附件 1：建设清单

序号	平台名称	建设内容	功能模块	主要技术参数	单位	数量
1	潮团年会支撑平台	年会系统	小程序软件开发服务	1.系统首页： 精心打造系统首页，塑造独特且吸引人的视觉风格，同时对整个界面进行美化处理，确保界面的美观性与易用性。合理规划并设置一级和二级栏目，优化信息架构，提升用户导航体验。 2.报名： （1）立即报名：参与者只需简单填写姓名、手机号和身份证号，选择参与的角色，即可立即完成报名流程。过程简短便捷，确保每位有兴趣的参与者都能轻松参与。 （2）报名确认：一旦完成报名流程，系统将自动发送确认通知，明确告知参与者报名已成功及具体细节。 （3）信息审核：为确保活动的严肃性与安全性，将对所有报名信息进行严格审核，防止虚假信息的流入，保障活动的真实性与合法性。 （4）报名信息概览：报名信息页面直观展示了所有参与者的报名状态、姓名、联系方式等关键信息，使组织者能够轻松掌握活动报名情况，确保管理的便捷性与高效性。 3.签到： （1）提供便捷签到功能，支持手工签到方式，确保签到的准确性和灵活性。 （2）关联后台，在后台自动生成详细的会务报表，为活动组织者提供有力的数据支持。 4.会务通知： （1）公告发布：建立有效的公告发布渠道，及时传达活动变更、重要通知等信息。确保用户第一时间获取关键资讯，提升活动透明度与参与度。 （2）公告管理：全面管理公告内容，包括发布、修改、删除等操作。确保信息及时更新，保持准确性，为用户提供可靠的活动资讯与服务。 5.后台报表生成： （1）支持将报名信息、签到信息生成详细的会务报表； （2）支持将报表导出为 Excel 或其他常用格式，有助于快速制作活动名单或通讯录。 6.行程安排与管理： 联络员建立行程，对行程进行安排，包括行程类型、时间、到达站点、行程备注、参会人员等信息的录入，使得主办方第一时间获取参会人员行	项	1

序号	平台名称	建设内容	功能模块	主要技术参数	单位	数量
				程信息，可以及时做出活动安排及调整，有效提升活动透明度与参与度。 7.酒店预订与管理： 展示丰富的酒店房型信息，提供便捷的酒店预订服务，为参会人员提供更多的住宿选择。 （1）房型展示：展示房型信息、数量、价格； （2）房型详细展示：以图文的方式展示房间的具体信息，方便嘉宾选择； （3）预定：选择房型为嘉宾预定酒店。 后台展示已预订酒店的团体的名称、房型、预订数量、联系人、团体名称、酒店名称、可居住人数、联系电话、操作日期等信息，支持操作删除功能。 8.基础资料管理：团体信息录入及更新、用户管理，支持团体信息的录入和用户管理。 9.数据上传与管理： 实现人员数据的自动保存和上传功能，以会议为单位进行数据的分类管理，确保数据的安全性和可追溯性。 10.报表生成与查询： 根据系统收集的数据，自动生成详细的参会人员报表，并提供强大的搜索查询功能，方便活动组织者快速获取所需信息。 11.用户统计： 对小程序和网页的登陆用户进行精准统计，为活动的推广和运营提供数据依据，以便更好地了解用户行为和需求。		
2			申请与备案	全面收集小程序和网页的申请资料，按照相关规定进行国内和国外双备案申请，并完成系统的部署工作，确保系统符合法律法规要求。		
3			小程序资料录入与更新	完成平台资料（参会人员报名，酒店安排、行程安排等）的录入和更新工作，保证系统数据的及时性和准确性。		
4		云相册	照片上传	具备权限的用户通过小程序上传图片。	项	1
5			图片审核	组委会审核图片，发布合规图片，退回、删除不合规的图片。		
6			图片展示	用户通过小程序，查看图片列表和制定图片。		
7			图片存储	提供≥50G 安全存储空间。		
8		云服务器	前端服务器	CPU≥4、内存≥16GB、系统盘≥100G、公网带宽≥10M	台	1
9			应用服务	CPU≥4、内存≥16G、系统盘≥100G、公网带宽≥	台	1

序号	平台名称	建设内容	功能模块	主要技术参数	单位	数量
			器	10M		
10			数据库服务器	CPU≥4、内存≥8G、存储空间≥300G、数据库版本 mysql 8.0	台	1
11		安全服务	云防火墙	1.支持 VTEP（VxLan Tunnel EndPoint）模式接入 VxLAN 网络，并可作为 VXLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通;支持通过绑定 VLAN、VNI(VXLAN Network Identifier)、远程 VTEP,手动管理 VxLan 网络；支持 MAC、VNI、VTEP 静态绑定； 2.支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能； 3.路由协议：支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于 12 种路由负载均衡方式，支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP 等方式的链路探测,同时 TCP 与 HTTP 可使用自定义目标端口进行测试； 4.支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件等方式告警，支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查； 5.支持应用识别,应用特征库包含的应用数量(非应用协议的规则总数）大于 2800 种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类； 6.支持多调度类相互嵌套最大 5 级的带宽管理设置。支持设置每 IP 最大或最小带宽，支持对每 IP 进行带宽配额管理，可通过优先级实现多应用的差分服务，并支持对剩余带宽进行基于优先级的动态分配； 7.支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP	台	1

序号	平台名称	建设内容	功能模块	主要技术参数	单位	数量
				Flood 攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC 反弹技术）、授权服务器防护（NS 重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施； 8.安全规则库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息； 9.支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，并可同时基于安全域、IPv4 和 IPv6 地址进行例外设置动作，可以设置解密或不解密，同时支持将解密后流量镜像到其他设备进行分析统计； 10.支持网络异常感知、安全事件分析、策略与处置、运维管理等功能，提供中英文双语管理界面，并在登录页面可选择 Web 页面使用的语言。		
12			云主机安全	1.支持自带高性能数据库，不需要额外单独采购数据库； 2.支持 windows/linux 主流操作系统； 3.支持无代理部署模式及有代理部署模式； 4.支持 Bitdefender、QOWL、云查杀、支持灵活开启或停用引擎；支持病毒文件自动隔离、自动删除、修复、监控多种处理方式。支持病毒查杀的结果生成报告； 5.支持启发式引擎、云查杀引擎、增强引擎、QDE（人工智能引擎）灵活开启、停用； 6.支持应用程序控制功能，可基于黑白名单方式对授信/风险程序进行控制，当主机完整性发生变化时，提供报警以及追踪痕迹功能，支持提供漏洞管理功能，针对扫描、识别的漏洞风险； 7.支持对应用协议的内容进行解析和识别，包括应预置应用分类协议库，针对分类配置阻断、允许策略； 8.提供数据中心威胁态势感知，大屏动态展示安全运维状况，结合地理位置信息全面呈现威胁攻击详情；支持按总流量、恶意流量、新建连接对流量进行统计和展示进行统计和展示；支持按照不同分组、虚拟机/终端、网络协议、网络协议组、国家/地区、城市，分不同威胁类别以柱状图、折线图（曲线图）、饼图、地图、原始日志等形式	个	3

序号	平台名称	建设内容	功能模块	主要技术参数	单位	数量
				进行展示；支持手动或者定时定期生成报表。		
13			云 web 应用防火墙	1.支持 HTTPS 服务器透明以及反向代理模式防护； 2.支持对 CPU、内存、硬盘的使用情况进行监控，并以实时图形化展示，同时可以基于自定义时间段进行历史数据查询； 3.支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标资产、安全防护攻击类型、攻击趋势、HTTP 并发请求及实时事件的统计； 4.支持爬虫防护、黑链防护，可设置防护检测级别和例外 URL； 5.支持业务流程控制，可设置处理动作（封禁、通过、阻断、重定向），并可以设置封禁时间，可设置优先级、有效时间、保护 URL、Referer URL 等规则，并允许 Referer 为空； 6.支持智能分析 DDOS 防护，内置≥五个防护等级，并可自定义防护等级； 7.支持移动端对资产的一键断网功能，提供网站一键下线以及批量下线的应急措施； 8.内置机器学习引擎，针对业务建模，可通过学习 URL、host 等信息展示网站结构树形图，并支持对 URL 的访问量和响应健康度进行图形化统计； 9.支持对接第三方 Radius 服务器认证系统，支持登录密码转换，防止密码明文传输； 10.支持系统运行状况表、安全状况总表、安全状况分表导出，支持自定义分析维度进行报表导出，分析维度包括攻击趋势、攻击严重级别、被攻击资产、被攻击 IP、攻击源 IP、攻击源地域等。	台	1
14			云防篡改	1.支持提供自我保护机制，网页防篡改客户端需有卸载密码方可卸载； 2.支持与同品牌 WAF 产品实时联动功能，配合实现针对篡改攻击的阻断功能，支持连线/断线状态下的篡改检测； 3.支持防护模式和监控模式两种模式的防篡改模式； 4.支持在断线情况下对网页文件目录的防护功能； 5.支持文件多线程同步，并可以设置文件空闲同步时间周期、发布时间周期等设置； 6.支持日志超出阈值告警，可设定日志存储空间	个	1

序号	平台名称	建设内容	功能模块	主要技术参数	单位	数量
				的告警阈值。		
15			云综合日志审计	1.基于大数据分析架构，具备高效性、实时性、灵活性和扩展性；通过 SSL 加密的 web 方式对本系统实现管理； 2.支持采集网络流量，解析协议不少于 ICMP、AMQP、Cassandra、DNS、HTTP、MySQL、Thrift、MongoDB、NFS 等，并且可以自定义监听端口； 3.提供 TOP10 资产告警事件趋势，支持动态展示事件总数与管理资产总数等基础信息，通过饼装图、折线图、柱状图图形化展示事件收集趋势、告警事件趋势、告警事件类型等相关重点信息。并支持资产总数、日志事件总数、系统健康状况的下钻查看详情； 4.支持自动生成主机访问关系图谱。关系图谱支持无限级延伸，支持拓展上下一级后自动绘制访问关系；支持关系图谱搜索、过滤，支持自定义关系节点图标;支持基于节点下钻查看日志信息、查看和拓展该点关系图等;对单位内的设备类型、应用类型、协议类型等信息为基础，梳理出设备、应用、协议等之间的访问关系，实时树立访问关系；支持根据内置事件类型，按照用户环境需求，定义无限级深度事件模型，绘制全网事件关联关系模型,提供基于模型而非特征的问题发现能力，辅助发现未知威胁;对单位服务器开放端口关系、服务器端口连接关系、服务代理关系、P2P 模型关系等； 5.对单位内的设备类型、应用类型、协议类型等信息为基础，梳理出设备、应用、协议等之间的访问关系，实时树立访问关系； 6.支持根据时间范围、级别、告警类型、告警全文关键字等方式快速检索安全事件告警； 7.支持添加对应的日志资产，资产可单独配置不同的接收方式，资产配置过程中可根据资产类型自动挂载对应的解析规则，无需重复操作，单一资产可挂载多个资产类型，可针对单一资产进行日志编码格式调整,编码格式不限于 UTF-8、GB/T 2312-1980、GBK 等。	台	3
16			云数据库审计	1.可支持小型、大型虚拟化云平台环境的审计，可支持软交换镜像，与云平台进行关联配置，达到虚拟化引流效果； 2.支持大数据 Hbase、solr、redis、MongoDB 等数据库； 3.支持创建用户配置应用部门，审计对象可配置	台	1

序号	平台名称	建设内容	功能模块	主要技术参数	单位	数量
				应用部门，达到不同用户管理不同审计对象； 4.支持数据库绑定变量审计、函数审计(sum 求和函数等）； 5.支持重复操作的统计审计规则，可根据在一定的时间内，重复某项操作达到设定的统计次数进行规则审计告警； 6.支持自定义报表，支持 Word、PDF、xls 格式报表导出； 7.提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身审计功能 8.提供审计数据管理功能，能够实现对审计数据的自动备份，支持增量、全量备份方式； 9.支持对 SQL 注入、跨站脚本攻击等 web 攻击的识别与告警。		
17			云堡垒机	1.支持微信小程序动态口令认证方式登录堡垒机，且当用户需要使用手机令牌登录时，需要强制绑定手机令牌； 2.支持 RADIUS、AD 域、LDAP、OIDC、CAS 等认证类型； 3.支持认证方式组合使用，例如使用 AD 域+手机短信、AD 域+Radius 认证、Radius 认证+手机令牌等多种组合方式登录，支持按用户访问的源 IP 地址进行不同的认证方式，例如内网可直接密码登录，外网 VPN 拨号接入需要使用双因子； 4.具备账号密码的防暴力破解功能，支持登录失败次数锁死设置，可自定义尝试密码次数，可设置锁定用户账号或 IP，可设置锁定时长，到期自动解锁或管理员手动解锁，可设置登录尝试密码失败之后，将登录尝试失败计数器重置为 0 次所需要的时间时长； 5.支持用户的登录时间、来源 IP 地址和来源 MAC 地址限制（黑名单或白名单），限制非法时间和非法地址登录堡垒机； 系统内置部门管理员、策略管理员、审计管理员、运维员等角色，并支持按模块和功能自定义角色权限，便于管理，用于复杂的业务场景需求；支持角色权限细粒度划分，包括新建部门、安全配置、网络配置、HA 配置、端口配置、外发配置、认证配置、工单配置、告警配置、系统风格等权限划分； 6.支持用户信息的批量修改，包括重置密码、移动部门、更改角色、删除网盘数据、解除手机令	台	3

序号	平台名称	建设内容	功能模块	主要技术参数	单位	数量
				牌、修改多因子配置、修改有效期、修改登录时间段限制、修改 IP 限制、修改 MAC 限制； 7.支持对部门设置 AB 段安全码，AB 段安全码由 2 个管理员保管，可使用 AB 段安全码对导出的敏感数据进行加密，解密时需要 2 个管理员同时解密； 8.可通过 Linux 应用发布的方式实现对火狐浏览器、Chrome 浏览器、达梦数据库、人大金仓数据库等的扩展支持； 9.支持对 MySQL、Oracle 和达梦数据库的访问操作进行控制，可基于库、表、命令实现对数据库操作的细粒度访问控制，执行动作包括但不限于断开连接、拒绝执行、动态授权、允许执行； 10.内置 OpenVPN 客户端。		
18			云漏洞扫描	1.支持自适应网络扫描，根据网络状况自动控制发包速率，避免影响用户网络； 2.支持 340000 条以上系统漏洞库，并按照漏洞类别及漏洞威胁程度进行分类； 3.系统应支持以树形结构展示网站目录结构，并在网站目录树子页面中展示该网页上存在的漏洞数量及详情，便于直观确定漏洞位置； 4.系统应支持 Web 登录认证扫描，支持基于 Cookie 认证、Form 认证、Basic 认证、NTLM 认证、Session 认证、Digest 认证的 Web 应用系统扫描； 5.支持至少三种漏洞验证方式如浏览器验证、注入验证、通用验证； 6.系统应支持对漏洞扫描结果标记不同状态，区分新建、已修复、误报等状态； 7.系统应支持 Web 弱口令检测，包含 http、https 类型的 web 弱口令检测，并且支持自定义请求页面的 URL 及响应内容的关键字，口令字典支持组合模式和标准模式并能够自定义访问端口及扫描频率； 8.系统能够检测中间件弱口令，包含但不限于：Tomcat、WebLogic、JBoss、WebSphere、GlassFish；系统能够检测摄像头弱口令：包含但不限于大华、华为、宇视、海康摄像头弱口令； 9.系统支持主机存活探测功能，支持标准、快速、全部和指定四种端口探测范围，支持 CONNECT 全连接扫描和 SYN 快速扫描两种 TCP 端口扫描方式； 10.系统应支持自定义对资产打标签，并支持根据标签进行检索。	台	1

序号	平台名称	建设内容	功能模块	主要技术参数	单位	数量
19		等保服务	等保服务	根据《中华人民共和国网络安全法》要求，配合、协助采购人对小程序进行网络安全定级、备案、测评工作。	项	1
20		会务服务	服务内容	资料录入与更新：提供专业人员配合会务组提供人员资料录入服务(服务期 20 天)，完成会务资料的录入和更新工作，保证系统数据的及时性和准确性。	项	1
21		短信服务	短信服务	提供短信服务套餐，包含≥78000 条短信，用于向报名人员及时传递潮团年会的会议通知、活动安排等重要信息，确保参会人员能够及时了解活动动态。	项	1

附件 2：报价函格式

报　价　函

我单位对该项目的报价内容无任何异议，现附报价表如下：

采购名称	总报价（元）
潮团年会支撑平台及会务服务项目	￥
金额（大写）　拾　万　仟　佰　拾　元　角　分	

注：本报价函包含服务费、人工费、材料费、管理费、采购、运输保管、安装、税金等及采购过程中未能预见的一切费用。

附：报价明细表

响应供应商法定代表人（签字或盖章）：

响应供应商名称（签章）：

日期：　　年　　月　　日

附：报价明细表格式

序号	平台名称	建设内容	功能模块	主要技术参数	单位	数量	单价	总价
1								
2								
3								
…								
合计（元）								

响应供应商法定代表人（签字或盖章）：

响应供应商名称（签章）：

日期：　　年　　月　　日