**网站维护安全检测内容**

|  |  |
| --- | --- |
| 服务项 | 服务要求 |
| **网站监测服务** | 定期对网络设备、网络安全设备、服务器系统、虚拟化系统等的安全运行状态进行巡检，对日志储存6个月情况进行检查，查看运行指标、受攻击情况和有关日志，出具巡检报告。对重要信息系统进行监测分析，结合内外部网络安全环境提供预警信息，形成监测预警报告。通过Web云监测平台结合网络安全服务专家人工监测分析的手段，对我院重要应用系统执行7x24在线监测，监测目标系统的可用性、安全性、内容风险、挂马威胁、网站钓鱼以及页面篡改等攻击行为。对我院网络设备、网络安全设备，以及可互联网访问的养护管理、微信办公机关事务等页面进行定期监测。其中专网监测定期对部署在专网内的网络设备、网络安全设备运行状况进行监测与日志收集、日志分析，监测频率每周不少于1个工作日；互联网页面监测由本次服务商提供技术手段或工具进行监测，对页面可用性和安全性进行监测，监测频率不少于每周5个工作日。以上监测过程中发现系统故障、安全风险、安全事件等问题情况应第一时间通知我院，并协同予以处置。服务单位自行提供的互联网页面监测手段或工具应无需安装额外的硬件、软件和系统插件，不改变现有的网络环境、不影响系统性能，支持敏感词信息发现，支持对恶意隐藏链接（暗链）、非法链接（搜索引擎流量劫持桥页链接）等进行检测，支持对网页木马检测，支持同时检测网页的HTTP、DNS、PING响应，支持DNS劫持告警。收集网络安全预警信息，结合我院实际，做好防范工作。协助我院完成省市网络安全信息通报要求中规定的月报、季报、重大事件处置表等材料的汇总上报。 |
| 供应商安全服务人员需对监测数据进行人工分析，对危险等级较高的威胁情报需在系统预警1小时内完成人工分析验证以甄别误报，对验证为真实攻击的事件需第一时间通报我院，并协同我院进行处置。 |
| 服务频次：连续性服务，每年度提供365天x24小时监测预警服务；成果交付：《徐州口腔医院网络系统运行监测报告》（月报、季报、年报）；服务月报在当月服务完成后3日内提交，季报在季度服务完成后5日内提交。 |