海宁市政府采购合同

一、通用必备条款部分

合同编号：HNCG2025018-H25012

政府采购计划（预算）确认号：临[2025]2392 号

预算金额：910000.00 元

采购人（以下称甲方）：**海宁市政务服务管理办公室**

供应商（以下称乙方）：**中国联合网络通信有限公司嘉兴市分公司**

采购代理机构：海宁市政府采购中心

采购方式：竞争性磋商

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律法规的规定，甲乙双方按照 HNCG2025018 项目采购结果签订本合同。

第一条 合同组成

本次政府采购活动的相关文件为本合同的组成部分，这些文件包括但不限于：

1.1 本合同文本；

1.2 采购文件与采购响应文件；

1.3 中标或成交通知书；

组成本合同的所有文件必须为书面形式。政府采购合同备案时，须提供以上（1）、（3）两项，如由社会中介机构代理，须提供代理协议，合同如有变更的，须提供变更协议。

第二条 合同标的与相关属性

2.1 本次采购的是**政务外网安全监管平台服务** 。

第三条 合同价款

3.1 本合同项下总价款为人民币（大写）**捌拾玖万捌仟捌佰**元整，（小写）**898800.00** 元。分项价款详见下表。

单位：人民币元

序号	名 称	数量	单位	金 额
1	政务外网安全监管平台服务	1	年	110000
2	网络流量采集服务	1	年	150000
3	违规外联监测服务	1	年	20000
4	漏描和渗透测试服务	1	年	20000
5	机器人服务	1	年	200000
6	运维服务	1	年	257000

7	硬件续保	1	年	141800

3.2 本合同总价款包括相关服务建设通过最终验收之前的所有含税费用及之后一年服务与运维所产生的一切含税费用。

3.3 付款手续和付款时间

3.3.1 付款手续

合同签订并完成相关服务建设期验收后预付 36 万元，平台服务与运维期结束后依据考核情况支付合同剩余金额，乙方向甲方办理结算手续，甲方需审核以下结算资料：合法发票，盖有政府采购备案专用章的《采购合同》复印件，甲方签收的“海宁市政府采购项目验收单”（预付时无须提供）、考核记录（预付时无须提供）等相关资料。

3.3.2 付款时间

甲方将审核后的结算资料按《海宁市政府采购资金支付管理暂行办法》提交至国库支付中心（或单位财务部门），经审核无误后，国库支付中心（或单位财务部门）在 7 个工作日内支付相应合同金额。

第四条 履约保证金

本项目不设置履约保证金。

第五条 合同的变更和终止

除《政府采购法》第 49 条、第 50 条第二款规定的情形外，本合同一经签订，甲乙双方不得擅自终止合同或对合同实质性条款进行变更。确有特殊情况的，须报同级财政部门备案。

第六条 合同的转让与分包

乙方不得擅自部分或全部转让其应履行的合同义务，同时也不允许分包。如乙方将项目转包或将不允许分包部分进行了分包，甲方有权解除合同并追究乙方的违约责任。

第七条 争议的解决

因履行本合同引起的或与本合同有关的争议，甲、乙双方应首先通过友好协商解决，如果协商不能解决争议，则向甲方所在地有管辖权的人民法院提起诉讼。

第八条 合同备案及其他

本合同一式四份，甲方、乙方、海宁市财政局和海宁市政府采购中心各执一份。

二、特殊专用条款部分

第一条 采购内容

序号	名称	数量	单位
1	政务外网安全监管平台服务	1	年
2	网络流量采集服务	1	年
3	违规外联监测服务	1	年

4	漏描和渗透测试服务	1	年
5	机器人服务	1	年
6	运维服务	1	年
7	硬件续保	1	年

第二条 合同履约期限

合同签订之日后60日内完成相关服务建设期验收；平台服务及运维期限为建设期验收合格后1年。

第三条 服务要求

3.1 政务外网安全监管平台服务

平台功能	功能子项	功能要求
运营工作台子系统	运营工作台	支持开箱即用的个人工作台界面。 支持默认展示工单、安全事件、威胁告警、脆弱性、预案、风险资产概况，支持展示报告生成情况。 统计指标支持点击下钻，展现进一步信息。 支持自定义工作台内容、内容分组。
	APT防护工作台	支持APT防护专项工作台，提供APT防护专项的威胁预警、环境监控、风险排查和安全事件与重要资产的实时监测。实现对系统APT风险预警、APT防御配置、APT实时监测、APT防御能力评估的一站式专项查看与管理。
		支持查看APT防护预警，内容包含预警名称、预警摘要、发布时间，威胁告警数量、受攻击资产数量、脆弱性资产数量、疑似风险资产数量等，并支持下钻至详情页。
		支持APT防护环境配置情况监控，包括APT防护相关数据源工作状态正常/异常/停止情况监测、终端安全APT防护策略开启状态监测、平台APT防护相关分析规则配置与启用情况检测。支持下钻到对应的功能页面查看详情。
		支持对系统中APT相关风险的集中监测。实现在工作台基于APT威胁情报快速新建排查任务，并自动更新任务的排查结果。
		工作台提供APT全景地图，图中支持显示包括海莲花、方程式、索伦之眼等40+热点APT组织信息，通过点击交互，可弹出APT组织相关信息，相关信息包含简介、归属地、最早发现时间、目标国家、目标领域、攻击方式、技术能力模型、相关报告链接等；APT全景地图同时显示本地APT情报总数、APT组织数量、较昨日新增数量、情报更新时间等信息。（提供产品功能截图证明）
		支持互联网资产和内网资产排查，互联网资产排查包含端口、IP、域名，内网资产排查包含业务系统、IP资产、影子资产等； 支持资产漏洞排查，包含当前存在中高危系统漏洞数量、近几年重大漏洞数量、当前存在中危web漏洞数量； 支持资产风险排查，包含风险资产数、高危端口资产数、弱口令数等。
		支持展示最新APT攻击源地址、重点资产风险监控等统计，并支持展示最新的5条APT安全事件，可下钻至详情页。

		支持 APT 防护场景的一站式配置入口，提供 APT 检测、APT 排查、APT 监测、APT 响应、实战模拟等功能配置导航
	勒索防护工作台	支持勒索防护专项工作台，提供勒索防护专项的威胁预警、环境监控、风险排查和安全事件与重要资产的实时监测。实现对系统勒索风险预警、勒索防御配置、勒索实时监测、勒索防御能力评估的一站式专项查看与管理。
		支持查看勒索威胁预警，内容包括预警名称、预警摘要、发布时间，威胁告警数量、受攻击资产数量、脆弱性资产数量、疑似风险资产数量等，并支持下钻至详情页
		支持勒索防护环境配置情况监控，包括勒索防护相关数据源工作状态正常/异常/停止情况监测、终端安全勒索防护策略开启状态监测、平台勒索防护相关分析规则配置与启用情况检测。支持下钻到对应的功能页面查看详情。
		支持对系统中勒索相关风险的集中监测。实现在工作台基于勒索威胁情报快速新建勒索排查任务，并自动更新任务的排查结果。
态势感知中心子系统	态势大屏	系统内置 9 张大屏，包括威胁攻击态势、资产安全态势、安全事件态势、安全成果态势、综合安全态势、威胁情报态势、运行监控态势、大数据中心态势、XDR 运行态势
		态势感知部分大屏元素支持自定义，选择经过仪表盘定义的图例替换原有大屏元素
		支持大屏轮播，支持自定义参与轮播的大屏，轮播间隔时间、轮播大屏顺序。
	仪表盘	支持自定义仪表盘配置，根据需要添加不同的监控组件，自定义选择过滤条件和过滤条件组的监控组件添加、修改和删除。 支持同时组合多种展示图形，如柱形图、堆积柱形图、折线图、分组折线图、面积图、饼图、环形图、表格、统计值、玫瑰图、气泡图、热力图、复合计算统计、上传图片、外部图片、外部网页等，可配置排序方法、TOP 数量、数据时间跨度。 仪表盘的图形位置和大小支持自由拖拽，所见即所得。 支持设置常用仪表盘，通过拖拽调整仪表盘的顺序，将选定的仪表盘设为首页，登录系统后将直接展示对应的仪表盘的内容。
	态势报告	提供报告下载列表，快速下载内置的安全态势日报、周报和月报。并提供报告下载列表，支持根据报告生成时间、报告类型进行快速筛选。
		内置周期性报告任务，包括安全态势日报、周报和月报的报告任务。 支持用户自定义即时、周期性（每日、每周、每月）的报告任务，自动生成报告并通过邮件发送、下载、导出等方式获取。支持在报告任务下导出 WORD/HTML/EXCEL/PPT 等格式，报告可指定人员进行分享。 报告中数据支持统计查询与过滤条件满足与、或、非、In、Not In、exist、like 字符串匹配、rlike 正则匹配等基础组合。支持报告图形化结果展示包括但不限于柱状图、饼图、面积图、趋势图、表格、统计、同比、环比、百分比、复合统计等。
		内置 10 余个报告模板。 支持用户自定义编辑报告模板，根据实际的业务需求自定义统计分析的指标对象，生成有针对性的分析报告，支持从原始日志与流量、安全设备告警、平台关联告警以及安全事件输出多个层面自动呈现统计数据。支持对概况、事件、IP 地址、端口、服务、事件严重程度、攻击种类、用户等数据进行统计。报表

		内容支持自定义编辑，直接引用图表、文本、链接、图片、宏变量、外部网页等元素。
分析中心子系统	智能检索	支持对原始日志、原始告警进行场景化检索。 支持针对原始日志、原始告警内容的不同场景，自动化推荐检索字段、列表字段进行检索
		支持对原始日志、原始告警、威胁告警、安全事件、漏洞、脆弱性、风险等进行检索分析。 支持添加结构化语言过滤条件和过滤条件组对内容进行查询，支持查询条件支持 and、or、not 等多重逻辑操作组合，支持等于、不等于、大于、小于、大于等于、小于等于、存在、不存在、属于（内置安全信息）、网段包含、字符串匹配、正则表达式匹配等多种操作符。
	威胁感知	支持查看威胁告警概览信息，包含开始时间、结束时间、告警阶段、告警次数、数据源、责任人、发起流程、安全设备等信息，且能进行下钻查看关联安全事件、执行 SOAR 预案、发起流程（运营工单、重保工单、通知通报）、告警加白、处置等操作； 支持查看原始告警列表并可以对原始告警进行 HQL 检索、过滤检索，同时在当前页面支持对原始告警详情查看和原始告警关联原始日志下钻查看。
		支持查看告警基础信息、证据信息、请求-响应信息、关键信息、处置建议、情报信息、其他信息等，其中攻击者组、受害者组、源地址、目的地址根据匹配逻辑富化资产信息或网段信息或情报信息并提示资产详情|网段详情|威胁情报，威胁图谱、处置预案的跳转入口；流量类告警相关字段高亮显示且支持下载 pcap 包分析和沙箱检测报告下载； 涉及进程异常的告警类型详情中支持进程树的绘制； 整体告警字段支持只看有值筛选以及解码助手，解码助手支持多种格式，包括 Unicode、BASE64、HEX、URL、JSON，对于不支持连网环境，提供二维码，扫描复制到其他设备进行解码； 支持告警级别调整记录查看 告警详情中支持提取相关实体，并能跳转到实体详情进行分析。
		在联网场景中，非威胁情报类型的告警详情中管理的外网 IP 支持情报富化，如命中可展示地理位置、运营商、AS、ASN、网络类型、匿踪类型、情报风险等级、情报风险类型、恶意类型、恶意家族、标签、置信度、阻断系数、阻断建议等信息。（提供产品功能截图证明）
		支持查看同类告警，可以参考历史研判经验，或者进行批量处置响应。
		支持内置关联分析规则不少于 900 条； 告警类型包括：扫描探测、主机异常、异常通信、漏洞攻击、运维监控、Web 攻击、账号异常、网络攻击、威胁情报、恶意程序、邮件攻击、多维关联、内容安全。
		支持 B 事件发生之前一定没发生 A 事件，如在管理员未登录时主机上创建异常定时任务， 说明可能是非人工创建或存在登录绕过风险，主机行为非常可疑。（提供产品功能截图证明）
		支持关联规则根据数据标准进行规则编写的自动化推荐，系统根据事件类型自动推荐其所属的对象，并且会自动判断规则内容是否与事件类型匹配。（提供产品功能截图证明）
		关联分析规则支持配置和管理，支持通过 WEB 界面新建、编辑关联分析规则。

		关联分析规则支持通过配置调用 SOAR 预案形成自动触发场景，支持触发周期、责任人的配置。支持指定告警阶段、告警级别和该告警使用的 ATT&CK 技战术。
		支持选择告警的任意字段、字段组合生成合并策略，引用相同合并告警规则且合并策略内容相同的告警会聚合为一条合并告警。 支持提供常用合并字段，供使用者快速设置合并策略。
		支持高级合并策略模型，在高级模式下，支持配置告警过滤条件，对满足不同条件的告警走不同合并策略；配置过滤条件支持 HQL 语言方式。（提供产品功能截图证明）
		支持关联分析过程中随时调用静态对象来快速完成分析模型的构建，避免频繁修改模型内容。 支持内置包括 IP 类、时间类、数字类和字符类的不低于 100 种常用的安全信息，如办公区 IP、工作时间段、黑名单 IP、常见服务端口、cmd 进程白名单、可疑进程列表等。 静态信息组的管理支持包括新建、删除、编辑、导入、导出、检索，并以树形结构进行分类管理。
		支持键值对类型信息组，支持日志中的 2 个字段与信息组内容进行匹配。 例如：设置服务器进程黑|白名单信息组，支持根据服务器 IP 设置不同的进程黑|白名单；支持日志中 IP、进程名均命中信息组告警，或 IP 命中、进程不命中告警。
	威胁情报	支持连接云端情报，通过 API 查询访问各类情报数据，包括 IOC、黄赌诈等黑灰产、攻击源 IP 及文件信誉等。 支持通过云端情报进行威胁告警富化；支持威胁实体下钻跳转至云端情报页面查看更多信息。 其中各类情报数量如下： IOC：历史总量不少于 4 亿 黄赌诈等黑灰产：历史总量不少于 100 亿 攻击源 IP：历史总量不少于 5 亿 文件信誉：历史样本总量不少于 300 亿
		支持拉取本地情报包，其中 IOC 情报不低于 1400 万，情报类型包括常规木马、僵尸网络、勒索软件、APT 攻击、挖矿软件、网银木马、后门软件、窃密木马、黑客工具、扫描探测、黑灰产、可疑威胁、蠕虫病毒、隐匿追踪、DGA、其他远控等。 支持情报离线更新及在线更新。 支持统计情报总数、今日更新条数、IP 情报总数、域名情报总数、URL 情报总数、命中告警数。 支持分类统计威胁情报数量及命中告警数。 支持统计展示情报告警摘要、命中情报资产分布情况、命中情报安全事件级别分布、命中情报家族/团伙、情报告警趋势、情报告警信息等。
	攻击发现	支持查看安全事件详情，包括不限于：概览、威胁图谱、告警、相关证据、影响面、处置信息。

		展示安全事件概览信息，包括不限于：数据源，攻击阶段统计，告警总量，待处置告警数据，影响面实体数量，其他实体数量，证据数据等。 ATT&CK 技战术，支持将安全事件中所有告警的攻击技战术，以矩阵形式展示。 杀伤链，支持根据告警先后顺序，以及告警的攻击者、受害者所处安全域绘制杀伤链。
		支持抽取安全事件中支撑分析研判的证据进行集中展示；支持证据跳转相应的告警查看完整上下文；支持的证据类型包括不限于：威胁情报、恶意样本鉴定结果、威胁特征。（提供产品功能截图证明）
		支持抽取安全事件中涉及到的内部实体（内网 IP、主机、账号）进行统一展示，支持查看实体名称、风险等级等信息，支持跳转相应的告警。
		支持安全事件将所有相关告警的处置建议进行统一汇总和展示，对每个告警有对应的分析内容和处置建议，提供兼容 ATT&CK 并且新增扩展的缓解建议和检测建议。
		支持研判分析过程中直接添加新的日志和告警信息进安全事件。
		支持自动化威胁猎捕模型，可在线编写脚本语言算法模型模拟分析人员溯源取证的过程，基于告警为入口触发条件的威胁场景自动溯源分析，向前、向后自动抽取若干分钟、小时和天为单位的数据，结合时间、过滤条件关联，多层逻辑嵌套、自动聚合分析包括日志、流量、告警等内容，聚合跨阶段展示整个威胁事件。（提供产品功能截图证明）
		支持将告警按照整个事件的攻击链、攻击方向聚合及攻击时间轴排序，整合为一个事件的完整攻击链阶段。 并根据聚合事件的安全评分模型化动态评估严重等级，模型维度包括不限于告警数量、告警等级、攻击阶段、威胁情报。
	关联分析规则	关联分析规则启动时，支持自动检测是存在同源规则，用户可快捷处置同源规则，避免产生重复告警。（提供产品功能截图证明）
		内置规则更新后，复制自该规则历史版本的自定义规则会自动增加“待更新规则“标签，支持用户一键同步规则更新或者忽略该规则更新。（提供产品功能截图证明）
资漏中心子系统	资产管理	支持资产信息管理，按资产组分视图展示；支持资产数据导入导出；支持资产属性字段自定义扩展。
		支持多层级资产组划分资产，提供自定义资产组功能； 支持多个视角的资产视图查看，包括普通分组、安全域、物理位置及未分组资产，支持将未分组资产默认加入“未分组资产”。
		支持通过接入流量日志或其他各类安全日志，标识未纳管资产，加入至资产确认资产列表中
	漏洞管理	漏洞可自动关联影响到的资产信息；支持对漏洞进行批量快速处置。
大数据中心子系统	数据解析	支持图形化在线配置数据解析规则； 支持规则嵌套和逻辑组合方式，能够对一组事件进行多层规则解析处理； 支持添加、删除、重命名、合并、拆分与裁剪现有字段，对范式化后字段再解析处理； 支持多种数据解析，包含精准匹配、包含再解析、正则匹配后从数据头、尾进行二次解析等处理 。

		支持字段解析的自动化智能推荐，根据该日志数据的特点自动推荐匹配优先的对象类型，同时在字段映射时自动推荐靠前的字段类型。系统用不同的颜色提示推荐字段的匹配程度，减少人为选择的错误并提高效率。（提供产品功能截图证明）
		支持配置自定义丰富化策略，指定日志中的任意字段，上传映射表，富化需要的字段。（提供产品功能截图证明）
	数据分权	每个新的组织机构建立以后，系统自动为该组织机构分配日志、告警、安全事件、资产脆弱性的默认权限，在此基础上用户可以根据实际业务需求进行字段级别的权限细化调整。（提供产品功能截图证明）
		支持针对日志、告警、安全事件、资产脆弱性使用不同的分权条件；支持通过任意可检索字段或字段组合进行数据分权的细化配置；支持按照组织机构配置用户对业务数据的查看权限，并对历史数据生效。（提供产品功能截图证明）
平台对接	对接服务	按需个性化对接网信潮之讯、海宁本地驾驶舱。

3.2 网络流量采集服务：提供政务外网全流量、嘉兴政务云海宁分中心云网络流量采集服务。具体要求如下表：

服务名称	服务子项	服务要求
网络流量采集服务	威胁流量展示	政务外网安全监管平台上展示政务外网、信创和非信创区政务云专有云和政务公有云实时威胁流量。
	数据采集策略制定服务	支持基于源地址、目的地址、服务、流量采样比、时间进行选择数据采集对象，可以针对采集对象进行网络流量数据采集和威胁检测数据采集，网络流量数据采集支持自定义流量载荷的格式和流量上下行载的长度。
	SSL旁路解密策略制定服务	支持基于SSL协议的HTTPS流量进行解密，可添加基于源地址、目的地址的解密策略。
		支持明文流量镜像。
		支持添加SSL入站检查配置文件。SSL入站检查配置文件中指定SSL解密证书。
	TCP流量采集服务	支持解析、生成及外发TCP流量日志。包括：传感器序列号、TCP数据流的结束方式、TCP数据流开始的时间、源IP、源端口、目的IP、目的端口、源mac、目的mac、协议、上行字节数、下行字节数、客户端系统信息、服务端系统信息、TCP 流的统计信息等字段。
	UDP流量采集服务	支持解析、生成及外发UDP流量日志。包含：传感器序列号、UDP数据流开始的时间、UDP数据流结束的时间、源ip、源端口、目的ip、目的端口、源mac、目的mac、协议、上行字节数、下行字节数、上行包数、下行包数段。
	Web访问流量采集服务	支持解析、生成及外发Web访问日志。包括：传感器序列号、日志生成时间、源ip、源端口、目的ip、目的端口、HTTP请求方法、HTTP包头的URI字段、uri_md5值、host字段、host_md5值、origin字段、cookie字段、ser-Agent字段、referer字段、链接来源、原始数据、http状态码、Content类型等字段。

	域名解析流量采集服务	支持解析、生成及外发域名解析日志。包括：时间、源 ip、源端口、目的 ip、目的端口、DNS 访问类型、Host、Host 字段_MD5 值、地址资源、MX 记录、响应结果状态、域名规范名称等字段。
	文件传输流量采集服务	支持 FTP/SMB/TFTP 三种协议的解析、生成及外发文件传输日志。包括：传感器序列号、协议、日志生成时间、客户端 IP、客户端应用端口、服务端 IP、服务端应用端口、传输模式、文件名字、文件 md5、文件类型等字段。
	邮件行为采集服务	支持解析、生成及外发 pop3、smtp、imap、webmail 协议的邮件行为日志。包括：传感器序列号、协议、message-id 信息、生成时间、源 ip、源端口、目的 ip、目的端口、邮件发送/接收时间、邮件抄送人、主题、被当前邮件回复的邮件 ID、密送人、附件名字、回访路径、邮件实际接收者、附件 md5、mime_type、邮件正文等字段。
	文件还原服务	支持分析多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB；可执行文件还原格式包含：EXE、DLL、OCX、SYS、COM、apk 等；压缩文件还原格式包含：RAR、ZIP、GZ、7Z 等；文档类型的还原格式包含：word、excel、pdf、rtf、ppt 等。
	Web 威胁检测服务	支持 Web 威胁检测，包括：Web 扫描攻击、Webshell 后门访问行为检测、DDoS、撞库攻击、SQL 注入攻击、跨站脚本攻击、命令执行和文件包含。
	备用探针(硬件)	硬件配置：机架式 2U 服 务器（含导轨），16 核心 32 线程（海光）CPU，128GB 内存，2*1GE 电口 + 2*10GE 光口(自带光纤模块)，550W 冗余电源，1*8T 3.5 寸企业级存储硬盘，3 个 USB 接口，3 网卡扩展槽，国产化品牌； 2、性能参数：应用层吞吐量：5Gbps，网络层吞吐量≤10Gbps 3、产品主要功能模块：流量采集、协议识别解析、威胁监测、策略管理等

3.3 违规外联监测服务：对政务外网违规外联情况进行 7×24 小时监测和处置。

服务名称	服务子项	指标要求
违规外联监测服务	违规外联事件分析服务	行为监测与识别：通过技术手段对网络中的设备行为进行实时监测，识别出可能存在的违规外联行为。 事件调查与溯源：在发现违规外联行为后，进一步调查该行为的主体、时间、频率、访问的外部网络地址等详细信息，追溯事件的根源，确定违规外联的操作人员、设备以及具体的操作过程，分析其背后可能存在的意图和动机。 风险评估与影响分析：评估违规外联事件可能对组织的信息安全造成的风险和影响程度，如是否导致了敏感数据的泄露、是否使内部网络遭受了病毒或恶意软件的攻击、是否破坏了网络的正常运行等，并确定事件的严重级别，以便采取相应的应对措施
	违规外联单位定位服务	收集和分析网络设备、安全设备、服务器等产生的日志信息，这些日志记录了网络中的各种操作和事件，通过对日志的详细审计和分析，可以追踪到违规外联行为的源头，确定具体的设备 IP 地址、MAC 地址等标识信息，进而定位到所属单位或部门。
	整改通报服务	在发现违规外联行为并完成初步调查后，及时向存在违规行为的单位或部门发送整改通知，明确指出存在的问题、违规行为的性质和严重性，并提供具体的整改措施和建议，指导其进行有效的整改，帮助其了解违规外联的风险和后果，提高其信息安全意识。并对整改进度进行实时跟踪。

	效果评估服务	对整改效果进行检测和验证，检查是否存在仍然存在的违规外联隐患或漏洞，确认是否已经有效阻断了违规外联行为，确保网络的安全性得到了实质性的提升

3.4 漏描和渗透测试服务：具体要求如下表：

服务名称	服务子项	服务要求
多样化安全检查服务	漏洞扫描服务	提供不少于 3 套不同品牌的扫描器能力；具备网络终端主机、云服务器资产高危端口、高危漏洞、弱密码进行异构安全风险检查等功能。 1、支持对网络设备、虚拟化平台、主流数据库、的扫描。 2、具备弱口令扫描功能，支持弱口令扫描协议数量≥10 种，允许用户自定义用户、密码字典。 3、支持对各种移动设备、国产化操作系统、网络设备、常用软件、应用系统、主流的云计算平台、物联网设备的识别和漏洞扫描。 4、支持主机扫描、网站扫描、数据库扫描、基线配置等多种任务类型。 5、支持常见数据库与国产数据库的登录扫描与漏洞检查。 6、支持 Kafka 等常见大数据组件的配置核查。 7、支持扫描任务的自动报表，包含 word、excel 等多种格式类型。 8、至少每季度开展一次全量漏洞扫描，输出报告(盖章)。
	重大信息系统渗透测试服务	1、每年开展不少于两次专业渗透，测试人员需结合自动化渗透测试系统开展政务云重点应用系统渗透测试工作，且重大信息系统的覆盖（含等保三级、关基等）。 2、在采购人的授权和监督下，模拟黑客对业务系统进行非破坏性的安全测试，查找存在的逻辑漏洞并进行利用。 3、对检测到的安全漏洞，现场进行人工的漏洞验证工作，在漏洞修复完成后在规定时限内完成复测，确保漏洞修复的有效性。 4、交付详细的渗透测试报告与漏洞修复建议(盖章)。

3.5 机器人服务：按需接入政务云侧、政务外网侧、部门侧机器人进行实时告警。具体要求如下表：

服务名称	服务子项	服务要求
	系统控制与调度服务	告警处理流程，支持周期性告警检测、增量数据处理和告警计数限制检查。
		配置管理，支持多配置节管理、集中式配置存储和配置自动持久化功能。
		错误恢复，支持自动重试、凭据自动更新和服务器时间同步功能。
		设备接入，支持自动化登录流程和安全 TLS 连接处理。
	告警处理与分析服务	告警过滤，支持双层过滤机制和复杂逻辑表达式，能有效减少误报。
		威胁评估，支持中等、高、严重三级威胁分类和实时告警评估。
		特定攻击监控，支持 IP 范围监控、扫描器检测和重点攻击检查功能。
		高级分析，支持告警汇总分析、深度告警解析和特殊数据包处理功能。

机器人服务	资产归集与IP查询服务	多模式查询，支持单IP查询、批量查询和智能识别内网IP类型功能。
		资产映射，支持自定义IP资产信息，实现IP与业务系统的关联映射。
		输出格式，支持标准输出、静默模式和文件输出等多种结果展示方式。
	通知与预警服务	通知渠道，支持钉钉企业通知、浙政钉通知、邮件通知等多种通知方式。
		通知策略，支持根据威胁级别的差异化通知策略和紧急情况下进行通知所有人。
		告警格式，支持富文本消息格式，提供详细的攻击上下文和威胁信息。
		汇总报告，支持定期生成攻击趋势、源IP分布和威胁类型等汇总分析报告。
	系统维护与管理服务	生命周期管理，支持系统启动、运行状态监控和正常/异常退出处理。
		日志记录，支持详细的运行日志记录，包括处理计数和错误情况。
		性能优化，支持高性能的数据处理和低资源占用的长期稳定运行。
		可扩展性，支持插件化扩展，可对接多种安全设备和第三方系统。
	系统集成服务	设备兼容，支持多种安全设备的接入，适应不同厂商的告警格式。
		环境适应性，支持Windows、Linux等多种操作系统环境，适应不同网络架构。
		部署灵活性，支持单机部署、云部署等多种部署方式。
	运行环境	提供机器人运行所需的配套运行环境。

3.6 运维服务

中标供应商须提供2名有相关攻防演练经验的驻场工程师。驻场工程师提供运维服务（7×24小时应急保障），配合制定和落实网络与数据安全管理制度，执行监督管理和检查工作，包括但不限于监管制度的建立、安全培训、安全意识宣贯、重保活动支撑，监管平台的维护，监管服务的常态化开展，监管问题的发现与通报等。具体内容如下：

运维服务	7*24小时实时对政务外网、政务云流量监测，对异常流量进行分析研判，对各类告警进行筛选，提取真实风险信息，对隐患进行反馈和闭环处置。危急告警不得遗漏。
	按需上机排查恶意程序，失陷主机攻击链溯源，遭受攻击时及时阻断等。
	护网和重保时期，进行7*24小时网络安全重点保障值守，并对网络安全情况进行及时响应与处置。
	对下发或自行发现的“三高一弱”网络安全隐患，进行及时排查与修复,闭环处置。
	每月进行政务外网安全隐患主动探测（高危端口与高危服务），对隐患进行反馈和闭环处置。
	进行海宁市政务云应用上线检测审核。
	有在网络安全攻防演练中，担任攻击队队员、裁判员等角色能力。
	撰写网络安全周报和月报（月报需中标方分管领导签字、盖章），每月提取2-3个典型案例形成PPT。
	协助安全管理制度制定、安全培训、安全宣贯。
	保障安全监管平台的稳定运行和安全。
	完成有关网络安全的其他事宜。

3.7 硬件续保

设备类型	型号	服务类型	数量	时长
政务外网出口防火墙	山石网科 SG-6000-E5660	原厂硬件保修服务、应用特征库更新服务	1	一年
外联监测设备	远望信息 ABPS1700-2H2X	原厂硬件保修服务、系统软件升级服务、威胁情报更新服务，监测服务授权	1	一年
网络流量探针	奇安信网神 TSGZNDS9000-TZ15M	原厂硬件保修服务、系统软件升级服务、威胁情报更新服务	2	一年
漏洞扫描设备	网神 SecVSS 3600 S5000-W020P	原厂硬件保修服务、系统软件升级服务	1	一年

第四条 考核要求

4.1 平台服务年 SLA 可用性≥99.99%，每下降一个百分点，扣除合同金额 1%，不可抗力情形需提供情况说明，业主方认可后予以剔除。

4.2 在服务和建设期内，因服务不到位导致发生重大网络安全事故的或被省级及以上通报的每发生一起扣除合同金额 10%。

4.3 利旧设备发生故障，要求在 1 小时内向响应，5 个工作日内无法修复的，需提供不低于现有配置设备备件，若原设备无法修复的，则备件留用以确保服务正常提供。

4.4 运维团队人员出现被保密办认定不宜承担相关工作的（无论发生时间），自动解约。

第五条 违约与赔偿责任

5.1 交付违约

5.1.1 每延期 1 天，乙方应向甲方支付合同总价 0.5%的违约金，但违约金的总数不超过合同总价的 10%.

5.1.2 每阶段如延期时间超过 20 天，甲方有权解除合同，除没收乙方履约保证金以外，并由乙方赔偿造成的损失。

5.2 保密违约

任何一方违反本合同所规定的保密义务，违约方应按本合同总价的 1%支付违约金。如包括利润在内的实际损失超过该违约金的，受损失一方有权要求对方赔偿超过部分。

5.3 其它条款违约任何一方违反本合同所规定的义务，除本合同另有规定外，违约方应按合同总价 1 %的金额向对方支付违约金。

5.4 如发生违约事件，守约方要求违约方支付违约金时，应以书面方式通知违约方，内容包括违约事件、违约金、支付时间和方式等。违约方在收到上述通知后，应于 5 天内答复对方，并支付违约金。如双方不能就此达成一致意见，将按照本合同所规定的争议解决条款解决双方的纠纷，但任何一方不得采取非法手段或以损害本项目的方式实现违约金。

第六条 其它

6.1如本合同附件中的条款或本合同签署之前所签署的任何文件与本合同的条款相冲突或不一致，以本合同为准。

6.2不可抗力

6.2.1由于地震、台风、水灾、火灾、战争等不能预见、不能避免并不能克服的不可抗力，直接影响本合同的履行或者不能按照合同的约定履行时，遇有上述不可抗力的一方可以免除相关合同责任。但遇有上述不可抗力的一方应立即书面通知对方，并在15天之内提供不可抗力的详细情况及合同不能履行，或者部分不能履行，或者需要延期履行的理由和有效的证明文件。按不可抗力对履行合同影响的程度，由双方协商决定是否解除合同，或者部分免除履行合同的义务，或者延期履行合同。一方迟延履行本合同时发生不可抗力的，迟延方的合同义务不能免除。

6.2.2受到不可抗力影响的一方，应尽可能地采取合理的行为和适当的措施减轻不可抗力对本合同的履行所造成的影响。没有采取适当措施致使损失扩大的，该方不得就扩大损失的部分要求免责或赔偿。

6.3任何一方欲改变通讯地址，应提前30天以书面形式通知对方。

6.4 如合同双方在履行本合同过程中发生争议，并进入司法等争端解决程序，任何一方可以将生效判决提交给本市的联合征信机构。

甲方（盖章）：海宁市政务服务管理办公室

地址：海宁市海州西路226号

法定代表人（授权代表）：

联系人：

联系电话：13957359105

日期：二〇二五年6月24日

乙方（盖章）：中国联合网络通信有限公司嘉兴市分公司

地址：嘉兴市洪兴路1281号

法定代表人（授权代表）：

联系人：15657376587

联系电话：

开户银行：

账号：

日期：二〇二五年6月24日