|  |  |
| --- | --- |
| **设备名称** | **医院信息安全服务四期** |
| 1. **互联网资产发现服务：**发现和管理医院互联网边界已成为网络安全和数据安全的刚性需求。互联网资产发现是通过搜索引擎及网络爬虫等多种技术相结合，通过对关键字、域名及IP的综合查询及关联分析，从而为中医院梳理出互联网资产全景图的服务。资产及应用发现后形成资产及应用系统清单，包含但不限于域名、IP 地址、系统名称、用途等； 梳理告警无主资产、老旧废资产、潜在攻击路径资产等内部资产，梳理供应链提供的信息系统（含定制开发和市场采购）、核心网络及安全产品、信息化平台或软件、服务类资产等。 2. **敏感信息泄漏检查服务：**持续开展互联网敏感信息泄露情况排查，收集IT资产信息，包括域名、IP、开放端口、证书信息、企业名称、备案信息、whois信息等作为搜索的敏感特征。再配合关键词如网络架构图、网络拓扑图、邮箱、密码、文件名、通讯录、内部资料、安装说明等在互联网敏感信息暴漏源中进行搜索发现。探测范围覆盖互联网的各种信息泄露渠道，覆盖互联网各类公开应用（如搜索引擎、代码托管平台、网盘等）。 3. **安全资讯与预警通告：**基于威胁情报、安全大数据以及攻防能力推出的网络安全情报类资讯服务，分别通过实时和定期2种方式推送。除了实时的高危漏洞预警和每周安全热点资讯外，还将通过月度安全通告为中医院汇总月度的高危漏洞、安全热点，威胁情报解读精华及漏洞分析统计，为中医院提供有价值的网络安全态势推送。 4. **渗透测试：**在授权和监督下，对指定敏感区域和业务系统采用黑盒结合灰盒方式和利用已知漏洞信息且重点关注弱口令、远程访问控制、SQL注入漏洞等问题进行非破坏性的模拟黑客攻击测试，发现漏洞不进行破坏，并协助进行修复，修复后进行复测，以确认漏洞是否被完全修复。 5. **入网安全评测：**规范建立本院新业务系统、对中医院新建设信息系统或旧系统升级扩容，发生重大变更的系统，在上线前进行上线前安全测评（具体系统由本院指定），包括符合性及基线配置核查、漏洞扫描、渗透测试等内容，均应通过入网安全测评后，才可接入网络中，避免为网络带来安全隐患。 6. **APT检测：**通过web日志分析和威胁情报分析挖掘APT攻击线索，提升医院对高级威胁看见的能力。通过安全大数据进行发掘和分析，因为任何攻击线索都会有相关联的其他信息被互联网数据捕捉到，所以从互联网进行挖掘可极大提升未知威胁和APT攻击的检出效率，而且由于数据的覆盖面更大，可以做到攻击的更精准溯源。 7. **API安全分析：**应用API安全卫士评估产品，针对医院的应用程序接口进行的安全技术评估，并通过人工服务对API资产梳理、对应用程序重要接口进行渗透测试，进而保护应用程序API安全，解决API资产捋不清、API攻击难识别、API数据泄露无感知、API安全管控无办法等一系列问题。 8. **驻场运营保障服务：**包括安全基线评估、安全策略优化、安全设备巡检、安全设备巡检、安全加固服务、态势感知监测服务、除日常网络安全运营工作外，对院内日常网络维护工作进行支撑，贴合实际工作执行，以适应院内网络安全管理工作需要。 9. **实战攻防演练：**攻击队评估服务最大限度模拟APT攻击手法，不限定攻击路径和手段，以不采用破坏性攻击为底线，以系统提权、控制业务、获取数据为目标，以最大程度暴露广东省中医院安全风险、发现广东省中医院防护和威胁发现短板为目的，深入评估其安全防护能力。攻击队针对目标系统、人员、软件、硬件和设备同时执行的多混合、基于对抗性的模拟攻击，以此来发现系统、技术、人员和基础架构中的存在的隐患。用尽可能接近真实环境攻击的方法来模拟黑客APT攻击，从而发现有可能被黑客利用的安全漏洞，以此对目标网络安全状况进行评估。 10. **钓鱼邮件演练服务：**钓鱼邮件测试服务基于社会工程学的原理，根据广东省中医院网络环境、邮件使用习惯和特征，结合组织内的热点事件，精心构造一份极具欺骗性、迷惑性，含有钓鱼链接的钓鱼邮件，模仿组织内部门向目标群体定向发送钓鱼邮件，进行钓鱼测试。基于测试结果，分析评估组织内部人员信息安全意识，尤其是对于钓鱼邮件识别的现状，为广东省中医院后续加强信息安全培训、提升技术防护手段，提供支撑依据 11. **网络安全应急演练服务：**组建防守方和攻击方在广东省中医院真实环境中进行实际的演练攻击，攻击方采用各种技术手段模拟黑客攻击，发起各类攻击事件，防守方检测和发现外部攻击，并对攻击采取相应的防护措施，导演方负责演练导演、监控进程、全程指导、应急处置、演习总结、技术措施与策略优化建议等技术咨询工作。 12. **网络安全应急响应服务：**在医院遇到突发安全事件后，采取专业的安全措施和行动，并对已经发生的安全事件进行监控、分析、协调、处理、保护资产等安全属性的工作；安排安全专家在2小时内到达现场，进行事件处置分析，协同加固，并出具相应报告；提供安全专家远程应急咨询服务。 13. **安全意识和技能培训：**组织信息技术人员深入学习掌握各类网络安全产品知识，使信息技术人员能够进一步掌握各类安全产品知识的配置、监控、维护、常见故障处理等。通过深入开展安全技能培训及安全运维专题培训，强化网络安全运维人员岗位技能，进一步提高运维团队网络安全运维能力和持续改进能力。编制安全意识宣贯材料，组织中医院全员进行安全意识教育培训，让相关人员了解当前的网络安全形势，已经发生的重要特殊或敏感时期的安全事件以及具体攻击方式方法，提出安全保障的底线和红线工作，涉及安全保障工作的操作工作规范等。 14. **CTF技术培训：**组织中医院安全运维人员开展CTF技术培训，提供CTF相关网络安全知识现场授课与及实际操作演练培训，为中医院培养了解、熟悉CTF竞赛相关理论知识与实际操作的人才，协助中医院选拔参加未来的各类医疗卫生行业CTF竞赛的人员、组建CTF参赛团队。 | |
| 1. **主要配置要求**   省中医院主要业务系统10个，次要系统50个，网络设备600，安全设备30，服务器（虚机300，实机200），终端6000。核心机房2个。  **互联网资产发现服务**：2次/年  **敏感信息泄露检查服务**：2次/年  **安全资讯与预警通告**：每周、每月  **渗透测试：**按需提供，不少于100个系统  **入网安全评测**：5个系统  **APT检测**：4次/年  **API安全分析**（包含工具）：4次/年  **驻场运营保障：**1人/年  **实战攻防演练**：1次/年  **钓鱼邮件测试**：1次/年  **应急演练服务：**1次/年，至少2个场景  **应急响应**：2次/年，10人天  **安全培训**：至少2次/年  **CTF技术培训（包含工具）**：5天/年 | |