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**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务**  **类型** | **描述** | **数量** | **单位** |
| 1 | 资产发现与梳理服务 | 针对所有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 | 1 | 次 |
| 2 | 漏洞扫描服务 | 1、综合运用多种最新的漏洞扫描与检测技术，能够快速发现网络资产，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，从而帮助用户在弱点全面评估的基础上实现安全自主掌控。2、输出检测报告 | 12 | 次 |
| 3 | APP检测测服务 | 提供开发中、上线前、运行中全生命周期安全检测，提供代码安全检测、配置安全检测等七个方面对终端产品进行专业、安全、高效的一站式检测，保障行业终端安全。 | 上限30次 | 次 |
| 4 | 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。 | 12 | 次 |
| 5 | 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。 | 6 | 次 |
| 6 | 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。 | 4 | 次 |
| 7 | 安全管理体系完善 | 根据客户现状，对规章制度和管理体系进行完善 | 1 | 次 |
| 8 | 安全培训 | 根据客户要求，进行安全意识、法律法规等方面的培训 | 1 | 次 |
| 9 | 安全咨询 | 当用户遇到通报或漏洞需要整改时，提供咨询服务，指导修复（具体修复操作需要系统运维商进行） | 不限 | 次 |
| 10 | IT资产摸排 | 针对客户内网服务器、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 | 1 | 次 |
| 11 | 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，对已知和未知威胁的防护和分析。 | 12 | 次 |

**三、商务要求**

**1、服务内容：**

### 1.1 资产发现与梳理服务

﻿资产梳理服务是指使用多种手段，发现包括服务器、数据库、中间件、网络设备等资产，并通过信息补全和深度扫描等方式完成资产属性的补全，最终实现未知资产的发现与管理。

服务方式：

资产梳理服务的服务方式为：

|  |  |  |
| --- | --- | --- |
| 服务方式 | 服务描述 | 服务特点 |
| 远程实施 | 无需场地、可对企业外网资产或通过跳板方式对内网资产等进行盘点 | 方便快捷 |
| 现场实施 | 在现场对内网资产/外网资产等进行盘点 | 全面覆盖 |
| 现场+远程实施 | 现场对内网资产、远程对外网资产等进行盘点 | 灵活性高 |

资产梳理服务所需服务资源有：

|  |  |  |
| --- | --- | --- |
| 人力 | 平台 | 工具 |
| 工程师 | 资产收集平台 | 空间测绘平台 |
| 资产梳理 |
| 其他工具 |

服务内容：

﻿对信息化资产设备进行梳理，给出建设资产安全管理的优化建议，重新登记为《信息资产登记表》

服务交付：

资产盘点服务各阶段服务交付物清单：《信息资产登记表》

### 1.2 漏洞扫描服务及APP检测服务

漏洞扫描服务（包含APP检测）是通过使用漏洞扫描器及其他开源漏洞检查工具，对操作系统、网络设备、安全设备、IoT 设备、中间件、Web 应用及APP、小程序等类型 IT 资产进行漏洞扫描的自动化的检测工作，发现现存的安全漏洞。该服务适用于快速批量查找主流安全漏洞，快速定位漏洞问题，保障行业终端安全。

服务方式：

漏洞扫描服务的服务方式为：

|  |  |  |
| --- | --- | --- |
| 服务方式 | 服务描述 | 服务特点 |
| 远程实施 | 不限制场地、可对企业外网资产进行漏洞扫描，通过跳板方式对内网资产进行漏洞扫描 | 方便快捷 |
| 现场实施 | 在现场对内网/外网资产进行漏洞扫描 | 全面覆盖 |
| 现场+远程实施 | 现场对内网资产进行漏洞扫描  远程对外网资产进行漏洞扫描 | 灵活性高 |

漏洞扫描服务所需服务资源有：

|  |  |  |
| --- | --- | --- |
| 人力 | 平台 | 工具 |
| 工程 | 中台支撑 | 漏洞扫描工具 |
| 其他工具 |

服务内容：

|  |  |  |
| --- | --- | --- |
| 服务人员 | 服务标准 | 服务内容 |
| 工程师 | 主机：一人天 20 台终端或服务器  应用：一人天 20 个网站（二级域名） | 1、前期沟通  2、漏洞扫描  3、漏洞修复  4、漏洞复测  5、交付报告 |

漏洞扫描，单次服务标准为：20 台终端或服务器或 20 个网站（二级域名）。需初级服务人员 1 名，为期 1 天。

前期沟通，实施服务人员，到达客户现场后，基于获取的项目信息，与客户侧项目对接人，进行需求确认。确认内容包含：

1）扫描范围 ：

2）扫描实施的时间

3）设备接入点

4）IP 地址的预留

5）配合人员

6）扫描 IP 的加白

7）扫描条件

漏洞扫描，根据客户提供的信息对操作系统、WEB 应用、中间件、网络设备、安全设备等 IT 资产进行漏洞扫描，漏洞扫描的测试范围包含：

|  |  |  |
| --- | --- | --- |
| 漏洞类型 | 威胁级别 | 具体漏洞 |
| 认证和授权类 | 高危 | 任意文件下载 |
| 越权访问 |
| 弱口令 |
| 账户管理不规范 |
| 文件上传 |
| 中危 | 用户名可枚举 |
| 暴力攻击 |
| 会话标识未更新 |
| 未授权访问 |
| 脆弱的SSL加密算法 |
| 会话令牌不应写入URL |
| 密码明文传输 |
| 验证码漏洞 |
| 低危 | 脆弱的加密方式 |
| 会话重放攻击 |
| 命令执行类 | 高危 | Struts2远程命令执行 |
| JBOSS远程命令执行 |
| HTTP.sys远程命令执行 |
| 文件包含 |
| tnftpftp客户端命令执行 |
| HP Data Protector 命令执行 |
| GNU Bash 命令执行 |
| Elasticsearch 命令执行 |
| 各类反序列化 |
| 命令执行 |
| 逻辑攻击类 | 高危 | 支付绕过 |
| 密码找回 |
| 任意密码登陆 |
| 绕过统一认证平台 |
| 中危 | 并发漏洞 |
| 低危 | 慢速HTTP攻击 |
| 短信攻击 |
| 邮件攻击 |
| 批量注册 |
| 注入类攻击 | 高危 | SQL注入 |
| XML注入 |
| XPATH注入 |
| 命令注入 |
| 服务器模板注入（SSTI） |
| 中危 | CRLF注入 |
| XFF注入 |
| 链接或框架注入 |
| JSON劫持注入 |
| 客户端攻击类 | 高危 | XSS |
| 中危 | CSRF |
| 服务端攻击类 | 高危 | WebServer Expect 头 XSS |
| 应用服务未授权访问 |
| 中危 | 数据明文传输 |
| 拒绝服务 |
| 低危 | 使用低版本应用服务 |
| 信息泄漏类 | 高危 | git泄漏 |
| svn泄漏 |
| 中危 | web服务器控制台泄漏 |
| Phpinfo()信息泄漏 |
| 目录遍历 |
| IIS短文件名泄漏 |
| HTML 注释敏感信息泄露 |
| 安装或示例页面未删除 |
| Cookie信息泄漏 |
| 低危 | Cookie缺少安全属性 |
| 敏感信息泄漏 |
| 异常信息泄漏 |
| 内网IP地址泄漏 |
| MS系列漏洞 | 高危 | 所有MS系列 |
| 其他 | 高危 | PHP multipart/form-data 远程 DOS 漏洞 |
| ASP.NET Padding Oracle 攻击 |
| SSRF |
| Web服务器解析漏洞 |
| Unicode编码转换漏洞 |
| SMB会话可获取远程共享列表 |
| Oracle Database Server 'TNS Listener'远程数据投毒 |
| Openssl 心脏滴血漏洞 |
| Linux Glibc GHOST 幽灵 |
| ssh用户名暴力枚举 |

最后对有疑问点和对可能造成数据变动的漏洞，进行人工手动验证。漏洞修复，包含以下几点：

1）对扫描出的漏洞，提供漏洞修复报告。

2）对企业修复人员，提出的问题进行解惑。

漏洞复测，在客户侧漏洞修复完毕之后对以下内容进行漏洞复测，包含：

1）操作系统方面。

2）Web 应用。

3）中间件。

4）网络设备、安全设备、Iot 设备等进行漏洞复测。

交付报告，所有漏洞修复完毕之后提供整体漏洞扫描报告，包含：

1）整体漏洞情况。

2）漏洞修复建议。

服务交付：

漏洞扫描服务各阶段服务交付物清单：《漏洞扫描及处理报告》

### 1.3安全巡检服务

服务方式：

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。

服务内容：

以环境稳定性、安全性为目标针对法院网络进行深入、严谨的日常性评估，对网络中存在的能在现有条件下排除的风险进行处理，并提供可视化报告和统计的一种服务。

日志分析：收集日志信息，并根据安全动态结合安全工程师的安全经验，分析指定设备的特定时间的日志信息，发现面临的安全风险，并提出建议。

策略优化：对安全设备进行策略检查，并根据检查结果提供改进建议；

状态检查：检查设备硬件和软件的运行状况。

隐患排除：对排查结果中存在的隐患（病毒、木马等）甄别风险并进行处理，及时排除。

服务交付：

安全巡检服务各阶段服务交付物清单：《安全巡检报告》。

### 1.4迎检协助服务

服务方式：

迎检协助服务的服务方式为：

|  |  |
| --- | --- |
| 服务方式 | 服务描述 |
| 远程 | 互联网或远程控制对安全事件进行迎检协助 |
| 现场 | 客户现场直接对安全事件进行迎检协助 |

迎检协助服务所需服务资源有：

|  |  |
| --- | --- |
| 人力 | 支持 |
| 中级工程师 | 应急响应工具 |
| 日志审计工具 |
| 攻击溯源 |
| 其他工具 |

服务内容：

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。

服务交付：

迎检协助服务各阶段服务交付物清单如下：《安全自查报告》、《需反馈的安全检查文件》

### 1.5应急响应服务

服务方式：

应急响应服务的服务方式为：

|  |  |  |
| --- | --- | --- |
| 服务方式 | 服务描述 | 服务特点 |
| 远程 | 互联网或远程控制对安全事件进行应急响应 | 方便快捷 |
| 现场 | 客户现场直接对安全事件进行应急响应 | 效果较好 |
| 单次 | 针对单次安全事件提供实时应急响应服 | 效果较好 |

应急响应服务所需服务资源有：

|  |  |
| --- | --- |
| 人力 | 支持 |
| 中级工程师 | 应急响应工具 |
| 日志审计工具 |
| 攻击溯源 |
| 其他工具 |

服务内容：

在发生确切的安全事件时，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，协助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，提出基于安全事件的整体安全解决方案，排除系统安全风险并协助追查事件来源、协助后续处置。

服务交付：

应急响应服务各阶段服务交付物清单：《应急响应服务报告》

### 1.6安全管理体系完善服务

服务方式：

安全管理体系完善的服务方式为：

|  |  |
| --- | --- |
| 服务方式 | 服务描述 |
| 现场 | 现场调研现有管理制度，与安全负责人进行访谈 |
| 远程 | 根据调研结果进行安全管理体系完善 |

服务内容：

为落实网络安全主管机关对于各部门网络安全的工作要求，同时根据实际存在的安全制度，通过专业高效的安全管理体系完善服务，准确定位整体安全需求，为安全体系完善确定科学依据。在安全现状和需求的基础上，明确信息安全建设目标，基于的信息安全现状、需求分析结果，参考国内外信息安全体系模型，在明确用户信息安全建设目标的前提下，建立符合用户的信息安全保障体系框架，针对各子体系模块进行详细设计，遵循整理和建设相结合、先易后难、兼顾工作量在各阶段的平衡分配的原则，协助用户完善安全管理体系建设。

服务交付：

安全管理体系完善服务交付物清单：《安全管理体系文件》

### 1.7安全培训服务

安全培训服务根据客户不同的培训需求，针对不同的培训对象，推出安全意识培训等培训。

安全培训服务的服务对象，以及被服务对象的收益，如下所示：

|  |  |
| --- | --- |
| 服务对象 | 企业收益 |
| 所有团体 | 人员：管理/攻击/防守能力、安全意识水平得到提升等 |
| 单位：整体防护体系得到加强 |

服务方式：

依据客户需求，培训服务方式如下：

|  |  |  |
| --- | --- | --- |
| 服务方式 | 服务描述 | 服务特点 |
| 远程培训 | 无需场地、可覆盖企业/团体所有员工 | 覆盖全员 |
| 现场培训 | 面团体特定群体进行 | 效果较好 |

安全培训服务相关服务资源有：

|  |  |
| --- | --- |
| 人力 | 教材 |
| 中级工程师 | 相关培训教材 |
| 高级工程师 |

服务内容：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 课程及师资 | 服务标准 | 服务内容及日程安排 | | 教材 |
| 上午 | 下午 |
| 常规安全意识培训1-2人（中级） | 次 | 1、签到  2、安全形式与法律法规  3、个人安全  4、企业安全  5、社会工程学防范 | 1、漏洞攻击演示  2、恶意链接钓鱼演示  3、恶意文件钓鱼演示  4、安全意识培训总结 | 培训 PPT |

安全意识培训，师资为1-2人，服务按次计算，通常一次服务时间为1天。常规安全意识培训，配备师资为：中级服务工程师，服务方式有：远程、现场、现场+远程三种。服务内容及日常安排为：

上午，PPT宣讲：

1) 签到。包含：部门、姓名、联系电话等。

2) 安全形式、法律法规。日常培训，安全形式介绍依托于近期网络安全事件；重大保障培训，安全形式介绍依托于历届活动总结。

3) 个人安全。从设备、口令、行为习惯等方面展开。如：个人终端，长期不更新补丁，存在永恒之蓝漏洞；使用类似111111的弱口令；习惯性在终端不加密记录重要业务说明、账户密码。

4) 单位安全。包含：APT攻击、勒索病毒、挖矿木马、源码泄露等风险场景介绍。

5) 社会工程学防范。包含：邮件钓鱼、网页钓鱼、社工平台钓鱼、二维码钓鱼、WIFI钓鱼、BadUSB钓鱼、近源攻击等场景。

服务交付：

安全培训服务服务交付物清单如下：

|  |  |
| --- | --- |
| 服务项目 | 交付物 |
| 前期沟通 | 培训内容确认单 |
| 培训准备 | 授课人员信息 |
| 培训内容相关课件 |
| 培训实施 | 签到信息记录 |

### 1.8安全咨询服务

服务方式：

安全咨询的服务方式为：

|  |  |
| --- | --- |
| 服务方式 | 服务描述 |
| 远程 | 根据漏洞或攻击利用情况进行修复指导 |

服务内容：

当用户遇到通报或漏洞需要整改时，由专业工程师分析服务器、终端、数据库及应用中间件等存在的安全漏洞，提出打补丁、强化帐号安全、修改安全配置、优化访问控制策略、增加安全机制等安全建议并指导修复，提高系统健壮性和安全性。

服务交付；

安全咨询服务交付物清单：《XX系统安全修复建议》

### 1.9 IT资产摸排服务

服务方式：

IT资产摸排的服务方式为：

|  |  |
| --- | --- |
| 服务方式 | 服务描述 |
| 现场 | 现场进行现有情况调研、机房设备清点等工作 |
| 远程 | 根据现场情况进行拓扑图完善、资产梳理等工作 |

服务内容：

针对客户内网服务器、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。

服务交付：

IT资产摸排服务交付物清单：《XX系统拓扑》

### 1.10 安全感知

服务方式：

安全感知的服务方式为：

|  |  |
| --- | --- |
| 服务方式 | 服务描述 |
| 现场 | 提供实时监测和预警，通过不断收集、分析和评估各种安全事件和威胁情报，以及对用户环境进行实时监测，提供及时的警报和通知。 |

服务内容：

实时监测：持续监测用户的网络、系统和应用程序，收集和记录各种安全事件和活动，包括登录尝试、异常流量、恶意软件等。

威胁情报搜集与分析：从多个来源获取威胁情报，包括公开的漏洞披露、黑客论坛、恶意软件样本等，并对其进行分析和评估，以确定对用户环境的潜在威胁。

异常行为检测：通过实时监测用户环境的正常行为模式，识别出不符合预期的活动，如非授权访问、异常登录、数据泄露等，及时发出警报。

日志分析：对系统和应用程序的日志进行实时分析，识别出潜在的威胁迹象和异常事件，帮助用户快速发现并应对安全问题。

恶意软件检测：使用先进的威胁检测技术，监测网络流量和文件，识别潜在的恶意软件和病毒，并提供及时的警报和清除建议。

外部风险评估：评估与用户相关的外部风险因素，如供应链安全、第三方服务提供商的安全性等，帮助用户了解潜在的安全风险。

实时警报和通知：根据监测结果和威胁评估，向用户发送实时警报和通知，包括电子邮件、短信或安全事件管理平台上的通知，以便用户能够采取适当的行动。

安全报告和分析：定期生成详细的安全报告，包括威胁分析、弱点扫描结果、异常活动等，帮助用户了解整体的安全状况和趋势。

通过安全感知服务可以及时发现和应对各种安全威胁和漏洞，提高整体的安全性，并减少潜在的损失。

服务交付：《安全态势报告》

**2、服务地点：**采购人指定地点

**3、服务期限：**维保期限从中标日起至2024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%。