一、开标一览表（报价表）

绍兴市生态环境局、绍兴衡业工程管理咨询有限公司：

按你方招标文件要求，我们，本投标文件签字方，谨此向你方发出要约如下：如你方接受本投标，我方承诺按照如下开标一览表（报价表）的价格完成 绍兴市生态环境局网络和数据安全整体运营项目【招标编号：SXHY-2025CG-0310】的实施。

开标一览表（报价表）（单位均为人民币元）

序号	名称	服务范围	服务要求	服务时间	服务标准	服务人数	服务单价	备注（如有）
1	漏洞扫描评估服务	绍兴市生态环境局内部网络环境、存储环境、应用系统等	**服务内容：**提供各类系统的安全漏洞检测服务，客观分析安全风险等级，并根据检测结果和危害分析，提供专业修复意见，协助修复漏洞，并进行复测； 1）安全漏洞检测：如操作系统、中间件、B/S 业务系统、数据库等漏洞； 2）业务逻辑漏洞检测：如后台登录处存在逻辑错误，登陆时没有错误次数限制用户登录，并且没有判断验证码过期，导致验证码可以重复使用，可被爆破用户名密码或撞库； 3）Webshell 检测：如网页后门程序、线程插入后门程序、扩展后门程序；	1 年	按照招标文件要求执行	3 人	7500.00	4 次/年

			4）弱口令核查，复用口令核查。 5）提供检测的漏洞数不少于230000条，兼容CVE、CNNVD、CNVD、Bugtraq等主流标准。 6）提供国产操作系统的漏洞扫描内容，包括麒麟（Kylin）、统信（UnionTech OS）、中兴新节点（NewStart CGSL）等。 7）提供操作系统、网络设备、数据库、中间件等漏洞扫描。 **时间要求：**每次进行现场服务时长不少于2天 **服务频率：**4次/年 **服务输出：**《漏洞评估报告》					
2	渗透测试服务	绍兴市生态环境局内部网络环境、存储环境、应用系统等	**服务内容：** 尝试验证每一个漏洞的真实威胁，同时查清漏洞的成因，做到自主可控可防，测试完成后，提出专业修复建议，协助解决安全问题。 渗透测试主要内容如下： Windows 系列操作系统渗透测试包括： 1）端口扫描；2）NetBIOS name service 测试；3）RFC 漏洞攻击；4）SMB 漏洞攻击；5）Windows DNS 测试；6）Snmp 漏洞测试；7）活动目录测试；8）Sql Server 弱口令测试；9）系统弱口令测试；10）终端服务弱口令测试；11）IIS 权限及溢出测试；12）	1年	按照招标文件要求执行	3人	15000.00	4次/年

			Exchange server 漏洞测试；13）ftp 弱口令测试。 Linux 系列主机操作系统渗透： SOLARIS、AIX、LINUX、SCO、SGI 等操作系统渗透测试包括： 1）端口扫描；2）ssh 弱口令测试；3）telnet 弱口令测试；4）Ftp 弱口令测试；5）Samba 弱口令测试；6）RPc 枚举和漏洞测试；7）NFS 漏洞测试；8）Snmp 漏洞测试；9）DNS 漏洞测试；10）rlogin,rsh 漏洞测试。 数据库系统的测试： 对 MS-SQL、ORACLE、MYSQL、DB2 等数据库应用系统渗透测试： 1）默认账号及弱口令攻击；2）存储过程漏洞攻击;3）数据库运行权限探测;4）提权漏洞攻击；5）低版本溢出漏洞攻击。 WEB 应用系统渗透： 对渗透目标提供的各种应用，如 JSP、PHP 等组成的 WEB 应用渗透测试： 1）检查应用系统架构、防止用户绕过系统直接修改数据库；2）检查身份认证模块，防止非法用户绕过身份认证；3）检查数据库接口模块，防止用户获取系统权限；4）检查文件接口模块，防止用户获取系统文件；5）检查其他安全威胁。					

			网络设备渗透： 对防火墙、入侵检测系统、网络设备进行渗透测试： 1）tftp 获取配置攻击；2）管理界面默认账号密码；3）snmp 读写权限攻击；4）telnet,ssh 默认账号弱口令攻击；5）低版本溢出漏洞攻击。 口令猜解： 口令猜测也是一种出现概率很高的风险，几乎不需要任何攻击工具，利用一个简单的暴力攻击程序和一个比较完善的字典，就可以猜测口令。 对一个系统账号的猜测通常包括两个方面：首先是对用户名的猜测，其次是对密码的猜测。 其他方面渗透： 除了上述的测试手段外，还会在渗透测试过程中使用的技术： 1）社会工程学；2）客户端攻击；3）拒绝服务攻击；4）中间人攻击。 **服务频率：**4 次/年，每季度不少于 1 次 **服务输出：**《渗透测试报告》 **人员要求：**国家注册信息安全专业人员-渗透测试工程师（CISP-PTE）。					
3	安全巡检服务	绍兴市生态环境局内部	**服务内容：**通过人工现场巡查方式对重要信息系统（业务系统、安全系统、网络系	1 年	按照招标文件	1 人	5000.00	4 次/年

		网络环境、存储环境、应用系统等	统）的运行状态、安全策略以及日志等风险进行识别、分析和定位，提出可行性修复建议，协助现场处置。 1、运行检查：对软硬件系统的运行状态进行检查，发现安全隐患，协助用户恢复。 2、策略检查：针对绍兴市生态环境局现有系统的安全策略和事件日志进行检查，对检查结果进行深入分析，协助用户整改。 3、日志分析：针对现有的安全设备系统进行日志分析，通过分析，明确安全设备的策略配置，防止因为安全配置不充分导致系统存在安全隐患，确保设备的安全性和完整性。 4、漏洞补丁修复支持：提供对服务器、软硬件等补丁修复远程支持。 **服务方式：**现场 **服务频率：**4 次/年 **服务输出：**《安全巡检报告》		要求执行			
4	重要时期安全保障	绍兴市生态环境局内部网络环境、存储环境、应用系统等	**服务内容：** 1）备战阶段：摸清家底。从黑客视角分析可能的攻击路径，以减少风险暴露面、事前防范和加固为主要目的，加强系统健壮性，提升黑客攻击成本。主要工作：互联网未知资产探测、业务资产黑盒测试与加固、全网信息系统（服务器、路由器、交换机、安全系统等）配置核查，策略精细化调优。外联	1 年	按照招标文件要求执行	1 人	15000.00	在省市护网演练、国庆春节等重大时机提供安全保障

			网等其他网络边界的开放服务和策略检查。 2）决战阶段：实时守护。开展异常流量的精准定位和分析，对恶意行为迅速封堵，不给攻击者可乘之机。主要工作：态势感知系统及各类网络安全系统的实时攻击监测和分析、攻击研判和快速响应。 3）战后阶段:复盘总结。结合安全事件，找出潜藏的系统脆弱点，分析攻击者惯用的攻击手法特点，提出精准防护建议，进一步提升系统健壮性，以及积累更多重保活动经验，精准施策，构筑安全堡垒。 **服务方式：**现场 **服务频率：**在省市护网演练、国庆春节等重大时机提供安全保障 **服务输出：**《重要保障时期安全服务方案》					
5	应急响应服务	绍兴市生态环境局内部网络环境、存储环境、应用系统等	**工作内容：** 在发生确切的网络安全事件时，应急响应实施人员应及时采取行动，限制事件扩散和影响的范围，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，提出基于安全事件解决方案，追查事件来源，协助后续处置。 应急响应范围包括： 1、突发网络安全设备通信异常； 2、失陷主机定位服务，病毒攻击分析、	1 年	按照招标文件要求执行	3 人	24000.00	按需响应，不限次数

			溯源和响应 3、安全系统升级或网络割接人员保障； 4、网络安全事件相关工作事务。 **服务方式：**现场 **服务频率：**按需响应，不限次数 **时间要求：**不限次数。1 小时内抵达客户现场，4 小时内控制风险、事件。 **服务输出：**《应急响应处置报告》、《安全加固建议方案》					
6	应急演练/攻防演练服务	绍兴市生态环境局内部网络环境、存储环境、应用系统等	**服务内容：** 应急演练服务/攻防演练围绕网络安全攻击场景，结合绍兴市生态环境局风险控制策略，制定或完善风险控制应急预案体系；以应急预案为基础，制定应急演练服务/攻防演练方案，通过应急预案和演练方案的培训，使得组织及人员明确其在演练过程中的职责范围、接口关系，明确应急处置的操作规范和操作程序。在演练的实施过程中，提供模拟网络攻击，协助工控环境单位、实施应急响应工作，包括预警与评估、 应急响应预案启动和应急处置工作。在应急演练服务/攻防演练结束后，对演练过程进行分析和回顾，协助工控环境机构撰写应急演练情况总结报告，并开展应急演练工作的审核，以确定改进目标和改进的具体工作内容。演练总结报告、演练审核结果作为策划阶段各项工作的	1 年	按照招标文件要求执行	5 人	42000.00	1 次/年

			改进要素，持续完善应急体系。 **服务方式：**现场演练 **服务频率：**1次/年 **服务输出：**《攻防演练方案》《应急演练方案》、《攻防演练总结报告》《应急演练总结报告》					
7	资产及攻击面梳理服务	绍兴市生态环境局内部网络环境、存储环境、应用系统等	**数据资产梳理：** 系统架构分析：对每个系统的架构进行详细分析，包括硬件设备（服务器、存储等）、软件系统（操作系统、数据库管理系统、应用程序等）以及网络拓扑结构，绘制系统架构图，明确各部分之间的关系和数据流向。 **数据资源盘点：** 无废城市系统：识别与固体废弃物产生、收集、运输、处理、处置等环节相关的数据表、数据字段，如废弃物产生单位信息、废弃物种类和数量、处理设施运行数据等。 浙里蓝天系统：梳理空气质量监测数据（包括各类污染物浓度、气象数据等）、污染源排放数据（工业源、机动车尾气排放等）、大气污染防治措施相关数据等。 机排系统：确定汽车尾气检测数据、在用车排放监管数据、燃油质量数据以及与机动车环保标志管理相关的数据等。 等等系统； 数据接口梳理：找出各系统与外部系统	1年	按照招标文件要求执行	2人	35000.00	1次/年

			（如其他政府部门系统、企业系统等）之间的数据接口，记录接口的类型（如 Web 服务接口、文件接口等）、数据传输频率、传输的数据内容等。 **网络及互联网资产梳理：** 域名嗅探：将网络流量中的 http 域名信息（包括但不限于域名、ip 地址、端口号、网站标题、协议）挖掘并展示，同时以 ip 为维度进行分类。 对 https 免证书加载即可探测域名信息（包括但不限于域名、ip 地址、端口号、网站标题、协议）。 资产详情：服务商能挖掘出相关资产的资产信息：包括但不限于资产的开启的端口、端口相关服务、应用版本号、网站标题、mac 地址、操作系统、主机名等。 可以对 IP 地址、服务为维度展示资产详情。 可根据资产梳理的 ip 范围、端口并发扫描数、应用识别并发数。 提供可视化方式显示隔离域内部连接关系，同时显示相关资产开启的活动端口与非活动端口。 根据隔离域视图内容（包括但不限于视图本体、资产开启的活动端口与相关服务、资产开启的非活动端口与相关服务)以 html、					

			docx、xls 格式输出报表。 **服务方式：**现场 **服务频率：**1 次/年 **服务输出：**《资产梳理报告》					
8	网络安全平台运维服务	绍兴市生态环境局现网安全设备如态势感知平台、防火墙、入侵防护设备	**服务描述：** 针对绍兴市生态环境局现网安全设备如态势感知平台、防火墙、入侵防护设备展开常态化的运维保障服务，综合分析相关告警日志。若出现黑客入侵事件，及时发现问题、追踪溯源，协助关技术人员处置事件，尽量降低安全风险。 **服务方式：**现场 **服务频率：**1 次/月 **服务输出：**《平台运维工作记录》、《安全事件分析与处置报告》	1 年	按照招标文件要求执行	1 人	3500.00	1 次/月
9	威胁态势检测服务	绍兴市生态环境局内部网络环境、存储环境、应用系统等	**1.态势分析平台要求：**2U 标准机架式设备,6 个千兆电口，2 个万兆光口,冗余电源，存储 240SSD，32TB，内存 128G； 为服务提供态势分析、安全监测、安全处置、资产管理、知识情报等能力。 全网态势：对全网资产概述、高危资产、漏洞、告警趋势、安全日志趋势、告警统计、最新告警名称和影响范围、热点威胁等内容的相关展示。 漏洞态势：主动发现内网漏洞功能并关联资产，漏洞分析类型包含 Web 安全、	1 年	按照招标文件要求执行	1 人	100000.00	全年

			WINDOWS 安全、通用等漏洞； 安全监测：日志概览，包括日志源数量、安全日志数量、审计日志数量、安全日志级别分布、安全日志类型排名、日志量趋势，支持概览时间设置。 性能监测：资产性能监测概览，支持监测设备总数、异常数、主机异常数、网络设备异常数、安全设备异常数展示，支持监控资产性能状态占比、性能告警 TOP10、规则类型事件分布、CPU 使用率 TOP10、内存使用率 TOP10、磁盘使用率 TOP10，支持性能监控详细列表，包括 IP、资产名称、归属安全域、资产类型、性能状态、连通状态、CPU 使用率、内存使用率、磁盘使用率、操作等。 工单管理：工单管理，支持指派相关责任人进行处理，支持对工单进行分组管理，分组类型包括我的工单、待处置工单、已处置工单、历史工单； 任务调度：周期性任务调度，可分析联动任务队列，根据当前负载情况，将所接收的周期性任务分别分配给各任务队列，实现态势感知平台对联动任务执行节点的资源进行合理利用，提供第三方机构检验报告或认证证书证明材料。 **2. 流量采集器要求：**服务期间提供流量监测探针要求，1U 标准机架式设备，内存					

			80,6 个千兆电口,4 个千兆光口插槽,1 个 CONSOLE 口，整机吞吐率≥2Gbps,监测吞吐率≥1Gbps； 包含:1 年攻击检测规则库、应用识别库、地理信息库升级许可；1 年僵尸主机规则库升级许可。 为保障服务期间系统运行的可靠性与稳定性，要求信息安全设备、系统软件的开发、生产符合 TL9000-HSV R6.3/5.7 标准。 攻击防护： 支持独立的攻击检测引擎，涵盖 12000 种以上的攻击检测规则库。规则库支持按照攻击类型、操作系统、风险等级、应用类型、流行程度等方式进行分类。 能够检测防御包括扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问、注入攻击、URL 跳转、跨站攻击、WebShell、浏览器劫持、文件漏洞攻击、工控漏洞攻击、车联网漏洞攻击、物联网漏洞攻击等在内的 17 大类超过 12000 种以上网络攻击事件。 对攻击逃逸报文进行深度智能检测防御； 针对邮件、文件、远程访问、数据库、WEB 应用等协议类型进行暴力破解检测防御，包括 SMTP、IMAP、POP3、FTP、SMB、TELNET、					

			LDAP、ORACLE、MYSQL、MSSQL、MONGODB、POSTGRESQL、DB2、REDIS、HTTP 等协议的口令暴力破解行为。 僵尸主机检测： 具有独立的僵尸主机特征库，能够对 11000 种以上僵尸主机行为进行监测，包括僵尸网络、木马控制、蠕虫、挖矿、勒索、移动端木马控制、APT 等多类型的僵尸主机行为。 对检测到的控制主机数量、僵尸主机数量实时统计，记录僵尸主机的攻击次数和控制主机的活跃次数，且支持以地图的形式展现控制主机/僵尸主机的地理分布。 记录僵尸主机事件排名、控制主机排名、僵尸主机排名，并可统计控制主机 Top10 和僵尸主机事件 Top10。 异常流量检测： 对 HTTP、FTP、SMTP、IMAP、POP3、TELNET 等服务的隐蔽通信检测，可设置相应警告、阻断动作，并可设置忽略知名应用。 DGA 域名检测，采用 DGA 智慧引擎进行检测，用户可设置敏感度。 异常行为检测包含异常应用检测和代理检测两种类型，异常应用如远程控制、隧道协议、违规应用；代理检测如应用代理、正向代理、反向代理。					

			IPv6 审计： 能够在 IPv6 网络中发现活跃 IP 地址，采用网络协议 IP 地址扫描方法，获取并记录该 IPv6 地址为中心预定范围内的其他活跃的 IPv6 地址，并采用路由发现方法获取到达记录的 IPv6 地址所经过的中间设备的 IPv6 地址。 加密流量检测： 支持卸载 SSL，实现对 HTTPS、IMAPS、SMTPS、POP3S、FTPS、RDP、MQTT、SIP 等加密流量的分析检测。 溯源取证： 支持攻击取证、僵尸主机取证、恶意程序样本、恶意程序无风险样本、威胁情报样本、威胁情报取证、WEB 防护取证、异常流量取证，取证类型支持报文取证和样本文件取证两种形式。 **3.服务频率：**全年					
10	网络优化提升服务	生态环境监测网络	**服务内容：** 生态环境监测网络调研规划与优化提升。主要包括以下内容： 1.安全设备管理： 配置、部署和管理防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等安全设备，以监控和阻止潜在的网络攻击。 更新和维护安全设备的防病毒引擎、黑	1 年	按照招标文件要求执行	2 人	100000.00	项目经理每周到场服务不少于 1 次，常态化运维服务每周

			名单、规则库等信息，确保其有效性。 2.系统和应用程序安全管理： 对操作系统、数据库、Web 服务器、应用程序等进行漏洞扫描、安全配置评估，并及时修补或优化安全设置。 监测和检查系统和应用程序的日志，及时发现和应对异常行为和安全事件。 3.访问控制与身份验证管理： 设计和实施访问控制策略，包括账号管理、权限分配、多因素身份验证等，确保合法用户的访问和操作。 管理和定期审计用户账号，及时禁用或删除无效或不再需要的账号。 4.恶意代码防范与处理： 配置和管理反病毒软件和恶意代码防护系统，对传入或内部传播的恶意代码进行及时检测、隔离和清除。 定期进行恶意代码扫描和安全漏洞评估，修补系统和应用程序的漏洞，防范恶意攻击。 5.安全策略与规范制定： 设计和编写网络安全策略、规范和最佳实践，并确保其落地和执行。 定期审查和更新安全策略，以适应新的威胁和风险。 6.事件响应与处置：					不少于 2-3 个工作日。

			建立应急响应计划和流程，指导员工在发生安全事件时的快速响应和处置。 对安全事件进行调查和分析，追踪攻击来源，并采取相应的措施防止再次发生。 7.漏洞管理与补丁管理： 定期进行漏洞扫描和漏洞评估，及时发现和修补系统和应用程序的漏洞。 管理和应用安全补丁和更新，确保系统和应用程序的安全性。 8.安全性能监测与优化： 监测和分析网络流量、日志和事件，发现异常行为和潜在威胁。 优化网络设备和安全配置，提高网络的安全性和性能。 **服务要求：**项目经理每周到场服务不少于1次，常态化运维服务每周不少于2-3个工作日。					
11	安全培训服务	绍兴市生态环境局全体员工	**服务描述：** 对全体职员进行网络安全意识培训，通过课堂演示、案例剖析等多个维度的授课方式，提升安全意识、规范日常工作行为，实现信息安全"人防"。 **培训讲师：**浙江省网络空间安全协会专家库入库专家并提供讲师社保证明。 **服务方式：**现场 **服务频率：**2次/年	1年	按照招标文件要求执行	1人	6000.00	2次/年

			服务输出：《安全意识培训课件》					
12	办公终端运维服务	绍兴市生态环境局国产和非国产的办公软件，及国产办公终端硬件，国产打印机	**工作内容：** 国产和非国产的办公软件，及国产办公终端硬件，国产打印机运维保障服务，按需响应，服务期一年。 **时间要求：**15 分钟内响应，2 小时内修复，硬件故障 24 小时内无法修复的提供备品备件。 **服务输出：**《维护记录》	1 年	按照招标文件要求执行	1 人	66000.00	全年
投标报价（小写）				606000.00				/
投标报价（大写）				陆拾万陆仟元整				/

投标人名称（电子签名）：宁波壹安信息科技有限公司

日期：2025 年 07 月 01 日

注：

1、投标人需按本表格式填写，**否则视为投标文件含有采购人不能接受的附加条件，投标无效；**。

2、有关本项目实施所涉及的一切费用均计入报价。**采购人将以合同形式有偿取得货物或服务，不接受投标人给予的赠品、回扣或者与采购无关的其他商品、服务，不得出现“0 元”“免费赠送”等形式的无偿报价，否则视为投标文件含有采购人不能接受的附加条件，投标无效；采购内容未包含在《开标一览表（报价表）》名称栏中，投标人不能作出合理解释的，视为投标文件含有采购人不能接受的附加条件的，投标无效。**

3、特别提示：采购代理机构将对项目名称和项目编号，中标供应商名称、地址和中标金额，主要中标标的名称、服务范围、服务要求、服务时间、服务标准等予以公示。

4、符合招标文件中列明的可享受中小企业扶持政策的投标人，请填写中小企业声明函。注：投标人提供的中小企业声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。