网络安全服务项目项目需求和有关说明

本项目为惠山区人民法院的网络安全服务项目，具体要求如下，供应商须提供满足以下要求的服务，不得有负偏离：

**一、项目概况**

本次建设内容包括：为惠山区人民法院提供网络安全服务

**二、服务清单**

|  |  |  |
| --- | --- | --- |
| **网络安全服务清单** | | |
| 序号 | 项目 | 服务频次 |
| 1 | 资产发现与梳理 | 服务期内1次 |
| 2 | 漏洞扫描 | 1月1次 |
| 3 | 安全巡检 | 1月1次 |
| 4 | 迎检协助 | 服务期内2次 |
| 5 | 应急响应 | 服务期内2次 |
| 6 | 安全管理体系完善 | 服务期内 1次 |
| 7 | 安全培训 | 服务期内1次 |
| 8 | 安全咨询 | 服务期内1次 |
| 9 | IT资产摸排 | 服务期内1次 |
| 10 | 安全态势感知 | 服务期 |

**三、商务要求**

**1、服务内容：**

1.1资产发现与梳理服务

针对需求IP进行全端口扫描，发现开放的端口、端口运行的服务、服务承载的组件等信息。

交付内容：《信息资产登记表》

1.2漏洞扫描服务

综合运用多种最新的漏洞扫描与检测技术，快速发现网络资产，准确识别资产属性、全面扫描安全漏洞，从海量数据快速定位风险，清晰定性安全风险，以及定位Web应用漏洞并给出修复建议和预防措施，对风险控制策略进行有效审核，帮助甲方在弱点全面评估的基础上实现安全自主掌控，并输出扫描报告。

交付内容：《漏洞扫描报告》

1.3安全巡检服务

由专业安全工程师定期针对服务器、数据库、网络设备和安全设备，进行策略的合理性和有效性检查，并对日志进行审计分析，记录保存检查和审计结果，并生成相应报告。

交付内容：《安全巡检报告》

1.4迎检协助服务

当国家、行业、上级、网安、网信等网络安全监管部门针对信息系统的安全检查时，协助解读检查文件，并针对文件中的检查项协助甲方自查和填报，完成各项检查，并配合甲方完成网信办或上级法院组织的攻防演练等。

交付内容：《安全自查报告》、《需反馈的安全检查文件》

1.5应急响应服务

应急响应服务提供入侵原因分析、业务损失评估、黑客溯源取证等安全服务，包含发生安全事件后的应急响应活动。10分钟内远程响应，如需现场处置，2小时内到现场。

交付内容：《应急响应服务报告》

1.6安全管理体系完善

根据甲方现状，对规章制度和管理体系进行完善。

交付内容：《安全管理体系文件》

1.7安全培训

根据甲方要求，进行安全意识、法律法规等方面的培训。

交付内容：培训内容相关课件

1.8安全咨询

当甲方遇到通报或漏洞需要整改时，提供咨询服务，指导修复（具体修复操作由系统运维商进行）。

交付内容：《XX系统安全修复建议》

1.9IT资产摸排

针对甲方内网服务器、应用，网络设备、安全设备等资产进行发现并协助梳理，完成后提供拓扑。

交付内容：《XX系统拓扑》

1.10安全态势感知

采集终端的静态和动态信息，包括软硬件资产信息、安全合规信息及运行信息，以数据为抓手，以攻击者视角看安全，实现对已知和未知威胁的防护和分析。

安全态势感知组成模块：

1. 安全运营：

包含安全运营工作相关的各类模块和管理功能，提供从安全态势、安全事件分析、溯源分析、响应处置的安全一站式工作平台。安全态势展示当前系统的全局安全状况；安全事件管理方便安全团队分析和处置威胁攻击；可视化BI分析和溯源取证帮助安全分析师找到威胁根源；响应预案SOAR 可对威胁进行自动化快速处置；智能仪表盘和自动化报告让安全团队及时掌握安全详情。

1. 大数据分析与处理：

大数据分析与处理模块包含数据采集、数据解析、数据标准化、数据丰富化、数据存储、数据检索与计算等功能。实现全量数据的集中采集、处理、存储、查询、分析，为上层模块提供数据检测与处理的基础。

大数据分析与处理模块拥有多类强大的数据分析引擎，可进行多源数据关联分析，实时数据分析和历史数据分析，可基于预置规则关联情报、资产分析生成相关安全告警。

大数据分析与处理采用分布式存储架构，可实现对海量数据的全量存储备份和平滑的数据扩容，成本低效率高。

态势感知平台能够对采集的探针数据、样本数据进行检测分析。通过各种检测分析技术，对海量多异构数据进行分析，确保各类威胁全面可视。

1. 探针以及第三方安全设备的分析：

态势感知服务可通过流量威胁检测探针，负责收集打点数据，送给后端，为后续的检测分析提供原始数据。同时也可分析各类第三方传统安全设备与系统，增强安全数据的多样化和安全数据对威胁的覆盖度。

安全态势感知服务效果：

1）多元异构数据采集、全视角分析

实现对各类第三方安全系统/设备的快速数据采集，利用统一的安全数据模型，可将多维度数据以统一、标准的方式进行处理和存储，使得安全人员可以全方位、全视角分析和处置恶意攻击。

2）整体协防、全局联动

有覆盖全球的网络神经元实时监控全网攻击，安全专家持续跟踪分析攻击团队和新型攻击事件，产出威胁情报和检测规则，并下发到本地态势感知一体机，一旦发现有新型恶意攻击，可瞬时部署到各个端点，实现全局联动、整体防御。

3）专家服务、高效运营

态势感知服务除了数据、工具、流程，还应提供专业的安全人员，依托于业内顶尖的安全专家，提供远程安全运营托管服务，可帮助客户进行安全事件的分析、研判、处置等工作，降低客户安全团队在技术、经验上的风险，提升安全运营的效率和效果。

交付内容：《安全态势报告》

**2、服务地点：**采购人指定地点

**3、服务期限：**维保期限从中标之日起至2023年12月31日。

**4、报价说明**

（1）报价应包含与本次采购项目有关的所有费用。同时，还应包含支付给员工的工资和国家强制缴纳的各种社会保障资金，以及供应商认为需要的其他费用等。

（2）供应商的任何错漏、优惠、竞争性报价不得作为减轻责任、减少服务、增加收费、降低服务质量的理由。

（3）供应商应入选“2023年度无锡市网络和数据安全技术支撑单位”。

**5、验收标准：**采购人根据国家有关规定、响应文件以及合同约定的内容

**6、付款方式：**项目验收合格，收到发票后支付中标金额的50%，服务期最后1个月支付50%。