政府采购合同

项目名称：绍兴市急救中心网络安全设备和安全服务项目

甲方：绍兴市急救中心

乙方：浙江安腾信息技术有限公司

签订地：浙江省绍兴市

签订日期：2023 年 6 月 12 日

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》及绍兴市急救中心网络安全设备和安全服务项目项目编号：ZJXSC2023-060 号采购文件要求，经公开采购，上列双方就中标服务买卖达成如下协议。

1.服务与设备名称、价格、次数（详见附件一）

序号	名称	品牌	型号	数量	单价	总价	交货期	质保期/服务要求（年限）	税率
安全设备									
1	主机安全加固系统	明焰安全	明焰主机安全防护系统 5.0	1	79500	79500	30 个工作日	质保期：3 年	13%
2	态势感知系统（核心产品）	绿盟	绿盟安全管理平台 ESP-HNX3-HH1010	1	195500	195500	30 个工作日	质保期：3 年	
			绿盟综合威胁探针系统 UTSNX3-HD4100	1	75000	75000	30 个工作日	质保期：3 年	
3	运维管控与安全运营平台	德是铠	DSK-OPS-VM	1	96000	96000	30 个工作日	质保期：3 年	
安全服务									
4	漏洞检测与加固服务	安腾信息	定制	4	8000	32000	1 年内，按服务进度	服务期：1 年	6%
5	安全巡检与加固服务	安腾信息	定制	4	5000	20000	1 年内，按服务进度	服务期：1 年	
6	应急响应服务	安腾信息	定制	1	20000	20000	1 年内，按服务进度	服务期：1 年	
总价（含税）		小写：518000.00							
		大写：伍拾壹万捌仟元整							

2.服务期、地点

2.1 服务期：合同签订之日起壹年。

2.2 服务地点：绍兴市急救中心。

3.付款方式

合同签订后30个工作日内支付合同价的40%，设备安装调试完成，经验收合格后付清余款。

甲方迟延支付乙方款项的，向乙方支付逾期利息。双方可以在合同专用条款中约定逾期利率，约定利率不得低于合同订立时1年期贷款市场报价利率；未作约定的，按照每日利率万分之五支付逾期利息。

4.甲方的权利和义务

4.1 按合同约定的付款方式及时向乙方支付合同款。

4.2 指派专人组织成立项目工作组，有权对乙方项目实施质量的监督检查和办理本合同中约定的事宜。

4.3 负责协调乙方与相关部门的关系，做好本项目实施中需要协调的工作。

4.4 对乙方在项目实施过程中呈报的有关报告在5个工作日内回复。

4.5 在正式接受乙方的验收报告后根据乙方的验收报告在5个工作日内组织验收。

5.乙方的权利和义务

5.1 按照本合同确定的工程进度认真、按时完成各阶段的任务，确保工作质量。及时向甲方提交书面汇报及各类文档，并须得到甲方书面确认。

5.2 应与甲方签订网络安全、保密协议，提供技术人员安全背景审查、技术资质资料，规范开展技术服务，乙方保证对接触到的甲方敏感信息、数据履行严格保密义务，非经甲方书面同意不得向第三方披露。

5.3 提交项目实施计划报甲方审批同意，按照甲方要求及时向甲方提交阶段性工

作汇报。

5.4 提供所有设备的安装、调试、开发、服务和培训的全部内容，包括完整、准确、详细的技术文档，在系统设计、开发、安装、调试中负责解决与本项目有关的相应技术问题。

5.5 在进行项目建设时，对项目的全部现场操作、运营保障、技术措施、可靠安全性负完全责任，承担在实施过程中非甲方原因发生的一切事故。

5.6 及时响应甲方的服务要求，认真做好现场技术服务。发生网络安全事件时，需在 10 分钟内响应、2 小时内抵达用户现场。

5.7 积极配合甲方做好项目验收工作，提交验收所需文档。

5.8 在本合同项目执行过程中，接受甲方的检查和监督。

5.9 在甲方单位工作时，遵守甲方相关规章、制度等。

5.10 乙方保证服务过程中规范操作，维护甲方的数据安全、网络安全，若因乙方过错导致甲方数据泄露、网络被入侵的，乙方愿意承担相关责任。

6 违约责任

6.1 除不可抗力外，如果乙方没有按照本合同约定的期限、地点和方式提供服务，那么甲方可要求乙方支付违约金，违约金按 1000 元/次计算，最高限额为本合同总价的 5 %；未按要求提供服务的违约金计算数额达到前述最高限额之日起，甲方有权在要求乙方支付违约金的同时，书面通知乙方解除本合同；

6.2 除不可抗力外，如果甲方没有按照本合同约定的付款方式付款，那么乙方可要求甲方支付违约金，违约金按每迟延付款一日的应付而未付款的 0.5%计算，最高限额为本合同总价的 5 %；迟延付款的违约金计算数额达到前述最高限额之日起，乙方有权在要求甲方支付违约金的同时，书面通知甲方解除本合同；

6.3 除不可抗力外，任何一方未能履行本合同约定的其他主要义务，经催告后在合理期限内仍未履行的，或者任何一方有其他违约行为致使不能实现合同目的的，或者任何一方有腐败行为（即：提供或给予或接受或索取任何财物或其他好处或者采取其他不正当手段影响对方当事人在合同签订、履行过程中的行为）或者欺

诈行为（即：以谎报事实或者隐瞒真相的方法来影响对方当事人在合同签订、履行过程中的行为）的，对方当事人可以书面通知违约方解除本合同；

6.4 任何一方按照前述约定要求违约方支付违约金的同时，仍有权要求违约方继续履行合同、采取补救措施，并有权按照己方实际损失情况要求违约方赔偿损失；任何一方按照前述约定要求解除本合同的同时，仍有权要求违约方支付违约金和按照己方实际损失情况要求违约方赔偿损失；且守约方行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式；

6.5 除前述约定外，除不可抗力外，任何一方未能履行本合同约定的义务，对方当事人均有权要求继续履行、采取补救措施或者赔偿损失等，且对方当事人行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式；

6.6 如果出现政府采购监督管理部门在处理投诉事项期间，书面通知甲方暂停采购活动的情形，或者询问或质疑事项可能影响中标结果的，导致甲方中止履行合同的情形，均不视为甲方违约。

7.解决合同纠纷的方式

7.1 凡有关本合同或与本合同中发生的争端，双方应通过友好协商，妥善解决。如通过协商仍不能解决时，可向当地的仲裁机构申请仲裁或人民法院起诉。

7.2 仲裁、诉讼、律师费用除仲裁机构和人民法院另有裁决外，由败诉方承担。

7.3 本合同一式肆分，甲乙双方各执贰份，合同应在双方签字盖章后开始生效。

甲方：

统一社会信用代码：

住所：

法定代表人或

授权代表（签字）：

联系人：

约定送达地址：

邮政编码：

电话：

传真：

电子邮箱：

开户银行：

开户名称：

开户账号：

乙方：

统一社会信用代码或身份证号码：

91330602MA2BHH2Q5N

住所：浙江省绍兴市越城区迪荡街道平江路2号复旦科技园绍兴创新中心1号楼23楼2301室

法定代表人或

授权代表（签字）：何青

联系人：何青

约定送达地址：

邮政编码：312000

电话：

传真：

电子邮箱：

开户银行：招商银行绍兴分行城东支行

开户名称：浙江安腾信息技术有限公司

开户账号：575904770311000 16

附件一：

1.安全设备清单：

序号	产品名称	产品参数	交付物	质保期	数量
1	主机安全加固系统	服务器安全管理系统管理控制中心+20个点客户端授权： 1.服务器安全管理系统管理控制中心，包括安全管理中心和审计中心，用于统一管理受保护的服务器端，统一下发策略，系统账户配置，日志审计等。 2.服务器安全管理系统20个点客户端授权，可对服务器系统安全涉及的控制点（如身份鉴别、敏感标记、强制访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防和资源控制等）形成立体防护，解决操作系统层面面临的恶意代码执行、越权访问、数据泄露、破坏数据机密性、完整性等各种攻击行为。 3.支持windows、linux、unix服务器操作系统。默认包含三年授权服务。	软件	三年	1套
2	态势感知系统（核心产品）	态势感知平台+流量探针： 1.平台参数：2U标准机架硬件，≥128G内存，≥256G SSD硬盘，≥16T SATA硬盘，支持RAID，≥6个千兆电口，≥2个接口拓展插槽，含交流冗余电源。 2.探针参数：1U机架式设备，含交流冗余电源，≥1TB硬盘，≥1个管理口，≥2个usb接口，≥1个RJ45串口，≥6个千兆电口，≥4个千兆光口，≥1个接口拓展插槽。	硬件	三年	1套
3	运维管控与安全运营平台	1.一体化、可视化、自动化、安全化、智能化的新一代开放式智能运维安全管理平台。 2.基于大数据技术、智能分析和可视化展示为基础开发的一套解决运维数据分析难题的系统平台。 3.通过采取主动的运维分析和实时态势感知，有效整合网络、服务器、机房基础环境、视频监控、资产等管理。 4.一个管理平台监测整体IT系统，用于解决T运维工作所面临的全方面需求。 5.1U19寸标准机架式主机，内置6个千兆网口，1个VGA接口，	硬件	三年	1个

		2 个 USB 接口。64G 硬盘，交流电源供电。 6. 硬件标准版。内置 100 个授权许可			

2. 安全服务清单：

序号	服务名称	服务期	数量	单位	备注
1	漏洞检测与加固服务	1 年	4	次	/
2	安全巡检与加固服务	1 年	4	次	/
3	应急响应服务	1 年	1	项	按需响应，无次数限制

附件二：安全设备技术参数

1.主机安全加固系统

技术指标	指标要求
产品要求	★服务器安全管理系统管理控制中心+20 个点(Windows:3 台 Linux:17 台) 1.服务器安全管理系统管理控制中心，包括安全管理中心和审计中心，用于统一管理受保护的服务器端，统一下发策略，系统账户配置，日志审计等。 2.服务器安全管理系统 20 个点客户端授权，可对服务器系统安全涉及的控制点（如身份鉴别、敏感标记、强制访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防和资源控制等）形成立体防护，解决操作系统层面面临的恶意代码执行、越权访问、数据泄露、破坏数据机密性、完整性等各种攻击行为。 3.支持 windows、linux、unix 服务器操作系统。默认包含三年授权服务。
安全机制	支持自我防护技术，即使客户端被意外关闭，防护依然有效。
主机资产信息全局展示与搜索	支持全量资产的关键字及语法搜索，支持检索的语法包括但不限于：服务器资产类、进程资产类、账号资产类、软件应用类、web 资产类、web 服务类、web 框架、数据库类、端口资产类、网络连接类、启动服务类、安装包类、计划任务类、环境变量类、内核类、类库资产类、注册表类、证书资产类进行检索。
服务器基础信息	支持以列表的形式，统一列出 Windows/Linux 服务器基础信息，并在列表中对服务器的关键软硬件进行统计，包括但不限于：CPU 数、CPU 核数、分区数、账户数、软件应用数、web 站点数、web 服务数、web 框架数、数据库数、端口数、网络连接数、启动服务数、安装包数、计划任务数、环境变量数、内核模块数、证书数、注册表数、类库数等。
进程资产	支持以列表的形式，统一列出 Windows/Linux 服务器进程资产，并可查看进程的软件包名、运行时间、同步时间、启动参数等信息。
端口	支持以列表的形式，统一列出 Windows/Linux 服务器端口资产，并可查看端口号、协议、端口状态、绑定 IP、监听进程等信息。
网络连接	支持以列表的形式，统一列出 Windows/Linux 服务器的进程连接资产，并可查看进程名称、协议、IP 地址、源端口、目标端口、目标 IP、连接状态、同步时间等信息。
应用白名单	支持对一台或一组服务器进行白名单学习策略，并可设置学习时长，学习后可形成应用列表及 HASH 值，对偏离学习列表以外的应用进行告警和拦截。
端口白名单	支持设置端口的暴露控制规则，包括但不限于：禁止/允许外网暴露、禁止/允许内网暴露等策略，并支持例外端口的添加。

外连白名单	支持对服务器的进程外连控制进行规则设置，包括但不限于：禁止/允许进程外连外网、禁止/允许进程外连内网，并支持进程白名单和例外进程的设置。
风险账户及弱口令检测	支持对服务器中复用的相同密码进行检测，可识别出某个密码被哪些服务器、哪个账户、哪个应用、哪个版本进行了复用。
病毒查杀	可对服务器杀毒引擎进行综合的设置，支持本地查杀、控制中心查杀的设置与切换，并可对某台服务器的查杀规则进行详细设置。
恶意扫描	以攻击者视角、受害者视角展示恶意扫描的事件，包括：服务器名称、负责人、所属部门、操作地址、最近发生时间、受害 IP、攻击 IP 等信息，并可将事件加入黑名单或白名单，还可对受害的 IP 进行防端口扫描、屏蔽扫描器等设置。
暴力破解	对暴力登录系统的账号和 IP 进行自动发现并上报暴力破解入侵事件，并可对攻击的 IP 进行封停、解封、加白等操作。
异常登录	支持以违规登录视角对异常登录行为进行监控及告警，并可查看违规登录的账号、来源 IP、登录区域、服务器 IP、操作系统等信息，并可进行登陆规则策略的设置和告警设置。
后门检测	对操作系统、文件、软件中存在的后门进行检测，包括：发现时间、后门名称、后门类型、风险等级、服务器名称、服务器 IP、操作系统等，并可进行隔离、删除、加白、下载等操作，并提供后门的详情信息。
webshell	支持对内存堆栈调用行为特征的分析，可有效检测常见工具的内存 WebShell 攻击，可对内存攻击行为告警及处置。
反弹 shell	支持查看反弹 shell 的详情，包括基本信息、连接进程信息、命令行信息，并以图形化的形式展示进程树信息，用于反弹 shell 的详细溯源。
本地提权	支持查看提权的详情，并以图形化的形式展示提权进程树信息，用于本地提权的溯源。
无文件攻击	支持实时监控服务器上发生的无文件攻击（漏洞型攻击、灰色工具型攻击、潜伏型攻击）事件，并对无文件攻击事件进行加白、标记处置等操作。
OOB 带外攻击	支持 OOB 带外攻击检测，并支持黑域名的添加与同步。
RCE 利用	基于行为分析，检测对外服务的远程命令执行漏洞利用行为，实现实时告警和追溯。
In-app WAF	支持通过插件的方式，工作于 IIS、Apache、Nginx 等 web 中间件内部，通过判断流量特征和 WAF 规则引擎，对访问流量进行监控或防护，阻断 SQL 注入、XSS、漏洞利用等 Web 攻击。

2. 态势感知平台：

指标项	具体指标要求
硬件架构与性能	★2U 标准机架硬件，≥128G 内存，≥256G SSD 硬盘，≥16T SATA 硬盘，支持 RAID，≥6 个千兆电口，≥2 个接口拓展插槽，含交流冗余电源。硬件配置及系统要求符合国产化

	或新创要求。
	平均处理能力（每秒日志解析能力 EPS）≥500EPS，含日志威胁管理、全流量威胁管理、脆弱性管理、网站安全检测、一键响应、态势感知等功能。
数据采集	平台应支持内置 600+设备日志解析规则查看以及筛选，包括但不限于网络设备、安全设备、终端主机日志、数据库等。
	平台应支持界面化配置规范化规则采集第三方日志实现异构日志格式归一化。
	平台应支持外部备份机制，支持超长日志存储，支持通过 NFS 自动备份日志到外部服务器上，支持备份日志自动加密存储，支持内外部存储统一展示，支持外部备份文件可恢复可搜索，提供产品功能截图证明。
威胁检测与分析	平台应支持规则分析能力，应支持不少于 300 种内置分析识别规则并支持内置规则的升级，支持用户自定义规则，用户自定义规则可以支持导入导出。
	平台应支持对失陷资产进行判定并提供失陷资产的判定依据，具备攻陷主机自动判定的能力，提供第三方权威机构证明材料。
	平台应支持简易模式和专家模式的两种自定义规则，可支持用户在选择日志类型、设置常见日志类型字段过滤条件之后，即可新建或编辑规则，从而生成事件。提供产品功能截图证明。
	平台应支持外部威胁分析，支持 Web 漏洞攻击、暴力破解、SQL 注入、XSS 跨站脚本攻击等分页面统计分析，支持外部攻击源 Top5、外部攻击源地区 Top5，支持影响资产 Top5、影响资产组 Top5 等。
	平台应支持横向威胁分析，支持僵木蠕、扫描探测等分页面统计分析，支持攻击者 Top5、受害者 Top5，支持攻击者资产组 Top5、受害者资产组 Top5 等。
	▲平台应支持主机、应用等弱口令访问行为的检测，弱密码应加密展示且需要管理员的二次独立认证授权后方可查阅明文弱口令。同时支持批量导出弱口令帐号能力以便于弱口令帐号的分发整改，提供第三方机构证明材料。
	平台应支持与城市热点认证计费系统对接，支持安全事件中动态 IP 对应到账户，并支持用户威胁分析。
资产管理	平台应支持多维度资产管理，进行多维度资产视图分析，系统至少内置五种视图：资产组视图、业务系统视图、组织结构视图、地理位置视图、行业视图。
	▲平台应具备资产保护的能力，提供第三方机构证明材料。

	平台应支持资产稽查比对，对于实时发现资产和已有资产库资产比对分析资产新增、变更、减少的情况；并支持对资产发现结果进行处理，可选择入库或者丢弃。
漏洞管理	平台应支持漏洞库管理能力，本地漏洞数应不少于5万，支持漏洞模板自定义和配置模板管理，支持漏洞库升级。
	平台应支持漏洞扫描结果手动和自动验证能力，可手动选择部分漏洞处置单进行验证扫描，支持漏洞批量处置；提供产品功能截图证明。
	平台应支持漏洞扫描结果自动生成漏洞处置单的能力，支持对漏洞处置单闭环处理，可设置漏洞处置单状态包括：新增、待修复、已修复、已验证、单次忽略、永久忽略；提供产品功能截图证明。
	平台应支持漏洞报表功能，可选择生成资产风险报表、系统扫描报表、网站扫描报表、漏洞处置报表、配置核查报表等，为客户撰写安全分析报告提供支撑。
态势呈现	平台应支持所监测网络安全情况的态势呈现能力，态势呈现包括但不限于综合安全态势、外部威胁态势、内部威胁态势、外连威胁态势、脆弱性态势、资产态势、运维响应态势。
	▲平台应具备确定网络安全态势分布的能力，提供第三方机构证明材料。
	平台应支持纵深防御体系可视化，边界防御、内网防御、安管中心动态展示安全建设运营效果，运营效率数字量化，响应手段可视化。
事件运维与监控	平台应支持对威胁、失陷主机、漏洞等事件进行统一运维处理，提供统一入口。
	平台应支持对各类运维事件进行运维处置，包括但不限于提交研判人员进行分析、忽略、误报、处置、优先处理等。
	平台应支持将威胁、漏洞、失陷资产等事件以工单的形式通知用户进行工单处理，支持邮件通知，提供产品功能截图证明。
一键封堵	平台应支持针对IP、域名、会话进行封堵，支持主机隔离、流量牵引等方式联动设备进行封堵，设备类型包括但不限于防火墙、抗拒绝服务系统、WEB应用防火墙、网络流量探针等。
	▲平台应支持封堵状态获取及查看，支持判断封堵成功、封堵失败、解封成功、解封失败等状态，提供产品功能截图证明。
报表管理	平台应支持自动报表，支持日报、周报、月报、季报、半年报、年报，支持按时自动生成报表，支持报表订阅，支持日历模式和列表模式可切换，支持基于报表类型、报表模板、报表名称、生成时间段的查询，查找指定的报表。

产品资质	具备安全管理平台类《计算机信息系统安全专用产品销售许可证》，提供有效证书复印件。
	具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》，提供有效证书复印件。
厂商资质	厂商须通过软件能力成熟度 CMMI Level 5 (V2.0)认证，提供相关证明材料。
	厂商应具备国家信息安全测评信息安全服务资质证书-安全开发类（二级），提供相关证明材料。

3.流量探针

指标项	具体指标要求
硬件需求	1U 机架式设备，含交流冗余电源，≥1TB 硬盘，≥1 个管理口，≥2 个 usb 接口，≥1 个 RJ45 串口，≥6 个千兆电口，≥4 个千兆光口，≥1 个接口拓展插槽。
性能需求	网络层吞吐量≥1.5 Gbps；http 吞吐量≥1.5 Gbps；包含流量采集、元数据提取、存储等功能。
流量采集	支持导入 HTTPS 证书，对流量进行解密和还原，含 SSL3.0、TLS1.0/1.1/1.2。
	支持 VXLAN、GRE、VLAN 流量解析。
	▲支持 5G 协议的深度解析和还原，包含 NAS、NGAP、PFCP、HTTP2、GTPv2 等。提供产品功能截图证明。
	支持 N12 鉴权攻击检测、5G 信令风暴检测、UE 异常检测，提供产品功能截图证明。
流量存储	支持对实时流量采集的 pcap 包进行全量存储，供追溯分析和取证使用。
常规检测	支持多种攻击特征，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测。
	支持对 sql 注入、XSS、SSI 指令、Webshell、目录遍历、远程文件包含等网络攻击检测。
高级威胁检测	支持针对 SMTP/POP3/IMAP 等协议的钓鱼邮件检测，识别邮件内容，结合威胁情报、病毒检测等进行多维度分析，判断是否为可疑钓鱼邮件。提供产品功能截图证明。
	支持隐蔽隧道检测，检测企图绕过防护的 ICMP/DNS 隐蔽通信隧道，发现 C&C 通信。
	支持基于SVM机器学习算法对海量DGA域名样本进行训练建模，识别僵尸网络，支持HTTP/邮件正文/DNS。提供产品功能截图证明。
风险行为	支持从侦查、暴力破解、弱口令、主机外联、翻墙、异地登录、访问违规网站维度分析呈现。

威胁研判	支持对检测的告警事件结合双向检测机制、元数据、原始数据包和研判模型进行深层次研判给出告警事件的攻击结果：尝试攻击、高可疑攻击、攻击成功、失陷。
威胁分析	支持对网络中的威胁进行统计，统计类型包括：威胁事件统计和趋势、攻击者统计和趋势、失陷资产统计和趋势、漏洞统计和趋势。
威胁取证	支持将存储的恶意文件与告警关联并提供下载便于取证。提供产品功能截图证明。
资产管理	支持用户自定义内网资产网段和分组。提供产品功能截图证明。
	支持对资产进行风险评估，结合威胁事件对资产判定为是否失陷。提供产品功能截图证明。
管理功能	系统应具备系统运行状态监控功能，能够实时查看 CPU 使用率、内存使用率、磁盘剩余空间、系统运行时间、接口状态、流量等信息。
产品资质	具备《计算机信息系统安全专用产品销售许可证》，必须为（综合型安全审计类），提供有效证书复印件。
	具备《国家信息安全漏洞库兼容性资质证书》，提供有效证书复印件。
厂商资质	厂商为 CNCERT 网络安全应急服务支撑单位（国家级），提供相关证明材料。
	厂商具备国家信息安全测评信息安全服务资质证书-安全工程类（三级），提供相关证明材料。

4. 运维管控与安全运营平台：

指标项	指标要求	
系统	★管理范围	监控节点数≥100，授权许可要求包含所有需要监控的设备类型模块功能，节点数量根据 IP 地址进行统计。
	监控类型	本项目要求对 交换机、服务器、操作系统、数据库、网络安全设备、业务数据，物联网数据，机房动力环境系统，日志数据，虚拟化系统，超融合，云数据，存储，备份系统等进行全景监控。所有设备类型的监控后续无须再新增模块。
	管理界面	全中文界面，采用 HTML5 技术，要求 B/S 模式的管理，界面友好，支持基于 Web 的图形用户界面（GUI），能够以简单、直观的方式显示信息，简化配置。
	操作系统	软件基于自主开发系统或是采用 CentOS 操作系统（64 位）；通过容器化部署，方便系统的整体迁移。
	数据库	采用时序数据库，满足高性能大并发量数据的存储要求和数据查询。
	用户	支持多用户基于角色的用户管理，可以按权限进行管理。

开发	定制开发	本次项目要求厂商对系统进行定制性需要开发，开发内容包括但不限制于1、多大屏类型的大屏展示页面；2、对设备的定制性开发扩展监控；3、各应用系统的监控； 4、资产管理的定制开发等内容。定制需求周期为三年。
		要求与其他各第三方系统进行整合对接定制开发。
		支持研发现场系统优化服务。
		支持 IT 运维流程设计服务。
		支持 ITIL 与 OA 业务系统对接。
展示	大屏模块	要求系统自动多类型大屏模板，模板数量不少于 8 个，要求能进行大屏定制化开发，本项目含二套定制化大屏。
		定制大屏展示，通过可视化图表实时展示系统运行状况，大屏要求对接视频监控画面，动力环境系统运行状况，安全告警状况等多视图多屏页面 。支持不同管理视图和实时拓扑图在大屏幕上切换；要求大屏展示界面美观，并可根据用户需求来开发定制大屏界面，大屏展示系统能抽取其他业务系统数据，进行数据可视化展示及告警，要求大屏可以结合 3D 机房模块进行立体化展示。
业务服务	业务服务管理组件	可根据需求，支持定制业务系统展示模块。
准入	▲准入管理	要求投标方提供的软件具备网络接入控制功能，无需第三方软件及硬件，就可以及时发现非法占用 IP 资源，内部设备非法跨网段接入，以及外部设备非法接入内部网络，并进一步定位到设备端口，实现实时干扰，保障全网的 IP 管理秩序和网络接入安全。
堡垒系统组件	▲堡垒系统组件	具备网络设备 web terminal 远程登录功能，支持 TELNET，ssh ，RDP，web 等登录方式。实现 WEB 端与本地管理完全一样的操作和功能。
		具备设备密码的管理功能。
		支持集中管理所有用户操作记录（提供产品截图，并提供相关佐证材料）。
呼叫中心	▲Web 呼叫中心	具备 web 呼叫中心功能，可进行在线的咨询及远程服务（提供产品截图，并提供相关佐证材料）。
监控管理	监控方式	支持 SNMP、MQTT,SSH、TELNET、SFLOW、IPMI、HTTP、Agent、Rsyslog、TCPDUMP、JDBC、JMX 和仿真等方式进行数据采集。
	IPV6 支持	支持在 IPv4 和 IPv6 双栈环境和过渡架构下实时监控，实现统一平台监控和管理。

网络设备监测	可直观显示网络设备实时运行状况。可直观查看网络设备的基本属性，如当前设备的状态、IP 地址、MAC 地址、网络连接等设备信息。监测各类主流品牌网络设备的网络流量、设备性能，采集 Ping 状态、设备累计运行时间、CPU 利用率、内存利用率、端口状态、VLAN 信息、日志文件、网络流量、丢包率、设备电源、硬盘状态、风扇等监测指标。 支持通过自定义 SNMP OID 脚本，采集扩展指标项。
安全设备监测	对支持 SNMP 协议的安全设备监控。监管内容包括端口状态、流量、端口错包率，端口丢包率等信息。
服务器硬件监测	提供服务器 CPU、内存、硬盘使用，温度、健康状况等查询接入节点的实时性能数据、历史趋势数据、当前活动告警等功能。
操作系统监测	支持 UNIX、LINUX、WINDOWS 及国产操作系统主机，UNIX 系统包括 SUN Solaris，HP UNIX，IBM AIX 等；采集信息包括 CPU、内存、磁盘空间、重要进程、服务、网卡流量、日志文件、文件系统等。提供对 Windows、IBMAIX、SUNSolaris、HP-UNIX、Linux、CentOS、NovellSuse、FreeBSD 及国产操作系统实现监控管理支持主机运行的实时参数显示；支持主机一体化展现图.可以在一张图上展现主机日志、主机的应用使用情况；可通过纯软件方式直接对设备硬件进行可视化，图形化管理。
数据库监测	系统提供 ORACLE、MSSQL、MySQL、Redis、Mongo 各类数据库的监测。监测连接时间、例程名、例程开始时间、归档日志模式、会话数、连接数、事务总数、死锁数、命中率、内存、表空间、系统等待时间以及用户自定义等指标，要求对 MySql 的监控指标不少于 70 个。
中间件监测	基于监视所记录的各种中间件的状态数据，可帮助业务人员分析服务响应速度变化的技术原因和规律，在业务受到影响前，主动发现潜在问题。提供对中间件各类关键参数指标的监控，这些指标包括：基本信息，数据库连接池信息、会话信息、任务信息、JTA、JVM、Servlet、EJB、JDBC、运行队列、内存信息、线程信息等等。
应用监控	支持对多种 web 应用的实时监控，对端口状态、响应时间、连接信息等提供关键参数管理。
无线系统监测	提供无线控制状态、CPU、内存占用、AP 的在线情况，接入终端数量的实时性能数据、历史趋势数据、当前活动告警等功能。
网络链路健康分析	对业务涉及的网络的流量、带宽、延迟等信息智能分析，并基于历史监测数据，对链路进行健康度评分。
历史曲线	支持所有监控参数的历史数据查询。

		支持所有监控参数数据的 1 年内的数据查询。
		支持用户自定义时间段的历史数据查询。
物联网整合	视频动环一体化整合	提供标准机架式 1U 硬件网关系统，要求对机房的温湿度，漏水，市点、UPS，空调、门禁，视频进行集中统一监控。
		本项目要求提供一体化可视物联硬件设备。设备要求具备视频录像及回放功能，提供传感器数据告警联动可抓拍图片并录像,按照事件关联，提高录像检索与回放效率。
		支持周界或人脸视频智能分析。
		可扩展支持各类 RS485、RS232，开关量接口的物联网设备数据对接。
监控视图	监控雷达	支持雷达扫描器；雷达扫描可以直观显示所监控的节点及正常与否。
		提供监控告警类型显示以及声音告警提示。
	节点视图	提供监控节点的设备类型、系统类型、运行服务状态的直观试图。
		提过节点运行正常率的最差 TOP10 排名。
		提过节点 CPU、Memory、Disk 的使用率的排名。
	▲机柜视图	对机房内的机柜使用情况进行统一的管理，系统能够很方便的对机柜内的设备摆放情况进行编辑、调整。并能实时显示设备当前的运行状态，在需要时，可以很方便的打开机柜内设备的真实面板图进行操作。（提供产品截图，并提供相关佐证材料）
	网络接口视图	提供设备网络接口的状态、流量、收发错包/丢包直观显示（提供产品截图，并提供相关佐证材料）。
日志管理	支持设备	支持网络设备（交换机、路由器），安全设备（防火墙）系统日志管理。
		支持 Windows 全系列主机和 Linux/Unix 全系列主机日志的管理。
	日志规则库	内置大于 1000 条以上日志规则库（提供产品截图，并提供相关佐证材料）。
	日志显示	采用瀑布式日志显示，根据时间排列。
	管理功能	支持自定义日志自动移除功能。
		支持自定义日志告警规则。
		支持日志实时告警功能。
		所采集日志可以按主机、时间、告警级别自动备份。
	统计图表	可按任意指定时间、指定设备、指定事件/告警类型等条件组合查询日志。
		提供日志告警级别的统计比例饼形图。
		提供日志告警主机的 TopN 图表。

		可按指定条件生成主机事件、日期、告警级别、告警事件来源、告警事件类型的统计图表。
资产管理	资产属性	可对信息资产的属性做定制化开发优化，具备链路资产功能。
	机房资产	支持机房机架物理拓扑显示，用户可以直观地看到每个机架上的每台设备的运行状态；可以看到设备的真实面板图；支持通过鼠标拖动进行机柜内设备布局信息的调整（提供产品截图，并提供相关佐证材料）。
	资产探测	可通过 IP/端口扫描，SNMP 扫描等多种方式进行资产探测，可获取网络资产中的 IP 地址、端口号、所开服务类别、服务版本及操作系统类型等信息。
	合同管理	支持合同管理；支持设备与合同的关联。
	维保折旧	支持设备的维保管理，具有维保到期提醒功能。
		支持资产折旧管理。
	▲二维码管理	通过智能手机扫描二维码可以查看设备的信息及状态，可以进行设备信息配置以及进行资产盘点，系统具备资产盘点状态显示功能（提供产品截图，并提供相关佐证材料）。
运维辅助	IP 地址管理	提过 IP 地址资源分配管理；提供 IP 地址使用历史回溯功能；可以对 IP 地址分配、使用数据生成 Excel 或 PDF 格式的统计报表。
	全网设备定位	支持全网统一 IP/MAC/设备端口对照一览表，支持跨网段、跨地域的 IP 地址管理，自动、动态、完整提供全网所有活动用户的网络连接位置信息，可根据 IP 地址-机器名-MAC-物理端口唯一对应关系，支持 IP 全网动态定位，迅速定位其所连接到的交换机端口，便于故障定位和问题查找。
	故障管理	支持对于运维中的故障问题记录、分类、统计功能。
		支持自定义故障级别。
		支持自定义故障分类。
		可以按时间周期、故障级别、故障类型提供故障记录的图表分析。
		提供故障记录的生成 PDF 格式文档，并下载。
	运维知识库管理	能够实现对运维文档的 WEB 管理。
		可以在线编辑、上传、下载运维技术文档。
		支持常用文档格式（WORD、EXCEL、PDF、JPG 等）。
	运维通讯录	支持运维应急通信录功能。
		通信录按公司划分。

拓扑管理	拓扑功能	支持多层次网络拓扑结构图。
		支持拖拽进行设备拓扑布局。
		支持托拽直接完成设备链路连接。
		直观显示网络链接流量数值或占用情况，并以不同颜色进行显示。
		直观显示设备监控及性能监控状态，并以不同颜色进行显示。
		显示设备互联端口以及流量来源端口（提供产品截图，并提供相关佐证材料）。
	拓扑配置	用户可以自定义、编辑、修改业务拓扑图，业务拓扑的元素包括主机、网络设备、安全设备、数据库、中间件、各种类型的服务和应用。
	拓扑融合	通过点击拓扑中的设备，可直接进入对应设备流量汇总列表页面。
		通过点击拓扑中的链路，可选择进入对应链路最近四小时、最近一周、最近一月的流量报表页面。
告警管理	监控告警	支持监控主机/设备的在线监控告警；
		支持各项性能监控数据的阀值监控告警。
		支持日志告警。
	告警方式	支持自定义告警分组。
		支持 EMAIL、微信、声音、短信告警方式。
	告警记录	记录全部的告警事件。
		可以提供告警的发生时间、恢复时间信息。
		提供运维人员对于告警的确认以及处理记录功能。
	工单	提供 ITSM 工单系统进行自动化工单流程。
报告报表	报告报表	支持自动定义生成报告报表功能。
		可针对节点生成全数据统计报告。
		可生成节点运行可用性、节点资源利用率的统计报告。
		可生成资产数据统计报告。
		可生成告警报告文档。
		提供报告下载功能。
	自动巡检	系统自动巡检，并对巡检的设备系统状态按健康、故障等分类，生成巡检报告。能根据现有的手工巡检模板进行定制化开发自动化巡检功能。
服务	升级服务	提供三年免费升级，并提供终身免费日常维护指导。

附件三：安全服务技术参数

1.漏洞检测与加固服务：

序号	招标参数要求
1	服务内容： 在授权的前提下，授权第三方安全服务工程师利用专业的漏洞检测工具对指定信息系统内的网络设备、操作系统等进行漏洞识别以及 web shell 进行检测，基于已知漏洞模拟黑客的攻击方法对系统和网络进行非破坏性的攻击尝试，验证漏洞的危害性和影响。
2	**服务次数：**4 次。
3	**服务方式：**现场和远程。
4	**服务对象：**市急救中心信息系统。
5	**服务工作量：**8 人天。
6	**服务输出：**《漏洞检测与分析报告》、《渗透测试与分析报告》、《漏洞修复报告》
7	**服务工具要求：** 1.工具具备分布式部署提供远端扫描引擎列表，列表需对设备状态、策略同步、规则同步、引擎类型等状态提供最直观的展示效果（请提供相应截图证明）。 2.工具需支持多种扫描方式，提供对 IP、域名、安全域、批量检测等目标扫描方式。 3.工具应具备操作系统、数据库、网络设备等主流系统的漏洞库列表，并提供至少 20 种以上的漏洞库分类。 4.工具具备对 DNS 服务的安全漏洞检查，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（请提供相应截图证明）。 5.工具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（请提供相应截图证明）。

2.安全巡检与加固服务：

序号	招标参数要求
1	服务内容： 信息系统运行状态检查：针对市急救中心现有信息系统运行状态进行检查，提前发现软硬件运行故障隐患，提供修复建议，协助处置。 网络安全设备策略核查：针对市急救中心现有信息系统安全策略和日志进行核查，对核查结果进行分析，发现潜藏攻击线索，提供优化建议，协助风险处置。
2	**服务次数：**4 次
3	**服务工作量：**8 人天

4	**服务方式：**现场和远程。
5	**服务对象：**市急救中心 IT 资产。
6	**服务输出：**《网络安全巡检报告》、《安全策略变更申请表》、《信息系统安全巡检手册》、《年度安全巡检服务报告》

3. 应急响应服务：

序号	招标参数要求
1	服务内容： 在发生确切的网络安全事件时，应急响应实施人员应及时采取行动，限制事件扩散和影响的范围，检查所有受影响的系统，在准确判断安全事件原因的基础上，提出基于安全事件解决方案，追查事件来源，协助后续处置。 应急响应范围包括： 1、突发网络通信异常； 2、网络攻击事件溯源分析和系统加固； 3、系统升级或网络割接人员保障； 4、网络安全相关的其他工作事物。
2	**服务方式：**现场和远程。
3	**服务对象：**市急救中心全网。
4	**▲次数和时间要求：** 在服务期内**按需响应，不限次数。应急人员需在 30 分钟内抵达现场。**（投标人须承诺并提供能够符合时间要求的充分证明材料，例如地图导航车程等）
5	**服务输出：**《网络安全事件应急响应报告》、《网络安全整改建议报告》

附件：4

保密协议

甲方：绍兴市急救中心

乙方：浙江安腾信息技术有限公司

鉴于甲乙双方在技术服务项目中的合作，双方认为有必要透露各方一定的涉密信息，双方透露的信息仅用于商业合作目的并且防止任何第三方使用该信息。

鉴于双方信息的重要性，双方同意遵守如下保密条款：

1. 保密内容：

对于乙方在甲方工作期间获得和知晓的甲方专有信息、主合同价款及属于第三方但甲方负有保密义务的信息，乙方均应保守涉密。专有信息包括（但不限于）如下所列：商业涉密、技术涉密、通信或与其相关的其他信息；无论是书面的、口头的、图形的、电磁的或其它任何形式的信息。包括（但不限于）数据、模型、技术、方法和其它信息均为承诺保密的专有信息。

2. 保密措施：乙方应当以审慎态度对待甲方的专有信息。

（1） 遵守甲方有关保密的各项管理规定；

（2） 未经甲方书面许可，乙方不得将所知的甲方专有信息以任何方式提供给任何第三方，也不得擅自披露这些信息；

（3） 除了完成双方约定的工作目的之外，未经甲方书面许可，不得擅自使用甲方的上述专有信息；

（4） 未经甲方书面许可，乙方不得将从甲方得到的任何文档、图纸、资料、磁盘、胶片等载有甲方专有信息的介质带出指定的工作范围。

（5） 对于乙方因工作需要必须携带出工作范围的数据资料，需经甲方书面许可后加密或封条存储，乙方必须严格保证该数据的保密性。

（6） 对于用户数据和服务结果数据的保管、访问，乙方无关人员不能访问；必需访问的人员，乙方要进行严格的访问控制；管理用户数据的人员应由乙方严格筛选。

（7） 当乙方在甲方工作期满离开时，乙方应将包含甲方上述专有信息的一切资料及其复印件如数交还甲方，不得擅自保留；

（8） 凡是项目所涉及到保存在乙方手里的相关电子形式的专有信息，乙方要保证该信息的保密性，未经甲方同意，不得以拷贝、邮件等所有传输方式传递给第三方或项目无关人员。同时在项目完成后必须在甲方的监控下销毁上述信息。

（9） 乙方必须保证项目中所提供的评估设备的安全性，对于评估设备的数量、型号、配置、主要的运行程序等以清单的方式向甲方相关项目负责人进行说明并提请使用，经过甲方的检查、确认、同意后方可进行使用和评估。

3. 对于甲方提供给乙方使用的任何资源，如网络、NOTES等，乙方都只能将其用于工作，而不能用于其他目的，特别是从事侵害甲方利益的活动。

4. 乙方同意遵守甲方的各项管理制度，甲方有权依据上述制度对乙方进行检查，并且对乙方违反制度的行为进行处罚。

5. 甲乙双方书面同意并书面确认，严守己方所掌握的对方的涉密信息并不向任何第三方透露上述涉密信息

6. 保密信息的例外

（1） 任何已出版的或以其它任何形式处于公共领域的信息，以及在披露时乙方通过其它合法途径已获得的信息；

（2） 乙方在获得这些信息前已获得的信息，并且没有附加不准使用和透漏的限制；

（3） 由第三方在不侵犯他人权利及不违反与他人的保密义务的前提下提供给乙方的信息，并且没有附加不准使用和透漏的限制；

（4） 乙方并非借助甲方保密信息而独立开发或取得的信息。

7. 甲方保证其披露的保密信息未侵犯第三方的专利权、商标权、著作权或其它权利。合作期限内，如因甲方提供的保密信息侵犯了第三方的合法权利或不真实，给乙方造成实际损失的，甲方应当承担赔偿责任。

8. 甲乙双方确认，任何一方因不可抗力（如法律、法规、国家政策调整等）而透露信息的，应当事先书面通知对方，并且尽力提供保护；

9. 甲乙双方确认，任何一方对其所接触并知悉上述涉密信息的员工对上述涉密信息负有保密义务，双方应通过一定书面手段保证上述承诺；

10. 甲乙双方确认，本协议未含之内容，属涉密性的，由双方另行补签书面协议；非属涉密性的，属于任何一方的权利；

11. 甲乙双方确认，所有涉密信息由甲方按照本协议规定透露，任何一方不能或将不能利用上述信息为自己或其他方开发信息、技术和产品，或与另一方的产品

进行竞争；

12. 本协议将依据中华人民共和国的法律解释并应用，不包括法律规范的冲突；

13. 本协议有效期为3年，自签署之日起生效。如保密期间，保密信息已进入公知领域成为公开信息的，乙方不再承担相关保密义务，本协议自动终止。

（以下无正文）

甲方名称：绍兴市急救中心

甲方代表（签字）：

时间日期：　　年　　月　　日

承诺公司：浙江安腾信息技术有限公司

承诺代表（签字）：

时间日期：　　年　　月　　日