xxglk2024p018

技术服务合同

合同编号：xxglk2024p0018

签订地点：琼海市

签订时间：2024 年 8 月 27 日

甲方：琼海市中医院

乙方：海南世纪网安信息技术有限公司

根据《中华人民共和国政府采购法》《中华人民共和国民法典》及（项目编号：FJQH-2024-019；项目名称：2024年琼海市中医院等级保护及安全服务的）《磋商文件》、乙方的《响应文件》及《成交通知书》，甲、乙双方同意签订本合同。详细技术说明及其他有关合同项目的特定信息由合同附件予以说明，合同附件及本项目的磋商文件、响应文件、《成交通知书》等均为本合同不可分割的部分。双方同意共同遵守如下条款：

一、合同服务

序号	项目名称	项目内容	单价（元）	数量	单位	小计（元）
1	医疗信息集成平台（三级）等保测评服务	三级系统的服务内容包括:安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个方面的安全测	¥68600.00	1	项	¥68600.00
2	HIS系统（三级）等保测评服务		¥68600.00	1	项	¥68600.00

3	互联网医院管理系统（三级）等保测评服务	评。3级测评内容有71个控制点、211个要求项	¥68600.00	1	项	¥68600.00
4	琼海中医院网站系统（二级）等保测评服务	二级系统的服务内容包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个方面的安全测评。2级测评内容有68个控制点、135个要求项	¥43000.00	1	项	¥43000.00
5	PACS系统（二级）		¥43000.00	1	项	¥43000.00
6	应急演练服务	根据国家法律法规要求，针对医院开展一次网络安全事件应急演练，应急演练以演示或者模拟环境的形式，以通信故障、系统安全、软硬件故障几大类进行编制再结合医院场景定制，并根据医院信息系统的实际情况，指导医院建立健全信息与网络安全事件应急响应工作机制，并对信息系统相关人员进行应急预案、应急技巧及对典型的网络安全事件进行预防等方面的培训。	¥36200.00	1	次	¥36200.00

7	网络安全培训服务	组织全院员工开展一次线下网络安全培训，邀请具有丰富网络安全经验和教学经验的专家担任培训讲师，根据医院情况制定培训内容，内容包括但不限于：网络安全意识培训、网络安全技能培训、网络安全等级保护测评培训、商用密码应用安全性评估培训、数据安全培训，以及定向网络安全专项培训等。	¥4000.00	1	次	¥4000.00
8	内网威胁分析服务	在医院内网部署先进的威胁分析设备，结合专业的人工分析手段，对医院内部网络的主机、应用系统和终端设备进行全面而深入的安全检测。服务内容包括：高级持续性威胁（APT）分析、数据分析、木马分析以及蠕虫分析等，旨在准确识别并评估内网中可能存在的各类安全威胁，如APT攻击、木马蠕虫、恶意文件、后门等。	¥40000.00	1	次	¥40000.00
9	合计					¥372000.00元

二、合同总价

合同总价为：￥ 372000.00 元，人民币大写 叁拾柒万贰仟元整 ；税率 6% ；该合同总价已包括人员、耗材、差旅、餐饮、现场服务、验收合格前及服务期内服务与响应等所有其他有关各项的含税费用。本合同执行期间合同总价不变，甲方无须另向乙方支付本合同规定之外的其他任何费用。

合同的组成包括

1、合同文本

2、开标一览表

3、分项报价明细

4、中标通知书

5、服务方案

6、甲乙双方约定的其他文件

三、质量要求

依据国家和行业指定标准开展技术服务工作，并出具符合等级保护管理部门要求的测评报告等相关报告。

四、项目工期、技术服务方式及服务地点

1.项目工期：等级保护测评服务在医院通知入场60日内完成所有测评服务工作，其他安全服务工作在签订合同起一年内根据医院实际需求开展相应安全服务。每项服务完成后的15天内向甲方出具报告。

2.技术服务方式：由乙方负责，开展现场或远程技术服务。

3.服务地点：甲方指定地点。

五、付款方式

技术服务费由甲方分期支付乙方。具体支付方式和时间如下：

1.当甲乙双方签订合同后，根据乙方所开具的合格发票在15个工作日内，甲方支付给乙方合同总金额50%，即支付人民币：￥186,000.00（大写人民币壹拾捌万陆仟元整）。

2.乙方完成所有服务工作且项目通过验收后，根据乙方所开具的合格发票在

15个工作日内，甲方支付给乙方合同总金额50%，即支付人民币：￥186,000.00（大写人民币壹拾捌万陆仟元整）。

六、质保期及售后服务要求

乙方对于评估中发现的应用系统、主机和网络设备漏洞，提供项目验收后一年内的跟踪服务，对本次评估范围内的问题提供远程或现场技术咨询，对于漏洞的修补、问题的排除给出建议和指导。

七、安装、调试、测评、分析：乙方必须依照招标文件的要求和投标文件的承诺，按照服务清单实施服务。

八、验收：按招标文件及投标文件技术参数进行验收。

验收由甲方组织，乙方配合进行：

1）技术服务工作成果的验收标准：完成合同约定技术服务，提交《网络安全等级保护测评报告》、《应急预案》、《应急演练总结报告》、《培训签到表》、《网络安全培训PPT》、《内网威胁分析报告》作为验收合格标准。

2）验收方式：乙方完成全部技术服务工作，出具相关报告后，甲方组织人员对乙方的技术服务及等保测评报告进行审核；

3）验收的时间和地点：按照合同约定，在项目执行完毕后10个工作日内，在甲方指定地点进行验收。

九、违约责任与赔偿损失

1) 乙方交付的技术服务报告不符合招标文件、报价文件或本合同规定的，甲方有权拒收，并且乙方须向甲方支付本合同总价5%的违约金。

2) 乙方未能按本合同规定的项目工期完成技术服务和交付报告，从逾期之日起每日按本合同总价3‰的数额向甲方支付违约金；逾期半个月以上的，甲方有权终止合同，由此造成的甲方经济损失由乙方承担。

3) 甲方逾期付款，每日按本合同总价的3‰向乙方偿付违约金。

十、争议的解决

1)合同执行过程中发生的任何争议，如双方不能通过友好协商解决，如协商不成，任何一方应向甲方所在地有管辖权的人民法院提起诉讼。为解决争议而发生的费用由违约方承担，其中包括但不限于为诉讼而支出的诉讼费用、律师代理费、差旅费用、保全费用、保全保险费、鉴定费、公证费等为维护合法权益而支出的一切费用。

十一、不可抗力：任何一方由于不可抗力原因不能履行合同时，应在不可抗力事件结束后1日内向对方通报，以减轻可能给对方造成的损失，在取得有关机构的不可抗力证明或双方谅解确认后，允许延期履行或修订合同，并根据情况可部分或全部免于承担违约责任。

十二、税费：在中国境内、外发生的与本合同执行有关的一切税费均由乙方负担。

十三、其它

1) 本合同所有附件、招标文件、投标文件、中标通知书通知书均为合同的有效组成部分，与本合同具有同等法律效力。

2) 在执行本合同的过程中，所有经双方签署确认的文件（包括会议纪要、补充协议、往来信函）即成为本合同的有效组成部分。

3) 如一方地址、电话、传真号码有变更，应在变更当日内书面通知对方，否则，应承担相应责任。

4) 除甲方事先书面同意外，乙方不得部分或全部转让其应履行的合同项下的义务。

十四、合同生效：

1）本合同在甲乙双方法定代表人或其授权代表签字盖章后生效。

2）合同一式五份。甲方三份，乙方一份，招标代理机构一份。

（以下无正文）

甲方：琼海市中医院（盖章）

法定代表人（授权代表）：

地　　址：

开户银行：

账　　号：

电　　话：

传　　真：

签约日期：2024年8月27日

乙方：海南世纪网安信息技术有限公司（盖章）

法定代表人（授权代表）：

地　　址：海口市龙华区大同路36号华能大厦第六层6B号

开户银行：交通银行股份有限公司海南省分行海口大同支行

账　　号：461601200018150195209

电　　话：0898-66598991

传　　真：0898-68919300

签约日期：2024年8月27日

见证单位：福建泉宏工程管理有限公司（盖章）

法定代表人（授权代表）：

地　　址：海口市美兰区美苑路春江一号小区A1702

电　　话：0898-65347183

传　　真：/

签约日期：2024年8月27日

附件1：

开标一览表

项目名称：2024年琼海市中医院等级保护及安全服务、琼海市中医院业务桌面一致性管控平台采购项目、国家传染病智能监测预警系统前置服务器采购项目

标包名称：A包，2024年琼海市中医院等级保护及安全服务

项目编号：FJQH-2024-019

服务内容	合同履行期限	报　价(人民币/元)	备注
（1）网络安全等级保护测评服务 （2）应急演练服务 （3）网络安全培训服务 （4）内网威胁分析服务	自用户通知进场起60个工作日内	大写：人民币叁拾柒万贰仟元整 小写：￥372000.00元	项目工期：等级保护测评服务将在医院通知入场60日内完成所有测评服务工作，其他安全服务工作在签订合同起一年内根据医院实际需求开展相应安全服务。 项目地点：琼海市中医院。

附件2：

分项报价明细

项目名称：2024年琼海市中医院等级保护及安全服务、琼海市中医院业务桌面一致性管控平台采购项目、国家传染病智能监测预警系统前置服务器采购项目

标包名称：A包，2024年琼海市中医院等级保护及安全服务

项目编号：FJQH-2024-019

序号	项目名称	项目内容	单价（元）	数量	单位	小计(元)
1	医疗信息集成平台（三级）等保测评服务	三级系统的服务内容包括:安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个方面的安全测评。3级测评内容有71个控制点、211个要求项	¥68600.00	1	项	¥68600.00
2	HIS系统（三级）等保测评服务		¥68600.00	1	项	¥68600.00
3	互联网医院管理系统（三级）等保测评服务		¥68600.00	1	项	¥68600.00
4	琼海中医院网站系统（二级）等保测评服务	二级系统的服务内容包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个方面的安全测评。2级测评内容有68个控制点、135个要求项	¥43000.00	1	项	¥43000.00
5	PACS系统（二级）		¥43000.00	1	项	¥43000.00
6	应急演练服务	根据国家法律法规要求，针对医院开展一次网络安全事件应急演练，应急演练以演示或者模拟环境的形式，以通信故障、系统安全、软硬件故障几大类进行编制再结合医院场景定制，并根据医院信息系统的实际情况，指导医院建立健全信息与网络安全	¥36200.00	1	次	¥36200.00

		事件应急响应工作机制，并对信息系统相关人员进行应急预案、应急技巧及对典型的网络安全事件进行预防等方面的培训。				
7	网络安全培训服务	组织全院员工开展一次线下网络安全培训，邀请具有丰富网络安全经验和教学经验的专家担任培训讲师，根据医院情况制定培训内容，内 容包括但不限于：网络安全意识培训、网络安全技能培训、网络安全等级保护测评培训、商用密码应用安全性评估培训、数据安全培训，以及定向网络安全专项培训等。	¥4000.00	1	次	¥4000.00
8	内网威胁分析服务	在医院内网部署先进的威胁分析设备，结合专业的人工分析手段，对医院内部网络的主机、应用系统和终端设备进行全面而深入的安全检测。服务内容包括：高级持续性威胁（APT）分析、数据分析、木马分析以及蠕虫分析等，旨在准确识别并评估内网中可能存在的各类安全威胁，如APT攻击、木马蠕虫、恶意文件、后门等。	¥40000.00	1	次	¥40000.00
9	合计					¥372000.00 元

附件3：

中标通知书

成交通知书

项目编号：FJQH-2024-019

海南世纪网安信息技术有限公司：

贵方于2024年08月06日参加2024年琼海市中医院等级保护及安全服务、琼海市中医院业务桌面一致性管控平台采购项目、国家传染病智能监测预警系统前置服务器采购项目的投标，经评委会全体成员评定和媒体公示，确定贵方为本项目的成交人，现将成交结果通知如下：

采购单位：琼海市中医院

项目名称：2024年琼海市中医院等级保护及安全服务、琼海市中医院业务桌面一致性管控平台采购项目、国家传染病智能监测预警系统前置服务器采购项目

项目编号：FJQH-2024-019

标包名称：A包

成交单位：海南世纪网安信息技术有限公司

成交金额：¥372000.00 元（人民币叁拾柒万贰仟元整）

请于成交通知书下发之日起30天内，持本通知书，与采购单位签订采购合同。

招标代理机构：（盖章）

法定代表人或委托代理人（签字或盖章）

2024年 8月8日

附件4：

网络安全等级测评与评估机构服务认证证书

DJCP

网络安全等级测评与检测评估机构

服务认证证书

证书编号： SC202127130010173

兹 证 明

海南世纪网安信息技术有限公司

统一单位信用代码： 914601003240712191

网络安全等级测评与检测评估服务

符合 TRIMPS-SC13-001:2021《网络安全等级测评与检测评估机构 服务认证实施规则》的要求。

注册地址：海南省海口市龙华区大同路36号华能大厦第六层6B号

办公地址：海南省海口市龙华区大同路36号华能大厦6层

首次颁证日期：2021年11月18日

颁证日期： 2023年12月08日 有效期至： 2024年11月17日

在一个监督周期内，本证书必须与本机构监督评价合格后签发的证书保持通知书合并使用方可有效。

签发人：

公安部第三研究所

证书有效性查询：www.cncagov.cn; www.trimps.net.cn; http://www.djbh.net 地址：上海市普陀路76号 电话：021-64318599; 021-64337892

附件5：

服务方案

1.等级保护测评服务

1.1 服务对象

包括但不限于以下系统：

序号	系统名称	安全等级	部署位置
1	医疗信息集成平台	三级	琼海市中医院本地机房
2	HIS 系统	三级	琼海市中医院本地机房
3	互联网医院管理系统	三级	琼海市中医院本地机房
4	琼海中医院网站系统	二级	
5	PACS 系统	二级	琼海市中医院本地机房

1.2 测评内容

等级测评主要分为两步开展实施。第一步，对信息系统进行定级和备案工作。第二步，对已经定级备案的系统进行十个安全层面的等级保护安全测评（包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个层面）。

其中安全测评分为差距测评和最终测评。差距测评主要针对已定级备案系统执行国家标准的安全测评，差距测评交付差距测评报告以及差距测评整改建议；差距整改完毕后，进行最终测评，最终测评将按照国家标准和国家公安承认的测评要求、测评过程、测评报告，对已定级备案的系统执行系统安全最终测评，最终测评交付具有国家承认的最终测评报告。

信息系统安全等级保护测评包括两个方面的内容：一是安全控制测评，主要测评信息安全等级保护要求的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体安全测评的基础。

1.3 测评流程

1.3.1 测评准备活动

测评准备活动包括：项目启动、信息收集和分析、工具和表单准备三项任务。在测评准备活动中，测评机构主要完成：1）启动测评项目，组建测评项目组；2）通过收集和分析被测系统的相关资料信息，掌握被测系统的大体情况；3）并准备测评工具和表单等测评所需的相关资料，为编制测评方案打下良好的基础。

项目内容	工作内容	输出成果
项目启动	1.组建测评项目组	向医院提交《项目计划书》、《提供资料清单》
	2.编制《项目计划书》	
	3.确定测评委托单位应提供的	
信息收集分析	定级报告分析	《系统基本情况分析报告》
	1.整理调查表单	
	2.发放调查表单给测评委托单	
	3.协助测评委托单位填写调查	
	4.收回调查结果	
	5.分析调查结查	
工具和表单准备	1.调试测评工具	确定测评工具（测评工具清单）、《现场测评授权书》、《测评结果记录表》、《文档
	2.模拟被测系统搭建测评环境	
	3.模拟测评	
	4.准备打印表单	

1.4 方案编制活动

方案编制活动包括：测评对象确定和测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发和测评方案编制四项任务。在方案编制活动中，测评机构主要完成确定测评对象和测评指标，选择测评工具接入点，从而进一步确定测评实施内容，并从已有的测评指导书中选择本次需要用到的测评指导书或开发相应的测评指导书，最后根据上述情况编制测评实施方案。

工作内容	工作详细任务	输出成果
一、测评对象确认	识别被测系统等级 识别被测系统的整体结构 识别被测系统的边界 识别被测系统的网络区域 识别被测系统的重要节点和业务应用 确定测评对象	《测评方案》的测评对象部分
二、测评指标确定	识别被测系统业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	选择对应等级的安全要求作为测评指标	
	就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标	
三、工具测试点确定	确定工具测试的测评对象 选择测试路径 确定测试工具的接入点	《测评方案》的测试工具接入点部分
四、测试内容确定	识别每个测评对象的测评指标	《测评方案》的单项测评
	识别每个测评对象对应的每个测试指标的	

	测试方法	实施和系统测评实施部分
五、测评指导书开发	从已有的测评指导书中选择与测评对象对应的手册	《测评方案》的测评实施手册部分
	针对没有现成测评指导书的测评对象，开发新的测评指导书	
六、测评方案编制	描述测评项目基本情况和工作依据	向医院提交《测评方案》
	描述被测系统的整体结构、边界和网络区域	
	描述被测系统的重要节点和业务应用	
	描述测评指标	
	描述测评对象	
	描述测评内容和方法	

1.5 现场测评活动

现场测评活动包括：现场测评准备、现场测评和结果记录、结果确认和资料归还三项任务。在现场测评活动中，测评机构首先应与医院就测评方案达成一致意见，并进一步确定测评配合人员，完成测评指导书各项测评内容，获取足够的测评证据。

工作内容	工作详细任务	输出成果
1.现场测评准备	现场测评授权书签署	会议记录、确认的授权委托书、更新后的测评计划和测评方案
	召开现场测评启动会	
	双方确认测评方案	

工作内容	工作详细任务	输出成果
	双方确认配合人员、环境等资源	
	确认信息系统已经备份	
	测评方案、结构记录表格等资料更新	
2.现场测评和结构记录	依据测评指导书实施测评	访谈结果：技术安全和管理安全测评的测评结果记录或录音文档审查结果：管理安全测评的测评结果记录配置检查结果：技术安全测评的网络、主机、应用测评结果记录表格、工具测试结果：技术安全测评的网络、主机、应用测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件实地查看结果：技术安全测评的物理安全和管理安全测评结果记录测评结果确认：现场核查中发现的问题汇总、证据和证据源记录、被测单位的书面认可文件。
	记录测评获取的证据、资料等信息	
	汇总测评记录，如果需要，实施补充测评	
3.结果确认和资料归还	召开现场测评结束会	
	测评委托单位确认测评过程中获取的证据和资料的正确性，并签字认可	
	测评人员归还借阅的各种资料	

1.6 报告编制活动

报告编制活动包括：单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成和测评报告编制六项任务。报告编制活动中，测评人员通过分析现场测评获得的测评证据和资料，判定单项测评结果及单元测评结果，进行整体测评和风险分析，形成等级测评结论，并完成最终的《信息系统等级测评报告》。

工作内容	工作详细任务	输出成果
1.单项测评结果判定	分析测评项所对抗威胁的存在情况	等级测评报告的单项测评结果部分
	分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较	
	综合判定单个测评项的测评结果	
2.单元测评结果判定	汇总每个测评对象在每个测评单元的单项测评结果	等级测评报告的单项测评结果汇总分析部分
	判定每个测评对象的单元测评结果	
3.整体测评	分析不符合和部分符合的测评项与其他测评项（包括单元内、层面间、区域间）之间的关联关系及对结果的影响情况	等级测评报告的系统整体测评分析部分
	分析被测系统整体结构的安全性对结果的影响情况	
4.风险分析	整体测评后的单项测评结果再次汇总	等级测评报告的风险分析部分
	分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性	

工作内容	工作详细任务	输出成果
	分析威胁利用安全问题后造成的影响程度	
	为被测系统面临的风险惊醒赋值	
	评价风险分析结果	
5.等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	等级测评报告的等级测评结论部分
	形成等级测评结论	
6.测评报告编制	概述测评项目情况	等级测评报告 提交医院
	描述被测系统情况	
	描述测评范围和方法	
	描述整体测评情况	
	汇总测评结果	
	描述风险情况	
	给出等级测评结论和整改建议	

1.7 测评成果

等级保护测评服务的成果包括但不限于：

- 《网络安全等级保护测评报告》。

2.应急演练服务

2.1 服务内容

2.1.1 编制应急预案

信息安全事件应急预案包括以下安全事件：

1) 有害程序事件：计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件；

2) 网络攻击事件：拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件；

3) 信息破坏事件：信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件；

4) 信息内容安全事件：违反宪法和法律、行政法规的信息安全事件；针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件；组织串连、煽动集会游行的信息安全事件；其他信息内容安全事件；

5) 设备设施故障：软硬件自身故障、外围保障设施故障、人为破坏事故、和其它设备设施故障。

2.1.2 演练场景设计

网络安全应急演练主要对运行环境安全、网络结构安全、设备运行安全、系统可用性、外界风险因素等各方面进行全面演练，主要覆盖重要信息系统、数据中心、灾备中心等重要基础设施，重要服务商应急保障能力，外部应急协调机制等，做到全面演练和专项演练相结合。

网络安全应急演练场景主要由桌面推演和实战演练两种方式：

（1）桌面推演：桌面推演是指参演人员根据应急预案，利用流程图、计算机模拟、视频会议等辅助手段，针对事先假定的演练情景进行模拟应急决策及现场处置的过程，验证应急预案的有效性，促进相关人员明确应急预案中有关职责，掌握应急流程及应急操作，提高指挥决策和各方协同配合能力。

（2）实战演练：实战演练是指参演人员利用信息系统真实生产环境模拟突发事件场景，完成判断、决策、处置等环节的应急响应过程，检验和提高相关人员的临场组织指挥、应急处置和后勤保障能力。实战演练还可分为指定科目演练和预先不告知科目的演练。

演练场景以可能出现的通讯故障、系统安全、软硬件故障等为重点，结合医院实际情况和关键风险点，将以下应急场景作为依据，设计出具体的应急事件：

1）通讯故障

演练在用户量激增、网络设备故障、通信线路被破坏、网络受到攻击等原因导致通讯中断和拥塞时的应急预案和应急处置方法。

2）系统安全

演练因病毒爆发、网络入侵攻击、篡改网站、中间人劫持等情形下的应急预案和应急处置方法。

3）软硬件故障

演练主要信息系统出现应用故障、数据库故障、存储设备故障、主机硬件故障等的应急预案和应急处置方法。

2.1.3 演练时间安排

网络安全应急演练服务的时间需根据信息部门的要求、现场情况、演练场景布置、时间安排等因素来确定，具体时间安排会在应急演练方案中以列表的形式给出。

2.1.4 应急演练方案

网络安全应急演练方案包含应急演练方案、应急演练脚本两部分，在演练开始前两周提供给信息部门审核和准备。演练方案包含应急演练场景选择、场景部

署方案、演练方法、演练时间安排、参演组织人员、注意事项等内容；演练脚本涵括场景设想、场景对白、处置指南等。

2.2 服务流程

2.2.1 应急演练计划

应急演练计划的工作任务包括梳理应急演练需求、明确应急演练目的、明确应急演练方式、制定应急演练计划等4个任务。

在医院演练需求不明确的情况下，服务人员根据残余风险类型确定应急演练需求。应急演练目的、应急演练方式在实施过程中通常在应急演练方案中体现。

2.2.2 应急演练准备

应急演练准备的工作任务包括成立应急演练组织机构、制定应急演练方案、制定应急演练脚本、准备应急演练环境4个任务。

应急演练组织包括应急演练领导小组、应急演练管理小组、应急演练技术小组、应急演练评估小组、应急响应实施组。

应急演练工作方案内容包括：指导思想、工作原则、演练目的、演练场景、演练时间地点、组织体系及职责、演练流程、其他准备事项、工作要求及有关附件等。应急演练脚本编制要结合应急演练目的、内容和形式。

2.2.3 应急演练实施

应急演练实施阶段的工作任务包括应急演练执行、演练过程与结果记录两个任务。

应急演练开始后，即可按照应急演练方案开展相关活动。具体步骤分为先期处置、现场处置、后期处置三个阶段。前期处置阶段要重点判断网络安全事件等级；现场处置阶段重点要确定网络安全事件应急处理方案；后期处置阶段工作主要是网络安全事件分析和完善网络安全事件应急预案两部分。

应急演练实施过程中，安排专门人员，采用文字、摄影、摄像、录音和工具记录等手段，全程采集应急演练相关资料。

2.2.4 应急演练总结

应急演练总结阶段的工作任务包括演练结果与过程评价、应急演练总结两个任务。应急演练总结主要根据应急演练结果对演练内容和效果做出评价、总结演练发现的问题并提出针对性的应对措施。

2.3 服务成果

本次应急演练服务的成果包括但不限于以下输出：

- 《网络安全应急演练预案》；
- 《网络安全应急演练总结报告》。

3.网络安全培训服务

3.1 培训内容

根据最新的国家法律法规要求和政策要求以及医疗行业相关要求，开展网络安全培训，培训的内容包含等级保护、网络安全意识、网络攻防、商用密码、数据安全等培训内容，以提高所有参训人员的网络安全意识和能力。

3.2 培训流程

在整个培训工作中，培训的流程划分为2个步骤来分别进行，其中包括：培训准备、培训实施。

（1）培训准备

在培训准备环节中，培训讲师提前与信息部门人员进行课题沟通，获取具体的培训需求分析并制定《培训方案和计划》，根据此文档安排课程以及准备环境和教材。同时制作相关宣传小册、编写相关的课件PPT、部署培训展示环境、准备《培训人员签到表》《培训评分表》等文档。

（2）培训实施

做好培训准备工作后，本单位对培训学员下发培训通知，根据选定的时间、地点进行线下培训交流。

3.3、培训成果

本次培训的成果包括但不限于以下输出：

- 《培训签到表》
- 《网络安全培训 PPT》

4.内网威胁分析服务

4.1 服务内容

内网安全威胁分析主要依托于专业设备的自动检测、并辅以人工分析判断，查找出内网中是否存在安全威胁。服务商将专业的内网安全威胁发现设备，部署在医院内网中，经过一段时间的监测及扫描后，根据设备收集到的数据信息及生成的分析结果，再结合人工分析、手工检测的方式，找出内网中存在安全威胁的原因和节点，阻断安全威胁、提取威胁特征、犯罪取证等。

具体服务内容如下：

（1）流量威胁分析

服务商技术人员在医院的网络核心出口处部署内网威胁分析设备，通过数据流量镜像的方式将所有数据引流到分析设备处进行分析，以便发现医院的网络异常流量、病毒木马攻击、异常 C&C 通讯、垃圾钓鱼邮件、其它可疑流量等。

（2）常规安全检查

对医院进行常规安全检查，检查对象包括：服务器、办公终端、Web 应用系统、网络设备等等，检查方式按常规安全检查开展进行，方法包括但不限于：主机登录检查、漏洞扫描、病毒扫描、后门检测、rootkit 检测、异常文件分析提

取、异常进程监测、日志分析等等。

（3）异常样本分析

对分析设备筛选出的异常样本进行沙盒分析和逆向分析，通过对二进制文件、脚本文件、办公文档或者电子邮件的分析，找出可能隐藏在恶意文件中的境内外 IP 地址、网站域名、攻击者特征、攻击行为等信息，从而推断该检查单位是否遭受 APT 攻击或恶意网络攻击。

（4）安全处置

对流量监测或者检查发现的存在较为明显的安全事件进行现场应急处置，包括但不限于以下方法：网络切断、隐患排查、病毒处理、木马查杀、样本提取、日志提取、破坏层度分析等等。

（5）报告编制

对现场设备采集的数据进行记录和分析，输出相应《内网威胁分析报告》。

4.2 服务流程

（1）工具部署

经过深入调研医院网络架构，为确保网络安全，在需要进行威胁分析的关键单位内网核心区域部署镜像端口。随后，将连接专用的威胁分析设备，并将其稳妥地安置在内网环境中，以便实时监控和分析潜在的网络威胁。

（2）数据采集

技术人员已完成威胁分析设备的部署工作。接下来，通过在内网中添加资产信息，该设备将能够启动数据收集流程。此流程至少需要持续2至3周，以确保数据的全面性和准确性。在此期间，技术人员将密切关注数据收集情况，并根据需要进行调整和优化。

（3）威胁分析和处置

技术人员运用专业设备对内网流量与数据实施严密监控与分析，旨在精准识别潜在的恶意流量、文件及程序。一旦发现安全事件，他们将迅速进行溯源，精准定位威胁源头，并与医院紧密协作，采取有效措施消除安全隐患，确保内网环境的安全稳定。

（4）威胁报告编制

根据威胁分析的结果，技术人员编制详尽的《内网威胁分析报告》。报告将详细列举检测到的安全威胁，分析其产生原因和潜在影响，并提出针对性的解决方案和建议。通过这份报告，医院可以全面了解内网安全状况，为制定有效的安全策略提供决策依据。

4.3 服务成果

本次内网威胁分析服务的成果包括但不限于：

- 《内网威胁分析报告》