政府采购合同书

采购编号：【KRDL】K5-2510147-02

网络安全体系建设项目（二期）

采购合同

甲　方：　西安理工大学

乙　方：　陕西泓腾网络科技有限公司

时　间：2026 年 3 月 17 日

采购合同

甲方：西安理工大学

乙方：陕西泓腾网络科技有限公司

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等相关法规，西安理工大学、陕西泓腾网络科技有限公司，双方本着友好平等协商、互惠互利的原则维护双方合法权益，达成如下协议。

一、采购内容

（一）项目名称：西安理工大学网络安全体系建设项目（二期）(项目编号：【KRDL】K5-2510147-02）。

（二）标的物及价款

序号	标的物名称	品牌/规格	生产厂家	单位	数量	单价（元）	小计（元）
1	堡垒机【核心产品】	绿盟/型号：OSMSNX3-HD650	北京神州绿盟科技有限公司	套	1	160000.00	160000.00
2	零信任安全接入系统	深信服/型号：aTrust-1000-B1050C	深信服科技股份有限公司	套	1	150000.00	150000.00
3	终端安全管理系统	深信服/型号：深信服统一端点安全管理系统V6.0	深信服科技股份有限公司	套	1	150000.00	150000.00
4	网络流量汇聚分流器	派网/型号：24X-100PRO	北京派网软件有限公司	台	1	250000.00	250000.00
5	安全MSS服务	深信服/型号：安全托管服务MSS-100	深信服科技股份有限公司	套	1	119660.00	119660.00

总价（人民币大写）： 捌拾贰万玖仟陆佰陆拾元整 合计（小　　写）： 829660.00 元
注：本合同总价一次性包死，不受市场价格变化因素的影响，从项目需求调研到设计、开发、实施、调试、验收、人员培训、接口开发和质保期等环节涉及到的一切费用，且包含系统所需对接其他系统的接口费用。

二、产品交付

1、根据项目招标文件要求和建设进度，合同签订后 60 个自然日内完成安装并交付采购人使用，包含但不限于硬件安装、软件部署、基本功能调试完成，并移交产品清单、技术文档，以及完成技术培训等。

2、实施地点：甲方指定地点。

三、产品质保期限

（一）货物质保期

1、堡垒机自验收合格之日起提供原厂工程师 5 年免费质保和售后服务。

2、零信任安全接入系统自验收合格之日起提供原厂工程师 5 年免费软硬件保修及升级服务。

3、网络流量汇聚分流器自验收合格之日起软硬件设备提供原厂工程师 5 年免费质保和维保服务。

4、终端安全管理系统自验收合格之日起提供原厂工程师 5 年免费软件升级服务。

（二）安全MSS服务期

1、安全 MSS 服务自验收合格之日起原厂工程师服务期为 1 年。

四、质保服务细则

1、完成硬件上架、软件安装、策略配置及第三方系统对接，保障产品快速上线。

2、提供管理员和用户培训，交付操作手册、常见问题指南，助力团队自主运维。

3、每季度巡检，输出健康报告与优化建议，持续提升性能与安全性。

4、提供软件升级包与硬件保修服务，核心设备可享备机先行,降低业务中断风险。

5、质保期内，产品出现任何非人为损坏的故障，乙方提供免费维修或更换服务。

6、乙方提供 7×24 小时 技术支持热线，包含电话、远程及现场技术支持，及时解答疑问。发生一般故障时，乙方应在接到甲方通知后 2小时内响应，并通过远

程方式尝试解决，若故障在 4 小时内无法远程修复，乙方工程师应在2 小时内（西安市内）到达现场；紧急故障30分钟内响应，必要时到达现场。

7、若故障在 24 小时内无法修复，乙方须在 72 小时内提供不低于原产品性能的备用设备供甲方临时使用，直至故障修复完毕。

8、自验收合格之日起，提供每周不少于2 天的固定线下驻场服务,服务期为一年。

五、重保时期执行标准

1、成立专项保障小组，派遣至少 1 名或以上具备相应资质的专业技术人员进行现场驻场值守，并明确项目经理和应急支持团队的人员名单与职责。确保责任到人，满足关键时期现场处置的即时性需求。

2、在重保期间提供现场及远程不间断的监测与值守服务。服务内容包括：实时日志分析、流量监测、安全事件告警研判，并增加硬件设备巡检频次（每天至少2次）。实现全天候的主动防御，及时发现潜在隐患。

3、制定详细的应急响应流程，对突发安全事件（如病毒爆发、黑客入侵）进行快速研判、抑制根除和恢复。确保事件发生时能有效闭环，最小化业务影响。

4、服务结束后，需提供完整的重保总结报告，内容应包括：安全事件处置记录、攻击溯源分析、系统薄弱环节以及后期加固建议。形成服务闭环，帮助用户提升长期安全能力。

5、在监测和处置过程中不泄露任何业务数据，且所有操作需可追溯、可审计，符合网络安全合规要求。保障甲方数据主权和业务隐私安全。

六、集成要求

根据此次招标文件要求，与甲方指定的第三方系统进行免费对接。

七、数据安全及保密协议

1、数据权属与范围：本服务过程中收集、产生的所有日志、告警、分析报告等数据（以下简称“安全数据 ”）其所有权均归甲方所有。

2、数据处理规范：乙方承诺其用于提供本服务的运营平台符合国家网络安全与数据合规要求。所有安全数据的存储与处理均应在甲方指定的境内环境或乙方符合等保三级要求的国内数据中心完成，不得跨境传输。

3、保密义务：乙方应对接触到的所有甲方安全数据及非公开信息承担严格保密责任，保密期限不因合同终止而解除。

4、服务终止处理：服务期满或合同终止后30 日内，乙方应将所有甲方安全数据（包括原始数据与衍生分析）以双方议定的可读格式完整返还，并出具书面证明，承诺已在甲方监督下彻底删除其服务器上的所有副本。

八、合同附件

1、招投标技术要求为本合同的附件，与本合同具有同等法律效力（详见附件 1）

2、安全 MSS 服务内容（详见附件2），附件中所有技术参数，特别是带“★ ”和“▲ ”的条款，均为合同的核心交付标准。任何一项的不符合（即“负偏离 ”），除非经甲方事先书面同意，均构成根本违约，甲方有权拒绝验收并要求乙方承担违约责任。

九、付款方式

项目实施完成，乙方并向甲方提交书面完工报告和试运行申请，不低于30 天试运行，经过甲方验收合格后，达到学校付款条件起 15 日内，支付合同总金额的100.00%，即 （人民币小写）：829660.00 元，（人民币大写）： 捌拾贰万玖仟陆佰陆拾元整。

十、发票开具

甲方付款前，乙方需先行提供符合国家规定的增值税专用发票。

甲方发票信息：

名称：西安理工大学

纳税人识别号：1261000043523042XN

地址：西安市金花南路5 号

开户行：中国银行西安金花南路支行

账号：102891574567

十一、乙方银行账户信息

名称：陕西泓腾网络科技有限公司

纳税人识别号：91610113MA6U2BW426

地址：陕西省西安市高新区唐延路11号1幢32201室

开户行：中国银行股份有限公司西安光华路支行

账号：102467781240

开户行行号：104791003411

公司法人：孙学梅

联系人：李新环　　联系电话：17691347221

十二、违约责任

1、合同违约情况按《中华人民共和国民法典》中的相关条款执行。

2、甲乙双方必须遵守本合同并执行合同中的各项规定，保证本合同的正常履行。

3、如因乙方工作人员在履行职务过程中的疏忽、失职、过错等故意或者过失原因给甲方造成损失或侵害，包括但不限于甲方本身的财产损失、由此而导致的甲方对任何第三方的法律责任等，乙方对此均应承担全部的赔偿责任。

4、未按合同要求提供设备或提供的设备质量或规格不能满足技术要求，甲方有权终止合同并对乙方违约行为进行追究，同时按政府采购法的有关规定进行相应的处罚。

5、乙方交付的产品或提供的服务不符合本合同及附件一技术要求的，甲方有权要求乙方在合理期限内无条件更换、重做或采取补救措施。若乙方未在规定期限内整改或整改后仍不符合要求，甲方有权要求退货或解除合同，乙方应赔偿甲方全部损失。

十三、解决合同纠纷的方式

1、在执行本合同中发生的或与本合同有关的争端，双方应通过友好协商解决，经协商不能达成协议时，则采取以下2 种方式解决争议：

（1）向西安仲裁委员会按其仲裁规则申请仲裁；

（2）向甲方所在地有管辖权的人民法院提起诉讼。

2、在仲裁期间，本合同应继续履行。

十四、其他约定事项

本合同甲乙双方分别签订，乙方签字盖章后，甲方代表按合同审签流程完成审签、盖章后合同生效。合同一式 陆 份，甲方 肆 份，乙方 贰 份。

甲方： 西安理工大学

（盖章）

法定代表人或授权代表：赵州平

通讯地址：西安市碑林区金花南路5 号

电　　话： 82312012

签订日期：2026年 3 月 24日

乙方： 陕西泓腾网络科技有限公司

（盖章）

法定代表人或授权代表：孙学梅

通讯地址： 陕西省西安市高新区唐延路 11 号 1 幢 32201 室

电　　话：17691347221

签订日期：2026年 3月 17 日

附件 1：

采购项目名称：网络安全体系建设项目（二期）

采购项目编号：【KRDL】K5-2510147-02

序号	标的名称	招标文件要求	投标产品技术参数	制造商家	规格型号	采购数量	单位
1	堡垒机【核心产品】	★标准机架式设备，冗余电源，数据存储容量≥4T，千兆光口≥2个，千兆电口≥4个。本次授权管理设备数≥300台，最大可管理设备数≥500台，最大字符并发数≥500个，最大图形并发数≥500个。	★无偏离，我司所投产品为1U标准机架式设备，冗余电源，数据存储容量4T，配置4个千兆光口，4个千兆电口。本次授权管理设备数300台，最大可管理设备数500台，最大字符并发数1000个，最大图形并发数500个。	北京神州绿盟科技有限公司	绿盟运维安全管理系统OSMSNX3-HD650	1	
2		支持基于角色的访问控制，可按部门、岗位、运维场景自定义角色权限，实现账号与运维人员的绑定，支持从AD/LDAP同步组织架构和用户；支持“最小权限原则”，权限粒度精确到“用户-设备-协议-操作命令”层级，授权策略，可按用户、用户组、目标设备、访问时间段、协议类型等进行组合授权；支持临时权限申请与审批流程（如工单审批），临时权限自动过期回收。	无偏离，我司所投产品支持基于角色的访问控制，可按部门、岗位、运维场景自定义角色权限，实现账号与运维人员的绑定，支持从AD/LDAP同步组织架构和用户；支持“最小权限原则”，权限粒度精确到“用户-设备-协议-操作命令”层级，授权策略，可按用户、用户组、目标设备、访问时间段、协议类型等进行组合授权；支持临时权限申请与审批流程（如工单审批），临时权限自动过期回收。				
3		▲支持本地静态密码、LDAP、短信、企微、钉钉等多种身份认证方式，含双因素认证，且通过运维隧道隔离，禁止运维客户端直接连接目标设备。	▲无偏离，我司所投产品支持本地静态密码、LDAP、短信、企微、钉钉等多种身份认证方式，含双因素认证，且通过运维隧道隔离，禁止运维客户端直接连接目标设备。				

4		支持通过浏览器页面H5方式发起运维操作；支持SSH、Telnet、Rlogin 、RDP、VNC、X11、FTP、SFTP、SCP、RZSZ等协议的操作行为。支持对Oracle(12c及以上)、MySQL(5.7及以上)、MicrosoftSQLServer(2016及以上)、DB2(11.1及以上)、PostgreSQL(10及以上)等数据库版本的访问行为审计。审计内容包含：所执行的SQL语句、SQL执行结果（成功/失败及返回数据）、操作时长等关键信息。	无偏离，我司所投产品支持通过浏览器页面H5方式发起运维操作；支持SSH、Telnet、Rlogin 、RDP、VNC、X11、FTP、SFTP、SCP、RZSZ等协议的操作行为。支持对Oracle(12c及以上)、MySQL(5.7及以上)、MicrosoftSQLServer(2016及以上)、DB2(11.1及以上)、PostgreSQL(10及以上)等数据库版本的访问行为审计。审计内容包含：所执行的SQL语句、SQL执行结果（成功/失败及返回数据）、操作时长等关键信息。				
5		支持全程完整记录所有键盘输入和回显内容，支持命令检索、违规命令实时阻断（如删除系统文件、禁用审计日志等操作）。支持全程录像，录像文件可回放、倍速播放、关键操作标记，可精确到秒级检索和播放等。	无偏离，我司所投产品支持全程完整记录所有键盘输入和回显内容，支持命令检索、违规命令实时阻断（如删除系统文件、禁用审计日志等操作）。支持全程录像，录像文件可回放、倍速播放、关键操作标记，可精确到秒级检索和播放等。				
6		支持水印的日志类型包括：数据库录屏日志中的水印，图形运维录屏日志中的水印，字符回放日志中的水印、应用发布运维的录屏日志中的水印。提供完整的操作日志、系统日志，支持关键字的全文检索和统计分析报表。所有操作日志支持日志导出（格式：CSV/PDF）和第三方日志平台（如SIEM）对	无偏离，我司所投产品支持水印的日志类型包括：数据库录屏日志中的水印，图形运维录屏日志中的水印，字符回放日志中的水印、应用发布运维的录屏日志中的水印。提供完整的操作日志、系统日志，支持关键字的全文检索和统计分析报表。所有操作日志支持日志导出（格式：CSV/PDF）和第三方日志平台（如SIEM）对接（支持Syslog/CEF				

		接（支持 Syslog/CEF 格式）。	格式）。				
7		▲支持 自动发现运维人员在运维过程中创建的后门账号行为，并以列表方式向设备管理员展示托管设备中所有的后门账号信息。支持 自动发现运维人员离职后遗留不用的僵尸账号，并以列表方式 向管理员展示托管设备中所有的僵尸账号，支持自定义未使用天数。	▲无偏离，我司所投产品支持 自动发现运维人员在运维过程中创建的后门账号行为，并以列表方式 向设备管理员展示托管设备 中所有的后门账号信息。支持自动发现运维人员离职后遗留不用的僵尸账号，并以列表方式 向管理员展示托管设备中所有的僵尸账号，支持自定义未使用天数。				
8		支持“一人一账号”绑定，禁止共享账号，记录账号全生命周期 日志。	无偏离，我司所投产品支持“一人一账号”绑定，禁止共享账号，记录账号全生命周期日志。				
9		支持 自定义 自动化脚本，可在线编辑和本地导入，支持 Windows 批处理脚本、WindowsPowerShell 脚本、LinuxShell 脚本、Python 脚本，支持设定任务为手动、定时和周期执行方式，支持登录后 自动执行脚本，执行完后堡垒机保存运维记录。	无偏离，我司所投产品支持自定义自动化脚本，可在线编辑和本地导入，支持 Windows 批处理脚本、WindowsPowerShell 脚本、LinuxShell 脚本、Python 脚本，支持设定任务为手动、定时和周期执行方式，支持登录后自动执行脚本，执行完后堡垒机保存运维记录。				
10		须具备由中国网络安全审查技术与认证中心颁发的网络关键设备和网络安全专用产品认证证书。	无偏离，我司所投产品具备由中国网络安全审查技术与认证中心颁发的网络关键设备和网络安全专用产品认证证书。				
11	零信任安全接入系统	★硬件及性能要求：标准机架式设备；内存容量≥16G，机械硬盘≥4T，固态硬盘≥128G，冗余电源，千兆电口≥6个、千兆光口≥4个。每秒并发连接数≥4000个，所投设备支	★无偏离，我司所投产品满足：硬件及性能要求：标准机架式设备；内存容量 16G，机械硬盘 4T，固态硬盘 128G，冗余电源，千兆电口 8 个、千兆光口 4 个、万兆光口 2 个。每秒并发连接数 4000 个，	深信服科技股份有限公司	aTrust-1000-B1050C	1	

		持并发用户数≥2000个，双向加密吞吐量≥1Gbps，配置2000个并发用户数的授权。	所投设备支持并发用户数2000个，双向加密吞吐量1Gbps，配置2000个并发用户数的授权。				
12		支持多因子认证功能，提供的认证方式应包括但不限于：静态口令、动态OTP、短信认证、企微/钉钉扫码认证、移动端协同认证等；对于移动端，还应支持指纹、人脸识别等生物识别认证方式；支持配置在触发异常环境的条件时，须完成增强认证才可登录。可配置的异常环境包括但不限于：账号首次登录、账号在该终端首次登录、账号在该地点首次登录、账号在新地点登录、账号在非常用地点登录、闲置账号登录、弱密码登录、异常时间登录等。	无偏离，我司所投产品支持多因子认证功能，提供的认证方式包括但不限于：静态口令、动态OTP、短信认证、企微/钉钉扫码认证、移动端协同认证等；对于移动端，还支持指纹、人脸识别等生物识别认证方式；支持配置在触发异常环境的条件时，须完成增强认证才可登录。可配置的异常环境包括但不限于：账号首次登录、账号在该终端首次登录、账号在该地点首次登录、账号在新地点登录、账号在非常用地点登录、闲置账号登录、弱密码登录、异常时间登录等。				
13		网络隐身与安全通信：支持网络隐身技术；支持双向TLS(mTLS)通信；支持智能链路选择和负载均衡。	无偏离，我司所投产品支持网络隐身与安全通信：支持网络隐身技术；支持双向TLS(mTLS)通信；支持智能链路选择和负载均衡。				
14		细粒度访问控制：支持基于应用、接口等多层级的细粒度访问控制。	无偏离，我司所投产品支持细粒度访问控制：支持基于应用、接口等多层级的细粒度访问控制。				
15		支持通过网络隐身、动态业务准入等机制实现可信访问，支持持续信任评估，一旦发现用户、设备或环境状态异常，可动态回收访问授权、实时阻断访问。	无偏离，我司所投产品支持通过网络隐身、动态业务准入等机制实现可信访问，支持持续信任评估，一旦发现用户、设备或环境状态异常，可动态回收访问授权、实时阻断访问。				

16		▲具备统一的策略决策点（策略引擎），能综合身份、设备、网络、应用等多个上下文源的信息进行实时风险评估与授权决策。提供可视化的策略编排界面，支持通过拖拽方式组合安全资产、访问条件、控制动作等元素，定义细粒度的访问控制策略。	▲无偏离，我司所投产品具备统一的策略决策点（策略引擎），能综合身份、设备、网络、应用等多个上下文源的信息进行实时风险评估与授权决策。提供可视化的策略编排界面，支持通过拖拽方式组合安全资产、访问条件、控制动作等元素，定义细粒度的访问控制策略。				
17		▲能自动发现通过隧道的应用流量，并基于规则对应用进行分类（如已知/未知应用）；支持基于多场景安全策略评估结果联动控制，如在Web应用访问场景中触发的安全策略评估结果，可以自动提供给用户登录场景进行调用。	▲无偏离，我司所投产品能自动发现通过隧道的应用流量，并基于规则对应用进行分类（如已知/未知应用）；支持基于多场景安全策略评估结果联动控制，如在Web应用访问场景中触发的安全策略评估结果，可以自动提供给用户登录场景进行调用。				
18		第三方系统集成：支持通过CAS、OAuth2.0、SAML等标准协议对接第三方IAM系统，实现与学校现有统一身份认证系统的单点登录对接。	无偏离，我司所投产品支持第三方系统集成：支持通过CAS、OAuth2.0、SAML等标准协议对接第三方IAM系统，实现与学校现有统一身份认证系统的单点登录对接。				
19		日志审计与分析：支持用户访问全周期多维日志审计（日志存储≥180天），包括但不限于：用户认证日志、WEB访问日志、客户端操作日志、终端安全日志。	无偏离，我司所投产品支持日志审计与分析：支持用户访问全周期多维日志审计（日志存储180天），包括但不限于：用户认证日志、WEB访问日志、客户端操作日志、终端安全日志。				
20		系统巡检：具备设备巡检功能，支持对设备自身的安全状态和策略配置进行巡检，并输出包含检测项、状态、问题描述及改进措施的	无偏离，我司所投产品支持系统巡检：具备设备巡检功能，支持对设备自身的安全状态和策略配置进行巡检，并输出包含检测项、状态、问题描述及				

		巡检报告。	改进措施的巡检报告。				
21		产品厂商具备中国网络安全审查技术与认证中心颁布的信息安全软件开发服务资质。	无偏离，我司所投产品厂商具备中国网络安全审查技术与认证中心颁布的信息安全软件开发服务资质。				
22	终端安全管理系统	★产品主要性能要求：管理平台 1 套，采用 B/S 架构，支持通过 HTTPS 方式登录管理控制台，支持一个管理控制台同时管理 Windows,Linux，信创操作系统，同时支持这些操作系统的服务器版和客户端版；服务器版授权点数≥300 点；终端授权点数≥50 点；	★无偏离，我司所投产品满足主要性能要求：管理平台 1 套，采用B/S 架构，支持通过 HTTPS 方式登录管理控制台，支持一个管理控制台同时管理 Windows,Linux，信创操作系统，同时支持这些操作系统的服务器版和客户端版；服务器版授权点数 300 点；终端授权点数 50 点；	深信服科技股份有限公司	深信服统一端点安全管理系统 V6.0（aES）	1	
23		▲具备勒索病毒防护能力，支持对勒索入侵的主流方式 RDP 爆破做全方位保护，支持展示勒索病毒处置情况，实时监控防止未授权加密及篡改；具备自动触发预篡改备份机制。	▲无偏离，我司所投产品具备勒索病毒防护能力，支持对勒索入侵的主流方式 RDP 爆破做全方位保护，支持展示勒索病毒处置情况，实时监控防止未授权加密及篡改；具备自动触发预篡改备份机制。				
24		▲支持基于威胁情报的云端联动机制。	▲无偏离，我司所投产品支持基于威胁情报的云端联动机制。				
25		支持用户普遍关心和危害程度高的威胁，提供专项检测和结果呈现，包括暴力破解、Shell 反弹、WebShell、PowerShell、本地提权、文档漏洞利用等。	无偏离，我司所投产品支持用户普遍关心和危害程度高的威胁，提供专项检测和结果呈现，包括暴力破解、Shell 反弹、WebShell、PowerShell、本地提权、文档漏洞利用等。				
26		支持病毒进程实时监控并处置，具备客户端本地病毒扫描查杀能力，可对病毒进行进程执行阻断、文件隔离/文件删除等操作，完整	无偏离，我司所投产品支持病毒进程实时监控并处置，具备客户端本地病毒扫描查杀能力，可对病毒进行进程执行阻断、文件隔离/文件删除等操				

		记录处置日志；支持病毒清除动作前备份功能。	作，完整记录处置日志；支持病毒清除动作前备份功能。				
27		支持自动化响应动作（网络封停、文件隔离、进程阻断）；支持自定义安全规则，包括合法登录规则、操作检测规则、IOA 进程检测规则、入侵检测白名单、失陷检测规则等。	无偏离，我司所投产品支持自动化响应动作（网络封停、文件隔离、进程阻断）；支持自定义安全规则，包括合法登录规则、操作检测规则、IOA 进程检测规则、入侵检测白名单、失陷检测规则等。				
28		支持 Windows 高危漏洞补丁免疫防御及批量一键修复；支持 Windows 环境下 C&C 可疑站点识别、恶意域名访问检测（可定位原始发起进程）；具备恶意行为监控能力，包括 Hosts 文件修改、安全策略修改、动态链接库注入、系统文件/进程/启动项修改、新启动程序等未知威胁的检测。	无偏离，我司所投产品支持 Windows 高危漏洞补丁免疫防御及批量一键修复；支持 Windows 环境下 C&C 可疑站点识别、恶意域名访问检测（可定位原始发起进程）；具备恶意行为监控能力，包括 Hosts 文件修改、安全策略修改、动态链接库注入、系统文件/进程/启动项修改、新启动程序等未知威胁的检测。				
29		集成至少 2 种独立杀毒引擎（本地引擎+云引擎），支持特征码查杀、启发式扫描、行为分析多维检测。病毒库更新：支持自动/手动更新，云引擎病毒库更新频率≤1 小时，本地引擎离线病毒库有效期≥7 天。查杀能力：对勒索病毒、木马、蠕虫、挖矿程序等恶意软件的检出率≥99%（提供近 6 个月第三方测评报告或公开检测数据）。	无偏离，我司所投产品集成 2 种独立杀毒引擎（本地引擎 + 云引擎），支持特征码查杀、启发式扫描、行为分析多维检测。病毒库更新：支持自动/手动更新，云引擎病毒库更新频率≤1 小时，本地引擎离线病毒库有效期≥7 天。查杀能力：对勒索病毒、木马、蠕虫、挖矿程序等恶意软件的检出率≥99%（已提供近 6 个月第三方测评报告）。				
30		具备 IOC 检测能力，支持的威胁类型包括但不限于：远控、钓鱼、僵尸网络、矿池地址、	无偏离，我司所投产品具备 IOC 检测能力，支持的威胁类型包括但不限于：远控、钓鱼、僵尸网络、				

		挖矿木马、勒索软件、窃密木马、远控木马、网络蠕虫、APT 攻击事件等恶意软件行为。	矿池地址、挖矿木马、勒索软件、窃密木马、远控木马、网络蠕虫、APT 攻击事件等恶意软件行为。				
31		支持全资产清点，（操作系统、应用软件、端口、账户等）。支持全网风险展示，包括未处理勒索病毒数量、暴力破解数量、WebShell 后门数量、高危漏洞等危险项及影响的终端数量。	无偏离，我司所投产品支持全资产清点，（操作系统、应用软件、端口、账户等）。支持全网风险展示，包括未处理勒索病毒数量、暴力破解数量、WebShell 后门数量、高危漏洞等危险项及影响的终端数量。				
32		提供三年软件升级，三年规则库升级。（提供承诺函，承诺函格式自拟）	无偏离，我司所投提供三年软件升级，三年规则库升级。（已提供承诺函）				
33		产品厂商具备中国网络安全审查技术与认证中心颁发的软件安全开发类安全服务证书资质。	无偏离，我司所投产品厂商具备中国网络安全审查技术与认证中心颁发的软件安全开发类安全服务证书资质。				
34	网络流量汇聚分流器	★硬件及性能参数：标准机架式设备；具备 100GE/40GE 自适应接口，数量≥4 个；10GE 接口数量≥24 个；设备吞吐量：≥500Gbps；时延要求≤1ms，时延抖动≤1ms；具备 1 个 100/1000Mbps 管理网络交换口等；双路冗余电源。	无偏离，我司所供型号 NGTAP-24X-100PRO 为标准机架式设备，具备 100GE/40GE 自适应接口，数量≥4 个；10GE 接口数量≥24 个；设备吞吐量：≥500 Gbps，满足时延要求≤1ms，时延抖动≤1ms；具备 1 个 100/1000Mbps 管理网络交换口等；双路冗余电源。	北京派网软件有限公司	24X-100PRO	1	
35		▲流量过滤/编排及规则数量：具备流量过滤及去重功能，包含源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议号、物理端口号、VLAN、T CPflag，以及上述条件的任意组合；支持配置≥2000 条规则。	无偏离，我司所供产品具备流量过滤及去重功能，包含源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议号、物理端口号、VLAN 、TCP flag，以及上述条件的任意组合，最大支持 65535 条规则。				

36		支持多种报文的识别及过滤分发，包括IPv4、IPv6、L2TP、GTP、IPSe c、PPTP、ICMP、GRE、TCP/UDP/SCTP 报文等。	无偏离，我司所供产品支持多种报文的识别及过滤分发，包括 IPv4、IPv6、L2TP、GTP、IPSec、PPTP、ICMP、GRE、TCP/UDP/SCTP 报文等。				
37		支持流量的汇聚与分流。	无偏离，我司所供产品具备流量的汇聚与分流功能。				
38		转发功能：支持特定流量进行数据的丢弃和转发功能，对未匹配流量进行输出。	无偏离，我司所供产品具备特定流量进行数据的丢弃和转发功能，对未匹配流量进行输出。				
39		失效保护：支持端口失效保护，在某个输出端口故障 Linkdown 时自动负载分担到其他输出端口。	无偏离，我司所供产品具备端口失效保护，在某个输出端口故障 Link down 时自动负载分担到其他输出端口。				
40		▲支持按物理端口添加 VLANTag，并且可以自定义，支持 4000 个以上自定义 VLAN 标签。同时，支持对链路上数据包的VLAN 进行剥离。	无偏离，我司所供产品具备按物理端口添加 VLAN Tag，并且可以自定义，支持 4000 个以上自定义 VLAN 标签。同时，支持对链路上数据包的 VLAN 进行剥离。				
41		支持 WEB 页面管理、命令行管理和 SNMP 管理。支持 Console、Telnet、SSH 的模式实现配置管理	无偏离，我司所供产品具备 WEB 页面管理、命令行管理和 SNMP 管理。支持 Console、Telnet、SSH 的模式实现配置管理。				
42		支持存储包括 SYSLOG 服务器日志各种运行日志及管理员操作日志；支持基于 NTP 协议的时钟同步管理；支持 SNMP 管理和 trap 告警；支持用户分级管理、密码定期更新提示；支持本地认证、Radius/TACACS+、LDAP 等多种登录认证鉴别技术，对登录用户进行身份鉴别。	无偏离，我司所供产品具备存储包括 SYSLOG 服务器日志各种运行日志及管理员操作日志；支持基于 NTP 协议的时钟同步管理；支持SNMP 管理和trap 告警；支持用户分级管理、密码定期更新提示；支持本地认证、Radius/TACACS+、LDAP 等多种登录认证鉴别技术，对登录用户进行身份鉴别。				

43	安全MSS服务	▲为不少于 100 个核心资产（数据中心资产IP数量）提供全年7*24小时连续性的安全保障，服务期一年，自项目整体验收合格之日起算。配置一名具有3年及以上网络安全从业经验的专属服务经理，组建专属服务响应群，实时响应安全咨询的需求。	▲无偏离，我司所投服务为不少于100个核心资产（数据中心资产IP数量）提供全年7*24小时连续性的安全保障，服务期一年，自项目整体验收合格之日起算。配置一名具有3年及以上网络安全从业经验的专属服务经理，组建专属服务响应群，实时响应安全咨询的需求。	深信服科技股份有限公司	安全托管服务MSS-100	1	
44		▲提供不低于以下的SLA承诺：（1）一般事件：日志产生到事件通告≤1小时、遏制影响时间≤4小时；（2）重大事件：日志产生到事件通告(MTTD)≤30分钟、遏制影响时间≤1小时；（3）一般威胁：日志产生到威胁通告≤2小时、遏制影响时间≤4小时；（4）重大威胁：日志产生到通告(MTTD)≤1小时、响应处置时间(MTTR)≤1小时；（5）应急响应：重大事件工作时间内应在15分钟之内进行响应，非工作时间30分钟之内进行响应，2小时上门处置或远程联动响应。	▲无偏离，我司所投服务提供以下的SLA承诺：（1）一般事件：日志产生到事件通告≤1小时、遏制影响时间≤4小时；（2）重大事件：日志产生到事件通告(MTTD)≤30分钟、遏制影响时间≤1小时；（3）一般威胁：日志产生到威胁通告≤2小时、遏制影响时间≤4小时；（4）重大威胁：日志产生到通告(MTTD)≤1小时、响应处置时间(MTTR)≤1小时；（5）应急响应：重大事件工作时间内应在15分钟之内进行响应，非工作时间30分钟之内进行响应，2小时上门处置或远程联动响应。				
45		安全现状评估：对业务系统及Web资产开展漏洞扫描，覆盖操作系统、数据库、常见应用/协议及Web通用漏洞。同时开展弱口令检测，检测范围包括SMB、MicrosoftSQLServer、	无偏离，我司所投服务提供安全现状评估：对业务系统及Web资产开展漏洞扫描，覆盖操作系统、数据库、常见应用/协议及Web通用漏洞。同时开展弱口令检测，检测范围包括SMB、Microsoft SQL Server、MySQL、Oracle、				

		MySQL、Oracle、SMTP、VNC、FTP、Telnet、SSH、Tomcat 等常见服务与应用。	SMTP、VNC、FTP、Telnet、SSH、Tomcat 等常见服务与应用。				
46		脆弱性管理：对系统漏洞和 Web 漏洞开展全量扫描及真实性验证，分析漏洞危害并输出可落地修复方案；通过工单跟踪修复闭环。对服务范围内的高危可利用漏洞提供防护建议并提供承诺函。	无偏离，我司所投服务提供脆弱性管理：对系统漏洞和 Web 漏洞开展全量扫描及真实性验证，分析漏洞危害并输出可落地修复方案；通过工单跟踪修复闭环。对服务范围内的高危可利用漏洞提供防护建议，已提供承诺函。				
47		安全问题处置：提供 7*24 小时威胁分析和鉴定服务，依托威胁检测能力，实时监测用户网络安全状态，对安全告警进行分析研判，生成处置工单，并定位真实威胁。	无偏离，我司所投服务提供安全问题处置：提供 7*24 小时威胁分析和鉴定服务，依托威胁检测能力，实时监测用户网络安全状态，对安全告警进行分析研判，生成处置工单，并定位真实威胁。				
48		服务要求：能提供服务成果的相关展示；至少包括具备服务质量的可视化展示，至少包括脆弱性/威胁/事件闭环率、平均响应时长、平均闭环时长等指标，以验证 SLA 达成情况。	无偏离，我司所投服务满足要求：能提供服务成果的相关展示；至少包括具备服务质量的可视化展示，至少包括脆弱性/威胁/事件闭环率、平均响应时长、平均闭环时长等指标，以验证 SLA 达成情况。				
49		服务交付物：服务期内，提供以下汇报材料和内容：包括但不限于《项目启动会 PPT》、《首次分析与处置报告》、《漏洞管理举证报告》、《漏洞清单》、《服务资产表》、《安全服务运营报告》、《应急响应报告》、《事件分析与处置报告》、《安全运营报告》、《安全通告》、《综合分析报告》、《季度汇报 PPT》、	无偏离，我司所投服务交付物满足：服务期内，提供以下汇报材料和内容：包括但不限于《项目启动会 PPT》、《首次分析与处置报告》、《漏洞管理举证报告》、《漏洞清单》、《服务资产表》、《安全服务运营报告》、《应急响应报告》、《事件分析与处置报告》、《安全运营报告》、《安全通告》、《综合分析报告》、《季度汇报 PPT》、《年度汇				

		《年度汇报 PPT》等。	报 PPT》等。				
50		★提供每周不少于 2 天的线下驻场服务，驻场人员具备网络安全监测、威胁分析、应急响应等能力，人员相对固定（调整人员须提前报采购人审批）。通过线上线下相结合的值班制度、轮班及应急增援预案，实现 7*24 小时的安全监控与响应。	★无偏离，我司所投服务提供每周不少于 2 天的线下驻场服务，驻场人员具备网络安全监测、威胁分析、应急响应等能力，人员相对固定（调整人员须提前报采购人审批）。通过线上线下相结合的值班制度、轮班及应急增援预案，实现 7*24 小时的安全监控与响应。				
51		配合网络安全宣传活动，（含讲座、素材的支撑）。每半年开展一次面向全校师生开展网络安全培训（须覆盖不同层级受众，采用案例分析等形式）培训后提供总结报告（参与情况及反馈优化建议）	无偏离，我司所投服务支持配合网络安全宣传活动，（含讲座、素材的支撑）。每半年开展一次面向全校师生开展网络安全培训（覆盖不同层级受众，采用案例分析等形式）培训后提供总结报告（参与情况及反馈优化建议）				
52		重保时期（上级部门指定/采购人通知的特殊保障时段）：根据需求增配驻场人员，提供 7×24 小时值守服务，制定专属《重保安全保障方案》。重保时期前两周完成漏洞检查、设备巡检、安全加固，保障期间每日输出《运营日报》，保障结束后输出《总结报告》。	无偏离，我司所投服务满足重保时期（上级部门指定/采购人通知的特殊保障时段）：根据需求增配驻场人员，提供 7×24 小时值守服务，制定专属《重保安全保障方案》。重保时期前两周完成漏洞检查、设备巡检、安全加固，保障期间每日输出《运营日报》，保障结束后输出《总结报告》。				
53		每季度开展资产进行指纹检测（涵盖操作系统、中间件、软件厂商等），并更新信息，保障资产指纹信息的准确性。每季度对资产进行存活性探测，对未存活/变更资产进行更新，保障资产信息的全面性。	无偏离，我司所投服务支持每季度开展资产进行指纹检测（涵盖操作系统、中间件、软件厂商等），并更新信息，保障资产指纹信息的准确性。每季度对资产进行存活性探测，对未存活/变更资产进行更新，保障资产信息的全面性。				

附件 2：安全 MSS 服务内容

第一条 服务概述与范围

1、服务目标：为甲方不少于 100 个核心数据中心资产（以 IP 地址计）提供为期一年的全天候（7*24 小时）网络安全运营保障服务；安全 MSS 服务自验收合格之日起服务期为 1 年。

2、服务团队：

（1） 乙方须配置一名具备3 年及以上网络安全从业经验的专属服务经理，作为单一联络点。

（2） 组建涵盖必要技术人员的专属服务响应群，用于实时响应甲方的安全咨询与服务请求。

第二条 服务等级协议

1、乙方承诺不低于以下服务等级标准：

事件/威胁类别	从日志产生到首次通告时间	遏制影响/响应处置时间
一般安全事件	≤ 1 小时	≤ 4 小时
重大安全事件	≤ 30 分钟	≤ 1 小时
一般安全威胁	≤ 2 小时	≤ 4 小时
重大安全威胁	≤ 1 小时	≤ 1 小时
应急响应	工作时间 15 分钟内，非工作时间 30 分钟内启动响应流程。	2 小时内提供上门处置或启动有效远程联动响应。

2、关键系统可用性：乙方用于提供监控、分析和管理的安全运营平台，其服务可用性应不低于 99.9%。

3、漏洞管理 SLA：对于扫描发现的高危漏洞，乙方应在报告中提供修复优先级建议，并对标记为“紧急”的漏洞提供 7 日内的修复跟踪与技术支持。

第三条 具体服务内容与要求

一、安全现状评估

1、对甲方指定业务系统及Web 资产进行全面漏洞扫描，覆盖操作系统、数据库、常见应用/协议及Web 通用漏洞。

2、开展弱口令专项检测，范围须包括但不限于：SMB、Microsoft SQL Server、MySQL、Oracle、SMTP、VNC、FTP、Telnet、SSH、Tomcat 等服务与应用。

二、持续性安全运营

1、脆弱性管理

(1) 定期对系统漏洞和Web 漏洞进行全量扫描，并对高危漏洞进行真实性验证。

(2) 提供包含漏洞危害分析、可落地修复方案的技术报告。

(3) 通过工单系统跟踪并推动漏洞修复闭环。

(4) 对服务范围内确认的高危、可利用漏洞，须提供临时的防护加固建议，并以书面承诺函形式提交甲方确认。

2、安全问题处置

(1) 提供 7*24 小时安全告警监测、威胁分析与鉴定服务。

(2) 对安全告警进行分析研判，生成处置工单，定位真实威胁，并推动处置闭环。

3、资产动态管理

(1) 每季度开展一次资产指纹信息检测，涵盖操作系统、中间件、软件厂商及版本等，更新《资产指纹信息表》，确保资产信息的准确性。

(2) 每季度对所有已识别资产进行存活性探测，更新《服务资产表》，对未存活或发生变更的资产进行标注，确保资产清单的全面性。

4、常态化驻场与响应

(1) 提供每周不少于2 天的固定线下驻场服务。

(2) 驻场人员须具备网络安全监测、威胁分析、应急响应等能力，且人员应相对固定。如需调整，须提前至少5 个工作日向甲方提交书面申请，获得甲方书面批准后方可执行。

(3) 通过线上线下结合的值班与轮班制度，确保 7*24 小时安全监控与响应能力。

5、专项服务重要时期保障

(1) 在甲方通知的特殊保障时段，乙方应根据甲方需求增配驻场人员。

(2) 保障开始前两周，制定并向甲方提交《重保安全保障方案》，完成漏洞检查、设备巡检与安全加固。

(3) 保障期间，每 日向甲方输出《重保运营日报》。

(4) 保障结束后 5 个工作日内，向甲方提交《重保总结报告》。

6、安全宣传与培训

(1) 配合甲方开展网络安全宣传活动，提供必要的讲座与素材支持。

(2) 每半年开展一次面向甲方指定受众（如全校师生）的网络安全培训，内容须采用案例分析等形式，并覆盖不同层级受众。每次培训后向甲方提供包含参与情况及反馈优化建议的《培训总结报告》。

第四条 服务过程与成果可视化

1、乙方须提供专用的服务成果可视化平台或定期报告，用于向甲方展示服务质量。

2、展示指标至少须包括：脆弱性闭环率、威胁处置闭环率、安全事件闭环率、平均响应时长、平均处置闭环时长等。

第五条 服务交付物清单

服务期内，乙方须按以下时间及频度要求向甲方提交交付物：

交付物名称	频度/时间要求	备注
《项目启动会材料》	服务启动后 5 个工作日内	含会议 PPT、会议纪要等。
《首次安全分析与处置报告》	服务启动后 1 个月内	
《漏洞管理举证报告》及《漏洞清单》	按月度/季度	详列漏洞详情、修复状态、闭环证明。
《服务资产表》	每季度更新	反映资产存活及指纹信息变更。
《安全服务运营报告》	按月/季度	涵盖运营数据、SLA 达成分析、事件分析等。
《应急响应报告》/《事件处置报告》	事件处置结束后2 个工作日内	
《安全通告》	发生重大漏洞或威胁时	紧急通告应在 12 小时内发出。
《季度汇报 PPT》	每季度结束后 10 个工作日内	
《年度汇报 PPT》及《综合分析报告》	服务结束前 15 个工作日内	
《重保安全保障方案》	重保开始前 10 个工作日	
《重保运营日报》	保障期间每日	

交付物名称	频度/时间要求	备注
《重保总结报告》	保障结束后 5 个工作日内	
《培训总结报告》	每次培训后 5 个工作日内	