# **第三部分 采购需求**

### **一、项目概况**

依据公安大数据安全技术要求，在确保网络架构稳定、设备可靠、边界清晰，充分考虑现网运行情况下，合理规划网络安全架构、业务安全架构、数据安全架构、云平台安全架构，从而构建内生安全能力，推进公安大数据安全体系“一中心、两体系、两能力”的建设，有力支撑温州市公安大数据智能化建设应用。

### **二、建设目标**

根据公安大数据智能化安全体系的指导思想、设计原则、建设思路，构建基于云计算、大数据、新一代公安网的安全、可信、合规的立体化纵深防御体系，形成科学实用的“体系化安全防护能力、规范化安全管理能力、综合化安全运维能力”，重点打造“一个中心（即安全管理中心）、两个体系（即零信任体系、安全防护体系）、两个能力（安全访问能力、数据交换能力），做到全网安全态势敏锐感知，安全威胁快速检测与处置，确保大数据全程可知、可控、可管、可查，变静态为动态，变被动为主动，为公安大数据智能化建设提供严密安全保障。

本项目建设目标如下：

目标一：建设零信任基础模块。

建设公安大数据安全保障体系-零信任基础模块，根据公安部“零信任体系”建设要求，建设认证服务、权限服务、业务安全策略控制等服务，实现对人员、设备、应用与服务实现全面数字身份管理，完成省市零信任体系一体化建设。

目标二：建设公安信息系统大数据安全审计平台。

基于相关规范标准，建设公安信息系统大数据安全审计平台，通过省、市平台之间级联接口，实现不同级别、不同区域、不同类型的应用系统/资源库之间日志信息的互联互通和可控共享。同时明确本级平台运维与管理要求，建立配套工作机制。多源化采集日志数据、流程化处理日志数据、异构化存储日志数据，结合温州公安应用日志数据和应用特点，开展深度挖掘分析，梳理异常行为模型，提升异常行为分析精度。

目标三：开展安全运营服务。

如风险评估服务、渗透测试服务、网络和数据安全专项检查服务、安全事件应急响应处置服务、重保服务、总结分析研判服务、安全制度建设、定制化安全培训服务及攻防演练、比武等内容。

### **三、建设内容**

#### **1.技术标准、规范**

1、国家规定的标准及规范，按最新的标准及规范执行。

2、行业标准及规范，按最新的标准及规范执行。

3、与服务有关的材料设备质量应符合中华人民共和国及产品品牌所在国的有关质量标准，上述标准如有不一致，执行两者中更严格的标准。

4、其它相关标准及规范，按最新的标准及规范执行。

#### **2.工作范围与服务期要求**

各供应商须按国家有关标准及规范完成采购文件规定的所有工作内容：

1、履行所有规定服务。

2、服务须达到采购文件规定的质量标准及使用要求。

3、本项目要求服务期为18个月。

#### **3.服务内容与技术要求**

#### **（一）安全运营体系服务**

###### ①服务要求及提交成果物

###### （1）漏洞扫描

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 服务次数 | 服务期内提供不少于12次 |
| 服务内容 | 采用业界认可的、专业的扫描工具，通过定制的扫描规则，形成安全扫描策略文档，对用户指定系统进行全面的自动化安全扫描，人工验证扫描结果，并输出安全扫描报告及修复建议。 |
| 输出物 | 《漏洞扫描报告》 |

###### （2）代码检测

|  |  |
| --- | --- |
| **技术指标** | **指标要求0** |
| 服务次数 | 服务期内不少于15个系统 |
| 服务内容 | 提供开源组件评估服务，提供开源组件评估报告或源代码检测服务。收集当前系统的源代码，在了解业务流和各模块功能和结构的情况下，以OWASP TOP 10为检查依据，检查系统代码在程序编写上的安全性和脆弱性以及结构性安全。  源代码安全性审计主要内容应包括：   1. 分析源代码是否能追溯到需求； 2. 分析源代码是否符合支持工具和编程语言分析； 3. 分析源代码是否满足模块化、可验证、易安全修改的要求； 4. 分析软件编码中所使用技术的安全性和方法的合理性。 |
| 输出物 | 《源代码检测报告》 |

###### （3）渗透测试

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 服务次数 | 服务期内不少于20个系统 |
| 服务内容 | 通过真实模拟黑客使用的工具、分析方法来对信息系统进行模拟攻击，并结合智能工具扫描结果，由工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题。主要分析内容包括逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误等以及其他专项内容测试与分析，重点发现信息系统应用层业务流程和逻辑上的安全漏洞和敏感信息泄露的风险，输出渗透测试报告。 |
| 输出物 | 《渗透测试报告》 |

###### （4）应急响应

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 服务次数 | 服务期内不限次数 |
| 服务内容 | 服务期内，通过远程和现场支持的形式协助采购人对遇到的突发性安全事件进行紧急分析和处理。  当出现安全事件时，必须及时进行响应，具体要求包括：  1、技术人员必须在2小时内到达现场；  2、对入侵事件进行分析，查找原因；  3、抑制入侵事件的进一步发展，将事故的损害降低到最小化；  4、排除安全隐患，消除安全威胁，协助恢复系统正常运作；  5、提交应急响应报告及系统安全改进方案。 |
| 输出物 | 《应急响应报告》 |

###### （5）重点时期保护

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 服务次数 | 服务期内提供2次 |
| 服务内容 | 重要时期根据要求提供人员远程或现场保障服务，服务期间保障工程师利用人工结合工具等方式对单位信息系统、网站、服务器等资产进行5\*8小时/7\*8小时/7\*24小时等不同形式的实时监测，及时处理发现的系统安全事件。  保障期间现场工程师应开展包括但不限于以下安全工作：  1、网络安全运行状态监测分析  帮助用户开展安全设备的性能指标、功能指标和硬件状态的巡检。根据巡检记录，针对关键链路和节点设备的CPU、内存、磁盘使用率、网络连通性、网络会话连接数、网络流量等指标设置正常运行区间值、异常运行区间值及告警方式，一旦相关指标发生异常，及时进行安全告警。针对监测指标产生的异常告警进行确认、分析，查找异常原因，提供解决方案，协解采购人完成安全整改和修复。  2、网络安全告警分析和预警  梳理网络和业务资产，针对网络收集的流量安全日志进行安全审计和分析，及时发现网络攻击和其它异常行为。对网络安全设备产生的扫描探测、SQL注入、跨站脚本攻击、木马后门上传等各类网络安全告警事件进行溯源分析和风险验证，帮助采购人快速完成安全响应。  3、安全事件应急处置  在发现信息完全威胁后第一时间进行跟进处理，最大限度的降低安全事故带来的危害，减少安全事故带来的影响，将采购人的安全损失降到最低。当入侵或者破坏发生时，对应的处理方法主要的原则是首先保护或恢复计算机、网络服务的正常工作；然后再对入侵者进行追查，并对整个应急响应过程进行记录。 |
| 输出物 | 《重保服务报告》 |

###### ②特别说明

在本次安全服务项目中，需要明确的是，所涉及的服务工具并未包含在本次服务的采购范围之内。此外，我方提出的能力要求仅用于参考，旨在为项目的整体方向提供指导性意见，但并不作为实际服务实施过程中的具体执行标准，也不参与最终的服务验收流程。验收以安全运营体系服务招标要求为准。

###### （1）关于漏洞检测，需提供相关工具如漏洞扫描工具，工具类型不限，需具备以下能力要求：

★1、产品具备《网络关键设备和网络安全专用产品安全认证证书》，提供有效证书复印件；产品符合《GB/T 20278-2022 信息安全技术网络脆弱性扫描产品安全技术要求》增强级的要求，（提供第三方测试报告证明并加盖安服工具原厂公章）；

2、产品具备国家信息安全漏洞库《CNNVD兼容性资质证书》，提供有效证书的复印件；

3、漏洞知识库支持自定义编辑，可编辑漏洞描述、修复建议、漏洞等级等内容，在扫描结果和导出报告中应展示编辑后的内容；

4、支持主机扫描、网站扫描、数据库扫描、基线配置、事件内容、弱口令扫描、存活主机探测、大数据漏洞扫描、物联网漏洞扫描、信创漏洞扫描十种任务类型；

5、厂商漏洞特征库大于300000条；提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNNVD、Bugtraq、CNCVE、CNVD等国际、国内漏洞库标准兼容；

6、支持VPN代理扫描，可在产品界面添加代理网络配置，实现公有云、隔离网等特殊网络环境下的漏洞扫描；

★7、具备弱口令扫描功能，支持弱口令扫描协议数量≥22种，包括FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP等协议进行弱口令扫描，允许用户自定义用户、密码字典，（提供功能截图证明并加盖安服工具原厂公章）；

8、扫描结果在产品界面中支持查看目标应用返回的软件版本，可以方便与漏洞描述对比进行漏洞验证；

9、管理人员可根据系统给出的漏洞参数、HTTP请求/响应数据，快速验证，一键验证漏洞。支持对Struts2远程命令执行漏洞进行命令执行和文件上传的渗透测试验证操作；

★10、支持对数据库内核入侵隐藏对象、隐藏用户的探测能力，（提供第三方机构证明材料并加盖安服工具原厂公章）。

###### （2）关于代码检测，需提供相关工具如代码检测工具，工具类型不限，需具备以下能力要求：

1. ★支持代码注入、跨站脚本、输入验证、危险函数、代码质量、API误用、密码管理、异常处理等常见安全缺陷问题的检测，二级缺陷类型不低于2000个。提供功能截图或证明材料
2. 支持根据检测语言类型配置可信数据源，提高检测准确性。可信数据源包括命令行参数、web表单、json字符串等，界面可选可信源配置类型应不少于15种。
3. 能够针对同种类型的安全问题成因路径进行统一展示，便于找到最佳修复节点。
4. 能够迅速定位某一特定源代码安全问题所在源代码行，对问题产生的整个过程进行跟踪。
5. 支持配置自动化检测策略，能够按天或周进行自动化周期性检测
6. 能够对项目中多次检测的结果进行对比，形成趋势分析
7. 支持本地直接发起检测任务，也可以从SVN、GIT、StarTeam、Azure DevOps、ClearCase 等代码仓库获取代码发起检测任务，同时源代码来源支持FTP和共享目录。
8. ★代码审计工具符合中国信息通信研究院的《静态应用程序安全测试工具能力要求》标准。（提供资质证明材料）

###### （3）关于web应用，需提供相关工具如web应用检测工具，工具类型不限，需具备以下能力要求：

★1、产品具备《网络关键设备和网络安全专用产品安全认证证书》，提供有效证书复印件；产品符合《GB/T 37931-2019 信息安全技术 Web应用安全检测系统安全技术要求和测试评价方法》的要求，（提供第三方测试报告证明并加盖安服工具原厂公章）；

★2、产品通过中国网络安全审查技术与认证中心获得IT产品信息安全认证证书，（提供证书复印件并加盖安服工具原厂公章）；

3、产品具备国家信息安全漏洞库《CNNVD兼容性资质证书》；

4、支持常见的WEB应用弱点检测，支持OWASP TOP 10等主流安全漏洞；

5、支持在漏洞知识库中单独选择某漏洞直接下发扫描任务以验证是否存在该漏洞；

6、支持定制扫描：用户可根据；目标扫描网站的特点以及所在网络环境，对扫描过程进行定制，如爬行、检测、过滤、网络环境等；

7、支持端口扫描和服务的协议及版本识别，支持自定义扫描端口范围；

8、支持IP地址的形式下发扫描任务并自动发现存在的Web资产。

###### （4）关于自动渗透，需提供相关工具如自动话渗透工具，工具类型不限，需具备以下能力要求：

1、漏洞探测功能支持使用POC对资产进行批量漏洞探测。指纹/POC探测扫描模式支持只识别指纹、识别指纹再进行POC探测、不需要指纹前置直接POC探测三种类型；

2、支持对能获取权限的漏洞进行漏洞利用，获取对方的服务器权限，包括但不限于代码执行、命令执行、文件上传、反序列化漏洞等的漏洞利用；漏洞利用功能能对漏洞进行植入webshell、命令执行、反弹shell等操作；

3、能够以投递agent的形式对内网进行web漏洞检测、常见服务漏洞、弱口令漏洞、并能通过web页面进行任务下发进行内网的web漏洞探测、服务漏洞、弱口令等进行内网的漏洞检测；

★4、支持对跨域资源共享漏洞、子域名劫持漏洞、任意账号密码重置逻辑漏洞的检测发现能力，（提供第三方机构证明材料并加盖安服工具原厂公章）。

★5、为保证服务质量，中标单位或服务原厂需提供一名渗透测试专家，具备CISP-PTS（渗透测试专家）、CISP-BDSA（大数据安全分析师）、CISAW（渗透测试）、CNVD原创漏洞资质，提供相关证明材料。

###### 关于应急响应，需提供相关工具如应急响应处置工具，工具类型不限，需具备以下能力要求：

1、产品具备国家信息安全漏洞库《CNNVD兼容性资质证书》，提供有效证书的复印件；

★2、支持设置线索，发现关键可疑行为，包括IP线索、关键词线索、文件名线索、时间线索的设置，（提供功能截图证明并加盖安服工具原厂公章）；

3、支持采集日志格式自定义分析，包含Liunx日志、Web日志、数据库日志格式自定义，通过自定义创建日志解析格式；

4、支持对所采集的系统配置数据、使用痕迹数据、运行状态数据、恶意代码情况、系统日志、中间件日志等进行数据分析；

5、支持手动分析，支持处置人员查看采集的数据信息，标记关键数据形成可疑行为事件；

6、支持根据所提供的线索自动发现关键可疑行为并进行标记，提供功能截图证明；

7、支持根据关键字搜索相关知识内容；

★8、支持根据勒索文件后缀查找对应解密工具，提供解密工具的下载、使用介绍等，（提供功能截图证明并加盖安服工具原厂公章）；

9、支持提供IP、域名、文件等威胁情报查询；

10、支持自定义设置策略规则、描述信息、处置建议等内容，可以应对高级事件类型溯源。

11、为保证服务质量，中标单位或原厂需提供一名应急响应专家，具备CISSP（信息系统安全专家）、信息安全工程师、CISP-CISE（注册信息安全工程师）、CISAW（应急服务）资质，提供相关证明材料。

#### **（二）比武及攻防演练服务**

①比武及攻防演练特别说明

在比武及攻防演练项目中，需要明确的是，所涉及的服务工具并未包含在本次服务的采购范围之内。此外，我方提出的能力要求仅用于参考，旨在为项目的整体方向提供指导性意见，但并不作为实际服务实施过程中的具体执行标准，也不参与最终的服务验收流程。验收需要输出相关交付文档，包括但不限于：《攻防演练整体方案》、《攻防演练总结报告》《演习重大战果报告》以及各类攻防演练涉及材料等，需要服务工程师签字、服务原厂盖章、业务签字或盖章。

（1）攻防比武大赛

提供至少一次10人以上的比武大赛服务。

比武大赛形式根据我局要求确定，不限于以下几种：

1、CTF夺旗赛：CTF夺旗赛模式提供若干不同类型的赛题，题目通过靶机或附件形式下发，参赛者需要运用相关网络安全技术对靶机或附件进行攻击、破解，在相应题目中获得的Flag（旗标文件）提交至评分系统，评分系统审核Flag正确后，参赛者将获得对应的分值。

2、AWD攻防对抗赛：AWD攻防赛模式中，各参赛者互为攻击方和防守方，实现真正的网络攻防对抗（Attack With Defence，攻防兼备）。参赛者在AWD攻防赛模式中，既要防守自己服务器，也要攻击其他参赛队伍的服务器。此模式既考查选手的攻击能力，也锻炼选手防御能力。

3、Break&Fix攻防赛：Break&Fix攻防赛既考查选手的攻击能力，也锻炼选手防御能力。比赛期间，选手只能访问自己的靶机，并对靶机进行攻击或修复操作。在Break（攻击、检测）环节攻击成功即可得分。在Fix（修复）环节由平台按轮次对选手靶机发起攻击，检测修复是否成功。与传统AWD攻防对抗赛不同的是，Break&Fix模式可避免其他参赛人员对己方靶机的干扰操作，可让参赛人员更加专注解题。

4、靶场综合渗透赛：靶场综合渗透涉及多层网络，可模拟真实网络生产环境。参赛者通过外部入口逐层渗透获取内网靶机相应权限，从而读取相应的Flag（旗标文件）。涉及的知识点有内网安全、反向代理、内网穿透、服务器提权、中间件安全、数据库安全等。综合渗透赛模式提供以下竞赛模拟环境：参赛选手以攻击者的身份对模拟的内网进行内网渗透、内网穿透等操作；该竞赛单元主要考察选手对内网知识、渗透知识的了解，例如信息收集、漏洞挖掘、主机探测、服务器权限提升等。

（2）攻防比武工具提供

提供一次攻防比武大赛并提供所需平台。

1、比武平台包含后台管理系统、攻击行为分析系统、可视化系统、审计流量存储系统等；

2、攻防比武平台能够进行攻防的演习全生命周期管理，演习前期通过平台初始化平台，初始创建账号，录入资源。演练中进行攻击过程审计，攻击成果管理，成果评审流程，攻击流量审计，可视化呈现。演习后数据报告汇总，数据导出。

★3、支持日志的汇集，要求具备在应用安全系统中进行精确风险检测的功能，（提供第三方机构证明材料并加盖安服工具原厂公章）；

★4、支持对攻击异常的检测，要求具备支持CC攻击的检测功能，（提供第三方机构证明材料并加盖安服工具原厂公章）。

（3）攻防演练

提供四次进行为期1周的攻防演练服务，提供专业的安全服务人员，配合我局民警进行攻防演练，从安全技术、管理和运营等多个维度着手，发现参演系统安全防御能力的问题和缺陷，帮助参演单位不断完善安全体系的建设，提升对抗新兴威胁的能力。

★为保证服务质量，中标单位或原厂在2023年1月以来获得省级及以上单位举办的攻防演练攻击组一等奖荣誉，提供证明材料。

（4）攻防演练培训

在每次攻防演戏服务后对本次攻防演习内容和历史攻防演练培训，通过理论讲解、案例分析、视频演示以及上机实操等丰富多样的授课方法，根据实际需求灵活定制课程并通过实战测试选拔出一批精干高效的信息安全网络技能精英。

★为保证服务质量，中标单位或原厂需提供一名培训专家，具备信息系统项目管理师、ISO27001主任审核员、CISAW（风险管理）、CISAW（安全运维）、CISI（注册信息安全讲师）资质。

#### **（三）审计服务中心级联**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 模块 | 子模块 | 功能描述 |
| 1 | 审计服务中心级联 | 温州市本级应用系统日志采集 | 完成上下级级联接入，接入124个应用系统，省厅回流85个，其中警务通APP9个，温州本地应用系统39个，市本级29个，鹿城区2个，瓯海区1个，平阳县2个，乐清市3个，温州交警1个、永嘉1个 |
| 2 | 鹿城区应用系统日志采集 |
| 3 | 龙湾区应用系统日志采集 |
| 4 | 瓯海区应用系统日志采集 |
| 5 | 洞头区应用系统日志采集 |
| 6 | 永嘉县应用系统日志采集 |
| 7 | 平阳县应用系统日志采集 |
| 8 | 苍南县应用系统日志采集 |
| 9 | 文成县应用系统日志采集 |
| 10 | 泰顺县应用系统日志采集 |
| 11 | 瑞安市应用系统日志采集 |
| 12 | 乐清市应用系统日志采集 |
| 13 | 龙港市应用系统日志采集 |
| 14 | 交警应用系统日志采集 |

#### **（四）审计服务中心对接**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 模块 | 子模块 | 功能描述 |
| 1 | 审计服务中心对接 | 省厅审计平台对接及日志回流采集、接入 | 完成对接上报任务管理，支持新增上报任务，包括上报名称、上报时间、上报周期、上报地址、上报类型、上报方式、状态、操作等内容。 |
| 2 | 温州审计平台日志归集、数据治理及日志上报 |

#### **（五）认证服务中心级联**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 模块 | 子模块 | 功能描述 |
| 1 | 认证服务中心级联 | 认证服务级联接口 | 级联内容门户级联、基础要素数据同步、应用互认、服务互认、终端环境感知互认和零信任体系统一认证服务级联等，具体包括以下级联服务接口： (1)应用目录级联 (2)系统认证级联 (3)用户目录级联 (4)机构目录级联 (5)服务目录级联 (6)数据目录级联 (7)权限映射关系目录级联 (8)认证服务级联 (9)实现省市两级认证服务级联 |

#### **（六）零信任体系接入验证服务**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 模块 | 子模块 | 功能描述 |
| 1 | 零信任体系接入验证服务 | 零信任体系接入验证服务 | 对接其他业务部门开发技术人员，指导开发技术人员针对业务系统进行改造，并提供验证业务系统对接完成接入服务，保障业务系统顺利对接“零信任”体系并接入温州市新一代公安信息网。 |

#### **（七）环境感知服务中心级联**

|  |  |
| --- | --- |
| **指标项** | **技术规格要求** |
| 环境感知分数同步 | 对接省厅环境感知，将终端感知分数进行同步省市两级平台，确保业务及终端的正常访问查询。 |
| 终端标识同步 | 对接省厅环境感知，将终端感知唯一标识进行同步省市两级平台，确保业务及终端的正常访问查询。 |
| 信息查询 | 对接省厅环境感知，省厅能够接收并处理市级的终端感知情况查询请求。 |

#### **（八）环境感知服务中心对接**

|  |  |
| --- | --- |
| **指标项** | **技术规格要求** |
| 对接审计服务中心 | 向审计服务提供环境感知的各类日志信息。 |
| 对接业务安全策略控制中心 | 环境感知服务感知到环境变更后，会将环境变更通知主动推送给业务安全策略控制服务作为决策依据 |
| 对接云桌面 | 能关联同一个访问中所使用的云桌面和物理终端上的身份标识，具备联动感知能力 |
| 云桌面基础安全感知 | 感知终端上是否安装了防病毒软件 感知终端上是否存在病毒 感知终端上的病毒库是否及时更新 感知终端上是否存在高危系统漏洞 感知终端上的漏洞库是否及时更新 感知当前系统是否加入域 感知当前登录的用户是否是域帐户 |
| 云桌面软件环境感知 | 支持按黑名单检测 支持按白名单检测  支持设置红名单 |
| 云桌面服务环境感知 | 支持按黑名单检测 支持按白名单检测  支持设置红名单 |
| 云桌面高危端口合规 | 支持按黑名单检测 支持设置红名单 |
| 密码维护要求感知 | 密码策略：密码长度最小值 密码策略：密码最短使用期限 密码策略：密码最长使用期限 密码策略：强制密码历史 密码策略：密码必须符合复杂性要求 密码策略：使用可还原的加密来存储密码 |
| windows防火墙控制感知 | 感知Windows防火墙是否开启 |

#### **（九）服务器安全加固软件**

|  |  |
| --- | --- |
| **指标项** | **技术规格要求** |
| 产品配置 | 为服务器提供安全安全防护，新建≥50个服务器安全防护授权。 |
| 主机资产清点 | 可以展示当前服务器、进程、账户、软件应用、Web资产、Web服务、Web框架、数据库、端口、网络连接、启动服务、安装包、计划任务、环境变量、内核模块等分类资产数量统计， |
| 行为管理 | 所投产品需支持对一台或一组服务器进行白名单学习策略，并可设置学习时长，学习后可形成应用列表及HASH值，对偏离学习列表以外的应用进行告警和拦截。 |
| 风险发现 | 对服务器系统级、数据库、中间件、应用级的弱口令、口令复用扫描，并可对扫描的结果进行修复验证，还可对口令风险的扫描任务进行设置，包括任务名称、目标服务器、扫描类型、扫描所用字典、执行周期等方式。 |
| 软件漏洞检测 | 可对服务器的软件漏洞进行综合扫描，并可对扫描方式、扫描周期进行设置，并以报告的形式展示软件漏洞扫描结果，包括：问题机器TOP5、影响最多漏洞TOP5、漏洞发现趋势等。软件厂商具备漏洞响应平台，平台在线白帽子数量大于8W，已发现漏洞数大于60W，（提供官网截图、软件著作权证书、并包含平台链接）。 |
| 基线检查 | 可支持等级保护2.0的二级、三级检查、测评、整改的业务检查。 |
| 病毒查杀 | 采用主动的方式进行自动化病毒查杀，可支持Bitdefender、ClamAV、Qowl等多引擎技术识别并查杀最新病毒。 |
| 威胁总览 | 支持统计并展示服务器的可疑威胁及告警信息，能够同时处理大量威胁事件，具备一种大规模事件处理的方法。 |
| 防恶意扫描 | 以攻击者视角、受害者视角展示恶意扫描的事件。 |
| 暴力破解检测 | 对暴力登录系统的账号和IP进行自动发现并上报暴力破解入侵事件。 |
| 后门检测 | 可以对操作系统、文件、软件中存在的后门进行检测。 |
| Webshell检测 | 自动识别web服务目录，并实时进行webshell后门的扫描 |
| 攻击溯源分析 | 支持记录当前所有服务器产生的事件日志，并提供筛选的功能和自定义时间段筛选查询，用户可通过安全日志快速锁定问题服务器，并进行相应处理。同时支持对安全事件进行溯源分析，对安全事件的等级、攻击类型、ATT&CK ID、ATT攻击阶段进行匹配。 |
| 无文件攻击 | 可通过无文件攻击检测引擎，对多种系统高危应用进行实时监控，实时监控服务器上发生的无文件攻击事件。及时告警，以便用户快速处置。 |
| 应用防护 | 支持通过插件的方式，工作于IIS、Apache、Nginx等web中间件内部，通过判断流量特征和WAF规则引擎，对访问流量进行监控或防护，阻断SQL注入、XSS、漏洞利用等Web攻击。 |
| 支持提供运行时应用自我保护功能（RASP）；可提供SQL注入防护能力、XSS防护能力且可自定义防护规则。（提供产品截图） |
| 系统防护 | 可以提供文件监控与防护功能，且支持防护模式和监控模式进行切换，需支持指定受保护路径以及例外路径的设置；支持对保护路径内的文件提供文件的读取、写入、重命名、链接、删除、执行、创建等权限控制功能，支持对保护路径内提供例外进程功能；（提供产品截图） |
| 网络防护 | 支持防端口扫描功能，且可设置单个IP请求时间范围、最大扫描端口数量、IP锁定事件等信息；所投产品需支持微蜜罐功能，且可设置返回文本信息以及监听端口。（提供产品截图） |
| 安全防护 | 支持对Agent进行统一管理，包括：Agent降级，Agent暂停，Agent异常重启，Agent安装的版本、可升级的版本占比情况进行统计，并可对Agent版本进行更新和同步，Agent性能保护。（提供产品截图） |
| 资质要求 | 产品支持IPv6，提供全球IPv6测评中心颁发的IPv6 Ready Logo 认证证书。 |
| 产品具备国家网络与信息系统安全产品质量监督检验中心颁发的信息技术产品安全测试证书。 |
| 产品具备中国网络安全审查技术与认证中心颁发的“IT产品信息安全认证证书”。 |
| 投标产品原厂具备中国网络安全审查技术与认证中心颁发的数据安全管理认证证书。 |

#### **（十）第三方测评**

提供对“温州公安大数据安全防护体系（软件）”的检测，主要对系统的功能性、可靠性以及易用性进行检测。

# **第四部分** **评审办法**

评审办法前附表

| **条款号** | **评审因素** | | **评审标准** | | |
| --- | --- | --- | --- | --- | --- |
| 1 | 评审办法 | | 本次评审采用综合评分法，综合评分法是指响应文件开启后满足采购文件全部实质性要求，且按照评审因素的量化指标评审得分最高的3名磋商供应商为成交候选人的评审方法。 | | |
| 2.1 | **▲资格审查** | | 2.1.1提供符合参加政府采购活动应当具备的一般条件的承诺函及有效的企业营业执照（或事业法人登记证书或其它工商等登记证明材料，自然人提供身份证)复制件（如为联合体，则联合体各方均应提供）； | | |
| 2.1.1落实政府采购政策需满足的资格审查材料： 无； | | |
| 2.1.3本项目的特定资格要求审查材料： 无； | | |
| 2.1.4商业信誉审查：  至本项目响应截止时间止未列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。（代理机构以响应文件开启当日在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）网页查询记录为准）  对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的磋商供应商，其磋商响应将作无效响应处理。 | | |
| 2.2 | **▲符合性审查** | | 磋商小组在评审过程中根据本“第四章评审办法”2.3.1~2.3.3条款规定的符合性审查内容要求对响应文件的有效性、完整性、响应文件的响应程度审查。  符合性审查其他要求： 无 | | |
| 2.3 | 比较与评价 | | 🗹采用综合评分法 | | |
| 2.3.1 | 分值权重构成 | | 磋商小组将对各磋商供应商的磋商报价、技术或服务水平、履约能力、售后服务等和业绩情况等方面进行综合评审，磋商小组各成员应当独立对每个有效磋商供应商的响应文件进行评价、打分。  各磋商供应商的综合得分为：最终报价得分+商务技术得分之和，总和为100分，其中：其中商务技术 80 分（商务技术权值 80 %），报价20分（价格权值 20 %）。 | | |
| 2.3.2 | 商务技术评分  标准 | 评审因素 | 评审标准 | 分值 | 备注 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | 供应商  综合实力 | 1、磋商供应商具有ISO9001质量管理体系认证得1分；  2、磋商供应商具有ISO27001信息安全管理体系认证得1分；  3、磋商供应商具有ISO20000信息技术服务管理体系认证得1分；  4、磋商供应商具有GB/T 27922-2011售后服务能力（五星级）认证的得1分。  （需提供全国认证认可信息公共服务平台（http://cx.cnca.cn/CertECloud/result/skipResultList）查询结果截图作为证明材料，未提供或证明材料不完善的不得分）。 | 4 | 客观分 |
| 经验业绩 | 磋商供应商自2022年1月1日（以合同签订最晚落款时间为准）以来具有类似网络安全项目案例的每个得1分，最高得3分。  注：需提供合同等证明材料复印件，否则不得分。 | 3 | 客观分 |
| 现状理解 | 磋商供应商对于本项目的业务现状、实施目标、建设内容的理解全面、充分，有利于项目目标的实现的情况进行评分。（评分范围：4,3,2,1,0） | 4 | 主观分 |
| 响应情况 | 对采购文件采购需求中“服务内容与技术要求”的符合情况进行评价打分：完全符合采购文件的要求的得30分，打“★”的条款每不满足一条扣2分，未打“★”的条款每不满足一条扣1分，分值扣完为止。 | 30 | 客观分 |
| 项目团队情况 | 1、投标供应商所投入的项目负责人具有网络规划设计师、信息系统项目管理师、网络与信息安全工程师，每提供一项证书得1分，最高得2分。 2、投标供应商所投入的技术负责人具有证书信息系统项目管理师、系统规划与管理师的，每提供一项证书得1分，最高得2分。 3、投标供应商所投入的安全负责人（一名）具有信息安全工程师、网络工程师、信息安全管理证书的，每提供一项证书得1分，最高得2分。 4、投标供应商所投入的项目组团队人员拥有安全防范工程师、中级系统集成项目管理工程师的，每提供一项证书得1分，最高得1分； （注：①以上全体人员证书签发机构应为人力资源和社会保障部及其下设机构（厅、局、鉴定中心等）或工业和信息化部及其下设机构（厅、局、教育与考试中心、标准化研究院等）或中国信息安全测评中心，否则不得分。②本项目组人员（除负责人）同一个人最多计算一种证书；③以上项目人员需提供完整有效的证书扫描件加盖公章，并提供投标截止时间前近三个月及以上在投标单位的社保证明扫描件加盖公章，不提供社保证明扫描件不得分。 | 7 | 客观分 |
| 组织实施方案 | 磋商供应商对于本项目的组织实施方案全面、充分，有利于项目目标的实现的情况进行评分。（评分范围：3，2,1,0） | 3 | 主观分 |
| 重点难点分析 | 磋商供应商对于本项目的重点难点分析全面、充分，有利于项目目标的实现的情况进行评分。（评分范围：2,1,0） | 2 | 主观分 |
| 服务方案 | 根据磋商供应商对于本项目漏洞扫描方案的全面、充分、科学合理情况进行评分。（评分范围：3,2,1,0） | 3 | 主观分 |
| 根据磋商供应商对于本项目代码检测方案的全面、充分、科学合理情况进行评分。（评分范围：3,2,1,0） | 3 | 主观分 |
| 根据磋商供应商对于本项目渗透测试方案的全面、充分、科学合理情况进行评分。（评分范围：3,2,1,0） | 3 | 主观分 |
| 根据磋商供应商对于本项目应急响应方案的全面、充分、科学合理情况进行评分。（评分范围：3,2,1,0） | 3 | 主观分 |
| 根据磋商供应商对于本项目重点时期保护方案的全面、充分、科学合理情况进行评分。（评分范围：3,2,1,0） | 3 | 主观分 |
| 根据磋商供应商对于本项目攻防演练大赛与攻防演练工具提供方案的全面、充分、科学合理情况进行评分。（评分范围：3,2,1,0） | 3 | 主观分 |
| 根据磋商供应商对于本项目攻防演练与攻防演练培训方案的全面、充分、科学合理情况进行评分。（评分范围：3,2,1,0） | 3 | 主观分 |
|  |  | 质量保障方案 | 磋商供应商对于本项目的质量保障方案全面、充分，有利于项目目标的实现的情况进行评分。（评分范围：3,2,1,0） | 3 | 主观分 |
|  |  | 售后服务方案 | 磋商供应商对于本项目的售后服务方案全面、充分，有利于项目目标的实现的情况进行评分。（评分范围：3,2,1,0） | 3 | 主观分 |
| 2.3.3 | 报价评分标准 | | （1）满足采购文件要求且报价最低的投标报价为评标基准价，其价格分为满分。  （2）其他磋商供应商的投标价格得分按以下公式计算：  投标报价得分=（评标基准价/有效评标价）× 价格权值 ×100（四舍五入，保留小数点后2位） | | |
| 落实政府采购政策需进行的价格扣除 | | 1）小微企业（含监狱企业、残疾人福利性单位）报价扣除 10 %，即评标价=投标报价× 90 %；  2）价格扣除比例或者价格分加分比例对小型企业和微型企业同等对待，不作区分。小型、微型企业、监狱企业、残疾人福利性单位不重复享受价格扣除政策。  3）未提供完整证明材料的，不享受价格扣除优惠政策  **注：专门面向中小企业采购的项目或者标项，不再执行价格评审优惠的扶持政策。** | | |