南通市第三人民医院网络安全改造项目

技术了解需求

## 一、建设目标与主要建设内容

本项目的建设目标是加强安全设备维保、数据库安全运维、专家值守服务和安全强化服务等内容的建设。遵循国家等级保护政策法规和医院行业相关安全建设标准，建立一整套合适的信息系统安全保障体系，并使得该管理体系能够切实可行地贯彻在南通市第三人民医院信息化相关工作的各个环节，成为信息安全建设的战略目标。

主要建设内容有以下四个方面：

1. **安全设备维保**

现有网络安全防护系统的核心系统是各边界防火墙和态势感知平台。防火墙和态势感知的安全规则库均已过期，需要对防火墙和态势感知平台进行维保升级。

1. **数据库安全运维**

数据安全内控管理安全系统，提供全面的资产防护能力，包括：敏感数据发现管理；防范敏感数据危险操作；限制特权账户随意访问敏感数据；利用身份管理、授权等机制对运维人员进行合规管理；协助运维人员实现工单管理和免密登陆；提供全面风险分析报告等功能。

1. **专家值守服务**

以保障风险管控效果为目标，以“人机共智”模式为手段，以7\*24小时持续在线守护为主线，协同本地安全服务人员，以“资产、脆弱性、威胁、事件”四个核心安全风险要素为抓手，提升组织安全风险管控能力和安全工作效果，为用户提供持续、有效、省心、便捷的安全托管服务。

1. **安全强化服务**

随着新型威胁的增多，特别是攻防演练常态化，安全防护越来越趋向实战化，现有的安全防守无法针对新型攻击进行防护。传统安全服务也无法涵盖攻击防守的所有范围。需要强化一下几个方面的安全服务，应对最新的攻击。

1. 渗透测试

对关键系统进行渗透测试，运用常见的黑客攻击技术进行模拟攻击，提前发现潜在的安全风险，并提供相应的加固方案。

2. 钓鱼演练

通过仿真客户重要业务系统，发送钓鱼邮件，模拟真实黑各进行邮件钓鱼攻击，有效验证与提高单位员工的安全意识水平。

3. 外网资产暴露面监测

通过外网云端扫描技术，探测互联网上潜在的未知资产，不必要开放的资产、网站后台，并自动验证互联网资产是否存在可利用漏洞、弱口令，提供暴露面收敛等相关整改建议。

4. 攻击诱捕

基于蜜罐的网络欺骗技术是主动防御和入侵检测技术，对捕获的数据和攻击行为进行分析，更好的了解和掌握入侵者的工具、策略和方法，从而事先做好主动防御措施，延缓攻击者对医院其它业务系统的攻击。

**二、需求清单及预算**

**项目软硬件配置数量、价格及预算清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **项目** | **配置参数** | **数量** | **单位** |
| **1** | 设备维保 | **安全态势感知平台 深信服 SIP-1000-E600**  **2年规则库升级**  硬件指标:1U，32G内存，SSD128G系统盘、SATA16T 存储、单电源，标配6个千兆电口; 安全感知平台基于海量的安全数据，通过机器学习、 UEBA、关联分析等智能技术，帮助客户看清业务、感知威胁、及时预警、快速响应。 | 1 | 台 |
| **安全态势感知探针 深信服 STA-100-B420**  **2年规则库升级**  性能指标:1Gbps，硬件指标:1U，SSD 64G、单电源，标配4个千兆电口+2 个千兆光口; 潜伏威胁探针主要通过旁路部署方式对全流量信息进行采集。 | 1 | 台 |
| **出口WAF 深信服WAF-2000-B2100**  **2年规则库升级**  性能参数：网络层吞吐量：20G，应用层吞吐量：2.8G，并发连接数：2200000，新建连接数（CPS）：150000，SSL VPN推荐用户数（单独购买）：30，SSL VPN最大用户数（单独购买）：150，SSL VPN最大理论加密流量（单独购买）：350M，IPSec VPN最大接入数：1000，IPSec VPN加密速度：600M。 硬件参数：规格：1U，内存大小：8G，硬盘容量：128G minisata SSD，电源：单电源，接口：6千兆电口+6万兆光口SFP+。 功能描述：深信服下一代防火墙以保障用户核心资产为目标，提供L2-L7层各类威胁的检测和防护，是一款能够有效应对传统网络攻击和未知威胁攻击的网络安全产品。 | 1 | 台 |
| **服务器区防火墙 深信服AF-2000-B2150**  **2年规则库升级**  性能参数：网络层吞吐量：25G，应用层吞吐量：3G，并发连接数：2200000，新建连接数（CPS）：150000，SSL VPN推荐用户数（单独购买）：30，SSL VPN最大用户数（单独购买）：150，SSL VPN最大理论加密流量（单独购买）：350M，IPSec VPN最大接入数：1000，IPSec VPN加密速度：600M。 硬件参数：规格：1U，内存大小：8G，硬盘容量：128G minisata SSD，电源：单电源，接口：6千兆电口+6万兆光口SFP+。 功能描述：深信服下一代防火墙以保障用户核心资产为目标，提供L2-L7层各类威胁的检测和防护，是一款能够有效应对传统网络攻击和未知威胁攻击的网络安全产品。 | 2 | 台 |
| **专线防火墙 深信服AF-2000-B1120**  **2年规则库升级**  性能参数：网络层吞吐量：3G，应用层吞吐量：250M，并发连接数：800000，新建连接数（CPS）：18000，IPSec VPN最大接入数：1000，IPSec VPN加密速度：100M。 硬件参数：规格：1U，内存大小：2G，硬盘容量：64G minisata SSD，电源：单电源，接口：6千兆电口。 功能描述：下一代防火墙以保障用户核心资产为目标，提供L2-L7层各类威胁的检测和防护，是一款能够有效应对传统网络攻击和未知威胁攻击的网络安全产品。 | 1 | 台 |
| **2** | 数据库安全运维系统 | 数据安全内控管理安全系统，提供全面的资产防护能力，包括：敏感数据发现管理；防范敏感数据危险操作；限制特权账户随意访问敏感数据；利用身份管理、授权等机制对运维人员进行合规管理；协助运维人员实现工单管理和免密登陆；提供全面风险分析报告等功能。产品参数：  1.虚拟化软件版本形式交付； 2.数据库实例≥4个； 3.基础功能（数据库准入、访问控制、运维审计等功能） 4.在线会话数≥1000 5.运维SQL吞吐量≥1000条/秒 6.含防假冒套件：1套 | 1 | 套 |
| **3** | 专家24小时值守服务 | 【按年收费】【数据中心资产（IP）数量≤20个】  1. 安全专持续服务，防护水平动态调整，安全工作主动开展安全运营服务，使用三阶共享专家模式，提供7X24小时持续服务，持续监测安全状态；并在安全事件发生前、发生时、发生后动态调整安全策略  2. 打通技术体系和管理体系，发挥两大体系的安全效益网络安全实则是风险管理的过程，在风险管理中存在技术和管理两种手段。在现实的风险管理过程中，技术与管理体系往往是割裂的，无法有机融合。通过安全运营服务，可通过技术的手段帮助解决技术体系的有效性问题，也能帮助解决管理体系落地难的问题。 | 1 | 年 |
| **4** | 安全强化服务 | **渗透测试**：对关键系统进行渗透测试，运用常见的黑客攻击技术进行模拟攻击，提前发现潜在的安全风险，并提供相应的加固方案 **钓鱼演练：**通过仿真客户重要业务系统，发送钓鱼邮件，模拟真实黑各进行邮件钓鱼攻击，有效验证与提高单位员工的安全意识水平 **外网资产暴露面监测**：通过外网云端扫描技术，探测互联网上潜在的未知资产，不必要开放的资产、网站后台，并自动验证互联网资产是否存在可利用漏洞、弱口令，提供暴露面收敛等相关整改建议 **攻击诱捕** 基于蜜罐的网络欺骗技术是主动防御和入侵检测技术，对捕获的数据和攻击行为进行分析，更好的了解和掌握入侵者的工具、策略和方法，从而事先做好主动防御措施，延缓攻击者对医院其它业务系统的攻击 | 1 | 年 |

**三、项目预算：48万元**