**广东省中医院安全服务需求**

# 服务目标

本次安全服务的目标是对省中医院的信息系统以及内网及专网范围内的业务系统以国内最先进的手段，加强网络信息系统安全性，最快、最全面、对业务影响最小的方式进行网络安全核查，提高网络攻击和安全威胁的应对和处理能力，提供报告和整改意见，协助提升安全防御能力，构建一套符合省中医院信息化发展的安全体系。

# 医院现状

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。以下是医院的信息网络安全拓扑图：



# 服务需求

根据医院安全状况，将安全服务的内容设计为以下内容：互联网暴露面安全评估服务、应用系统渗透测试、新系统上线安全评估、重要时期保障服务、安全意识与技能提升培训服务、安全认证考试服务、网络安全急响应服务、攻击队评估服务、敏感信息泄露情报服务、钓鱼邮件演练服务、网络安全应急演练服务、综合安全评估、安全驻场服务共13项服务，以下是安全服务内容的具体需求：

1. **互联网暴露面安全评估服务**

基于网络扫描、搜索引擎、互联网基础数据引擎主动探测广东省中医院在互联网上暴露的资产，形成明确的资产清单。帮助广东省中医院发现未知资产。

通过数据挖掘和调研的方式确定广东省中医院资产范围，之后进行主动精准探测深度发现广东省中医院暴露在外的IT设备、端口以及应用服务，并由安全专家对每个业务梳理分析，结合业务特点对资产重要程度、业务安全需求进行归纳，最终针对性的形成广东省中医院的资产画像，精准探测互联网暴露面。

输出《互联网资产发现报告》。

1. **应用系统渗透测试**

在医院的授权和监督下，对医院认为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，并协助医院进行修复，修复后进行复测，以确认漏洞是否被完全修复。

测试对象不少于15个应用系统

输出：渗透测试报告

1. **新系统上线安全评估**

规范建立本院新业务系统、重大版本变动后的业务系统上线安全流程，在服务期内提供上线业务系统风险评估服务（具体系统由本院指定）。服务提供商自带（或利用本院已有安全服务工具）针对本院重要网站与业务系统进行漏洞扫描、漏洞验证和渗透测试工作，并提供相应的测试报告。要求采用专用安全工具对网站进行扫描，发现漏洞后进行手工验证，验证漏洞的真实性以及影响范围。另外一方面通过专业的渗透测试人员模拟黑客攻击对新系统进行渗透测试工作，全面发现新系统可能存在的风险，检查后给出详细的评估报告以及处理建议，评估对象不少于5个应用系统

检测内容包括：

1. 漏洞扫描

重要网站与业务系统上线前进行系统漏洞扫描工作，检测系统管理是否存在弱口令、信息泄露、代码执行、认证绕过等高危安全漏洞。

1. 渗透测试

针对B/S架构、C/S架构业务系统或APP系统进行渗透测试。

渗透测试过程主要依据安全厂商已经掌握的安全漏洞信息，模拟黑客的真实攻击方法对系统和网络进行非破坏性质的攻击性测试。这里，所有的渗透测试行为将在用户的书面明确授权和监督下进行。

输出：《xxx系统上线安全检测报告》

1. **重要时期安全保障**
2. 重要时期保障

重大时刻（如“两会”、重大活动、会议等），医疗行业往往是非法组织攻击的主要对象。所以在重大时刻，需要分别制定相应的防护策略和保障机制。

针对重大时刻（如“两会”、重大活动、会议等）安全运行保障的需求，提供的信息安全保障，制定完善的安全保障流程以及保障组织，重大时刻网络安全保障服务对象主要为各个网络系统及业务平台。

在特殊时期，以“事前准备、事中保障（值守、监控、应急、处置）、事后总结（复盘、提升）”的思路来保障本院信息系统的安全。

1. 安全迎检

安全检查是一种手段，是一种方法，是信息安全工作的一个重要环节，是以查代促、以查促改、以查促管、以查促防，旨在推动提高信息安全工作能力和防护水平。

依据相关部门安全检查指导文件，协助本院顺利完成各项网络安全检查；协助制定网络安全检查方案，并派遣人员组成迎检小组，检查的内容包括网络层安全、应用层安全、终端安全等，如针对网站检查，对SQL注入攻击、跨站脚本攻击、弱口令、木马病毒检测、端口开放情况、系统管理权限开放情况、访问权限开放情况、网页篡改情况等进行监控，认真检查保管系统安全日志进行检查。

1. 输出：安全值守报告、安全迎检总结等
2. **安全意识与技能提升培训服务**

A. 安全技术培训

通过安全技术培训，使信息技术人员熟悉并掌握安全运维流程制度及行业政策法规。

组织信息技术人员学习运维流程、规章制度，协助做好IT运维管理管理平台上线及具体执行文档的输出，落实安全运维管理制度。

组织信息技术人员学习交流国家政策法规及监管要求，提升安全运维合规管理水平。

组织信息技术人员运维运营管理标准化培训，提高运维团队责任意识。

组织信息技术人员信息安全风险教育，提高运维团队风险意识。

a) 安全及网络技术专题深入培训

通过深入技术培训，使信息技术人员进一步提高网络、安全技术水平，提升网络运维能力。

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。

组织信息技术人员深入学习安全技术知识，巩固提高运维团队安全技术水平，及时掌握最新网络攻击风险防范手段。

组织信息技术人员进行数据中心架构培训，使运维团队熟悉掌握整体架构及数据中心内部分区、分层、模块化架构规划设计及实现。

b) 安全运维技能提升培训

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。

组织网络安全运行状态及安全事件分析技能培训，使信息技术人员成员具备网络安全性深入分析及风险预测能力。

加强信息技术人员运维运营管理培训，使信息技术人员掌握运维运营相关流程，并能落实到日常运维工作中。

组织网络安全评估技能培训，使运维团队具备网络安全评估能力，能从网络架构、设备环境、设备安全运行状态、配置规范性、网络性能、网络事件、运维管理、硬件生命周期、业务连续性等方面进行网络安全评估，并能据此提出优化加固措施。

c) 培训内容包括但不限于以下内容：

 国家等级保护流程与相关内容

 医疗行业等级保护建设案例分享

 医疗行业内外网互联安全建设风险

 医疗行业网站建设和漏洞防范介绍

 医疗行业数据库安全和漏洞防范介绍等。

B. 工作项目输出:培训计划、培训方案、课程教材、培训成效评估等

1. **安全认证考试服务**

“注册信息安全专业人员-渗透测试工程师”，英文为Certified Information Security Professional - Penetration Testing Engineer，简称CISP-PTE。持证人员主要从事信息安全技术领域网站渗透测试工作，具有规划测试方案、编写项目测试计划、编写测试用例、测试报告的基本知识和能力。

提供2人的注册信息安全专业人员-渗透测试工程师（CISP-PTE）认证考试培训

1. **网络安全急响应服务**

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。

达到第一时间恢复医院业务，追踪失陷原因并提供可行性建议，避免同类安全事件再次发生的目的。

服务内容范围为医院现场发生的信息破坏事件（篡改、泄露、窃取、丢失等）、大规模病毒事件、网站漏洞事件等信息安全事件时，由服务商提供应急响应专家协助处置现场突发安全事件。其中，应急响应事件服务内容范围具体包括以下内容：勒索病毒、挖矿木马、蠕虫病毒、APT事件、网站挂马、网站暗链、网站篡改、漏洞事件、数据泄露以及其他安全事件。

在处理应急事件时，查找定论问题根源，提供安全事件主导定位跟踪服务，直到确认问题，协助后续工作排查与应急总结汇报工作。

按需提供应急响应，提交《应急响应服务报告》

1. **攻击队评估服务**

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，深入评估企业安全防护能力。

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。

**评估点包括：**

* 系统：深入的攻击队评估将测试并暴露多个领域的漏洞。
* 整体IT架构防护能力：网络、应用、路由器、交换机、电子设备等。
* 人员：职工、独立承包商、供应商、部门和业务合作伙伴等。
* 物理：IOT设备、门禁、智能终端等。
* 安全监控能力：日志保存、审计能力、APT攻击发现响应能力

评估后成果确认分为编写报告和协助整改两个阶段，渗透测试工程师会绘制渗透路线并对系统的安全性做评估，并协助医院实施安全整改工作。

输出：《攻击队评估测试报告》

1. **敏感信息泄露情报服务**

敏感信息泄露情报服务是以攻击队视角，监控广东省中医院的敏感信息泄露情况的情报服务，监控范围覆盖互联网的各种信息泄露渠道。

服务探测范围覆盖互联网的各种信息泄露渠道，一次服务、全网情况一网打尽，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）。

探测的数据泄露渠道包括：

* 搜索引擎类：Google、Baidu、sougou、360、bing、yahoo等；
* 代码托管平台类：GitHub、Bitbucket、Gitee、Gitlab等；
* 漏洞平台类：国家信息安全漏洞库、国家信息安全漏洞共享平台、freebuf、补天漏洞响应平台、安全客等；
* 网盘类：百度云盘、新浪微盘、QQ微云网盘、115网盘等；
* 文库类：百度文库、豆丁、道客巴巴等；
* 社交平台类：微信公众号、微信小程序、微博、QQ群、论坛、贴吧等；
* 社工信息类：姓名、电话、邮箱等；
* 招商、业务相关类：招标信息、招聘信息、子公司信息；
* 资产信息类：whois查询、SPF记录查询、指纹识别、子域名、目录、端口等；
* 网页快照类。

输出：《敏感信息泄露情报分析报告》

1. **钓鱼邮件演练服务**

钓鱼邮件是目前非常普遍的一种社会工程学攻击方式，据统计，约92%的数据泄露事件、社会工程学事件与鱼叉式网络钓鱼攻击有关。

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。

输出：《xxx钓鱼邮件演练报告》

1. **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。通过攻防演练，通过实战，真刀真枪的检验广东省中医院的安全产品、安全策略、安全体系、人员能力和协同处置等多方面内容。

总体的应急演练的基本流程主要包括如下阶段：准备阶段、监测及事件分析阶段、事件处理阶段、结束响应阶段、总结及预警阶段这5个阶段。

1. 准备阶段

包括了人员、组织的准备以及技术的准备，技术准备主要是要建立监控管理的技术体系和平台，为事件发生后的技术分析，及时的通告和响应等提供条件和保障。同时，尽可能地在事前做好相应的安全防范工作，准备好进行应急处理的技术工具等内容。

1. 监测及事件分析阶段

监测人员通过手动监测方式以及在准备阶段建设好的安全运行管理中心的监测方式，监测是否有异常现象的发生；当发生异常情况时，根据异常的性质与影响，决定是否向相关人员进行报告。上报方式除了通常的电话外，还可以利用安全运行管理中心平台中的告警机制，根据告警级别的不同，通过工单、邮件、短信的方式上报和通知到相关人员。

上报到应急响应管理小组后，对异常情况进行分析，判断事件类型，识别攻击的性质以及攻击强度，同时根据事件影响决定是否报告网络与信息安全工作小组；在必要的时候，向公安机关报案以获得帮助；

1. 事件处理阶段

根据事件的不同，采取不同的处理方案，启用相应的专题应急预案，对于常见的、主要的事件类型，在本预案中附带了两个典型场景应急演练流程，如需其他场景，需要后续根据实际情况中进行调整。该阶段中的技术处理主要为抑制事件的影响，并进行根除。

1. 结束响应阶段

网络与信息安全工作小组根据之前判断的攻击信息，采取必要的技术手段控制攻击行为、恢复系统服务并对攻击的来源进行追踪；必要时向公安机关通报相关信息，对攻击者进行抓捕。

1. 总结汇报阶段

当攻击事件结束后，系统恢复正常，由网络与信息安全管理小组对整个事件进行总结分析，向网络与信息安全领导小组进行汇报；网络与信息安全领导小组组织相关人员就本次事件总结经验教训，同时从中总结预警方案和内容，一方面进一步改进和完善应急响应体系，另一方面在公司内部的发布渠道上，适时发布总结后的预警信息，从而逐渐完善信息安全的整体安全保障能力。

输出：《xxx应急演练报告》（含方案、演练脚本）

1. **综合安全评估**

通过对提供服务的信息系统以及内网及专网范围内的业务系统进行综合环境评估能够有效发现业务系统网络方面的结构合理性，主机方面的访问控制、身份识别，应用方面的逻辑安全、安全功能，数据库方面的数据安全，管理方面的制度和规范等安全漏洞和安全风险，为全面有效落实安全管理工作提供资料，有助于加强安全管理，推动医院做好每项安全工作。

* 对广东省中医院的信息系统以及内网及专网范围内的业务系统以国内最先进的手段，最快、最全面、对业务影响最小的方式进行远程漏扫和配置核查，发现安全漏洞，提供报告和整改意见，协助提升安全防御能力。
* 在现场进行网络、主机、应用、数据库、中间件、安全管理方面的配置核查，包括手工检查、安全审计和安全策略评估，对不合理项提供改善建议，更好地保障各业务系统的正常运行，全面提升网络安全保护水平。

输出：《信息系统资产收集调研表》、《风险评估实施方案》、《安全扫描申请单》、《网络与应用安全合规检查项》、《风险评估问题清单与整改建议》、《风险评估分析报告》。

1. **安全驻场服务**

在服务期间，提供1名专职技术人员驻点在广东省中医院提供安全驻场服务，工作职能、概述如下：

1人，采用每周不低于5\*8驻场方式进行考勤，作为小组主要的固定技术实施人员，根据科室制定的《网络安全运营制度》，按照工作任务清单逐项、按期开展网络安全运维工作，以及运营小组交办的其他安全管理工作，除技术运维外也包括安全管理相关的事务类工作。包括但不限于：

* **安全基线评估：**采用最佳配置核查实践对全网范围的操作系统、数据库、中间件、网络设备、网络安全设备、网络边界进行分析和配置核查
* **安全策略优化：**安全策略优化是指对安全控制策略是否起到作用、是否合理高效进行检查和改进，可以及时地发现和控制风险。在运维服务的过程中，需要持续地对信息系统各个层面的安全策略进行优化，需要通过工具及人工的方式进行检测、分析、优化。
* **安全设备巡检：**信息安全产品运行维护是指在信息安全产品常态化运行过程中所进行的一系列维护工作，包括设备运行安全监测、设备运行安全审计、设备及策略备份更新等工作。
* **安全漏洞扫描：**通过漏洞扫描工具进行安全扫描评估，可以及时发现信息系统中存在的安全漏洞，通过对Windows、Linux服务器及安全设备漏洞的整改，可以及时地消除安全漏洞可能带来的安全风险。
* **安全加固服务：**在检测评估工作结束后，根据列出的问题清单和实际安全需求，对网络设备、安全产品、操作系统、应用系统、数据库等信息资产的安全配置策略和漏洞协助医院实施安全加固。
* **态势感知监测服务：**协助医院运维人员，从事态势感知平台系统的日常巡检、日常告警处置、定期统计报告、流量分析、安全规则调优等工作，与二线专家建立快速响应通道，帮助医院及时对安全事件的进行分析和反馈，提升安全运营工作效率。
* **** 除日常网络安全运营工作外，对科室日常网络维护工作进行支撑，贴合实际工作执行，以适应广东省中医院网络安全管理工作需要。

输出：《基线评估核查报告》、《安全策略优化报告》、《设备巡检报告》、《安全漏洞扫描报告》、《安全漏洞加固方案建议》、《态势感知平台运营报告》

**需求方案报价要求：**

以下附上具体安服项目需求表格（每项内容单独报价）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务项** | **服务内容** | **服务频次** | **服务输出** |
| 1 | **互联网暴露面安全评估服务** | 通过调研的方式确定互联网资产范围，之后基于IP或域名，采用 WEB扫描技术、操作系统探测技术、端口的探测技术、服务探测技术等各类探测技术，对互联网侧的主机/服务器、安全设备、网络设备、工控设备、WEB应用、中间件、数据库、邮件系统和DNS系统等进行主动发现，并生成资产及应用列表，列表中不仅包括设备类型、域名、IP、端口，更可深入识别运行在资产上的中间件、应用、技术架构的详细情况（类型、版本、服务名称等）。 | 每季度1次，全年共4次 | 《互联网暴露面安全评估服务》 |
| 2 | **应用系统渗透测试** | 对web应用系统进行非破坏的模拟攻击或入侵，利用服务方掌握的漏洞情报和测试人员的专业知识来识别web应用系统的漏洞。检测过程涉及对目标系统进行主动分析，以发现可能由于系统配置不当而导致的潜在漏洞，包括已知和未知的软件缺陷以及流程和技术措施中的操作弱点，并协助应用方进行修复，修复后进行复测，以确认漏洞是否被完全修复。 | 全年15个系统渗透测试服务 | 《xxx应用系统安全检测报告》 |
| 3 | **新系统上线安全评估** | 对新上线系统进行安全评估，发现系统存在的技术风险，防止系统带伤上线，一般由漏洞扫描、配置核查、渗透测试等多个服务组成。 | 全年5个业务系统上线评估 | 《xxx系统上线安全检测报告》 |
| 4 | **重要时期保障服务** | 在重要时期提供网络安全专业现场值守服务、依托威胁流量监测系统，提供网络安全专家服务，协助进行更复杂、更深入的安全威胁和事件研判，并且对攻击影响范围、后果进行分析，发现安全防御体系和策略的实战缺陷，并配合进行紧急整改。对重保过程中发现的新漏洞，进行验证，并协助进行紧急处置。 | 15人天重要时期保障服务 | 《xxx重要时期安全保障报告》 |
| 5 | **安全意识与技能提升培训服务** | 安全意识培训：对全体员工进行信息安全意识类的培训，包括政策法律法规解读、日常安全防范等，使员工在日常工作中提升信息安全意识。运维安全意识培训：对日常运维技术人员进行技术方面的日常安全运维方面培训，包括运维安全基础知识、如何提高运维安全水平、服务器常见安全风险、安全与合规等方面，以提升安全操作意识及安全工作规范。 | 2次安全培训服务 | 《安全意识培训教材》、《运维安全意识培训教材》 |
| 6 | **安全认证考试服务** | 提供“注册信息安全专业人员-渗透测试工程师”认证考试培训 | 2人考试培训 | 《认证培训教材》 |
| 7 | **网络安全急响应服务** | 在省中医发生确切的安全事件时，应急响应实施人员及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏服务基础上，实施人员协助省中医检查所有受影响的系统，在准确判断安全事件原因的基础上，提出基于安全事件整体安全解决方案，排除系统安全风险并协助追查事件来源、提出解决方案、协助后续处置。 | 按需要响应支持 | 《xxx应急响应报告》 |
| 8 | **攻击队评估服务** | 通过远程与现场的蓝队评估服务，采用最大限度模拟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，深入评估用户网络安全防护短板。  | 全年共1次服务 | 《攻击队评估报告》 |
| 9 | **敏感信息泄露情报服务** | 以攻击视角，聚焦于分析医院敏感信息泄露情况，探测范围覆盖互联网的各种信息泄露渠道，并对敏感信息利用场景、方式进行关联分析。全面覆盖互联网的常用信息泄露渠道，如搜索引擎、代码托管平台、文库、社交平台、漏洞平台、网页快照、网盘等，信息范围包括社工信息类、资产信息类等。 | 每半年1次，全年共2次 | 《敏感信息泄露情报分析报告》 |
| 10 | **钓鱼邮件演练服务** | 基于社会工程学的原理，根据用户网络环境、邮件使用习惯和特征，结合组织内的热点事件，精心构造具有欺骗性、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。 | 全年提供1次服务 | 《xxx钓鱼邮件演练报告》 |
| 11 | **网络安全应急演练服务** | 协助省中医组织策划和开展应急演练，包括制定演练计划、编制演练工作方案、设计演练脚本、配合准备演练环境、动员与培训、演练过程记录和总结等工作。 | 全年提供1次2个场景服务 | 《xxx应急演练报告》（含方案、演练脚本） |
| 12 | **综合安全评估** |  通过对提供服务的信息系统以及内网及专网范围内的业务系统进行综合环境评估能够有效发现业务系统网络方面的结构合理性，主机方面的访问控制、身份识别，应用方面的逻辑安全、安全功能，数据库方面的数据安全，管理方面的制度和规范等安全漏洞和安全风险，为全面有效落实安全管理工作提供资料，有助于加强安全管理，推动医院做好每项安全工作。 | 1次/年 | 《信息系统资产收集调研表》、《风险评估实施方案》、《安全扫描申请单》、《网络与应用安全合规检查项》、《风险评估分析报告》、《风险评估问题清单与整改建议》 |
| 13 | **安全驻场服务** | 1、**安全基线评估：**采用最佳配置核查实践对全网范围的操作系统、数据库、中间件、网络设备、网络安全设备、网络边界进行分析和配置核查2、**安全策略优化：**安全策略优化是指对安全控制策略是否起到作用、是否合理高效进行检查和改进，可以及时地发现和控制风险。在运维服务的过程中，需要持续地对信息系统各个层面的安全策略进行优化，需要通过工具及人工的方式进行检测、分析、优化。3、**安全设备巡检：**信息安全产品运行维护是指在信息安全产品常态化运行过程中所进行的一系列维护工作，包括设备运行安全监测、设备运行安全审计、设备及策略备份更新等工作。4、**安全漏洞扫描：**通过漏洞扫描工具进行安全扫描评估，可以及时发现信息系统中存在的安全漏洞，通过对Windows、Linux服务器及安全设备漏洞的整改，可以及时地消除安全漏洞可能带来的安全风险。5、**安全加固服务：**在检测评估工作结束后，根据列出的问题清单和实际安全需求，对网络设备、安全产品、操作系统、应用系统、数据库等信息资产的安全配置策略和漏洞协助医院实施安全加固。6、**态势感知监测服务：**协助医院运维人员，从事态势感知平台系统的日常巡检、日常告警处置、定期统计报告、流量分析、安全规则调优等工作，与二线专家建立快速响应通道，帮助医院及时对安全事件的进行分析和反馈，提升安全运营工作效率。 | 1人/年 | 《基线评估核查报告》《安全策略优化报告》《设备巡检报告》《安全漏洞扫描报告》《安全漏洞加固方案建议》《态势感知平台运营报告》 |

# 安全服务工具要求

为了更好的支撑安全运行监测服务，安全服务内容中所需要的渗透测试工具需具备以下要求：

1）可实现自动化渗透测试，贯穿整个渗透过程的操作，包括信息收集、指纹管理、漏洞发现、漏洞利用、后渗透攻击等。（提供功能截图）

2）可以根据可编程平台提供的接口编写自己的攻击插件，实现自定义的攻击需求。（提供功能截图）

3）可利用http协议、DNS协议等远程获取带外数据。（提供功能截图）

4）可通过内置的方法反弹交互shell到平台，执行vim、交互执行操作等功能。（提供功能截图）

5）需具备公安部销售许可证（提供相关证明材料，并加盖公章）

# 服务单位资质要求

1.企业均应具有独立法人资格并在广州市设立的分支机构，持有工商行政管理部门核发的营业执照，按国家法律经营。

2.企业需具备由中国网络安全审查技术与认证中心出具的 CCRC信息安全服务资质-安全运维资质证书；

3. 企业需具备由中国网络安全审查技术与认证中心出具的 CCRC信息安全服务资质-应急处理资质证书；

4．企业需具备由中国网络安全审查技术与认证中心出具的 CCRC信息安全服务资质-风险评估资质证书；

5. 企业需具备由中国信息安全测评中心出具的；国测信息安全服务资质-安全运营类资质证书；

6.企业需具备由中国信息安全测评中心出具的；国测信息安全服务资质-风险评估类资质证书；

7.企业需为国家信息安全漏洞库（CNNVD）技术支撑单位；

8.企业被有关部门责令停业、企业财产被查封和冻结或者处于破产状态的，不允许参加本项目报名。

9. 本项目不接受联合报价。