|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务名称** | **服务内容** | **服务频率** | **服务年限** |
| 1 | 等保测评 | 医院业务系统等保测评服务，包含两个三级和一个二级系统，完成定级备案，等保测评工作并获取备案证书。其他业务系统协助医院完成等保一级备案。 | 三级系统：每年一次二级系统：每两年一次 | 三年 |
| 2 | 终端安全防护服务 | 提供≥800个PC终端的安全防护服务，服务要求如下：1、提供windows系统屏幕水印功能服务，灵活定义屏幕水印内容，可设置不透明度、生效范围和生效时间段等，如有敏感信息泄露可以通过水印信息辅助做溯源；2、提供应用管控服务，包括IM、下载工具、代理工具、办公软件等，并且支持新增自定义应用，辅助客户限制恶意软件、盗版软件的使用，加强正版软件配置规范建设，事前可拦截终端进程运行，事中可结束终端应用的运行，事后可审计进程管控日志；3、提供对Windows停更的系统提供专项防护服务，包括0day漏洞防护、文件防护、暴破入侵防护、系统脆弱点识别和风险端口封堵等多项核心功能；4、提供不同攻击阶段的主要攻击手法检测服务，对包括但不仅限于以下攻击手法精准检测，执行、持久化、权限提升、防御逃逸、凭证窃取、横向移动等攻击手法检测记录。显示事件详情，展示攻击手法对应的高危操作和威胁实体；5、提供显示攻击事件命中的ATT&CK相关技术服务，并对此技术做简要说明。便于用户了解攻击者的操作行为和目的，评估整体影响面；6、提供基于本地缓存信誉检测与全网信誉检测服务，构建全网信誉库的检测引擎，做到内网一台威胁，全网感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置有效提升查杀效率，减少终端资源开销；7、针对Windows系统，提供实时监控所有非授信驱动及黑客工具的装载、运行等行为的服务,发现风险行为时进行提示和拦截，同时，支持设置敏感时间段，监控敏感时段内可疑驱动的装载、运行等行为，发现风险行为时进行提示和拦截。输出《PC终端威胁分析报告》。 | 7\*24小时/年 | 三年 |
| 3 | 服务器端安全防护服务 | 提供≥200个服务器端的安全防护服务，服务要求如下：1、提供勒索病毒整体防护详情展示，直观展示最近七天勒索病毒防护效果，包括已处置的恶意文件数量、已拦截可疑行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数 ；2、提供安全策略一体化配置服务，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell检测和威胁处置方式、暴力破解的威胁处置方式和Windows白名单信任目录；3、提供对终端账户信息进行梳理服务，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、可疑root权限账号、长期未使用账号、夜间登录、多IP登录进行账号分类查看，支持统计最近一年未修改密码的账户；4、提供展示最新公布的热点漏洞信息服务，并且梳理出其中的高可利用漏洞统一展示在热点漏洞页面，方便运维人员一键对当前已接入的终端进行漏洞检测，同时支持设置热点漏洞定时检测；5、提供展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离；7、提供Linux服务器SSH远程登录保护服务，可开启SSH远程登录二次认证，以防止黑客利用弱密码脆弱性对服务器的入侵；支持设置验证码验证或自定义密码验证，支持设置登录认证提示、生效时间段和免二次认证白名单。输出《服务器威胁分析报告》。 | 7\*24小时/年 | 三年 |
| 4 | 安全运维服务 | 一、服务概述综合运用丰富的技术经验及威胁情报知识库，借助安全服务平台等强大的设备对接能力及安全检测能力对安全日志、流量进行分析研判并对发现的威胁进行定位，并对分析发现的安全问题制定安全运营相关台账，做好安全问题通告和处置管理工作。服务期内要求在医院本地部署一体化安全运营托管服务平台，平台须具备IT资产管理、脆弱性管理、威胁监测、响应与处置等能力，提供7\*24H持续性开展网络安全保障工作，与医院一同构建持续、主动、闭环的安全运营体系。服务IT资产包含医院终端电脑和服务器、云主机等，资产数量≥1000个。二、服务要求1、运营准备阶段1.1、安服工具部署：在用户本地部署一体化安全运营托管服务平台，安服工具提供“资产管理、脆弱性管理、威胁监测、响应与处置”等能力。服务平台需覆盖医院内网、DMZ区和互联网。1.2、资产管理（1）资产梳理服务：探测单位主机、网站资产，包括探测主机操作系统、开放端口、应用服务、协议版本等，探测网站子域名、url、web框架、备案号、微信小程序、微信公众号、APP应用程序等，形成资产清单，并定时探测更新。（2）攻击面检测服务：联动外网云端扫描系统，探测互联网上潜在的未知资产、不必要开放的资产，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。（3）提供互联网暴露面收敛建议：建议关闭不必要开放到互联网的资产、端口、后台url页面，减少攻击面。2.1、脆弱性管理服务（1）漏洞扫描服务：对主机、网络设备、操作系统、数据库、中间件等进行常态化的漏洞与弱口令扫描，提供漏洞、弱口令扫描结果台账与整改建议。提供漏洞优先修复建议：基于攻防视角评估资产漏洞风险，识别可实际产生风险的漏洞，提供漏洞修复的优先级建议，可大幅减少漏洞整改工作量。（2）漏洞屏蔽：对于无法整改修复的漏洞，提供漏洞屏蔽技术手段，使扫描器扫得到资产，但扫描不到漏洞，规避漏洞暴露风险。（3）网站风险监测：主域名及子域名网站进行7\*24小时网站监测，包含：web漏洞、篡改、黑链/挂马、敏感文件、敏感词、可用性、域名劫持等7个维度开展实时监测，并可通过邮件、飞书、钉钉、企业微信等告警形式提供网站风险预警服务。2.2、威胁管理服务（1）流量威胁监测：旁路部署流量检测探针（含8W+IDS规则），监测互联网出口与服务器区域边界流量，基于威胁计分算法精准识别恶意IP。（2）蜜罐威胁诱捕：旁路部署高交互或无漏洞的仿真蜜罐，精准诱捕攻击蜜罐的失陷主机，实时零误报定位攻击威胁：勒索病毒传播、内网主机被远控后横向攻击（如钓鱼远控、供应链威胁）。（3）主机威胁监测：在服务器上安装轻量级主机Agent，包括可在公有云主机安装，保护云主机；事前监测：能识别与阻断主机攻击、Web攻击、暴力破解（SSH、RDP、SMB）和异常登录等入侵行为、针对服务器横向攻击行为，可识别HTTPS加密流量中的攻击行为；事后监测：实时监测webshell、反弹shell、网页篡改等行为。（4）智能AI+威胁情报服务：智能AI研判分析：自动威胁告警进行降噪研判分析，自动研判出各种威胁类型：非法外联、外网攻击、内网横向、暴力破解、利用成功等；威胁情报：关联全球威胁情报，精准检测网络中的病毒域名请求、恶意IP流量威胁。2.3、处置与预警自动化旁路阻断服务：（1）外网威胁实时封堵：专家精准研判外网威胁告警，使用旁路阻断技术，实时封堵外网攻击IP地址，大幅降低被入侵风险；（2）内网非法外联阻断：自动阻断内到外的病毒木马外联行为。（3）告警事件及时响应：发生相关风险告警，通过邮件、飞书、钉钉、企业微信等形式及时通知用户，及时响应。3、运营成果可视通过本地部署一体化安服工具，数据统一汇总在安服工具上，用户可随时使用安服工具的功能，以及各场景大屏展示功能。 | 7\*24小时/年 | 三年 |
| 5 | 渗透测试服务 | 提供针对医院业务系统的渗透测试服务，模拟黑客攻击的方式，对业务系统的安全漏洞、安全隐患进行全面检测，最终目标是查找业务系统的安全漏洞、评估系统的安全状态、提供漏洞修复建议。 | 2次/年 | 三年 |
| 6 | 风险评估 | 提供新系统在入网前或未备案系统进行安全风险评估服务，包括人员访谈、漏洞检测、基线核查等，从而评估业务系统的安全状况，查找不符合安全要求的配置项以及安全风险点。 | 20套/年 | 三年 |
| 7 | 安全应急演练 | 提供安全应急演练服务，参照等保要求协助医院制定完善应急预案，开展周期演练，按流程处置突发安全事件：1、服务方应协助需方制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容,并定期进行应急预案的演练，演练频率不低于1次/每年；2、服务方应针对突发的安全事件，及时进行评估风险，按需对高危对象进行紧急安全策略加固；3、服务方应针对突发的安全事件，对病毒或恶意代码进行安全扫描与紧急查杀，并采取其他措施消除安全风险；4、服务方在安全事件报告和响应处理过程中，应按流程进行汇报，分析和鉴定。 | 2次/年 | 三年 |
| 8 | 安全巡检服务 | 提供安全巡检服务，每季度一次例行安全设备巡检，巡检内容为分为硬件状态检查、安全性检查和稳定性检查，详细要求如下：1、硬件状态检查包含：设备电源指示灯，网口指示灯，设备ALARM灯，CPU，内存等使用情况；2、安全性检查包含：配置备份，等保合规项检查，备机替换等；3、稳定性检查为对设备月度运行状态进行分析，包含：设备流量分析，系统日志分析和巡检脚本分析。 | 4次/年 | 三年 |
| 9 | 网络安全应急响应服务 | 提供1年应急响应服务，一旦医院发生网络安全事件，一般事件半小时内远程响应技术指导，重要事件2小时内现场响应处置，防止网络瘫痪、系统中断等对医院运营带来影响。 | 按需/年 | 三年 |
| 10 | 重大节日网络安全保障服务 | 提供重要时期安全保障服务，在重大会议、节假日等特殊时期内，指派安全攻防经验丰富的安全专家，对医院目标系统进行安全值守和保障，对业务系统的安全状况进行实时监控和日志分析。在重大节日期间，当目标遭受黑客入侵攻击时，值守人员应立即对入侵事件进行分析、检测、抑制、处理，查找入侵来源并恢复系统正常运行，完成后给出应急响应报告，报告中将还原入侵过程，同时给出对应的解决建议。 | 按需/年 | 三年 |
| 11 | 安全策略优化服务 | 提供安全策略优化服务，安全策略的维护随着时间的推移，会变得繁杂不堪，充斥着过时的信息、不正确的主机或网络定义，以及不再为业务提供支持的规则。需要定期对安全策略的生命周期进行管理，及时关闭未使用策略，同时对策略的设置进行最小化窗口检查。 | 按需/年 | 三年 |
| 12 | 网络安全培训 | 提供网络安全培训服务，针对全院人员进行1次网络安全培训服务（提升网络安全意识、提高安全用网技能），针对信息科进行网络安全运维培训（提升信息科技术人员网络安全运维能力）。 | 2次/年 | 三年 |
| 13 | 网络安全设备备机服务 | 根据医院当前网络安全设备部署情况，需提供7\*24小时备机服务，服务期内须将网络安全设备清单备机放置于医院机房，当安全设备发生故障无法恢复时，能够及时用备机进行更换，确保医院业务快速恢复，网络安全设备备机清单如下：数据中心防火墙2台，杀毒软件系统1套，外联区专线防火墙1台，外网防火墙1台，态势感知平台1台，潜伏威胁探针1台，数据库审计1台，漏洞扫描1台，网匣1台，上网行为管理1台，堡垒机1台，日志审计1台，网管系统2套。所提供备机性能和授权需满足医院业务使用需求。若备机出现故障导致无法正常使用，需及时更换相应设备，保障业务正常运行。 | 7\*24小时/年 | 三年 |
| 14 | 医院音视频系统安全服务 | 1、对医院信息发布系统，显示屏、LED屏幕等进行安全巡检，保障信息发布系统网络安全；2、对医院会议系统、远程医疗会诊系统、手术示教系统、移动医护系统、护理看板系统等音视频系统进行安全巡检，存在网络安全风险及时输出整改方案并协助医院整改，保障医疗健康数据信息安全。3、服务频次不低于每季度一次。 | 4次/年 | 三年 |