

# 佛山市高明区人民医院

## 态势感知系统需求说明

### 一、项目简介

本次需建设一套态势感知系统（网络流量探针、安全感知平台），并对接佛山市关键信息基础设施保护系统。另外，需对照三级安全等级保护标准完成我院 HIS 系统和医院信息平台 2 个系统的测评整改。

### 二、性能需求

#### （一）、关键性能（不可负偏移）

分类	详细描述	单位	数量	备注
态势感知系统	硬件外形：软硬一体化 2U 标准机架式设备； 电源：1+1 冗余电源 CPU：4 核 8 线程*1 内存：32G 硬盘容量：2T*2，带 RAID1，可用磁盘空间不小于 2T ； 接口数量：标配 10 个； 接口类型：千兆 RJ45 网口*2(管理口*2)、千兆 RJ45 网口*4、千兆业务 SFP 光口*4（标配千兆多模光模块*2） 接口扩展：（千兆 RJ45 网口*4 + 千兆 SFP 光口*4 ）或 万兆 SFP 光口*2 或 万兆 SFP 光口*4 MTBF 大于 65000 小时 吞吐率：1.5Gbps <b>数据外送：可按客户化需求做过滤</b>			
	1. 网络流量探针  2. 安全感知平台  1. 部署环境，必须满足纯软件形态部署模式，软件形态支持部署在物理机/虚拟机/云环境； 2. 满足吞吐率≥2Gbps，每秒处理性能≥10000EPS； 3. 平台需包括以下主要系统和引擎模块： 1) 大数据离线分析系统 2) 用户异常行为分析系统 3) 深度感知智能引擎 DSI 4) 安全事件智能研判引擎 5) 安全自动响应编排引擎 4. 平台具备云端威胁情报订阅模块：内置威胁情报离			

		线库并支持更新，支持在线查询与溯源			
安全服务内容	3. 网络安全扫描服务	检测网络设备、操作系统、数据库和应用服务中存在的安全漏洞，提供漏洞评估报告和修复建议。	次	2	针对医院信息系统（HIS 系统、医院管理平台系统）（三级）系统
	4. 安全渗透测试服务	利用各种主流攻击技术对客户授权指定的网站系统做模拟攻击测试，提供渗透测试报告和改进建议。	次	2	针对医院信息系统（HIS 系统、医院管理平台系统）（三级）系统
	5. 信息安全加固服务	针对安全漏洞和安全配置评估中发现的安全漏洞和配置缺陷，提供加固意见和方案，配合客户完成配置修复。	次	2	针对医院信息系统（HIS 系统、医院管理平台系统）（三级）系统
	6. 安全应急演练服务	根据实际环境，提供专项应急演练方案，准备演练场景，以模拟演练的方式检验应急预案和应急流程是否完善，提高应急处理能力。	次	2	
	7. 安全运维服务	每月第一周定期上门巡检一次，其他周远程巡检，每月共 4 次，服务期为一年	项	1	

## （二）主要技术参数

### 1.网络流量探针

指标项	指标要求
硬件外形	软硬一体化 2U 标准机架式设备；
硬盘容量	可用磁盘空间不少于 2T*2；RAID1
接口数量	标配千兆管理口 $\geq 2$ 千兆业务 RJ45 网口 $\geq 4$ ，千兆业务 SFP 光口 $\geq 4$ 支持端口扩展
电源	1+1 冗余电源
吞吐量	1.5Gbps
部署方式	旁路镜像模式部署，不影响服务器处理性能和网络架构

分 布 式 部 署	支持分布式部署，管理中心可实现告警统一管理 支持添加和删除探测器配置 支持根据添加探测器情况，配置探测器名称、发送时间、发送目录等信息
自 定 义 配 置	管理中心和探测器之间的数据传输速率、时间、发送目录都可自定义；（提供截图证明并加盖原厂公章）
审 计 功 能	支持全流量审计，包含网络第 2-7 层数据流量； 可选择特定协议或 IP 地址自定义检测； 支持自定义 IP 地址的访问监测； 基于丰富的特征库和识别库对全流量行为审计并深度匹配
	详细记录所有的审计数据包，可展现审计数据包的时间、客户端 IP、服务端 IP、应用层协议、报文、返回码、详细信息等。
协 议 解 析	支持解析应用层协议不低于 100 多种，如 HTTP、SSL、FTP、SMTP、POP3、TFTP、TCP、UDP、NFS、SNMP、ICMP、RTMP、DNS、IRC、SMB 等 支持对应用层协议 HTTP/DNS/FTP/IMAP/POP3/SMTP/SMB/DNP3 等可做深层解析还原，并进行全审计 支持对传输层 TCP/UDP 流量统计 对应用流量可做流量统计分析
动 态 沙 箱 检 测	对存在恶意行为的文件输出完整的二进制动态分析报告 动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险 支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中体现（提供截图和专利证明并加盖原厂公章）
攻 击 样 本 提 取	可以提取出攻击的完整样本文件，并提供对该文件下载的能力
文 件 威 胁 指 数	可展示威胁程度最高的文件样本 MD5、威胁指数、传播次数，病毒检测、静态检测和动态检测结果等内容（提供截图证明并加盖原厂公章）
	根据文件传播情况分析受感染主机、接受云端威胁情报、关键威胁行为可视化、回连主机 host 和完整沙箱分析报告 根据云端威胁情报展示云端是否确认、传播协议类型、传播次数、云端确认结果等
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，并对敏感信息快速定位，实现对敏感信息访问行为的有效监测（提供截图证明并加盖原厂公章）
登 录 信 息 识 别	识别网络中 WEB、QQ 等各种应用的登录行为，提取登录 IP、登录账户、登录网站域名等登录信息以及对 WEB 账户的密码进行弱密码校验，发现网站中存在的弱密码风险；
加 密 流 量 解 析	支持对 HTTPS 流量的解析还原（提供截图证明并加盖原厂公章）

威胁分析	支持流量异常行为检测，如网络蠕虫、木马、后门、僵尸、间谍软件、网络漏洞、网页漏洞、跨网站攻击、钓鱼邮件、暴力攻击、数据库注入攻击、ARP 欺骗、DoS 攻击等
	支持详细展现发现的威胁内容，包含时间、攻击源 IP、攻击目的 IP、网络层协议、应用层协议、规则描述、风险相关参照等信息
流量构成分析	可展现某 IP 在指定时间范围内的总流量、上下行流量大小及该 IP 下所有应用的总流量、上下行流量大小； 可展现某应用在指定时间范围内的总流量、上下行流量大小及该应用下所有 IP 的总流量、上下行流量大小；
流量趋势分析	支持最近 1 小时、3 小时、6 小时、12 小时、24 小时和自定义时间段的协议统计分析，包含应用层流量统计和传输层流量统计信息
	支持对不少于 2000 种应用流量数据进行统计，包含但不限于 QQ、迅雷、VPN、PPTV、天猫等各种应用（提供截图证明并加盖原厂公章）
	支持对传输层和网络层流量数据进行统计，包含但不限于 TCP、UDP、IP、ICMP 等
三权分立用户管理	提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立，支持自定义管理用户权限和角色
告警与报表	告警可详细展示风险级别、发生时间、告警名称、客户端 IP、服务器 IP、报文内容（URL、请求头、请求参数、请求内容）
	支持 SYSLOG、FTP、KAFKA 等接口进行审计、风险等各种信息外送（提供截图证明并加盖原厂公章）
	报表能够支持 WORD、PDF、EXCEL 等格式导出
资质证书	产品具有销售许可证（必须是 APT 安全监测类） 产品具有具有国家计算机病毒防治中心《APT 安全检测产品》检验报告 产品具有具有国家保密科技中心颁发的《恶意代码检测系统》涉密信息系统检测证书

## 2. 安全感知平台

分类	指标项	指标要求
基本要求	产品形态	1. 为灵活适应部署环境，必须满足纯软件形态部署模式，软件形态支持部署在物理机/虚拟机/云环境； 2. 满足吞吐率 $\geq 2\text{Gbps}$ ，每秒处理性能 $\geq 10000\text{EPS}$ ；
	资源配置（医院提供）	资源配置要求：CPU 资源 $\geq 24$ 核，内存 $\geq 256\text{GB}$ ，硬盘容量 $\geq 20\text{TB}$ ；
	数据类型	3. 支持通过多种类型的安全、泛安全类数据接入采集，应包括但不限于设备日志数据、流量数据、弱点漏洞数据、系统性能数据、威胁情报数据、资产人员数据；

		<ol style="list-style-type: none"> <li>支持通过流量采集设备采集接入全流量数据，包含流量中的请求包和返回包等信息，并可在数据检索中体现包信息；</li> <li>支持接入文本格式、CVS 等格式的文件数据，可通过模板文件的填写导入实现资产数据的导入和管理；</li> <li>支持通过云端对接、本地导入或手动编辑的方式，接入威胁情报数据。</li> </ol>
	采集与解析	<ol style="list-style-type: none"> <li>具备单独的日志采集模块，支持的接入的数据至少包括异构安全设备日志、网络设备日志、应用中间件日志、操作系统等网络环境中的日志数据，并不限制设备品牌和型号；</li> <li>日志采集方式应支持但不仅限于 Syslog、kafka、ftp、部署代理等 4 种方式（要求提供截图并加盖厂商公章）；</li> <li>具备单独的流量采集模块，支持全流量数据的接入，包含流量中的请求包和返回包等信息，并可在数据检索中体现包信息；</li> <li>支持接入应用服务器的性能类数据，包括但不限于 CPU、内存和磁盘的使用情况数据；</li> <li>无需配置解析规则与设备日志对应关系，自动完成解析</li> </ol>
安全检测能力	安全事件检测	内置多种安全模型，实现包括如下安全事件与场景的检测：拖库行为、Oday 攻击行为、弱口令、暴力破解、Web 攻击行为、邮件攻击行为、文件威胁、木马回连、DoS 攻击、SMB 行为、违规登录行为、黑产黑链、隐蔽信道通信、FTP 异常行为、恶意 DNS 通讯、设备性能异常等。（要求提供截图并加盖厂商公章）
	全流量深度检测	<ol style="list-style-type: none"> <li>支持全流量审计，包含网络第 2-7 层数据流量</li> <li>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，并对敏感信息快速定位，实现对敏感信息访问行为的有效监测</li> </ol>
安全分析能力	分析模型与指标管理	<ol style="list-style-type: none"> <li>支持规则模型，支持通过用户自定义规则提炼安全日志中的安全事件价值，将安全日志的任意字段进行筛选过滤、阈值设定、结果集包含等；支持同时设定多种条件，规则立即生效后即可产生安全事件和告警。</li> <li>支持关联模型，支持通过关联规则将跨越多个设备来源的多源异构安全日志进行关联分析；支持依据安全事件的相关规律，发现相关事件中隐藏的高级威胁及安全风险，设定阈值条件，触发安全告警。</li> <li>支持统计模型，支持从安全日志中发现重要的统计型特征；支持在实时流计算过程中统计日志中的任意字段中的数值，如事件数统计、求和、均值、最大值、最小值等统计策略。</li> <li>支持情报模型，支持通过最新的威胁情报信息与安全日志碰撞发现最新和潜在的安全威胁，与安全日志中的信息实时碰撞产生告警，通知用户及时处置。</li> <li>模型可通过串并联方式组合编排，前一个模型的输出可以作为后一个模型的输入，支持分析模型多层级编排；（要求提供截图并加盖厂商公章）</li> </ol>
	AI 高级分析	<ol style="list-style-type: none"> <li>平台内置不少于 8 种机器学习分析场景模型，可检测发现勒索挖矿告警数异常、安全设备日志数异常、网络会话数异常、域名请求数异常等特定场景条件下的安全态势异常；</li> <li>平台具备 AI 高级机器学习算法；（提供相关专利证明）</li> <li>支持自定义部署 AI 机器学习模型，允许用户选用的高级机器学习算法不少于 4 种，通过输入任意指标类数据进行模型训练，发现异常行为并生成安全事件与告警，辅助发现潜在的安全风险</li> </ol>

	网络实体分析画像	实现实体间网络互访关系的多级钻取，支持>10 跳的流量关联关系分析，支持通过端口、协议、异常访问类型过滤关联关系。（要求提供截图并加盖厂商公章）
	调查溯源	支持网络协议全文高级检索，对不同类型协议支持动态字段查询和展示（提供给第三方检测报告）
可视化安全分析	安全态势可视化	<ol style="list-style-type: none"> <li>支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测等多个维度进行可视化展示，提供不少于 10 种大屏展示界面（要求提供截图并加盖厂商公章）。</li> <li>可视化视角覆盖系统、边界、应用、安全设备等监测维度；</li> <li>支持外部对内部攻击、内部跨安全域横向攻击、内部外连攻击等威胁方向监测</li> </ol>
安全应用和运营	智能检索	<ol style="list-style-type: none"> <li>支持对原始日志数据、安全告警数据进行分类检索，从检索结果可关联威胁情报和资产信息并一键跳转；</li> <li>支持检索结果导出，导出内容字段可自定义选择，支持 excel 或 CSV 格式</li> </ol>
	数据字典管理	<ol style="list-style-type: none"> <li>支持管理系统中原始日志、安全事件、安全告警的所有字段和取值，每个字段均有清晰的说明；</li> <li>支持数据标准管理，用户可以根据实际需求，对字典进行编辑，支持手动修改、增加或删除相应的字段。</li> </ol>
	威胁情报	<ol style="list-style-type: none"> <li>支持通过离线导入或手动编辑添加的方式，形成本地威胁情报，允许用户自建行业情报库，并实现情报库的增删改查、导入、导出功能（要求提供截图并加盖厂商公章）；</li> <li>支持统计情报源碰撞命中情报数量，针对任意单条无效情报可实现禁用；</li> <li>支持本地化威胁情报查询,包括但不限于 IP、域名、文件 HASH</li> </ol>
	资产管理	<ol style="list-style-type: none"> <li>支持通过流量来发现资产，显示资产总数及风险资产数（需提供第三方检测报告并加盖厂商公章）；</li> <li>支持资产信息的全量导入导出，支持从资产管理平台同步资产；</li> </ol>
	业务拓扑监控	<ol style="list-style-type: none"> <li>支持拓扑图的增加、修改、删除、导入、导出，支持创建业务或网络拓扑，支持建立平面拓扑和 3D 拓扑。</li> <li>支持监控安全域、Web 业务系统、服务器、终端、安全设备等至少 5 种网络实体类型（提供截图并加盖厂商公章）；</li> <li>支持通过拓扑中各个节点的安全态势状况进行计算，对拓扑所对应的业务系统进行整体健康程度的详细量化评判。</li> </ol>
	安全运营	<ol style="list-style-type: none"> <li>支持统一的安全运营工作台，在工作台可以集中查看当前用户的待办工单、最新通报预警状态</li> <li>工单详情与备注支持多种内容格式，包括但不限于文字、图片、超链接、表格、代码片段、附件等类型；</li> <li>支持工单举证信息一键溯源，工单处置人员可以直接定位到工单关联的原始信息进行查看（要求提供截图并加盖厂商公章）；</li> <li>支持通过安全告警自动派发工单到对应的安全管理员，支持自定义编辑预警信息内容；</li> <li>支持将预警信息直接转为内部通报，支持将通报内容作为工单定向指派。</li> </ol>
	分析报告	<ol style="list-style-type: none"> <li>支持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，安全分析中的所有字段内容，都可以作为报告的统计对象，并自定义时间范围实现报告导出</li> </ol>

	联动处置	<ol style="list-style-type: none"> <li>1. 支持与安全设备进行联动，通过平台直接下发联动策略，进行安全事件的阻断，支持的安全防护设备类型至少应包括 waf、防火墙；</li> <li>2. 支持与不同品牌的安全设备实现联动</li> </ol>
	黑白名单	<ol style="list-style-type: none"> <li>1. 支持通过黑白名单功能对分析对象进行过滤筛选；</li> <li>2. 支持通过任意字段进行组合，配置筛选条件并生成黑白名单过滤规则</li> </ol>
系统管理	运维监控	<ol style="list-style-type: none"> <li>1. 支持平台本身的计算、存储资源利用率监控；</li> <li>2. 支持数据集与数据索引健康度监控；</li> <li>3. 支持对平台各组件运行健康状态的集中监控</li> </ol>
	用户管理	<ol style="list-style-type: none"> <li>1. 提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立，支持根据对象属性自定义划分系统管理角色和一般用户角色，按照数据和功能分级灵活设置用户权限。</li> </ol>
	系统恢复	<ol style="list-style-type: none"> <li>1. 支持安全模型的启用状态恢复出厂设置；</li> <li>2. 支持通过权限认证实现数据恢复出厂设置</li> </ol>
对接要求	接口对接	<ol style="list-style-type: none"> <li>1. 支持与现网日志审计产品无缝对接，获取当前归档日志数据进行关联分析</li> <li>2. 为响应广东省安全罩要求，产品需支持佛山市公安局态势感知平台接口对接</li> </ol>
其他要求	资质要求	<ol style="list-style-type: none"> <li>1. 产品及采集设备具备公安部销售许可证；</li> <li>2. 原厂商具备信息安全服务资质安全工程类三级资质；</li> <li>3. 原厂商通过 ISO27001 信息安全管理体系认证；</li> <li>4. 原厂商通过 CMMI5 认证；</li> <li>5. 原厂商应具有专业的大数据安全分析团队，要求支持团队至少 5 人具备 CISP-BDSA（大数据安全分析师）资质；</li> </ol> <p>（所有资质要求需提供证明文件加盖原厂公章）</p>

### 3.网络安全扫描服务

对所需评估的网络、信息系统进行安全扫描，采用专业安全扫描工具与人工检查相结合的方式，检测主机的安全策略实施现状，检测主机是否存在本地漏洞，对网站和应用系统进行安全扫描，发现漏洞，提供扫描报告，并根据扫描报告给出漏洞整改或修复建议，协助单位技术人员完善本地策略的实施。其范围包括如下：

#### 1、安全机制的评估

安全机制是根据安全要求，实施适宜的控制措施，确保将风险降低到一个可接受的程度管理机制，一套完善的安全机制是对整个网络的保障。机制的完善与否是评估的主要内容。

#### 2、网络构架的评估

网络的构架的评估是对网络的结构评估，一个合理的网络结构可以有效的防止黑客的攻击。

#### 3、操作平台的评估

操作平台是服务器、工作站等网络设备所运行的操作系统，它是网络中的基本单位，是

网络提供正常服务的基础，操作平台的评估是网络安全评估中最重要的部分。

4、网络设备的评估

网络设备的评估是对网络中的网络安全设备、路由器、交换机的安全评估，包括系统自身的缺陷和基本配置两部分。

专业安全扫描服务工具要求：

指标项	指标子项
产品要求	1. 提供《计算机信息系统安全专用产品销售许可证》 2. 提供《涉密信息系统产品检测证书》
产品功能	具备以下产品功能： 1. 系统漏洞扫描； 2. 网站漏洞监控； 3. 数据库漏洞扫描； 4. 基线配置核查； 5. 工控漏洞扫描； 6. 大数据漏洞扫描； 7. APP 漏洞扫描； 8. Docker 漏洞扫描； 9. WIFI 安全检测。
等级保护 专项功能	具备以下等保专项功能： 1. 支持新建等级保护测评任务，包括 SAG 等级、备案证明编号、被测单位、测评单位等信息。 2. 支持设置等级保护测评信息，包括机房、网络设备、安全设备、服务器、终端、数据库、业务系统等，以及安全人员、安全文档、安全服务、访谈人员等。 3. 内置有等保合规库，测评任务包含等保 1.0 和 2.0 两种任务。 4. 支持将扫描结果与信息安全等级保护合规库进行关联分析，生成满足规范要求的等级保护测评报告。

4.安全渗透测试服务

由安全工程师模拟黑客的行为模式，采用黑客的漏洞发现和利用技术，以及尽可能多的攻击方法，对目标应用系统的安全性进行深入分析，验证当前的安全防护措施，找出风险点，提供有价值的建议。渗透测试对象包括应用服务系统（WEB 系统）以及相关的其他系统。

针对 WEB 系统的渗透测试服务，至少包含如下典型的漏洞类型，并针对所有漏洞进行安全验证：

1) 跨站脚本：跨站脚本（即 XSS）漏洞允许攻击者向其他用户发送恶意代码。浏览器不能判断该脚本是否可被信任，因此会在用户上下文中执行此脚本。恶意人员可利用跨站脚本构造诱骗页面，诱骗用户登陆，进而获取登陆者的用户名、密码等敏感信息，进行非法活动。

2) SQL 注入: WEB 应用程序接收的用户输入在没有对输入的字符进行恶意字符过滤的前提下, 直接用来拼接 SQL 语句, 造成了 SQL 注入漏洞。攻击者利用此注入漏洞, 通过对数据库的猜解, 可得到应用系统管理员的用户名和密码, 进而获取站点的上传权限得到 webshell, 利用权限提升控制服务器, 对整个外部和内部网络系统造成重大损失。

3) 代码执行: 让程序将输入的内容作为代码来执行, 从而获得远程系统的访问权限。

4) 目录遍历: 由于 WEB 服务器配置不正确或 WEB 服务器自身存在漏洞, 可导致非法人员下载服务器端的文件。攻击者利用此漏洞可遍历服务器目录, 造成诸如应用系统源代码、内网地址等相关重要信息泄露, 并由此可能暴露出更严重的安全漏洞, 为非法者进一步攻击提供了可能的机会。

5) 文件包含: 脚本在包含文件时, 直接使用用户提交上来的数据作为文件名。这些数据在使用前并没有进行适当的验证。

6) 脚本源码泄露: 把脚本文件名作为参数可能读取该脚本的源代码。该脚本在包含文件时, 直接使用用户提交上来的数据作为文件名。这些数据在使用前并没有进行适当的过滤。

7) 物理路径泄漏: 远程攻击者可以利用这类漏洞获得服务器物理路径信息。当客户端请求一个不存在的文件时, 会返回一些出错信息, 这可能允许攻击者了解服务器的配置情况, 可能有助于发动进一步攻击。

8) 应用错误信息: 这种漏洞会泄漏一些 WEB 的内部信息, 这些信息可能会包括 WEB 开发使用的语言、中间件、开发框架、数据库的名称、版本号等, 这些信息都会有助于黑客进行进一步的准确攻击。

9) 备份文件: 备份文件通常是开发人员为备份他们的工作而创建的, web server 上备份文件可能包含敏感信息, 从而被攻击者利用。

渗透测试服务配套工具详细功能需求如下表:

序号	指标子项
1	支持网络地址自动快速扫描
2	支持资产集中管理
3	支持主机/应用识别服务
4	支持 appscan 检测结果文件导入
5	支持 AWVS 检测结果文件导入
6	支持 nessus 检测结果文件导入
7	支持 OWASP ZAP 检测结果文件导入
8	支持国产网络安全漏洞扫描产品检测结果文件导入
9	支持渗透测试结果 excel 文件导入

序号	指标子项
10	支持基于上述结果文件导入，自动化输出渗透测试报告
11	基于国密算法加密通道的中文管理界面。

## 5.信息安全加固服务

针对网络安全扫描服务和安全渗透测评服务过程中发现的系统漏洞、安全隐患和配置缺陷，结合单位实际情况，提供加固建议和方案，协助配合用户完成整改修复。

## 6.安全应急演练服务

为了健全单位的运行应急机制，检验网络与信息安全综合应急预案和业务技术专项应急工作机制及有效性，验证相关组织和人员应对网络和信息安全突发事件的组织指挥能力和应急处置能力，满足突发情况下网络与信息系统运行保障和故障恢复的需要，确保信息系统安全畅通，提供安全应急演练，以不断提高各部门开展应急工作的水平和效率，发现预案的不足，进一步完善应急预案。

根据实际环境，提供专项应急演练方案，准备演练场景，以模拟演练的方式检验应急预案和应急流程是否完善，提高应急处理能力。

## 7.安全运维服务

- 1、每月第一周定期上门巡检一次，其他周远程巡检，每月共 4 次，服务期为一年。
- 2、巡检范围：网络安全设备（或按项目约定的范围）
- 3、巡检方式：现场巡检+远程巡检
- 4、巡检项
  - 1) 运行状况巡检：资产能否正常登陆；CPU、内存、硬盘存储空间使用率；设备许可；规则库、病毒库等更新升级（在许可范围内）；系统时间；接口流量等
  - 2) 安全基线巡检：身份标识和鉴别措施；身份鉴别信息复杂度；登录失败处理；登录连接超时；安全的远程管理；账号权限分配；默认账号、默认口令；过期或多余账户；安全审计；系统服务、默认共享、高危端口；远程管理地址限制；配置备份和恢复；

3) 安全日志巡检：资产日志审计启用情况；日志本地或外发存储情况；日志采集和存储情况；

4) 安全事件巡检：收集分析最近一个月内的安全事件日志，针对分析结果提出安全建议；

5) 安全巡检统计分析：对安全巡检结果进行统计分析，提供安全巡检报告。

5、对已部署的安全产品提供运行维护和技术支持服务，包括医院各类信息安全、网络安全、终端安全系统的日常巡检和运维保障。定期巡查安全产品运行状态；根据实际需要进行策略调整；日常巡检维护、安全策略优化、故障处理、应急处理、安防措施有效性验证等。

6、形成专业报告，达到安全风险有预防、安全事件有记录、出现问题可追溯的信息安全监控状态，保障医院各系统正常、安全、稳定、高效运行。

### **三、付款方式要求**

1.货物到位后 30 天内，支付 30%。

2.项目验收（产品实施完成后，且收到评测服务机构出具合规的验收测评报告）后 30 天内支付 60%。

3.验收 1 年后 30 天内支付 10%。

### **四、售后服务要求**

1.态势感知系统保修和维护服务：提供三年的免费保修服务。

2.售后服务热线：保证提供 7\*24 的服务，及时响应医院的售后服务需要、及各种技术咨询。

3.故障响应：在接到医院的故障报修信息后，在 4-6 小时内给予实质性响应，指派工程师立即协助用户对故障情况进行处理。

4.在试运行期间，需派出有经验的技术人员负责系统的运行和维护，若系统出现问题或故障，免费进行故障处理和软件更新。

2020-12-25