**需求技术参数书**

1. 项目名称： 2023年度智慧医院网络安全组件升级加固项目
2. 项目概况与设备数量：

为进一步推进医院信息安全工作开展，申请购置应用未知攻击感知服务三年（服务已含硬件部分）。

具体技术参数及配置要求：

|  |  |
| --- | --- |
| **类别** | **服务描述** |
| **服务要求** | 1、提供旁路分析Web全流量镜像， Web入侵检测和Web漏洞感知服务。  2、提供保存Web流量镜像，具备攻击取证及回溯分析能力服务。  3、提供并支持攻击事件合并，可按时间阶段、IP、攻击手段、风险级别、境内境外IP等方式合并事精的功能服务。  4、提供现场技术支持，解决远程无法处理的问题，包括软硬件故障恢复、问题诊断或维修等。  5、提供备件保障服务，当设备无法在规定时间内恢复的，提供同型号的备机。  6、提供软件版本、规则库升级服务，当系统有新版本发布时及时通知用户，对升级工作提供技术支持、新功能的技术培训，包括结合用户实际使用对新版本信息进行评估并给出建议，配合升级和回退方案拟定、测试演练和投产支持等。  7、提供移机、扩容等技术支持服务，根据用户需要，提供技术支持，包括调试、参数定义、逻辑卷划分、数据迁移、相关功能软件工具安装、远程备灾方案的实施和调试服务等。  8、提供专家服务：包括7\*24小时技术专员“电话”、“邮件”技术支持，5\*8小时技术专员“微信”技术支持，实时协助分析日志，7\*24小时项目经理、业务人员“电话”、“邮件”、“微信”需求对接，7\*24小时高危及受控日志远程分析服务，7\*24小时高危0Day/Nday漏洞预警及响应通报，现场巡检分析日志或现场应急响应。  9、提供重要时段保障服务，根据需要在特殊时段（如：重要会议、黄金周长假、攻防演练、重大投产变更等用户认定的特殊时段）提供7X24小时响应服务、事前巡检、日志分析及优化服务。  10、提供 **Web威胁检测服务能力，并**支持http会话双向数据流的追踪和检测分析，如服务器返回的网页中包含特定敏感关键字、泄密数据库信息时报警。（提供服务工具的截图证明）  11、提供  **DNS检测服务能力** ，并支持域名解析：支持对访问的所有域名进行解析和分析（包含正常的访问记录），并记录的字段包括：会话时间、来源IP、域名IP、DNS服务器IP、DNS返回记录、查询域名、协议、长度、数据源、信息摘要等。（提供服务工具截图证明）  12、提供**风险告警服务能力：①**支持提供充足证明此次告警的信息，报警内容包含完整的双向数据包，包括HTTP报文头部、URL、POST数据包，以及服务器返回的内容，同时针对每条单独的告警下载PCAP报文；（提供服务工具截图证明）②支持以网页快照形式展示服务器返回的内容；（提供服务工具截图证明）③支持在告警中展示数据包交互的文件，如:PDF、word、excel等 （提供服务工具截图证明）④支持http、mysql、ssh、smb、ftp、远程桌面等协议的双向分析。可在同一个规则内关联分析一个TCP会话的双向报文，当请求包含有指定攻击报文，返回包含有受影响的报文时，才发出报警。在同一条报警日志中要求同时展示双向报文 （提供服务工具截图证明）⑤支持检测服务器泄漏大型数据文件事件,如服务器返回超过20兆的数据文件。（提供服务工具截图证明）  13、提供**告警管理与回溯分析服务能力，①**支持通过时间、IP、Url、Post数据包、状态码、检索关键字等内容进行回溯分析，同时支持在溯源结果的基础上去除包含特定关键字的记录，支持复现整个攻击事件全部HTTP报文的关联分析。（提供服务工具截图证明）②支持通过时间、IP、关键字、get参数、目的主机、日志类型、状态码、端口、协议等多个关键字及正则表达式的模式进行全文检索和回溯分析。（提供服务工具截图证明）③支持存储全量的Web应用交互双向数据包，包含正常交互的http日志数据包，且有单独页面展示，http日志数据包需包括HTTP报文头部、URL、POST数据包，以及服务器返回的内容（提供服务工具截图证明）  14、提供**管理控制服务能力，①**支持以多个关键字及正则表达式的方式制定请求包检测规则：可同时按域名主机关键字、URL关键字、文件名关键字、请求报文、等多维度以多个关键字及正则表达式的方式制定检测规则。（提供服务工具截图证明）②支持以多个关键字及正则表达式的方式制定返回包检测规则：可同时按域名主机关键字、URL关键字、文件名关键字、返回报文、返回页面MD5等多维度以多个关键字及正则表达式的方式制定检测规则。（提供服务工具截图证明）  15、提供**行为分析能力，**支持用户和实体行为分析(user and entity behavior analytics,UEBA），可自动关联分析多个会话、日志、行为；可自定义关联分析策略；关联时长不少于10分钟。（提供服务工具截图证明）  16、提供**研判助手能力**，针对每条单独的告警，可自动关联该IP在48小时内的异常请求详情，同时关联该IP触发攻击的类型、该IP触发的攻击的次数、其他IP触发该攻击类型的次数、其他IP访问该URL次数等协助用户研判此次攻击的危害，并可标记为高危、中危、低危和忽略，提供忽略加白功能等（提供服务工具截图证明）  17、提供**漏洞检测能力**，可自主扫描操作系统及网站漏洞。包括缓冲区溢出、SQL注入、跨站脚本漏洞（XSS）、信息泄漏等常见的Web应用漏洞（提供服务工具截图证明）  18、支持扩展**旁路阻断能力**，服务工具旁路部署时，可实现TCP及URL级别的阻断，达到防火墙和应用防火墙阻断的效果。（提供服务工具截图证明） |
| **服务工具要求** | 1、2U机架式设备，冗余电源，CPU核数≥6核；内存容量≥64G；硬盘容量≥20TB ；管理口≥1；千兆电口≥4；万兆光口≥2；处理能力≥1Gbps ；监控并发连接数≥200万。 2、IP碎片包重组能力≥20M。 3、支持存储不少于100亿条Url日志，并可导出Url记录。 4、支持保存1-6个月的Web双向数据包，同时能够保存请求包和响应包。（提供服务工具截图证明）   1. 服务工具要求具有公安部颁发的计算机安全销售许可证书。   6、服务工具要求具有中国网络安全审查技术与认证中心颁发的中国国家信息安全产品认证证书。 7、服务工具要求相关技术应具备境内发明专利，每具备一项发明专利证书。  8、服务工具要求具有国家互联网应急中心认定的“CNVD国家信息安全漏洞共享平台”技术组成员。 |