合同号：2023-XXZX-012

常州市第一人民医院

网络安全态势感知系统

采购合同

项目编号：常采竞磋[2022]0142号

项目名称：网络安全态势感知系统

甲　　方：常州市第一人民医院

乙　　方：中电鸿信信息科技有限公司

2023年1月

合同主要条款

甲方：常州市第一人民医院

乙方：中电鸿信信息科技有限公司

签订地点：江苏 常州

根据常州市政府采购中心 2022 年 12 月 9 日进行的常采竞磋[2022]0142 号 号招标结果，甲、乙双方本着平等互利的原则，通过共同协商，根据《中华人民共和国政府采购法》、《中华人民共和国民法典》及有关法律法规，就相关事宜达成如下合同。

一、合同标的名称、型号、规格、数量、单位、单价、金额、品牌。

合同标的名称	开票名称	系统序号	系统分项	数量	单位	含税价格（元）
网络安全态势感知系统	信息技术服务	1	态势感知平台	1	台	225171
		2	安全探针 1	1	台	68219
		3	安全探针 2	1	台	121710
		4	安全服务	1	项	74900
总计	490000 元（人民币肆拾玖万元整）					

注：本合同含税总价为人民币￥【490000】元（ 大写：【肆拾玖万元整】；本合同适用增值税税率为 6%。

二、合同标的技术要求

以下文件是本合同不可分割的组成部分，具有同等法律效力，如果不同文件的条款之间有冲突，文件之间的优先效力顺序如下：

1、本合同及其附件，包括附件 1：网络安全态势感知系统功能需求与技术要求、附件 2：安装运行验收报告模板。

2、常州市第一人民医院网络安全态势感知系统招标文件。

3、乙方提交的投标文件。

4、招标文件及相关的资料。

5、乙方投标的其他资料及承诺。

6、经甲、乙双方确认的其他补充协议及相关资料。

三、包装、运输与保险

1、乙方提供的设备应为原厂包装。

2、乙方负责确保按期按质交货。

四、到货、安装、调试及验收

（1）产品参照项目清单进行逐项验收，并满足用户提出的相关功能要求和技术参数要求。

（2）系统按合同规定的验收标准和投标文件要求进行验收，当两者发生矛盾时，以所有文件中最高性能指标为准。

五、 权利和义务

1、甲方权利和义务

1.1甲方在乙方项目实施过程中，指定王坚、冷烽为本合同项目甲方负责人，以书面授权形式提交乙方备案。项目负责人负责项目实施过程中的协调、沟通工作，如代表甲方提出需求变更、发起并召开需求研讨会、协商并签订合同备忘录、确认进度等一切工程实施事宜。

1.2甲方有权按照医院管理制度对乙方实施人员进行日常管理，有权要求乙方更换甲方认为不称职的乙方项目负责人。甲方负责对项目实施过程的全过程监督，审核乙方制定的项目计划（包括培训方案），对系统的设计、实施进度及建设质量方面进行监督和指导。甲方可自行或安排项目监理按月对乙方工程进度确认，乙方在工程开始实施后的每个月向甲方提交进度确认申请，甲方应在收到确认申请之日起7个工作日内对工程进度予以确认，并向乙方出具书面的进度确认单，逾期未确认的，乙方应发书面通知提示甲方确认，若甲方仍未确认的，视为甲方已确认乙方提出的进度。

1.3甲方协助乙方提供项目所需的信息、数据、资料。

1.4甲方帮助协调和落实与本合同相关的部门有关工作，帮助乙方解决建设过程中的有关困难和问题，保障项目顺利进行。

1.5系统正式交付甲方使用后，甲方按规定对系统进行日常维护和操作，备份数据。一旦出现故障甲方应立即采取措施，保护好数据库，并立即通知乙方。

2、乙方权利和义务

2.1 乙方应按照本合同要求提供服务。乙方指定周忱凯为本合同项目乙方负责人，代表乙方在合同履行期间行使权利和义务，其他任何未经乙方授权人员的签字、承诺均不产生法律效力，在未经过甲方同意，乙方不得在项目建设期间更换项目负责人。

2.2 乙方应妥善使用、保管甲方提供资源，并及时向甲方反馈建设与服务过程中发现的问题，重大问题提出书面报告。

2.3 在甲方系统使用过程中，乙方应确保系统的正常运行和维护，不得因开发人员的出

差、调职、离职等原因出现响应不及时的情况，如响应不及时，甲方有权采取必要补救措施及要求乙方在规定时限内弥补缺陷，并有权向乙方提出索赔。

2.4 在甲方提供的条件达到运行标准后，由甲方正式书面向乙方提出安装调试和测试要求，乙方负责在 1 个月内完成安装调试、测试、人员培训等系统上线工作，待甲方验收合格或视为验收合格后交付甲方正式使用。

2.5免费维护包括为适应系统的环境和其他因素的各种变化，保证系统正常工作而对系统所进行的维护、修改，包括软硬件系统功能的改进和解决系统在运行期间发生的问题，应用软件/硬件固有的或潜在性缺陷、或以当时技术水平未发现/不能解决的缺陷、或甲方提出的更正性、适应性、完善性和预防性维护；若涉及系统架构及在本合同约定外的进一步功能扩展或者系统新增等服务应另行协商签订新合同（但系统架构系前述原因除外）。对于应用软件维护可通过远程网络等途径提供维护，确保系统安全平稳运行。

2.6在系统正常上线后质保期内，如需现场服务，乙方有义务按照甲方要求安排开发人员在甲乙双方约定时间内到现场进行开发解决急需需求；对影响甲方系统正常运转而现场人员不能解决需乙方重新调派人员现场解决的，重大故障现场响应时间为6小时之内，一般故障现场响应时间为24小时内，超过前述时间，每超过1次，质保期顺延1月。对于非乙方原因导致的系统故障，由此产生的相关费用由甲方承担，具体额度由双方协商确定。

2.7 在项目建设过程中，乙方应接受甲方的各项管理制度，主要项目管理人员或主要技术人员若有特殊情况需要离开甲方单位的，应向甲方项目负责人提出说明，并获得甲方许可方可离开。

2.8乙方按合同约定向甲方提交支付申请。

2.9乙方不得在软件系统中留有任何可能导致甲方或甲方用户数据泄露的软件设置，并严格要求其工作人员（任何形式的人员，包括服务外包人员、远程协助人员等，下同）在接触到甲方及甲方用户的数据、信息与保密资料时严格遵守相关信息安全制度及保密制度的操作。乙方不得使用系统相关数据、信息和资料从事违法、犯罪等不正当活动，不论该信息、数据和资料是否经过去隐私化处理。除非取得甲方同意，否则乙方及乙方工作人员不得采取任何技术手段搜集、获取、使用甲方的数据、信息及资料或以任何形式向第三方泄露该信息或数据；如违法以上信息造成的一切民事或刑事等后果由乙方承担。

2.10 乙方提供的软件及伴随服务不得侵犯第三人知识产权。

六、付款方式

本合同含税总价为人民币￥【490000】元（大写：【肆拾玖万元整】。

1、合同签订完成后，甲方支付合同价格的 30% 的预付款，即人民币￥147000 元整（大写：【壹拾肆万柒仟元整】。

2、系统安装调试验收合格且培训完成之后支付合同价格的 60%，即人民币￥294000 元整（大写：【贰拾玖万肆仟元整】。

3、免费维护阶段的服务无质量问题，在免费维保期结束之后，付清合同软件价格的 10% 尾款，即人民币￥49000 元整（大写：【肆万玖仟元整】。

甲方付款前，乙方开具项目总金额且税率为 6%增值税专用发票，甲方按照医院签票流程走付款程序，具体到账时间以甲方付款流程为准。

甲方账户信息如下:

甲方单位名称：常州市第一人民医院

纳税人识别号：123204004672858558

开户行：中国工商银行股份有限公司常州天宁支行

账号：1105020309000043779

乙方账户信息如下：

乙方单位名称：中电鸿信信息科技有限公司

纳税人识别号：91320000668382125D

开户行：中国建设银行南京湖北路支行

账号：32001881436059000588

七、 质量保证期与售后服务

1、本项目要求整个系统、设备免费质保为三年，维保到期后每年维保费用为本合同总额的 10%。设备（系统）质量保证日期为项目整体验收合格之日起计算。

2、质保期内，因货物质量问题导致的各种故障的技术服务及维修所产生的一切费用由乙方负责承担。

3、乙方应针对货物的特点对甲方有关人员在货物的性能、原理、操作要领、维修和保养等各个方面进行免费现场培训。

4、人员培训

对甲方员工进行该技术内容操作使用和维护保养的培训不少于 16 小时。对甲方员工进行设备安全培训。提供设备运行、调试、维护过程中必要的专用工具、软件，以及对相关人员进行工艺设置、设备运行、调试和维护过程中相关的专用工具及软件使用的培训。乙方免费提供一定数量的培训资料。

八、违约责任

1、甲、乙双方任何一方不履行合同义务或者履行合同义务不符合合同约定的，均视为违约。违约方应当承担继续履行、采取补救措施或者赔偿损失等违约责任。

2、甲、乙双方在完成签署的书面确认事项后，任何一方提出变更要求，并经另一方确认生效，导致服务进度延迟的，不视为变更提出方违约；但若因此而给另一方造成损失的，由提出变更一方赔偿另一方直接经济损失。

3、如乙方提供的服务不符合合同约定，甲方可要求乙方在限定的时间内予以改进，并再次提交甲方确认。若由此导致建设进度延迟的，甲方可视延迟情况可以要求乙方承担合同价款的5%的违约金责任。

5、违约方的全部赔偿责任，包括但不限于因合同、侵权、违约或者违反保证引起的赔偿。

6、乙方违反本合同项下的义务，除应当承担相应的违约责任，还应当赔偿由此给甲方造成的损失，包括但不限于甲方为实现债权而支付的保全费、诉讼收费、律师费、公证费、鉴定费、评估费、拍卖费等费用。

九、解决纠纷的方式：

因履行本合同发生争议协商解决不成的提交甲方所在地人民法院诉讼管辖。

十、生效：

本合同自各方盖章且法定代表人或委托代理人签字之日起生效。

十一、其他

1、为保障甲方系统实现长期、持续、稳定的运行，在免费维护期满后，在同等条件下甲方可优先选择乙方继续负责本项目的维护、更新、扩展等后续服务工作。若因特殊情况导致乙方无法为甲方提供系统后续维护工作的，或乙方报价高于第三方但又不接受降价为甲方提供后续维护工作的，乙方应当向甲方开放源代码。

2、除甲、乙两方在合同中约定的条款外，其他未尽事宜均以补充协议形式另行约定，补充协议与本合同具有同等效力，补充协议与本合同约定不一致的以补充协议约定为准。

3、本合同壹式捌份，甲方执肆份，乙方执肆份，均具有同等法律效力。

甲方：常州市第一人民医院

单位名称（章）：常州市第一人民医院

单位地址：常州市天宁区局前街185号

法定代表人签字或签章：

委托代理人：

日期：2023年 2月16日

乙方：中电鸿信信息科技有限公司

单位名称（章）：中电鸿信信息科技有限公司

单位地址：南京市玄武大道699-1号

法定代表人签字或签章：

委托代理人：

日期：2023年 2月10日

附件1：网络安全态势感知系统功能需求与技术要求

一、建设要求

（1）态势感知管理平台：要求可以对各探针进行数据收集，可提供数据分析功能，可以清晰的分析出针对医院内网针对网络资产的攻击和潜在威胁，提供安全策略，提供可视化的统一管理。

（2）探针 1：部署在服务器外网交换机，用于检测针对我院互联网资产的攻击和潜在威胁。

探针 2：部署在内网核心交换机，用于检测医院内网存在的潜在威胁。

二、技术参数和服务要求

2.1 态势感知平台技术参数要求

技术指标	指标要求
硬件参数	▲要求所设备内存≥64G，配置硬盘≥4*4T，产品提供不少于 4 个千兆电口，产品采用标准 2U 架构，提供不少于三年原厂软硬件质保和软件及规则库升级服务，提供厂商售后服务承诺函且加盖厂商公章
功能参数	▲支持不同安全视角展示多个独立的大屏展示功能，不小于 16 个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（需提供产品功能截图证明且加盖厂商公章）
	*支持 700 种以上安全设备、网络设备、DHCP 服务器、蜜罐、中间件等设备日志接入，支持 syslog、winlogbeat、jdbc、wmi、webservice、ftp、snmp trap 等接入方式（需提供产品功能截图证明且加盖厂商公章）
	▲支持自定义分支管理权限，分支管理员具备独立的管理页面，只能管理和查看所属分支的业务和终端资产的安全信息且具备完整的功能展示（需提供产品功能截图证明且加盖厂商公章）
	*支持通过主动发送微量包的扫描方式探测潜在的服务器（未知资产）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（需提供产品功能截图证明且加盖厂商公章）
	*支持资产多级分支管理，最多可至 15 级分支，支持资产全生命周期自动管理，包括资产自动发现、多级资产、资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等（提供产品功能截图证明且加盖厂商公章）
	▲密码检测技术基于人工智能学习技术（无监督自我学习）提取登陆成功的特征，通过人工智能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，包括响应体内容、响应体关键字、响应体、响应体长度（提供产品功能截图证明且加盖厂商公章）

	*具备基于人工智能的 webshell 通信流量检测，可检出加密（如冰蝎）的通信流量。具备 650+webshell 规则检测，且覆盖 webshell 整个攻击阶段检测，包括 webshell 上传点探测、webshell 上传下载、webshell 通信
	*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
	*具备元数据行为分析引擎：httpflow、dnsflow、adflow、icmpflow、maillflow 等，通过异常行为分析，结合各类机器学习算法完成未知威胁检测。包括：内网穿透、代理、远控、隧道、反弹 shell 等事后检测场景
	▲支持挖矿专项检测页面，具备挖矿攻击事前、事中和事后全链路的检测分析能力，综合运用威胁情报、IPS 特征规则和行为关联分析技术，如检测发现文件传输（上传下载）阶段的异常，对挖矿早期的准备动作即告警（提供产品功能截图证明且加盖厂商公章）
	▲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（提供产品功能截图证明且加盖厂商公章）
	*支持平台内置的静态文件检测引擎、AI 智能引擎、未知威胁查杀引擎、webshell 检测引擎，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

2.2 安全探针 1 技术参数要求

技术指标	指标要求
硬件参数	▲吞吐量≥1Gbps，内存≥8G，硬盘≥64GB SSD，产品提供不少于 6 个千兆电口+2 个千兆光口，需提供三年原厂硬件质保和软件及规则库升级服务，提供厂商售后服务承诺函且加盖厂商公章
功能参数	*支持旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响
	▲支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、NetworkDevice、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击等服务漏洞攻击检测（提供产品功能截图证明且加盖厂商公章）
	*支持 FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、等协议暴力破解检测（提供截图证明并加盖原厂商公章）
	*支持 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 整站系统漏洞等网站攻击检测（提供产品功能截图证明且加盖厂商公章）

	*支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等（提供产品功能截图证明且加盖厂商公章）
	*支持传输协议审计日志，包括 https 协议日志、http 协议审计日志、DNS 协议审计日志、邮件协议审计日志、SMB 协议审计日志、AD 域协议审计日志、WEB 登录审计日志、FTP 协议审计日志、Telnet 协议审计日志、ICMP 协议审计日志、LLMNR 协议审计日志（提供产品功能截图证明且加盖厂商公章）
	*支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC 通信等僵尸网络行为检测
	▲支持 5 种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求（提供产品功能截图证明且加盖厂商公章）
	*支持 IP，IP 组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式（提供产品功能截图证明且加盖厂商公章）
	*支持流量抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式（提供产品功能截图证明且加盖厂商公章）

2.3 安全探针 2 技术参数要求

技术指标	指标要求
硬件参数	▲吞吐量≥2Gbps，内存≥8G，硬盘≥480 SSD，产品不少于 6 个千兆电口+2 个万兆光口，配备冗余电源，需提供三年原厂硬件质保和软件及规则库升级服务，提供厂商售后服务承诺函且加盖厂商公章
功能参数	*支持旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响
	*支持报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意 UR 监测模式，可完成模式匹配并生成事件，可提取 URL 记录和域名记录
	▲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（提供产品功能截图证明且加盖厂商公章）
	*内置 URL 库、IPS 漏洞特征识别库、应用识别库、WEB 应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库（提供产品功能截图证明且加盖厂商公章）
	*支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、NetworkDevice、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击等服务漏洞攻击检测（提供产品功能截图证明且加

	盖厂商公章）
	*支持 FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、等协议暴力破解检测（提供截图证明并加盖原厂商公章）
	*支持传输协议审计日志，包括 https 协议日志、http 协议审计日志、DNS 协议审计日志、邮件协议审计日志、SMB 协议审计日志、AD 域协议审计日志、WEB 登录审计日志、FTP 协议审计日志、Telnet 协议审计日志、ICMP 协议审计日志、LLMNR 协议审计日志（提供产品功能截图证明且加盖厂商公章）
	*支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC 通信等僵尸网络行为检测
	▲支持 5 种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求（提供产品功能截图证明且加盖厂商公章）
	*支持 IP，IP 组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式（提供产 品功能截图证明且加盖厂商公章）
	*支持流量抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式（提供产品功能截图证明且加盖厂商公章）

2.4 安全服务要求

服务类	服务内容
服务内容	*需要对用户资产进行全面发现和深度识别，并在后续服务过程中触发资产变更等相关服务流程，确保资产信息的准确性和全面性
	*提供对操作系统、数据库、常见应用/协议、Web 通用漏洞与常规漏洞进行漏洞扫描
	*提供弱口令扫描，针对信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat 等
	*提供检查支撑信息化业务的主机操作系统、数据库、中间件的基线配置情况，确保达到相应的安全防护要求。检查项包含但不限于帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制等配置情况
	*需要分析判断主机是否感染了勒索病毒；是否已感染勒索病毒文件；根据已发生的漏洞攻击行为分析判断否存在勒索病毒攻击等
	*需要对发现的问题进行处置，包含内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等
	*提供针对漏洞利用攻击行为、Webshell 上传行为、Web 系统目录遍历攻击行为、SQL 注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行

	为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务风险点
	*服务方需对失陷主机进行分析研判（如后门脚本类事件），并给出修复建议
	*需要提供客观的漏洞修复优先级指导，不能以漏洞危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度（提供相关截图证明，且加盖厂商公章）
	*需要针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的漏洞，自动生成漏洞工单，安全专家跟进漏洞状态，各个处理进度透明，方便用户清晰了解当前漏洞的处置状态，将漏洞处理工作可视化（提供相关截图证明，且加盖厂商公章）
	*支持实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件（提供相关截图证明，且加盖厂商公章）
	*支持针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助用户快速恢复业务，消除或减轻影响
	*支持面向用户的安全态势展示，展示出当前用户遭受的威胁事件信息以及脆弱性信息统计，使得用户能直观感受到当前的风险态势情况（提供相关截图证明，且加盖厂商公章）
	*安全专家根据安全事件分析的结果以及处置方式，根据用户授权情况按需对安全组件上的安全策略进行调整工作
	*支持展示出当前工单数量和工单处置状态，使得用户能详细查看服务处置过程，查看安全事件闭环效果，掌握当前专家服务进度，监督服务质量
	*支持展示出当前需要用户审批的工单及其具体情况，使得用户能完成与服务人员的协同处置，共同确保安全威胁和事件得到准确处置
	*支持使用 finebi 平台，自定义配置统计数据，包括告警数据，工单数据，工单平均处置时长等数据，来统计当前平台的运营效率，直观体现出当前运营能力，同时可对服务专家处置效率进行考核
	*支持根据不同场景，灵活选择不同的组件组合形成新的报告模板，以便于用户查看不同场景和维度的服务报告。可从时间范围，开始时间，结束时间、漏洞攻击，网络流量，恶意攻击，脆弱性等维度组合新的报告模板。下载报告时，选择相应场景的模板进行下载即可
服务质量监督	*服务方需为用户提供服务监控门户，在门户中可查看业务安全状态，处置中的失陷事件以及针对这些事件的处置进度，处置责任人、联系方式等信息，方便用户实时了解服务方的服务效果（提供相关截图证明，且加盖厂商公章）
	*服务方需有具备服务质量可视化展示，用户能通过可视化的数据，清晰的了解安全专家的服务水平，至少包括漏洞闭环率、漏洞平均响应时长、

	漏洞平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长（提供相关截图证明，且加盖厂商公章）

三、实施方案及要求

1.资产梳理

需要对服务范围内资产（不小于 20 个互联网资产）进行全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP 地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理；当资产发生变更时，安全专家对变更信息进行确认与更新。

2.平台安装部署

需要基于用户实际网络及部署环境，进行上架、安装、调优平台软硬件

3.安全数据接入与治理。

需要接入用户的网络流量日志、威胁情报、脆弱性数据和 IT 基础设施的告警日志，实现安全数据的标准化没后续安全建模提供数据基础，

4.威胁分析建模

需要针对预定义和自定义的安全关联分析场景，侯建分析规则与模型，识别位置威胁，对安全设备告警进行大幅降噪。

5.威胁研判与响应处置

需要通过威胁情报、基于攻击链的调查分析等，对威胁进行分析研判。梳理安全运营流程，构建处置剧本，通过工单或 SOAR 对常晟的告警时间进行统一响应处置。

6.全局展示与持续监测

需要通过安全指数、大屏可视化、自定义 BI，直观反映安全建设与运营情况，掌握全网健康度，并持续监测威胁。

附件2 ：安装运行验收报告模板

<table>
<tr><td colspan="2">合同名称：</td><td></td><td>合同编号：</td><td></td></tr>
<tr><td colspan="2">甲方使用部门：</td><td></td><td>验收地址：</td><td></td></tr>
<tr><td colspan="2">乙方安装工程师：</td><td></td><td>服务联系电话：</td><td></td></tr>
<tr><td rowspan="6">主要货物信息</td><td>序号</td><td>产品型号</td><td>产品编号或描述</td><td>数 量</td></tr>
<tr><td>1</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td></td><td></td><td></td></tr>
<tr><td>3</td><td></td><td></td><td></td></tr>
<tr><td>4</td><td></td><td></td><td></td></tr>
<tr><td>。。。。。。</td><td></td><td></td><td></td></tr>
<tr><td colspan="5">验收内容 ：</td></tr>
<tr><td colspan="3">甲方项目负责人签字：

甲方部门公章：

年 月 日</td><td colspan="2">乙方授权代表签字：

乙方公章：

年 月 日</td></tr>
</table>