南理工法字（信息）【2022】第0019号总第0705号

南阳理工学院威胁分析与响应服务平台建设项目采购合同

甲方：南阳理工学院

乙方：郑州顺腾科技有限公司

根据《中华人民共和国政府采购法》和《中华人民共和国民法典》，项目编号：南阳政采公开-2022-49 名称：南阳理工学院威胁分析与响应服务平台建设项目的中标通知书、招标文件、投标方投标文件的要求，经甲、乙双方协商，本着平等自愿、诚实信用的原则，签订本合同并遵守以下条款：

一、采购产品的名称、商标、型号、制造厂商、数量、金额、交货时间

1、合同总价：RMB 926000 元整（玖拾贰万陆仟元整）。

2、采购清单及具体要求详见附件（乙方投标文件投标报价一览表）。

3、交货时间：合同签订之日起 15 日历天内供货安装调试完毕。

注：合同总价为包含设备硬件、预装软件、运输、保险、安装调试、售后服务、培训等一切费用在内的南阳市范围内规定的地点交货价，该价在合同履行期间固定不变。

二、货物产地及标准

1、货物为全新的产品，表面无划伤、无碰撞，无任何缺陷。

2、标准

本合同所指的货物应符合招标文件要求、乙方投标产品所列出的配置、技术参数及各项要求，同时应符合中华人民共和国国家质量及国家安全环保标准。

3、国内制造的产品必须具备出厂合格证。

4、乙方应将所供产品的用户手册、保修手册、有关资料及配件、备品备件、随机工具等交付给甲方，甲方须知的重要资料应附有中文说明。

三、交货方式、交货地点、安装与调试

货物由乙方送货至甲方指定的地点，并负责安装与调试至甲方认可的最佳状态，

甲方不承担设备安装、调试费用。

四、包装

乙方交付的货物应为制造商原厂包装，包装箱号与设备出厂批号一致。

五、验收方式、质量保证期及售后服务要求

1、验收时，乙方须提供合同约定产品中甲方指定产品的质量检测报告，质量检测报告应由地市级及以上国家质量技术管理部门出具。

2、甲乙双方以本合同约定的产品技术参数、配置、安装为标准进行验收，验收合格后由甲方签署验收证明文件。

3、货物质量保证期和免费维修期根据乙方在投标文件中的承诺和原装产品生产厂家的保质期承诺，质保期为叁年。质量保证期和免费维修期内，乙方对建设项目及采购产品无条件包修、包换、包退。

4、质量保证期内，整机或零部件非人为因素不能使用而更换部分的质量保证期和免费维修期相应延长。

5、乙方负责向甲方提供现场操作及维修保养方面的培训。

六、付款方式

甲方验收项目合格后，乙方开具符合甲方财务要求的增值税专用发票，甲方于乙方开具发票且具备付款条件之日起5日内付清乙方全部费用。

七、违约责任

1、乙方不能按本合同规定的时间交付并安装完成的，或在合同规定的时间内（包括安装、调试）达不到验收标准的，乙方须向甲方支付本合同总价5%的违约金。

2、乙方不能按本合同规定的时间交付并安装完成的，或在合同规定的交货时间内（包括安装、调试）达不到验收标准的，除乙方按照第七款第1条交纳违约金外，从逾期之日起乙方需另外每日按本合同总价2‰的数额向采购单位支付违约金；逾期十五天以上的，甲方有权终止合同，由此造成的甲方经济损失由乙方承担。

3、验收时，甲方如发现乙方交付的产品品种、型号、规格、质量一项或多项不符合合同约定的产品技术参数、配置等，除乙方按照第七款第1条及第2条交纳违约金外，乙方已交付的货物由甲方存留，直至在规定的时间内交付合同约定的产品，并达

到验收标准；规定的时间到后，乙方交付的货物仍未达到合同约定的，甲方终止合同。

4、乙方不按其售后服务承诺响应甲方的服务请求的，乙方须向甲方支付合同总价5%的违约金。

5、甲方不按合同规定接收货物，或无正当理由不按政府采购办的要求办理结算手续的，甲方须向乙方支付本合同总价5%的违约金。

八、提出异议的时间和方法

1、甲方在验收中如发现货物的品种、型号、规格、质量不符合约定的，应在妥善保管货物的同时，合理期间向乙方提出书面异议。

2、乙方在接到甲方书面异议后，应在24小时内作出处理并予以书面说明；否则，即视为乙方默认了甲方提出的异议。

3、甲方因违章操作、保管保养不善等自身因素造成质量问题的，不得提出异议。

九、不可抗力

任何一方由于不可抗力原因无法履行合同时，应在不可抗力事件结束后 1 天内向对方通报，以减轻可能给对方造成的损失；在取得有关机构的不可抗力证明或双方谅解确认后，允许延期履行或修订合同，并视情况免于承担部分或全部的违约责任。

十、争议的解决

1、如甲、乙双方出现争议尽可能协商解决，如协商不成，可向南阳市有管辖权的人民法院起诉。

2、因货物质量问题发生的争议，统一由南阳市质量技术监督局鉴定，其鉴定为最终鉴定。货物符合质量技术标准的，鉴定费由甲方承担；货物不符合质量技术标准的，鉴定费由乙方承担。

十一、其它

1、合同所有附件均为合同的有效组成部分，与合同具有同等的法律效力。合同附件包括：南阳理工学院威胁分析与响应服务平台建设项目的招标文件、乙方投标文件及招标过程中形成的其他文件。

2、本合同经甲乙双方法人代表或授权代理人签字盖章之日起生效。

3、本合同一式柒份：甲方持有伍份，乙方持有贰份。均具有同等法律效力。

甲方：（公章）

授权代理人：

日期：2022.7.26

地址：河南省南阳市长江路 80 号

电话：0377-62075392

传真：

甲方开户行：南阳市农行理工学院支行

甲方账号：1670 5601 0400 00013

甲方账号名称：南阳理工学院

甲方统一社会信用代码：124113004190374430

乙方：（公章）

法定代表人(授权代理人)：张俊伟

日期：2022.7.26

地址： 郑州市金水区福元路157号12号楼24层2404号

乙方手机：15981988896

传真：037185966278

乙方开户行：中国银行股份有限公司郑州银基王朝支行

乙方账号：246845025389

乙方账号名称：郑州顺腾科技有限公司

乙方统一社会信用代码：91410105MA3X6A2N3J

企业规模：微企业 小企业 中型企业 大型企业（请在相对应选项划 √）

南阳理工学院威胁分析与响应服务平台建设项目建设标准

序号	产品名称	技术要求	数量	单价／万	合计／万
1	网站监测与风险扫描系统	**安恒 DAS-WSM-A3760** 1、2U 机架式，每颗 CPU 10 核，物理内存 64G，2 电口、4 光口，冗余 1+1 电源模块,配备 4 个千兆多模 SFP 光纤模块。 2、扫描对接：系统的监测引擎能力可以对大批量网络资产进行监测扫描，扫描结果与信息安全调度平台进行数据对接。 3、联动：实现与学校校园网网站防火墙 WAF、资源统一管理平台等网络设备的对接联动。 3、开放数据接口，支持提供对外 Open API，扫描的结果可通过 API/kafka 形式提供给学校第三方大数据平台。 4、提供 web 漏洞扫描、主机漏洞扫描、弱口令扫描、安全事件扫描和内容风险扫描。 5、提供暗链监测功能，帮助学校快速的确认和处理漏洞。支持 web 漏洞扫描结果提示功能，可帮助学校快速的确认和处理漏洞。	1 套	23	23

郑州顺腾科技有限公司 合同专用章 4101034928737

		6、支持对安全事件进行扫描监测，包括暗链、挂马、黑页、挖矿脚本、webshell、坏链等，支持自定义设置扫描层数。可设定专用引擎进行 nDay 漏洞的自动检测，支持对特定单位资产在特定时间段进行扫描检测。支持对网页内容进行扫描监测，包括外链、身份证信息泄露、黄赌毒等不良信息、敏感内容、错别字等等。 7、支持快速模式、智能模式、标准模式、深度模式扫描，不同的扫描模式扫描的深度、扫描内容不一样；智能扫描模式可以支持扫描的 web、暗链和不良事件提示。 8、一键巡检，一键检查项包含但不限于数据健康、探针健康检查、大数据集群健康、Elasticsearch 健康、实时流计算引擎健康、管理服务健康、服务器节点健康等多种维度检查，并能提供处置建议，一键导出各类服务的故障日志，包括但不限于 Elasticsearch、Logstash、Kafka、实时计算引擎、操作系统等。 9、处置对接：要求系统开放数据接口，并实现与校园网现有校园网智能安全管理平台实现定制对接，实现一键告警与处置，达到数据共享与交换。 10、提供灵活的账户管理体系，除系统默认的管理员、审计员等角色外，还可自定义用户角色，指定菜单和功能权限。支持对内网资产、外网资产、云端资产、云端			

		VPC 资产的扫描，可通过一个平台，多个扫描引擎统一展示扫描结果。 11、支持使用用户自己部署的节点进行扫描，当用户节点扫描能力不足时，支持使用云端扫描引擎进行扫描，扫描结果可以在本地系统统一查看。业务平台和引擎中台解耦，既支持用户通过平台扫描资产及资产弱点，也支持用户基于引擎中台自己开发业务平台。 12、系统平台可实现资产、人员、部门的关联，能快速定位风险和相关联系人，并进行短信、邮件、钉钉群等多途径及时告知。 售后服务支持：提供 5 年免费升级维护；提供安装调试后 1 天在线操作培训；提供 24 小时支持热线；本地应急响应时间<=2 小时。			
2	安全运维服务与攻防演练	**安恒安全运维服务与攻防演练** （1）提供 1 年专职云端安全事件管理服务与每月不少于 2 周的现场值守服务，及时发现网络中对目标资产的网络攻击与威胁，由安全运营团队进行进一步的人工溯源分析；完善学校的整体信息化安全监测和保障体系， 提供专业的网络信息安全相关设备及运维服务，至少包含安全巡检、网络及信息系统的网络信息安全监控分析、安全扫描、主机防护、策略优化、 渗透测试、应急响应	1 项	17	17

		等。针对学校业务系统、接入网络、业务数据等实施安全保障，及时向学校汇报系统安全隐患与整改建议，按要求完成相应的安全控制，在密码管理、安全策略、漏洞扫描、网络分析等方面做好安全防护运维与协助工作。工作时段与非工作时段均需提供 7×24 小时的报障受理。 （2）巡检要求：对校园网内安全设备进行巡检，及时发现采购单位信息系统存在的隐患与安全漏洞，并与学校共同解决存在的问题与隐患，包括但不限于主要工作内容包括：突发事件相关信息的收集、事件的分析、报告提交、问题解决建议等。 （3）风险评估；按照教育行业网络安全基线安全规范要求对系统进行核查，出具核查报告。对当年新上线信息系统进行安全检测，检测内容包括但不限于：操作系统安全漏洞、物理环境、应用软件、安全配置等。至少每月一次，从漏洞、配置弱点两个维度发现资产的脆弱性，包括漏洞的脆弱性和配置暴露的脆弱性。 （4）渗透性测试服务：对学校相关业务系统进行渗透测试，包括本地和远程渗透测试，要求完成对学校所有业务系统的人工渗透测试，并给出详细的渗透测试报告；根据渗透测试结果进行安全加固，并在加固过程中对疑			

		难问题进行解答。当完成加固后，各潜在服务供应商针对加固成果进行复核测试。安全服务期内新上线业务系统以及系统更新后做增量测试；常备自动化渗透测试平台，此项需提供工具平台快速测试、漏洞验证、钓鱼类社会工程学攻击、暴力破解等功能界面； （5）安全分析服务：对信息系统定期检测（工具扫描及安全专家人工检测），及时发现信息系统（网络架构、网络设备、服务器主机、操作系统、数据库和用户账号、口令等安全对象）存在的各种安全隐患，提出系统加固建议以及相关的应急措施。同时对相关服务系统与安全产品进行日志分析，为用户量身定制可读性强的专业报告，并针对报告中提出的问题提供修补建议。另外关注教育行业的安全动态，对于新出现的安全风险事件，提早做出预防措施。 （6）无线安全评估：对开放的无线网络进行安全检测，模拟黑客攻击，全面深度测试。 （7）关键时期安全保障服务：为确保客户在重保期间业务系统持续、稳定的运行，确保重要业务操作行为的可审计，抵御黑客、恶意代码、病毒等对用户信息系统的攻击与破坏，防止对用户信息系统的非法、非授权访问、恶意篡改、挂马等等，在重大活动时期（两会、国庆等）， 合同专用章			

		通过派遣专业工程师开展安全检查、驻场保障以及应急值守等，对客户重要系统进行安全保障。 （8）应急响应：根据事件类别，提供全年的应急响应服务，通过远程和现场支持的形式协助客户对遇到的突发性安全事件进行紧急分析和处理。紧急事件主要包括：勒索病毒、病毒和蠕虫事件、黑客入侵事件、数据泄露、挖矿事件等。 （9）安全通告处置服务：提供最新的安全咨询信息，包括安全漏洞和补丁，在出现高危漏洞和突发重要事件时，将提供相应的紧急安全事件通告，内容将包含测试方法、影响范围、修复建议等内容。其内容来自各主流厂商、安全研究组织以及信息安全研究团队所提供的安全漏洞信息、安全新闻、安全研究报告等。 （10）提供1个教育系统网络安全保障专业人员ECSP培训名额，含报名费，考试费以及培训费等费用。 **攻防演练：** （1）提供2022年南阳理工学院网络安全应急演练服务。演练类型为实战演练，在学校网络管理中心搭建专用的网络环境并配以充足的攻击资源，组织由3支攻击团队（每支团队不少于2人，时间不少于7天），协同各个二级单位作为防守方参与的大规模网络安全应急演练。			

		（2）搭建演练监控指挥平台，保障演练过程中落实“全程监控、全程审计、全程录屏、全程录像”的安全管控措施，确保被攻击目标系统业务不停顿、数据不泄露、信息不窃取。攻防演练应急指挥平台包括后台管理系统、攻击方系统、可视化展示子系统和视频监控系统。 （3）演练汇报准备，对演练过程进行选材编辑，制作成不少于30分钟左右的视频，做好各项汇报准备工作。邀请有关领导，利用实际场景和视频，进行演练汇报。对演练进行全面总结，形成专报上报。			
3	流量分析系统	**安恒 DAS-ABL-SP46000** 1、2U标准机架式设备，1+1冗余电源；吞吐率：20G；千兆RJ45网口*2、千兆RJ45网口*4、千兆业务SFP光口*4、万兆SFP光口*2（配备6个千兆多模SFP光纤模块，2个万兆多模SFP光纤模块）。 2、高可用性与对接要求：与学校使用的信息安全调度平台对接实现处置同步，达到处置与安全闭环；支持根据添加探测器情况，自定义探测器名称、发送时间、发送目录等信息，并可显示不同探测器的IP、版本、状态和最近24小时的风险信息。 3、敏感信息识别：实现对关键字、数据来源等的自定义，通过内容深度匹配流量中的敏感信息，并对敏感信息快	1套	30	30

		速定位，实现对敏感信息访问行为的有效监测。 4、支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、同步验证、信息收集等功能。 5、数据对接定制：实现与校园网智能安全平台告警数据对接融合，并将结果统一管理，以便于漏洞信息的及时发现和预警处理；支持 kafka、短信、邮件、syslog、ftp、钉钉等告警方式，支持对 kafka、syslog 发送的风险信息进行 AES 加密。 6、加密流量解析：支持对 HTTPS 流量的解析还原；流量代理分析：处理和分析第三方接入流量，满足用户对其他平台流量无法分析溯源需求。 7、数据库关联告警对接定制：自动关联行为分析的详细展现，包含 SQL 注入取数据、表单破解、XSS 测试、目录穿越读取文件等。支持实现基于恶意数据库操作语句的关联告警。 8、可以实现对接威胁情报中心，支持离线和在线两种情报更新方式，支持原始告警与学院原有威胁情报碰撞检测并展示威胁情报命中告警数量； 9、具备流量威胁深度检测能力，支持异常会话检测、WEB 攻击检测、挖矿行为检测、僵木蠕检测、Webshell 文件			

		检测、异常文件检测、漏洞利用检测、DoS 攻击检测、扫描行为检测、配置风险检测、异常登录检测、横向移动检测、违规访问检测等；具备流量协议内容深度还原。 10、提供 24 小时支持热线；5 年软硬件免费升级；本地应急响应时间<=2 小时。			
4	NAT 日志管理系统	**山石 SG-6000-HSA-10D** 1、基于简化维护管理成本考虑，要求设备形态须采用专用独立的硬件服务器形态；存储容量≥16TB， 提供≥4 个 10/100/1000M 自适应电口用于管理和日志接收。 2、硬件参数：2U 机架设备，2 颗物理 CPU,内存 32G，系统存储 SSD240G，存储容量 16TB，4 个千兆口，1+1 冗余电源。 3、能够无缝对接出口防火墙 NAT 日志,满足 180 天 NAT 日志存储 支持记录详细 NAT 日志信息（包括时间、源地址、目的地 址、端口以及转换后地址等元素），日志处理速度≥10 万 EPS。 4、与学校现有上网身份认证系统无缝对接。 5、3 年软硬件免费升级；本地应急响应时间<=2 小时。	1 套	11.6	11.6
5	关联分析系统	**安恒 DAS-ABL-SER60** 1、2U 机架式，双电源，配置 4 个工作管理口；内存 64GB；	1 套	11	11

		硬盘 16T。（配 2 个多模 SFP 光纤模块），1 个 console 口。 2、定制要求：支持基于跨设备的多事件关联分析；支持识别出口防火墙解析私有协议二进制日志的定制，支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件；进行关联分析的规则可定制。 3、与学校现有网络安全平台实现无缝对接。 4、数据对接同步：支持和原有堡垒机进行数据对接同步，对绕过堡垒机而登录主机的行为，关联分析进行实时告警。 5、售后服务支持：提供 3 年升级维护；提供 24 小时支持热线。			