**一、项目概述**

因近年来信息安全事件频发，为了响应国家对网络安全的号召，拟针对我院当前信息安全防护体系进行全方面的检验工作。实现针对采购人当前基础内网、互联网、数据中心网络等目标为对象第三方攻防演练应急与渗透服务采购。基于上述目标进行一次全面综合性安全检验，实现查漏补缺工作，从而为后期采购人的安全建设与整改工作提供参考依据。

**二、技术服务要求**

1.总体技术要求

通过本项目的成功实施，将达到以下主要目标：

1.1对采购人内网、互联网、数据中心网络存储和服务器等基础设施安全威胁的分析，研究相关应对措施；

1.2对采购人数字化建设威胁源进行监测与处理同时协助采购人完成安全加固，保障业务系统不受网络攻击等引发停摆；

1.3安全加固工作完成后配合采购人完成模拟攻防演练，验证安全加固的效果；

1.4为采购人组织一次安全意识和攻防能力评估，根据安全意识评估结果，为采购人信息部门员工提供信息安全培训。

2.主要服务内容：

2.1以服务采购方式由第三方服务投标人提供工具和服务：对采购人数据中心基于威胁建模、行为分析技术，对全院数据流量进行检测，引入多种数据源分析；基于大数据分析和威胁情报共享技术提供全网安全威胁分析处置和安全加固服务；

2.2根据采购人当前的信息安全建设现状开展信息安全攻防演练，涉及资产评估，风险评估，渗透测试，安全整改加固，大型重保期间的驻场运维。具体要求如下：

**（1）全网潜伏安全威胁分析和安全加固**

在采购人数据中心部署全流量分析平台，在核心交换层与内部安全域部署潜伏威胁探针，通过网络流量镜像在内部对用户到业务资产、业务的访问关系进行识别，基于捕捉到的网络流量对内部进行初步的攻击识别、违规行为检测与内网异常行为识别。具体要求如下：

| 工作分类 | 分项工作 | 内容说明 |
| --- | --- | --- |
| 安全威胁分析 | 1）恶意病毒感染分析 | 通过工具发现网络或者系统遭受病毒木马威胁，通过识别病毒特征、找出路径、定位感染文件和感染范围，确定病毒感染真实存在，验证失陷主机真实存在。 |
| 2）明文传输和弱口令分析 | 通过抓包分析和逐条登录验证等方式，确认该类弱点是否真实存在，并依据登录网络环境判断是否存在威胁和风险。 |
| 3）网络攻击分析 | 网络攻击验证，包含内网攻击验证和外网攻击验证。内网攻击方面像SMB内网爆破等。该类攻击产生特点有：因网络延迟、账户密码错误、错误策略配置、权限配置不当和信息系统请求协议或方式不规范等。验证主要内容包括，暴力破解验证、木马攻击验证、邮件威胁验证、文件威胁验证和风险访问验证等。外网攻击验证主要分析互联网APT威胁。 |
| 4）业务风险分析 | 主要针对开放高危端口验证和高危行为画像验证等。开放端口验证又分为互联网开放端口验证和内网开放端口验证。行为画像验证，主要验证网络请求行为的时间、方式、请求过程和结果等方面，验证该行为是否为高危行为。 |
| 5）安全威胁分析 | 结合以上威胁分析工具给出信息，整体安全分析业务面临的外部威胁和内部弱点。 |
| 安全事件溯源 | 1）病毒木马溯源 | 依据用户系统弱点、网络拓扑结构和业务流情况，结合数据请求方式和内容，通过工具给出的信息，找出病毒创建时间、感染时间、传播路径等信息分析出病毒木马最早入侵原因。 |
| 2）内部网络攻击溯源 | 内网攻击分析溯源过程中，依据威胁分析工具、标准化操作流程和专家工作经验，真实溯源事件过程。在分析前需了解用户网络拓扑图、安全架构、业务数据流和数据访问流等。分析内网攻击行为原因（人为、系统请求和主机异常等），逐项分析，定位攻击源、攻击行为、攻击路径和攻击目的。 |
| 3）互联网攻击溯源 | 基于大数据分析平台，结合过往经验，外部攻击给出定性说明，如APT攻击、合规安全检测、僵尸网络攻击、肉鸡攻击、恶意扫描嗅探、黑客渗透和“小白学习”等 |
| 已发现安全事件处置 | 1）病毒事件处置工具查杀 | 通过工具快速查杀网络、主机及信息系统感染病毒，并通知用户重启设备 |
| 2）病毒事件处置人工查杀 | 一些新型病毒，杀毒工具尚未更新或其他需要，安全工程师会通过查看进程、监听端口、定位路径的方式找到怀疑文件，查看文件创建时间、配置文件和运行日志确定是否为病毒，保存记录，用户确认后清除的方式进行病毒查杀。 |
| 3）网络攻击事件处置 | 网络攻击处置分为互联网攻击处置和内网攻击处置。互联网攻击处置，溯源攻击是通过防火墙关闭对外高危端口或对恶意攻击IP黑名单模式进行控制和屏蔽的方式，处置外部攻击，降低外部威胁；对必须开放端口，如80端口。给出加固建议，保护对外服务，确保互联网攻击得到处置。对内网络攻击事件处置，通过隔离攻击源、限制访问源地址、限制访问源端口、限制访问流量和访问时间等方式解决内网攻击事件。在整个内网处置过程中，安全工程师找出最佳处置方式，验证方案可行，再作为知识方式传递给用户。 |
| 安全应对措施 | 1）网络架构加固建议 | 依据安全事件溯源分析结果、信息安全合规性要求和用户业务安全需求，给出网络架构加固建议。建议主要包含边界安全建设、边界动态防御、网络安全域划分、网络数据流控制、网络运维区安全、应用系统区和数据区安全的动态防御体系等。建议设计过程中，充分考虑用户的业务需求和发展，设计架构需要满足易运维、易管理、易扩展等方面需求，特别是虚拟化和云化快速发展阶段，还需要保障能利旧和创新等方面内容。 |
| 2）系统架构加固建议 | 根据威胁分析工具，发现信息系统和主机存在SQL注入、跨站脚本编制、未加密登录请求、应用组件版本低、系统未更新补丁和开放高危端口等方面加固。加固方案类型包括，针对弱点处置方案，如：依据安全工具建议处置方案、依据分析工程师经验处置方案和其他专家给出建议方案。 |
| 3）信息安全管理体系加固建议 | 依据国内相关法律法规和国际相关标准，结合用户相关管理体系，为用户提供信息安全管理体系参考文档。 |

**（2）安全运营服务**

投标人应根据采购人的实际情况，组织专家团队为采购人提供完善的安全运营服务。

|  |  |  |
| --- | --- | --- |
| **服务类** | **技术类型** | **内容及要求** |
| 安全运营服务 | 服务内容 | 在重要保障时期，安全运营服务可帮助组织防范网络安全重大风险，遏制网络安全重大事故，全力做好期间网络安全保障工作。  一、服务内容  1、运营成熟度评估  1.1、资产识别与梳理  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。  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，并将信息录入到安全运营平台中进行管理；  1.2、安全现状评估：包含脆弱性、病毒类事件、攻击行为、失陷类事件等安全现状的评估  1.3、问题处置：建立安全事件的进度监控机制，现场T1上门提供首次处置服务。  1.4、运营能力评估  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。  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。  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。  2、持续有效运营  2.1、漏洞管理  漏洞分析与管理：通过漏洞扫描工具识别系统安全漏洞，结合多种信息对识别的漏洞进行优先级排序，最后提出切实可行的漏洞修复指导。同时，借助漏洞跟踪管理平台，可以有效地追踪资产漏洞生命周期，清楚地掌握资产的脆弱性状况，实现漏洞全生命周期的可视、可控和可管。  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。  最新漏洞预警与响应（可选）：梳理重要业务资产的详细信息，形成设备指纹后导入到漏洞管理平台中，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，提供最新漏洞的修复指导。  漏洞协助处置（可选）：输出可行的漏洞处置方案，客户审核通过后，由服务人员协助用户对漏洞进行验证处置工作，并对已修复后的漏洞进行复测，帮助服务使用方将漏洞的影响降到可接受范围内。  2.2、威胁管理  威胁分析与通告：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。  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、攻击类、漏洞利用类、失陷类的安全事件，并提供相应解决方案。  策略管理：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。  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。  2.3、事件管理  事件分析与处置：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。  应急响应：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，同时还原攻击路径，分析入侵事件原因，指导用户进行安全加固、提供整改建议、防止再次入侵。 |

**（3）安全风险评估**

|  |  |  |
| --- | --- | --- |
| **服务类** | **技术类型** | **内容及要求** |
| 安全风险评估 | 服务内容 | 一、服务概述：  服务工程师通过自研工具对组织信息资产面临的威胁、存在的脆弱性、现有防护措施及综合作用而带来风险的发生可能性进行评估，最终提供完整的风险评估报告及修复建议。  二、具体服务内容：  1.资产识别  使用工具对包括：业务系统、服务器、安全设备、网络设备等进行自动化扫描发现、识别、评估，可覆盖所有的资产，根据业务对资产的实际依赖程度区分重要资产，脆弱性识别、威胁识别、风险分析等后期工作将针对重要资产进行识别；  2.脆弱性评估  弱点存在于物理环境、硬件、软件、业务系统等各个方面，这些都可能被各种安全威胁利用来侵害用户的资产，让资产的价值受损。主要工作如下：  漏洞扫描：使用工具的漏洞扫描功能，快速从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全漏洞，并给出关于安全隐患的详细信息；  基线配置核查：使用工具的基线配置核查功能识别信息系统的安全配置情况；  3.威胁评估  分析用户信息系统存在的威胁种类，确定威胁分类的标准；综合威胁来源、种类和其他因素后得出威胁列表；针对每项需要保护的信息资产，尽可能全面的发现资产所面临的威胁；  4.防护能力评估  识别已有的安全控制措施，分析安全措施的有效性，确定威胁利用弱点的实际可能性，指出当前安全措施的不足；  5.风险分析  综合考虑资产本身的价值、威胁发生几率、脆弱性的破坏力、现有防护能力等因素分析资产可能存在的安全风险，结合风险对业务战略的影响程度区别明确风险处置计划；  6.风险评估报告  根据资产识别、脆弱性评估、威胁评估、防护能力评估的输出结果进行风险分析之后，通过工具输出风险评估报告，风险评估报告中为用户提供符合业务需求的安全整改建议。  三、服务交付物  《风险评估报告》 |

★2.3成果要求

**全网潜伏安全威胁分析和安全加固：**本阶段需要提交的文档包括但不限于：《四川省妇幼保健院威胁分析报告》《四川省妇幼保健院安全应对措施整改建议书》。上述正式报告需提供：电子档、纸质文档。其中若涉及到有过程文档、原始数据文档、测试用例文档等相关辅助性文档均提供电子档。

**安全运营服务：**本阶段需要提交的文档包括但不限于：《安全服务运营报告》、《首次威胁分析与处置报告》、《事件分析与处置报告》、《安全通告》、《综合分析报告》。上述正式报告需提供：电子档、纸质文档。其中若涉及到有过程文档、原始数据文档、测试用例文档等相关辅助性文档均提供电子档。

**安全风险评估：**本阶段需要提交的文档包括但不限于：《四川省妇幼保健院风险评估报告》。上述正式报告需提供：电子档、纸质文档。其中若涉及到有过程文档、原始数据文档、测试用例文档等相关辅助性文档均提供电子档。

★2.4保密要求

投标人对过程文档、原始数据文档、测试用例文档、最终成果资料等与本项目有关的所有资料要严格保密，不得以任何形式对第三方泄露。投标人对此提供承诺函，格式自拟。