# 态势感知系统特征库软件升级

# 及质保参数

1. 商务要求

1.授权时间：1年。

2.要求自签订合同之日起免费提供系统软件升级更新升级包和升级指导。

3.要求兼容现有管理平台及软件。

4.授权规模：安全感知系统平台特征库\*1，安全感知系统探针特征库\*2。

5.其他要求

(1)要求定期提供系统软件升级包、更新授权以及远程升级指导。

(2)在升级过程中的疑难问题，要求可获取远程升级指导及支持，响应时间不超过2小时。

(3)要求提供定制的软件升级授权问题的咨询与处置。

1. 技术参数

1.安全感知系统平台

（1）要求支持配置全部大屏的展示对象的名称自定义、统计周期设置、资产组织自定义选取、单位所在地、展示风险、LOGO显示、实时告警启用、大屏启停等。

（2）要求支持配置可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，可清晰直观看清失陷主机对其他主机的影响，评估受损情况，方便客户快速处置。支持通过首页搜索框输入IP/域名/URL/端口/通信对进行搜索，支持基于列表模式展示横向攻击、违规访问、风险访问、可疑行为、正常访问等详细信息，建立全方位的持续性的检测能力。支持入口点溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息，帮助管理人员快速找到攻击入口点。（需提供截图证明并加盖原厂商公章）

（3）要求支持配置勒索专项检测页面，帮助客户更好的应对日益严峻的勒索风险，支持对勒索主题的安全告警进行统一展示和管理，支持以勒索病毒的感染途径/方式为维度进行分类，包括勒索常用端口、勒索常用漏洞、RDP爆破、感染勒索病毒、黑客勒索攻击、勒索C&C通信等维度，支持展示受害资产以及受害资产攻击数TOP5，支持以列表的形式展示勒索事件，包括最近发生时间、威胁描述、威胁定性、勒索风险、威胁等级、受害者IP、攻击次数等信息（需提供截图证明并加盖原厂商公章）

（4）要求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。

（5）要求支持配置挖矿专项检测页面，更好的应对日益严峻的挖矿风险，避免数据窃取和监管通报，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，以实现挖矿病毒的全面检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，便于掌握各阶段挖矿主机分布情况，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者IP、攻击次数、威胁情报等信息（需提供截图证明并加盖原厂商公章，且所投产品必须提供第三方权威检测机构关于“挖矿专项检测”功能项相关的产品检测报告）

（6）要求支持弱密码识别主动扫描，支持加密协议的弱口令登录检测，支持SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL等协议。

（7）要求支持威胁定性引擎以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认，从而确认安全告警的优先级顺序，支持基于人工渗透、程序自动化、业务相关风险、其它4个维度对告警进行分类，帮助安全人员快速定位高危告警并及时处置。（需提供截图证明并加盖原厂商公章）

（8）要求支持PPT格式导出摘要报告，报告内容包括：网络安全整体解读、网络安全风险详情、告警及事件响应盘点，用户可直接通过导出的PPT报告进行工作汇报，高效体现工作价值。（需提供截图证明并加盖原厂商公章）

（9）要求支持短信/邮件/微信告警推送。告警条件、推送频率、推送时间等可自定义；短信邮件告警支持策略编辑，可将不同告警内容发送至不同的责任人；脆弱性可支持风险类型、严重等级、数据来源和推送频率自定义。（需提供截图证明并加盖原厂商公章）

（10）要求支持web登录结果自定义，可根据登录行为检测是否登录成功，支持基于响应状态码、响应内容格式、URL、关键字、服务器IP地址、所属资产组等信息判定成功或失败的通用规则设置，支持机器学习引擎持续学习用户登录行为，生成登录成功规则模型。

2.安全感知系统探针

（1）要求支持命令注入检测、PHP代码检测、XSS攻击检测、Webshell上传检测、SQL注入检测、XXE攻击检测、JAVA代码检测、SQL非注入型检测、MYSQL解析增强、php反序列化检测等自定义配置启用、高检出、低误报模式。（需提供截图证明并加盖原厂商公章）。

（2）要求支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Network Device、Media漏洞攻击、Shellcode漏洞攻击、Scan漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、IPS云防护、Web漏洞攻击等服务漏洞攻击检测（需提供截图证明并加盖原厂商公章）。

（3）要求支持Application漏洞攻击、File漏洞攻击、Scan漏洞攻击、Shellcode漏洞攻击、System漏洞利用攻击、Web Activex等客户端漏洞攻击检测。

（4）要求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。

（5）要求支持5种场景的日志传输模式,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（需提供截图证明并加盖原厂商公章）。

（6）要求支持传输协议审计日志，包括https、http、DNS、邮件协议审计日志、SMB、AD域、WEB登录、FTP、Telnet、ICMP、TELNET、ICMP 、SNMP 、SSL 、SIP 、ONVIF 、mongo、NFS 、SOCKS 、dhcp、netbios\_nbns、全流量元数据审计、数据库审计协议等。（需提供截图证明并加盖原厂商公章）。

（7）要求内置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。

（8）要求支持流量抓包分析，基于五元组灵活抓取数据包，可定义配置源IP、源端口、目的IP和目的端口、传输层协议以及标签类型（vlan、vxlan、mpls）选择添加抓包任务，接口额外提供标签选项，帮助安全工程师高效分析威胁。（需提供截图证明并加盖原厂商公章）

（9）要求内置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、白名单库等。（需提供截图证明并加盖原厂商公章）

（10）要求支持设备内置简单命令行管理窗口，便于基础运维调试；可实时监控设备的CPU、内存、存储空间使用情况；能够监控监听接口的实时流量情况。

1. 其他要求

1.项目管理

服务商需提供完善的项目管理方案，包含但不限于实施进度表、项目组织结构、项目质量控制等。

2.成员组成

（1）实施工程师：1人，要求具备同类项目管理工作经验，并报院方认可。

（2）项目开发人员：具备同类项目实施经验。

3.项目验收

（1）实施完毕后，由信息网络中心组织验收。

（2）验收时服务商单位必须派代表在场，验收合格后，由服务商单位签署检验合格证书。

4.售后服务要求

服务期间，应提供电话、电子邮件等多种方式的技术咨询服务。公司应提供7\*24小时全天候服务技术服务支持，节假日有备班人员随时响应。包含远程技术支持和现场技术支持两种方式。

5.培训要求

服务商要求根据医院实际需要提供多种培训方式，对各类人员提供适当的培训内容。要求达到用户能够独立操作使用本系统的目标。

6.安全要求

服务期内配合甲方定期开展网络安全自查，自查内容至少包括系统日常运行情况、系统漏洞等；配合甲方定期进行安全审计，审计内容至少包括系统账号、权限、操作行为和安全技术措施有效性等，及时发现和处理信息系统运行过程中的安全隐患，减少或避免网络安全事件的发生。