测能力。 |
| Web攻击检测 | 支持检测针对WEB应用的攻击，如SQL注入、XSS、系统配置等注入型攻击； |
| 支持跨站请求伪造CSRF攻击检测； |
| 支持其他类型的WEB攻击，如目录遍历、弱口令、权限绕过、信息泄露、文件包含、文件写入攻击等检测 |
| Webshell攻击检测 | 支持基于工具特征的WEBSHELL检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：冰蝎、中国菜刀、小马上传工具、小马生成器等 |
| 支持基于Webshell函数的攻击检测，如文件包含漏洞、任意文件写入、任意目录读取、任意文件包含、preg\_replace代码执行等 |
| 支持基于代理程序的攻击检测，如TCP代理程序、HTTP代理程序等 |
| 网络攻击检测 | 支持多种攻击检测，能更全面的从流量中发现威胁，如：协议异常、网络欺骗、黑市攻击、代码执行等 |
| 策略配置 | 文件还原 | 支持对HTTP、FTP\_DATA、SMB、SMTP、POP3、WEBMAIL、IMAP、TFTP、QQ、NFS等类型协议的流量进行文件还原 |
| 抓包分析 | 支持通过设备对流量进行抓包分析，可定义抓包流量双向或单向、数量、IP地址、端口或协议类型 |
| 语义分析 | 支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力 |
| 敏感信息检测 | 为保证我校师生个人信息数据安全和数字化资产的数据安全，须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 |
| 自定义弱口令 | 支持自定义弱口令字典，支持HTTP、HTTPS、Telnet、FTP、POP、SMTP、IMAP等协议的自定义弱口令检测 |
| HTTPS威胁检测 | 支持旁路HTTPS解密、威胁检测 |
| 高级参数 | web端提供针对恶意扫描、Flood攻击、IP碎片攻击、ARPSpoof、PingSweep等检测策略配置功能。 |
| 管理功能 | 部署模式 | 支持旁路部署，可同时接入多个镜像口，每个镜像口相互独立不影响 |
| 系统配置 | 支持数据传输加密，确保数据传输的安全性 |
| 支持威胁告警信息发送给syslog服务器，支持将威胁告警、威胁等级、网络日志、攻击结果、威胁类型等日志传输给KA\*\*A、威胁分析平台。 |
| 支持与集中管理平台进行联动，统一进行情报、规则的升级。 |
| 服务 | 签订合同时提供五年原厂商质保服务承诺函及授权书。 |
| 产品兼容性要求 | 为保证主库漏洞兼容性，要求威胁分析模块通过中国信息安全测评中心CNNVD兼容性检测 |

**4.1.3安全配套服务**

为确保配套服务质量，提升学校的网络安全保障能力，安全配套服务需由设备原厂商提供服务，即与高级威胁监测安全系统为同一厂商，安全服务人员均为设备原厂商提供经相关安全专业认证的人员。提供安全运营分析，弱口令扫描与处置，漏洞扫描与处置，渗透测试与处置，基线检查与处置，网络安全架构评估，Webshell后门检测与处置，安全情报推送的配套服务，其中提供的安全配套服务，均需进行问题排查，跟踪，处置，解决，并提供报告。

服务团队项目经理需拥有丰富的信息安全行业从业经验，且拥有丰富的项目管理经验和网络安全攻防实战能力，信息安全工作从业多年，要求全日制本科信息安全专业。

**4.1.3.1安全运营分析**

近几年针对教育行业典型网络安全问题中较突出的是勒索病毒事件、挖矿木马事件、弱口令、应用系统常规漏洞过多、安全设备/系统自身安全性不够、内网分层分域不精细，安全隔离措施不强等问题。故本次结合学校的常见网络安全问题，在进行安全防护措施补齐的基础上，配套7\*24小时安全运营分析。

安全运营分析提供全天候威胁事件持续发现及处理，提供7\*24威胁事件检测响应能力，快速识别APT攻击、勒索病毒、远控木马、挖矿木马、Web攻击等日常高频威胁事件，将最新的威胁情报结合学校实际流量状况，业务应用，得出精准的威胁分析结果，使学校尽早发现问题、解决问题。

**服务内容**

|  |  |
| --- | --- |
| 服务内容 | 说明 |
| APT告警深度分析 | 人工确认APT告警，对受害ip的流量行为、资产特性、时间节点、学校性质和APT组织进行关联分析，排查告警产生原因、攻击路径和影响范围，并给出处置建议。 |
| 普通IOC告警分析 | 人工确认告警，对受害IP与远控端的流量进行分析，并给出处置建议。 |
| 传感器漏洞分析 | 分析传感器的Webshell上传告警、网页漏洞告警和网络攻击告警，确认入侵成功事件、排查影响访问并给出处置建议；聚合传感器的攻击数据，梳理出高威胁IP。为确保漏洞分析质量，安全运营分析人员需拥有较强的漏洞挖掘实力。 |
| 爆破行为分析 | 分析ftp、smb、oracle、mysql、mssql、ssh、postgresql、pop3、smtp等协议的登录失败行为进行分析，提取发起爆破行为的IP，并确认是否爆破成功。 |
| 网站后门分析 | 深入分析网络流量，发现网络中存在的网站后门，溯源分析、行为分析、影响分析并给出处置建议。 |
| 数据库安全分析 | 深入分析数据系统登录行为、高风险数据操作语句，发现数据库系统异常登录、sql注入漏洞和系统命令执行等。 |
| 邮件安全分析 | 深入分析邮件系统的登录行为，恶意邮件投递行为。 |

**服务价值**

通过安全运营平台提供7\*24威胁事件检测响应能力，快速识别APT攻击、勒索病毒、远控木马、挖矿木马、Web攻击等日常高频威胁事件，适用于日常运营、HW及红蓝对抗、重保等不同应用场景。

提供专业的威胁处置服务及整改建议，并完成威胁事件的闭环处置工作，从而缩短安全事件的平均检测时间（MTTD）和平均响应时间（MTTR）。

**服务方法**

通过现场与远程2种方式结合提供：

现场服务 – 安全分析工程师应按照学校实际需求，到学校现场进行分析，在学校允许的管理终端上通过Web方式连接高级威胁监测安全系统，完成部分分析工作，其他分析工作需通过工具标本方式、以及人工分析方式在学校现场完成，如在现场发现高危告警事件，在授权的情况下可进行验证，编制报告并提交学校，并解决问题。

远程服务 – 后端远程提供7\*24威胁事件检测响应能力，安全分析工程师通过远程方式接入高级威胁监测安全系统，提取安全分析所需基础数据，在云端运营中心进行安全分析，编制报告并推送学校，并解决问题。

**闭环处置**

根据对学校7\*24威胁事件监测及安全运营分析发现的安全威胁，提供对应的安全威胁整改服务并进行持续威胁跟踪，同时出具《安全运营分析解决报告》。对部分不具备整改条件的，需解释原因并得到用户同意认可后方可结束处置流程。

**服务频率**

针对学校提供7\*24威胁事件检测及安全运营分析，由设备原厂商提供五年安全运营分析服务。

**交付成果**

《安全运营分析解决报告》

《安全运营巡检报告》

**4.1.3.2弱口令扫描****与处置**

**服务内容**

以口令为切入点检查身份认证安全方法主要包括：

口令强度检查；

认证过程网络数据加密算法检查；

口令存储方式检查；

口令策略配置检查。

在服务工作中，设备原厂商通过专业的漏扫设备并结合其他第三方工具，比较快速的进行全端口扫描（0-65535），进而进行弱口令猜测扫描。扫描过程包括：1、全端口扫描；2、服务确认；3、弱口令测试；4、推进整改； 5、复测结果； 6、持续跟进。

具体检查网络协议包括但不仅限以下：SSH、RDP、SMB、SQL Server、FTP、Telnet、SMTP、Oracle。

**闭环处置**

根据对学校弱口令扫描的安全问题，提供对应的弱口令整改服务并进行持续问题跟踪，同时出具《弱口令测试跟踪解决报告》。对部分不具备整改条件的，需解释原因并得到用户同意认可后方可结束处置流程。

**服务频率**

针对学校所有业务系统和网站，由设备原厂商提供不少于每两个月1次（2年，共12次）的弱口令扫描与处置服务。

此外针对新上线的业务系统（按IP地址数量核算），由学校指定服务时间，提供两年内不少于60个IP地址弱口令扫描与处置服务。

**交付成果**

交付物资料包括不限于如下内容：

《弱口令测试报告》

《弱口令测试复核报告》

《弱口令测试跟踪解决报告》

**4.1.3.3漏洞扫描与处置**

**服务方法**

漏洞扫描评估主要依靠带有安全漏洞知识库的网络安全扫描工具对信息资产进行安全扫描，并需由设备原厂商提供漏洞扫描与处置服务，厂商需具备较强的漏洞挖掘能力，投标方案中需说明厂商近3年向国家信息安全漏洞库的漏洞共享能力情况，且要求漏洞共享个数不少于10000个。漏洞扫描评估是能对被评估目标进行覆盖面广泛的安全漏洞查找，能够真实、全面地反映主机系统、网络设备、应用系统所存在的网络安全问题和面临的网络安全威胁。

**服务流程**



并根据以上流程，提供二次复测漏洞扫描，以及复测漏洞扫描结果的跟踪，复测漏洞处置的解决。

**服务内容**

| 检测内容 | 目标 | 范围 |
| --- | --- | --- |
| 网站系统漏洞检测 | 对信息系统中指定网页范围进行信息系统高危脚本漏洞检测验证，包括SQL注入、XSS攻击、恶意执行逻辑错误等典型脚本漏洞信息。 | 应用组件: APACHE |
| 应用组件: IIS |
| 应用组件: TOMCAT |
| 脚本语言：ASP |
| 脚本语言：PHP |
| 脚本语言：JSP  |

**闭环处置**

根据对学校漏洞扫描发现的安全问题，提供对应的漏洞整改服务并进行持续问题跟踪，同时出具《漏洞修复结果跟踪表》《漏洞复测修复结果跟踪表》《漏洞扫描总解决汇报表》。对部分不具备整改条件的，需解释原因并得到用户同意认可后方可结束处置流程。

**服务工具要求**

1、漏洞扫描工具需具备对 DNS 服务的安全漏洞检查能力,包括 DNS 缓存中毒、DNS 拒绝服务漏洞、签名欺骗等至少 100 种以上的相关漏洞库。

2、漏洞扫描工具需具备对 iOS、Android、Blackberry、windowsphone 等操作系统的扫描能力,并提供至少 50 种以上的相关漏洞库。

3、漏洞扫描工具需具备对后门检测的安全漏洞检查,包括对 Microsoft IIS 特洛伊木马检测、Mac OS X 恶意程序等常见后门漏洞的安全检测并提供至少 100 种以上的相关漏洞库。

**服务频率**

针对学校所有的业务系统和网站，由设备原厂商提供不少于每两个月1次（2年，共12次）的漏洞扫描与处置服务。

此外针对新上线的业务系统（按IP地址数量核算），由学校指定服务时间，提供两年内不少于60个IP地址的漏洞扫描与处置服务。

**交付成果**

交付物资料包括不限于如下内容：

《XX系统漏洞安全扫描报告》

《漏洞修复结果跟踪表》

《XX系统复测报告》

《漏洞复测修复结果跟踪表》

《漏洞扫描总解决汇报表》

**4.1.3.4渗透测试与处置**

**服务方法**

针对网站及Web类系统模拟黑客攻击，发现应用层面可能存在的SQL 注入、XSS（跨站脚本）、CRLF 注入、目录遍历、文件包含、输入验证、认证、逻辑错误、Google Hacking、密码保护区域猜测、字典攻击、特定的错误页面检测、脆弱权限的目录、危险的 HTTP 方法（如：PUT、DELETE）、信息泄露、structs2漏洞、Cookie欺骗、源代码泄露、恶意网络地址转移、http响应头截断、备份文件遗留隐患等各类型已知安全漏洞和安全隐患。

**服务流程**

渗透测试服务将参考下列信息规范进行工作：

信息安全风险评估规范（GB/T 20984-2007）

信息安全管理实用规则（GB/T 19716-2005)(ISO/IEC 17799:2000)

信息系统安全风险评估实施指南

信息系统审计标准（ISACA）

OWASP OWASP\_Testing\_Guide\_v3

OWASP OWASP\_Development\_Guide\_2005

OWASP OWASP\_Top\_10\_2010\_Chinese\_V1.0

OWASP Mobile Security Project

且渗透测试服务主要分为五个阶段，包括测试前期准备阶段、信息收集阶段、测试阶段实施、复测阶段实施以及成果汇报阶段：



**服务内容**

|  |  |  |
| --- | --- | --- |
| 常规分类 | 检测工具 | 检测方式 |
| Web安全 | SQLMAP；IIS短文件名漏洞测试工具；bash远程命令执行测试工具等 | 利用 SQLMAP；IIS短文件名漏洞测试工具； bash远程命令执行测试工具等；对信息泄露，SQL注入；第三方组件安全；命令执行；代码执行等系统漏洞进行渗透测试服务；并进行修改以及跟踪解决出现的问题，出具测试，跟踪，解决报告 |
| 业务逻辑安全 | burpsuite ； cookieedit； redis数据库连接工具 | 利用 burpsuite ； cookieedit； redis数据库连接等工具对会话，越权访问，未授权访问，验证码缺陷等进行渗透测试服务，并进行修改以及跟踪解决出现的问题，出具相关测试，跟踪，解决报告 |
| 中间件安全 | dex9jar 、dex2jar、 dex11jar等工具 | 利用dex9jar 、dex2jar、 dex11jar等工具进行中间件配置；反序列化命令执行；远程代码执行；文件解析代码执行等进行渗透测试服务，并进行修改以及跟踪解决出现的问题，出具测试，跟踪，解决相关报告。 |
| 服务器安全 | jd-gui、jadx 、enjarify 、Apktool | 利用jd-gui、jadx 、enjarify 、Apktool等工具进行应用防护软硬件缺陷，已存在的脚本木马；域传输漏洞；服务器未授权访问等问题进行渗透测试服务，并进行修改以及跟踪解决出现的问题，出具测试，跟踪，解决相关报告 |

**闭环处置**

根据对学校渗透测试发现的安全威胁，提供对应的安全威胁整改服务并进行持续问题跟踪，同时出具《渗透测试解决情况表》。对部分不具备整改条件的，需解释原因并得到用户同意认可后方可结束处置流程。

**服务工具要求**

1、可实现自动化渗透测试,贯穿整个渗透过程的操作,包括信息收集、指纹管理、漏洞发现、漏洞利用、后渗透攻击等模块。

2、可以根据可编程平台提供的接口编写自己的攻击插件,实现自定义的攻击需求。

3、可利用 http 协议、DNS 协议等远程获取外带数据;可通过内置的方法反弹交互 shell 到平台,执行 vim、交互执行操作等功能。

**服务频率**

由设备原厂商提供两年内不少于30个域名（站群按照一个域名来核算）的渗透测试服务。

**交付成果**

交付物资料包括不限于如下内容：

《XX渗透测试报告》

《漏洞修复跟踪表》

《XX渗透测试复测报告》

《渗透测试解决情况表》

**4.1.3.5基线检查与处置**

基础环境评估是在系统部署阶段通过安全基线检查工作，发现各类服务器、网络设备、安全设备等IT设备自身存在的安全漏洞和薄弱环节，并对发现的脆弱性进行识别、分析、修补、检验，消除、降低IT设备的高、中风险隐患，防范安全事件发生，避免信息系统脆弱性被非法利用，增强信息系统安全防范能力，保障业务的可持续性。

**服务内容**

**1）操作系统**

针对WINDOWS、LINUX、UNIX、AIX、HP-UNIX等操作系统进行系统配置的人工检查，尽量减少服务器因操作系统设置不当生的安全弱点，提升服务器自身的抗攻击能力，并根据应用系统的不同情况，提供定制式安全策略建议，使操作系统的安全级别达到理想化状态。

**2）数据库**

针对mysql、SQLServer、ORACLE、INFORMIX、PostgreSQL等数据库进行系统配置的人工检查，尽量减少数据库系统因配置不当产生的安全弱点，提升数据库系统的安全性。

|  |  |
| --- | --- |
| 检查方式 | 内容 |
| 数据库人工检查内容 | 帐号安全 |
| 数据库连接安全 |
| 数据库安全组件配置 |
| 日志配置 |
| 通信协议 |
| 设备其他安全要求 |

**3）Web服务器、中间件人工检查内容**

针对IIS、TOMCAT、WEBLOGIC、Apache、Jboss 的Web服务器、中间件进行配置人工检查，利用系统自身的安全功能提高Web服务器、中间件的安全性。

|  |  |
| --- | --- |
| 检查方式 | 内容 |
| Web服务器、中间件人工检查内容 | 管理应用限制检查 |
| 列出目录检查 |
| 禁止访问Web目录之外的任何文件 |
| http请求的消息主体的大小 |
| 默认端口 |
| 错误页面重定向 |
| 禁止列表显示文件 |
| 防范拒绝服务攻击 |
| 缺省安装的无用文件 |
| 版本号及其它敏感信息的隐藏 |
| 账号管理，认证授权 |
| 日志配置 |
| 通信协议 |
| 设备其他安全要求 |

**服务流程**

安全基线检查服务通过“自动化工具+人工检查”方式来完成。自动化工作目前主要有安全基线检查系统或检查脚本工具两种方式。安全基线检查系统通过远程登录检查的方式工作，可以完成绝大部分设备的检查。但针对物理隔离或网络隔离的设备就需要使用检查脚本工具方式来补充完成检查工作。

人工检查主要参考安全基线检查来进行人工的检查，主要包括网络设备安全配置基线、安全设备安全配置基线、操作系统安全配置基线、数据库安全配置基线、中间件安全配置基线等。

通过以上两种模式形成检查报告，并配合学校，针对域名基线检查结果进行相关的跟踪，以及解决出现的问题，并最终汇总成一个解决报告提供学校。



**闭环处置**

根据对学校基线检查发现的安全问题，提供对应的安全问题整改服务并进行持续问题跟踪，同时出具《XX信息系统基线检查解决记录表》。对部分不具备整改条件的，需解释原因并得到用户同意认可后方可结束处置流程。

**服务频率**

针对学校所有的业务系统和网站，由设备原厂商提供不少于每两个月1次（2年，共12次）的基线检查与处置服务。

此外针对新上线的业务系统（按域名数量核算），由学校指定服务时间，提供两年内不少于60个域名的基线检查与处置服务。

**交付成果**

交付物资料包括不限于如下内容：

《XX信息系统的登录信息汇总表》

《XX信息系统基线检查报告》

《XX信息系统基线检查差距分析表》

《XX信息系统基线检查解决记录表》

**4.1.3.6网络安全架构评估**

**服务内容**

安全技术评估主要从攻防角度针对网络层的风险点进行全面评估，并提供相应的评估报告和整改意见。安全技术评估内容包括：网络层（网络架构、边界安全、通信安全、策略安全等）。

在资产及应用发现的基础上，安全专家对每个业务梳理分析，依据信息系统实际情况、业务特点、资产重要度等信息，结合信息安全的最佳实践进行归纳，最终针对性地形成学校专属的资产画像，构建起学校专属的信息安全资产画像。资产画像构建完成后可根据域名、IP、端口、中间件、应用、技术架构、变更状态、业务类型（自定义）等条件对资产进行查询、统计，并能对资产进行周期变化监控。

**服务流程**

本项服务流程应包括1、确定调研内容2、确定调研对象3、安全评估 4、评估结果报告 5、针对评估问题如何解决。

**服务内容**

| 序号 | 评估指标 | 评估方法 |
| --- | --- | --- |
| 1 | 结构安全 | 检查网络拓扑情况、核查核心交换机、路由器，评估分析网络架构与网段划分、隔离等情况的合理性和有效性。 |
| 2 | 访问控制 | 检查防火墙等网络访问控制设备，测试系统对外暴露安全漏洞情况等，评估分析信息系统对网络区域边界相关的网络隔离与访问控制能力；检查拨号接入路由器，评估分析信息系统远程拨号访问控制规则的合理性和安全性。 |
| 3 | 安全审计 | 检查核心交换机、路由器等网络互联设备的安全审计情况等，评估分析信息系统审计配置和审计记录保护情况。 |
| 4 | 边界完整性检查 | 检查边界完整性检查设备,接入边界完整性检查设备进行测试等过程，评估分析信息系统私自联到外部网络的行为。 |
| 5 | 入侵防范 | 评估分析信息系统对攻击行为的识别和处理情况。 |
| 6 | 恶意代码防范 | 检查网络防恶意代码产品等过程，评估分析信息系统网络边界和核心网段对病毒等恶意代码的防护情况。 |
| 7 | 网络设备防护 | 检查交换机、路由器等网络互联设备以及防火墙等网络安全设备，查看它们的安全配置情况，包括身份鉴别、登录失败处理、限制非法登录和登录连接超时等，考察网络设备自身的安全防范情况。 |

**闭环处置**

根据对学校网络安全架构评估中所检查发现的问题，提供对应的整改服务并进行持续跟踪，同时出具《XXX网络安全调研评估跟踪问题解决报告》。对部分不具备整改条件的，需解释原因并得到用户同意认可后方可结束处置流程。

**交付成果**

交付物资料包括不限于如下内容：

《XXX网络安全调研评估调研表》

《XXX网络安全调研评估报告》

《XXX网络安全调研评估跟踪问题解决报告》

**服务频率**

由设备原厂商提供不少于每年1次（2年，共2次）的网络安全架构评估。

**4.1.3.7Webshell后门检测与处置**

**服务介绍**

通过专业的威胁检测设备，查找分析服务器有无异常代码、异常进程、异常网络流量、异常用户、异常登录或操作日志等，从相关的日志和应用后门程序检测等方面进行审查，从而对应用系统是否存在木马等恶意程序、是否被远程控制、是否被窃取信息等进行检测，发现安全隐患。

**服务内容**

专项检测操作系统、应用的木马、rootkit、Webshell等后门，有效拦截未知Webshell并及时发现网站程序中存在的漏洞，并对利用漏洞进行的攻击进行防护。包含已知Webshell自动隔离、未知Webshell实时防护、SQL注入漏洞防护、文件上传漏洞防护、Struts2漏洞防护、反序列化漏洞防护等。

**闭环处置**

根据对学校Webshell后门检测中发现的安全问题，提供对应的安全问题整改服务并进行持续问题跟踪，同时出具《Webshell后门跟踪解决报告》。

**交付成果**

交付物资料包括不限于如下内容：

《Webshell后门检测报告》

《Webshell后门复测报告》

《Webshell后门跟踪解决报告》

**服务频率**

针对学校所有的业务系统和网站，由设备原厂商提供不少于每两个月1次（2年，共12次）的Webshell后门检测与处置服务。

此外针对新上线的业务系统（按IP地址数量核算），由学校指定服务时间，提供两年内不少于10个IP地址的Webshell后门检测与处置服务。

**4.1.3.8**安全情报推送

**服务内容及方法**

通过推送实时的高危漏洞预警和每周安全热点资讯，提出最新安全防护观点，同时通过月度安全通告为我方汇总月度的高危漏洞、安全热点，威胁情报解读精华及漏洞分析统计，提供有价值的网络安全态势推送。

**交付成果**

交付物资料包括不限于如下内容：

《XXXX漏洞预警安全预警通告》

《安全热点周报》

《月度安全通告》

**服务频率**

由设备原厂商提供两年内不少于15次安全情报推送。

**4.2.现场安全应急响应**

**4.2.1服务介绍**

为确保学校在遇到突发信息安全破坏事件（篡改、泄露、窃取、丢失等）、大规模病毒事件、网站漏洞事件等信息安全事件时，学校能够迅速有效地从安全事件中恢复过来，并将信息丢失和被盗以及服务被破坏的程度降到最低。

现场安全应急响应需由设备原厂商提供服务，现场安全应急响应人员需为设备原厂商正式任职员工，需提供社保缴纳材料依据。由于现场应急响应服务及处置对服务人员的专业性要求极高，现场安全应急响应人员需具备足够的应急响应服务能力。

**4.2.2服务内容**

应急响应服务通过在遇到突发安全事件后采取专业的安全措施和行动，并对已经发生的安全事件进行监控、分析、协调、处理、保护资产等安全属性的工作。以达到第一时间采取紧急措施，恢复学校业务正常运行，追踪失陷原因并提供可行性建议，避免同类安全事件再次发生的目的。保障我方网络安全，最大程度的减少安全事件给我方所带来的经济损失以及恶劣的社会负面影响。

应急响应处置步骤应包括：

1、准备阶段

准备阶段主要完成安全事件预判、应急响应工作方案制定、人员物资到位等工作，为后续应急响应工作的顺利进行提供决策性依据，快速定位并解决问题，减少学校损失。

2、检测阶段

检测阶段主要完成现场排查分析、制定响应策略等工作，通过对现场安全事件情况进行排查分析，确定安全事件类型，评估安全事件可能产生的影响，并针对事件制定详细的应急响应策略。

3、抑制阶段

抑制阶段主要完成抑制方案的制定与实施等工作，现场应急专家及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏，并确保封锁方法对涉及相关业务影响最小。

4、根除阶段

根除阶段则主要完成根除方案制定、实施以及效果判定等工作，根据事件抑制情况以及有关事件或行为的分析结果，找出事件根源，明确相应的补救措施并彻底清除。

5、恢复阶段

恢复阶段主要根据抑制阶段和根除阶段情况，选择合适的系统恢复方案对学校系统进行恢复。

总结阶段

6、总结阶段主要完成应急响应事件报告输出工作，现场应急专家通过对以上各阶段处理过程进行记录总结，并整理与事件相关信息及时反馈给学校。

**4.2.3服务流程**

1、远程支持：提供7\*24小时电话应急响应服务，5分钟内响应并提供远程技术支持（远程支持不计入现场安全应急响应服务次数）；

2、现场支持：远程无法解决的需1小时到达现场，协助校方降低事件影响，并针对引发事件的原因提供解决建议。应急响应完成后提供相关服务报告。

**4.2.4服务频率**

由设备原厂商提供两年内不少于10次现场安全应急响应服务。

**4.2.5**交付成果

工作输出

服务成果为：

安全事件处置完成，系统得到恢复。

找到安全事件发生原因并提供安全解决方案。

《XX系统（事件）应急响应报告》

《应急响应服务确认单》

**4.3现场重保值守服务**

**4.3.1服务介绍**

为应对日益严峻复杂的网络安全形势，学校需承担起护航亚运会、迎接二十大的重要责任，为全面提高学校网络安全突发事件综合应对能力，本次项目配套现场重保值守服务，在重要时期及活动（亚运会、二十大、国庆等）期间，安排专业工程师对重要信息系统（网站）提供值守、监测预警等服务，确保重要时期学校关键信息系统和数据资产安全，保障有事件无事故。

重保服务整体工作分成备战阶段服务、临战阶段服务、决战阶段服务三个阶段服务，其中备战阶段服务、临战阶段服务是在重大活动或者会议开始前为安全保障工作做准备，主要负责重保期间队伍组建、重保方案设计、重保单位安全检查等工作；决战阶段服务是为重大活动或者会议过程中安全保障工作提供技术支撑，主要负责重保期间各重要单位网络安全的监测、应急值守、应急处突、攻防演习等工作，并应该具备相关重保各大问题事件的完整处置流程的解决方案。现场重保值守服务需由设备原厂商提供服务，现场重保值守人员需为设备原厂商正式任职员工，需拥有社保缴纳材料依据。

**4.3.2服务流程**

重保工作内容包括：

1.安全监测

重保决战期间，为了及时掌握重保重要信息系统运行情况，降低因安全问题而造成的负面影响，可对重保重要信息系统进行多方位的安全监测工作，以便能够及时发现并处理系统存在的安全问题，防止事态的蔓延。安全监测工作是由具备丰富攻防实战经验和信息安全工作经验的专业人员提供，应配备有国家认可的注册信息安全专业人员开展相应的服务，投标时需提供相应人员的能力凭证且投标时提供的重保值守人员与实际到场的服务人员必须一致，到场服务时需提供身份证明。服务人员通过网站安全监测，全流量威胁监测两方面工作来开展。

2.安全值守

根据各重保重要单位值守需求情况，在重保决战阶段，需配备由项目管理专业人士（投标时需提供人员能力凭证）对安全服务人员进行重保工作安排。协助各单位运维值守人员，在现场进行5×8安全值守。主要通过现场监测，定期巡检，排障处理，事件上报，应急处置，监督整改等方面工作来保障值守单位信息系统的安全运行。

3.应急处突

重保决战期间应急处突小组应进行现场值守待命，需配备由IT服务管理专业人员、零信任安全专家负责所有突发安全事件的处置工作，投标时需提供相应人员的能力凭证且投标时提供的应急处置人员与实际到场的服务人员必须一致，到场服务时需提供身份证明。发生突发安全事件后，由专家团队和相关重保单位领导现场立即组织分析并作出决策，下发应急处置任务，重保领导协调技术人员开展应急处置；应急处突小组接到应急处置任务立即赶赴现场配合重保重要单位进行应急处置。

4.总结与报告

重保活动结束后，应该召集参与重保工作的各类人员，对重保工作全过程的工作内容进行信息收集和经验报告总结，通过总结与报告工作，发现重保工作中还存在问题的地方，并提供相关问题解决方案，积累经验，为下一次的重保工作提供更有力的支撑。

**4.3.3服务频率**

由设备原厂商提供两年内不少于50人/天现场重保值守服务。

**4.3.4**交付成果

交付物资料包括不限于如下内容：

工作输入：《重要时期安全保障服务方案》

工作输出：《重要时期安全保障服务工作总结》；《重保阶段日报》

**4.4**网站云防护服务

由于网站云防护所需的工具需具有专业要求进行解析服务，所以本次项目需由设备原厂商服务团队提供，本次需提供不少于20个域名一年的网站安全云防护服务，将外部访问者访问学校网站的请求及网络流量通过DNS方式就近牵引到防护节点，在该节点进行相应的安全防护、流量清洗后将干净的流量发送到源站，源站再返回正确的值，完成整改访问、防护。需包含以下服务： Web攻击防护、 DDoS攻击共享型防护、高防DNS服务、网站缓存加速。

4.4.1网站安全防护

1) Web漏洞攻击防护

通过部署云端网站安全防护系统对Web攻击进行拦截，防止数据库被拖库、网页被恶意篡改、网站被挂马、被挂链接、网站敏感信息泄露等网站安事件的发生。

2) 抗拒绝服务

DDoS攻击防护：通过云端防护的方式对DDoS攻击进行防护，防止攻击者通过使用工具或僵尸网络对网站发动SYN Flood攻击、TCP Flood攻击、ICMP Flood攻击、UDP Flood攻击、Smurf 攻击、Land攻击等大流量的攻击方式，堵死用户网站出口带宽，导致网站服务器无法对外提供服务。

CC攻击防护：通过本地或云端方式防止黑客通过CC攻击的方式对网站服务器的应用层资源进行消耗而导致网站拒绝服务。

高防DNS：通过云端接管DNS域名服务商的网站域名解析权限，提供高防DNS能力，防止域名服务商无法抵御DNS攻击而导致网站域名无法正常解析。

3) 威胁情报

需要对僵尸网络IP地址、攻击IP地址、网吧等高风险场合IP、扫描IP地址等恶意IP地址的访问或攻击进行有效阻断。

**4.4.2网站安全加速**

针对静态资源：HTML、JS、CSS、图片等资源进行加速。通过遍布全国的CDN节点，对这类资源缓存，当访问者访问源站时，就近节点可获取到所需的静态资源，无需再向源站去获取资源，提升访问速度，降低源站的带宽利用及源站服务器负载。

4.4.3网站安全管理

通过综合安全能力的提供，通过管理平台可统一管理WEB攻击防护、CC攻击防护、网站加速优化及设置、一键处置网站（一键关停服务）、攻击日志导出、报表管理及导出等管理功能。

4.4.4网站云防护工具技术需求

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 服务要求 | 提供不少于20个域名一年的网站安全云防护服务;包含以下服务： Web攻击防护、 DDoS攻击共享型防护；正常业务请求并发：1000QPS、提供移动端运维平台、包含非标准端口配置、一年售后服务、防护周期内的防护引擎、防护规则升级服务、7x24小时电话支持服务、产品远程技术支持：包含防护接入、防护过程中产品问题支持。 |
| 服务工具 | 提供云端防护账号交付，以 SaaS 的方式为用户提供网站安全防护服务（非硬件盒式WAF、非盒式抗DDoS攻击产品、非集成WAF及抗D功能的防火墙类产品，非虚拟机化WAF）。 |
| Web攻击防护 | 支持服务器隐身，使得黑客无法获取服务器真实IP地址，防止黑客对服务器的各种攻击。 |
| 支持HTTPS网站防护。 |
| 支持HTTP/HTTPS协议合规性检查，包括畸形报文、HTTP版本检查、报文头缺失、请求方法限制、协议违规等。 |
| 支持服务器敏感信息泄露防护，包括服务器类型信息、服务器版本信息、敏感路径信息泄露、网站源码泄露等。 |
| 应能识别和阻断SQL注入攻击、Cookie 注入攻击、命令注入、跨站脚本攻击、文件包含攻击、LDAP注入、XPATH注入、爬虫攻击、Struts2命令执行攻击等常见的WEB攻击。 |
| 支持ASP木马、JSP木马、PHP木马、一句话木马、菜刀工具等多种形式的WEB Shell后门的上传防护。 |
| 支持对Appscan、Awvs、Pangolin、Burpsuite、啊D、明小子、Nikto等扫描器的扫描防护。 |
| 支持细粒度的WEB防护配置，至少支持对24大类Web安全漏洞类型对设置白名单，当设置生效后，针对某URL的该类WEB攻击不在防护。 |
| DDoS攻击防护 | 支持对SYN Flood攻击、Frag Flood攻击、ACK Flood攻击、UDP Flood攻击、ICMP Flood攻击等常见的流量型DDOS攻击进行清洗。 |
| CC攻击防护 | 可以防护针对网站的CC攻击。 |
| 支持根据进入云平台流量大小来对攻击进行CC攻击判断，即攻击流量超出管理员配置流量阈值后，对攻击源进行HTTP协议验证、JS防御或图片验证防御。 |
| 支持配置强制缓存功能，当触发CC攻击防护时，可对用户自定义配置的URL按照选定的类型进行缓存，如样式、JS、图片、静态HTML、首页、多媒体文件、文档类型、压缩文件等，保证相关内容仍可正常对外访问。 |
| 支持根据源站总并发连接数和访问源单IP并发连接数对攻击进行CC判断，并发连接数超出管理员配置并发连接数阈值后，对攻击源进行自动防御、JS防御或图片验证防御。 |
| 支持根据服务器响应时间对访问源进行CC攻击判断，响应时间超出管理员配置响应时间阈值后，对攻击源进行JS防御或图片验证防御。 |
| 支持CC白名单功能，可针对IP、URL进行白名单配置。 |
| 支持User-Agent报名单，可针对User-Agent内容进行白名单配置。 |
| 爬虫攻击防护 | 搜索引擎（百度、谷歌、必应、360、搜狗、神马搜索）及恶意爬虫识别及防护；同时开启后即有默认防护配置（宽松/中等/严格）。支持针对URL做单独的爬虫防护配置。可使用威胁情报中心的威胁情报信息。 |
| 支持配置强制缓存功能，当触发爬虫攻击防护时，可对用户自定义配置的URL按照选定的类型进行缓存；如样式、JS、图片、静态HTML、首页、多媒体文件、文档类型、压缩文件等，保证相关内容仍可正常对外访问； |
| 敏感词过滤 | 支持内置完备的敏感词信息库，开启默认防护策略时，可主动监测网站首页有无敏感词，如果存在便产生告警 |
| 支持用户自定义URL、敏感词内容，细粒度的对响应方向进行检测，当响应内容包含自定义敏感信息时，则可对内容进行告警、替换\*、阻断和重定向动作 |
| 只读保护 | 可以提前通过爬虫缓存用户网站页面文件，在即使源站服务器出现WEB攻击、网页被篡改、服务器宕机、网络线路故障、网站服务异常等问题，依然可以通过缓存页面强制对外提供完整的静态缓存页面访问服务。 |
| 用户可以自定义镜像URL、非镜像URL、开始镜像时间等参数，同时可以格式化镜像数据。 |
| 访问控制 | 对在特定时间段内某IP地址或IP地址段是否能够访问特定URL进行访问控制。 |
| 对不同国家和中国的不同省市能否访问保护网站进行访问控制，并能够基于IP地址添加例外访问黑白名单。 |
| 对包含特定的 USER-Agent字段内容的访问进行访问控制。 |
| 对图片、音频、视频、压缩文件、可执行文件等内容进行防盗链访问控制。并允许设置IP地址段例外策略。 |
| 加速缓存 | 有全国性的节点机房，按照最小响应时间，最优访问服务等智能算法为用户自动选择节点机房，以提升用户访问效果。 |
| 日志报表 | 支持网站访问次数统计，访问IP数统计，PV数统计，漏洞攻击数统计、CC攻击数统计等攻击访问统计。 |
| 每个二级域名有独有的攻击访问统计报表。 |
| 支持WEB攻击统计报表，攻击统计报表，攻击URL TopN报表等。 |
| 支持WEB攻击报表，包括WEB攻击次数，攻击IP数，攻击者全国分布图，攻击IP TopN。 |
| WEB攻击日志至少包含攻击类型、攻击IP、IP归属地、攻击URL及参数，攻击次数等参数。 |
| 攻击报表包括攻击次数，攻击IP数，攻击者全国分布图显示，攻击IP TopN。 |
| 攻击日志至少包含攻击类型、攻击IP、IP归属地、攻击URL、攻击事件、攻击次数等参数。 |
| WEB访问日志至少包含访问时间、客户端IP：端口、域名、URL、目标IP：端口、源站IP:端口、请求方法等参数 |
| 支持流量对比报表，能直观的展示回源流量与加速流量的对比及回源次数和加速次数的对比。 |
| 安全报表 | 支持自定义时间段的报表功能，能直观的显示本周及历史周网站遭受的WEB攻击、攻击等攻击情况。 |
| 支持月度简报功能，能每月定时向指定邮箱发送月度简报，展示网站安全防护情况。 |
| 内容包括拦截漏洞数、本周遭受的攻击数、攻击次数最多的IP、受攻击最多的域名，WEB攻击的趋势报表、遭受的CC攻击的趋势报表，WEB攻击方式TopN、遭受CC攻击的URL TopN，WEB攻击源IP全国分布位置，CC攻击源全国分布位置等内容 |
| 支持WORD或PDF格式导出下载。 |
| 攻击告警 | 支持对Web攻击、CC攻击、爬虫攻击进行自定义攻击阈值告警。同时支持自定义统计周期、告警方式（邮件、短信）、告警接收人、告警接收组信息。支持将多个告警人添加为一个告警组，支持对同一告警组下所有告警人做相同告警配置。 |
| 大屏展示 | 提供网站攻击数据可视化展示，为用户提供网站攻击态势感知能力，包含：攻击类型占比、网站服务状态码占比、网站流量情况、防护TOP10排名、攻击记录、WEB攻击/CC攻击分析、攻击源国家等维度的展示。 |
| 一键关站 | 支持一键关闭外部对源站的访问，达到一键关站的效果，并可以指定关站响应码（301,302时可以指定跳转URL）或者制定响应页面，默认响应403。 |
| 多因子认证 | 支持登录账号的多因子认证，包含：密码、验证码、短信验证方式，确保登录安全。 |
| 三元用户管理 | 支持超级管理员、普通管理员、审计管理员等管理员角色。超级管理员可以创建其他所有管理员并拥有系统最高权限；普通注册管理员只可以查看并配置自己域名的权限；审计管理员智能审计配置及日志报表。 |
| 移动运维 | 支持移动端运维，支持与网关、端点安全设备的命令下发、以及结果反馈（包括但不限于一键封堵IP，一键断网，一键杀毒）。支持通过微信推送安全事件（包括但不限于黑链，WEBSHELL，僵尸网络）等功能。 |
| 产品销售许可 | 计算机信息系统安全专用产品销售许可证 |

**4.5网站云监测服务**

由于网站云监测所需的工具具有专业要求进行并可进行平台的配套监测服务，所以本次项目需由设备原厂商服务团队提供，本次需提供不少于20个域名一年网站云监测平台的使用权；并提供以下内容：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；提供不少于20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小时电话售后服务。

**4.5.1违规内容安全监测**

采用安全云平台上内容安全检测组件，对网站内容的自动化、持续检测，并发现问题实时告警，快速通知相关人员及时处置，保障互联网业务安全稳定运行，并以全程可视的方式让用户随时随地掌握安全状况。提供敏感词发现的技术手段，支持全站监测，可定位敏感词位置和内容，提供内容篡改的历史对比图。

**4.5.2网站黑链监测**

提供基于大数据支撑的黑词暗链发现技术手段，支持全站对于潜藏在页面深处的第三方黄赌毒广告类链接进行监测并告警，可定位源代码篡改的位置和内容。

**4.5.3网站可用性监测**

WEB服务可用性监测。支持华北、华东、华南、海外机房超过40个检测节点，确保电信、联通和移动都具备监测点；支持网站故障原因定位，不限于：响应连接被重置、连接超时、http状态码、连接被拒绝等；

可用性监测配置。可支持get/head/post三种方式对HTTP/HTTPS服务进行监控，监控频率支持自定义。支持对自定义的URL进行HTTP/HTTPS监控。支持对监测域名的IP协议栈情况进行实时识别，并且根据识别结果分别配置IPv4和IPv6的监测节点。支持在高级配置中，自定义监测节点，并且配置异常节点阈值和超时阈值。

**4.5.4网站挂马监测**

采用特征分析和沙箱行为分析技术对网站进行木马检测分析，实现快速、准确的发现和定位网页木马，确保用户在第一时间发现感染的木马并及时消除。对木马威胁进行报警、通知、处置管理。

**4.5.5网站漏洞扫描**

可以扫描以下漏洞：

|  |  |
| --- | --- |
| 漏洞类型 | 漏洞 |
| 认证和授权类 | 遍历数据、越权访问、文件上传、任意文件下载、任意文件读取等 |
| 命令执行类 | 远程命令执行、各类反序列化漏洞、文件包含等 |
| 注入攻击类 | SQL注入、XSS注入、XML注入、XPATH注入、CRLF注入、链接或框架注入等 |
| 服务端攻击类 | 应用服务未授权访问 |
| 信息泄漏类 | 版本管理软件信息泄漏、web服务器控制台地址或网站后台泄漏、phpinfo()信息泄漏、目录遍历、敏感信息泄漏、安装或测试文件未删除、cookie信息泄漏、心脏滴血漏洞等 |
| 其他 | 各类CMS漏洞（织梦、骑士、大汉等）、各类webserver/中间件漏洞、struts 2组件相关漏洞、IIS组件漏洞、服务端请求伪造（SSRF）、URL重定向、DNS域传送漏洞、HTTP Host头攻击等 |

**4.5.6网站云监测工具技术需求**

|  |  |  |
| --- | --- | --- |
| 指标大类 | 指标项 | 指标要求 |
| 服务要求 | 服务要求 | 提供不少于20个域名一年网站云监测平台的使用权；并提供以下内容：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；提供不少于20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小时电话售后服务。 |
| 服务工具 | SaaS平台 | 系统基于云架构，无需用户部署任何软硬件，通过账号可以直接进行管理。 |
| 监测节点 | 监测节点保障 | 为了保证监测服务质量，需要全国范围内具备至少10个云监测节点 |
| 监测能力 | 扫描深度 | 每日扫描网站一万个以上，扫描深度最高可达9880 |
| 资产管理 | 监测网站统计 | 最近一周告警趋势、待验证告警总数和各类型总数、已验证告警总数和各类型总数、待验证 高危告警数最多的资产信息；监测网站总数、当前账号监测网站总数、已知资产/未知资产数量及比率、已开启/未开启监测资产数量和比率；下发的通知数、尚未完成的通知数的统计。 |
| 监测资产列表展示 | 支持按照区域、行业、授权状态等维度展示资产列表；按照网站名称、负责人信息、负责人邮箱等信息搜索指定资产；直观查看被监测网站信息展示，需要包含以下信息：域名、所属账号、网站名称、所属单位、地区、行业、网站负责人、告警通知接收人、授权状态、监测状态 |
| 支持查看网站资产详情 | 可自动获取网站备案信息，需要包含以下信息：备案信息：主办单位 主办单位性质、网站备案号 、网站名称 、网站首页地址、审核日期 、注册信息、安全信息、页面快照注册信息：注册商 、域名服务器、责任人姓名、责任人邮箱、责任人电话安全信息：各类型告警数量统计、页面快照、网站IP地址列表、网站DNS列表 |
| 支持网站目录结构展示 | 支持展示网站目录结构， |
| 网站外链和坏链监测 | 支持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 |
| 支持资产管理 | 支持对于本单位所负责运营的资产，允许进行资产的新建、编辑以及删除工作。 |
| 支持IPv6网站资产监测 | 支持录入IPv6资产并进行进行漏洞扫描，网站黑链，违规内容，内容变更和网站挂马的监测。 |
| 支持新建资产 | 新建资产具体可支持域名、网站名称、机构名称、所属地域标识、行业分类等表示添加资产，同时支持资产的的批量导入。 |
| 未知资产识别 | 支持根据资产域名解析其子域名和关联ip，识别未知资产 |
| 一键资产监测开启 | 支持对于特定资产进行一键监测开启、一键监测关闭等操作 |
| 漏洞暴露面 | 热点漏洞情报预警 | 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客户 |
| 风险暴露面资产清单 | 支持列表展示最新漏洞情报关联的资产信息，提供资产预警能力 |
| 网站通知人管理 | 网站通知人管理 | 支持列表维护网站资产联系人信息，包括：联系人姓名、手机号码、邮箱、告警通知类型、威胁等级、风险暴露面通知、关联网站数量； |
| 支持新增通知人 |
| 支持批量添加通知人 |
| 支持手机和邮件接收告警信息 |
| 支持配置接收信息类型和等级 |
| 资产接收漏洞情报信息及暴露面资产信息 |
| 支持自定义邮件和短信接收频次，时间区间等； |
| 支持关联接收告警的网站范围 |
| 安全告警通知 | 安全告警状态分阶段展示 | 可按照验证、处理等2个阶段进行不同状态展示，方便详细了解安全告警所处状态，需包含以下安全状态：1、验证阶段：未验证、已确认2、处理阶段：待响应、待处理、已处理、已超时 |
| 安全告警搜索 | 支持按照区域、行业（省/地/县）、告警类型、安全等级、安全告警状态、关键字等多条件组合搜索功能 |
| 安全告警白名单 | 支持对告警加入白名单的功能，白名单的确定可根据告警的监测网站关键词、告警范围、告警类型、威胁等级等要素来制定。 |
| 通知告警查看 | 支持自动添加网站责任人信息、自定义通知转发对象功能；能够查看被通知的基本信息、安全告警列表。 |
| 提供通知处理过程的时间轴，并可追踪通知处理的全过程，可对相关人的处理行为进行记录。 |
| 通知状态查看 | 支持查看通知处理状态； |
| 支持查看通知总数、近一周新增加的通知数、已完成的通知数、未响应的通知数； |
| 通知和响应时间查看 | 支持查看通知对象的基本信息、通知下发的时间、通知响应的时间、通知处理的状态、通知详情。 |
| 短信、邮件通知 | 支持短信、邮件将通知发给网站负责人； |
| 快捷生成短URL分享链接，供被监管单位随时随地登陆通知进行处理； |
| 支持勿扰配置，可以按需设置接受通知的时间； |
| 告警自动通知 | 支持按照用户、资产、告警类型等维度配置自动通知； |
| 通知信息反馈 | 支持URL登陆查看通知，并支持快速转发通知，可跟踪告警处理进度、发表告警处理意见和与监管方互通信息。 |
| 监测报表管理 | 报表模板自定义 | 支持监测报表模板名称、报表展示周期、报表是否导出、报表导出类型等模块自定义。 |
| 报表详情展示 | 监测报表支持通过不同维度展示被监测网站状况，报表详情需包含以下内容：报表情况综述：包含针对统计对象的整体概述、统计周期内总体评估与建议；监测概览：该报表包含统计网站、页面数量，包含漏洞情报、网站挂马、可用性、违规内容等类型告警数量。安全威胁变化与评估：统计周期内与上一周期相比，新增安全告警、重复安全告警、已解决安全告警等变化状况；告警分布与趋势分析：告警分布地区、行业、类型等展示；网站漏洞、网站内容安全、网站稳定性、网站情报类告警分析等具体分析和展示；最新互联网安全资讯展示 |
| 报表查看 | 报表可按照设定周期自动生成、一键重新生成、一键删除。 |
| 支持报表以PDF、WORD等格式导出。 |
| 支持报表的在线查看。 |
| 用户管理 | 用户信息展示 | 支持显示用户账号、单位名称、所属区域、管理员类型、手机号、账号类别、所属母账号、账号有效期等信息的展示。 |
| 用户账号分级管理 | 支持多级账号管理，同级账号多角色管理，包含管理员、运维人员、普通运维人员； |
| 用户账号权限管理 | 支持母账号对子账号登录的一键切换；支持子账号的密码修改、账号新建 |
| 用户账号添加 | 支持对新建账号名称、单位类型、授权查看类型、生效时间、生效网站数进行配置 |
| 漏洞扫描 | 网站漏洞监测 | 对发现网站存在的SQL注入、XSS跨站脚本、目录遍历、文件包含、备份文件、敏感文件等漏洞，检测内容覆盖WASC分类的多种Web应用漏洞和OWASP TOP10网站漏洞进行管理；定期跟踪漏洞的修复情况从而使网站的漏洞得以快速修复，降低网站被入侵的风险。 |
| 利用POC对目标网页进行WEB漏扫，发现SSQL注入漏洞、命令注入、CRLF注入、LDAP注入、XSS跨站脚本漏洞、路径遍历漏洞、信息泄漏漏洞、URL跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞、等安全漏洞问题 |
| mysql、redis、ftp、ssh等弱口令进行监测 |
| 漏洞自动化验证 | 支持针对常见漏洞进行程序自动化验证，具有基于互联网的漏洞响应平台，并可将自动验证漏洞生成安全告警 |
| 漏洞扫描任务管理 | 支持立即下发扫描；支持扫描任务开始时间配置；周期任务单个或批量停止、中断、继续； |
| 监测周期自定义 | 支持多引擎扫描网站存在的安全漏洞，并支持自定义监测周期。默认全站1周/次（可调整为3天、5天、7天、15天、30天） |
| 扫描策略自定义 | 扫描范围上支持全量扫描、快速扫描；扫描方式上支持深度扫描、广度扫描；支持开启附件检测；支持并发量配置； |
| 安全告警监测 | 威胁情报联动 | 支持与漏洞响应平台的联动，可实时同步主流的漏洞响应平台等漏洞信息，具有基于互联网的威胁情报中心。 |
| 内容变更监测 | 对首页、重点页面进行网页内容变更检测；首页检测：变更部分包含外链、敏感词、黑词、HTML之外内容产生告警；重点页面检测：只要内容有变化就告警；支持白名单配置 |
| 违规内容监测 | 结合海量词库及人工识别，通过机器学习手段，提供敏感词发现的技术手段，支持全站监测，可定位敏感词位置和内容，提供内容篡改的历史对比图。 |
| 支持分别配置一级页面和二级页面的监测频率，支持任务并发量配置，支持用户自定义敏感词，支持开启OCR识别，支持添加附件检测。默认全站30分钟/次，支持自定义首页5分钟/次、二级15分钟/次 |
| 网站黑链监测 | 提供基于大数据支撑的黑词暗链发现技术手段，支持全站对于潜藏在页面深处的第三方黄赌毒广告类链接进行监测并告警，可定位源代码篡改的位置和内容。 |
| 支持分别配置一级页面和二级页面的监测频率，支持任务并发量配置，支持用户自定义黑词。默认全站30分钟/次 |
| 支持自定义首页5分钟/次、二级15分钟/次 |
| 网站外链监测 | 识别并定位网站外部链接位置 |
| 网站后门监测 | 对目标网站进行监测、查看是否被植入后门 |
| 挖矿脚本监测 | 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。 |
| 可用性监测 | WEB服务可用性监测。支持网站故障原因定位，不限于：响应连接被重置、连接超时、http状态码、连接被拒绝等； |
| 可用性监测配置。可支持get/head/post三种方式对HTTP/HTTPS服务进行监控，监控频率支持自定义。支持对自定义的URL进行HTTP/HTTPS监控。支持对监测域名的IP协议栈情况进行实时识别，并且根据识别结果分别配置IPv4和IPv6的监测节点。 |
| 支持在高级配置中，自定义监测节点，并且配置异常节点阈值和超时阈值。 |
| 网站挂马监测 | 采用特征分析和沙箱行为分析技术对网站进行木马检测分析，实现快速、准确的发现和定位网页木马，确保用户在第一时间发现感染的木马并及时消除。对木马威胁进行报警、通知、处置管理。 |
| 云端运营 | 云端运营 | 提供云端7\*24小时告警人工运营服务，并提供问题处置建议和咨询；为确保人工运营服务及时处理告警，需支持云计算安全类一级响应信息安全服务能力并要求能力材料依据支撑，并需具有重大活动运营支撑服务。 |
| 安全监测频次 | 网站漏洞扫描 | 默认全站1周/次（可调整为3天、5天、7天、15天、30天） |
| 网站黑链监测 | 默认全站30分钟/次，支持自定义首页5分钟/次、二级15分钟/次 |
| 内容变更监测 | 指定页面URL30分钟/次 |
| 违规内容监测 | 默认全站30分钟/次，支持自定义首页5分钟/次、二级15分钟/次 |
| 可用性监测 | 默认15分钟/次，最高可调整为2分钟 |
| 挂马监测 | 默认全站30分钟/次 |
|  | 安全性 | 监测平台必须满足网络安全等级保护三级要求 |

**4.6本地化售后服务要求**

本次项目需由设备原厂商服务团队提供服务，本次采购方案包括以下服务:

（1）响应时间：当系统使用过程中出现故障时，需在20分钟内响应，若出现远程无法进行诊断或解决的情况下，需在4小时内到达现场进行维护解决。

（2）现场巡检服务：由设备原厂商的巡检工程师提供每季度一次的高级威胁监测设备的现场巡检服务；每次安排2名设备原厂商的巡检工程师到现场巡检，至少一名具备PMP或以上认证证书。

（3）远程技术支持服务：提供5\*8小时（QQ和TeamViewer）远程技术支持服务；提供在线技术回复服务，建立问题及时反馈回复微信群或钉钉群,配置有专门运维人员在线及时回复解答疑问。

（4）服务文档管理: 按照约定时间定期以电子邮件形式保质保量提交各类巡检报告、季度巡检详情。

（5）提供7\*24小时的电话咨询服务，包括日常技术咨询和指导服务等。

**4.7其他要求**

（1）设备原厂商应根据采购人的需求，对所提供的系统保证全面、有效、及时的技术支持和运营维护服务。 （2）设备原厂商应提供的伴随服务：安装、调试、验收、培训、服务期内系统的运行及维护保养等一切服务。设备原厂商应在投标文件中详细说明技术服务的范围和程序。 （3）系统运行期间，设备原厂商应指定具有其厂商社保证明（提供自投标日起前六个月的社保证明）的人员，和富有经验的技术人员在现场负责系统的运行和维护，提供至少4名技术工程师，并具有不少于10人的后备工程师团队。

（4）本项目所涉及的产品功能、服务等需实际配置，无需二次授权，授权数量在无明确标定的情况下视为无授权数量限制。

（5）需提供由设备原厂商实施的以下安全服务内容：

 1）提供不少于5年的高级威胁监测安全系统原厂维保服务，维保服务期间，免费提供设备维修、软件升级、威胁情报库更新、规则库升级等；

 2）提供不少于5年7\*24小时的威胁事件检测与安全运营分析服务；

 3）针对用户所有业务系统和网站，提供不少于每两个月1次（2年，共12次）弱口令扫描与处置服务。另外针对校方新上线业务系统，可由校方指定时间，提供两年不少于60个IP弱口令扫描与处置服务；

 4）针对用户所有业务系统和网站，提供不少于每两个月1次（2年，共12次）漏洞扫描与处置服务。另外针对校方新上线业务系统，可由校方指定时间，提供两年不少于60个IP的漏洞扫描与处置服务；

 5）针对用户所有业务系统和网站，提供不少于每两个月1次（2年，共12次）基线检查与处置服务。另外针对校方新上线业务系统，可由校方指定时间，提供两年不少于60个域名的弱基线检查与处置服务；

 6）针对用户所有业务系统和网站，提供不少于每两个月1次（2年，共12次）Webshell后门检测与处置服务。另外针对校方新上线业务系统，可由校方指定时间，提供两年不少于60个IP的Webshell后门检测与处置服务；

 7）提供两年内不少于30个域名（站群按照一个域名来核算）的渗透测试服务；

 8）提供两年内不少于2次的网络安全架构评估；

 9）提供两年内不少于15次的安全情报推送服务；

 10）提供两年内不少于10次的现场安全应急响应服务；

 11）提供两年内不少于50人/天的现场重保值守服务；

 12）提供一年内不少于20域名的网站云监测服务；

 13）提供一年内不少于20域名的网站云防护服务。

**演示**

一、演示内容：

**演示要求1**（威胁分析模块功能-可视化展示-大屏可视）：为帮助我校充分展示安全建设效果，支持不同安全视角展示设备内置不少于16个独立的大屏展示功能，包括全网安全态势感知大屏、分支安全态势、安全事件态势、通报预警态势、资产态势大屏等，同时能满足多种场景的监控，比如日常运维、护网场景。支持对安全事件、外部攻击者、ATTCK能力图谱等维度进行自定义设置实现实时告警展示，支持大屏轮播，可在一个屏幕上自动切换轮播不同的大屏，所有大屏可自定义播放顺序。

**演示要求2**（威胁分析模块功能-资产管理-资产探测）：为了帮助我校便捷管理信息化资产及发现影子资产，提升资产风险管理能力，支持通过主动发送微量包的扫描方式探测潜在的服务器（影子资产）以及学习服务器的基础信息，资产指纹信息包括资产类型、端口、操作系统、MAC地址、主机名等。

**演示要求3**（威胁分析模块功能-行为分析-登录行为分析）**：**为了解决校园网存在大量弱密码的问题，提高弱密码检测精准度，弱密码检测弱密码检测逻辑分为登录入口、弱密码定义、登陆结果三个步骤，登陆结果检测技术基于UEBA学习技术（无监督自我学习）提取登陆成功的特征，通过UEBA技术对响应体内容和登录跳转路径进行持续学习训练登录成功特征，并支持安全导出弱密码日志和脆弱性感知报告。

**演示要求4**（威胁分析模块功能-响应处置-联动处置）：处置中心的多个模块的安全事件内置多个处置策略模板，为保障我校安全处置效果及效率须对接学校校园安全基础设施（包括防火墙、终端安全响应系统、超融合内建安全）实现联动封锁、访问控制，完成终端安全响应系统联动一键查杀、进程取证，完成关闭超融合上的中毒虚拟主机，完成对超融合上中毒的虚拟主机进行快照，保证核心业务数据不丢失等功能。

**演示要求5**（威胁分析模块功能-报表管理-报表导出）**：**为了帮助管理员高效汇报，体现安全工作价值，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报告。并且可快速生成月度、季度、年度PPT报表，摘要报告支持PPT格式导出；包含网络安全整体解读、网络安全风险详情、告警及事件响应盘点等。

**演示要求6**（威胁分析模块功能-重保模式-重保任务）**：**因校方有重保任务，为确保校方有效完成重保任务，所以该设备必须支持重保模式，在设备模式上有重保模式模块，模块可开启，具备实战化攻防中心，支持备战阶段的对外服务器外网暴露面分析、内网服务器暴露面梳理。实战阶段的实时攻击分析，实时展受害者IP、攻击者IP、XFF、攻击结果、攻击次数、威胁类型、威胁等级、状态码等20个以上类型。实战阶段的全过程可视溯源分析可以查看攻击者画像，包括攻击概览、攻击统计趋势、攻击详情等信息。

**演示要求7**（威胁分析模块功能-行为分析-访问行为分析）**：**为保证我校行为分析的举证效果和准确性，实现挖矿、木马等用户风险行为快速定位，需要与我校本地专业上网行为审计设备进行对接，实现用户账号信息同步，支持上网提醒、冻结账号、查询账号，提升管理及溯源查询效率，以基于用户身份进行威胁管控。

**演示要求8**（威胁分析模块功能-系统管理-安全专项告警联动处置）**：**支持文件、邮件、勒索、挖矿相关安全事件专项页面展示，且所有专项告警支持直接进行联动处置，联动处置支持自动调用内置处置策略模板，也支持自动化编排的自定义处置流程策略。支持根据自身业务和安全运维经验自定义告警/事件，以便提高告警的精确度，减少运维成本。

**演示要求9**（全流量威胁发现模块-策略配置-敏感信息检测）**：**为保证我校师生个人信息数据安全和数字化资产的数据安全，须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。

**演示要求10**（全流量威胁发现模块-流量采集-日志传输）**：**为适应我校不同时期带宽占用和安全级别的场景需求，须至少支持5种类型日志传输模式,包含标准模式（占用带宽中等、安全等级中等）、精简模式（占用带宽小、安全等级低）、高级模式（占用带宽大、安全等级高）、局域网模式（横向访问检测）、自定义模式。

二、演示U盘

1.根据“电子交易/不见面开评标”原则，响应供应商需将上述演示内容进行系统演示及讲解过程录制视频，该录制视频演示时长不超过15分钟以mp4格式存储于U盘；响应供应商须自行核验U盘中的视频能正常播放，保证视频无需转码即可直接用主流播放器打开播放。

2.演示U盘可以EMS或顺丰邮寄形式在响应截止时间前递交，演示U盘应当密封包装并在包装上标注演示U盘、响应项目名称、标项、响应供应商名称并加盖公章。

3.未按磋商文件要求提供演示U盘及演示内容，导致专家无法正常评审的风险由响应供应商自行承担。

▲4.未提供演示，磋商响应无效。

**第三章 供应商须知**

**供应商须知前附表**

|  |  |  |
| --- | --- | --- |
| **条款号** | **内容** | **说明与要求** |
| （一） | 适用范围 | 本磋商文件适用于浙江金融职业学院数据中心高级威胁监测与安全管理项目 的磋商、评审、成交、验收、合同履约、付款等（法律、法规另有规定的，从其规定）。 |
| （二） | 采购方式 | 本次采购采用竞争性磋商（线上电子交易）方式进行。 |
| （三） | 竞争性磋商委托 | 1.▲供应商授权代表必须为供应商本单位在职职工，并提供2020年12月（含）以后任意一月社保缴纳证明（授权代表为法定代表人可不提供）。2.如供应商代表不是法定代表人，须提供法定代表人授权委托书（格式详见磋商文件第六章）。 |
| （四） | 磋商费用 | 1.不论磋商结果如何，供应商均应自行承担所有与磋商有关的全部费用；2.成交供应商在成交通知书发出之日起七个工作日内，向采购代理机构交纳代理服务费；3.成交供应商逾期支付代理服务费，须承担代理服务费每日百分之三的违约金，逾期十日未支付的，采购代理机构有权向杭州仲裁委员会对成交供应商提起仲裁，仲裁费用（包括仲裁受理费和仲裁处理费）均由成交供应商承担。4.代理服务费收费标准（差额累进）：

|  |  |
| --- | --- |
| **成交金额（万元）** | **收费标准（费率，%）** |
| 100以下 | 1.05 |

 不足叁仟元按叁仟元计算。 |
| （五） | 磋商保证金（元） | 无。 |
| （六） | 联合体响应 | 本项目（是）接受联合体响应。 |
| （七） | 转包与分包 | 1.本项目不允许转包；2.供应商根据磋商文件的规定和采购项目的实际情况，拟在成交后将成交项目的非主体、非关键性工作分包的，应当在响应文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。 |
| （八） | **信用记录** | 根据财库[2016]125号《关于在政府采购活动中查询及使用信用记录有关问题的通知》要求，采购代理机构会对供应商信用记录进行查询并甄别。信用信息查询的截止时点：响应截止时间；（1）查询渠道：“信用中国”（www.creditchina.gov.cn）、“中国政府采购网”（www.ccgp.gov.cn）；（2）信用信息查询记录和证据留存具体方式：采购代理机构经办人和监督人员将查询网页打印、签名与其他采购文件一并保存；（3）信用信息的使用规则：供应商被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的，拒绝其参与政府采购活动。 |
| （九） | 资格审查要求的资格证明材料 | **资格审查要求的资格证明材料(均需加盖公章)：**（1）有效的法人或者其他组织的营业执照等证明文件，自然人的身份证明（2）符合参加政府采购活动应当具备的一般条件的承诺函（3）落实政府采购政策需满足的资格要求：无（4）本项目的特定资格要求证明材料：无。 |
| （十） | **响应文件份数** | **电子加密响应文件：政府采购云平台在线上传一份；备份响应文件：密封包装后EMS或顺丰邮寄形式递交一份（邮寄地址：杭州市西湖区玉古路173号中田大厦11楼H室，浙江求是招标代理有限公司（杨立凯）收，电话：0571-87670301，寄出后将（快递单号、项目名称、公司名称、联系方式等相关信息）发至：zb02@qszb.net，以便查收）。****特别说明：双休日和法定节假日不收件，供应商自行承担邮寄风险。** |
| （十一） | **磋商报价** | 1.报价应按磋商文件要求的格式编制、填写报价内容（可自行增行），未按磋商文件要求编制、填写的响应文件可能被拒绝；2.本次磋商采用人民币报价；3.最后磋商报价是履行合同的最终价格，有关本项目实施所涉及的一切费用均计入报价。▲4.采购人将以合同形式有偿取得货物或服务，不接受供应商给予的赠品、回扣或者与采购无关的其他商品、服务。 |
| （十二） | **响应有效期** | ▲从提交响应文件的截止之日起90天。在原响应有效期满之前，如果出现特殊情况，采购人或采购代理机构以书面形式通知供应商延长响应有效期。 |
| （十三） | 评审方法和评审标准 | 详见“第四章 评审方法和评审标准”。 |
| （十四） | 评审结果公示 | 评审结果公示媒体：浙江政府采购网（http://zfcg.czt.zj.gov.cn）。 |
| （十五） | 签订合同 | 成交通知书发出之日起30日内。 |

**一、总则**

供应商应仔细阅读磋商文件的所有内容，按照磋商文件的要求提交响应文件，并对所提供的全部资料的真实性承担法律责任。

**（一）适用范围**

本磋商文件适用于浙江金融职业学院数据中心高级威胁监测与安全管理项目 的磋商、评审、成交、验收、合同履约、付款等（法律、法规另有规定的，从其规定）。

**（二）定义**

1.“采购人”系指浙江金融职业学院；

2.“采购代理机构”系指组织本次竞争性磋商的浙江求是招标代理有限公司；

3.“供应商”系指响应磋商、参加竞争的法人、其他组织或者自然人；

4.“书面形式”包括合同书、信件和数据电文(包括电报、电传、传真、电子数据交换和电子邮件)等可以有形地表现所载内容的形式；

5.“电子加密响应文件”系指通过政采云电子交易客户端（政采云响应客户端）完成响应文件编制后生成并加密的数据电文形式的响应文件（文件扩展名为.jmbs），“备份响应文件”系指与“电子加密响应文件”同时生成的数据电文形式的电子文件（文件扩展名为.bfbs）；

“电子签名”系指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据；“公章”系指单位法定名称章。因特殊原因需要使用冠以法定名称的业务专用章的，响应时须提供《业务专用章使用说明函》（附件1）。

磋商文件对响应文件签署、盖章的要求适用于电子签名。

6.“▲”系指实质性要求条款，供应商应当做出实质性响应。

**（三）采购方式**

本次采购采用竞争性磋商（线上电子交易）方式进行。

**（四）竞争性磋商委托**

1.▲供应商授权代表必须为供应商本单位在职职工，并提供2020年12月（含）以后任意一月社保缴纳证明（授权代表为法定代表人可不提供）。

2.如供应商代表不是法定代表人，须提供法定代表人授权委托书（格式详见磋商文件第六章）。

**（五）磋商费用**

1.不论磋商结果如何，供应商均应自行承担所有与磋商有关的全部费用；

2.成交供应商在成交通知书发出之日起七个工作日内，向采购代理机构交纳代理服务费；

3.成交供应商逾期支付代理服务费，须承担代理服务费每日百分之三的违约金，逾期十日未支付的，采购代理机构有权向杭州仲裁委员会对成交供应商提起仲裁，仲裁费用（包括仲裁受理费和仲裁处理费）均由成交供应商承担。

4.代理服务费收费标准（差额累进）：

|  |  |
| --- | --- |
| **成交金额（万元）** | **收费标准（费率，%）** |
| 100以下 | 1.05 |

不足叁仟元按叁仟元计算。

5.磋商保证金（元）：无

**（六）联合体响应**

本项目（是）接受联合体响应。

**（七）转包与分包**

1.本项目不允许转包；

2.供应商根据磋商文件的规定和采购项目的实际情况，拟在成交后将成交项目的非主体、非关键性工作分包的，应当在响应文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。

**（八）质疑和投诉**

1.供应商认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、采购代理机构提出质疑。质疑供应商对采购人、采购代理机构的答复不满意，或者采购人、采购代理机构未在规定时间内作出答复的，可以在答复期满后15个工作日内向本级财政部门提起投诉。

**2.供应商提出质疑应当提交质疑函和必要的证明材料，质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。质疑函应当包括下列内容：**

（1）供应商的姓名或者名称、地址、邮编、联系人及联系电话；

（2）质疑项目的名称、编号；

（3）具体、明确的质疑事项和与质疑事项相关的请求；

（4）事实依据；

（5）必要的法律依据；

（6）提出质疑的日期。

供应商为自然人的，应当由本人签名；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签名或者盖章，并加盖公章。

3.提出质疑的供应商应当是参与本项目磋商响应活动的供应商。**供应商在法定质疑期内应一次性提出针对同一采购程序环节的质疑。**

4.根据《政府采购质疑和投诉办法》第三十七条的规定，投诉人在全国范围12个月内三次以上投诉查无实据的，由财政部门列入不良行为记录名单。

投诉人有下列行为之一的，属于虚假、恶意投诉，由财政部门列入不良行为记录名单，禁止其1至3年内参加政府采购活动：

（1）捏造事实；

（2）提供虚假材料；

（3）以非法手段取得证明材料。证据来源的合法性存在明显疑问，投诉人无法证明其取得方式合法的，视为以非法手段取得证明材料。

**（九）采购项目需要落实的政府采购政策**

**1.**本项目原则上采购本国生产的货物、工程和服务，不允许采购进口产品。除非采购人采购进口产品，已经在采购活动开始前向财政部门提出申请并获得财政部门审核同意，且在采购需求中明确规定可以采购进口产品（但如果因信息不对称等原因，仍有满足需求的国内产品要求参与采购竞争的，采购人、采购机构不会对其加以限制，仍将按照公平竞争原则实施采购）。

**2.支持绿色发展**

采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构将依据国家确定的认证机构出具的、有效的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。供应商须按磋商文件要求提供相关产品认证证书。

▲采购人拟采购的产品属于政府强制采购的节能产品品目清单范围的，供应商未按磋商文件要求提供国家确定的认证机构出具的、有效的节能产品认证证书的，响应无效。

修缮、装修类项目采购建材的，采购人应将绿色建筑和绿色建材性能、指标等作为实质性条件纳入磋商文件和合同。

为助力打好污染防治攻坚战，推广使用绿色包装，政府采购货物、工程和服务项目中涉及商品包装和快递包装的，供应商提供产品及相关快递服务的具体包装要求要参考《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》。

**3.支持中小企业发展**

中小企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。

符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

在政府采购活动中，供应商提供的货物、工程或者服务符合下列情形的，享受中小企业扶持政策：

在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受中小企业扶持政策。

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

对于未预留份额专门面向中小企业的政府采购货物或服务项目，以及预留份额政府采购货物或服务项目中的非预留部分标项，对小型和微型企业的最后报价给予10%的扣除，用扣除后的价格参与评审。接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的政府采购货物或服务项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%以上的，对联合体或者大中型企业的报价给予3%的扣除，用扣除后的价格参加评审。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定的条件并提供《残疾人福利性单位声明函》的残疾人福利性单位视同小型、微型企业；

符合《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）规定的监狱企业并提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业证明文件的，视同为小型、微型企业。

可享受中小企业扶持政策的供应商应按照磋商文件格式要求提供《中小企业声明函》，供应商提供的《中小企业声明函》与实际情况不符的，不享受中小企业扶持政策。声明内容不实的，属于提供虚假材料谋取中标、成交的，依法承担法律责任。

中小企业享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

除财库《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）、《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）规定企业类型以外的供应商不享受中小企业扶持政策。

**二、磋商文件**

**（一）磋商文件的构成**

本磋商文件由以下部分组成：

1.采购邀请

2.采购需求

3.供应商须知

4.评审方法和评审标准

5.拟签订的合同文本

6.响应文件格式

7.本项目磋商文件的澄清、答复、修改、补充的内容

**（二）供应商的风险**

供应商没有按照磋商文件要求提供全部资料，或者供应商没有对磋商文件在各方面作出实质性响应是供应商的风险，并可能导致其响应被拒绝。

**（三）磋商文件的澄清与修改**

1.提交首次响应文件截止之日前，采购人、采购代理机构可以对已发出的磋商文件进行必要的澄清或者修改，澄清或者修改的内容作为磋商文件的组成部分。

澄清或者修改的内容可能影响响应文件编制的，采购人、采购代理机构会在提交首次响应文件截止时间至少5日前，以书面形式通知所有获取磋商文件的供应商；不足5日的，采购人、采购代理机构会顺延提交首次响应文件截止时间。

2.磋商文件的修改将以书面形式通知所有获取磋商文件的供应商，并对其具有约束力。供应商在收到上述通知后，应立即向采购代理机构回函确认。若无书面回函确认，视同供应商已收到磋商文件修改的通知，并受其约束。

3.磋商文件澄清、答复、修改、补充的内容为磋商文件的组成部分。当磋商文件与磋商文件的答复、澄清、修改、补充通知就同一内容的表述不一致时，以最后发出的书面形式文件为准。

4.磋商文件的澄清、答复、修改或补充都应该通过本采购代理机构以法定形式发布，采购人非通过本机构，不得擅自澄清、答复、修改或补充磋商文件。

**三、响应文件的编制**

**（一）响应文件的组成**

响应文件（电子加密响应文件）由**资格文件、报价文件、商务和技术文件三部分**组成（格式详见磋商文件第六章）。供应商应将响应文件各部分**分别上传**至政府采购云平台指定位置。

响应文件组成：详见“第六章 响应文件格式”目录

**（二）响应文件的签署和份数**

1.供应商应按照磋商文件和政府采购云平台的要求，根据响应文件的组成规定的内容及顺序通过政采云电子交易客户端（政采云响应客户端）编制加密响应文件，响应文件内容不完整、编排混乱导致响应文件被误读、漏读或者查找不到相关内容的，是供应商的责任。

2.响应文件须由供应商在规定位置加盖公章，供应商应写全称。

3.响应文件不得涂改，若有修改错漏处，须由供应商加盖公章，或者由法定代表人或其授权的代表签名。响应文件因字迹潦草或表达不清所引起的后果由供应商负责。

**4.响应文件份数：**

**电子加密响应文件：政府采购云平台在线上传一份；备份响应文件：密封包装后EMS或顺丰邮寄形式递交一份（邮寄地址：杭州市西湖区玉古路173号中田大厦11楼H室，浙江求是招标代理有限公司（杨立凯）收，电话：0571-87670301，寄出后将（快递单号、项目名称、公司名称、联系方式等相关信息）发至：zb02@qszb.net，以便查收）。**

**特别说明：双休日和法定节假日不收件，供应商自行承担邮寄风险。**

**备注：**

**（三）响应文件的上传、递交、修改和撤回**

1.响应文件的上传、递交：

（1）电子加密响应文件的上传：

▲a.供应商应在响应文件提交截止时间前将电子加密响应文件成功上传至政府采购云平台，否则响应无效；

b.电子加密响应文件成功上传后，供应商可自行打印响应文件接收回执。

（2）备份响应文件的密封包装、递交：

a.供应商在政府采购云平台完成电子加密响应文件的上传后，可以EMS或顺丰邮寄形式在响应文件提交截止时间前递交以介质（U盘）存储的数据电文形式的备份响应文件；

b.备份响应文件应当密封包装并在包装上标注响应项目名称、供应商名称并加盖公章（非电子签章），供应商逾期送达或者未密封包装的备份响应文件采购代理机构将予以拒收；

▲c.通过政府采购云平台成功上传的电子加密响应文件已按时解密的，备份响应文件自动失效。响应文件提交截止时间前，供应商仅递交备份响应文件而未将电子加密响应文件成功上传至政府采购云平台的，响应无效。

▲d.响应截止时间前，供应商仅递交备份响应文件而未将电子加密响应文件成功上传至政府采购云平台的，响应无效。

2.供应商应当在响应文件提交截止时间前完成响应文件的上传、递交，并可以补充、修改或者撤回响应文件。补充或者修改响应文件的，应当先行撤回原文件，补充、修改后重新上传、递交。响应文件提交截止时间前未完成上传、递交的，视为撤回响应文件。响应文件提交截止时间后上传、递交的响应文件，政府采购云平台及采购代理机构将予以拒收。

3.供应商因未在线参加开标而导致电子加密响应文件无法按时解密等一切后果由供应商自行承担。

4.供应商应按照磋商文件和政府采购云平台的要求，根据响应文件的组成规定的内容及顺序通过政采云电子交易客户端（政采云响应客户端）编制加密响应文件。

**备注：**

**供应商可通过浙江省“电子交易/不见面开评标”学习专题提前进行专题学习，熟悉操作，避免影响采购活动（https://edu.zcygov.cn/luban/e-biding）。**

**（四）响应文件的语言及计量**

响应文件以及供应商与采购人或采购代理机构就有关磋商响应事宜的所有来往函电，均应以中文汉语书写。除签名、盖章、专用名称等特殊情形外，以中文汉语以外的文字表述的响应文件视同未提供（有中文汉语说明的除外）。

**（五）磋商报价**

1.报价应按磋商文件要求的格式编制、填写报价内容（可自行增行），未按磋商文件要求编制、填写的响应文件可能被拒绝；

2.本次磋商采用人民币报价；

3.最后磋商报价是履行合同的最终价格，有关本项目实施所涉及的一切费用均计入报价。

▲4.采购人将以合同形式有偿取得货物或服务，不接受供应商给予的赠品、回扣或者与采购无关的其他商品、服务。

**（六）响应有效期**

▲从提交响应文件的截止之日起90天。在原响应有效期满之前，如果出现特殊情况，采购人或采购代理机构以书面形式通知供应商延长响应有效期。

**四、响应无效的情形**

未响应磋商文件“▲”标记条款要求的，响应无效。

**1.在资格审查时，如发现下列情形之一的，响应文件将被视为无效：**

（1）资格证明材料不全的，或者不符合磋商文件要求的；

（2）供应商不具备磋商文件中规定的资格要求的；

（3）资格文件未按要求签署、盖章的。

**2.在符合性审查、商务和技术评审时，如发现下列情形之一的，响应文件将被视为无效：**

（1）商务和技术文件未按要求签署、盖章的；

（2）未提供或未按要求提供响应函、法定代表人授权委托书；

（3）法定代表人委托授权代表参加响应但未提供符合要求的授权代表社保缴纳证明的；

（4）未提供或未如实提供采购需求偏离表的；

（5）明显不符合磋商文件要求，或负偏离达到规定数目的；

（6）响应技术方案不明确，存在一个或一个以上备选（替代）响应方案的；

（7）响应文件含有采购人不能接受的附加条件的；

（8）法律、法规和磋商文件规定的其他无效情形。

**3.在报价评审时，如发现下列情形之一的，响应文件将被视为无效：**

（1）最后报价超过磋商文件中规定的预算金额或最高限价的；

（2）最后报价具有选择性的。

特别说明：磋商小组认为供应商的最后报价明显低于其他供应商最后报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评审现场合理的时间内提供书面说明，必要时提交相关证明材料；供应商不能证明其最后报价合理性的，磋商小组应当将其作为无效响应处理。

**4.有下列情形之一的，视为供应商串通，其响应无效：**

（1）不同供应商的响应文件由同一单位或者个人编制；

（2）不同供应商委托同一单位或者个人办理磋商事宜；

（3）不同供应商的响应文件载明的项目管理成员或者联系人员为同一人；

（4）不同供应商的响应文件异常一致或者最后报价呈规律性差异；

（5）不同供应商的响应文件相互混装。

**五、响应文件开启**

采购代理机构按照磋商文件规定的时间通过电子交易平台组织开启，所有供应商均应当准时在线参加。供应商不足3家的，不得开启。

开启时，电子交易平台按开启时间自动提取所有响应文件。采购人或代理机构依托电子交易平台发起开始解密指令，供应商按照平台提示和磋商文件的规定在半小时内完成在线解密。

**响应文件未按时解密，供应商提供了备份响应文件的，以备份响应文件作为依据，否则视为响应文件撤回。响应文件已按时解密的，备份响应文件自动失效。**

**特别说明：如遇政府采购云平台电子化开启或评审程序调整的，按调整后程序执行。**

**六、评审程序**

磋商小组成员应当按照客观、公正、审慎的原则，根据磋商文件规定的评审程序、评审方法和评审标准进行独立评审。未实质性响应磋商文件的响应文件按无效响应处理，磋商小组应当告知提交响应文件的供应商。

磋商文件内容违反国家有关强制性规定的，磋商小组应当停止评审并向采购人或者采购代理机构说明情况。

**（一）资格审查**

开启后，磋商小组依据法律法规和磋商文件的规定，对供应商的资格条件进行审查。

对未通过资格审查的供应商，磋商小组告知其未通过的原因。

通过资格审查的供应商不足3家的，不再评标。

**（二）信用信息查询**

根据财库[2016]125号《关于在政府采购活动中查询及使用信用记录有关问题的通知》要求，采购代理机构会对供应商信用记录进行查询并甄别。信用信息查询的截止时点：响应截止时间；

（1）查询渠道：“信用中国”（www.creditchina.gov.cn）、“中国政府采购网”（www.ccgp.gov.cn）；

（2）信用信息查询记录和证据留存具体方式：采购代理机构经办人和监督人员将查询网页打印、签名与其他采购文件一并保存；

（3）信用信息的使用规则：供应商被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的，拒绝其参与政府采购活动。

联合体信用信息查询：两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，应当对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

**（三）符合性审查**

磋商小组对符合资格的供应商的响应文件进行符合性审查，以确定其是否满足磋商文件的实质性要求。

**（四）磋商**

磋商小组所有成员应当集中与单一供应商分别进行磋商，并给予所有参加磋商的供应商平等的磋商机会。

在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组通过政府采购云平台以书面形式同时通知所有参加磋商的供应商。

供应商应当按照磋商文件的变动情况和磋商小组的要求通过政府采购云平台提交磋商记录，并由其法定代表人或授权代表签名或者加盖公章。

供应商的磋商内容无法通过政府采购云平台上传的，可在规定时间内（不少于半小时）通过指定的电子邮箱（zb02@qszb.net）或传真号码（0571-87666116）提交。

**（五）最后报价**

磋商文件能够详细列明采购标的的技术、服务要求的，磋商结束后，磋商小组应当要求所有实质性响应的供应商在规定时间内提交最后报价，提交最后报价的供应商不得少于3家。

磋商文件不能详细列明采购标的的技术、服务要求，需经磋商由供应商提供最终设计方案或解决方案的，磋商结束后，磋商小组应当按照少数服从多数的原则投票推荐3家以上供应商的设计方案或者解决方案，并要求其在规定时间内提交最后报价。

最后报价是供应商响应文件的有效组成部分。符合《政府采购竞争性磋商采购方式管理暂行办法》（财库〔2014〕214号）第三条第一、四项情形的，提交最后报价的供应商可以为2家。

**（六）综合评分**

经磋商确定最终采购需求和提交最后报价的供应商后，由磋商小组采用**综合评分法**对提交最后报价的供应商的响应文件和最后报价进行综合评分。

综合评分法，是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。

**（七）汇总商务技术得分**

磋商小组各成员独立对进入最后报价的供应商的商务和技术文件进行评价，并汇总商务技术得分情况。

现场监督员如发现分值汇总计算错误、分项评分超出评分标准范围、客观评分不一致以及存在评分畸高、畸低情形的，应由相关人员当场改正或作出说明；拒不改正又不作说明的，由现场监督员如实记载后存入项目档案资料。

**（八）排序与推荐**

磋商小组应当根据综合评分情况，按照评审得分由高到低顺序推荐3名以上成交候选供应商，并编写评审报告。符合《政府采购竞争性磋商采购方式管理暂行办法》（财库〔2014〕214号）第二十一条第三款情形的，可以推荐2家成交候选供应商。评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术指标优劣顺序推荐。

按照浙财采监[2013]24号《关于规范政府采购供应商资格设定及资格审查的通知》第九条规定：如多家供应商提供相同品牌相同型号的产品参加同一政府采购项目响应的，应当按一家供应商认定。评审时，应取其中通过资格审查后的最后磋商报价最低一家为有效供应商；最后磋商报价相同时，取技术分最高者；均相同时，由磋商小组集体决定。

非单一产品采购项目中，作为关键核心部分的单一产品品牌、型号均相同且报价占项目总报价50%以上（含本数，下同）的，视为提供的是同品牌同型号的产品；多家供应商中，有一家供应商的报价达到50%以上，提供同品牌同型号产品的供应商均按一家供应商认定。

**（九）编写评标报告**

评审报告应当由磋商小组全体人员签名认可。磋商小组成员对评审报告有异议的，磋商小组按照少数服从多数的原则推荐成交候选供应商，采购程序继续进行。对评审报告有异议的磋商小组成员，应当在报告上签署不同意见并说明理由，由磋商小组书面记录相关情况。磋商小组成员拒绝在报告上签名又不书面说明其不同意见和理由的，视为同意评审报告。

**（十）补充说明**

采用竞争性磋商采购方式采购的政府购买服务项目（含政府和社会资本合作项目），在采购过程中符合要求的供应商（社会资本）只有2家的，竞争性磋商采购活动可以继续进行。

**七、成交与合同**

**（一）成交**

1.采购代理机构在评审结束后2个工作日内将评审报告送采购人确认。采购人在收到评审报告后5个工作日内从评审报告提出的成交候选供应商中，按照排序由高到低的原则确定成交供应商，也可以书面授权磋商小组直接确定成交供应商。采购人逾期未确定成交供应商且不提出异议的，视为确定评审报告提出的排序第一的供应商为成交供应商。

2.采购代理机构在成交供应商确定后2个工作日内公告成交结果，同时向成交供应商发出成交通知书，并将磋商文件随成交结果同时公告。

3.评审结果公示媒体：浙江政府采购网（http://zfcg.czt.zj.gov.cn）。

**（二）合同授予**

1.采购人与成交供应商应当在成交通知书发出之日起30日内，按照采购文件确定的合同文本以及采购标的、规格型号、采购金额、采购数量、技术和服务要求等事项签订政府采购合同。采购人不得向成交供应商提出超出采购文件以外的任何要求作为签订合同的条件，不得与成交供应商订立背离采购文件确定的合同文本以及采购标的、规格型号、采购金额、采购数量、技术和服务要求等实质性内容的协议。

2.成交后无正当理由拒不与采购人签订政府采购合同，将被取消成交资格，并处以采购金额千分之五以上千分之十以下的罚款，由政府采购监督管理部门列入不良行为记录名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照。

**八、验 收**

采购人组织对供应商履约的验收。大型或者复杂的政府采购项目，应当邀请国家认可的质量检测机构参加验收工作。验收方成员应当在验收书上签名，并承担相应的法律责任。如果发现与合同中要求不符，供应商须承担由此发生的一切损失和费用，并接受相应的处理。

采购人可以邀请参加本项目的其他供应商或者第三方机构参与验收。参与验收的供应商或者第三方机构的意见作为验收书的参考资料一并存档。

严格按照采购合同开展履约验收。采购人成立验收小组，按照采购合同的约定对供应商履约情况进行验收。验收时，按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，应当出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料应当存档备查。

验收合格的项目，采购人将根据采购合同的约定及时向供应商支付采购资金、退还履约保证金。验收不合格的项目，采购人将依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《中华人民共和国民法典》。供应商在履约过程中有政府采购法律法规规定的违法违规情形的，采购人应当及时报告本级财政部门。

**九、可中止电子交易活动的情形**

采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购代理机构可中止电子交易活动：

1.电子交易平台发生故障而无法登录访问的；

2.电子交易平台应用或数据库出现错误，不能进行正常操作的；

3.电子交易平台发现严重安全漏洞，有潜在泄密危险的；

4.病毒发作导致不能进行正常操作的；

5.其他无法保证电子交易的公平、公正和安全的情况。

出现前款规定情形，不影响采购公平、公正性的，采购代理机构可以待上述情形消除后继续组织电子交易活动；影响或可能影响采购公平、公正性的，应当重新采购。

**第四章 评审方法和评审标准**

**一、评审方法**

本次评审采用综合评分法，总分为100分。评分过程中采用四舍五入法，并保留小数2位。

供应商评审综合得分=商务分+技术分+价格分

商务分、技术分按照磋商小组成员的独立评分结果的算术平均分计算，计算公式为：商务分、技术分=（磋商小组所有成员评分合计数）/（磋商小组组成人员数）。项目评审过程中，不得去掉最后报价中的最高报价和最低报价。

**二、评审标准**

|  |  |  |
| --- | --- | --- |
| **评审因素** | **分值** | **评分细则** |
| **价格分（30）** |
| **最后磋商报价** | **30** | 价格分采用低价优先法计算，即满足磋商文件要求且最后磋商报价最低的供应商的价格为磋商基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：磋商报价得分=（磋商基准价/最后磋商报价）×30%×100 |
| **商务分（6）** |
| **质保期** | **1** | 质保期在满足磋商文件要求的基础上每延长一年加0.5分，最多加1分，延长时间不足一年的不计入加分，质保期不满足磋商文件要求的响应无效。 |
| **业绩** | **3** | 响应方或制造商自2019年1月1日以来（以合同签订时间为准）同类项目业绩（以提供的完整合同扫描件为准）：每提供1份合同业绩得1分，最高得3分。 |
| **软件著作权** | **2** | 响应方或制造商具有与本项目相关的软件著作权登记证书，每提供一份的1分，最高2分。 |
| **技术分（64）** |
| **响应产品的响应程度** | **16** | 不符合（负偏离）技术要求中注“▲”条款（不可偏离）的响应无效；响应产品全部满足竞争性磋商采购文件明确的技术条款要求的得满分；允许偏离的技术条款低于技术要求（负偏离）的，每项扣2分，允许偏离的技术条款低于技术要求（负偏离）达到9条及以上的响应无效。扣完为止 |
| **演示** | **20** | 响应供应商须按第二章采购需求“演示内容”中的10项内容进行演示，每项最高2分，总计20分。未提供实体系统演示，仅以PPT、图片格式等方式的演示每项最高得1分（具体演示内容在采购需求中体现）。 |
| **项目方案** | **4** | 供应商对学校现有网络安全的理解，对学校安全基础设施整体整合方案的详尽程度、经济性、合理性、可行性等。 |
| **4** | 具体解决方案的完整性、可行性、有效性等。 |
| **3** | 项目实施计划，人员排班、拟投入设备等情况。 |
| **4** | 项目维护计划（对用户故障的响应、处理、定期巡检等情况）。 |
| **3** | 项目的功能测试、试运行及验收方案的合理性、可行性情况等。 |
| **拟投人人员** | 3 | 为保证项目实施高效及准确，需配备所投设备原厂项目经理作为技术负责人，提供相关材料证明其专业素质、技术能力、同类项目实施经验情况（响应文件中提供技术负责人人员履历、资质证书扫描件、2020年1月至今任意一月依法缴纳社会保障资金的证明材料，不提供不得分） |
| 3 | 除技术负责人外其他专业技术人员组成、数量、专业素质、技术能力、经验等情况（响应文件中提供其他专业技术人员人员履历、资质证书扫描件、2020年1月至今任意一月依法缴纳社会保障资金的证明材料，不提供不得分） |
| **培训方案** | **2** | 培训方案的计划、地点、组织、人员配备、软硬件资料、培训讲师等内容进行等情况； |
| **售后服务** | **2** | 售后服务的响应的合理性、可行性等。 |

**说明：**

**1.根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，对符合规定的小微企业报价给予10%的扣除后计算价格得分。**

对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%以上的，对联合体或者大中型企业的报价给予3%的扣除，用扣除后的价格参加评审。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

**2.根据《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）的规定，**监狱企业参加政府采购活动时，提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件的，在政府采购活动中，监狱企业视同小型、微型企业，享受预留份额、评审中价格扣除等政府采购促进中小企业发展的政府采购政策。

**3.根据《关于促进残疾人就业政府采购政策的通知》（财库[2017]141号）的规定，**符合条件的残疾人福利性单位在参加政府采购活动时，提供财库[2017]141号文件规定的《残疾人福利性单位声明函》的，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等促进中小企业发展的政府采购政策。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

**第五章 拟签订的合同文本**

**浙江金融职业学院采购合同**

（本合同为合同样稿，最终稿由三方协商后确定，签订合同时删除括号内容）

 合同编号：

 确认书号：

**甲方**（采购人）：浙江金融职业学院

**乙方**（供应商）：

**鉴证方:**

甲、乙双方根据 关于 项目编号为 的项目采购的结果，签署本合同。

**一、货物（服务）内容及合同价格**

金额单位：元

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **货物（服务）名称** | **型号规格** | **配置要求** | **数量** | **单位** | **单价** |
| 此处填写采购货物 |  |  |  |  |  |
| 合计 |  |  |  |
| 合同总价大写： 小写：￥  |  |

注：1.商品型号、数量、配置要求及使用单位地址等详见附件清单。

2.以上合同总价包含产品到达用户并能正常使用所需的一切费用。

**二、技术资料**

1.乙方应按采购文件规定的时间向甲方提供使用货物（服务）的有关技术资料。

2.没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品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。

**三、质保期和履约保证金**

1.质保期 年。（自交货验收合格之日起计）

2.履约保证金 元。[合同签订后一周内，成交供应商向采购人提交合同金额2.5%的履约保证金，履约保证金自交付验收合格后12个月内无质量问题和维护问题由采购人无息退回成交方]

**四、质量保证及服务承诺（含招投标过程中指定的条款，包括特别服务承诺）**

1.乙方保证本合同中所供应的商品是最新生产的符合国家技术规格和质量标准的出厂原装合格产品。如发生所供商品与合同不符，甲方（使用方）有权拒收或退货，由此产生的一切责任和后果由乙方承担。

2.乙方提供的货物在质保期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴更换：由乙方承担所发生的全部费用。

⑵贬值处理：由甲乙双方合议定价。

⑶退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

3.在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

4.上述的货物在质保期内免费保修，因人为因素出现的故障不在免费保修范围内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

5.根据磋商文件要求条款可以增加记录。

**五、调试和验收**

1.甲方对乙方提交的货物依据采购文件上的技术规格要求和国家有关质量标准进行现场验收。货到并在完成响应各项要求后，甲方需在五个工作日内验收。

2.乙方交货前应对产品作出全面检查和对验收文件进行整理，并列出清单，作为甲方收货验收和使用的技术条件依据，检验的结果应随货物交甲方。

3.甲方对乙方提供的货物在使用前进行调试时，乙方需负责安装并培训甲方的使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做最终验收。

4.对技术复杂的货物，甲方应请国家认可的专业检测机构参与验收，并由其出具质量检测报告。

5.验收时乙方必须在现场，验收完毕后作出验收结果报告。

**六、交货期（或者施工工期）、交货方式及交货地点**

1.交货期（或者施工工期）：

2.交货方式：

3.交货地点：

**七、货款支付**

1.付款方式：合同签订后一周内，成交供应商向采购人提交合同金额2.5%的履约保证金，履约保证金自货物交付验收合格后12个月内无质量问题和维护问题由采购人无息退回成交方。

2.预付款：

3.付款方式。

4.付款按财政政策执行，因迟延到货以及不符合财政资金支付时间要求等原因造成不能及时付款的，甲方不承担责任。

**八、税费**

本合同执行中相关的一切税费均由乙方负担。

**九、知识产权**

乙方应保证所提供的货物或其任何一部分均不会侵犯任何第三方的知识产权。

**十、产权担保**

乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

**十一、转包或分包**

本合同范围的货物，应由乙方直接供应，不得转让他人供应，否则，甲方有权解除合同，没收质量保证金并追究乙方的违约责任。

验收费用由乙方负责。

**十二、货物包装**

1.乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

2.使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

**十三、违约责任**

1.甲方无正当理由拒收货物的，甲方向乙方偿付拒收货款总值的百分之五违约金。

2.甲方无故逾期验收和办理货款支付手续的,甲方应按逾期付款总额每日万分之五向乙方支付违约金。

3.乙方逾期交付货物的，乙方应按逾期交货总额每日千分之六向甲方支付违约金，由甲方从待付货款中扣除。逾期超过约定日期15个工作日不能交货的，甲方可解除本合同。乙方因逾期交货或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

4.乙方所交的货物品种、型号、规格、技术参数、质量不符合合同规定及采购文件规定标准的，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

**十四、不可抗力事件处理**

1.在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2.不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3.不可抗力事件延续120天以上，双方应通过友好协商，确定是否继续履行合同。

**十五、诉讼**

双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向甲方所在地法院起诉。

**十六、合同生效及其它**

1.合同经甲、乙、鉴证方三方签名并加盖单位公章后生效。

2.合同执行中涉及采购资金和采购内容修改或补充的，须经财政部门审批，并签书面补充协议，经报政府采购监督管理部门备案后，方可作为主合同不可分割的一部分。

3.竞争性磋商采购文件、响应文件、磋商记录等与本合同具有同等法律效力。

4.本合同未尽事宜，遵照《民法典》有关条文执行。

5.本合同一式六份，具有同等法律效力，甲方执三份、乙执二份、鉴证一份。

甲方（盖章）：浙江金融职业学院

地址：杭州下沙高教园东区学源街118号

开户银行：中国工商银行杭州经济技术开发区支行

帐号：1202050509900029173

法定（授权）代表人：

签名日期： 年 月 日

乙方（盖章）：\*\*\*\*

地址：\*\*\*\*\*

开户行：\*\*\*\*\*

开户帐号：\*\*\*\*\*

法定（授权）代表人：

签名日期： 年 月 日

合同鉴证方（盖章）:浙江求是招标代理有限公司

法定代表人或主要负责人:

鉴证日期: 年 月 日

**附件清单：**

 人民币：元

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **货物（服务）名称** | **品牌** | **规格型号** | **单位及数量** | **性能及指标** | **单价** | **小计** |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |
| **合计金额大写： 小写：￥ 元**  |

**第六章 响应文件格式**

**目 录**

**▲1.资格文件（单独上传）**

**资格审查要求的资格证明材料(均需加盖公章)：**

**（1）有效的法人或者其他组织的营业执照等证明文件，自然人的身份证明**

**（2）符合参加政府采购活动应当具备的一般条件的承诺函**

**（3）落实政府采购政策需满足的资格要求：无**

**（4）本项目的特定资格要求证明材料：无。**

**2.报价文件**

（1）初次报价一览表

（2）中小企业声明函（若属于中小企业）

（3）属于监狱企业的证明文件（若属于监狱企业）

（4）残疾人福利性单位声明函（若属于残疾人福利性单位）

**3.商务和技术文件**

（1）响应函

（2）法定代表人授权委托书

（2）2020年12月（含）以后任意一月供应商授权代表社保缴纳证明

（3）供应商同类合同一览表

（4）采购需求偏离表

（5）货物配置清单

（6）项目方案

（7）拟投人人员

（8）培训方案

（9）售后服务

（10）供应商需要说明的其他文件和材料

**资格文件**

**资格审查要求的资格证明材料(均需加盖公章)**

**（1）有效的法人或者其他组织的营业执照等证明文件，自然人的身份证明**

**说明：**

**1.如供应商是企业（包括合伙企业），提供在工商部门注册的有效“企业法人营业执照”或“营业执照”；**

**2.如供应商是事业单位，提供有效的“事业单位法人证书”；**

**3.如供应商是非企业专业服务机构的，提供执业许可证等证明文件；**

**4.如供应商是个体工商户，提供有效的“个体工商户营业执照”；**

**5.如供应商是自然人，提供有效的自然人身份证明。**

**（2）符合参加政府采购活动应当具备的一般条件的承诺函**

**致：浙江金融职业学院、浙江求是招标代理有限公司**

我方（供应商名称） 参加（项目名称） 项目的采购活动并承诺如下：

一、我方满足《中华人民共和国政府采购法》第二十二条规定：

（一）具有独立承担民事责任的能力；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和社会保障资金的良好记录；

（五）参加本项目政府采购活动前三年内，在经营活动中 **没有** 重大违法记录。（重大违法记录是指供应商因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚）

（六）法律、行政法规规定的其他条件。

二、未被信用中国（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

三、不存在以下情况：

1、单位负责人为同一人或者存在直接控股、管理关系的不同供应商参加同一合同项下的政府采购活动的；

2、为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后再参加该采购项目的其他采购活动的。

四、以上事项如有虚假或隐瞒，我方愿意承担一切后果和责任。

**供应商名称（电子签名/公章）：**

**日期： 年 月 日**

**（3）落实政府采购政策需满足的资格要求：无**

**（4）本项目的特定资格要求证明材料：无。**

**报价文件**

**（1）初次报价一览表**

采 购 人：浙江金融职业学院

项目名称：数据中心高级威胁监测与安全管理项目

项目编号：QSZB-Z(H)-B22216(CS)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **品牌** | **规格型号****或具体服务** | **产地** | **数量** | **单价（元）** | **金额（元）** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **说明：采购人将以合同形式有偿取得货物或服务，不接受供应商给予的赠品、回扣或者与采购无关的其他商品、服务。****总价（人民币元）****小写：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****大写：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

**说明：**

1.此表在不改变格式要求的情况下，可自行增行。

2.有关本项目实施所涉及的一切费用均计入报价。

**3.以上表格要求细分项目及报价，在“规格型号（或具体服务）”一栏中，货物类项目填写规格型号，服务类项目填写具体服务。**

**供应商名称（电子签名/公章）：**

**日期： 年 月 日**

**（3）中小企业声明函（货物）（若属于中小企业）**

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46 号）的规定，本公司（联合体）参加*（单位名称）*的*（项目名称）*采购活动，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

*1. （标的名称）* ，属于*（采购文件中明确的所属行业）行业*；制造商为*（企业名称）*，从业人员 人，营业收入为 万元，资产总额为 万元，属于*（中型企业、小型企业、微型企业）*；

*2. （标的名称）* ，属于*（采购文件中明确的所属行业）行业*；制造商为*（企业名称）*，从业人员 人，营业收入为 万元，资产总额为 万元，属于*（中型企业、小型企业、微型企业）*；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

注：

1.中小企业参加政府采购活动，应当出具财库〔2020〕46号文件规定的《中小企业声明函》，否则不得享受相关中小企业扶持政策。

2.从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

3.《中小企业声明函》填写不全的，视为未提供《中小企业声明函》（从业人员、营业收入、资产总额在中小企业划型标准规定中不涉及的除外），不享受价格优惠。如项目包含“多件”标的物的，需按标的物项数逐项填写。

4.供应商提供《中小企业声明函》内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。

5.本项目只以《中小企业声明函》作为评判供应商是否属于中小企业的唯一依据。

**（4）属于监狱企业的证明文件（若属于监狱企业）**

**监狱企业参加政府采购活动时，应当提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。**

**说明：**

一、监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地（设区的市）监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业参加政府采购活动时，应当提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

二、在政府采购活动中，监狱企业视同小型、微型企业，享受预留份额、评审中价格扣除等政府采购促进中小企业发展的政府采购政策。

**（5）残疾人福利性单位声明函（若属于残疾人福利性单位）**

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141号）的规定，**本单位为符合条件的残疾人福利性单位**，且本单位参加\_\_\_\_\_\_（采购人）单位的\_\_\_\_\_\_（项目名称）项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日 期：

**说明：**

一、享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：

（一）安置的残疾人占本单位在职职工人数的比例不低于25%（含25%），并且安置的残疾人人数不少于10人（含10人）；

（二）依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；

（三）为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；

（四）通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；

（五）提供本单位制造的货物、承担的工程或者服务（以下简称产品），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

前款所称残疾人是指法定劳动年龄内，持有《中华人民共和国残疾人证》或者《中华人民共和国残疾军人证（1至8级）》的自然人，包括具有劳动条件和劳动意愿的精神残疾人。在职职工人数是指与残疾人福利性单位建立劳动关系并依法签订劳动合同或者服务协议的雇员人数。

二、符合条件的残疾人福利性单位在参加政府采购活动时，应当提供财库[2017]141号文件规定的《残疾人福利性单位声明函》，并对声明的真实性负责。

三、在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等促进中小企业发展的政府采购政策。

残疾人福利性单位属于小型、微型企业的，不重复享受政策。

**商务和技术文件**

**（1）响应函**

**致：浙江金融职业学院、浙江求是招标代理有限公司**

我方参加浙江金融职业学院数据中心高级威胁监测与安全管理项目 （项目编号：QSZB-Z(H)-B22216(CS)）项目，为此，我方提交电子加密响应文件一份、以介质（U盘）存储的数据电文形式的备份响应文件 份。宣布同意如下：

1.我方已详细审查全部“磋商文件”，包括修改文件（如有）以及全部参考资料和有关附件，已经了解我方对于磋商文件、采购过程、成交结果有依法进行询问、质疑、投诉的权利及相关渠道和要求。

2.我方在磋商响应之前已经与贵方进行了充分的沟通，完全理解并接受磋商文件的各项规定和要求，对磋商文件的合理性、合法性不再有异议。

3.响应有效期自提交响应文件的截止之日起90天。

4.如成交，本响应文件至本项目合同履行完毕止均保持有效，我方将按“磋商文件”及政府采购法律、法规的规定履行合同责任和义务。关于代理服务费，我方承诺按照磋商文件的规定履行并承担相应的责任。

5.我方同意按照贵方要求提供与磋商有关的一切数据或资料。

6.与本磋商有关的一切正式往来信函联系：

|  |  |
| --- | --- |
| 联系人： |  |
| 职务： |  |
| 手机： |  |
| 电子邮箱： |  |
| 地址： |  |
| 开户银行： |  |
| 银行账号： |  |

**供应商名称（电子签名/公章）：**

**日期： 年 月 日**

**（2）法定代表人授权委托书**

致：浙江金融职业学院、浙江求是招标代理有限公司

我\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（姓名）系\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（供应商名称）的法定代表人，身份证号码：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

现授权委托本单位在职职工：\_\_\_\_\_\_\_\_\_（姓名），身份证号码：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_，以我方的名义参加浙江金融职业学院数据中心高级威胁监测与安全管理项目 标项 的磋商活动，并代表我方全权办理针对上述项目的磋商文件开启、磋商、评审、签约等具体事务和签署相关文件。

我方对被授权人的签名负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。被授权人在授权书有效期内签署的所有文件不因授权的撤销而失效。

被授权人无转委托权，特此委托。

▲供应商授权代表必须为供应商本单位在职职工，并提供2020年12月（含）以后任意一月社保缴纳证明。

法定代表人（签名或盖章）：

**供应商名称（电子签名/公章）：**

**日期： 年 月 日**

|  |
| --- |
| 法定代表人身份证明：授权代表身份证明： |

**（2）2020年12月（含）以后任意一月的供应商授权代表社保缴纳证明**

**（授权代表为法定代表人可不提供）**

**（3）供应商同类合同一览表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **采购人** | **项目名称** | **数量** | **合同金额****（万元）** | **附件页码** | **合同签订时间** | **采购人联系人****联系方式** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**说明：**

**1.供应商须提供上述业绩合同扫描件；**

**2.所有合同扫描件应清晰，应能体现合同签订时间、双方签名盖章等内容；**

**3.供应商应在不涉及商业秘密的前提下尽可能提供详细的合同扫描件内容。**

**供应商名称（电子签名/公章）：**

**日期： 年 月 日**

**（4）采购需求偏离表**

采 购 人：浙江金融职业学院

项目名称：数据中心高级威胁监测与安全管理项目

项目编号：QSZB-Z(H)-B22216(CS)

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **磋商文件要求** | **响应规格** | **是否偏离（提供说明）** |
| **采购资金的支付方式、时间、条件** |
| 1 |  |  |  |
| 2 |  |  |  |
| …… |  |  |  |
| **服务要求** |
| 1 |  |  |  |
| 2 |  |  |  |
| …… |  |  |  |
| **技术要求** |
| 1 |  |  |  |
| 2 |  |  |  |
| …… |  |  |  |

**说明：**

**1.逐项按照磋商文件要求填写响应规格；**

**2.偏离说明是指对磋商文件要求存在不同之处的解释说明。偏离系指：正偏离（高于采购需求）、负偏离（低于采购需求）、无偏离（满足采购需求）；**

**3.如不填写或未如实填写，自行承担磋商响应风险。**

**供应商名称（电子签名/公章）：**

**日期： 年 月 日**

**以下内容格式自拟**

**（6）项目方案**

**（7）拟投人人员**

**（8）培训方案**

**（9）售后服务**

**（10）供应商需要说明的其他文件和材料。**

**附件1：业务专用章使用说明函**

（采购人）、（采购代理机构）

我方 (供应商全称)是中华人民共和国依法登记注册的合法企业，在参加你方组织的（项目名称）项目（项目编号）响应（响应）活动中作如下说明：我方所使用的“XX专用章”与法定名称章具有同等的法律效力，对使用“XX专用章”的行为予以完全承认，并愿意承担相应责任。

特此说明。

供应商（法定名称章）：

日期： 年 月 日

**附：**供应商法定名称章（印模） 供应商“XX专用章”（印模）

**附件2：联合协议**

**（以联合体形式响应的，提供联合协议；本项目不接受联合体响应或者供应商不以联合体形式响应的，则不需要提供）**

（联合体所有成员名称）自愿组成一个联合体，以一个供应商的身份参加（项目名称）【招标编号：（采购编号）】响应。

一、各方一致决定，（某联合体成员名称）为联合体牵头人，代表所有联合体成员负责响应和合同实施阶段的主办、协调工作。

二、所有联合体成员各方签署授权书，授权书载明的授权代表根据磋商文件规定及响应内容而对采购人、采购机构所作的任何合法承诺，包括书面澄清及相应等均对联合响应各方产生约束力。

三、本次联合响应中，分工如下：（联合体其中一方成员名称）承担的工作和义务为： ；……。

四、（联合体其中一方成员名称）提供的全部货物由小微企业制造，其合同份额占到合同总金额 %以上；……。**（未预留份额专门面向中小企业采购的的采购项目，以及预留份额中的非预留部分采购包，接受联合体响应的，联合体其中一方提供的货物全部由小微企业制造，且其合同份额占到合同总金额 30%以上，对联合体报价给予3%的扣除）**

五、如果成交，联合体各成员方共同与采购人签订合同，并就采购合同约定的事项对采购人承担连带责任。

六、有关本次联合响应的其他事宜：

1、联合体各方不再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

2、联合体中有同类资质的各方按照联合体分工承担相同工作的，按照资质等级较低的供应商确定资质等级。

3、本协议提交采购人、采购机构后，联合体各方不得以任何形式对上述内容进行修改或撤销。

**联合体成员名称(电子签名/公章)：**

**日期： 年 月 日**

**附件3：分包意向协议**

（**成交后以分包方式履行合同的，提供分包意向协议；采购人不同意分包或者供应商成交后不以分包方式履行合同的，则不需要提供。**）

（供应商名称）若成为（项目名称）【招标编号：（采购编号）】的成交供应商，将依法采取分包方式履行合同。（供应商名称）与（所有分包供应商名称）达成分包意向协议。

一、分包标的及数量

（供应商名称）将 XX工作内容 分包给（某分包供应商名称），（某分包供应商名称），具备承担XX工作内容相应资质条件且不得再次分包；

……

二、分包工作履行期限、地点、方式

三、质量

四、价款或者报酬

五、违约责任

六、争议解决的办法

七、其他

（分包供应商名称）提供的货物全部由小微企业制造，其合同份额占到合同总金额 %以上。**（未预留份额专门面向中小企业采购的的采购项目，以及预留份额中的非预留部分采购包，允许分包的，分包供应商提供的货物全部由小微企业制造，且其合同份额占到合同总金额 30%以上的，对大中型企业的报价给予3%的扣除）**

**供应商名称（电子签名/公章）：**

**分包供应商名称：**

**日期： 年 月 日**

**附件4：**

**政府采购活动现场确认声明书**

浙江求是招标代理有限公司：

本人经由 （单位）负责人（法人代表）

 （姓名）合法授权参加 数据中心高级威胁监测与安全管理项目 项目（编号：QSZB-Z(H)-B22216(CS)）采购活动，经与本单位法人代表（负责人）联系确认，现就有关公平竞争事项郑重声明如下：

一、本单位与采购人之间：

□不存在利害关系；

□存在下列利害关系：

 A.投资关系 B.行政隶属关系 C.业务指导关系

 D.其他可能影响采购公正的利害关系（如有，请如实说明） 。

二、现已清楚知道参加本项目采购活动的其他所有响应供应商名称，本单位：

□与其他所有响应供应商之间均不存在利害关系；

□与 （响应供应商名称）之间存在下列利害关系：

 A.法定代表人或负责人或实际控制人是同一人

 B.法定代表人或负责人或实际控制人是夫妻关系

 C.法定代表人或负责人或实际控制人是直系血亲关系

 D.法定代表人或负责人或实际控制人存在三代以内旁系血亲关系

 E.法定代表人或负责人或实际控制人存在近姻亲关系

 F.法定代表人或负责人或实际控制人存在股份控制或实际控制关系

 G.存在共同直接或间接投资设立子公司、联营企业和合营企业情况

 H.存在分级代理或代销关系、同一生产制造商关系、管理关系、重要业务（占主营业务收入50%以上）或重要财务往来关系（如融资）等其他实质性控制关系

 I.其他利害关系情况。

三、现已清楚知道并严格遵守政府采购法律法规和现场纪律。

四、我发现响应供应商 之间存在或可能存在上述第二条第 项利害关系。

 响应方代表（签名）：

2022年7月8日

**备注：响应方须在响应文件解密后，通过电子邮件形式，向邮箱地址（zb02@qszb.net）发送《政府采购活动现场确认声明书》（上表）。**