## 一、技术要求

**1、安全驻场运维服务**

服务要求：合同期内，根据采购人要求，每周提供不少于1个工作日的安全驻场运维服务，且驻场人员不能随意变更，若遇变更情况需取得采购人同意。

服务内容：

（1）安全巡检服务。

每周定期使用多种手段，对网络设备、安全设备、服务器、操作系统、应用系统等进行周期性的状态检查、补丁管理等安全巡检，及时掌握当前网络、系统的威胁状况，修复发现的系统安全隐患或新的安全漏洞。采取有针对性的安全措施，确保IT设备及系统持续保持良好的安全状况，保障系统、设备的安全和高可用性，每周巡检需提交巡检结果报告及安全建议。

（2）安全策略梳理服务。

根据实际需求及相关标准对安全设备的策略进行优化，使安全设备的防护效果达到最佳，同时满足等保及相关法律法规的要求。

（3）安全日志分析服务。

不定期针对日常 IT 运维、网络安全事件、IT 故障等场景，提供分析日志，发现日常安全威胁、快速排查故障、提前解决处理可能发生的安全事件。

（4）资产梳理服务。

通过采用自动化探测工具+人工复核的服务模式，定期对采购人内网的所有存活IP进行识别梳理，不定期提供资产台账及网络拓扑图包括资产类型、操作系统、开放端口、应用类型等信息，并能够实时展示资产的安全风险指数。

（5）网络流量走向梳理服务。对网络中的业务流量走向进行梳理。

（6）日常网络故障协助处理服务。针对日常工作中发现的网络故障进行协助处理。

**2、安全漏洞扫描服务**

服务要求：合同期内，根据采购人需要，每季度提供不少于1次的安全漏洞扫描服务，需提交安全扫描结果报告。

服务内容：为采购人提供包括但不限于网络设备、操作系统、数据库、web应用系统在内的安全漏洞扫描服务，提供主机漏洞台账与报告，并根据漏洞风险等级、漏洞被利用可能性、漏洞加固或规避措施等内容，为采购人单位进行漏洞处置决策提供参考依据。

**3、安全配置核查和安全加固服务**

服务要求：合同期内，根据采购人需要，每季度提供不少于1次的安全配置核查服务，协助相对应的加固，需提交核查结果报告。

服务内容：通过现场人工实施，辅之以安全基线工具，对采购人的网络设备、主机、数据库、中间件等常见应用的安全策略配置进行科学、全面、认真的检查，输出专业的检查报告，分析和修补其中的脆弱性配置，以保障信息系统长期保持在高度可信的安全状态。

**4、网络安全培训服务**

服务要求：合同期内，根据采购人需要，提供不少于1次的网络安全培训服务，协助培训资料整理存档，需提交培训PPT。

服务内容：

1. 安全意识培训：针对目前主流的网上诈骗、个人信息泄露、办公安全意识等进行全面的讲解。需要配套相应的安全攻击过程演示等，保证培训过程中的生动性。
2. 安全技能培训：通过专业网络安全技术人员对采购人情况调研，了解到采购人具体网络安全技能薄弱处，从而对采购人定制化培训课程，提升管理人员的专业能力。

**5、网络安全应急演练服务**

服务要求：合同期内，根据采购人需要，提供不少于1次的网络安全应急演练工作，通过网页挂马、网页篡改、病毒感染、邮件钓鱼等真实事件对采购人的安全性进行实战演练，检测采购人的安全防范意识及应急处置能力。

服务内容：

1. 根据采购人实际情况提供网络安全应急演练方案。
2. 网络安全应急演练过程中提供技术协助进行应急演练。
3. 根据应急演练结果完善采购人网络安全应急预案。

**6、网络安全应急支撑服务**

服务要求：合同期内，根据采购人需要，需在1小时内到现场，进行应急响应支撑工作。

服务内容：发生确切的安全事件时，网络安全技术人员通过现场或非现场等方式进行信息收集工作，详细了解掌握事件发生的始终、现状、可能的影响，对事件进行详细分析，提供事件处理建议，并协助采购人解决此次事件，待事件处理结束后，技术人员整理事件分析、事件处理的过程记录和相关资料进行处置汇报。

**7、安全管理制度服务**

服务内容：合同期内，根据采购人需要，指导并协助采购人完善单位相关信息安全管理制度，并且在日常的网络安全建设、运维中，提供制度落实的相关建议。

**8、信息安全风险评估服务**

服务要求：合同期内，根据采购人工作安排，由采购人指定一个业务系统进行风险评估，评估完成后提供《信息安全风险评估报告》。

服务内容：针对采购人指定的业务系统进行风险评估，从风险管理的角度，系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，为防范和化解信息安全风险，或者将风险控制在可接受的范围，制定有针对性的抵御威胁的防护对策和整改措施。

**9、安全迎检服务**

服务要求：合同期内，根据需求配合采购人做好相关安全检查前期准备工作，配合相应佐证材料整理，配合采购人做好现场检查工作。

服务内容：按照监管部门每年下发的网络安全检查文件要求，配合采购人完成相应检查表格填写和文档准备。

**10、渗透测试服务**

服务要求：合同期内，按照采购人需求，针对外网系统提供不少于2次的应用系统渗透测试服务，并提供渗透测试报告。

服务内容：由具备高技能和经验丰富的安全服务人员发起，并模拟常见黑客所使用的攻击手段对目标系统进行模拟入侵，目的在于充分挖掘和暴露系统的弱点，从而让管理人员了解其系统所面临的威胁。

**11、重保值守服务**

服务要求：合同期内，在重要时期或重要活动时提供重保值守服务。重保值守服务期间提供攻击诱捕与威胁检测系统一套。

服务内容：在重要时期或重要活动期间，提供服务工程师，在采购人核心节点驻守，协助采购人监测、防护网络攻击并进行追踪、取证、溯源分析，及时发现和处置各种网络攻击事件，确保采购人指定信息系统的安全。要求充分利用采购人现有各种安全防护、监测设备，对全部攻击行为进行实时监测，攻击监测数据必须具备实时性、全面性及可视化能力，能够进行攻击者行为审计，必要时进行攻击行为阻断，确保所有攻击行为处于受控状态。

**12、安全通告服务**

服务要求：合同期内，提供不定期的安全通告服务。

服务内容：通告包括安全漏洞（补丁）通告、安全威胁通告、安全业界动态、恶意代码防范、紧急通告等多项内容，同时提供“紧急安全漏洞通告”和“紧急安全威胁通告”。并在第一时间进行相关安全通告的整理并以正式邮件等形式及时告知采购人安全管理人员。

**13、协助信息安全整改服务**

服务要求：合同期内，提供对发现的网络安全问题协助采购人进行整改。

服务内容：针对在日常运维过程中发现的网络安全问题，需要协助采购人相关技术人员进行整改。

**14、安全服务工具**

服务要求：合同期内，提供一套满足安全服务工作的工具供采购人使用，为了防止数据泄露，要求服务工具须本地部署。

服务工具要求：须与原有安全服务工具进行数据对接，无需二次数据采集，服务工具须包含攻击面管理、资产探测及管理、威胁诱捕、主机安全、流量监测等能力，精准发现问题、快速解决问题、有效控制风险，提供上述描述相关能力授权许可。

服务工具授权许可：

1)提供攻击面管理功能授权许可**（响应文件中须提供供应商盖章确认的承诺函证明）；**

2)提供资产探测及管理功能授权许可**（响应文件中须提供响应供应商盖章确认的承诺函证明）**；

3)提供威胁诱捕功能授权许可**（响应文件中须提供响应供应商盖章确认的承诺函证明）**；

4)提供主机安全功能授权许可**（响应文件中须提供响应供应商盖章确认的承诺函证明）**；

5)提供流量监测功能授权许可**（响应文件中须提供响应供应商盖章确认的承诺函证明）**；

6）提供安全服务工具对接承诺函**（响应文件中须提供响应供应商盖章确认的承诺函证明）。**

1. **项目团队**

供应商须为本项目拟派不少于4人的项目团队，其中须包含一名项目经理。

**注：以上“技术要求”为实质性要求，必须完全满足，否则响应无效。**