漳州片仔癀国药堂医药连锁有限公司
网络安全服务项目公开比选公告

我司为加强网络安全建设，拟进行网络安全服务项目采购，欢迎符合条件的公司参加比选，具体比选信息如下：

一、比选单位名称：漳州片仔癀国药堂医药连锁有限公司

二、比选项目名称：网络安全服务项目公开比选

三、采购内容：

1、网络安全服务（详见附件 1：网络安全服务项目采购清单）

技术和服务要求：

1. 中选方需负责各项相关网络安全。

2. 提供的网络安全服务必须等于或高于网络安全服务的规格要求。

3. 提供网络安全相关运维服务，包括但不限于中选方上门服务时，中选方需提供 7*24 的上门维修服务。

四、参与比选的公司资质要求：

1、具有独立承担民事责任的能力，参选时应提交营业执照复印件；

2、具有履行合同所必须的技术和服务的能力；

3、参选企业须提供厂家对参选企业的授权书(或独家支持函、支撑单位声明等)证明材料。授权方需为系统备案地所在省市级或市级以上网安或网信的技术支撑单位，并提供证明材料；

4、为保证服务质量，参选公司人员需配备 1 名中级以上(含中级)工程师作为项目经理，负责本次项目总沟通协调工作。

5、保证提供的一切材料真实、有效；

6、本比选项目不接受联合体参选；

7、未提供《参选方关联企业情况声明》的按作废处理。

五、参与比选的公司需报送资料内容包括：

1、企业资质(加盖公章):提供营业执照等相关资质文件;

2、团队实力(加盖公章):提供项目团队人员具备的专业技术证书复印件;

3、报价单(加盖公章):按附件 2 规定格式填写;

4、比选承诺函(加盖公章):按附件 3 规定格式填写;

5、参选方关联企业情况声明(加盖公章):按附件 4 规定格式填写。

6、实施方案:提供详细的等级保护测评实施方案。

7、参选企业须提供厂家对代理商的授权书、独家支持函、支撑单位声明等证明材料。

8、其他材料要求请参考附件 5《评分标准》。

六、比选要求

1、参选文件须密封送交至漳州片仔癀国药堂医药连锁有限公司，外封套应写明:参选公司的全称、地址、项目名称，并在骑缝上加盖公章。

2、参选文件寄出截止时间：2025 年 11 月 20 日 17 时 30 分（以参选文件寄出时间为截止时间），并于文件寄出当天 17 点 30 分前将快递单号信息发送至邮箱：gytxx@pzhgyt.com。

3、参选文件寄送地址：企业管理部 17720920575 福建省漳州市芗城区琥珀路 1 号 2 幢片仔癀大厦三楼（请在包裹外部备注“国药堂网络安全服务项目”）。

4、参选文件份数:正本一份、副本一份。

七、评审办法

1、评审小组:由漳州片仔癀国药堂医药连锁有限公司相关部门人员组成。

2、比选暂定时间为:2025 年 11 月 25 日(若有特殊情况则以实际为准)。

3、比选地点:漳州片仔癀国药堂医药连锁有限公司。

4、中选方式:根据评审小组评分，综合得分最高者中选。若得分相同者，则取报价低者为第一中选候选人。

八、合同签订

1、中选人确定后比选人将于3日历天内通知中选公司。

2、签订合同

中选人在收到比选人的中选通知书后3日历天内，应按比选文件的要求，以报价单中的报价为合同金额，与比选人签订合同。如果中选人未按规定与比选人签订合同，则视为放弃中选，参选人须向比选人赔偿中选金额的20%为违约金。如果给比选人造成的损失超过赔偿金额的，还应当对超过部分予以赔偿，同时依法承担相应法律责任。出现此种情形，按照确定的中选候选人顺序，比选人可以向第二中选候选人授选。

九、联系方式

不明之处请咨询:安全部（信息与网络安全组），0596-2937016，邮箱:gytxx@pzhgyt.com。

漳州片仔癀国药堂医药连锁有限公司

2025年11月14日

附件 1：网络安全服务项目采购清单

序号	服务类型	服务内容	交付物	频率
1	渗透测试服务	1. 提供安全渗透检测服务，由专业安全人员模拟入侵者所用的常见手段对测试目标发起模拟入侵的过程，高强度的检测系统安全漏洞提供安全漏洞修补建议。对 web 等进行模拟攻击测试，获取相关权限,包括暴力破解、溢出攻击、监听、SQL 注入、XSS、业务测试等手段，获取相关权限,测试以获得权限为目的；对新业务系统做上线前安全检测，分析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，并以此识别信息系统的安全风险，提出相应的整改方案。 2. 根据整改报告协助督促各产商整改，直至解决落实所有的解决方案。帮助单位预防和解决潜在的安全风险，保障业务系统上线后安全。	《渗透测试报告》	1 次/年/3 套系统
2	基础环境评估服务（漏扫+基线）	1、通过评估工具以本地扫描的方式对评估范围内的系统和网络进行安全扫描，从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和威胁。 2、采用最佳配置核查实践对操作系统、数据库、中间件、网络设备、网络安全设备进行配置核查。	《安全漏洞扫描报告》 《安全基线检查报告》	1 次/季度
3	攻防演习防守服务	为“护网”、“攻防演习”中防守单位提供支撑服务，做到事前现场资产梳理与风险检查，事中监测分析与应急处置，事后总结与安全加固，在实战中有效提升网络安全保障能力。	《攻防演习防守日报》 《攻防演习防守总结》 《攻防演习防守工作方案》	按需/年
4	互联网资产发现/企业网络资产排查	通过数据挖掘和调研的方式确定企业资产范围，之后基于 IP 或域名，采用各类探测技术，对信息系统相关的主机/服务器、安全设备、网络设备、工控设备、WEB 应用、中间件、数据库、邮件系统和 DNS 系统等进行主动发现，并生成资产及应用列表，列表中不仅包括设备类型、域名、IP、端口，更可深入识别运行在资产上的中间件、应用、技术架构的详细情况（类型、版本、服务名称等）。	《互联网资产排查报告》	1 次/年
5	安全运营服务	通过 7*24 小时安全监测，发现网络流量中的网络安全攻击、网络安全脆弱性等问题，并将检测数据回传至安全运营平台进行监测分析。	事件分析报告	全年
		基于资产发现、流量安全检测、威胁情报，以及人工数据录入等安全数据，由专业安全技术人员基于攻防视角进行全面地监测分析，对各类安全告警事件开展手工验证，并根据相关规则优化分析能力，提高分析结果的准确性，及时发现掌握业务应用系统的安全状况，分析内容包括网页漏	事件分析报告	

序号	服务类型	服务内容	交付物	频率
		洞利用分析、网络攻击分析、数据库安全分析、恶意软件分析、密码爆破行为分析等。		
		对用户上报的安全事件进行及时响应，通过对异常流量、攻击日志及病毒日志分析，实时发现安全事件并协助用户进行处置闭环，帮助客户快速恢复业务，消除或减轻影响。	事件分析报告	
		根据用户实际运营情况，输出安全运营月报。	安全运营月报	
6	安全巡检服务（含服务器主机加固）	派遣专业技术人员在现场对网站系统，服务器和网络安全设备进行安全检查，进行木马查杀、攻击日志分析、漏洞扫描等手段全面核查分析，发现高风险问题，及时开展安全加固工作。加固工作包含: 1、提供服务器安全加固服务，提供加固工具，工具可实现对云端与本地服务器的统一运维管理、安全策略维护及全网安全日志分析、威胁溯源等。 2、通过服务器加固工具，实现安全加固操作系统和应用，有效防御服务器的黑客入侵和恶意代码，并提供微隔离、资产清点、风险管理、补丁管理、基线检查、攻击溯源等一体化服务器安全加固服务。 3、加固工具首页界面支持展示资产数量显示，包含服务器、进程、web 框架、数据库、账户、软件应用、口、网络连接、web 服务、安装包等显示。 4、加固工具支持根据策略对病毒文件进行检测和告警，对病毒样本基本库至少能检测其中的 95%。对病毒样本流行库至少能检测其中的 98%，对误报样本库的误报率不能超过 0.1%。支持对虚拟化环境中统一检测的策略管理，避免统一检测对虚拟化环境应用造成影响。	《安全巡检报告》	2 次/年
7	日常应急响应服务	1.当发生安全事件时，及时进行响应。提供专业安全工程师协助进行问题溯源分析，查找问题来源，进行应急处理，提供相关报告和改进优化建议。 2.支撑方式：可远程或现场方式，大故障或者重大故障必须提供现场支撑。 3.时效性：5 分钟内电话响应，30 分钟内远程响应支撑，需现场支撑事件要求 2 小时内现场支持。	《应急响应报告》	全年
8	安全通告预警	安全预警是定期以邮件或当面沟通形式向用户通告业内安全态势、重大舆情信息、重要系统漏洞及补丁信息等:对于紧急重大类漏洞信息，以最快时间通过邮件或电话向客户告知漏洞危害、影响范围及应对方案等。	《安全通告》	全年

序号	服务类型	服务内容	交付物	频率
9	安全培训	内容涵盖安全领域的各个多面，通过安全专题培训的学习和配套的教学实验，进一步提高客户对信息安全工作的重视，加强提升信息安全主管部门专业化工作水平，保障业务连续稳定。	《全员安全意识培训 PPT》	1 次/年
10	网络安全等级保护测评服务(三级)(含等保咨询服务)	1、等保咨询是一种协助客户建立等级保护体系并通过等保测评的咨询服务。等保咨询服务遵循《信息系统安全等级保护实施指南》协助客户从系统定级、差距评估、方案设计、建设整改、系统测评五个方面进行等保体系的建设，达到符合国家等级保护的基本要求，顺利通过测评中心测评的目标。 2、测评机构须依据国家《中华人民共和国计算机信息系统安全保护条例》(国务院 147 号令)、《信息安全等级保护管理办法》(公通字[2007]43 号)、《信息安全技术网络安全等级保护基本要求 GBT22239-2019》、《信息安全技术网络安全等级保护测评要求 GBT28448-2019》等法规要求进行信息系统安全等级测评并出具《等级保护测评报告》。	《系统定级备案 表》 《专家评审报告》 《差距分析报告》 《制度体系》 《整改报告》 《等级保护测评 报告》	1 次/年/ 1 套系统

附件 2：网络安全服务项目报价表

序号	服务类型	服务内容	交付物	频率	报价（元）
1	渗透测试服务	1. 提供安全渗透检测服务，由专业安全人员模拟入侵者所用的常见手段对测试目标发起模拟入侵的过程，高强度的检测系统安全漏洞提供安全漏洞修补建议。对 web 等进行模拟攻击测试，获取相关权限，包括暴力破解、溢出攻击、监听、SQL 注入、XSS、业务测试等手段，获取相关权限，测试以获得权限为目的；对新业务系统做上线前安全检测，分析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，并以此识别信息系统的安全风险，提出相应的整改方案。 2. 根据整改报告协助督促各产商整改，直至解决落实所有的解决方案。帮助单位预防和解决潜在的安全风险，保障业务系统上线后安全。	《渗透测试报告》	1 次/年	
2	基础环境评估服务（漏扫+基线）	1、通过评估工具以本地扫描的方式对评估范围内的系统和网络进行安全扫描，从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和威胁。 2、采用最佳配置核查实践对操作系统、数据库、中间件、网络设备、网络安全设备进行配置核查。	《安全漏洞扫描报告》《安全基线检查报告》	1 次/季度	
3	攻防演习防守服务	为“护网”、“攻防演习”中防守单位提供支撑服务，做到事前现场资产梳理与风险检查，事中监测分析与应急处置，事后总结与安全加固，在实战中有效提升网络安全保障能力。	《攻防演习防守日报》《攻防演习防守总结》《攻防演习防守工作方案》	按需/年	
4	互联网资产发现/企业网络资产排查	通过数据挖掘和调研的方式确定企业资产范围，之后基于 IP 或域名，采用各类探测技术，对信息系统相关的主机/服务器、安全设备、网络设备、工控设备、WEB 应用、中间件、数据库、邮件系统和 DNS 系统等进行主动发现，并生成资产及应用列表，列表中不仅包括设备类型、域名、IP、端口，更可深入识别运行在资产上的中间件、应用、技术架构的详细情况（类型、版本、服务名称等）。	《互联网资产排查报告》	1 次/年	
5	安全运营服务	通过 7*24 小时安全监测，发现网络流量中的网络安全攻击、网络安全脆弱性等问题，并将检测数据回传至安全运营平台进行监测分析。	事件分析报告	全年	

序号	服务类型	服务内容	交付物	频率	报价（元）
		基于资产发现、流量安全检测、威胁情报，以及人工数据录入等安全数据，由专业安全技术人员基于攻防视角进行全面地监测分析，对各类安全告警事件开展手工验证，并根据相关规则优化分析能力，提高分析结果的准确性，及时发现掌握业务应用系统的安全状况，分析内容包括网页漏洞利用分析、网络攻击分析、数据库安全分析、恶意软件分析、密码爆破行为分析等。	事件分析报告		
		对用户上报的安全事件进行及时响应，通过对异常流量、攻击日志及病毒日志分析，实时发现安全事件并协助用户进行处置闭环，帮助客户快速恢复业务，消除或减轻影响。	事件分析报告		
		根据用户实际运营情况，输出安全运营月报。	安全运营月报		
6	安全巡检服务（含服务器主机加固）	派遣专业技术人员在现场对网站系统，服务器和网络安全设备进行安全检查，进行木马查杀、攻击日志分析、漏洞扫描等手段全面核查分析，发现高风险问题，及时开展安全加固工作。加固工作包含: 1、提供服务器安全加固服务，提供加固工具，工具可实现对云端与本地服务器的统一运维管理、安全策略维护及全网安全日志分析、威胁溯源等。 2、通过服务器加固工具，实现安全加固操作系统和应用，有效防御服务器的黑客入侵和恶意代码，并提供微隔离、资产清点、风险管理、补丁管理、基线检查、攻击溯源等一体化服务器安全加固服务。 3、加固工具首页界面支持展示资产数量显示，包含服务器、进程、web 框架、数据库、账户、软件应用、口、网络连接、web 服务、安装包等显示。 4、加固工具支持根据策略对病毒文件进行检测和告警，对病毒样本基本库至少能检测其中的 95%。对病毒样本流行库至少能检测其中的 98%，对误报样本库的误报率不能超过 0.1%。支持对虚拟化环境中统一检测的策略管理，避免统一检测对虚拟化环境应用造成影响。	《安全巡检报告》	2 次/年	
7	日常应急响应服务	1.当发生安全事件时，及时进行响应。提供专业安全工程师协助进行问题溯源分析，查找问题来源，进行应急处理，提供相关报告和改进优化建议。 2.支撑方式：可远程或现场方式，大故障或者重大故障必须提供现场支撑。 3.时效性：5 分钟内电话响应，30 分钟内	《应急响应报告》	全年	

序号	服务类型	服务内容	交付物	频率	报价（元）
		远程响应支撑，需现场支撑事件要求 2 小时内现场支持。			
8	安全通告预警	安全预警是定期以邮件或当面沟通形式向用户通告业内安全态势、重大舆情信息、重要系统漏洞及补丁信息等:对于紧急重大类漏洞信息，以最快时间通过邮件或电话向客户告知漏洞危害、影响范围及应对方案等。	《安全通告》	全年	
9	安全培训	内容涵盖安全领域的各个多面，通过安全专题培训的学习和配套的教学实验，进一步提高客户对信息安全工作的重视，加强提升信息安全主管部门专业化工作水平，保障业务连续稳定。	《全员安全意识培训 PPT》	1 次/年	
10	网络安全等级保护测评服务（三级）(含等保咨询务)	1、等保咨询是一种协助客户建立等级保护体系并通过等保 测评的咨询服务。等保咨询服务遵循《信息系统安全等级保 护实施指南》协助客户从系统定级、差距评估、方案设计、 建设整改、系统测评五个方面进行等保体系的建设，达到符 合国家等级保护的基本要求，顺利通过测评中心测评的目 标。 2、测评机构须依据国家《中华人民共和国计算机信息系统 安全保护条例》(国务院 147 号令)、《信息安全等级保护 管理办法》(公通字[2007]43 号)、《信息安全技术网络安 全等级保护基本要求 GBT22239-2019》、《信息安全技术网 络安全等级保护测评要求 GBT28448-2019》等法规要求进行 信息系统安全等级测评并出具《等级保护测评报告》。	《系统定级备案 表》 《专家评审报告》 《差距分析报告》 《制度体系》 《整改报告》 《等级保护测评 报告》	1 次/年/1 套系统	
报价费用总计（元）：					

参选方：（盖章）

报价人：

日　期：

附件 3

比选承诺函

致:漳州片仔癀国药堂医药连锁有限公司

我方_____(参选单位名称)，在此作如下承诺:

1、完全理解比选公告的一切规定和要求。

2、报价在有效期内持续有效。

3、若中选，我方将按照比选公告及我方报价文件的具体规定与贵公司签订网络安全服务项目协议，并按项目的要求提供相应的服务，按时完成网络安全服务工作。

4、在整个询价、报价过程中及结束后，未经贵单位书面同意，我方若有违规、违约行为，我方将按合同承担违约责任。

5、在整个询价、报价过程中及结束后，未经贵公司书面同意，我方保证不向任何第三方泄露本次询价、报价的任何信息、资料及内容。

6、报价文件中所有关于报价单位资格的文件、证明、陈述均是真实的、准确的。若有违背，我方承担由此而产生的一切后果。

7、本比选文件符合国家有关监管要求。

8、本承诺函与法律服务协议具有同等法律效力。

9、我方对在此次比选过程中获取的贵公司的信息和数据负有保密义务，未经贵公司允许不得透露给第三方。

10、近三年未曾受到监管部门处罚，其服务对象也未曾因报告涉及的相关事项违反国家规定接受处罚。

11、经初步调查，我方及我方相关参与职员与漳州片仔癀国药堂医药连锁有限公司及其关联方不存在股权等利益关系。

比选单位:

负责人或授权代表:(签字)

日期:

附件 4

参选方关联企业情况声明

我公司郑重声明如下，

1、参选方名称：

2、本公司的直接控股、管理关系情况和直接下级控股、管理关系情况

直接上级控股、管理单位名称	对本单位的控股（出资）比例(%)	单位负责人	联系电话	单位地址
……				
直接下级控股、管理单位名称	对本单位的控股（出资）比例(%)	单位负责人	联系电话	单位地址
……				

属于同一直接上级控股、管理单位的其他兄弟单位情况

其他兄弟单位名称	对本单位出资比例（%）	单位负责人	联系电话	单位地址
……				

我公司郑重承诺：如未提供或经核实未如实填写本公司的控股、管理单位情况，将被按作废处理。

参选方名称(加盖公章)：

法定代表人或授权代表(签字或盖章)：

日期：

说明：若无关联企业，则在上述表格中填写“无”。

附件 5

漳州片仔癀国药堂医药连锁有限公司
网络安全服务项目评分标准

1、价格项(35 分)

比选内容及标准	分值
价格分=35*(1-|(参选公司报价-所有参选公司平均报价)/所有参选公司平均报价|)， 计算分数时四舍五入取小数点后 2 位数。	35 分

2、商务项(30 分)

比选内容及标准	分值
参选企业注册资金≥1000 万，得 2 分， 500 万≤注册资金<1000 万，得 1 分， <500 万，不得分。	2 分
参选单位具备风险评估三级认证(需提供相关证明材料)。	5 分
具备省级或以上网络与信息安全信息通报中心支撑单位证书(需提供相关证明材料)。	
具备安全运维三级认证情况(需提供相关证明材料)。	
在本项目实施过程中人员配备情况(需提供相关证明材料)。	3 分
为保障项目实施顺利，提供与漳州片仔癀药业股份有限公司及其下属公司的合同或其他合作证明材料(需提供相关证明材料)。	2 分
为了保证项目的顺利实施，确保项目质量达到预期目标，等保测评人员要求情况(需提供相关证明材料)。	6 分
为保证测评现场具有应急技术处理能力，供应商所采用测评机构须获得过系统备案地所在省市级或市级以上网安或网信的技术支撑单位聘书(需提供相关证明材料)。	6 分
在本项目实施过程中组员要求：项目组成员具有至少两份 CISP 认证，CISP 认证项目经理须具备 PMP 认证与 CISP 认证（相关人员需提供近三月社保证明，否则不记入有效人员）。	6 分

3、技术项(35 分)

比选内容及标准	分值
提供项目解决方案，包括但不限于如下几点：项目背景与目标、需求分析、解决方案设计、风险管理、测试与验收、部署与维护、文档与培训。	5 分
提供项目实施计划，包括但不限于如下几点：项目概述、项目范围、资源管理、任务分解、风险管理、沟通计划、质量管理、交付与验收、维护与支持。	6 分

参选人须注明本次渗透测试服务厂商（需提供服务厂商相关平台官网截图及网址并加盖投标人公章证明且必须持有厂商代理证书）： （1）服务厂商须提供安全服务配套在线漏洞情报检索平台，支持关键漏洞≥1.9 万、全量漏洞检索≥18 万； （2）全量漏洞支持按照危险等级、补丁情况、POC|EXP、CVSS 分数、漏洞年份、定级情况、关键漏洞、漏洞利用集成状态、漏洞收录时间、在野利用等 15 项查询条件进行查询。	3 分
参选人使用的渗透工具应具有如下功能（应提供相关截图证明）： （1）可选择是否启用 Autopwn，选择漏洞检测场景，配置端口范围等；提供完整的 SDK 和使用说明文档，并提供代码自动生成功能，可以快速编写插件； （2）支持完善的插件提交、插件审核、插件导入功能，无延迟载入插件库；提供一键进行漏洞高级功能利用，包括执行命令、执行 SQL、上传文件、反弹 Shell、上传 GTWebshell、下载文件等。	3 分
加固工具首页界面支持展示资产数量显示，包含服务器、进程、web 框架、数据库、账户、软件应用、端口、网络连接、web 服务、安装包等显示。（证明材料需由国家互联网信息办公室、公安部、工业和信息化部、国家认证认可监督管理委员会四部门发布的《承担网络关键设备和网络安全专用产品认证》中检测机构出具的检测报告）。	3 分
提供服务器安全防护服务工具，该工具支持： 根据策略对病毒文件进行检测和告警，对病毒样本基本库至少能检测其中的 95%。 对病毒样本流行库至少能检测其中的 98%，对误报样本库的误报率不能超过 0.1%。 支持对虚拟化环境中统一检测的策略管理。 （证明材料需由国家互联网信息办公室、公安部、工业和信息化部、国家认证认可监督管理委员会四部门发布的《承担网络关键设备和网络安全专用产品认证》中检测机构出具的检测报告）。	3 分
支持基于系统扫描的结果，下发 Web 深度扫描任务，能够针对 Web 和系统扫描的结果深入的进行风险综合分析（需提供功能截图）； 内置扫描任务报表、基线检查报表、资产报表、漏洞报表、对比报表和自定义报表模板； 自定义的维度包括且不限于资产（主机存活性、主机指纹、端口、web 指纹等）、漏洞（修复方案、CVSS 评分、漏洞细节、漏洞描述、漏洞危害、影响范围等）进行筛选（需提供功能截图）； 支持 html、Word、excel、pdf 等多种格式报表导出。	3 分
开展护网服务，合同期内，在市委网信办、市网安等上级部门明确的重要时期，按照文件要求制定网络安全保障方案；按方案要求提供人员驻守应急支撑；交付成果：《攻防演习防守方案》、《攻防演习前安全检查报告》、《攻防演习值守日报》、《应急处置报告》、《攻防演习工作总结汇报》；报告周期：以上级部门通知要求为准； 实战攻防演习期间提供，流量监测工具，具备网页漏洞利用检测、webshell 上传检测、网络攻击检测、威胁情报检测能力，提供以上功能截图及流量监测工具提供承诺函； 流量监测工具，支持基于工具特征的 WEBSHELL 检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：中国菜刀变形、小马上传工具、小马生成器等。	2 分
IP 地址管理：支持对系统内自动发现及人工录入的 IP 地址进行管理，维度包含但不限于查看 IPV4 地址、IPV6 地址、端口数、域名数、运营商、位置、ASN、来源依据、分组、标签等，支持对已发现的 IP 地址进行筛选、删除、聚合和下载等操作，筛选维度包含但不限于发现日期、更新日期、IP 地址、网段、运营商、位置、ASN 编号、来源、发现依据、分组、标签等维度；支持自动识别 WAF、CDN、企业邮箱、云存储等相关资产并生成标签； 漏洞详情：支持查看漏洞详情，展示维度包含但不限于漏洞 ID、漏洞等级、漏洞名称、漏洞类型、检测方式、受影响资产、CVE 编号、CVND 编号、CNNVD 编号、CVSS 评分、漏洞证明过程、漏洞描述、扫描对象、漏洞证明过程、漏洞危害、缓解建议、发现时间、跟进时	4 分

间、复测状态、跟进记录等；支持漏洞结果导出报告、分享链接等操作。	
1、投标人必需提供服务门户 portal 账户，且门户至少具备如下主要功能（需提供功能截图）： 事件查看与检索：通过 portal 账号登录服务门户查看事件列表，其中按状态划分，状态为待处置、已处置、处置中三中状态，支持查看的事项列表信息有事项名称、事项类型、责任单位、采购人名称、紧急程度、危害程度、下发时间、响应时长、整改次数等内容； 事项处置管理：支持对事项进行流程化处置，其中支持上下级单位的事项下发与确认，事件处置、审核意见、事项退回、事项复测等操作，支持跟踪事项全流程节点动态； 资产查看与检索：支持查看采购人下关联的 ip 资产、设备资产、网站资产、应用系统；支持以树形式查看关联的资产；支持查看所有资产的详细信息，服务门户资产暂不支持修改，数据有运营管理平台进行数据同步 待确认资产：支持由 portal 账号端主动录入待确认资产信息，数据同步至运营管理端，由管理端执行资产运营入库动作； 所提供的的服务门户应支持当前我司探针设备接入，或由供应商自行提供与服务门户相匹配的探针设备。	3 分