附件1

长江产业投资集团网站集约化项目

建设规范要求

一、功能要求

##### （一）渠道管理

##### **1.站点管理**

提供站点分类管理，支持对分类进行增、删、改的操作。

支持多站点独立管理，各网站自主维护，包括站点栏目、模板、用户、权限等。不同站点向不同的目标WEB服务器分发，支持虚拟主机方式的内容分发。

支持通过TXT文档导入多个站点、栏目，实现网站栏目的快速创建与维护，栏目层次和数量没有限制。

站点拥有自己频道及栏目结构、页面布局设置、用户配置、权限管理等，支持多类型的数据传输和任务分发。

支持选择模板、向导式复制建站功能，提高建站效率。

支持对手机网站（HTML5网站、手机APP）进行管理和属性设置。

**2.微信管理**

支持微信公众号的绑定、分组以及公众号操作权限的设置操作，面向管理人员提供服务。

##### （二）文档管理

系统提供对网站、APP、微信、IPAD等服务终端的一体化采编功能，支持所见即所得的高适配预览，支持一键排版、一键发布、一键撤稿功能；提供微信可视化的图文式混编混排及组稿功能。

实现编辑内容的所见即所得，可即时查看页面预览效果。

支持文档录入、浏览、修改、删除、导入、导出等操作，文档可调整排序位置，具有文档引用、复制、移动操作功能。

文档录入支持复制、粘贴功能，可添加多幅图片及文档附件，支持插入超链接、表格、图片、符号、HTML 代码、音频、视频等元素。

支持从Word 文档中直接拷贝内容粘贴到编辑器中，并可根据情况选择是否过滤掉无关的格式代码。

内容采编支持文章录入、外部链接、附件下载等方式。

文档录入支持一键转载。

支持自动生成摘要和关键词。

图片缩略图能根据不同的尺寸要求进行灵活引用、并支持正文图片在线裁剪、添加水印。

微信采编，支持图、文、音视频混编混排功能，支持微信组稿编辑功能，支持微信素材管理功能。支持对应稿件发送到指定帐号进行预览。

##### （三）文档审核

待编、待审状态的文档支持由具有相关权限的用户进行送审、送签。待审、待签状态的文档，若审核未通过，可以由具有相关权限的用户打回。其中，待审状态的文档只能打回到待编状态，待签状态的文档可以选择打回到待编或待审，默认打回到上一级待审状态。

##### （四）稿件发布

提供完全发布、快速发布、更新发布、独立发布、撤销发布等操作。

支持定时发布功能，可以设定自动发布的时间。

提供完善的发布监控功能。

##### （五）栏目管理

栏目是站点内容组织分类的模块，稿件按照栏目分类进行发布、存储与管理。

栏目管理具体应实现下列功能：

1.系统可清晰展现栏目结构和站点归属的关系，并提供多种栏目导航方式，方便用户查找及相应管理操作。

2.系统应实现栏目管理对信息发布良好支撑，支持栏目复制、隐藏、移动、导入和导出管理等功能。

3.栏目支持直接连接到外部链接，可满足不同栏目的发布需求。

4.栏目支持RSS聚合，搜索引擎SEO优化管理功能。

##### （六）模板管理

支持所见即所得的模板编辑工具，可实现鼠标拖拉的页面设计，无需写代码。

提供丰富的栏目和功能资源模块，可实现页面内容与风格的灵活配置。

支持模板的预览、备份、恢复、复制等功能。

模板支持专题、新闻回顾、在线直播、嘉宾访谈等特殊的定制效果。

支持模板语法自动检查。

提供模版权限管理功能。

支持模板导入、导出功能，模板的导入支持的格式有zip、asp、jsp、xml、htm、html。

##### （七）信息发布

支持站点发布、分级栏目发布、信息单独发布等发布操作，并可以指定文档发布后在页面显示的顺序。

可支持静态化发布、动态发布和动态静态相结合多种发布方式。

支持压缩、加密发布，支持Zip压缩算法的信息发布管理。

##### （八）信息智能处理

考虑到对海量信息的集中管理与维护，为提高编辑效率，降低政治风险，系统需要提供文档智能处理功能。管理员可启用或关闭自动抽取摘要和关键字智能处理功能。

自动抽取摘要和关键词：点击自动摘要按钮，系统根据当前文档的内容自动抽取摘要和关键词，并且将抽取的结果直接显示在关键词和摘要文本框中。用户可以在抽取摘要后再进行手动修改。

##### （九）用户管理

支持用户管理和组织机构管理，实现不同的用户分级。

##### （十）权限管理

支持按各类用户角色预设置权限，如平台角色、站点角色、栏目角色等。

支持权限分级管理、分级下放。

##### （十一）在线调查

可以通过互联网及调查系统把传统的调查过程在线化、智能化，并做出深度分析，最终形成专业调查报告。

##### （十二）智能检索

支持模糊检索、搜索词辅助提示、拼音检索、整句检索等搜索。后台提供多站点索引管理、排序权重、检索模板、词典管理等功能。

##### （十三）日志管理

日志需要记录系统中一个操作发生时相关的信息数据。日志管理模块需要记录所有操作，做到有据可查，也能根据需要通过多种方式对记录的操作日志进行检索和查询，主要包括日志的管理和日志的浏览。

操作日志共分为如下几种：

操作日志：记录用户操作事件，例如新建、查询、修改等操作。

发布日志：记录用户执行的发布事件，例如文档发布、站点发布等操作。

分发日志：记录服务器端文档调整的事件，例如新建或修改服务器端的文件等操作。

安全日志：记录用户的登录情况，何时登录、何时退出，已经IP等信息。

系统日志：记录用户操作过程中的异常、警告、调试信息以及性能相关的日志信息。

##### （十四）文档统计

查看所有可见站点的文档统计情况。统计类型包括：部门统计、站点统计、发稿人统计、作者统计、栏目统计、来源统计。

##### （十五）敏感词管理

敏感词设置能对文档中出现的敏感词进行检测和替代，减少人工核实的工作量，保证文档质量。（词库按年计费）

二、技术规格要求

##### （一）整体架构

系统架构：计划建设一个集团级的网站系统。系统能够实现网站系统全部核心功能建设，在充分考虑招标方已建和建设中的计算机应用系统基础上，在充分保护原有软硬件设备投资的前提下，提供完整的系统解决方案。同时考虑平台的先进性，提供高于目前使用场景的架构解决方案，满足随着业务不断发展对性能、功能的高要求。

遵循标准：遵循J2EE、XML、JDBC、EJB、SNMP、HTTP、SFTP、TCP/IP、SSL等业界主流标准，前端框架应使用目前较流行的Vue.js，Angular.js，React.js等。

易实现：产品平台化，具有快速灵活的基础架构，功能扩展性强，便于二次开发。系统具有较强的配置功能，对于新对接业务系统（除在系统实现的特殊场景定制化开发）原则上要求不需要新开发程序，采用拖拉、配置的方式即可实现对接，对常用参数提供灵活配置，如系统参数配置、报表参数配置，以及可能涉及到的审批流程等各种流程配置。

性能指标：系统本身应不对用户数量进行限制，成交方在系统设计上应充分考虑采购方目前的用户规模、业务需求，在保证系统服务质量的前提下，设计系统规模、软件功能和业务功能相适应的系统，支持采购方未来业务发展的需求。

运行管理：提供日常运行监控和完整的系统维护管理方案，提供图形化交易日志收集、审计和分析系统进行系统问题查找，支持对接集团监控系统。

数据备份：应提供系统数据的备份、恢复方案和历史数据及日志的归档清理机制，避免数据量过大影响性能。

数据标准：系统应符合集团数据治理标准，配合集团数据标准落地。

安全性：各功能模块中数据的存储、传输、下载、分析、应用等过程必须具有加密功能或设置严格的权限控制，密码等敏感信息的加密存储应支持国密加解密，并且支持业内主流加密机厂商的产品对接，确保数据不重复、不遗漏、不丢失、不被窃取和篡改。文件传输必须用安全的传输协议（如：sftp）禁用ftp等进行文件传输。

权限管理：系统设置多种用户管理权限，可设置、可调整、可扩充。

用户管理：有不同类型的操作用户和管理用户，按不同的数据级别或权限使用系统。

##### （二）性能要求

1、不限制系统注册用户数，系统性能不小于1000TPS。

2、系统响应迅速及时，系统登录，打开、刷新页面的响应时间在1秒内，一般的报表展示查询，查询响应时间不大于3秒。

3、实时匹配响应时间应能满足业务系统要求，不影响对接业务系统正常交易。

##### （三）系统监控要求

1、系统监控方案需符合集团系统运维管理规范，方便系统维护人员查看应用系统运行中的各项静态和动态信息，监控系统的运行情况，并满足接入集团集中监控平台的要求。

2、提供完善的日志管理功能，以支持系统的维护和运作管理。

3、提供系统操作日志，支持操作的可追溯与可审计。

##### （四）扩展性要求

1、应用系统应具备模块化、参数化和插件式特征，对接业务系统采用参数配置化，交互界面模板化的方式。

2、业务功能和管理功能及系统配置提供高度参数化，方便灵活。

3、解决方案充分考虑功能模块扩展，比如采用组件化设计。

4、系统开发时应考虑到其开放性，以能够方便地实现扩充满足新的业务需求。

##### 三、网络安全等保环境要求

本项目运行所依赖的安全环境必须满足三级等保要求，需提供以下服务，报价清单中需包含以下内容。

##### （一）服务清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务名称 | 服务内容 | 数量 | 备注 |
| 1 | 防火墙 | 详见技术服务参数及要求 | 2 | 台 |
| 2 | WEB应用防火墙 | 详见技术服务参数及要求 | 2 | 台 |
| 3 | 堡垒机 | 详见技术服务参数及要求 | 1 | 台 |
| 4 | 数据库审计 | 详见技术服务参数及要求 | 1 | 台 |
| 5 | 漏洞扫描 | 详见技术服务参数及要求 | 1 | 台 |
| 6 | 网页防篡改 | 详见技术服务参数及要求 | 1 | 套 |
| 7 | 态势感知系统 | 详见技术服务参数及要求 | 1 | 套 |
| 8 | 备份系统 | 详见技术服务参数及要求 | 1 | 套 |
| 9 | 服务器杀毒 | 详见技术服务参数及要求 | 1 | 套 |
| 10 | 三级等保安全测评服务 | 详见技术服务参数及要求 | 1 | 项 |
| 11 | 网络安全改造技术服务 | 详见技术服务参数及要求 | 1 | 项 |

##### 详细技术服务参数要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务名称 | | | 主要规格、技术参数 |
| （一）防火墙 | | | | |
| 1 | 规格性能 | | | 端口：≥8个10/100/1000M自适应电、≥6个SFP插槽、≥4个SFP+插槽；  性能：吞吐量≥10Gbps，并发连接≥180万，每秒新建连接≥10万/秒；  授权及服务：3年硬件维保服务、3年病毒防护特征库升级服务、3年入侵防御特征库升级服务。 |
| 2 | 部署模式 | | | 支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备；支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式。 |
| 3 | 内容过滤 | | | 支持邮件内容过滤功能，有效防止恶意邮件及信息外泄。可根据邮件SMTP命令、发件人、主题、附件、IP及邮件大小进行邮件过滤。 |
| 4 | 访问控制 | | | 支持一体化安全策略：可基于安全域、MAC地址、IP地址、服务、时间、用户、应用等属性，配置防病毒、入侵防御、内容过滤、URL过滤、文件过滤、Web防护、SSL解密、弱密码防护、防暴力破解、会话老化时间等高级访问控制功能；支持图形化整体策略展示效果。 |
| 5 | 漏洞扫描 | | | 漏洞扫描支持产品内置的默认模板以及自定义模板进行漏洞扫描，可扫描出漏洞名称、漏洞级别、漏洞描述、CVE-ID、CNNVD-ID等信息；支持查看资产关联的漏洞信息，并跳转到详情。 |
| 6 | 入侵防御 | | | 系统预定义超过11000条主流攻击规则，包含对应IPS规则的级别、防护对象、操作系统、CVE编号等详细信息。 |
| 7 | Web防护 | | | 支持独立的Web防护模块，系统定义超过4500条WAF规则防护功能，支持常规HTTP漏洞、SQL注入、组件、CMS、WebShell和XSS等类型的Web防护；支持HTTP协议的URL、Method、Referer、User-Agent、Cookie、URL-args等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制。 |
| 8 | 应用识别 | | | 系统定义最大超过6200种主流应用，支持识别多种主流应用，支持应用自定义并对自定义的应用进行分组，支持根据标签选择应用，支持自定义应用的导入和导出。 |
| 9 | 威胁情报 | | | 支持通过关键IP、域名、文件HASH在线检索威胁情报并查看威胁详情。支持检测C&C、勒索软件、僵尸网络、挖矿软件、矿池地址等安全攻击类型。 |
| 10 | 规则升级 | | | 支持单独的恶意样本检测规则升级功能，方便对恶意样本检测功能进行扩充。 |
| 11 | 黑名单 | | | 黑名单容量规格支持最大100万条。 |
| （二）WEB应用防火墙 | | | | |
| 1 | 硬件参数 | | | 端口：≥6个10/100/1000M自适应电口，≥8个千兆SFP插槽，≥2组bypass，≥1个扩展插槽；  性能：网络吞吐量≥6Gbps，应用层处理能力≥1.5Gbps，网络并发连接数≥120万，HTTP并发≥80万，HTTP新建连接数≥15000/s；  授权及服务：Web安全保护≥128个站点，三年WAF软件特征库服务，三年硬件维修服务。 |
| 2 | 基本功能 | | | 具备专业的Web应用安全防护能力，实现对跨站脚本（XSS）、注入式攻击（包括SQL注入、命令注入 、Cookie 注入等）、跨站请求伪造等应用攻击行为防护，发现威胁即刻进行拦截。 |
| 3 | 客户端防护 | | | 支持客户端安全防护，能够通过WAF向服务器返回信息插入特殊的HTTP报头（包括X-Frae-Options、X-Cantent-Type-Options、Content-Security-Policy）以保护客户端免受相应攻击）。 |
| 4 | Web服务自发现 | | | 支持自动发现网络环境中存在的Web业务系统，记录服务器的IP、Port、域名等信息。 |
| 5 | 应用防护 | | | 支持客户端安全防护，插入特殊的HTTP报头以保护客户端免受某些攻击包括但不限于增加以下安全报头：X-Frame-Options（用于防护客户端免受Clickjacking攻击）、X-Content-Type-Options（以防止浏览器将文件解释为内容类型声明以外的其他内容）。 |
| 6 | HTTPS防护 | | | 支持HTTPS站点SSL算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果。 |
| 7 | 机器学习 | | | 支持设定学习的周期，域名信息，可信任的客户端IP，不可信的客户端IP以及不学习的URL信息。 |
| 8 | CC防护 | | | 支持对CC攻击进行检测和防护，能够配置URL参数、请求头部字段、目的IP、请求方法、地理位置组成的匹配条件;能够对请求速率、请求集中度、请求离散度进行检测；支持从请求头字段获取真实源IP地址。 |
| （三）堡垒机 | | | | |
| 1 | 规格性能 | | | 端口：≥6个千兆电口，≥2个扩展槽位；  性能：支持≥150路图形会话或≥400路字符会话并发；  授权及服务：三年标准售后服务、授权100个被管资源数，不限制运维用户数量。 |
| 2 | 部署模式 | | | 支持HA部署、双活部署模式，审计数据能自动同步至备机，可自定义是否同步录像审计；支持多台堡垒机异地备份部署，每台设备都能提供运维和审计服务，配置数据自动同步；支持集群部署模式，中心可采用HA，节点可以横向扩展，实现统一登录入口、统一配置同步、审计日志集中存储、实时会话集中监控，以满足业务增长需求。 |
| 3 | 身份认证 | | | 系统提供身份认证，自然人（员工帐户）登录系统时支持静态口令、Radius认证、LDAP、AD域、数字证书认证、动态令牌认证、USBKEY认证。 |
| 4 | 运维协议  支持 | | | 支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin、X11；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具。 |
| 5 | 数据库协议运维代理 | | | 标准支持DB2、Oracle、MySql、SQL Server、PostgreSQL、KingbaseES、DM、GBase8a、GBASE8s的协议运维代理，可实现自动登录，自动登录可直接调用本地windows系统的数据库客户端工具（包括ssms、sqlwb、DBeaver、mysqlcli、MySQLWorkbench、MySQLFront、DbVisualizer、PLSQL、SQLPlus、Toad、ToadforDB2、db2cmd、QuestCentral、pgAdmin3、psql、Ksql、Isql、DIsql、DMmanger、GBaseDateStudio、navicat系列等），无需应用发布前置机。 |
| 6 | 自动化运维 | | | 支持自动化编排能力，通过编排动作流的方式，对目标资产进行定时或周期性的自动化运维。动作流可包括：上传文件、执行命令、下载文件等。动作流会按设定好的顺序进行执行，对于常见的运维工作，如升级、巡检等，均可通过此能力快速执行。 |
| （四）数据库审计 | | | | |
| 1 | 规格性能 | | | 端口：≥6个千兆自适应电口，≥4个SFP接口，扩展槽≥1个；  性能：SQL审计处理能力（速率）≥40000SQL/S  授权及服务：提供三年硬件维修服务，数据库实例授权数≥16个。 |
| 2 | 数据库类型 | | | 支持Oracle（包括21C及其他版本）、Clickhouse、MySQL、SQL Server、Sybase ASE、DB2、Informix、Cache（包括2021及其他版本）、 PostgreSQL（14及其他版本）、Vastbase、Teradata、MariaDB、Hana、LibrA、Sybase IQ、TiDB、Vertica、PolarDB、PolarDB-X、Percona-MySQL、Percona-MongoDB等主流数据库的审计；支持达梦、南大通用（GBase）、高斯（GaussDB）、人大金仓、K-DB、神舟通用（Oscar）、OceanBase、HighGo DB、天翼云数据库Teledb-MySQL、天翼云数据库Teledb-PostgreSQL等国产数据库的审计；支持MongoDB、HBase、Hive、Redis、Elasticsearch、Cassandra、HDFS、Impala、Graphbase、Greenplum、Spark SQL、SSDB、ArangoDB、Neo4j、OrientDB 等数据库的审计。 |
| 3 | 过滤规则 | | | 支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则或规则白名单；支持在设置日志检索条件时，检索条件可根据历史信息自动弹出，即输入检索条件时支持智能联想。 |
| 4 | 报表自定义 | | | 支持自定义报表，自定义报表支持告警名称、告警等级、操作类型、操作系统用户名、数据库名/实例名、主机名、数据库账号、客户端IP、客户端工具、数据库类型、客户端端口11种统计维度，支持来自审计日志、告警日志、会话日志的29种统计指标，根据以上条件进行灵活选择后生成报表。 |
| 5 | 资产组管理 | | | 支持资产组管理；对于与产品相关的关联数据，支持分组管理，分组管理包含IP组、数据库账号组、应用用户组、时间组、对象组。 |
| （五）漏洞扫描 | | | | |
| 1 | 硬件参数 | | | 端口：千兆电口≥6个，扩展插槽≥2个；  性能：Web扫描任务并发数为5个域名。系统扫描IP地址支持1024个，支持扫描A类、B类、C类地址，系统扫描≥50个IP地址并行扫描；  授权及服务：提供3年漏洞特征库升级，提供3年软、硬件维保服务。 |
| 2 | 系统架构 | | | 系统为B/S架构，并采用SSL加密通信方式，用户可以通过浏览器远程访问设备，方便用户操作，支持多用户同时登录操作。 |
| 3 | 漏洞特征库 | | | 漏洞特征库大于230000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。 |
| 4 | 漏扫设备 | | | 支持对各种网络主机、操作系统、网络设备（如交换机、路由器、防火墙等）、常用软件以及应用系统的识别和漏洞扫描。支持扫描云平台的漏洞，覆盖OpenStack、KVM、VMware、Xen等主流的云计算平台。 |
| 5 | 扫描协议 | | | 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。 |
| 6 | Web应用漏洞扫描 | | | 提供Web应用漏洞扫描功能，支持常见Web漏洞类型的扫描，包括SQL注入、跨站脚本、命令执行、命令注入、代码注入、弱口令、目录遍历、URL跳转、文件包含、反序列化漏洞、文件上传、CSRF跨站请求伪造、信息泄露等。支持OWASP TOP10等主流安全漏洞。 |
| 7 | 数据库支持 | | | 支持Oracle、MySQL、SQLServer、DB2、Informix、PostgreSQL、Sybase、达梦、人大金仓的授权数据库漏洞扫描。数据库扫描的漏洞库数量大于3000条。漏洞知识库与CVE、CNNVD等国际、国内漏洞库标准兼容。 |
| （六）网页防篡改 | | | | |
| 1 | 性能参数 | | | 可管理终端数量≥50点。 |
| 2 | 支持系统 | | | 支持操作系统包括：Windows 2000-2016 32/64位；Redhat、CentOS、SUSE、Ubuntu 32/64位；支持Web服务器包括：Apache 20-24、IIS6、IIS7、IIS8、IIS10、Java系列（JBoss、Tomcat、Weblogic、Websphere）等；支持数据库包括：MSSQL、Oracle、Sybase、Informix、DB2、MySQL等关系型数据库；Mongodb、Cassandra等非关系型数据库。 |
| 3 | 系统展示 | | | 支持展示Web服务器的系统信息、监听端口、运行进程、账号（包括隐藏账号）等信息。 |
| 4 | 阻断拦截 | | | 支持通过配置IP或页面路径，对特定的访问者或页面进行放行或拦截。 |
| 5 | 文件防护 | | | 支持文件名解析漏洞防护、禁止浏览畸形文件、敏感信息防泄漏。 |
| 6 | 实时防护 | | | 支持实时防护网站常见的SQL注入攻击、XSS跨站攻击、Web容器及应用漏洞攻击。 |
| 7 | 病毒防护 | | | 支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码。 |
| 8 | 网页文件防护 | | | 支持各类网页文件的保护，包括静态和动态网页以及各类文件信息。 |
| （七）态势感知（平台） | | | | |
| 1 | 规格性能 | | | 提供一台配套平台服务器：2U机架式服务器，CPU:≥2颗 （≥16核心，≥32线程，主频≥2.4GHz ）；内存≥256G DDR4；硬盘：≥2块960G SSD+12\*4TBSATA 3.5；电源：冗余双电源；网口：≥4个千兆电口+2个万兆光口（含两个SFP+多模光模块）；  授权及服务：提供三年产品标准维保服务（含硬盘保留服务），自签收之日起开始计算。平台性能支持扩容，授权200个日志数据源的采集能力。提供3年软件基础维保服务，包括远程技术支持服务，包括用于修复产品问题和功能问题的软件更新服务。提供3年威胁情报失陷情报库更新授权，提供3年威胁情报查询分析授权，提供3年漏洞知识库更新授权。 |
| 2 | 资产发现 | | | 支持人工录入、流量自动发现、主动扫描发现、EDR同步、WEB自动发现、物联网同步等不少于5种的资产数据接入方式；流量自动发现方式能自动识别资产类型，如Web服务器、DNS服务器、邮件服务器、FTP文件服务器等多种类型资产，支持web业务系统自动发现；支持批量确认流量发现的资产；支持提供资产同步标准化接口，支持第三方通过自定义设置同步数据源进行资产同步。 |
| 3 | 资产管理 | | | 安全设备资产管理支持一键访问设备的管理界面、大屏投屏演示及设备原始日志，支持查看设备在线状态；提供未知安全设备发现功能，可自动识别安全设备的设备地址、设备名称、产品名称、来源方式等，支持对设备归属组织架构及设备类型进行的修改。 |
| 4 | 工作台自定义 | | | 工作台支持自定义个性化配置，支持以拖拽组件的方式进行画布页面设置，页面可选组件包括“CVE漏洞利用、SOAR、WEB安全、内网病毒、原始告警、告警监控、安全事件、安全日志、安全设备、工单、平台概览、快速搜索、持续攻击、文件分析、资产管理、风险资产”等，可选组件不少于65个。每个组件均支持点击“收藏组件”按钮进行自定义收藏。 |
| 5 | 态势大屏 | | | 支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示，提供不少于10块大屏展示界面，并可根据“组织架构”筛选大屏展示数据范围，支持自定义大屏轮播时间和大屏轮播顺序。 |
| 6 | 安全运营 | | | 支持监测安全运营情况，包括平台已运行天数、本周告警数、待办工单数、通报数；支持安全监测，监测内容包括已失陷资产数、风险资产数、安全域数量、WEB业务系统数量、资产数量等；支持实时流量监控、日志吞吐量监控、运维告警监控、磁盘容量监控；支持WAF、IDS、防火墙、EDR等安全设备接入情况监测，支持失陷资产、横向威胁、外部态势、威胁狩猎、风险资产、业务全景、关联引擎、情报引擎等一键跳转。 |
| 7 | 规则模型 | | | 平台内置包括规则模型、关联模型、统计模型、情报模型、AI模型等安全分析模型，用户根据实际需求对上述模型进行添加、编辑、删除、复制等；安全分析模型支持自定义新增，新添加的模型可选择适用的作用域，如全局通用、单选机构，如选择单选机构即选择应用的组织架构，可通过字段映射、静态值、模板、表达式等多种方式自定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容。 |
| 8 | 智能检索 | | | 支持智能检索语句分析，支持检索语句的中文、英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；支持将检索语句一键翻译为中文，提高可读性；保留搜索语句历史记录。 |
| 9 | 安全分析场景 | | | 支持主机感染勒索病毒、网站被植入webshell、主机感染挖矿木马、主机感染恶意程序、主机被高危漏洞攻陷、主机被外部远控、内网横向攻击、内网横向探测、主机对外扫描、主机对外攻击、主机被爆破成功、发现APT攻击事件等10种以上的内置安全分析场景，针对分析场景支持至少3个任意字段聚合变量检索。 |
| 10 | 探针管理 | | | 对接入到平台的探针进行统一运维监控，平台上可查看探针注册时间、设备IP、版本信息、许可证信息、数据上送条数、CPU利用率、内存使用率、磁盘使用率、网络流量大小、数据上送条数等，并支持许可的导入和导出。 |
| （七）态势感知（流量探针） | | | | |
| 1 | 部署要求 | | | 为了更大程度发挥统一纳管和安全态势感知平台能力，本次项目使用的安全态势流量感知探针需与新增安全态势流量感知探针及新增安全态势感知系统进行平滑对接。 |
| 2 | 规格性能 | | | 端口：千兆电口≥6个，千兆SFP口≥4个，扩展板卡插槽≥1个；  性能：开启网络流量采集、威胁数据采集和日志上报功能情况下混合流吞吐量≥1Gbps，HTTP并发连接数≥300万，HTTP新建连接速率≥10万/秒；  授权及服务：提供三年全功能特征库升级服务，包括3年硬件维修服务。 |
| 3 | 审计范围 | | | 支持双向流量审计，可对请求和响应内容进行审计；支持IPv4和IPv6网络环境下的部署，可同时对IPv4和IPv6网络流量分析检测。 |
| 4 | 协议解析 | | | 支持解析HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOW V9、TFTP、SRV6、HTTP2、NNTP等协议报文，并提供审计协议类型的端口号配置，可根据需要变更端口号；支持GTP、PFCP、NGAP等5G协议解析和审计；支持识别QQ、WEB、LDAP、FTP、TELNET、SMTP、POP3、SMB、RADMIN、ORACLE、MSSQL、SYBASE、MYSQL、DB2、PostgreSQL、REDIS、MQTT等登录行为；支持多层 VLAN、VXLAN、MPLS、GRE等网络流量的解析检测。 |
| 5 | 告警降噪 | | | 支持自动对系统告警事件降噪收敛处理，以基于实体的事件分类方式，将TOP30异常客户端IP、安全事件发生次数用不同颜色柱状图排序展示，可一键下钻查看原始告警数量及攻击状态；导出报表支持的枚举信息至少包含客户端IP、服务端IP、成功次数、风险次数、事件次数、事件名称、风险级别、攻击状态、首次发生时间、最近发生时间等。 |
| 6 | 告警抑制 | | | 支持告警抑制功能，在重复攻击手段下能够减少相同告警数量，提高用户分析效率，可自行设置告警抑制周期、告警上限、抑制阈值、持续时间、启用维度等。 |
| 7 | 敏感信息 | | | 支持识别流量中的个人敏感信息，包括身份证、银行卡、手机号、港澳通行证等，并展示传输信息的协议、网站域名、URL、客户端IP、服务端IP，便于用户发现敏感信息的传输安全隐患和处置。 |
| 8 | 异常告警 | | | 支持对流量中的数据包、会话连接、重传包、网络报文等状态进行检测，可对业务网络流量传输异常告警；支持异常行为模型，可对流量中的各类数据包进行统计，并通过图表形式展示，便于用户分析网络流量健康状态，支持的数据包类型不少于5种。 |
| 9 | 运营模式 | | | 风险查询支持一键切换运营模式和专业模式，满足不同场景的研判需求。运营模式可自由选择常用条件，如事件类型、风险级别、攻击状态、规则ID、回放包ID、报文、CVE/CNNVD编号等；专业模式支持多语法组合查询，包含但不限于AND、OR、NOTIN、IN、==、!=，专业模式包含数据窃取、恶意文件投递、内部横向扩散等7种常用查询模版外，支持通过历史筛选条件新增自定义模版，方便后续查询使用。 |
| 10 | 深度检测 | | | 支持包含30种以上的深度检测模块，可支持shiro反序列化、蚁剑、哥斯拉、冰蝎3.0、冰蝎4.0等检测能力，且能识别如shootback、TunnaProxy、dnscat2、reGeorg、reDuh、CobaltStrike等隧道通信工具。 |
| 11 | 沙箱逃逸 | | | 支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现，采用多并发沙箱检测技术，集成主流的操作系统winXP、win7、win10、linux等多种检测环境，结合平台内置反病毒引擎和静态分析技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析。 |
| 12 | 数据外送 | | | 具备风险数据外送至第三方平台的能力，支持以KAFKA、FTP、SFTP、SYSLOG数据接口输出风险信息；支持元数据外送至第三方平台的能力，支持以KAFKA、FTP、SFTP、SYSLOG数据接口输出审计信息、会话应用识别信息、会话应用流量统计信息、传输层流量统计、应用层统计信息、登录行为统计信息和文件检测信息。 |
| 13 | 健康度评估 | | | 支持资产风险及健康度评估，支持对资产活跃程度分类，支持对资产分组，可配置资产IP所属的组织和网段，以展示资产层级关系。可自定义配置资产分组属性，包括但不限于资产等级、所属地理位置、内外网属性、单位地址、责任人等。 |
| （八）备份系统 | | | | |
| 1 | 配置 | | | 机型：2U机架式；  CPU：2\*Intel 至强银牌CPU，≥2.2GHz/10核20线程；  内存：≥128GB，系统盘：≥2\*480GB SSD；  数据盘：≥12\*6TB SATA；  阵列卡：≥2GB缓存RAID卡（含掉电保护）；  网络接口：≥2\*1GE 电口，2\*10GE 光口（含多模光纤模块）；  软件授权：50TB后端备份容量授权，支持Windows、Linux、Unix、自主可控等客户端平台，客户端数量不做限制，配置国产平台数据库备份，Oracle RAC集群备份，NDMP备份，数据库实时日志备份，数据库容灾演练模块。  三年硬件维保，三年软件远程支持服务及软件升级服务。 |
| 2 | 资质 | | | ▲备份软件自主研发，提供源代码安全审计证书复印件。 |
| 3 | 保护功能 | 平台兼容性 | | 具备广泛的国产兼容性，包括但不限于达梦、TiDB、AntDB（亚信）、Vastbase、MogDB等数据库，Zstack，华为云Stack等虚拟化平台备份与恢复。提供产品兼容性认证证书。 |
| 4 | 平台安全性 | | ▲支持管理员，审计员、安全员、操作员、监控员、池复制员六员管理模式，角色权限颗粒度最小化，通过角色权限管理保障系统管理操作的安全性，无需人工定义即可开启使用。（需提供相关功能截图并加盖厂商公章） |
| 5 | 文件保护 | | 支持文件、对象存储、Hadoop 资源的作业历史中查看具体备份内容，并支持按文件名搜索。可验证作业实际备份内容与预期结果的一致性，便于备份系统的运维巡检或审计检查。（需提供相关功能截图并加盖厂商公章） |
| 6 | 操作系统保护 | | 支持把Windows 操作系统的备份数据直接生成为VMWare、KVM、H3C CAS等虚拟平台支持数据，通过挂载方式实现即时恢复。 |
| 7 | 数据库应用保护 | | ▲支持DMRWC和DMMPP集群的备份与恢复。支持自动识别达梦集群，提供节点可视化管理，支持恢复到数据库的任意时间点。（需提供相关功能截图并加盖厂商公章） |
| 8 | 性能 | | | ▲支持Oracle高效备份，完全备份平均速率大于1GB/S，提供CNAS盖章的第三方测试报告复印件并加盖制造商公章。 |
| 9 | ▲备份系统集群备份性能≥3GB/S，提供CNAS盖章的第三方测试报告复印件并加盖制造商公章。 |
| 10 | 可管理性 | | 管理方式 | ▲支持批量修改多个备份任务的目标存储池，满足存储设备空间耗尽快速迁移备份任务的需要。（需提供相关功能截图并加盖厂商公章） |
| 11 | ▲支持重删存储池的空间使用图表，显示空间使用和节省率趋势。  支持重删指纹库异常修复和优化，包括指纹库重建和重分片、碎片自动整理机制等，保障重删备份恢复性能。 （需提供相关功能截图并加盖厂商公章） |
| 12 | 资质 | ▲投标产品必须具有全球IPv6测试中心测试颁发的IPv6 Ready Logo认证证书。（提供原厂盖章的证书复印件，及网站查询链接） |
| （九）服务器杀毒 | | | | |
| 1 | 安全防护功能 | | | 支持对CPU使用率监控、内存占用率监控、磁盘读写监控、上下行流量监控。 |
| 2 | 支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端进行熔断。 |
| 3 | 违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意IP，支持黑名单告警和阻断。 |
| 4 | 支持防端口扫描，锁定恶意的端口扫描，并记录告警；提供内核级防火墙（业务间流量东西向隔离）功能，包括IP、端口、协议、流向等细粒度权限控制。 |
| 5 | 支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露；对内网的恶意攻击行为进行识别（漏洞利用、横向移动），可阻断恶意探测行为。 |
| 6 | 防病毒功能 | | | 支持自定义病毒处理方式，包括自动处理、记录、删除。优先对病毒文件进行修复，并且将修复前的病毒文件进行备份。 |
| 7 | 提供专门的勒索风险评估功能；提供专门的针对已知勒索病毒的防御引擎，并提供功能开关项；对于已知勒索病毒确保进程无法启动。 |
| 8 | 提供专门的针对未知勒索病毒的防御引擎，并提供功能开关项。对于未知勒索病毒确保无法加密。支持白名单设置。 |
| 9 | 提供专门的挖矿风险评估工具；提供专门的挖矿实时防御工具，并提供功能开关。 |
| 10 | 支持强力查杀，对于无法普通隔离的病毒文件强制停止进程并隔离或动态移除到删除队列。 |
| 11 | 管理功能 | | | 管理平台支持一键卸载客户端、一键设置客户端卸载密码、一键停止/恢复所有防护、一键解除绑定。 |
| （十）三级等保安全测评服务 | | | | |
| 1 | 整体要求 | | | 投标人应完成信息系统定级报告及定级材料的准备、整理，完成信息系统去公安机关的备案工作。 |
| 2 | 信息系统安全等级保护测评需要的运行环境（如场地、网络环境等）由招标人提供，投标人应详细描述需要的运行环境的具体要求。 |
| 3 | 投标人应提供本次信息系统安全等级保护整改的整体实施方案，包括项目时间安排、阶段性文档提交等，并负责实施整改。 |
| （十一）网络安全改造服务 | | | | |
| 1 | 网络安全改造 | | | 提供网络安全设备和软件等系统的安装、联调、测试、部署和支撑环境（网络、系统）的整体调研评估，技术支持，优化改善、日常运维等服务。 |