|  |
| --- |
| 托管检测与响应服务 |
| 序号 | 参数内容 |
| 1 | 针对用户指定的服务资产（IP）提供安全专家在服务期内全天候7×24小时持续在线守护，同时要求安全专家主动识别安全风险（弱密码、勒索风险等）并跟进闭环，可以有效预防安全事件的发生，并提供全方面的安全托管能力，包括资产管理、脆弱性管理、威胁管理、事件管理、定期运营汇报等。并依据相关规范，利用漏洞扫描工具扫描网络中的核心服务器、重要的网络设备以及WEB业务系统，包括服务器、交换机、防火墙等的Web漏洞扫描、系统漏洞扫描/数据库漏洞扫描、信息泄漏检测、弱口令检测。对网络设备进行安全漏洞检测和分析，对识别出的能被入侵者用来非法进入网络或者非法获取信息资产的漏洞，并将这些漏洞信息与业务资产信息通过漏洞管理平台进行统一关联、展示与追踪，使得管理人员可以有效地追踪业务资产漏洞全生命周期，实现漏洞信息全生命周期的可视、可控和可管。 |
| 2 | ▲服务资产数量：不少于30个IP资产；服务频率：12个月7\*24小时。 |
| 3 | ▲针对服务范围内的资产提供全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全托管平台中进行管理；当资产发生变更时，安全专家对变更信息进行确认与更新。 |
| 4 | ▲具体服务内容如下：4.1资产识别与梳理4.1.1资产发现与识别 借助安全工具对用户资产进行全面发现和深度识别，并在后续服务过程中触发资产变更等相关服务流程，确保安全运营中心中资产信息的准确性和全面性。且为医院提供深度威胁狩猎服务（频率1次/季度）：安全专家可针对内/外网或特定业务系统及特定漏洞，基于客户业务定制检测逻辑，尽可能快地发现漏洞或攻击痕迹，发现潜在的安全隐患和已失陷的主机/被钓鱼成功的员工/账密信息泄露等，最大限度地降低攻击者造成的危害，评估造成的损失等内容，最终帮助客户验证风险并推动发现的问题和隐患进行闭环处理。4.1.2资产信息梳理与管理 结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理；当资产发生变更时，安全专家对变更信息进行确认与更新。4.1.3脆弱性评估 系统与Web漏洞扫描：对操作系统、数据库、常见应用/协议、Web通用漏洞与常规漏洞进行漏洞扫描。弱口令扫描：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等基线配置核查：检查支撑信息化业务的主机操作系统、数据库、中间件的基线配置情况，确保达到相应的安全防护要求。检查项包含但不限于帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制等配置情况4.1.4病毒类事件评估勒索病毒事件分析：安服专家分析判断主机是否感染了勒索病毒；是否已感染勒索病毒文件；根据已发生的漏洞攻击行为分析判断否存在勒索病毒攻击等。挖矿病毒事件分析：安服专家分析是否感染了挖矿病毒/木马；是否处于挖矿状态；根据已发生的漏洞攻击行为分析判断是否存在以植入挖矿木马为目的的漏洞攻击等蠕虫病毒事件：安服专家确认文件是否被感染，定位失陷的代码并进行修复4.1.5攻击行为评估 针对漏洞利用攻击行为、Webshell上传行为、Web系统目录遍历攻击行为、SQL注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务风险点。4.1.6失陷类事件评估失陷主机分析：安全专家对失陷主机进行分析研判（如后门脚本类事件），并给出修复建议。潜伏威胁分析：安全专家分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出解决建议。含：对外攻击、APT C&C通道、隐藏外联通道等外联威胁行为。4.2问题处置4.2.1脆弱性问题处置 针对内网脆弱性，安全专家分析研判后提供实际佐证材料，并给出修复建议。4.2.2病毒类事件处置针对病毒类事件。安全专家提供病毒处置工具并主导查杀10个实例。若超过10个实例，安全专家固化出实际可行的措施，确保用户可进行查杀病毒。4.2.3入侵攻击行为处置针对分析研判确认的入侵行为，安全专家给出策略调整建议。如果有AF设备等，在获得授权后，在服务时间内安全专家调整安全策略。4.2.4失陷类事件处置针对勒索、挖矿类事件。安全专家主导处置工作，并提供最大程度溯源服务（如涉及到重装业务系统，提供重装指导）；安全专家定位恶意文件路径并提供查杀指导（授权情况下，可由我方直接操作）；并分析有无异常进程与服务，发现异常进行通告（授权情况下，可由我方直接对异常情况进行操作）。针对后门脚本类事件。安全专家主导处置工作，提供专杀工具对感染服务器进行全面后门脚本查杀，并提供最大程度溯源服务。针对隐藏通信通道、可疑外发行为。安全专家提供实际佐证材料，并给出修复建议，提供最大范围的溯源服务。配合定位异常进程以及恶意文件，并提供查杀建议（客户授权情况下，我方开展查杀工作。默认主导查杀10个实例，若超过10个实例，固化出实际可行的措施，确保用户可进行查杀病毒。）4.3运营能力评估4.3.1安全调查采用线上调查问卷的方式，调研用户是否具备资产管理、漏洞管理、威胁监测技术、风险评估、应急预案等方面的信息安全措施。4.3.2安全运营能力成熟度评估采用线下访谈的方式，对用户信息安全措施进行调研评估。内容包含管理策略、资产管理、漏洞管理、威胁监测、威胁情报、风险评估、应急预案管理、安全事件管理。并根据调研的内容输出安全运营能力成熟度。4.3.3安全运营能力成熟度解读结合评估出的安全运营能力成熟度以及客户业务，提供安全能力差距分析报告解读。4.4漏洞管理4.4.1漏洞分析与管理漏洞扫描与验证：每月针对服务范围内的资产的系统漏洞和Web漏洞进行全量扫描，并针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。每日针对变更的资产执行增量扫描，并针对发现的漏洞进行验证。漏洞修复优先级排序与通告：基于漏洞扫描结果、资产重要性及漏洞的威胁情报，对漏洞进行重要性排序，确定修复的优先级；并将最终结果通告给用户漏洞落地性处置建议：对漏洞进行分类并书写漏洞分类处置方案，并通过工单系统跟踪修复情况。漏洞复测与状态追踪：对修复的漏洞进行复测，关闭正常修复的漏洞的工单。制定漏洞闭环服务报告，并向管理层进行汇报4.4.2弱口令分析与管理 实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等。针对不同行业提供行业密码字典，有针对性的进行内网弱口令检测。并将检测发现的问题通过工单系统跟踪修复状态。4.4.3最新漏洞预警与响应资产指纹信息梳理：梳理信息化资产详情（含操作系统、中间件、数据库、应用框架，开发语言等指纹信息）并将梳理的信息录入安全运营平台。最新漏洞预警与排查：实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。最新漏洞处置指导：一旦确认漏洞影响范围后，安全专家提供专业的处置建议，处置建议包含两部分，补丁方案以及临时规避措施。最新漏洞复测与状态跟踪：由安全专家对该最新漏洞建立状态追踪机制；跟踪修复状态，遗留情况。4.4.4漏洞协助处置制定处置方案：根据用户实际业务场景需求，制定最适合的漏洞处置方案。处置方案验证：根据漏洞处置方案，在用户提供的测试环境中开展漏洞处置方案验证工作，观察处置方案对测试环境产生的影响，并提供最优修复方案建议。漏洞处置实施：在用户授权下，对漏洞进行处置工作，并验证漏洞是否依然存在以及配合验证业务影响面。4.5威胁管理4.5.1威胁分析与通告 结合大数据分析、人工智能、云端专家提供安全事件发现服务：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态,发现各类安全事件，并自动生成工单实时监测网络安全状态，对攻击事件自动化生成工单,及时进行分析与预警。攻击事件包含境外黑客攻击事件、高级黑客攻击事件、持续攻击事件。实时监测网络安全状态，对病毒事件自动化生成工单,及时进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发DOS型、C&C访问型、文件感染型、木马型。安全专家针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机，将深度关联分析的结果通过邮件、微信等方式告知用户4.5.2流行威胁通告与排查 结合威胁情报，安全专家排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固主动分析与响应 每月主动分析病毒类的安全事件：安全专家提供病毒处置工具，并针对服务范围内的业务资产使用病毒处置工具进行病毒查杀，对于服务范围外的业务资产，安全专家协助用户查杀病毒；每月主动分析攻击类的安全事件：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗，当用户无防御措施时，提供攻击类安全事件的处置建议。每月主动分析漏洞利用类的安全事件并验证该漏洞是否利用成功，提供工具协助处置；每月主动分析失陷类的安全事件并协助用户处置，并提供溯源服务4.5.3策略管理 策略调配：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新策略定期管理：安全专家每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。策略调整：安全专家根据安全事件分析的结果以及处置方式，按需对安全组件上的安全策略进行调整工作。4.5.4持续攻击对抗 通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗。通过全网大数据分析，发现有境外黑客或高级黑客正在攻击，立即采取行动封锁黑客行为。4.6事件管理4.6.1事件分析与处置 对用户上报的安全事件进行及时响应。实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助客户快速恢复业务，消除或减轻影响。4.6.2应急响应 入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。入侵威胁清除：排查攻击路径，恶意文件清除。入侵原因分析：还原攻击路径，分析入侵事件原因。加固建议指导：结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵。4.7运营可视4.7.1安全运营可视化 通过安全运营平台，随时查看业务资产安全状态。在线展示所有事件监测结果、防御过程和防御结果。在线展示所有服务内容、流程和事件处理进展。4.7.2定期安全运营汇报 定期总结阶段性安全运营情况发送给用户，并向用户总结汇报。 |
| 5 | ▲暴露面梳理：使用安全工具对服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险。 |
| 6 | 服务催单：针对服务平台生成的工单，用户可按需催单，服务平台采用短信等方式通知安全专家，督促投标方第一时间处理。 |
| 7 | 实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件。 |
| 8 | ▲策略定期管理：安全专家每月对招标方的安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。投标方云端服务平台应当具备丰富的策略检查工具（要求不少于40种策略检查的工具），支持排查安全设备防护策略配置的合理性。 |
| 9 | ▲基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件客户可以在平台上直接发起服务咨询，云端进行紧急响应和处置。 |
| 10 | ▲提供服务监控门户，在门户中用户可查看业务安全状态，处置中的失陷事件以及针对这些事件的处置进度，处置责任人、联系方式等信息，方便用户时刻了解服务供应商的服务效果；平台支持的安全检测规则应超过1000个，且覆盖内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等。 |
| 11 | 支持展示出当前工单数量和工单处置状态，使得招标方能详细查看服务处置过程，查看安全事件闭环效果，掌握当前专家服务进度，监督服务质量。 |
| 12 | 支持展示出当前需要招标方审批的工单及其具体情况，使得招标方能完成与服务人员的协同处置，共同确保安全威胁和事件得到准确处置。 |
| 13 | ▲支持安全态势展示，展示出当前遭受的威胁事件信息以及脆弱性信息统计，并支持服务专家按照资产类别、威胁类型进行定制化筛选查看，能直观感受到招标方当前的风险态势情况。 |
| 14 | ▲本项目使用服务工具支持将收集的安全日志上传到本院现有的安全服务平台上，并支持在该平台上对服务工具进行管理（提供相关功能界面截图证明，加盖投标人公章）。若本项目使用服务工具无法与现有医院安全平台兼容并无法统一控制管理正常运行，医院不再另外采购配套设备，中标供应商须按照采购人的实际使用需求提供整套同等性能配置的设备以替换，提供的设备的硬件资源和性能配置须等于或更优于医院现有的设备资源、性能配置的总和。且服务期满后，安全服务工具的产权归用户单位所有。 |
| 15 | ▲为了保证安全监测的效果，需要安全服务平台具备检测规则的自定义功能，以满足日益复杂的安全趋势所带来的安全需求。 |
| 16 | ▲中标方需阶段性将安全运营情况发送给用户，并向用户总结汇报。交付物名称包含不限于：《事件调查报告》、《事件处置报告》、《应急响应报告》、《威胁狩猎服务报告》、《安全服务值守日报》（每日）、《安全运营报告》（周报）、《首次分析与处置报告》（首次交付）、《事件分析与处置报告》（周报）、《未公开威胁报告》（周报）、《综合分析报告》（月报）、《漏洞分析与管理服务报告》（周报）、《月报总结快报》、《半年度总结报告》、《年度总结报告》等;▲中标后采购人有权要求中标方严格按照上述频率要求提供服务交付物，确保满足采购人安全需求。如中标方未能按时提供，采购人有权终止服务合同，中间产生任何费用由中标方自行承担。▲中标后服务购买方有权要求中标方提供演示平台对服务平台进行功能演示，确保满足采购人安全需求。发现虚假应标的行为将予以废标处理并保留对该厂商追究相关责任的权利。▲为了保证本次安全服务实效性，对安全事件做到快速监测、发现、阻断、溯源、总结报告，需要对现场的态势感知平台进行联动响应，支持实时接收安全设备检测到的安全事件信息、安全日志数据提供7\*24小时的安全托管服务；（提供产品界面截图并加盖投标人公章） |

|  |
| --- |
| ▲商务要求  |
| 合同签订期 | 自成交通知书发出之日起7日内。 |
| 交付使用时间及地点 | 1.交付使用时间：自签订合同之日起，7个工作日内完成项目实施并交付采购人使用。2.交付地点：广西南宁市广西壮族自治区江滨医院(采购人指定地点)。 |
| 付款方式 | 1、项目服务半年后，采购人向成交人支付合同总金额的50%。2.项目维护期满后，采购人向成交人支付合同总金额的50%。3.付款前中标人须开具全额发票给采购人。中标人未开具发票的，采购人有权不进行支付。 |
| 质量要求 | 1.质量达到国家验收合格标准。2.供应商所提供的服务、技术参数等质量必须与响应文件和承诺相一致。 |
| 保密和廉洁要求 | 成交人必须如约承担合同履行时所应该尽的一切保密、廉洁义务。成交人对项目实施过程中的资料、数据进行保密，未经采购人书面同意不得泄露，且保密责任不因合同的中止或解除而失效，否则，需承担相应的法律责任。 |