1. **采购内容及要求**
2. **项目概述**
	1. 项目背景

随着衢州市围绕着“智慧城市”建设规划有序的推进数字化和智慧化转型，信息化服务和形式也更加的多元化，政务云平台、基于大数据分析与决策一体化的智慧综合管理平台、工业及产业互联网平台等信息基础设施的建设，以及智慧交通、智慧医疗、智慧环保、智慧金融等智慧化应用的开展，信息网络环境日益复杂，所面临的网络安全形势也愈加严峻，对衢州市管理者的能力要求也越来越高。衢州在享受数字化所带来诸多便利的同时，也面临着由数字化所带来的诸多风险，特别是积累的海量政务数据资源，这些数据无疑是衢州乃至国家的重要战略资源，如何确保对这些数据资源的安全可控、合理使用，是衢州市政府在数字化转型过程中必须要对待的重大问题。

因此，建设一体化的城市大脑数据风险管控平台，利用大数据、人工智能等技术，汇聚衢州市各个角落的安全数据资源，在城市关键信息基础设施及重要智慧应用和信息安全领域进行融合计算，实现城市运行的生命体征感知、公共资源的合理调度、科学的决策指挥、安全事件的预测预警，从而快速有效的感知全市信息化相关安全风险并进行有效的预警和智能化调度，开启用“数据说话、用数据决策、用数据管理”的新模式。实现全市网络空间监测、预警、防御、管控的信息安全闭环成为必然。

* 1. 项目建设内容

衢州智慧城市网络安全中心”项目从战略支撑基础、知识库、技术体系、安全服务体系四个维度进行顶层设计，建设内容主要包含：

（一）衢州市智慧城市大数据安全中心，衢州市智慧城市大数据安全中心以网络安全、数据监管治理为切入点，形成安全管理中心，使得整体安全监管形成了一个抓手，符合国家大数据发展战略以及十三五发展规划要求。在对网络安全行为和轨迹进行持续监控和记录、追踪溯源的同时保障以政务数据安全为核心，建立有效支撑衢州市政务数据服务业务的安全体系架构，全面保障政务系统和政务数据的安全。

（二）网络安全协调指挥平台建设，按照浙江省网信办的网络安全协调指挥体系的建设指南，需要建设实时监测、态势感知应急指挥、信息通报、情报分析、检查调查、管理评价、追踪溯源八大业务系统。

（三）视频专网安全防护体建设，前端物联网设备的安全通过安全态势感知和通报预警，及时感知和防护物联网络安全风险，全方位保障视频专网整体的安全稳定；应用安全即城市大脑安全防护，通过可信接入代理实现应用的统一可信接入，提供业务应用访问安全通道服务；根据设备环境、用户行为等数据及可信环境感知状态，动态控制用户的应用访问，保证业务应用访问的安全策略控制及强制实施。实现可信接入。

（四）网络安全研判平台建设，在攻防靶场实战系统进行实战攻击演练，了解信息安全漏洞的特点和危害，提升网安人员网络安全攻防能力、主动进攻能力等提供有效技术支撑。

* 1. 项目建设目标

秉承资源集约化、运转高效化、团队专业化的建设理念，打造一支技术过硬、素质较高、平台先进的安全团队，让衢州成为智慧城市的安全领航者，数字经济的安全守卫者。

通过衢州城市网络安全中心建设，实现城市安全治理能力现代化和安全治理体系现代化，让城市安全决策科学化、安全治理现代化、安全服务集约化、应急处置协同化。实现城市未知威胁分析预判，已知威胁联动处置。通过数据融合创新，赋能网络安全治理数字化、城市安全管理精细化；通过创新人才培养机制，促进城市人才结构调整，激发社会创新创业活力，实现城市数字经济快速发展。

衢州城市网络安全中心以城市数字基础设施、重要数字资产和信息系统为保护对象，以大数据和人工智能为核心技术，以网络安全态势感知、通报预警和协同联动为安全手段，以安全资源的集约化利用为重要原则，以生态化的服务为安全中心运行模式，利用“实时”、“全样”、“精准”的安全大数据建立全程在线、全域覆盖、实时反馈的“城市网络安全态势地图”，从而快速有效的感知、预警、调度、处置全市网络安全风险，提高管理决策的科学性和精准性，提升城市管理效率和应急响应能力，助力城市的数字化转型和数字经济发展。

构建衢州市数字资产安全监管图普，快速形成城市信息资产底图，对发现的信息资产进行分类管理，快速区分信息资产的类别，并针对所有资产进行安全监测，针对外部威胁及资产自身存在的漏洞进行总体的风险监测，形成城市级可视化安全风险热点分布。无缝对接安全大数据监测结果，实现城市级安全协同指挥能力，提升城市应对突发安全事件的能力。

构建城市级云端安全防御能力，对城市云平台及云上业务提供主动安全防御能力，构建集约化的安全防御体系，强化城市级应急联动处置能力、重大活动安保能力和综合安全管理能力，为衢州“政府数字化转型“及”城市数字化发展“提供强有力的安全保障。

通过数据共享及数据联动分析，实现城市的安全业务协同，赋能社会安全治理；通过数据共享、开放，激发社会关于数据的创新创业活力，为城市治理和城市数字化发展进行赋能。助力城市传统产业转型升级、促进城市新旧动能转换是城市网络完全中心建设的初衷；通过以建促产、以产促城的创新驱动发展，提升本地数字经济指数，通过产业数字化、数字产业化发展，逐步形成城市数字化，逐步提升数字经济在经济总量中的占有率，助力产业转型。

**项目采购内容**

## 1、智慧城市大数据安全中心

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序 号** | **系统名称** | **功能模块名称** | **功能子模块名称** | **主要性能参数** | **数量** |
|  **1** | **智慧城市大数据安全中心** | **智慧城市网络安全中心** | 硬件平台 | 硬件规格： CPU ≥24核（12核\*2，主频2.10 GHz，16.5 MB L3 Cache），内存≥256GB（16G\*16，DDR4 26R），配置企业级存储磁盘总容48TB（4Tb\*12，7.2k 3.5 SAS 12GB/S）；接口要求：千兆电口\*4（可选万兆双口RJ45、千兆四口RJ45、万兆双口光纤等多种网络接口）；冗余1+1电源模块，滑轨 | 2台 |
| 大数据智能平台 | 大数据智能分析平台是融合了大数据技术和人工智能算法的安全运营系统。平台部署在用户的业务网络环境中，通过威胁发现、智能研判和自动化响应处置，实现安全运营的闭环管理，提高安全运维工作效率，构建智能安全运营体系。平台包括以下主要系统和引擎模块：大数据离线分析系统，用户异常行为分析系统，深度感知智能引擎DSI，安全事件智能研判引擎安全自动响应编排引擎。通过智能分析研判识别出真正有效的攻击和事件，结合用户实际场景进行全面溯源与取证、自动化响应处置，实现安全运营和管理的闭环。处理性能：数据采集和处理性能≥10000EPS，每条数据大小>1KB；10亿数据关键字查询结果响应时间<2秒。产品形态：支持横向平滑扩展，可以通过增加硬件服务器数量的方式增加平台集群的计算处理性能。数据接入：支持通过多种类型的安全、泛安全类数据接入采集，应包括但不限于设备日志数据、流量数据、弱点漏洞数据、系统性能数据、威胁情报数据、资产人员数据；支持通过流量采集设备采集接入全流量数据，包含流量中的请求包和返回包等信息，并可在数据检索中体现包信息；支持接入文本格式、CVS等格式的文件数据，可通过模板文件的填写导入实现资产数据的导入和管理；支持通过云端对接、本地导入或手动编辑的方式，接入威胁情报数据。★数据共享：大数据平台中的安全数据，包括告警数据、资产数据、工单等至少20种可共享给第三方系统，实现数据共享和交换（要求提供API接口文档）；同时支持原始日志、标准化数据、告警数据≥3种数据的共享和交换。深度感知智能引擎DSI：行为审计与可疑通信检测，支持违规操作、违规访问、违规应用、违规外发等300种以上行为审计检测规则，可针对任意单条规则进行启用和禁用；支持隧道通信、可疑内容、恶意IP、恶意域名、恶意证书、远程控制等3000种以上可疑通信检测规则，可针对任意单条规则进行启用和禁用。扫描探查检测：支持端口扫描、服务扫描、Web扫描、扫描器指纹检测等300种以上的扫描探查检测规则，可针对任意单条规则进行启用和禁用。漏洞利用检测：支持SMB漏洞、RDP漏洞、软件漏洞、设备漏洞、系统漏洞、拒绝服务漏洞、shellcode等7000种以上漏洞利用检测规则，可针对任意单条规则进行启用和禁用。恶意文件检测：支持挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell等25000种以上恶意程序检测规则，可针对任意单条规则进行启用和禁用。配置风险检测：支持弱口令风险、明文传输风险、HTTP配置风险、中间件配置风向、数据库配置风险、服务配置风险等100种以上配置风险检测规则。主机和账号检测：支持端口异常、主机对外扫描、主机对外攻击等主机异常检测能力，对任意单条检测规则支持启用和禁用。支持登录异常、暴力破解、行为异常等账号异常检测能力，对任意单条检测规则支持启用和禁用。Web攻击检测：支持Webshell请求、XSS攻击、SQL注入、远程代码执行、命令注入、远程文件包含、本地文件包含、文件上传、路径遍历、信息泄露、越权访问、XXE注入、网页篡改等13类、6000种以上web攻击检测规则，对任意单条检测规则支持启用和禁用。安全分析模型：平台应内置包括规则模型、关联模型、统计模型、情报模型、离线模型等在内的≥5大类安全分析模型；安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由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；★支持对安全日志里200个以上字段，包括但不限于应用协议、目的IP、目的主机名、目的端口、目的用户名、数据流方向、情报IOC等进行任意形式的逻辑与或非形式组合建模，运算方式包括但不限于AND、OR、等于、不等于、大于、小于、属于、不属于、存在、不存在等，并能根据组合方式自动生成运算表达式（提供截图）。安全自动化响应编排引擎：支持前端拖拽式交互设计安全风险分析研判策略和联动响应剧本，支持多种策略编排动作，包括但不限于数据源、分析组件、处置响应等，可自动判断策略编排是否合理并弹窗提示支持通过任务看板查看自动响应任务的数量、状态、运行趋势；可查询并追踪每条自动化响应任务的运行阶段查看详细信息，任务执行过程中可加入安管人员控制环节，通过邮件、短信方式将告警和分析报告推送到对应用户。支持与不同品牌的网关类安全产品进行联动防护，防护策略支持设置每次阻断不同时长生效时间，时间设置包括10分钟，30分钟，6小时，24小时，72小时，永久阻断；支持与EDR集成联动，一键查杀木马病毒。用户异常行为分析系统：AI高级分析，平台内置不少于8种机器学习分析场景模型，可检测发现勒索挖矿告警数异常、安全设备日志数异常、网络会话数异常、域名请求数异常等特定场景条件下的安全态势异常；支持自定义部署AI机器学习模型，允许用户选用的高级机器学习算法不少于4种，通过输入任意指标类数据进行模型训练，发现异常行为并生成安全事件与告警，辅助用户发现潜在的安全风险。★网络实体分析画像：实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型过滤关联关系，支持通过一键溯源进行威胁关系的自动拓展；支持与终端检测类产品对接，查看主机进程、软件版本、漏洞病毒情况（提供截图）。大数据离线分析系统：场景化分析，支持暴力破解、Web攻击、恶意程序、端口扫描等内置安全分析场景，基于场景特性进行默认条件的数据聚合分析，支持至少3个任意字段的快速聚合分析，聚合后的所有数据均支持快速统计分析，展示统计排序信息，支持分析结果导出。支持自定义场景安全分析，可对安全告警的任意字段进行聚合分析，支持的聚合的字段不少于300个，支持分析结果导出；支持智能检索语句分析，支持检索语句的中英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；检索语句支持快速保存，历史检索语句快速导入；检索语句可直接发布成实时分析模型，对实时数据进行分析与告警。安全事件智能研判引擎：取证分析，支持调查场景的四维自定义攻击流向图取证，攻击趋势取证、攻击链分布取证、和实体信息取证，展示攻击者和受害者的威胁情报与资产信息，可联动会话详情，点击查看不同溯源维度的会话详情，通过请求头，payload等详情字段定位攻击。★历史数据分析：支持对原始日志的数据挖掘分析，可选择柱状图、折线图、面积图、表格、数值图、饼状图等多种报表样式自由对历史数据的任意字段进行可视化统计分析，辅助研判安全事件风险（提供截图）。安全态势可视化：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 ；支持立体、平面、球面等多种维度的网络实体关系透视，可在大屏上展示不同实体的标签属性，包括但不限于DNS服务器、监管单位、邮件服务器、黑客组织、WEB服务器等。仪表盘：支持可视化图表类型≥15种，包括但不限于时序图、饼图、柱状图等；统计类图表支持展示升序或降序的TOP5到TOP100，可针对数据中任意字段的计数、平均值、求和、最大值、最小值、唯一值等≥5种算子的统计结果配置可视化图表；可视化图表可通过拖拽配置组装成仪表盘，仪表盘不少于7种布局类型，仪表盘展示时支持时间范围自定义选择。安全运营门户：平台应具有统一的安全运营门户，作为多个安全态势分析与感知功能的统一入口，集成态势感知、威胁狩猎、通报预警、异常监测、运行监测等多个功能模块，实现平台内部业务、数据、服务、资源的无缝整合与集成；支持每个用户配置个人专属的统一门户，可配置项包括门户名称、应用名称、应用图标等；一门户应支持与第三方产品集成，一键跳转至产品功能界面。智能检索：支持对原始日志数据、安全告警数据进行分类检索，从检索结果可关联威胁情报和资产信息并一键跳转；支持不少于10000条检索结果导出，导出内容字段可自定义选择，支持excel或CSV格式。★资产管理：支持通过流量无侵入式自动发现资产，支持发现终端、Web服务器、DNS服务器、邮件服务器、FTP文件服务器等类型≥5种，其中web服务器支持自动识别服务域名和服务站点名称；支持资产信息的全量导入导出；支持一键访问安全设备的管理界面、监控大屏、设备日志、处置联动记录；支持以单个IP地址、IP区间、子网掩码等3种模式录入安全域信息。业务拓扑监控：支持拓扑图的增加、修改、删除、导入、导出，支持创建>50个业务或网络拓扑，支持建立平面拓扑和3D拓扑；支持监控安全域、Web业务系统、服务器、终端、安全设备等至少5种网络实体类型；支持在拓扑图上一键点击跳转查询相应网络实体的安全日志。安全运营：支持统一的安全运营工作台，在工作台可以集中查看当前用户的待办工单、最新通报预警状态；工单详情与备注支持多种内容格式，包括但不限于文字、图片、超链接、表格、代码片段、附件等类型；支持工单举证信息一键溯源，工单处置人员可以直接定位到工单关联的原始信息进行查看；支持通过安全告警自动派发工单到对应的安全管理员，支持自定义编辑预警信息内容；支持将预警信息直接转为内部通报，支持将通报内容作为工单定向指派。安管协作：组织架构中各级单位支持设定独立的安全管理员、业务系统、安全域；支持多级管理员间资产风险信息的隔离和共享，总部用户管理员可以分配下属组织架构的功能权限，支持按月和按周考核各组织架构的安管工作成果。分部安全管理员只可以使用所属组织架构具备的功能，只能管理与分析所属组织架构的资产和数据，分部具备单独的态势感知大屏；分析报告：支持用户自定义编辑报告模板，根据实际的业务需求自定义统计分析的指标对象，生成有针对性的分析报告，安全分析中的所有字段内容，都可以作为报告的统计对象，并自定义时间范围实现报告导出；内置深度威胁分析、攻击者取证等2个以上报告模板，报告订阅支持通过邮件方式在设定时间点发送日报、周报、月报到不同邮箱，可配置订阅规则数量≥10条。重大活动保障：支持重大活动保障任务前期、中期、后期分阶段的任务管理，保障预案管理；支持任意保障区域和系统，支持设置保障监控拓扑，支持重大保障态势大屏实时监测；保障监测视角覆盖云管端、边界、应用、安全设备等监测维度≥6种； 黑白名单：支持通过黑白名单功能对分析对象进行过滤筛选；支持通过任意字段进行组合，配置筛选条件并生成黑白名单过滤规则。一站式运维：支持大数据平台本身的计算、存储资源利用率监控；支持数据集与数据索引健康度监控；支持对平台各组件运行健康状态的集中监控；支持平台运行状态告警，运行监测引擎可独立于安全分析引擎工作，展示运维告警趋势、分布等；持大数据平台一键巡检，一键检查项包含但不限于数据健康、探针健康检查、大数据集群健康、Elasticsearch健康、实时流计算引擎健康、管理服务健康、服务器节点健康等多种维度检查，并能提供处置建议，一键导出各类服务的故障日志，包括但不限于Elasticsearch、Logstash、Kafka、实时计算引擎、操作系统等。用户管理：提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立，支持根据对象属性自定义划分系统管理角色和一般用户角色，按照数据和功能分级灵活设置用户权限。个性化配置：支持常用配置参数的前端可视化修改，如信任IP、页面嵌套开关、首页缓存开关、告警推送主题、测试告警推送内容、ES集群IP、告警聚合条数上限配置、字体、主题皮肤颜色、产品名称LOGO等的前端可视化配置，满足用户的个性化配置需求。 系统恢复：支持安全模型的启用状态恢复出厂设置；支持通过权限认证实现数据恢复出厂设置。级联管理：适配部、省、市、区、县的多级部署架构；总部支持查询全网安全态势和告警，分部只支持查询单位内部相关的安全态势和告警。 | 2套 |
| 威胁情报模块 | 1.模块具备云端威胁情报订阅模块：内置威胁情报离线库并支持更新。2.设备支持采用情报数据进行实时检测防御。3.设备支持在线查询与溯源：云端提供对IoC威胁类型、多源情报、WHOIS、开放端口、SSL证书等多维度的溯源分析；4.云端服务：支持订阅高级威胁分析情报，云端提供最新APT入侵、0day漏洞预警、病毒变种情况等分析报告订阅。5.支持通过离线导入或手动编辑添加的方式，形成本地威胁情报，允许用户自建行业情报库，并实现情报库的增删改查、导入、导出功能；情报记录包含情报置信度、标签、组织名称、地理位置、运营商等信息；支持查看情报源中有效情报数量、最近更新时间、今日更新情报数量；情报查询支持通过IOC同时跨越多个情报源查询，结果汇总展示；碰撞情报IOC支持通过情报源、IOC类型、标签、置信度等多维度进行碰撞分析，内置威胁情报条数不少于400万条。 | 三年 |
| （流量分析系统）（网络流量综合探针） | 硬件外形：标准机架式设备；电源：1+1冗余电源内存：128G硬盘容量：硬盘容量：2T\*2，带RAID1，可用磁盘空间不小于2T；接口数量：标配10个；接口类型：千兆RJ45网口\*2(管理口\*2)、千兆RJ45网口\*4、千兆业务SFP光口\*4、万兆SFP光口\*2接口扩展：千兆RJ45网口\*4+千兆SFP光口\*4或万兆SFP光口\*2MTBF大于65000小时吞吐率：10Gbps1.具备流量威胁深度检测能力，支持异常会话检测、WEB攻击检测、挖矿行为检测、僵木蠕检测、Webshell文件检测、异常文件检测、漏洞利用检测、DoS攻击检测、扫描行为检测、配置风险检测、异常登录检测、横向移动检测、违规访问检测等13大类、超过4万条威胁检测规则2.具备流量协议内容深度还原，包括http、dns、smb、ftp、smtp、pop3、imap、tls、tftp、ikev2、krb5、ssh等协议3.具备流量会话还原，还原所有流量会话数据支持外送，包括流ID、会话开始时间、会话结束时间、来源IP、来源端口、目的IP、目的端口、传输协议、应用协议、上下行流量、上下行数据包个数、会话时长、是否触发告警等；具备网络入侵攻击报文检测引擎，触发告警，记录入侵攻击事件，记录：事件名称、来源IP、来源端口、目的IP、目的端口、原始流ID、攻击报文、传输协议、应用协议、原始内容等。4.支持行为审计、漏洞利用、可疑通信、DDOS、恶意程序、配置风险、账号异常、主机异常、Web攻击、横向移动等12大类、68小类攻击检测规则，规则总量不少于4万条。支持对系统CPU、内存、磁盘、网口状态、网口流量、外送流量等指标进行可视化监控。5.支持可视化配置数据外送类型以及每种数据类型的字段是否发送。 | 1套 |
| 漏洞体系库及风险收集 | 1.建设完善的漏洞体系库，不仅仅实现了现有的已知漏洞信息同步，更实时同步我方安全漏洞信息，漏洞库的建设是信息安全保障工作中一项极为关键的基础性和长期性工作。大量的网络失泄密案件和信息安全问题均与漏洞的存在息息相关。漏洞库通过其漏洞收集、分析、通报和面向应用的工作机制，提高衢州市政府应对信息安全威胁的能力和风险管理水平。2.通过国内外开源/商用情报、全网流量捕获、用户分析情报、Sumap与全网爬虫风险情报联盟共享等手段收集风险情报，通过收集和自动采集CNVD、CNCERT、IPDB、漏洞盒子等第三方漏洞平台等安全数据，提升外部安全情报的接入能力，同时补充公开的安全情报数据和外部组织机构的监测数据，增强安全监测的全面度，也为通报预警提供更多的数据来源。进一步提升衢州市智慧城市系统网络安全监测能力。3.对接云端及第三方漏洞库，实现现有的已知漏洞信息同步，并同步我方安全漏洞信息，提升外部安全情报的接入能力，增强安全监测的全面度，扩展大数据智能平台分析数据的维度。 | 三年 |
| 与省安全平台对接 | 浙江政务系统包含了省级系统（大数据局）和市级系统（衢州、嘉兴、绍兴、台州、湖州、宁波等），省市系统之间需要数据传输，省级系统提供接口供市级系统查询（http接口通信）。**资产zw-assets\_data：**提供与第三方资源管理系统的接口以实现资源共享、同步更新、信息的查询和导入等功能。同时内置资产通用属性接口，用于实现与第三方资产管理系统的数据格式相互转换；资产管理模块中各项资产的属性值将参与到安全事件管理、脆弱性管理、风险管理、拓扑视图、报表系统等其它安全管理模块；提供资产的手动和自动发现，资产接入或者移除，能够自动更新，并作出提示，对新接入资产进行预管理，对移除资产进行记录管理；提供资产指纹探测扫描功能，包括资产网络属性、系统版本、应用组件信息及指纹信息等，扫描结果直接应用于二期建设的业务资产拓扑功能；将安全事件与资产进行绑定关联，实现以资产视角的安全事件管理，在资产拓扑视图上直接展现安全事件的信息，支持钻取溯源等安全处置功能。**攻击告警zw-alert-attack：**攻击态势主要关注来自同地区的攻击源对内部资产的威胁情况，实时监控境内境外攻击源的地域分布和国家排行，掌握各攻击链阶段的威胁变化趋势和最新外部攻击事件。**漏洞告警zw-alert-vulnerability：**漏洞检测功能需要支持主动的系统、应用层、中间件、数据库漏洞检测，漏洞库具备实时更新和自定义功能；可检测主流windows、Linux、国产操作系统漏洞；内置通用性弱口令字典，并可增加自定义字典的漏洞检测发现功能设计，基于安全自主研发的漏扫引擎，通过深度扫描、漏洞检测、木马检测、逻辑漏洞检测等方式对扫描对象进行全面的探测与检查，以脆弱性和漏洞为导向,以安全风险管理为基础, 对资产进行深度遍历。支持主流的漏洞。采用强大的过滤模块，过滤掉重复或者不必要的网页链接，提高运行效率。单引擎单位时间的发包速率的可控化，可以有效防止扫描数据量过大影响系统正常运行的问题。 扫描数据实时存储，扫描过程中实时存储扫描数据和结果，不管是由于程序自身引擎中断、进程人为关闭，还是机器断电引起扫描中断，扫描数据都不会丢失，可以进行断点续扫。系统内置可更新的漏洞知识库模块，对扫描出来的漏洞提供详细的解决方案参考。 提供接口可以导入第三方漏洞扫描结果。**黑链告警zw-alert-black\_link：**针对邮件恶意链接的模拟行为分析技术，邮件社工行为攻击通常会利用伪造发件人信息，来获取被攻击者的信任，欺骗用户点击指定的链接或者文件，一旦用户点击那么将出现被植入木马的情况。针对发件人欺骗的行为进行分析，发现伪造发件人必须通过伪造邮件服务器的方式实现，我们可以通过绑定邮件服务器IP地址，对于所有绑定IP地址的邮件服务器进行判断，以此发现发件人欺骗的攻击行为并进行告警。**挂马告警zw-alert-trojan：**支持木马回连行为检测，完整覆盖特种木马传输、恶意IP/URL访问、异常数据传输多个阶，对病毒木马进行扫描，快速发现各种已知特征的恶意文件攻击行为；用DGA（Domain Generate Algorithm，域名生成算法）发现僵尸/木马通讯；通过检测网络流量中的DGA域名，有效定位网络内部已经被僵尸/木马控制的主机；基于对木马回连行为的深度分析，提取其中的恶意回连C&C IP/URL，再对这些IP/URL同步到相应的阻断防护设备上，生成相应策略。在网络中出现相关行为时，利用WAF、FW等设备对反向数据进行阻断，将APT智能学习到的WEB服务器反向木马回连行为进行阻断，实现基于反向数据的阻断并进行告警。**钓鱼告警zw-alert-fishing：**对于邮件钓鱼行为，可以通过对所有邮件传输过程中携带的URL链接进行分析，并对URL链接进行模拟点击操作，分析打开URL过程中传回的数据，发现各种邮件钓鱼的恶意行为阻断并进行告警。**违规内容zw-alert-content\_illegal：**通过以下多个角度对违规违法行为检测：信息泄露，通过漏洞利用窃取用户信息。不良信息内容，实现对不适宜信息内容检测审计。敏感信息过滤，实现对身份信息、关键字、数据源等的自定义，实时掌握流量中的敏感信息定位，实现对不合规行为有效监测。隐私权侵害，通过策略获取信息系统内部系统访问权限，侵犯数据隐私。**内容变更zw-alert-content\_change：**文件解析和内容识别，非结构化文档类型识别及内容解析，包括doc、docx、xls、xlsx、ppt、pptx、pdf、zip、rar、7z、txt等等。通过关键字、普通表达式、正则表达式、中文自然语言识别等对数据内容进行识别和匹配。网络传输数据审计，通过监听电子邮件（SMTP协议、IMAP协议）、WEB（HTTP协议）、文件传输（FTP协议）和网络共享传输（SMB协议）等传输数据的内容解析，对敏感数据的违规传输进行审计和告警。终端数据使用管控，终端层面的基于内容识别的敏感数据管控，包含外设（移动存储、光驱刻录、打印、剪贴板、截屏，蓝牙、网卡、红外、串口等）和网络（WEB、文件共享、邮件、远程连接、FTP、P2P下载、IM即时通信、云盘、网盘等），实时阻断敏感数据在终端的违规外发和泄露。**安全事件zw-event\_data：**当有安全事件发生时及时产生安全告警，并以资产为核心视角，直观了解自身网络环境中存在风险资产。通过攻击链形式进行展示，剖析从扫描探查阶段到资产破坏阶段资产失陷全过程。感知失陷、异常资产，从海量的日志中提取有价值的资产溯源路线，实时追踪排查告警来源。基于过往数据进行拟合分析，发现事件发展的历史趋势和规律，为未来的安全事件决策提供数据支撑。能够从历史数据中进行深度挖掘与整合，达到分析过往、了解当下、预测未来的检测效果。**WEB应用防火墙（WAF）日志zw-equipment-waf：**对WEB应用攻击检测防护方面，除了对已知可防护的攻击类型实现全面的拦截以外，还具备对应用访问全审计的功能。全审计指对所有的WEB请求进行审计分析记录，不仅可以提供详细的访问日志分析，还可以图表的形势展现WEB服务的业务访问情况。通过对访问记录的深度分析，可以发掘出一些潜在的威胁情况，对于攻击防护遗漏的请求，仍然可以起到追根索源的目的。**防火墙日志zw-equipment-firewall：**研究采集设备部署与网络进行连接后，需要能够主动对指定网络范围内的设备进行设备信息探测，基于设备指纹库主要进行主机类型、端口扫描、版本侦测、操作系统侦测，探测技术具有防火墙规避技巧，可以综合应用到四个基本功能的各个阶段。对于不能识别的设备将设备信息传输到综合安全监管系统对设备进行进一步分析，另外提供强大的脚本引擎功能，脚本可以对基本功能进行补充和扩展。**网络入侵检测日志zw-equipment-attacks：**面对全流量威胁进行识别，并通过双向流量检测对网络流量行为（例如数据报文恶意特征匹配、资源使用情况、使用者的访问行为等）判定，识别出病毒、木马、敏感信息等异常行为。威胁行为分析，组件根据数据包特征和流量行为对流量进行深度解析，通过对数据流中威胁行为识别，达到恶意流量检测的目的。通过流量深度解析，系统异常、网络木马、异常端口访问、网络扫描、DoS、通用协议命令解码、WEB应用漏洞利用及程序攻击、恶意文件及病毒攻击、异常威胁、异常用户名登录请求、可疑执行代码等非正常和非RFC遵从的请求行为以风险级别实时呈现，为威胁风险分析和管理提供依据。威胁行为识别，通过以下几个方面对威胁行为进行识别：基于4000+条规则库进行特征匹配；根据资源使用状况或者使用者访问行为进行识别；基于异常检测技术识别威胁行为，例如病毒、木马、攻击等；通过索引实时查询页面告警信息。网络病毒监测预警日志。**网络脆弱扫描日志zw-equipment-vulnerability：**提供主流扫描设备的数据接入功能，实现对接入数据的对比、去重，形成整体脆弱性报告；各个资产的整体脆弱性展示，对整个网络的脆弱性进行展示，支持根据扫描器类型、CVE/CNVD编号、弱点名称、危害程度以及受影响的资产等条件进行检索；脆弱性数据与资产和资产域，对资产域内的脆弱性分布展示；跟踪脆弱性被利用行为，实现分析和溯源。APT检测系统日志zw-equipment-apt：提供高级威胁监测：病毒、蠕虫、木马、DDoS、扫描、SQL注入、XSS、缓冲区溢出、欺骗劫持等攻击行为检测；以及未知威胁的检测：包括C&C隐秘通道检测、CallBack特征检测、未知恶意文件等APT检测能力。**威胁发现设备数据日志zw-equipment-threat：**威胁情报是针对内部和外部威胁源的动机、意图、能力以及战技过程的详细叙述，威胁情报可以帮助企业和组织快速了解到敌对方对自己的威胁信息，从而提前做好威胁防范、更快速地进行攻击检测与响应、更高效地进行事后攻击溯源。对企业而言，威胁情报的应用/消费是实现情报价值的关键，通过安全威胁分析与预警平台和威胁情报的集成，实现全网的基于威胁情报的协同联动，才能发挥平台与情报的最大价值。安全威胁情报管理用于支撑外部威胁的分析和定位，功能包括威胁情报获取、威胁情报输入与维护、外部资产发现和监控、情报关联分析。威胁情报获取：本功能提供对威胁情报信息的自行添加或通过情报服务商获取的能力。威胁情报主要包含战略情报、战术情报以及漏洞情报；威胁情报维护：提供手动添加威胁情报功能，以及用于威胁情报信息的删除、修改、启用、标注等，方便威胁情报管理威胁情报关联分析：通过威胁情报对外部资产发现和监控用于发现暴露于互联网侧的资产信息，并对资产的威胁状况进行监控，对外部攻击者进行关联分析。威胁情报碰撞检索：本功能提供对内置威胁情报以及云端威胁情报和第三方威胁情报的碰撞检索功能，用户可使用本入口快速碰撞情报。▲在服务期内，无偿按要求做好与省相关平台对接。 | 1套 |
| Web应用防火墙 | ▲硬件规格：标准机架式；标配网口：千兆电口管理口\*2；千兆业务电口\*4（含2组硬件BYPASS模块）；千兆业务光口\*4（标配GE多模SFP模块\*2，不含硬BYPASS模块）；硬盘容量：1T；内存：16G；USB口：USB2.0口\*2；串口：RJ45口\*1；电源：1+1热插拔冗余电源。性能规格：保护站点：无限制；硬件性能：应用吞吐量≥8Gbps；HTTP最大并发数≥40万；HTTP最大新建数≥4万。部署模式：支持透明串接、反向代理、旁路镜像等多种部署模式部署，支持链路聚合。高可用：支持集群模式、主-主模式、主备模式、硬件BYPASS、软件BYPASS。保护对象：支持多条链路数据的防护，防护网段数量不限；支持ipv4/ipv6双协议栈；支持保护站点快速向导配置部署。 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。 HTTPS防护：支持透明串接和旁路反向代理下的TTPS业务的安全防护。攻击检测：支持对跨站脚本(XSS)和注入式攻击（包括SQL注入、命令注入 、代码注入、文件注入、LDAP注入、SSI注入等）的检测防护；支持对HTTP请求关键字段进行合规性的检测（包括Host字段、User-Agent、Content-type字段等）；支持对HTTP头部各字段内容长度进行限制并可以自定义调整限制大小，包括参数名长度、参数值长度、HTTP请求头部长度、URI长度、cookie长度、User-Agent长度、Content-type长度、Host长度等。Webshell检测：内置Webshell检测规则，可以对上传的文件内容进行检查，防止恶意Webshell文件上传，对已经上传的webshell发起请求的行为进行拦截阻断。敏感信息泄露检测：内置身份证、银行卡、手机号、社保号等个人敏感信息数据，对服务器返回的敏感个人信息数据通过星号进行隐藏，并支持用户自定义敏感词；能够检测防止服务器导致的信息泄露行为，包括：目录信息泄露、服务器信息泄露、数据库信息泄露、源代码泄露等信息泄露行为。爬虫、扫描器等自动化工具的安全检测：内置安全规则可有效识别Acunetix、nessus 、WebScan、Webdump等扫描器的扫描行为；内置安全规则可有效识别baidu、google、yahoo等常见网络爬虫的访问行为。盗链攻击检测：内置防盗链规则，可实现全站盗链保护，也可以针对特定的文件类型（jpg、png、gif等）进行盗链防护。同时可以设置允许盗链访问的第三方网站的白名单域。自定义规则：支持丰富的自定义规则，支持对请求头部的各个字段包括Host、User-Agent、Cookie、Content-type、Referer、Content-Length、请求参数名称、参数内容进行安全检测，同时也支持多个检测检测条件进行组合，满足对复杂场景的安全检测需求。智能语义分析：内置对SQL注入、XSS攻击检测的语义分析规则。机器学习：1、系统内置机器学习安全引擎，通过机器学习可以对用户web业务系统建立安全的访问模型，学习的内容包括URL、参数、参数类型、参数长度、cookie等信息；2、支持设定学习的周期，需要学习的域名信息，可以设定可信任的客户端IP，不可信的客户端IP以及不学习的URL信息；3、模型数据可以显示学习中的URL数量，学习完成的URL数量、检测中URL数量、学习失败的URL数量，同时可以显示各个阶段的占比情况；4、内置通用的机器学习模型，无需对现网业务进行学习，通过与云端联动，数据模型可实现自动更新。智能攻击者锁定：支持智能识别攻击者，对网站连接发起攻击的IP地址进行自动锁定禁止访问网站；可配置攻击者识别策略和算法以及攻击者锁定时间。CC防护功能：支持细粒度检测条件，可基于URL、请求头部字段、目标IP、请求方法等多种组合条件进行检测，检测指标可通过URL访问速率和URL访问集中度、请求离散度三重检测减少误判率；检测的客户端对象可支持IP、IP+URL、IP+User\_Agent多种算法，客户端IP支持应用层字段解析，并支持自定义检测字段功能；支持基于地理位置的识别，可设置不同地理区域的检测，杜绝海外肉机攻击。地图态势分析：按地理区域对攻击次数等进行统计，通过地图展示，并在地图上可以指定某一地理区域进行访问控制，阻断此区域 IP的访问。云端威胁情报订阅模块：威胁情报支持离线和在线更新。云端威胁情报联动：支持云端威胁情报联动，可主动发现包括僵尸网络、代理IP、扫描主机、黑产IP等恶意IP发起的访问行为，针对恶意IP的访问行为进行告警并拦截，威胁情报数据可实现离线更新和在线更新。APT联动：WAF支持与APT产品联动实现对未知威胁的感知拦截。 云端高防联动：WAF与云端高防中心联动，通过WAF一键开启防护，实现3-7的DDOS安全防护，最高可提供1T抗D服务。安全审计：能详细记录攻击事件的HTTP请求头信息，含请求的URL、UserAgent、POST内容，cookie等所有的请求头内容；能详细记录服务器响应头信息，服务器响应内容。日志分析：根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率。访问审计：具备审计网站正常访问流量的能力，提供按小时，天、月份生成用户的访问数据；能记录、查询所有用户对网站的访问情况，包括访问的URL、客户端IP、服务器返回的状态码；能够统计分析出用户所访问URL TOP10数据；能够统计分析出用户所访问分文件类型；能够统计分析出搜索引擎的TOP10数据；能够统计分析出客户端所使用操作系统的TOP10数据。报表：支持自定义报表、定时报表、支持各类导出格式（WORD,PDF等）；根据PCI-DSS要求，对用户的应用进行合规性评估，生成合规报表。告警方式：支持Syslog、手机短信、邮件等多种告警方式。规则升级：规则库支持手工、在线升级两种方式，在线升级可支持规则定时检查新版本和在线更新，确保WAF能够针对新型的、突发型的Web攻击进行防护。管理方式：支持HTTPS方式进行设备管理。账户管理：设备管理采用管理员与审计员分离。SNMP管理：支持标准网管 SNMPv3，并且兼容SNMP v1和v2c。NTP：支持NTP时间同步。产品要求：产品需获得公安部产品销售许可证（增强级）；产品具备自主知识产权，提供计算机软件著作权证书。 | 1台 |
| APT攻击预警平台 | ▲硬件规格：标准机架式设备；电源：1+1冗余电源 CPU：10核20线程\*2 内存：128G 硬盘容量：2T\*2，带RAID1，可用磁盘空间不小于2T ；接口数量：标配12个；接口类型：标配千兆管理口\*2，千兆业务口RJ45网口\*4，千兆业务SFP光口\*4 （标配千兆多模光模块\*2），万兆SFP光口\*2（标配万兆多模光模块\*2）接口扩展：千兆RJ45网口\*4+千兆SFP光口\*4或千兆RJ45网口\*8 或千兆SFP光口\*8或万兆SFP光口\*2 或万兆SFP光口\*4性能参数：MTBF 大于65000小时吞吐率：网络层10Gbps，应用层4GbpsWEB检测：HTTP最大并发数20万/秒邮件检测：邮件处理数: 300万封/24小时文件检测：10万个/24小支持管理节点50个全流量检测：支持全流量检测，可根据需求打开或关闭全流量检测功能。审计协议：支持解析HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、Mysql、MSSQL、DB2、Oracle、HTTPS、SMTPS、POP3S、IMAPS等协议报文（HTTPS、SMTPS、POP3S、IMAPS加密协议解析需要导入服务器私钥证书），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LDAP登录行为识别；支持VXLAN镜像流量解析检测。检测风险类别：支持检测WEB攻击、异常访问、恶意文件攻击、远程控制、WEB后门访问、发件人欺骗、邮件头欺骗、邮件钓鱼、邮件恶意链接、DGA域名请求、SMB远程溢出攻击、WEB行为分析、隐蔽信道通信、暴力破解（包括SSH、TELNET、RDP、FTP暴力破解）、挖矿等风险。告警黑白名单过滤：支持对文件白名单、发件人邮箱白名单、发件人域名白名单、黑域名白名单、黑IP白名单、域名白名单、客户端IP白名单、服务端IP白名单、WEB风险特征白名单进行设置；私网IP地理位置定义：支持对私网地址IP地理位置信息添加，在产生告警时，定义IP可正常显示所属地理位置信息。弱口令风险检测：支持对Telnet、FTP、POP3、SMTP、IMAP等协议进行弱口令检测。告警详细展现：可支持详细展现告警级别、时间、威胁名称、状态、客户端IP、客户端IP所在地理位置、服务端IP、服务端IP所在地理位置、报文、操作等信息，包含请求URL、请求类型、请求内容、请求头、Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Accept-Charset、Keep-Alive、Connection、Cookie、请求参数、响应码、返回长度等信息。主机威胁分析：可自动对内网主机进行威胁指数分析，详细展示具体的威胁指数、威胁活动、历史威胁指数、遭受的攻击类型、攻击次数、攻击状态等可根据不同威胁指数的主机实现攻击溯源和攻击过程的可视化分析。可通过攻击源、攻击目的对攻击路线进行统计，包括攻击的行为、告警，并以直观的图形化形式展示。木马回连分析：可自动学习网络流量中包含的各种可疑C&C IP/URL，包含各种可能对内网存在影响的IP和域名；快速识别网络中存在的恶意回连行为，包含回连主机IP、服务器IP、时间、行为等；对基于木马回连的非法数据传输等行为进行取证分析，包括回连主机IP、服务器IP、传输数据大小、协议类型等攻击地图展示：可通过攻击源和目的的地理位置信息，以世界地图和中国地图的形式展示，并实现世界地图和中国地图自动切换直观展示攻击路径。协议解析：支持 HTTP、HTTPS（需要导入服务器私钥证书）协议解析，检测WEB攻击。双向审计：支持双向审计，对请求和响应都进行审计攻击检测：支持SQL注入、命令注入、跨站脚本、代码注入、协议错误攻击检测。WEBSHELL检测：支持WEBSHELL检测，可检测访问webshell的行为，包含具体对应的URL、返回码、返回数据包内容等，可显示一句话类webshell后门是否植入成功。自定义WEB审计规则：支持根据来源IP、MAC、HTTP请求方法、URL、请求头、请求参数、响应码等内容设置审计规则高、中、低等风险等级。白名单功能：支持WEB特征攻击风险白名单设备，可基于类别、规则、IP灵活配置。动态分析：自动关联行为分析的详细展现，包含SQL注入取数据、表单破解、XSS测试、目录穿越读取文件、多人访问Webshell、APT攻击等。场景化分析：支持场景化的分析能力，对发现的告警进行二次关联，支持对勒索病毒、网站后门、邮件APT攻击等事件进行预警。DNS协议分析：具备DNS协议分析能力，发现受感染主机、危害程度、被感染病毒类型、回连C&C域名、DNS返回详情、恶意主机明细等行为。与WAF联动：支持将分析到的WEBSHELL攻击、木马回连和恶意攻击行为同步到WAF，实现APT深度威胁分析与WAF联动阻断。协议解析：支持解析webmail、SMTP、POP3、IMAP、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）类型报文。Webmail攻击检测：支持基于webmail攻击类型检测，包括sql注入、跨站、命令注入等攻击检测。社工类攻击检测：对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接。恶意附件检测：支持邮件恶意附件行为检测。解析协议：支持 HTTP、FTP、SMB、SMTP、POP3、IMAP、HTTPS、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）等协议传输文件检测。文件类型：支持doc, xls, ppt, swf, pdf, java, rar, zip, rar, exe, vbs, scr, html，js等多种文件解析。自定义文件类型：可添加或删除指定分离的文件类型，并可选择适用的协议类型（HTTP可进一步按GET、POST来配置）。特征检测：对文件进行特征匹配，利用已知的特征库发现恶意的可执行文件及非可执行文件。Shellcode检测：通过分析文件中的二进制代码，找到文件溢出攻击的代码，并能找到APT攻击中的0day攻击。动态沙箱检测：对存在问题的文件输出完整的二进制动态分析报告；动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险；对文件关键行为进行截图；可展示文件中版本信息、段信息、资源信息、导入表、字符串信息、删除文件信息等内容；可展示ROP行为检测；可展示具体文件的行为，包括所有的注册表行为、进程行为、互斥量、进程运行的函数、返回结果、返回值等信息；可显示文件运行过程中企图访问的IP、域名，以及域名及对应的IP。子文件扫描：对文件内部嵌入的子文件可进行二次扫描，分析安全性。攻击样本提取：可以提取出攻击的完整样本文件，并提供对该文件下载的能力。文件威胁指数：可展示威胁程度最高的文件样本MD5、威胁指数、传播次数，病毒检测、静态检测和动态检测结果等内容；根据文件传播情况分析受感染主机、接受云端威胁情报、关键威胁行为可视化、回连主机host和完整沙箱分析报告；根据云端威胁情报展示云端是否确认、传播协议类型、传播次数、云端确认结果等。远程控制检测：支持根据威胁情报、DGA域名请求、IDS规则、用户配置数据，发现被远程控制的内部主机。DGA域名请求检测：具备DNS协议解析功能，发现发起DGA域名请求的失陷主机。挖矿行为检测：可发现利用失陷主机挖矿的行为。本地威胁情报：设备集成离线的高可用威胁情报库 ，支持离线环境下，根据威胁情报进行检测，增量威胁情报随策略升级包升级。云端威胁情报：支持自动从APT云端获取最新威胁情报。协同防御：支持将本地恶意文件攻击的病毒类型等信息上传到APT云端，提升协同防御能力。策略自动更新：支持自动从APT云端更新策略。紧急事件上传：支持紧急事件上传云端，帮助客户关注紧急事件。抓包任务：同时支持至少16个抓包任务抓包，每个抓包任务可配置抓包规则，按照IP、端口、协议等信息进行抓包，将抓取的原始流量包保存于本地以供后续分析和取证使用，每抓包任务最大抓包20MB。三权分立用户管理：提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立，支持自定义管理用户权限和角色。风险处理：支持根据需要对风险状态进行选择处理中、处理完成、延迟处理、拒绝处理等。一键登录排错：支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、同步验证、信息收集等功能。设备状态监控：支持对设备的CPU、内存等状态进行监控，并在设备界面中进行展示。 知识库：根据不同的风险信息，提供风险分析和处置建议知识库。告警与报表：告警可详细展示风险级别、发生时间、告警名称、客户端IP、服务器IP、报文内容（URL、请求头、请求参数、请求内容）；可根据需要针对单个告警添加白名单；支持kafka、短信、邮件、syslog、snmp、ftp等告警方式；支持对kafka、syslog发送的风险信息进行AES加密传输；支持同时发送多人、单条发送、发送统计等高级告警功能；报表能够支持WORD、PDF等格式导出。日志数据管理：审计数据保留策略应至少满足天数和百分比两个控制参数，支持web界面可配置，且恢复数据不影响正常的审计功能。对审计日志可自动备份并加密，必须导入设备才能进行恢复查看，并可自动释放磁盘空间。产品要求：产品需获得公安部产品销售许可证（必须是APT安全检测类）。 | 1台 |
|  **2** | **数据安全管控平台** | 硬件平台 | 产品规格： CPU ≥24核（12核\*2，主频2.10 GHz，16.5 MB L3 Cache），内存≥256GB（16G\*16，DDR4 26R），配置企业级存储磁盘总容48TB（4Tb\*12，7.2k 3.5 SAS 12GB/S）；接口要求：千兆电口\*4（可选万兆双口RJ45、千兆四口RJ45、万兆双口光纤等多种网络接口）；冗余1+1电源模块，滑轨 | 3台 |
| 数据安全管控平台 | 数据安全管控平台提供了数据流动视角下的安全管控能力。利用复杂系统建模方法和大数据智能分析能力，建立适应数据动态流动的安全管控机制，从网络、数据、业务、人员四个视角对数据流动场景下的关键节点进行合规监控和防护，对发现的网络攻击和数据安全风险进行及时预警和通报。以管控平台为基础工具，建立资产识别→安全防护→监管监测→响应处置的数据安全运营体系，数据安全管控平台采用“分层解耦”的设计理念，将平台分为数据汇聚层、数据处理层、数据分析层和数据应用层，各层之间采用集中数据总线进行数据传输和交换，以此降低各类数据应用对底层数据存储之间的强依赖性，各层之间独立工作，保障各层之间稳定运行，同时方便安全业务扩展。网络资产梳理：对组织内部的网络基础设施按部门、系统进行梳理和管理：支持网络资产以EXCEL格式手动导入；支持网络资产按组织、系统和类型进行管理、统计和可视化展现。数据资产梳理：数据资产进行集中发现和管理，基于数据库探测对其数据进行识别并按数据的来源、用途、敏感程度进行分类分级打标，建立全局的数据资产目录，主要功能包括：数据库探测：在全网或指定网段内发现未知数据库服务，数据库类型至少包括Oracle、DB2、MySQL、MariaDB、SQLServer、PostgreSQL、ElasticSearch、MongoDB、Hive；支持数据账号权限配置的自动发现和梳理，账号信息至少包括用户、角色、授权事件、只读和读写权限；敏感数据识别：基于不同数据源，根据数据特征对目标数据库进行敏感数据的自动扫描，支持关键字、正则、中英文分词、字典的4种内容匹配技术；支持身份证、电话号码、银行卡号、网络标示等脚本识别技术；支持Unicode、GB18030、GBK、UTF-8等数据编码格式；数据分类分级：根据数据的来源、用途、数据的价值、内容敏感程度对数据进行分类分级打标，并支持标记和变更数据类别和级别。★数据资产管理：基于数据的分类分级打标，形成组织内部的数据资产目录，数据的结构至少包含数据库实例、表、视图、字段类型，支持周期性轮训对梳理结果进行一致性比对（提供截图）；数据安全治理，始于数据资产梳理。数据资产管理模块可通过自动化方式扫描用户的数据库表，建立全局的数据资源目录，并内置了敏感数据识别规则，可以有效识别敏感数据在系统内的分布情况。提供数据资产测绘、数据资产盘点、基础设施资产、用户身份信息管理服务，形成全市数据底图。同时数据资产管理模块支持对数据库、表、字段的备注定义和分类打标，可根据数据价值和特征，梳理出核心数据资产，对其进行分级分类，从而落实对数据更为精细的安全管理措★安全分析模型：支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由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；支持对安全日志里200个以上字段，包括但不限于应用协议、目的IP、目的主机名、目的端口、目的用户名、数据流方向、情报IOC等进行任意形式的逻辑与或非形式组合建模，运算方式包括但不限于AND、OR、等于、不等于、大于、小于、属于、不属于、存在、不存在等，并能根据组合方式自动生成运算表达式（提供截图）；平台内置包括规则模型、关联模型、统计模型、情报模型、离线模型等在内的≥5大类安全分析模型。AI高级分析：平台内置不少于8种机器学习分析场景模型，可检测发现勒索挖矿告警数异常、安全设备日志数异常、网络会话数异常、域名请求数异常等特定场景条件下的安全态势异常；支持自定义部署AI机器学习模型，允许用户选用的高级机器学习算法不少于4种，通过输入任意指标类数据进行模型训练，发现异常行为并生成安全事件与告警，辅助用户发现潜在的安全风险。网络实体分析画像：实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型过滤关联关系，支持通过一键溯源进行威胁关系的自动拓展；支持与终端检测类产品对接，查看主机进程、软件版本、漏洞病毒情况。网络安全监管监测：对网络资产的运行情况进行实时监测，及时发现安全漏洞和网络入侵行为，并进行风险的告警，包括：主机和账号异常检测：支持端口异常、主机对外扫描、主机对外攻击等主机异常检测能力，对任意单条检测规则支持启用和禁用；支持登录异常、暴力破解、行为异常等账号异常检测能力，对任意单条检测规则支持启用和禁用；恶意文件检测：支持包括挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell等25000种以上恶意程序检测规则，可针对任意单条规则进行启用和禁用；漏洞利用检测：支持包括SMB漏洞、RDP漏洞、软件漏洞、设备漏洞、系统漏洞、拒绝服务漏洞、shellcode等7000种以上漏洞利用检测规则，可针对任意单条规则进行启用和禁用；配置风险检测：支持包括弱口令风险、明文传输风险、HTTP配置风险、中间件配置风向、数据库配置风险、服务配置风险等100种以上配置风险检测规则；挖矿行为检测：12种以上的服务器挖矿行为分析，支持不同币种挖矿分析，包括但不限于：莱特币、比特币、门罗币、大零币、蚂蚁矿池等币种。数据安全监管监测：围绕业务场景开展的数据流动安全监管，将业务场景分解到数据流和数据节点进行细粒度的监控，实现基于业务规则的数据流动安全监管，包括：数据库节点管理：支持对业务场景的数据流进行梳理和拆分，并对数据流转节点进行统一管理，至少包含安全域、服务器、应用、服务、服务实例、访问端点、数据对象和人员账号等8类数据流节点；基于业务的数据建模：支持通过简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑建模和策略配置；敏感数据的访问监控：支持对敏感数据访问进行监控，对越权访问高敏数据等行为进行及时的告警；特定数据流转监控：支持特定数据的访问和流转过程及数量，并基于数据流转路径的智能学习，及时发现业务场景的数据流转变换，以修正现有的数据流模型；数据接口访问监测：支持接口访问进行统计，并结合业务规则对高频的访问行为进行及时的告警；数据接口异常监测：支持数据接口异常监测对接口的健康状况进行实时监测，包括高延时、返回报错、404异常访问进行监测并及时告警。数据安全监管监测服务-数据监管：对敏感数据流转日志信息进行记录和分析，确保每一条数据的来源、流向和被执行的处理操作（计算、分析、可视化等）能被有效的记录和查询，从而发现敏感数据的泄露和违规范围行为。数据安全监管监测服务-业务场景监管：对关键业务进行分解，针对业务开展涉及到的业务事项、数据流和数据节点进行安全监管，准备把握业务开展过程中的数据调用、流转和使用情况，及时发现数据滥用、违规使用和不可用等情况。面向多部门协同的业务场景或复杂的数据流转场景，根据数据的流向，利用数据流节点，采用简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑配置和统一管理。同时，基于业务需求对其节点及节点之间的数据流转设置监控策略。基于业务的数据流转拓扑作为数据、业务和人员安全监控的参考基线，包括节点对象的访问量、访问流量、访问速率、请求延时、异常访问和敏感数据访问的监控，同时支持对特定数据的全网数据流转拓扑自动梳理。数据安全监管监测服务-基础设施监测：对电子政务网络和政务云平台等基础设施的脆弱性、外部威胁和运行情况进行安全监管，及时发现安全漏洞和网络入侵行为，提高基础设施的安全可靠性。采用自动发现、手工录入、批量导入等方式，对全网基础网络资产信息（包括主机、安全设备资产等）进行统一梳理和统计，通过对资产从单位、系统等多方位的类型划分，以图表形式帮助客户整体掌握当前组织结构下，资产总量、各单位的系统数量、系统所使用的资产数量等信息，从不同维度对基础资产进行分析，帮助使用者直观、快速的掌握资产整体情况。★数据安全监管监测服务-人员权限监管：支持特权人员的数据访问操作行为进行监督审核，确保相关人员的操作及行为在权限范围内，操作合理合规，同时可对越权行为及高危操作进行告警和记录（提供截图）。数据安全监管监测服务-人员监管：对用户的应用访问行为进行记录和审计，通过用户行为分析发现用户异常访问行为，避免数据泄露事件和数据滥用事件的发生。对于接入数据库的行为提供多维度的监控，包括身份管理、应用防假冒、防撞库、直连控制和免密登陆等。身份管理通过应用程序名、IP地址、主机名、操作系统账户、数据库账户、数据库实例名、时间等因素进行任意组合，形成登陆认证规则，防止人为恶意将其他的应用改成业务系统应用，假冒应用访问数据库，进行非法操作。将系统管理员、数据库管理员、第三方代维人员和运维开发人员等的身份进行统一管理，使运维操作更加规范、透明、可控，构建多维度数据库接入认证体系；特权账号访问控制对数据库运维账号等特权账号实现访问控制，可禁止DBA、SYSDBA、Schema User、Any等特权用户访问和操作敏感数据，可限制DBA账户权限，访问敏感数据集合需要经过授权审批，实现特权用户权限分离管理；细粒度数据授权，数据授权管理是指完成了对身份的合法性验证后，还需对数据资源访问基于应用程序名、IP地址、操作系统账户、数据库实例名、时间等进行授权，实现权限进行集中管理，形成统一权限库安全知识库：建立安全知识库的，管理维护安全相关的标准、指导性文件等，支持上传、下载和在线阅读，组织机构安全文档集中存储，统一管理，便于知识查找和应用。安全合规检查：平台内置安全合规检查模板，支持自定义检查模板及快速下发，被检查单位按要求将检查项的证据材料上传，实现一站式的快速检查。安全知识学习平台：给机构内部成员提供统一的安全学习资源的下载途径，为数据安全专项培训提供教材资料；安全合规检查，平台内置数据安全检查模版和检查要求，可自行配置形成数据安全检查表，下发至各级部门（子平台），并支持在平台完成检查项确认和材料上传，形成检查一体化、标准化和自动化；汇聚多源安全分析引擎数据，生成风险信息并进行多维度关联分析、研判，包括风险分析决策，编排调度，联动处置。数据安全运营服务态势感知：围绕数据安全全生命提供多种态势感知能力。安全总体态势大屏直观展现出用户整体系统的风险情况。主要从风险概况、风险部门情况、区县风险地图、实时告警监控、风险类别排行以及整体风险趋势情况几个方面呈现整体系统的安全总体态势；数据流动大屏直观展现出用户敏感数据流动安全的情况。主要由数据流动安全评估、数据库异常TOP、异常前置机分布、API访问异常TOP、权限身份异常访问TOP、数据流动实时风险监控、共享平台之间的流动链路示意图等几部分组成；预警大屏主要对用户的预警单进行了监控。从总体预警通告概览（展示预警单总数及各等级分布情况）、市级风险告警、区域预警分布、预警趋势等方面进行详细分析；敏感数据分布监控大屏主要从各维度对敏感数据分布情况进行了分析监控。可对敏感数据的分布一目了然。从敏感数据变化、所在数据库排名、保护情况、敏感业务类型分布情况、应用访问情况、访问热度、等级分布、等级分布变化趋势等几方面进行展现；安全事件态势大屏主要对安全事件进行全面的分析展现。主要从事件风险等级、事件类型、区域、发生的时间趋势、实时事件、实时告警、工单的处理情况、处置效率等方面对安全事件。数据安全运营服务可视化展示：安全运营服务主要关注来自全世界不同地区的攻击源对内部资产的威胁情况，实时监测最新的告警事件，形成攻击者地域、风险资产、攻击类型分布的态势展示，外部攻击态势，主要关注来自全世界不同地区的攻击源对内部资产的威胁情况，实时监控境内境外攻击源的地域分布和国家排行，掌握各攻击链阶段的威胁变化趋势和最新外部攻击事件。攻击者追踪溯源，可视化分析大屏，为安全运维人员提供攻击行为分析、团伙分析、攻击取证信息、攻击趋势、攻击手段，攻击影响范围等信息，支持任意攻击者信息查询，可生成详细的攻击者溯源报告，并能够一键导出报告；资产威胁溯源可视化分析大屏，为安全运维人员提供包括被攻击行为分析、影响资产范围分析、攻击取证信息等，支持任意资产查询，可呈现被访问趋势、被攻击趋势、被攻击手段、资产状态，资产评分等信息。数据安全运营服务通报预警：对网络安全态势进行监测和预警，提供但不限于通报预警服务，时间通报服务，事件预警服务等。通过通报预警功能将各单位需要注意的风险快速下发到具体的单位，下级单位负责人可快速查看本单位存在的风险。数据安全运营服务指挥调度：工作台提供了工单、预警情况快速查看情况处理工单功能。主要包括工单的各状态情况统计并可链接查看；各级别预警单情况统计并可链接查看；待办工单快速处理和最新预警查看通道。落实人员管理，建立各单位活动的人员管理库，建立专项处置任务查看活动关键节点能力，承担重大活动安保任务。数据安全运营服务应急处置：根据各类数据安全监测及通报的情况，进行事件处置，及时消除影响和危害，包括隐患提醒服务，通报跟进服务，追踪溯源服务。同时平台可通过工单处理流程，将风险、预警项快速安排具体人员进行跟踪处理，实现责任到人，形成风险闭环。一键生成工单，支持对平台扫描发现的资产弱点、网络风险事件、数据风险事件、预警单一键生成工单，使其进入工单处理流程；工单处理流程，从未处理->处理中->已完成，可对所有工单状态进行跟踪处理，实现责任到人，形成风险闭环；安全报告，报告管理模块提供综合报表模板自定义组合排版功能。可根据用户需求自行组合综合性报表模板，如：安全总体分析报告、数据流动报表、告警情况分析报告等。提供Word、PDF等多种格式下载功能，且综合报表的子模块支持自定义。报告订阅模块支持综合报表周期性生成，如日报、周报、月报，且支持自动投递邮箱功能。★工单处理：支持将高安全风险、预警项快速的分配给具体的人员进行跟踪处理，实现责任到人，形成风险闭环（提供截图）。安全报告：按周期性自动生成由各维度分析报告组成的综合报表，如日报、周报、月报、年报，且支持自动投递邮箱功能。一键预警平台发现的风险事件：支持对平台扫描发现的资产弱点、网络风险事件、数据风险事件一键快速发起预警单到风险所属单位。收到预警的单位可将预警单一键生成工单指派给具体的负责人进行处理。自定义下发风险预警：支持自定义添加上级部门下发的风险预警或外部接收到的风险预警到具体的下属单位进行预警通告，使其引起注意。晾晒台：基于工单处理情况进行统计排名，统计维度包括待办工单、滞留24小时工单、滞留3日工单、滞留7日工单、总资产数、风险资产数、风险概率，支持导出统计排名。用户管理：提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立，支持根据对象属性自定义划分系统管理角色和一般用户角色，按照数据和功能分级灵活设置用户权限。系统恢复：支持安全模型的启用状态恢复出厂设置；支持通过权限认证实现数据恢复出厂设置。 | 3套 |

## 2、网络安全协调指挥平台

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **系统名称** | **功能模块名称** | **功能子模块名称** | **详细功能描述** | **数量** |
| 1 | 网络安全协调指挥平台 | 硬件 | 数据支撑系统硬件平台（专网区+互联网区） | 硬件规格：标准式机架设备、4个千兆电口+2万兆光口、cpu10核（10核\*1，CPU主频 2.2GHz，L3缓存 13.75MB）：、内存：256G（16G\*16，DDR4 26R）、硬盘48TB（4Tb\*12，7.2k 3.5 SAS 12GB/S）、raid5（2GB SAS 12G RAID 卡）、双电源； | 2台 |
| 业务系统硬件平台（专网区+互联网区） | 硬件规格：标准式机架设备、4个千兆电口+2万兆光口、cpu10核（10核\*1，CPU主频 2.2GHz，L3缓存 13.75MB）：、内存：256G（16G\*16，DDR4 26R）、硬盘48TB（4Tb\*12，7.2k 3.5 SAS 12GB/S）、raid5（2GB SAS 12G RAID 卡）、双电源； | 2台 |
| 分布式部署监测引擎平台（互联网区） | 硬件规格：标准机架式设备；内存32G；存储容量：标配1T；电源：双电源；网络数量：千兆电口\*2；最多可接入40个引擎。管理平台：网站统一管理中心，安全信息中心子系统，任务管理子系统、权限管理子系统、安全告警子系统、安全报告报表子系统、日志管理子系统。引擎调用管理：支持实现引擎智能调度，可将任务负载均衡分配至饱和度较低的引擎；任务下发前调用引擎进行扫描目标访问速度确认，择优下发至负荷小速度快的引擎。API接口：系统数据接口须符合《浙江省网络安全协调指挥平台建设指南》中对安全隐患数据接口的要求。须能实现与本次建设的衢州市网络安全协调指挥平台系统对接，为平台提供基础网站安全监测隐患数据。 | 1台 |
| 分布式部署网站监测引擎（互联网区） | 硬件规格：标准机架式设备；内存32G；存储容量：标配1T；网络数量：千兆电口\*2；单系统支持扫描不少于100个网站数。7\*24自动监测：支持7\*24小时自动监测服务、实现对网站漏洞监测、网页木马监测、敏感内容、可用性实时监测；平台支持周期性、单次与指定时间的监测。API接口：系统数据接口须符合《浙江省网络安全协调指挥平台建设指南》中对安全隐患数据接口的要求。须能实现与本次建设的衢州市网络安全协调指挥平台系统对接，为平台提供基础网站安全监测隐患数据。支持协议：支持http、https、wap协议；支持web2.0解析、Flash解析；支持包括Basic、Digest、NTLM在内的认证方式。代理模式：支持HTTP和SOCKS代理，并支持相应代理的认证方式。监测策略：支持漏洞扫描、网马监测、敏感关键字监测、可用性监测的独立策略设置，可独立配置监测周期、监测深度、监测页面数、监测引擎的独立指定；支持策略的灵活配置，可配置网站中扫描页面黑白名单，爬行名单等，支持在权限较高的管理后台中监测；支持限制扫描引擎的最大并发连接数，防止对网站产生过大访问压力；须具备基于JAVA的网页动态安全漏洞检测方法或技术。漏洞扫描：支持网页漏洞扫描，扫描SQL注入、XSS跨站脚本、伪造跨站点请求（CSRF）、网页木马、隐藏字段、表单绕过、AJAX注入、弱配置、敏感信息泄漏、弱口令、Xpath注入、LDAP注入、框架注入、操作系统命令注入、Flash源代码泄漏、Flash跨域攻击、Cookie注入、敏感文件、第三方软件、其他各类CGI漏洞等各种类型；系统厂家应为《信息安全技术 Web应用安全扫描产品安全技术要求》标准起草单位之一；须支持漏洞风险跟踪视图，进行历史风险跟踪与比对；支持对注入类漏洞进行渗透功能，能实现提取数据库类型、名称、表与字段等数据；支持对漏洞进行自定义检测功能，支持修改测试请求再次检测；支持对漏洞检测过程展现与分析，可比对正常请求与检测攻击的区别；系统须支持提供漏洞验证功能；须提供漏洞修复建议自定义功能，提供单独的漏洞提供建议；须提供漏洞修复建议自定义功能，提供单独的漏洞提供建议。可用性监测：支持对网站的应用可用性监测，访问延时监测，能及时识别网站的应用异常；支持对网站域名安全监测，及时识别域名解析变更，解析域名所在地，可检测域名劫持并告警；支持可用性异常告警，可配置异常超过多长时间即进行告警。网站监测：支持多种挂马方式检测，如：Iframe、CSS、JS、SWF等；须具备针对Javascript恶意代码的智能检测方法或技术。外链监测：支持检测页面中的可疑外链；支持检测页面中的错链、坏链。敏感关键字监测：支持定义关键字内容与分组；支持各种语义分析识别关键字。 | 3台 |
| 千兆以太网交换机 | 主要参数传输速率10/100/1000Mbps交换方式存储-转发背板带宽336Gbps/3.36Tbps包转发率132MppsMAC地址表支持黑洞MAC地址，支持设置端口MAC地址学习最大个数端口参数 端口结构非模块化端口数量52个端口描述48个10/100/1000Base-T自适应以太网端口，4个千兆SFP口控制端口1个Console口功能特性 堆叠功能可堆叠。VLAN支持基于端口的VLAN，支持QinQ，支持Voice VLAN，支持协议VLAN，支持MAC VLA。QOS支持802.1p/DSCP优先级标记，支持包过滤功能，支持SP/WRR/SP+WRR队列调度，支持基于端口的限速，支持基于流的重定向，支持时间段。组播管理支持IGMP Snooping，支持MLD Snooping，支持组播VLAN。网络管理支持命令行接口（CLI）配置，支持Telnet远程配置，支持通过Console口配置，支持SNMP（EImple Network Management Protocol），支持RMON（Remote Monitoring）告警、事件、历史记录，支持iMC网管系统，支持WEB网管，支持系统日志，支持分级告警，支持IRF，支持NTP，支持电源、风扇、温度告警。安全管理支持用户分级管理和口令保护，支持AAA认证，支持Radius认证，支持HWTACACS，支持SSH2.0，支持端口隔离，支持 802.1X，支持端口安全，支持MAC地址认证，支持IP Source Guard，支持HTTPs，支持PKI(Public Key Infrastructure，公钥基础设施)，支持EAD。 | 1台 |
| 关键信息基础设施单位流量数据采集专用设备 | ▲硬件规格：标准机架式设备；电源：1+1冗余电源 内存：32G 硬盘容量：2T\*2，带RAID1，可用磁盘空间不小于2T ；接口数量：标配10个； 接口类型：千兆RJ45网口\*2(管理口\*2)、千兆RJ45网口\*4、千兆业务SFP光口\*4（标配千兆多模光模块\*2）接口扩展：千兆RJ45网口\*4 +千兆SFP光口\*4 或万兆SFP光口\*2或万兆SFP光口\*4性能规格：MTBF 大于65000小时吞吐率：网络层2Gbps，应用层1GbpsWEB检测：HTTP最大并发数7万/秒邮件检测：邮件处理数: 150万封/24小时文件检测：5万个/24小时支持管理节点10个部署方式：旁路模式部署。文件攻击检测：对网络中传输的文件进行分离和检测，检测方式包含病毒引擎检测、静态分析、动态沙箱分析、基因图谱分析，发现病毒、木马、蠕虫等已知和未知恶意文件传播行为，并结合ATT&CK出具文件沙箱分析报告WEB攻击检测：对各种WEB攻击进行检测，支持SQL注入、命令注入、跨站脚本、代码注入和协议错误攻击检测，包含WEB攻击、WEB后门访问、WEB行为分析等Mail攻击检测：对邮件社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接、邮件恶意附件等失陷主机检测：通过识别DGA域名请求、异常流量、隐蔽信道通信，匹配远控工具指纹库、漏洞利用库和威胁情报等，多维度全方位发现失陷主机内部渗透检测：通过识别内网中横向扩散及渗透攻击行为，如内网扫描探测、恶意样本扩散、漏洞利用攻击及隧道搭建等行为，发现可疑的跳板机和被利用主机异常流量检测：对检测对象的会话特征进行多维度监控统计，并根据正常的网络行为建立模型，并分析检测对象多个异常参数的关联关系，判断是否有异常行为产生。包括DGA域名访问、远程控制行为、挖矿行为、漏洞利用、暴力破解、隐蔽信道传输及弱口令利用等异常流量的检测智能报表：提供综合威胁分析、主机威胁分析、文件威胁分析、外部威胁分析等多个智能报表，方便快速总览网络威胁情况，提供全方位多视角分析报告，有效替代人工威胁分析元数据日志提取：对网络流量元数据进行日志提取，并可通过多种方式外送到大数据平台型产品，提取的日志包括常见应用层协议的审计日志、风险日志、会话应用识别信息、会话应用流量统计信息、传输层流量统计信息、应用层流量统计信息等综合管理：提供综合管理和关联分析能力，实现告警数据挖掘、多维度关联分析、APT攻击链分析、攻击者视角分析和整体安全威胁态势分析等功能，同时可提供云端高级分析服务 | 5台 |
| 2 | 实时监测系统 | 监测总览模块 | 实时监测系统完成对全市网站安全监测、关键信息基础设施单位流量监测数据等获取，总体呈现并展示监测对象所受的攻击威胁、破坏、窃密、渗透等威胁信息，以及该对象网络、系统、数据等安全隐患和漏洞信息。应能及时发现、识别网络攻击威胁，监测恐怖组织、黑客组织、不法分子等的攻击活动、攻击行为、攻击方法手段；监测重点保护对象所受的攻击威胁、破坏、窃密、渗透等情况，以及重点保护对象的网络、系统、大数据等安全状况、存在的漏洞、隐患等，对全市的网络安全险情提供预警能力，为通报、预警、指挥等工作机制流程提供支撑。实时监测系统要能提供多种监测能力，包括重点网站监测能力、流量监测能力、网站安全防护数据对接能力、第三方威胁情报对接能力、工控系统安全监测能力。支持查看平台监测的系统数、安全事件数、安全隐患数、设备告警数。支持查看安全事件和安全隐患的区域分布。支持查看安全事件、安全隐患和设备告警的趋势统计。支持安全事件分类统计和事件及隐患的行业排名。★建立全维度实时监测体系，监测方式至少包括：网站监测、流量检测、资产探测等（提供截图）。 | 一项 |
| 网站监测模块 | 网站监测引擎管理，任务调度，周期设置；网站隐患数据对接；网站篡改事件数据对接支持对多网站创建监测任务，支持以区域、监测周期、任务模板、标签、备注等条件创建监测任务。平台监测周期、任务模板、以及监测时长支持自定义填写或选择。支持任务详情查看，包括历史监测记录，单次监测任务详情，任务状态等。支持查看、导出扫描结果，包括扫描纪录，该次扫描纪录的威胁，支持查看威胁详情。支持查看最新隐患详情、累计隐患查询和隐患录入。最新隐患详情可导出存在隐患的网站信息及威胁列表，查询隐患详情，包括所属单位、网站名称、域名、区域、扫描时间、隐患个数、分级分类、隐患列表（包含隐患类型、等级、出现次数、发现厂商）等。支持隐患录入和查看、导出网站累计隐患列表及列表报告下载。支持对针对扫描出的隐患做通报，包括对公安、单位发布提醒或者发布限期整改。 | 一项 |
| 流量监测模块 | 支持按照事件告警级别、数据类型、风险类别、客户端IP、响应码、时间范围等查询告警信息，并支持导出，对接流量监测引擎，实时攻防数据获取，包括僵木蠕毒传播、Web攻击、钓鱼邮件、恶意文件、DDOS攻击等；识别攻击者IP、攻击方式、攻击时间、攻击目标。 | 一项 |
| 资产探测模块 | 基于云端资产探测引擎，支持对辖区内的邮件资产、互联网资产、工控资产等进行检索查询，支持资产普查数据对接，支持实现IP段资产情况分析，包括操作系统、开放端口、开放协议、可能使用用途等。 | 一项 |
| 网站安全防护数据 | 支持对接云防护产品告警日志。 | 一项 |
| 第三方威胁情报数据 | 手机号安全情报，识别风险画像标签，包含黑灰产活跃信息，基本归属地信息等；IP安全情报，输出IP的识别风险画像标签，包含黑灰产活跃信息，基本归属地信息等；邮箱风险画像，输出邮箱地址的信息和风险描述；安全事件数据接入；网站、系统漏洞数据接入；其他数据内容定制。 | 一项 |
| 工控监测系统模块 | 对接在线工控系统识别引擎；支持对接工控系统主动上报的监测数据。 | 一项 |
| 3 | 资产普查模块 | 资产总览模块 | 提供监管范围的整体情况、统计情况，并提供资产管理的核心向导。资产普查系统设计主要采集关键信息基础设施资产要素信息，如资产类型、系统版本、资产归属等。实时掌握资产运行态势，为准确评估各类隐患风险影响范围提供数据支撑。支持重点单位、重点系统、政务云系统、省直属系统和接入地市等类型资产展示，且支持交互，可对某一类型单独突出，做重点展示；需体现区域内资产指纹底数，指纹概况需包含存活IP、开放端口种类、开放协议种类、数据库、操作系统等信息。直观展示辖区内网络资产的整体统计状况，统计的维度包括单位总数、系统/网站总数、服务器数等。支持单位数、服务器数、网站与系统的行业分布；支持网站系统数、服务器数在单位资产排行统计；支持各操作系统在重点监管系统中的占比、端口使用情况占比、服务占比情况、服务器外地部署情况。 | 一项 |
| 资产管理向导 | 资产管理向导过程共计分为四大过程，新增向导、查询向导、导入向导、导出向导。 | 一项 |
| 资产分析模块 | 基于服务器管理数据可快速定位受影响的系统、服务器等受影响资产范围。 | 一项 |
| 资产管理模块 | 支持对单位信息的维护与管理，提供对单位信息的增删改查。支持从单位查询到相关系统与服务器等信息。支持对单位的网站与系统进行管理，包括网站与系统的增删改查、导入导出、系统报告、网站档案等。对监管范围的单位进行管理与维护，提供增删改查等功能，并能查看单位整体评价，关联系统与服务器对监管范围的网站与系统进行管理，提供增删改查功能，并能够查看网站与系统的整体评价对监管范围的服务器进行管理，提供增删改查功能。对监管范围的IDC进行管理，提供增删改查功能，标识各IDC的管理范畴与服务器信息。对监管范围的动态IP端进行管理，为溯源分析、威胁识别提供个人IP的识别提供辅助数据录入，支持增删改查 | 一项 |
| 4 | 信息通报系统 | 安全事件管理 | 支持接入第三方数据源上报的网络安全事件；支持对安全事件进行管理，并可通过区域、发现时间、事件等级、事件类型、发现厂商、通报状态、关键字等进行高级查询。 | 一项 |
| 信息同步机制 | 支持建立信息同步机制，对各单位、主管单位、监管单位发布信息同步；支持按照发布时间、关键字查询公告信息，支持公告详情查看；可以快速切换我发布的公告和我接收的公告；支持发布新的公告，内容包括信息标题、公告内容、接收单位、接收人、反馈时间、附件等。 | 一项 |
| 信息通报模块 | 支持建立信息通报机制，实现与通报系统对接，完成信息通报流程；支持建立隐患提醒、整改流程；支持建立安全事件通报流程；支持建立隐患、事件跟进机制；支持将我收到的、我发布的、抄送我的、待我审核的安全事件通报进行统一汇总，包括事件通报跟进、隐患整改管理和隐患提醒管理。可查看通报的事件信息，包括通报的详情（包括发布人、接收人、通报状态等）、事件详情、该次通报的通报记录等信息，实现对整个通报过程进行跟踪记录。支持通报的签收、处置和反馈。支持Web端通报的同步发布、接收和处置反馈。支持对通报过程进行跟踪记录，完整记录预警任务发起、查阅、处理和审核等各阶段的时间点、处理人员和操作内容等详情，查看通报详情、通报记录、隐患详情。支持提醒管理，对发现的最新隐患发布提醒或下载报告，支持指定通知接收人、通报类型、隐患详情描述及上传附件。对发现的最新隐患下发限期整改通知或下载报告，支持指定通知接收人、整改类型、整改限期日期、隐患详情描述及上传附件。 | 一项 |
| 专项预警模块 | 支持按照红色、橙色、黄色和蓝色不同等级发布有针对性的预警，预警信息内容需包括接收单位信息、基本情况、危害评估、处置要求、反馈时间、附件等。 | 一项 |
| 报告中心模块 | 支持生成不少于四种类型的报告，报告类型至少包括综合报告、安全通报报告、整改通知书、整改统计报告。支持用户自主选择报告数据范围，并且可支持查看历史生成的报告。支持按照区域、时间范围生成综合报告；支持查看历史报告。支持按区域、行业、网站等级、具体单位、具体网站等维度生成安全通报报告。支持根据预先设定的模板，生成整改通知书。整改通知书应包含区域、行业、网站等级、单位类型、具体单位、具体网站等信息。并支持查看整改统计报告。支持针对四种报告设置报告模板，包括设置首页LOGO、页眉页脚、具体报告文案等信息。 | 一项 |
| 5 | 应急指挥系统 | 重大活动管理模块 | 支持针对重大活动建立安保任务。 | 一项 |
| 人员管理模块 | 支持建立活动的人员管理库，应用在不同活动中使用。活动库应包含支撑单位、安全专家、安全专家组等人员。支持配置每天的值班人员，值班人员应包括值班公安和值班的技术专家。 | 一项 |
| 应急预案库模块 | 支持建立应急预案库，应包括四种等级、四种类型的应急预案。 | 一项 |
| 专项处置 | 支持多种渠道建立处置任务；支持查看活动关键节点，查看任务信息与处置进度；支持对人员进行调度，包括将处置任务下发给值班专家等人。 | 一项 |
| 现场调查模块 | 支持组织相关单位开展现场调查；支持实现调查结果存档。 | 一项 |
| 6 | 检查督查系统 | 现场检查基本情况统计 | ★支持对现场检查工作从不同维度进行统计，包括检查资产总数、发现的漏洞数量、年度检查的任务信息、渗透测试的情况、检查队伍评价等。支持创建检查任务，包括任务名称、负责人、任务时间、检查对象、任务模板、支撑队伍等信息（提供截图）。支持检查任务管理功能，包括编辑、删除、查询、查看详情、上传任务结果、评价任务情况等操作。现场检查模块需要从不同维度对工作情况进行统计说明，主要包括年度检查的任务信息、发现的漏洞数量、渗透测试的情况、检查资产总数、检查队伍评价（平均星级排序，平均星级可有半颗星）。 | 一项 |
| 建立检查任务 | 提供创建检查任务的功能入口，支持创建检查任务。 | 一项 |
| 任务清单 | 任务创建成功后在任务清单中存档，支持任务的基本管理，编辑、删除、查询、查看详情、提交报告、评价任务情况等。 | 一项 |
| 自查统计 | 自查统计主要针对安全自查的工作维度进行数据统计，显示整体工作情况，主要维度包括自查任务的数量统计、自查任务的进度情况显示、自查单位数量、自查渠道提交的漏洞数量、资产数量、测试报告数量。 | 一项 |
| 发布自查任务 | 网信用户可以创建自查任务，并通过通知系统通知相关单位。 | 一项 |
| 单位用户端提交检查结果 | 系统在单位端开放自查模块，接收自查任务，自查任务需要有自查清单，对自查任务可以下载检查模板，查看检查要求。完成自查工作后，可以根据模板上传自查结果。 | 一项 |
| 7 | 事件案例系统 | 数据接入与存储 | 实现对多源异构数据的标准化汇聚接入、预处理和存储。 | 一项 |
| 大数据分析与挖掘 | 基于机器学习、知识计算、概率统计、聚类关联等基础分析引擎为上层业务提供基础分析支撑服务；通过综合关联分析、趋势预测、威胁事件专项分析、情报挖掘、决策支持等引擎，面向业务进行多源数据分析挖掘。 | 一项 |
| 事件案例归档 | 具有典型事件案例的归档能力，结合攻击链、扩线分析等方式方法，总结归纳已发生的攻击事件与行为，对典型案例进行研判分析，并完成归档，以建立事件案例库。为后续的网络安全工作，提供科普、教育、警示的作用。★支持对归档的隐患提醒进行收藏、批注和增删改查，如通过区域、等级、发起方、所属单位、标签、关键字对归档的隐患提醒进行查询（提供截图）。 | 一项 |
| 事件案例研判 | 支持对归档事件的研判分析，由平台或组织发现的攻击行为为起点，通过，经过关联分析、扩线分析，产生威胁分析拓扑以及攻击画像，而后通过专家或平台结合受攻击系统的等级情况，进行影响评价与定性，对于相关的事件、行为进行合并归档，最后产生事件案例的最终说明。 | 一项 |
| 8 | 考核评估系统 | 统计分析模块 | 支持综治考核统计，按照单位考核得分进行高低进行排名，支持考核单位所属行业及行政区域显示；支持按年切换查看历史数据。对安全监测、安全检查、应急处置过程中产生的安全数据和结果进行汇总分析，形成总结性安全报告。支持日常考核统计，按照系统级别、时间对漏洞/事件趋势、最新安全事件、自检完成情况进行展示；支持对现场检查工作情况、本发安全服务情况、本地系统建设情况等进行展示和评分。支持数据报送统计，对技术支撑单位提供的数据量、数据质量进行综合统计，数据报送类型有资产数据、漏洞数据、事件数据、攻击威胁数据。 | 一项 |
| 安全评价模块 | 支持对辖区内成员单位、行业主管单位、下属行政区域网络安全状态的整体评价，支持按天、周、月、季度、半年、年度进行安全评定。安全评价是常态化的安全监控，主要以发现问题，是否安全为角度。 | 一项 |
| 工作质量考核模块 | 支持对支撑单位现场检查工作及提供的数据质量进行评分，其中，检查工作采用五星考评机制进行考评，得分在支撑单位考核中直接给出。数据质量基于漏洞数据、事件数据、攻击威胁数据、资产数据四个维度进行评价。支持数据质量评分，由系统根据后台数据的数据量、数据质量自动计算得出，评价时需给出具体评价说明。数据质量的评价从漏洞数据、事件数据、攻击威胁数据等维度评价。 | 一项 |
| 9 | 态势感知系统 | 综合态势分析 | 支持网络安全总体态势分析，包括当前监管对象统计、实时监测隐患数统计、通报预警统计、风险趋势、高危系统排名、高危地区排名、监测对象分布统计、事件与隐患统计、通报预警统计等内容。从整体情况分析安全态势，从区域情况分析安全态势，从监控目标类型分析安全态势，统计各纬度监控数据量级，统计安全隐患、事件最多的行业、单位、信息系统，统计各类安全事件、隐患的占比，统计隐患、事件、攻击情况的趋势变化，实时显示最新高危以上隐患和事件。地图需支持全屏化展示，显示街道地图，便于重点时期对于网络安全事件应急处置进行指挥调度。且具备地域列表按钮，点击对应的地域，地图需支持跳转到对应地域的地图；页面数据支持同时从不同时间维度筛选出数据作为展现，时间维度至少包含：近一周、近一个月、近三个月、近一年等。监管对象分类至少包含重点单位、重点系统、政务云系统、市直属系统、ICP备案和接入地市等几类。实时监测隐患事件分类至少包含网站后门、DDOS攻击、僵木蠕病毒、入侵攻击、反共、黑页、博彩等类型。风险趋势、高危系统排名、高危地区排名、监测对象分布、事件与隐患、通报预警统计等内容需支持查看详情。 | 一项 |
| 资产态势分析 | 支持重点单位、重点系统、政务云系统、接入区县等类型资产展示，且支持交互，可对某一类型单独突出，做重点展示。支持不同监管对象资产指纹、行业分布、类型分布、安全等级分布的统计展示。从多纬度统计资产分布情况，包括资产类型、操作系统、协议端口等，统计最新行业、单位、信息系统安全指数。需体现区域内资产指纹底数，指纹概况需包含IP段数、存活IP、开放端口种类、开放协议种类、数据库、操作系统等信息。 | 一项 |
| 隐患态势分析 | 统计市内、区县威胁隐患数量，实时展示最新发现的高危以上安全隐患情况，统计各单位、系统威胁隐患情况，统计各隐患类型的占比分布，统计各类型安全隐患爆发趋势。支持安全隐患分析，内容需包括隐患统计及分类、专项隐患统计、第三方威胁情报接入展示、最新隐患、隐患趋势、隐患区域位置统计、行业隐患分布、高危系统排名等；开放接口支持第三方威胁数据接入，并且对各数据源及隐患类型进行统计。支持按时间粒度对隐患区域位置统计、行业隐患分布和高危系统排名等内容进行筛选统计展示。支持对struts2、webshell等专项隐患进行消息推送；隐患区域位置统计、行业隐患分布、高危系统等内容需支持详情展示,展示隐患排行TOP5的系统。 | 一项 |
| 网络攻击态势分析 | 支持网络攻击分析，内容需包含网络攻击分类及统计、监控总览及分类、最新攻击消息、攻击趋势、受攻击行业分布、攻击类型分布、攻击区域/受攻击区域排名、攻击IP/受攻击IP排名、攻击源流量等。网络实时攻防情况：攻击者、攻击目标、攻击事件、攻击方式统计；攻击行为画像：攻击分类统计，包括DDOS攻击、WEB攻击、僵木蠕传播等。受攻击影响对象统计，攻击源统计监控总览需按系统数、攻击数、访问数和高危系统数进行分类统计。攻击趋势、受攻击行业分布、攻击区域/受攻击区域、攻击IP/受攻击IP需支持查看详情。支持按时间、攻击类型分布、攻击区域（境内攻击源/境外攻击源）、攻击IP/受攻击IP排名等内容进行筛选统计和展示。支持实时攻击地图可视化模拟当前攻击/访问状态，需采用迁徙图进行攻击的可视化展示,支持以2.5D拓扑模式呈现。 | 一项 |
| 安全事件态势分析 | 安全事件类型统计，新安全事件情况，事件名称、类型、数据来源、事件说明、时间等。安全事件分布统计，安全事件证据情况，行业、区域事件统计。支持安全事件分析，内容需包含重点监测系统数、安全事件数、安全事件分类统计、事件趋势、最新事件概览、事件类型分布、事件区域排名、事件取证展示等。安全事件分类需包含拒绝服务攻击、扫描探测、隐患利用、有害程序、信息篡改等类型。事件趋势、事件类型分布、事件区域排名需支持详情展示；支持按时间或行业对安全事件分类统计、事件趋势、最新事件概览、事件类型分布、事件区域排名、事件取证等内容进行筛选统计和展示。支持对安全事件查看截图取证详情。 | 一项 |
| 预警处置态势分析 | 统计市内、区县通报工作进展情况，统计市内、区通报工作效率，统计各单位通报反馈情况，统计最新安全通报及其跟进情况，统计预警工作开展情况。支持预警态势分析，内容需包含一般预警数量统计、专项预警数量统计、预警等级分布、处置效率统计、预警列表、专项预警行业统计、专项预警区域分布、近一年预警统计等。专项预警统计数据需包含政府机关、行政机关、教育、能源、金融、交通、水利、卫生医疗、社保、环境保护、公共事业、信息服务等行业。 | 一项 |
| 10 | HW演练 | 基线检查 | 根据既定的检查规范及方法，采用人工检查用表（checklist）、脚本程序或基线扫描工具对评估目标范围内的主机系统安全、数据库安全、中间件安全等进行系统的策略配置、服务配置、保护措施以及系统和软件升级、更新情况等。 | 三年 |
| 专项排查 | 采用人工和工具相结合的方式针对客户系统的服务器逐个做webshell后门排查，做到确保客户系统服务器本身的安全性保障。 | 三年 |
| 远程安全评估 | 提供Web、数据库、基线配置核查、操作系统、软件、弱口令、端口与服务识别的综合漏洞扫描功能，能够准确发现网络中各主机、设备、应用、数据库等存在的网络安全漏洞，从而发现网络安全问题，起着评估整个系统安全的重要作用。 | 三年 |
| 可信众测 | 采取远程漏洞挖掘的方式进行服务，服务范围包含但不仅限于Web应用系统安全测试、手机移动客户端安全测试、嵌入式设备（含智能设备）安全测试。 | 三年 |
| 渗透测试 | 模拟黑客的攻击方法对系统和网络进行非破坏性质的攻击性测试，目的是侵入系统，获取系统控制权并将入侵的过程和细节产生报告给用户。 | 三年 |
| 总结 | 将对本次安保工作进行全面总结，针对客户目前的安全防护水平、存在的不足、安保中遇到的问题等进行总结，形成书面材料，并与客户相关人员充分沟通，为客户后期信息安全建设提出建设性意见。 | 三年 |

## 3、网络安全研判平台

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **系统名称** | **功能模块名称** | **功能子模块名称** | **详细功能描述** | **数量** |
| 1 | 网络安全研判平台 | 攻防实训平台 | 平台硬件 | 硬件规格：标准机架式设备；电源：1+1冗余电源；CPU：10核\*2，主频2.2GHz,13.75MB L3缓存；内存：16G\*8，DDR4；硬盘容量：4T\*4，3.5寸，SAS；固态盘：960G SSD\*2；电口：千兆网口\*4；光口：万兆光口\*2（带多模光模块）。许可授权：允许同时60人同时在线实训或竞赛。 | 2台 |
| 综合管理系统 | 综合管理是培训系统、实操系统、仿真功能、实训工具库、攻防对抗系统统一化、集中化3A认证管理平台，具有云计算、云资源统一调度管理能力。性能：单台设备并发30人。产品要求：具有《中华人民共和国国家版权局》颁发的计算机软件著作权登记证书。工作模式：平台采用HTTPS安全协议加密；提供全中文WEB管理界面，无需安装任意客户端软件或插件。平台提供物理机管理，支持手动添加关联多台物理机设备资源；支持多台主机资源的集群管理，支持集群的横向扩容，并能通过弹性云计算方法自动轮询调度虚拟主机。平台支持容器、KVM两个类型的集群管理，其中KVM支持至少三种以上的集群类型。平台提供网段管理，支持配置多IP地址段，用以自动分配创建的实例化资产。平台支持发布公告信息，可按照角色、部门、个人为公告发布对象进行发布，发布的内容可附带文本、附件等资源。平台支持查看软硬件资源创建情况的统计，包括已创建交换机总数、路由总数、场景总数、主机总数等数据信息。支持查看平台整体资源占用和分配情况，包括CPU、内存、硬盘、虚拟机、路由、交换机等。支持查看单物理机硬盘、内存、CPU的使用情况。支持查看平台日志吞吐量的相关数据情况。平台支持对实例进行管理，包含虚拟机、docker容器等类型实例，可对实例进行关机、重启、回收、快照的创建与恢复、重置等独立操作与统一化管理，同时支持查看实例的IP和开放的端口号，支持通过浏览器的方式操作虚拟终端。平台支持日志审计功能，支持记录和查看平台用户的操作日志信息，支持日志检索以及日志批量导出。 | 1项 |
| 培训学习系统 | 具有网络安全、主机安全、应用安全、数据库安全、中间件安全五大层面课程与实验资源，支持按阶段、部门、岗位、难易程度进行学习、实训，具有完善的动态考核机制对学员学习效果、知识与技能掌握实际情况进行全方位考核。系统内置资源含初级、中级、高级，课件具有培训课件、多媒体课件、CTF实验课件。课程支持三级标签管理，每个课程可以拥有多个标签，平台能够按照标签进行课程的分类和筛选，同时课程支持按照难易程度进行划分和筛选。平台支持用户自定义编排课程，支持将课程设置为公开课，设置为公开课的课程，所有人均有权使用，当为非公开课的时候，课程为用户私有课程，只有创建者才能使用。课程可设置多个知识点及关联相关课程，通过关联课程功能可建立多课程之间的关联管理，单个课程可包含理论知识、实验、考试、作业等内容，课件资源类型支持PDF、WORD、MarkDown、视频、实验靶机、场景等；平台支持关联引用知识库和考试中的资源，快速创建课程，课程支持当前参与学习人数和完成学习人数的统计。平台提供学习路径管理功能，内置常用学习路径资源，同时支持教员自行添加与组建新的学习路径，学习路径支持分阶段管理，同时每个阶段按顺序设置多门学习课程。平台提供培训管理功能，支持教员以班级的维度进行学习计划的制定和下发，并对学习成果进行管理。★平台支持通过关联内置课程制定培训计划，单场培训支持添加多个班级，针对人员的学习情况，可以以个人、单个班级、整场培训的纬度进行人员及相关学习成果的管理，包括学习进度、作业提交情况及分数、考试情况及分数，支持教员对学员作业和考试进行批改、打分（提供截图）。支持课程目录导航，快速进行章节的切换，导航中显示章节的课时数和个人学习进度，同时当课程拥有多个课程资源的时候，支持课程资源的快速切换。课程支持随堂笔记和作业功能，学员可以提交和查看自己的学习笔记和作业，教员可以查看课程中所有学员的课堂笔记。视频和课件，支持以普通模式和全屏模式进行播放，视频支持切换倍速、调整播放进度。实验课程支持关联实验工具，工具类型支持虚拟机型和下载型，虚拟机型工具可直接在界面启动后直接使用。实验课程支持实验的拓扑展示及拓扑的构建和回收，支持通过拓扑图，点击查看终端详情并进入虚拟终端操作界面进行终端的管理和操作，支持拓扑和实验内容的同屏展示，支持虚拟机终端操作界面与实验内容的同屏展示。实验环境支持开机、关机、重启、重置、生成快照、恢复快照、回收资源等操作方式，同时具有自动回收资源、实验环境超时自动回收、延长实验时间的能力。平台支持学员统一查看我参与的课程、路径、培训，以及相关学习进度、作业及考试的情况和得分，作业支持根据已上交、未上交的状态进行筛选，考试支持根据已未开始、进行中、已结束的状态进行筛选。 | 1项 |
| 安全实训系统 | 提供进行有针对性的信息安全上机实验服务，提供各种漏洞场景，并且提供详细的实验步骤说明，结合理论教学，在真实的系统中去了解黑客如何利用漏洞对系统造成破坏，提高漏洞检查、测试、防御的能力。平台支持用户自定义安全研究课题，并能够对自己的安全研究进行管理，同时可以公开安全研究与成果，跟所有人共享。创建安全研究时，支持设置难度等级，关联安全场景，支持用户针对自定义安全场景开展安全研究工作，提交研究成果，研究成果支持上传附件或关联平台漏洞作为相应成果，附件类型支持word、pdf、mp4等格式。平台支持对安全研究的参与人数进行统计，对安全研究成果进行管理，对成果数量、成果浏览量进行统计。支持查看安全研究场景拓扑，并支持安全场景的构建、回收、重新创建、快照的生成与恢复，支持通过拓扑图，点击查看终端详情并进入虚拟终端操作界面进行终端的管理和操作，拓扑图支持展示创建的实例清单和相关实例的实时状态。支持对场景的实例资源进行管理，安全研究的创建者可以以资源分组的方式查看所有研究人员创建的实例资源并进行管理，对分组内的实例资源进行一键回收，安全研究参与者可查看自己创建的实例资源，并进行管理。 | 1项 |
| 攻防对抗系统 | 攻防对抗系统支持CTF夺旗、CTF闯关、CTF攻防主流三种竞赛模式，内置了丰富的网络安全攻防题型及典型攻防对抗业务环境场景，提供了灵活的自主可定制功能，具有十六种2D、3D可视化大屏竞赛数据展示，支持技能领域方向展示，使竞赛过程更具趣味化，直观的展示竞赛结果。有效的开展网安人才培养、人才挖掘、人选选拔。支持混合竞赛模式，一场竞赛可包含多个阶段，每个阶段可添加不同赛制类型，同时支持依据人数、分值、排名等设置阶段的准入条件，赛制类型支持CTF夺旗赛、BTC闯关赛、AWD攻防赛、CTL领地赛四种。平台支持多场赛事并行运行且相互之间不干扰。每场竞赛都支持独立首页展示，首页包含竞赛的基本信息、阶段基本信息、竞赛规则、奖励等信息。竞赛内支持公告功能，允许管理员或裁判向所有选手发布公告，公告内容支持图片、文字及附件的形式。赛题支持以类别、标签、难度、套题等多个维度进行分类管理，可根据靶机、附件、题目等多类信息进行赛题检索，同时赛题支持查看解题提示和解题思路，赛题支持共享靶机和独占靶机的模式，对于共享靶机的赛题支持靶机负载。★竞赛支持平台用户和非平台用户两种人员组织模式，平台用户模式通过关联平台内用户组织竞赛，用户的竞赛相关成绩可被记录到用户信息中，支持可延续性，非平台用户模式通过导入临时用户的方式组织竞赛，此类用户仅限于当次比赛使用，成绩没有可延续性；竞赛支持单兵作战模式和团队作战模式，并支持设置最大参赛人数或团队数，对团队赛支持设置团队最大人数（提供截图）。竞赛支持设置作弊处罚方式，包括不处罚、只警告、扣除所答题分数、自动禁赛四种方式。竞赛支持设置是否对选手开放排行榜，是否在大屏显示排行榜，并同时支持对大屏的标题和logo进行配置。竞赛支持配置靶机访问的IP白名单，白名单中的IP地址支持访问任意靶机。竞赛内用户分为管理员、裁判、选手、观众四种角色，支持通过批量导入、关联平台用户（平台用户模式竞赛）或手工添加（非平台用户模式竞赛）的方式添加竞赛相关用户，支持导出相关选手或团队信息。支持对团队及个人基本信息、积分、排名、团队状态（正常、作弊、禁赛）等内容的查看，支持对积分及团队状态、团队名称进行筛选查看。可对选手进行禁赛、解禁、设置作弊、取消作弊等操作，对被禁赛的选手将不能继续参加竞赛，支持对选手进行加减分处理，并支持选择自动发布公告。竞赛根据比赛设定的时间自动开始和结束比赛，同时支持以手工的方式提前开始、和提前结束，并可对竞赛进行暂停和恢复的操作。竞赛列表支持查看赛事基本信息，包括：参赛模式、阶段情况、比赛起止时间、参与人数、竞赛状态、比赛题目数量、题目靶机数量等信息。竞赛开始后，支持自动构建靶机环境，并为环境制作初始快照，竞赛开始前，支持提前手动构建靶机环境，可对靶机进行一键准备、一键回收、批量开机、关机、重启、重置、回收、生成快照、切换竞赛网络、切换中立网络等功能。竞赛概述支持对整场比赛相关情况进行概览，包括竞赛基本信息、实际参赛人员情况、赛题准备进度情况、竞赛靶机状态、竞赛阶段相关信息，阶段信息包括阶段的类型、时长、题目准备情况、参赛人数、题目难易程度、阶段状态、阶段准入条件，并提供快速入口进入相关信息的配置界面。竞赛过程中，支持对本场竞赛和各阶段的基本信息进行配置，包括竞赛名称。支持对单个竞赛阶段的独立管理和配置，其中包含该阶段下的选手、题目、解题思路、各类竞赛展示榜单等资源的统一管理。竞赛开始前和过程中都支持添加新的阶段。阶段支持根据设定的时间自动开始和结束，同时支持以手工的方式提前开始、和提前结束，并可对阶段进行暂停和恢复的操作阶段概述支持对当前阶段相关情况进行概览，包括阶段基本信息、参赛人员情况（包括正常选手人数、作弊选手数量、禁赛选手数量）、题目准备情况、靶机准备情况、阶段倒计时等内容，并提供快速入口进入相关信息的配置界面。阶段提供赛事监控功能，支持对阶段中所涉及到的所有靶机的相关信息进行查看和管理，包括靶机的基本信息、靶机的服务状态、靶机归属团队/选手信息、靶机当前网络状态、需准备靶机总数、已准备靶机数量、服务异常靶机数量，并支持对靶机进行一键准备、一键回收、批量开机、关机、重启、重置、回收、生成快照、切换竞赛网络、切换中立网络等功能。阶段内用户支持手工关联，或选手满足阶段准入条件后自动进入的方式进行添加。竞赛支持选手以附件的形式上传解题思路，支持管理端对解题思路进行查看和管理，并支持下载或批量导出解题思路。支持在比赛过程中新增赛题。CTF夺旗赛开题方式支持题目自动全开、按顺序两种形式，顺序开题模式支持用户手工打开任意题目。CTF夺旗赛计分方式支持防PY模式，普通模式和递减模式，其中防PY模式是指选手得分为题目总分除以解出题目的选手数量，递减模式支持按分数比例递减和按固定分值递减，并可设置最低比例和最低分值。CTF夺旗赛赛题支持以分组的方式进行管理，支持将题目设置为隐藏题，隐藏题只有在手动设置显示后选手才可见。CTF夺旗赛对于多靶机和多附件的题目，支持以题目的视角查看相关题目的靶机情况和附件情况，包括靶机的基本信息和分配情况，附件的基本信息和分配情况等。CTF夺旗赛在阶段开始前和进行中，可对题目的名称和描述进行修改，对于未被解出的题目可以进行题目分值的修改。CTF夺旗赛支持积分榜、奖牌榜、解题速度榜等维度的数据统计，其中，解题速度榜支持以题目或选手的视角进行查看，并支持以上榜单的导出。CTF夺旗赛的非共享靶机只允许拥有靶机的选手进行访问，其他选手无法访问，各靶机之间实现网络隔离，不能互相访问。BTC闯关赛的计分方式可支持普通计分和通关前三名额外加分的计分方式；BTC闯关赛概述页，支持展示各关卡当前的通过情况。BTC闯关赛，支持对题目的基本信息进行配置，并支持对题目内关卡的基本信息进行配置，同时支持显示或隐藏关卡，显示关卡难度、顺序、分值、过关、闯关人数等信息。BTC闯关赛的所有选手独享靶机环境，且只允许拥有靶机的选手进行访问，其他选手无法访问，各靶机之间实现网络隔离，不能互相访问。BTC闯关赛支持查看个人积分榜和团队对积分榜并支持积分榜的导出。AWD攻防赛的计分方式可支持固定计分方式和零和计分方式，支持手动设定分值。★AWD攻防赛，支持设置初始分值和每轮的时长，支持设置是否对选手开放重置靶机功能，支持设置靶机重置保护时间，支持开启靶机重置扣分模式，该模式下支持配置最大免费重置次数及超出次数后的扣分分值（提供截图）。AWD攻防赛各团队之间的靶机环境互相隔离，只允许选手端进行访。单场AWD攻防赛支持关联多道赛题，支持设置题目的开放和隐藏。AWD攻防赛支持竞赛中的流量数据抓取，提供大屏展示竞赛攻防过程。AWD攻防赛支持积分榜、攻击榜、防守榜、运维榜等维度的数据统计，其中，运维榜是指因服务故障扣分数量的排行榜，并支持以上榜单的导出。CTL领地赛支持初始全开或手动开启区域两种开题方式。CTL领地赛支持分别设置普通题及领地题的独立计分方式，且可设置普通题的计分方式为独占或者递减两种方式，递减方式支持设置递减比例和最低比例，同时支持设置最大得分人数。CTL领地赛支持设置是否开启选手自有领地以及是否提供自由领地靶机的用户名与密码，并支持设置初始保护时间。CTL领地赛支持以区域的方式进行题目分组，支持夺旗题和领地题，针对区域进行开启或隐藏设置，并支持针对赛题进行开题、关题、显示、隐藏等操作。CTL领地赛支持积分榜、领地占领数量榜、CTF积分榜、拓荒榜等维度的数据统计，其中，拓荒榜是指选手第一个占领新领地数量的统计排行榜，并支持以上榜单的导出。★CTF夺旗赛支持全题型动态FLAG的方式进行防作弊；CTF夺旗赛通过防PY计分模式防止选手共享答案（提供截图）。BTC闯关赛所有选手独占环境，而且每一套环境都是动态FLAG，确保所有选手拥有不同的FLAG。AWD对抗赛FLAG是通过选手拥有的随机TOKEN提交申请获取，确保每一个FLAG都只有当前团队可用，防止交换FLAG。竞赛拥有排行榜和可视化中心，排行榜可查看整场比赛选手的总分、排名和各阶段分值，可视化中心包含整场比赛及各阶段的得分曲线、实时事件、积分榜和态势大屏等大屏展示。★态势大屏支持以雷达图形式展示选手的技能分布，支持自定义剧情的展示，自定义剧情包括对话、视频、图片等形式，支持展示选手的攻防态势和解题情况（提供截图）。 | 1项 |
| 课程资源体系 | 平台内置信息安全基础、应用安全、安全运维、安全编程、安全工具、攻防竞赛6大类课程，具体包含安全术语、安全意识、保密意识、网络安全法、密码学、网络安全、网络安全协议、系统安全、Web安全、渗透测试、代码审计、移动安全、二进制安全、物联网安全、工控安全、安全加固、安全防护技术、应急响应、编程技术、数据库技术、渗透工具、逆向工具、CTF夺旗赛等方向的课程。同时，平台根据安全运维工程师、软件逆向工程师、渗透测试工程师等职业方向规划学习路径。 | 1套 |
| 信息安全初级课程：含网络安全形势、HTTP协议技术、Web安全架构、数据库安全、网络渗透测试技术六门标准课程，31节课件。实验：具有网络安全、主机安全、数据库安全、应用安全四大层面实验，共11节实验。 | 1套 |
| 信息安全中级课程：恶意代码技术、Web安全技术、Web安全测试技术、Web开发技术、源代码审计、中间件安全，共100节实验：操作系统运维技术、评估与加固、渗透测试、数据库安全技术、入侵检测、防火墙技术、密码学，共200节。 | 1套 |
| 信息安全高级课程：高级渗透测试技术、二进制技术、攻防实战技术，共30节。实验：计算机病毒与木马分析、攻防技术、安全加固、数字安全、安全编程、网络嗅探技术、Web加固技术，共400节。 | 1套 |
| Wen应用课程：包括web应用方向的多个国际主流实训实验，共91节。 | 1套 |
| 信息安全精品课程：涵盖CVE漏洞、应急响应、安全防护、渗透测试等多个安全测试及防护方向的课程，共111节。 | 1套 |
| 信息安全竞赛题库：具有Web应用安全技术、密码学技术、加密解密技术、逆向工程技术、数据取证技术、数据分析技术、运维技术、开发技术、渗透测试技术、缓冲区溢出技术、逆向工程技术，内置了150道知识与技能体系题库。 | 1套 |
| 千兆以太交换机 | 主要参数传输速率10/100/1000Mbps交换方式存储-转发背板带宽336Gbps/3.36Tbps包转发率132MppsMAC地址表支持黑洞MAC地址，支持设置端口MAC地址学习最大个数端口参数 端口结构非模块化端口数量52个端口描述48个10/100/1000Base-T自适应以太网端口，4个千兆SFP口控制端口1个Console口功能特性 堆叠功能可堆叠。VLAN支持基于端口的VLAN，支持QinQ，支持Voice VLAN，支持协议VLAN，支持MAC VLA。QOS支持802.1p/DSCP优先级标记，支持包过滤功能，支持SP/WRR/SP+WRR队列调度，支持基于端口的限速，支持基于流的重定向，支持时间段。组播管理支持IGMP Snooping，支持MLD Snooping，支持组播VLAN。网络管理支持命令行接口（CLI）配置，支持Telnet远程配置，支持通过Console口配置，支持SNMP（EImple Network Management Protocol），支持RMON（Remote Monitoring）告警、事件、历史记录，支持iMC网管系统，支持WEB网管，支持系统日志，支持分级告警，支持IRF，支持NTP，支持电源、风扇、温度告警。安全管理支持用户分级管理和口令保护，支持AAA认证，支持Radius认证，支持HWTACACS，支持SSH2.0，支持端口隔离，支持 802.1X，支持端口安全，支持MAC地址认证，支持IP Source Guard，支持HTTPs，支持PKI(Public Key Infrastructure，公钥基础设施)，支持EAD。 | 2台 |
| 2 | 课程更新 | 资源更新服务 | 提供每年50道CTF和5道AWD赛题的资源更新 | 三年 |
| 实时提供课程、实验及实训的内容资源更新(需视内容组开发计划而定)更新5个场景、50个带环境的漏洞，其余资源实时更新； |
| 3 | 资料库 | 数据采集 | 数据类型覆盖新闻、论坛、运营商、邮箱、购物、游戏、生活、视频、军事、体育、商城、社交、招聘、医院、银行、酒店等网站类型信息。 | 三年 |
| 4 | 审计设备 | 硬件规格：标准机架式硬件，1个console口网口类别：6个千兆工作管理口(1管理口+1HA口+4审计口)硬盘：1T内存：8G日志处理能力2000EPS（峰值：4000EPS）全面日志采集：全支持Syslog、SNMP、XML、FTP及本地文件等协议实现对各种资产进行日志采集，智能关联分析：实现全维度、细粒度关联分析，内置众多的关联规则，支持网络安全攻防检测、合规性检测，及云计算租户间可轻松实现各资产间的关联分析。可视化展示：实现所监控的信息资产的实时监控、信息资产与客户管理、解析规则与关联规则的定义与分发、日志信息的统计与报表、海量日志的存储与快速检索以及平台的管理。通过各种事件的归一化处理，实现高性能的海量事件存储和检索优化功能，提供高速的事件检索能力、事后的合规性统计分析处理。支持各种网络部署需要，包括日志聚合、日志过滤、事件过滤、日志转发、特殊日志格式支持(如单报文多事件)等。产品要求：产品获得公安部计算机信息系统安全产品销售许可证。产品获得中国信息安全认证中心颁发的《IT产品信息安全认证证书》，需符合《日志采集与分析产品安全技术要求》，并提供完整的检测报告复印件。工作模式：独立完成审计日志采集，不依赖于设备或系统自身的日志系统；审计工作不影响被审计对象的性能、稳定性或日常管理流程；审计结果存储于独立存储空间；自身用户管理与设备或主机的管理、使用、权限无关联；提供全中文WEB管理界面，无需安装任意客户端软件或插件。功能扩展：采用解决方案包上传对产品进行功能扩展，无需要代码开发。日志收集：支持Syslog、SNMP Trap、OPSec、FTP协议日志收集；支持使用代理(Agent)方式提取日志并收集；支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等；设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，BEA，中国电信，安氏，帕拉迪，apc，arbor，clam，戴尔（dell），digium，东方电子，EMC，中国电力科学研究院，Eudora，google，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局），永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克），Hardened-PHP，foundertech(方正)，三零盛安，allot，蓝盾，IBM，金诺网安，网威，nortel(北电)，citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS系统日志，Linux/UNIX syslog、IIS、Apache等；支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。日志分析：可以以日志等级进行过滤；应该可以通过自定义配置将用户不关心的日志过滤掉；支持对收集到的重复的日志进行自动的聚合归并，减少日志量；支持可由用户定义和修改的日志的聚合归并逻辑规则；支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备；支持对收集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展；可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息（公网情况）；支持基于内存的实时关联分析，跨设备的多事件关联分析；支持自定义条件的事件进行聚合。具备安全评估模型：评估模型基于设备故障、认证登陆、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件；内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等5大类50子类的安全分析场景；进行关联分析的规则可定制；三维关联分析：支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。日志备份：可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比；支持日志备份自动传送到远程服务器。日志查询：支持B/S模式管理，支持SSL加密模式访问；支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询；支持用任意关键字对所有事件进行高性能全文检索；支持可指定多个查询条件进行组合查询；支持将查询的条件存储为查询模版，方便再次使用；极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。应用性能监控（APM）：支持如下应用的性能监控（Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris）、数据库（mysql、oracle）、应用服务器（weblogic、tomcat）、web服务器（apache）；支持应用性能历史详情回溯查看；支持如下性能监控参数支持监控Windows操作系统如下参数：cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数；支持监控Linux操作系统如下参数：一分钟系统负载、5分钟系统负载、15分钟系统负载、cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数支持监控Mysql如下参数：查询缓存命中率、键缓存命中率、立即获得锁数、连接数、线程数、每秒SQL查询数、每秒发送字节、每秒接收字节；支持监控Oracle如下参数：库缓存命中率、内存排序比率、词典缓存命中率、SGA数据缓存命中率、重做日志缓存命中率；支持监控Apache如下参数：总访问数、写日志次数、每秒发送字节数、长连接数、关闭连接数、空闲活动数、查询DNS数、正在发送数、请求完成数、负载、等待连接数、总数据量、读操作数、工作线程数、空闲线程数、CPU占用率支持监控应用服务器（tomcat、weblogic）如下参数：活动线程数、堆内存（已用）、守护线程数。脆弱性管理：支持从IBM Rational AppScan导入资产弱点漏洞信息；支持从安恒明鉴Web应用监测工具导入网站弱点漏洞信息；支持从安恒明鉴数据库弱点扫描器导入数据库弱点漏洞信息；支持从NetSparker Web应用扫描器导入网站弱点漏洞信息；支持从Nessus网络扫描器导入网络弱点漏洞信息；支持从OpenVAS扫描器导入弱点漏洞信息；内置73000+条CVE漏洞数据知识库；内置数十项符合OWASP的Web漏洞数据知识库。地理安全系统：内置GeoSec地理安全子系统，内置世界以及中国安全GIS地图；支持用地理地图展示来源威胁的趋势；支持用地理地图展示目的威胁的趋势；支持在地理地图上标注威胁事件的发生分布；内置IP地址到经纬度的转换库；支持以地理信息类进行统计的数据报表；支持切换Google地图（需要连通互联网）。告警功能：可预设置安全告警策略；支持数据阀值设置，超过阀值将产生告警；可以通过邮件、短信和屏幕显示进行告警；支持自动防止报警信息在短时间内大量发送(告警抑制)；具备报警合并和在一个时间段内抑制报警次数的能力。综合查询及报表管理：内置合规性报表1000+种；内置SOX、ISO27001、WEB安全等解决方案包；内置完善的等级保护合规报表；内置综合性自动化审计报告；支持用户自定义报表；自定义的报表支持多个统计维度的数据集合；支持报表导出为PDF和Word格式文件。用户管理：根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理；系统自带自身管理日志；注册用户资产时，提供自动发现识别能力；提供一键式故障排除功能；提供自助式的升级接口，支持对产品升级、规则升级。部署方式：支持分布式部署；支持集中式管理和升级模式；支持分级管理模式；采用B/S架构操作方式，无需客户端安装；支持监控设备自身CPU、内存、磁盘等工作运行状况。 | 1台 |
| 5 | 漏洞扫描设备 | 硬件规格：扫描管理平台B/S架构；标准机架式设备；1\*RJ45串口；6\*GE电口；2\*USB口；硬盘1T ；内存16G。部署方式：支持旁路部署，无需改变原有的网络架构；分布式部署。扫描对象：Web漏洞扫描、数据库漏洞扫描、主机软件漏洞扫描、基线配置核查。功能要求：产品要求界面友好，并有详尽的技术支持文档，所有图形界面要求中文。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方便对产品访问操作，支持多用户同时登录操作。提供分布式部署，上级管理设备能够方便查看下级设备状态。提供三权分立的账户体系，支持上下级部门管理，非上下级的不同部门任务、资产隔离。提供审计功能，能够对登录日志、操作日常进行记录和查询，并可以将日志导入导出操作。厂商漏洞策略库大于40000条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与国际CVE、国内CNNVD漏洞库标准兼容。系统内置不同的策略模板如针对Linux、Windows操作系统等模板，同时允许用户定制扫描策略模板。用户可自定义扫描范围、定义扫描端口、扫描使用的参数集等具体扫描选项。支持Windows系列操作系统，支持Linux主流操作系统（Centos、Redhat、Debian、Fedora、Ubuntu、Suse等），支持Unix主流操作系统（AIX、HP-UX、Solaris等）。支持对Web、FTP、电子邮件等应用系统、Apache等web中间件服务器以及Office等常用软件进行漏洞扫描。可以自定义扫描端口范围、端口扫描策略。提供采用SMB、SSH、Telnet、SNMP等协议对Windows、Linux系统进行登录授权扫描。具备弱口令扫描功能，提供多种弱口令扫描协议，包括SMB、RDP、SSH、TELNET、FTP、SMTP、IMAP、POP3、MySQL、MSSQL、REDIS、RTSP等协议进行弱口令扫描，允许用户自定义用户、密码字典。支持发现非默认端口启动的服务，支持服务的协议识别、版本。同IP不同端口同漏洞的结果应明确给予端口标识。支持对误报的漏洞进行修正，避免将误报结果导出。支持7种以上端口探测方式，如： TCP ACK、TCP SYN、TCP Connect、TCP Null、TCP Xmas、TCP Window、TCP Fin等。支持HTML、WORD、PDF、XLS报告格式。配置核查模块：产品提供系统安全配置核查功能，能够对主流操作系统、中间件、无线设备、虚拟设备的安全配置项目进行检查。Windows系统支持提供离线检查工具，将检查结果导入平台查看。Web扫描模块：产品提供Web应用漏洞扫描功能，支持对Discuz、大汉CMS、PHPCMS、DEDECMS、ECSHOP、WordPress、eWebEditor、FCKeditor、Struts2等国内外常见第三方组件扫描；能够检测GET、POST、User-Agent、Cookie等多种方式提交的HTTP请求参数，并进行相应检测。能够通过Cookie的方式支持对带验证码的应用系统进行扫描；存在误报漏洞可通过产品在扫描结果处支持以即时通讯的方式第一时间反馈给厂商协助修改；支持识别国内外主流Web应用防火墙品牌；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。数据库模块：支持Oracle、Mysql、SQLServer、DB2、informix、达梦、人大金仓的授权数据库漏洞扫描。产品要求：[产品需获得公安部产品销售许可证](#_销售许可证)（增强级）；产品具备自主知识产权，提供计算机软件著作权证书。 | 1台 |
| 6 | CTF竞赛培训 | 针对CTF比赛提供专项培训，培训周期为7天，理论课程和事件操作相结合。频率为一年一次。培训课程：WEB安全：SQL注入漏洞；上传漏洞；文件包含漏洞；实操上机练习WEB安全：跨站脚本漏洞；任意文件操作（读取/下载）漏洞；命令执行漏洞；逻辑漏洞和越权漏洞逆向：汇编基础介绍；逆向基础知识讲解；工具介绍（IDA、OD）介绍；逆向类题目实战讲解密码学：古典密码学讲解；ctf密码学解题技巧；上机练习隐写/取证：隐写术；上机练习；取证；上机练习移动安全技术：Android静态静态分析、动态调试；IOS安全测试、IOS安全测试工具；客户端安全、数据交互安全；服务端安全、业务安全、环境安全CTF解题技巧：ctf解题技巧；攻防对抗赛解题技巧；实战训练 | 三年 |
| 7 | 专用计算机设备 | 便携计算机 | 性能规格：CPU：6核12线程\*1（主频2.6 GHz，12MB L3缓存）；内存：16G 2400MHz DDR4；硬盘：256G SSD +1T HDD；显卡：RTX2060显存6G；显示屏：17.3英寸144Hz电竞屏。 | 5台 |
| 高性能台式计算机 | 性能规格：：CUP：6核12线程\*1（主频3.2 GHz，12MB L3缓存）；内存：16G 2666Mz DDR4;硬盘：256G SSD+2T HDD；显卡：GTX1070 8G；显示器：24.5英寸 144Hz。 | 5台 |
| 台式计算机 | 性能规格：CUP：性能规格：CUP：6核12线程\*1（主频3.2 GHz，12MB L3缓存）；内存：8G 2666Mz DDR4;硬盘：128G SSD+1T HDD；显卡：GTX1060 3G；显示器：24.5英寸 144Hz。 | 36台 |
| 智能终端 | 海思 麒麟990 5G ；EMUI 10；8GB；128GB；全网通；5G版 | 2台 |
| 高通 骁龙888；MIUI 12；12GB；256GB；全网通；5G版 | 1台 |
| 高通 骁龙888；Origin OS 1.0；8GB；128GB；全网通；5G版 | 2台 |
| 新型嵌入式设备 | 性能规格：配置智能穿戴、智能家居等新型嵌入式设备、支持技术研究和验证测试，蓝牙通话心率监测计步器运动手环智能穿戴电话手表  | 5台 |
| 服务器 | CPU：10核20线程20\*2（CPU主频2.2GHz，13.75MB L3缓存）;内存：16GB\*2 RDIMM DDR4；硬盘：600G\*5 SAS 10K 2.5英寸硬盘；RAID卡卡：2G缓存,支持RAID 0,1,5,等；电源：1+1高效冗余热插拔电源；网络控制器：支持OCP卡、PHY卡或PCI-E卡网络模块，本次配置双口万兆网卡（带多模模块）+双口千兆网卡；原厂3年免费整机硬件保修。 | 1台 |
| CPU：10核20线程20\*2（CPU主频2.2GHz，13.75MB L3缓存）;内存：32GB\*2 RDIMM DDR4；硬盘：900G\*9 SAS 10K 2.5英寸硬盘；RAID卡卡：2G缓存,支持RAID 0,1,5,等；电源：1+1高效冗余热插拔电源；网络控制器：支持OCP卡、PHY卡或PCI-E卡网络模块，本次配置双口万兆网卡（带多模模块）+双口千兆网卡；原厂3年免费整机硬件保修。 | 1台 |
| 网络设备 | 交换容量≥336Gbps，整机转发性能≥96Mpps，整机可用端口数≥28，其中千兆电口≥24，千兆光口≥4；设备单端口支持的MAC地址用户数≥4k；支持静态路由、RIP、OSPF、BGP。 | 3台 |
| 8 | 专业工作设备 | 上网设备 | 支持通过加密代理、VPN等方式加密上网流。 | 1套 |
| 安防设备 | 工作环境安全防护、通过视频监控等方式对工作环境进行24小时安全监控管理。 | 1套 |
| 知识库  | 提供特征库、漏洞库、安全工具库等服务。 | 1套 |
| 临机设备 | 支持植入、绕过、提取等多种工作方式。 | 1套 |
| WiFi设备 | 具备WIFI网络信号探测及放大，用于对WIFI开展安全工作。 | 1套 |
| 邮箱工具 | 支持对邮箱开展安全检查工作。 | 1套 |
| 密码字典工具 | 支持对已知对象的多种密码生成方式的应用 | 1套 |
| 网络密码工具 | 支持路由器等网络设备以及各类网络应用的相关操作 | 1套 |
| 链路系统 | 提供安全链路，支持加密。 | 1套 |
| 链路接入设备 | 支持以太网，无线网等设备接入方式，支持以太网，5G，光纤等互联网接入方式，支持故障情况断网（不支持BYPASS功能），支持黑白名单过滤，支持行为审计。 | 1套 |
| 指纹库工具 | 提供信息系统、网站等指纹信息。 | 1套 |
| IP查询工具 | 支持IP地址相关信息的查询。 | 1套 |
| 系统远程服务 | 支持面向Mac OSX、Windows、Linux、Android系统的远程协助。 | 1套 |
| 网站扫描 | 通过对网站或主机进行扫描获取数据。 | 1套 |
| 9 | 服务支撑 | 信息获取 | 实现对主流社交平台信息获取。 | 三年 |

## 4、视频专网安全防护

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **系统名称** | **功能模块名称** | **功能子模块名称** | **详细功能描述** | **数量** |
| 1 | 物联网安全态势感知平台 | 态势感知平台 | 硬件规格：标准机架式设备；1+1冗余电源；硬盘：4T\*12；内存：256G；接口：4个千兆电口、4个千兆光口。性能参数：处理能力，支持最大接入资产数量50000台（项目建设周期内超过50000点免费升级）。监测能力，支持最低数据更新时间5分钟。数据处理模块：进行数据格式化存储，采用机器学习、人工智能算法进行预分析并做处理，上报给管控中心。安全防护模块：具备病毒云查杀、DDOS防护、漏洞管理、登录防护、防端口扫描、进程防护、网络防护等内核级安全防护功能安全管控子系统：基于海量威胁情报数据，为安全态势分析提供情报信息来源，同时生成对应管控策略，安全防御态势感知模块：实现全网安全态势感知，具备攻击态势、资产态势、区域态势、资产画像等功能。态势感知能力要求：以可视化方式展示总体态势、区域态势、资产画像、攻击态势等效果；对整体安全情况进行统计，包含资产位置分布，资产安全状态、资产统计、最新威胁展示、趋势分析、资产在线情况、厂商类型、高危区域等功能；自动绘制区域网络关系图，可切换展示区域态势，显示可疑外连、可疑进程、区域资产类型、区域威胁类型等数据；实时展示最新的攻击威胁，包含最新威胁次数、外部恶意IP数量、高危资产排行top5、攻击来源地区TOP5、攻击目标IP top5、攻击类型饼图。并滚动显示最新威胁（时间、源IP、目标IP、攻击类型、威胁等级）；针对资产进行安全画像，以百分制的方式进行资产安全评分，并展示资产的安全状态、基本信息、网络进程关系图、状态性能趋势等。资产管理要求：可查看资产所对应的：资产编号、资产IP、资产类型、CPU型号、资产内存、状态等信息；可新增资产信息，包括资产的区域、经纬度等；支持对资产IP、资产型号进行搜索，可删除单个资产或批量删除勾选的资产；可查看资产的基本信息、进程列表、监听端口、网络连接、云查杀和漏洞信息；支持对辖区内资产进程、监听端口、网络连接、恶意病毒文件进行管控策略下发，完成安全管控处置；支持资产管理精简模式（资产按照安全等级和类别进行区分和筛选）。引擎管理能力：支持多个引擎的集中管理，引擎数据对接到平台；支持对引擎的一键管控、登录管理；支持接入引擎的智能分类、自定义添加、引擎状态监控。数据接入能力：可统一收集分析各种安全设备关键安全日志，支持下级单位等安全日志与平台日志接收格式兼容；可从资产、威胁、准入、审计等维度进行安全的监控和分析，快速识别异常安全行为和事件。数据加密管控：支持对管辖资产数据安全加密功能开启、关闭配置；支持对管辖资产加密周期设定；支持对管辖资产加密服务器的自定义添加、弹性扩展；支持管辖资产的数据加密功能批量配置；支持管辖资产加密状态的实时查看、加密过程日志查看。安全防护能力：支持配置防护策略，包含防护规则和恶意IP、端口等策略下发。用户管理：系统自带自身管理日志；采用B/S架构操作方式，无需客户端安装；支持监控设备自身CPU、内存、磁盘等工作运行状况。离线升级能力：可通过WEB界面对平台进行离线版本升级。数据安全：运行安全，不得改变检查对象当前配置，不影响检查对象正常运行 ，不影响检查对象所属网络正常运行 ，不在检查对象中遗留痕迹；存储安全，检测工具应对所有检查数据采用加密算法进行加密，防止监察数据被非法读取；痕迹安全，检测工具应对所有检查数据采取痕迹消除措施，以防止信息泄露；数据分析，支持分级部署，可无缝对接视频监控态势感知平台，统一联动管理，统一数据分析和展现，形成区域网络安全态势概况。 | 1套 |
| 数据加密子系统 | 硬件规格：标准机架式设备 电源：1+1冗余电源 内存：16G 存储：2T，raid1 板载网口个数：4个，配置专用国密加密卡。设备性能：支持最高5500次/秒的协同签名，支持1500次/秒并发密钥请求。产品要求：支持国密标准加密算法，涉及产品需具备商用密码产品认证证书。加密算法：加密模块支持国产SM2、SM3、SM4标准加密算法。数字签名算法：协同签名模块支持国产SM2、SM3、SM4数字签名算法。部署模式：支持集群化分布式部署，支持高可用部署方式，出现设备宕机等故障时，完成主机和备机的切换，确保关键应用的持续正常运转。功能要求：支持对业务系统数据在终端上完成加密，加密后密文转发；支持用户与应用双向身份认证、数据完整性保护；支持密文密钥分离，业务服务器不接触密钥；★支持用户自主更新密钥，自主选择更新周期，实现数据自主可控（提供截图）；密钥生成、存储、分发的安全性满足国密要求；可根据需求定制化开发，实现端到端全程加密、传输加密、存储加密等功能；提供第三方加密身份，增强用户对应用平台的信任；不影响用户体验，不改变用户原有使用习惯。技术要求：软件密码模块通过GM/T 0028-2014《密码模块安全技术要求》安全等级二级认证。软件密码模块提供数据加解密能力；软件密码模块支持定制需求提供不同版本，如Java，C，Javascript，Objective-C等版本；软件密码模块可与协同签名系统交互，实现终端身份认证及数据完整性保护等功能；软件密码模块支持对密钥进行分片及安全存储；安全私钥分量托管协同签名系统，保证用户私钥在终端存储和使用的安全性；协同签名系统支持业务端硬件特征绑定认证，通过增强用户访问鉴别机制，阻止非法设备接入系统；支持密钥由业务终端和服务器协商产生，采用密钥分割技术保存密钥，确保密钥安全性；密钥管理模块符合商用密码密钥托管环境建设要求，实现密钥的管理、分发等；密钥管理模块可作为密钥管理中心，为其他业务系统分配密钥；密钥管理模块支持对密钥流转过程的生命周期管理；采用专用的密钥管理服务器，具备应急告警机制，故障时向指定邮箱发送告警邮件。兼容性：可在各类终端、应用系统中集成国密软件密码模块，支持iOS、Android终端、PC客户端；支持Windows、Linux操作系统多种内核版本。性能指标：支持终端业务数据加密；终端加密计算时间控制在毫秒级别，不影响用户使用体验。 | 1台 |
| 2 | 物联网准入 | 架构：基于B/S管理模式，支持SSL加密访问.资质：具有独立自主知识产权。硬件架构：标准机架式；配置冗余式电源；硬盘2\*2T(配备RAID0/1)；接口数量：4个千兆电口；最大支持入网许可数 9999点(项目建设周期内超过19998点免费升级)。支持大型网络的入网窗口管理，管理员可根据各个项目分配不同的入网区域、入网IP窗口、入网窗口时效、入网审核方式；入网审核时，可直观查看入网设备的资产类型和指纹信息识别设备类型以及安全状态，阻断违规设备、仿冒设备接入。自动对视频传输网络进行拓扑绘制部署方式：支持旁路部署；设备宕机或断网不得影响正常入网；支持双机部署，支持HA主备机心跳IP检测及虚地址管理模式；支持虚拟化部署，可部署在公有云/私有云环境中。设备管理：支持按照EXCEL模板批量导入\导出网络设备；支持通过TELNET、SSH、SNMP协议自动管理网络设备；支持自动发现网络设备硬件型号和软件型号，并自动适配对应的管控模板和运维模板；支持批量录入TELNET、SSH、SNMP交互信息。设备管控：支持自动学习、安全扫描、身份认证、人工审核、项目报备结合的多种混合准入管控模式；支持全网统一管控或特定网络端口按需管控的自由策略；支持自动发现现有网络环境的所有内网终端、前端设备、服务器、安全设备、办公设备等信息，并自动纳入信任列表；支持自定义学习时间，学习时间结束后自动启动准入管控。设备同步：部署期间无须管理员对网络设备执行任何指令操作；支持自动同步SNMP配置，自动下发SNMP配置；支持自动同步VLAN信息，自动同步接口PVID；支持自动同步MAC地址表、ARP表、VLAN表、ACL组合；设备面板：支持图形化呈现网络设备的所有接口（包括已用接口、离线接口、未用接口、关闭接口、ACCESS接口、TRUNK接口）；支持堆叠交换机的图形化分层展示；支持图形化呈现网络设备的CPU趋势图、RAM趋势图；支持呈现运行时间、运行版本、设备型号、设备品牌；支持图形化定位HUB、小交换机、虚拟集群的位置和下联检索；支持各接口下联终端信息检索（包括主机名、IP地址、MAC地址）；支持IP地址、MAC地址的模糊检索和精确检索，并闪动提示。网络区域：支持根据业务职能分配网络区域，网络区域应不少于生产区域、终端区域、安全区域、外来区域、候审区域、隔离区域等；支持集中管控全网VLAN，支持查阅设备关联VLAN、支持全网推送VLAN、支持单独推送VLAN；支持同一VLAN ID，不同IP网段的共同管理和分组管理。动态拓扑：支持自动生成动态的网络拓扑；网络拓扑中可查阅交换机信息和交换机之间的连接信息。地址管理：支持可视化的IP地址图，直观地呈现各VLAN下的IP分配情况（包括已用IP、未用IP、保留IP等）；支持通过IP地址、MAC地址、主机名快速检索和定位全网终端的所在位置和在线状态；支持IP地址、MAC地址的模糊检索和精确检索，并闪动提示。终端发现：实时监测并发现接入内网的PC、平板电脑、智能手机、哑终端等设备，能够在第一时间隔离阻断并通知管理员；入网设备在连接内网任何位置时，将被强制隔离、通过WEB Portal引导至候审页面；支持准确定位HUB、小交换机下的设备入网，能够在第一时间隔离阻断并通知管理员。环境支持：支持无线WiFi环境下，自动弹出WEB Portal候审页面；支持有线 Hub 环境下，自动弹出WEB Portal候审页面。定向引导：支持终端入网URL重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，支持HTTP/HTTPS的重定向引导；能通过浏览器完成身份认证、安全检查、注册申请、人工审核等全流程的便捷式引导管理。身份认证：内置内部人员的身份认证管理模块，无需第三方RADIUS支持；支持联动第三方AD域控、LDAP、RADIUS身份认证系统。终端入网：提供安全客户端和无客户端等多种入网管理模式；无客户端部署时，应支持对现有网络环境的零影响和透明部署，仅针对特定终端、特定区域、未授权入网设备实时发现和拦截；外部终端入网时，应支持入网有效时间管理，超时则自动退网。★支持直接对交换机自动下发、自动回收、动态转化的ACL策略，包括但不限于端口级IP ACL\MAC ACL（提供截图）。终端绑定：支持IP/MAC两者强制绑定；支持可信任终端的位置移动时的透明放行，无须二次认证或审核；非信任终端的位置移动时的强制隔离，即使连接HUB亦可拦截。HUB管理：能够发现内网私接的HUB、傻瓜交换机等非网管设备；能够采用VLAN隔离、关闭端口等方式禁止Hub下联PC接入网络；能够针对HUB下多个终端须分别认证、分别审核才能分别入网；禁止HUB下联的任意一台终端放行即全部入网的安全隐患。指纹合规：内置终端电脑、移动终端、服务器、数据库、虚拟机、摄像机、公安专用设备等资产的指纹识别能力，支持自定义指纹规则；支持自动识别网站类业务系统名称和访问端口，纹合规规则支持发现专用网络的违规设备进行告警或信任。弱密码检测：支持自动扫描摄像机和NVR/DVR的弱密码检测；支持自定义密码字典。违规外联检测：支持无客户端的违规外联检测；支持自动扫描全网设备是否存在内外网同时连接的违规外联。★入网项目窗口：支持大型网络的入网窗口管理；管理员可根据各个项目分配不同的入网区域、入网IP窗口、入网窗口时效、入网审核方式；入网审核时，可直观查看入网设备的资产类型和指纹信息（提供截图）。病毒管控：支持与江民、亚信、腾讯等主流防病毒管理中心和防病毒网关联动，自动调取在线资产的活动病毒信息；支持实时检测是否安装江民、亚信杀毒软件程序；支持实时发现病毒感染源并定位位置，支持实时告警或隔离；支持隔离病毒散播的同时不影响正常业务应用的访问。安全管理报表：内置多功能安全管理报表，内置报表应不少于入网资产分析报表、入网风险分析报表、全网入网报告、网络使用分析报表等；支持提供每日入网报告、每周入网报告、每月入网报告，并提供导出和打印功能。安全审计：内置内部审计功能，精细记录管理员的控制台操作，支持快速检索和审计导出功能；内置准入审计功能，精细记录系统后台的运行记录（包括后台认证流水、后台同步流水、后台监听流水等记录），支持快速检索和审计导出功能。安全告警：支持邮件告警、弹窗告警方式提醒管理员异常情况；支持登录告警、认证告警、HUB告警、ARP告警等异常告警。用户及角色管理：内置自定义角色管理，支持自定义三权分立角色；支持自定义管理用户，支持管理用户的安全IP地址限制。安全策略管理：支持密码复杂策略，要求管理账号和准入账号符合密码安全要求；支持密码定期修改，要求管理账号和准入账号符合密码变更要求；支持登录锁定策略，针对多次密码错误行为进行账户安全锁定。系统状态管理：内置CPU、内存、磁盘健康度监控，具备趋势监控和安全告警；内置网口流量监控，具备负载监控和安全告警；支持控制台的系统升级、组件重启、系统重启和系统关机。系统网络管理：支持NTP时间设置；支持控制台的网络IP设置和网口自定义增加、定义和查阅。可信运维联动：支持与堡垒机维系统联动；支持自动发现违规运维终端，支持自动告警并拦截违规运维会话。终端系统联动：支持与内网终端系统联动；支持自动同步内网终端客户端的用户注册信息；支持自动检查终端电脑是否安装客户端，是否卸载客户端。 | 2台 |
| 3 | 物联网安全心 | 软件规格：为终端提供系统内核级安全防护能力；为终端提供内核级安全感知能力；基于国密加密算法，提供端到端加解密功能。授权数：20000（项目建设周期内超过20000点免费升级）。★终端感知：可感知终端基本信息，包括终端品牌、型号、MAC、内存（总/使用内存）、CPU（型号、使用率）、系统版本信息等；可感知终端启动进程；可感知终端网络连接信息（IP、端口、协议、状态、流量）以及关联进程信息；可感知终端开放端口信息及服务类型、关联进程信息；可实时监控终端系统日志、网络访问情况等（提供截图）。★安全防护：支持配置终端安全访问控制策略配置ACL，以允许/拒绝数据包进出；支持终端进程防护，针对恶意进程可阻断；支持终端网络关系防护，针对异常链接可阻断；支持终端端口监听，可对端口开放权限进行管理（提供截图）。数据安全：支持终端数据传输端到端加密，加密过程保证完整性；支持国密加密算法，支持包括SM2, SM3, SM4, SM9算法；密钥分发采用国密算法（SM2, SM3, SM4)，保证过程安全；支持终端传输过程加密、签名认证；支持设备生成数字签名用于双向身份认证、数据完整性保护（具备相关资质）。升级功能：支持进行OTA版本自动升级。 | 三年 |
| 4 | 物联网安全监测平台 | ▲硬件指标：标准机架式设备；资产遥感授权：20000个（IP）；流量采集口：4\*千兆电口/2\*万兆单模光口/2\*万兆多模光口；数据处理性能：60万并发会话；存储：48TB；数据存储周期：180（天）；电源：1+1冗余电源。探测能力：支持最低轮询探测周期一分钟。物联网终端资产识别、资产监测、漏洞监测、非法接入监测，前端感备在线感知监测预警，实现物联网终端威胁可视化、实时检测、周期性监测，输出风险管理报表，构建物联网终端一站式安全风险评估平台。部署模式：采用旁路接入方式，不对现有网络造成影响。无需在任何终端设备安装代理软件，实现快速便捷部署；支持数据采集与数据分析的分布式部署模式。产品形态：产品须为软硬件一体化交付。授权数：20000个（项目建设周期内超过20000点免费升级）。设备安全监测：实现不间断对全网设备进行设备安全检测，包括：资产识别 -- 对在网资产进行识别，提供以下资产信息：（1）设备类型、品牌型号、系统版本；（2）应用名称、品牌、版本；（3）服务类型、端口等信息。设备指纹库 -- 基于识别的资产信息建立设备指纹库；资产监测 -- 对资产进行持续监测，包括以下监测信息：（1）资产在线状态监测；（2）资产变更和IP冒用监测；非授权/未知资产入网监测；视频设备安全风险分析 -- 对视频设备进行安全漏洞扫描检测，分析设备安全风险状况。★信令安全监测：对可能对视频设备、视频数据等造成影响的高危信令、分析与告警；对信令的来源、时间、频繁度不同的角度进行综合分析，及时发现信令异常情况（提供截图）。 边界安全监测：实现不间断对全网进行边界安全检测，包括：违规外联 –监测范围内终端的两网互通（同时连接内网和互联网）的行为，一旦发现，定位其终端地址（内网IP和互联网IP）； 网中网 --提供网中网分析，监测视频网中存在的私有局域网情况，包括NAT设备、网闸设备、小型路由器、代理服务器等。网内攻击监测：实现对网络中存在的网内攻击行为进行检测，包括：恶意扫描 --监测网络中频密或大规模的访问其它主机设备、服务端口（例如文件共享用端口）的行为，提供发起扫描的设备地址、所在地市、被扫描最多主机、被扫描最多端口等详细信息[；](#证明材料3)其中包括提供对应的详细通信记录，包括开始时间、结束时间、扫描源（地址、端口）、被扫描目标（地址、端口）等信息；提供在不同时间段的扫描次数分布，用于分析扫描攻击行为的趋势。定向扫描 -- 监测通过专网对全网设备特定端口或特定设备全端口扫描的行为； 病毒木马 -- 监测病毒或木马程序利用已知漏洞进行大规模传播的行为。提供病毒木马对应的详细通信记录以及特征信息，包括开始时间、结束时间、病毒源（地址、端口）、被攻击目标（地址、端口）等信息。异常行为监测：实现对网络中存在的异常行为进行监测，包括：频繁访问业务系统 -- 监测对特定业务系统的进行频繁访问的异常行为，提供频密访问业务系统的终端设备地址、所在位置、被访问系统的地址、端口、名称等详细信息[；](#证明材料3)网络异常连接 -- 监测在一定时间段内对大范围网络IP发起访问连接请求，或频繁地试图访问连接特定的IP等的异常行为，提供发起访问连接的源地址、目的地址、时间、端口等信息。安全隐患监测：实现对网络中存在的安全隐患进行监测，包括：安全隐患 -- 对使用默认口令、弱口令、默认端口的安全风险隐患进行监测和发现；用户可以自定义扫描目标、类型、扫描时间策略。系统会根据目标地址范围进行弱口令扫描，对目标系统进行探测，以确认是否存在可正常访问的弱口令；DNS请求 -- 对内网的终端设备持续互联网DNS异常请求进行监测。违规行为监测：实现对网络中存在的违规行为进行监测，包括：违规设备 --监测网络违规设备（移动设备/WIN8）接入，提供设备接入地址、设备类型、所在地市位置等信息；违规站点 -- 监测网络中的未报备的WEB站点、论坛站点，提供服务器地址、访问方式、所在位置等信息；DNS服务 -- 监测网络中的未报备的DNS服务器，提供服务器地址、所在位置、解析域名详细信息等信息；FTP服务 -- 监测网络中存在的FTP服务器，一旦发现，提供服务器地址、端口、FTP软件类型、是否运行匿名登录、所在地市等信息。可配置定义对特定厂家的FTP服务器类型的分析。可监测用户访问FTP服务器的行为，一旦发现，提供用户终端地址、FTP服务器地址、上传下载文件名、文件大小、用户名、密码等信息。支持按娱乐影音文件、软件、图片、其它等类型进行分析[；](#证明材料3)联网聊天 -- 分析网络中搭建的聊天服务器、使用的聊天终端，提供设备IP地址、所在位置、聊天工具等信息；游戏行为 -- 监测范围内的网络游戏行为，一旦发现，可记录其游戏主机、位置、游戏端口、游戏名（包括版本号）等相关游戏特征信息。监控台：提供展现全局监测情况的展示功能，监控台各个展示页面以模块化布局，并可由用户自定义。数据取证：实现对发现各种的监测告警行为提供数据取证功能：行为取证 -- 对行为进行取证留存，包括以下行为：（1）访问行为；（2）文件传输行为；（3）传输指令行为。网络原始数据包 -- 在网络异常产生时，提供最原始的通信记录数据，为安全行为分析等提供证据。报表：提供报表自动生成功能，提供灵活的报表策略管理，可根据策略自动生成报表，并自动通过邮件发送给接收者。告警管理：提供告警事件类型、类别、等级、内容、告警时间、持续等告警事件管理。提供告警事件名称、类型、状态、级别、告警时间、签收时间、处理时间、处理人、处理结果等告警事件处置管理。用户管理：提供用户增删改查在内的用户管理。提供用户与角色关联的权限管理，权限分配的最小单位为菜单级。日志管理：提供系统操作的操作人、时间、类型、事件、访问地址等在内的日志记录。探测策略管理：提供可自定义配置的探测策略管理。产品要求：产品具备自主知识产权，提供计算机软件著作权证书。 | 1套 |
| 5 | 威胁分析服务 | 次数：每年提供不低于12次威胁分析服务，服务提供全面的威胁数据分析与最终分析报告。方式：威胁监测与分析服务将采取现场的服务方式，利用工具和人工进行对客户网络环境中的安全事件进行分析。邮件系统风险监测与分析服务：采用专业监控设备，部署在邮件系统的所在区域，采用旁路部署的方式，针对邮件系统可能面临的多种潜在风险，如暴力破解、异常附件，WEBMAIL审计，协议监测，别名异常监测，指纹异常，逆向MX，自动外发，邮件炸弹，钓鱼邮件，账号异常，位置异常进行监测与分析，针对监测内容，定期分析，提高邮件系统安全性。网络流量威胁监测与分析服务：采用专业监控设备， 部署在互联网或者重要区域节点边界，旁路部署模式，对网络中存在的多种威胁时间，如僵尸网络、远程控制、网站后门、网页篡改、DDOS攻击、漏洞利用、网络盗号、数据泄露、攻击事件、设备安全等进行监测，定期对监测结果进行分析，提高监测准确率，降低网络安全风险。未知威胁监测与分析服务：采用专业安全监控设备，旁路部署在如互联网、邮件，办公等重要环境，针对常见协议，如HTTP，POP３，FTP等，和传输中的各种文件进行监测，对协议异常和文件异常进行实际运行监控和分析，不依赖已知特征库，对监控中出现的问题进行人工分析和验证，判断威胁的范围，途径，利用的弱点并提供清楚建议，提高抵御防范APT攻击的能力。 | 三年 |
| 6 | 终端管理系统 | 终端管理中心软件：实现对终端的统一管理和策略下发。自主知识产权：软件要求在中华人民共和国境内开发，具备自主知识产权。易用性：软件界面友好，易于安装、配置和管理，并有详尽的技术文档。软件图形界面以及各类技术文档均为中文。数据耦合性：软件可根据具体业务需求进行配置和功能定制化开发。分布式架构：软件支持分布式部署，用于提升数据处理性能。许可：1000个服务器授权（服务期内超过1000点免费升级）。支持的操作系统; Windows server 2008、win7、win8、win10 、Window2003 、XP等，Redhat、CentOS、SUSE、Ubuntu等。 Web服务器: IIS、Apache，Java系列(Weblogic，Websphere，Tomcat，Jboss)等数据库: MSSQL，Oracle、Sybase、Informix、DB2、MySQL等关系型数据库；Mongodb、Cassandr等非关系型数据库。系统性能监控：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，在达到配置阈值时报警。系统安全性模块：支持防端口扫描，防违规外联，锁定恶意的端口扫描及外联行为，并记录告警；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。支持反渗透监控，包括横向渗透的危险操作等。支持网站防护，包括SQL注入、XSS、Web应用及容器漏洞防护、访问控制、屏蔽扫描器等。支持智能检测防御CC攻击，并可进行高、中、低三档设置。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。支持流量画像，支持全网流量可视化、应用级流量可视化；支持威胁横向扩散路径可视化与一键阻断；支持违规外联路径可视化与一键阻断。支持登录防护，包括以系统账号为粒度的异常登录防护、支持五个任意维度(任意地理位置，任意IP，任意域名，任意计算机名，任意时间)的系统登录访问策略设置、防暴力破解、弱口令检测并告警。触发登录防护后，自动联动添加微隔离规则。支持显示隐藏的系统账户。具有系统漏洞扫描和修复功能，提供真实漏洞补丁。管理中心可作为补丁服务器，支持管理中心可上网和不可上网2种情况。提供离线补丁下载器，按需智能获取内网所需补丁。支持对文件变化的审计。支持对外设的行为监控、权限管理、行为审计。支持用户录制定制化的配置模板，应用到所有或者指定的机器上；自带10个以上默认模板。对关键操作，比如病毒查杀等关键安全项检查支持创建自动巡检任务，定时执行。支持开启进程白名单，只允许受信任的进程启动。防病毒模块：支持进程主动式防御，在进程启动、文件创建时自动触发。支持域环境下普通账户登录的病毒木马查杀及策略的配置。开启进程监控后能完全预防已知病毒的危害。提供专门的勒索风险评估功能。至少需要包含：弱口令检测、系统漏洞检测、恶意进程检测、高危端口检测等能力。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。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。提供专门的挖矿风险评估工具。评估项目至少包括：弱口令、系统漏洞、恶意进程、DNS历史查询、违规外联等。提供专门的挖矿实时防御工具，并提供功能开关。自研免疫引擎通过强制访问控制技术免疫WannaMine1.0/2.0/3.0等免杀病毒。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。支持部分病毒感染文件的修复功能，对于二进制文件可剥离感染部分，保证应用正常使用。可防范、检测并清除隐藏于电子邮件、公共文件夹及数据库中的计算机病毒、恶性程序、病毒邮件。支持查杀映像劫持类型的病毒。支持查杀防范网页中的恶意代码。支持对压缩文件、打包文件查、杀毒（默认支持9层压缩扫描，可根据用户需求增加扫描层数）。支持内存查杀毒。支持运行文件查杀毒。支持支持图片、视频等多媒体文件的查杀毒。支持查杀各类Office文档中的宏病毒。支持查杀各类Office文档格式夹带型木马。在线病毒库升级。告警功能：告警类型包括：异常文件、网站防护、性能监控、登录防护；告警内容至少包括事件发生时间、事件类型、访问的资源、 IP源地址等详细内容；告警方式包括：Email，短信，声音，syslog，snmptrap，自定义。升级系统：支持离线升级及在线自动升级，包括管理中心平台、客户端程序、病毒库、补丁库、Web后门库、违规外联黑名单库；客户端程序支持在线热升级，升级之后旧版本驱动等程序无残留。集中管控：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；支持导出已安装客户端程序的资产清单。支持导出日志；能够通过统一的管理中心对多个服务器或主机进行监控；能实时检测工作组件工作状态以及系统关键资源的运行状态；能对服务器或主机节点进行分组管理。用户管理：支持多级用户管理：系统管理员、租户管理员；至少支持以下帐号管理功能：帐号创建、帐号授权、帐号属性修改和帐号删除；进行身份认证，用户切换角色时，必须进行重新认证；支持超时重新认证机制并能够定义用户认证尝试的最大允许失败次数。管理界面：支持SSL的Web界面；许可到期前提醒。可视化功能：能展示各个服务器或主机节点的信息，运行状态、活动规律、行为变化趋势和详细资料，以及历史行为数据查询、全局安全态势等。能监测节点遭受网络攻击的趋势信息，可以直观的了解攻击目标、攻击源、攻击方式的变化趋势和详细资料。安全事件：提供重大事件应急响应预案。软件升级：提供3年的病毒库、程序升级服务。应急响应：对于新发现的病毒、零日漏洞，厂商能够于24小时内作出响应，及时通知用户，并提供专应急预案、处置工具或专杀工具。技术支持:支持7x24小时威胁溯源服务。勒索保险:提供与本产品相结合的勒索保险业务。该业务需要要明确的使用梯度。产品要求：[产品需获得公安部产品销售许可证](#_销售许可证)。 | 1套 |
| 7 | 运维审计系统 | ▲硬件配置：标准机架式；标配网口：千兆电口管理口\*2，千兆业务电口\*4，千兆业务光口\*4（含2个千兆SFP多模光模块），硬盘容量：1T\*2，RAID 1；内存：8G，USB口：USB2.0口\*2，串口：RJ45口\*1，电源：1+1热插拔冗余电源。可管理设备数量：授权资产：500个 。并发性能：并发字符连接最大500个，并发图形连接最大100个，并提供第三方权威机构检测报告证明。系统安装与存储：系统须安装在专用的CF卡或固态盘中，审计数据存储在磁盘中，防止操作系统故障导致审计数据丢失。设备部署：设备采用旁路部署，不得影响业务环境；须支持HA主备模式，管理口和心跳口须支持多链路端口绑定功能，防止单网卡或单线故障。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。用户角色：支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理。用户管理和用户策略：支持用户的批量导入/导出，按用户类型等分组方式；支持用户安全策略功能，如密码锁定次数、密码有效期、密码复杂度、用户有效期、用户登录时间限制、用户登录IP范围等。部门层级管理：支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据。部门用户管理：每个部门可以管理本部门及下级部门的用户角色：部门管理员、运维管理员、审计管理员、运维员。部门资源管理：每个部门的部门管理员可以管理本部门及下级部门的主机、授权关系、策略。部门审计管理：各部门审计管理员可以管理本部门及下级部门的运维会话日志。与第三方认证对接：支持与AD、LDAP、RADIUS、吉大正元、北京CA认证系统联动登录堡垒机，[支持自动同步AD/LDAP用户](%22%20%5Cl%20%22_AD/LDAP%E7%94%A8%E6%88%B7%E5%90%8C%E6%AD%A5)。短信口令认证对接：支持与get、post、soap发送方式的http短信网关平台进行联动，实现短信动态口令双因素认证机制，如与阿里云短信服务、SendCloud联动。手机APP动态口令认证：支持手机APP动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定APP动态口令。双因子认证：堡垒机须内嵌动态令牌和usbkey认证引擎，可同时使用动态令牌和USBkey。多种双因子认证同时使用：基于不同的用户设置不同的双因子认证模式，如user1用动态令牌、user2用USBkey、user3手机APP动态口令认证。多种认证组合使用：支持域认证与双因子认证结合使用，如同时使用AD/LDAP用户名+AD/LDAP密码+手机APP动态口令登录堡垒机、同时使用AD/LDAP用户名+AD/LDAP密码+短信口令登录堡垒机。认证窗口全局设置：支持认证窗口的全局设置：可以选择启用哪种或者哪几种认证登录窗口。支持的协议和应用：支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；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。主流数据库运维管理：支持DB2、oracle、mysql、sqlserver主流数据库协议代理运维，可直接调用本地windows系统的数据库客户端工具，支持自动登录、无需应用发布前置机。IE代填：IE代填应用发布：HTTP/HTTPS协议的web设备，且可以直接代填账号和密码。混合云管理：可以通过socks5/http/ssh等代理协议连接管理异地云资源区中私有网络的云主机。分组管理：支持对设备进行按设备类型分组、按部门分组，支持设备批量导入/导出。登录模式：支持设备帐户和密码的自动登录、手工登录、二次自动登录模式自动收集和自动授权：支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权。设备密码管理：导出的设备信息文件加密存储，解密时须由2个管理员同时解密才能查看到设备信息文件内容。申请工单：运维人员可以向管理员申请需要访问的设备，申请时可以选择：设备IP、设备账户、运维有效期、备注事由等，并且运维工单以邮件方式通知管理员。审批工单：管理员对运维工单进行审核之后以邮件方式通知给运维人员；如果允许，则运维人员才可访问；否则就无法访问。自动改密：支持定期自动修改windows服务器、网络设备、linux/unix等目标设备密码功能。改密保护机制：支持完善的自动改密安全保护机制，包括：改密前备份、备份失败不改密、改密后备份、密码文件加密；支持发送方式，包括邮件、FTP、SFTP等。密码容错机制：支持自动密码恢复、手工验证密码、密码强度控制等。多种浏览器登录：Web访问方式：至少支持使用IE、谷歌、火狐三种浏览器打开堡垒机的Web页面直接调用mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX等运维客户端工具。H5运维方式：支持ssh、telnet、rlogin、rdp、vnc协议的H5运维，无需本地运维客户端工具。数据库运维：支持通过堡垒机页面直接调用本地Windows系统里的plsql、sqlplus、toad、sqlwb、ssms、mysql.exe等数据库客户端工具。客户端工具登录：客户端访问方式：支持使用本地的mstsc/Xshell/SecureCRT/Putty等客户端工具登录堡垒机访问图形或字符设备，视图界面一致性、搜索能力。SFTP/FTP的客户端登录：支持使用本地的winscp/flashFXP/SecureFX等客户端工具登录堡垒机访问SFTP/FTP设备。SSH网关代理直连：支持使用本地的SecurCRT/Xshell/OpenSSH工具通过SSH网关代理方式直接登录字符设备。数据库代理直连：支持在mac电脑里使用navicat工具通过堡垒机登录mysql、oracle等数据库服务器。批量自动登录字符主机：支持批量登录字符设备功能：能自动生成SecurCRT/Xshell工具的批量登录文件，实现在工具中批量自动登录多台设备。域用户自动登录主机：AD/LDAP环境，支持直接使用登录堡垒机的AD/LDAP用户及密码可以直接自动登录到服务器里。运维审计日志：支持对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志。Zmodem传输审计：支持保存SSH的sz/rz命令（zmodem）传输的原始文件。SFTP/FTP传输审计：支持保存SFTP/FTP传输的原始文件。RDP粘贴板审计：支持保存RDP粘贴板（桌面之间复制-粘贴）传输的原始文件。RDP磁盘映射审计：支持保存RDP磁盘映射传输的原始文件。RDP文字记录：支持对RDP屏幕文字内容、标题窗口、键盘输入的记录和搜索定位。SQL记录：支持审计主流数据库（如DB2、oracle、mysql、sql server）运维中的SQL语句，可进行关键信息定位查询。全文检索：支持全局搜索审计日志，无需区分图形/字符/文件/应用类型，只需通过关键信息直接搜索定位。日志数据归档：审计数据支持通过SFTP/FTP方式自动归档，并在页面中可以查询哪些数据是否归档，可以设置归档成功之后自动删除数据，归档后的数据可以用专用播放器离线查看。运维规则策略：支持通过基于时间、IP/IP段、用户/用户组、设备/设备组、设备账号、命令关键字、控制动作、黑白名单等组合访问控制策略，授权用户可访问的目标设备。二次审批：对重要设备启用登录审核功能，运维人员须向管理员申请登录，管理员允许之后才可登录；否则无法登录。命令审批：支持对重要命令进行审核：运维人员执行命令后，须等到管理员审批通过后才可执行成功。自动运维任务：支持自动推送命令任务，如可自动备份交换机/路由器的配置信息、可自动执行周期任务；并将结果以邮件/FTP/SFTP的方式发送给相关管理员运维空闲时间限制：支持运维空闲会话时间全局设置限制功能。运维报表格式：内置丰富的报表统计模板，可点击柱状图、饼状图或曲线图进行数据钻取分析，且支持PDF、doc、html格式导出。运维报表内容：内置根据运维人员和组生成各种维度的分析报表，维度包含总为运维次数、时长、活动时长、会话起止时间、会话大小、命令数、上传下载文件数，分别从全局及平均值、最大值、最小值、单次运维、单个会话等角度提供非常有价值有意义的报表。自动发送报表：支持运维报表自动定期发送，提供一键导出符合等级保护、SOX法案要求的综合分析报告。系统自审：支持自身审计，包括但不限于：系统状态检测、登录日志、用户配置日志、设备配置日志、授权配置日志、策略配置日志、运维访问日志、系统配置日志等。系统日志报表：支持系统日志报表统计功能，包括但不限于登录日志统计、配置日志统计、运维访问日志统计等，可以导出报表。告警输出：支持邮件/syslog方式输出告警日志。SNMP输出：支持SNMP方式输出系统信息。排错功能：提供排错工具：ping、TCP端口检测、UDP端口检测、路由跟踪等API接口：需提供用户、资产、授权的增删改查等API接口，允许第三方平台调用堡垒机的API接口，实现用户、资产、权限自动同步到堡垒机，简化堡垒机配置工作量。与同品牌数据库审计联动：支持和同品牌数据库审计系统进行联动，将通过SSH/RDP等加密方式操作数据库的行为整合到数据库审计中，实现数据库行为的统一集中查询、展示、审计分析等。与同品牌SOC联动：支持和同品牌的SOC系统进行联动，对绕过堡垒机而登录主机的行为，SOC进行实时告警，并且与SOC进行日志关联性分析。产品要求：[产品需获得公安部产品销售许可证](#_销售许可证)。 | 2台 |
| 8 | 城市大脑安全防护 | 日志审计系统 | 硬件规格：标准机架式设备，1个console口网口类别：6个千兆工作管理口(1管理口+1HA口+4审计口)硬盘：1T内存：8G双电源日志处理能力4000EPS（峰值：5000EPS）可扩展项：磁盘：单个磁盘可扩展至4T(仅有1个盘位)网口：可扩展至10个（4电、4光）产品要求：产品获得公安部计算机信息系统安全产品销售许可证。工作模式：独立完成审计日志采集，不依赖于设备或系统自身的日志系统；审计工作不影响被审计对象的性能、稳定性或日常管理流程；审计结果存储于独立存储空间；自身用户管理与设备或主机的管理、使用、权限无关联；提供全中文WEB管理界面，无需安装任意客户端软件或插件。全面日志采集：全支持Syslog、SNMP、XML、FTP及本地文件等协议实现对各种资产进行日志采集，智能关联分析：实现全维度、细粒度关联分析，内置众多的关联规则，支持网络安全攻防检测、合规性检测，及云计算租户间可轻松实现各资产间的关联分析。可视化展示：实现所监控的信息资产的实时监控、信息资产与客户管理、解析规则与关联规则的定义与分发、日志信息的统计与报表、海量日志的存储与快速检索以及平台的管理。通过各种事件的归一化处理，实现高性能的海量事件存储和检索优化功能，提供高速的事件检索能力、事后的合规性统计分析处理，支持各种网络部署需要，包括日志聚合、日志过滤、事件过滤、日志转发、特殊日志格式支持(如单报文多事件)等。功能扩展：采用解决方案包上传对产品进行功能扩展，无需要代码开发。日志收集：支持Syslog、SNMP Trap、OPSec、FTP协议日志收集；支持使用代理(Agent)方式提取日志并收集；支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等；设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，BEA，中国电信，安氏，帕拉迪，apc，arbor，clam，戴尔（dell），digium，东方电子，EMC，中国电力科学研究院，Eudora，google，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局），永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克），Hardened-PHP，foundertech(方正)，三零盛安，allot，蓝盾，IBM，金诺网安，网威，nortel(北电)，citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS系统日志，Linux/UNIX syslog、IIS、Apache等；支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。日志分析：可以以日志等级进行过滤；应该可以通过自定义配置将用户不关心的日志过滤掉；支持对收集到的重复的日志进行自动的聚合归并，减少日志量；支持可由用户定义和修改的日志的聚合归并逻辑规则；支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备；支持对收集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展；可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息（公网情况）；支持基于内存的实时关联分析，跨设备的多事件关联分析；支持自定义条件的事件进行聚合。具备安全评估模型：评估模型基于设备故障、认证登陆、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件；内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等5大类50子类的安全分析场景；进行关联分析的规则可定制。三维关联分析：支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。日志备份：可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比；支持日志备份自动传送到远程服务器。日志查询：支持B/S模式管理，支持SSL加密模式访问；支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询；支持用任意关键字对所有事件进行高性能全文检索；支持可指定多个查询条件进行组合查询；支持将查询的条件存储为查询模版，方便再次使用；极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。应用性能监控（APM）：支持如下应用的性能监控（Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris）、数据库（mysql、oracle）、应用服务器（weblogic、tomcat）、web服务器（apache）；支持应用性能历史详情回溯查看；支持如下性能监控参数：支持监控Windows操作系统如下参数：cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数；支持监控Linux操作系统如下参数：一分钟系统负载、5分钟系统负载、15分钟系统负载、cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数；支持监控Mysql如下参数：查询缓存命中率、键缓存命中率、立即获得锁数、连接数、线程数、每秒SQL查询数、每秒发送字节、每秒接收字节；支持监控Oracle如下参数：库缓存命中率、内存排序比率、词典缓存命中率、SGA数据缓存命中率、重做日志缓存命中率；支持监控Apache如下参数：总访问数、写日志次数、每秒发送字节数、长连接数、关闭连接数、空闲活动数、查询DNS数、正在发送数、请求完成数、负载、等待连接数、总数据量、读操作数、工作线程数、空闲线程数、CPU占用率支持监控应用服务器（tomcat、weblogic）如下参数：活动线程数、堆内存（已用）、守护线程数。脆弱性管理：支持从IBM Rational AppScan导入资产弱点漏洞信息；支持从安恒明鉴Web应用监测工具导入网站弱点漏洞信息；支持从安恒明鉴数据库弱点扫描器导入数据库弱点漏洞信息；支持从NetSparker Web应用扫描器导入网站弱点漏洞信息；支持从Nessus网络扫描器导入网络弱点漏洞信息；支持从OpenVAS扫描器导入弱点漏洞信息；内置73000+条CVE漏洞数据知识库；内置数十项符合OWASP的Web漏洞数据知识库。地理安全系统：内置GeoSec地理安全子系统，内置世界以及中国安全GIS地图；支持用地理地图展示来源威胁的趋势；支持用地理地图展示目的威胁的趋势；支持在地理地图上标注威胁事件的发生分布；内置IP地址到经纬度的转换库；支持以地理信息类进行统计的数据报表；支持切换Google地图（需要连通互联网）。告警功能：可预设置安全告警策略；支持数据阀值设置，超过阀值将产生告警；可以通过邮件、短信和屏幕显示进行告警；支持自动防止报警信息在短时间内大量发送(告警抑制)；具备报警合并和在一个时间段内抑制报警次数的能力。综合查询及报表管理：内置合规性报表1000+种；内置SOX、ISO27001、WEB安全等解决方案包；内置完善的等级保护合规报表；内置综合性自动化审计报告；支持用户自定义报表；自定义的报表支持多个统计维度的数据集合；支持报表导出为PDF和Word格式文件。用户管理：根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理；系统自带自身管理日志；注册用户资产时，提供自动发现识别能力；提供一键式故障排除功能；提供自助式的升级接口，支持对产品升级、规则升级。部署方式：支持分布式部署；支持集中式管理和升级模式；支持分级管理模式；采用B/S架构操作方式，无需客户端安装；支持监控设备自身CPU、内存、磁盘等工作运行状况。 | 2台 |
| 9 | 用户行为分析系统 | 硬件规格：CPU ≥24核（12核\*2，主频2.10 GHz，16.5 MB L3 Cache），内存≥256GB（16G\*16，DDR4 26R），配置企业级存储磁盘总容48TB（4Tb\*12，7.2k 3.5 SAS 12GB/S）；接口要求：千兆电口\*4（可选万兆双口RJ45、千兆四口RJ45、万兆双口光纤等多种网络接口）；冗余1+1电源模块，滑轨。性能要求：需采用列式存储，压缩比不低于20倍；在每条数据不小于1KB情况下，单套数据采集和处理性能应不小于30000EPS（Event per second）。聚焦用户及攻击者行为特征使用有监督、无监督和自适应的学习技术自动生成高真实度的实体风险特征，根据用户会话钻取将用户行为及相关特征展现在登入登出时间轴上，通过时间轴能够看到风险数值缓慢变化还是突然增长，同时每个评分都对应有评分原因，使安全团队能够快速进行安全调查。使用多种数据源，如流量、日志、第三方告警等，将不同的数据源数据链接在一起，通过关联分析发现更多异常行为，以提供准确的用户行为洞见并呈现有关企业内威胁活动和风险行为的更完整视图。特征管理：需提供特征增删改查功能，应支持自定义界面创建和自定义编程创建两种创建方式；应支持通过数据关联、数据过滤、特征计算与事件评分、特征得分与映射到风险总得分计算编程方式创建。UEBA特征；应支持通过数据关联、时序特征、AI异常检测、特征得分与映射到风险总得分计算界面方式创建UEBA特征；创建特征，应支持历史对比，包括但不限于前1天、前2天、前1天+前2天、前1周和前2周等；应支持时间区分，包括但不限于昼夜、周末、节日和凌晨/上午/下午/晚上等；创建特征，针对数值型特征字段，应支持包括但不限于mean均值、sum求和、median中位数、mode众数、min最小值、max最大值、distinct count非重复计数和variance方差等计算操作；创建特征，时序字段应支持包括但不限于collectorReceiptTime（采集器接收时间）、deviceReceiptTime（设备接收时间）、endTime（结束时间）和startTime（起始时间）等；创建特征，聚合粒度需支持最小1分钟颗粒度；创建特征，需提供添加过滤条件功能；需内置不少于100种UEBA用户特征场景；特征调度需支持最小1分钟调度周期；需提供各类用户特征评分的权重，可根据具体的安全业务场景进行权重调整，可分别对特征的权重设置为0、1~100或∞，便于重点关注某类风险；需提供特征列表功能，应支持查看包括但不限于特征名称、特征分组、特征描述、SQL、数据表、创建人、创建时间、状态和最近运行时间等信息，同时应支持全文搜索；需提供Backfill功能，可以补全所有未计算时间段数据或任务失败时间段数据。AI模型：需提供AI模型增删改查功能；需提供AI模型列表，应支持查看包括但不限于模型名称、模型分组、模型描述、所用特征名称、所选算法、算法参数、实时检测周期、创建人、状态、创建时间和最近运行时间等信息，同时应支持全文搜索；创建AI模型，应支持包括但不限于up/down异常、daily周期性异常、weekly周期性异常、新出现实体异常、阈值异常和潜伏型异常等算法；创建AI模型，应支持历史对比，包括但不限于前1天、前2天、前1天+前2天、前1周和前2周等；应支持时间区分，包括但不限于昼夜、周末、节日和凌晨/上午/下午/晚上等；应支持预览异常结果；创建AI模型，实时检测周期需支持最小10分钟调度周期；需提供AI模型计算任务列表，应支持查看包括但不限于任务ID、模型名称、任务类别、任务计算节点、任务开始时间、任务结束时间、任务时长、运行状态和详细信息等信息，同时应支持全文搜索。时序异常探索：需提供单时序异常探索功能，可针对AI模型进行特征时序异常探索，可以查看标记列表、异常列表和同时段异常等信息，同时应支持钻取原始日志操作；提供预测功能，预测时长应支持包括但不限于一天、一周和一月等；需提供综合异常探索功能，可针对多个AI模型进行交集或并集综合异常探查，可以查看异常排名、异常时间线、标记列表和异常列表等信息，同时应支持快捷标签和实体过滤等操作。风险评估：★需提供用户风险评分功能，能够根据个体的异常、群组对比和历史趋势等维度，按照100分风险最高评分标准综合进行用户风险评分 （提供截图）；需提供用户总体风险概览，能够直观展示包括但不限于活跃用户总数、最近一周活跃用户数、最近一周高风险用户数、日志总数、用户风险排行、关注用户、最近一周趋势图、用户风险分布图和风险类型分布等信息；需提供自定义调整用户总体风险刷新周期功能，需支持最小1分钟调度周期；需提供风险阈值调整功能，能够针对高、中、低和无4个风险级别进行区间调整；需提供针对特定用户进行用户行为画像功能，能够从风险趋势和全局画像两种模式进行用户行为画像；需提供风险趋势模式用户行为画像，能够直观展示包括但不限于风险评分、风险趋势图、风险详情和处置建议等信息，风险详情可根据风险级别和时间轴进行排序，可自定义时间范围；需提供全局画像模式用户行为画像，能够直观展示包括但不限于风险评分、风险趋势图和时间轴等信息，同时提供数据源和风险类型视角进行用户行为画像；全局画像模式中数据源视角包括但不限于VPN日志、AD域日志、DB审计（数据库审计）、NTA日志（网络流量分析系统）、DPI日志（深度报文解析系统）、OA日志（办公自动化系统）、WINDOWS主机日志、NIX主机日志、邮件审计、EDR日志（终端检测与响应系统）、人事信息、API日志（应用程序接口）、门禁日志、饭卡消费日志、车库出入日志、监控日志、钉钉考勤、上网行为审计日志、IPS日志（入侵防御系统）、IDS日志（入侵检测系统）、WAF日志（WEB应用防护系统）、APT日志（高级可持续威胁防御系统）、USM日志（统一安全管理平台）、堡垒机日志、威胁情报、SYSMON日志（微软系统监视）、防火墙日志和其他第三方终端日志等数据源信息；全局画像模式中风险类型视角包括但不限于恶意程序、账号失陷、暴力破解、漏洞扫描、数据泄露、账号活动偏离自身基线、账号活动偏离部门基线、账号异常登录、账号异常修改、API违规调用、API违规访问、API违规申请、账号暴力破解、账号失陷、恶意扫描、数据库勒索、数据泄露、数据库SQL注入、账号被盗、账号违规共享、远程办公效率分析、邮件违规收发、邮箱炸弹、邮件欺诈、账号敏感资源访问、账号越权访问、数据破坏、离职员工账号未注销、异常下载和爬虫行为等风险类型；全局画像模式中特征对应事件需提供多种可视化图表，应支持自适应和固定两种排序方式，便于排查某个用户最有风险事件。用户管理：需提供界面可视化创建修改用户信息和表格批量导入用户功能；需提供设置切换定义主键功能，应支持在多个账号属性中任意选取作为用户主属性，其他属性可关联作为从属性；可对重点用户账号进行关注操作。日志查询：支持原始日志查询。★态势大屏：需提供用户行为风险态势可视化大屏，应能够清晰展示活跃用户总数以及变化趋势，高风险用户数以及变化趋势，无风险、低风险、中风险和高风险各类用户风险分布，日高风险用户数最近一周趋势，风险类型文字云等信息；并且在大屏中央可以展示正常用户和高风险用户分布情况；同时对于特定的高风险用户，可以轮播展示用户名、职务、工号、账号、邮箱账号、风险评分、较上次风险浮动、当前风险排名、风险趋势以及各类异常图表信息（提供截图）。 | 1台 |
| 10 | 前置应用机 | 性能规格：双电源；cpu：10核；内存：256G（16G\*16，DDR4 26R）；硬盘：48TB；双电源；支持raid5。位于应用系统服务器端与客户端之间的独立处理机系统,担负数据格式转换、连接管理、业务流管理外围调度、外围处理，并把业务数据交后台应用服务系统处理等任务。 | 2台 |
| 11 | 监控管理 | 定期巡检：“一机两用”监控系统提供每月一次的巡检服务，重点检查系统运行情况，切实提升“一机两用”监控系统正常运行率。巡检的内容包括：1）新补丁公布时，为补丁库导入新的经过测试和病毒检测的补丁。2）根据网络实际使用情况，对系统安全策略进行合理的修改。3）如果系统有升级的情况，进行相应的升级维护，并说明升级有关的具体事宜。4）检查系统服务器的安全状况。主要检查系统服务器相关资源的占用情况，系统自身补丁更新情况，以及对系统进行病毒检查。5）对系统服务器报警信息的检查。重点检查报警信息的处理情况，结合报警内容，配合管理员处理内网中主要存在的一些问题。6）培训安全管理员的产品使用技巧。重点在巡检过程中对一机两用系统的相关操作使用技巧、常见问题的处理等方面对管理员进行指导和培训。7）对系统产生的数据进行备份并整理。每次巡检时，对服务器端的数据库及相关审计日志进行备份，并对原有无用数据进行清理，以保证服务器运行的稳定性和安全性。由使用方提供一台专门的备份服务器，除了能够备份数据外，还能在主服务器出现严重故障而无法正常运行时，由安装在备份服务器上的一机两用程序接管主服务器的工作。8）收集使用单位对产品的良好建议，并研发分析产品进行改进。9）每次巡检后向提供巡检报告。技术支持：安排技术服务工程师，每月10日至20日使用专用工具对服务器列表进行清理，确保每月服务器漏洞扫描工作的准确性；每月20日至下月10日，使用专用工具对“一机两用”监控系统注册率、“一机两用”监控系统补丁下载率、防病毒软件覆盖率等公安部考核数据进行清理。安排技术服务工程师，每月对“一机两用”监控系统的运行情况进行一次巡检，确保系统正常运行。产品升级：及时为“一机两用”监控系统版本维护、升级的最新升级文件包，并为现场升级提供建议方案，协助做好产品的升级工作。应急响应：故障按影响程度分为四级，一级故障定义为：由于产品原因造成网络局部或全部瘫痪；二级故障定义为：服务器端程序无法正常运行；三级故障定义为：产品部分功能无法实现；四级故障定义为部分客户端出现异常等。建设方在接到故障报告后，须在十五分钟内给出口头应急措施，一小时内给出完整解决方案。一级故障或二级故障，在电话或其他即时通讯软件无法提供解决办法的情况下，尽可能在应急措施后先恢复网络正常，并视路程距离在最短时间内赶赴现场处理。三级故障和四级故障一般以远程支持的方式解决，由于产品本身原因无法解决的，需在两天内赶赴现场负责处理。维保总结文档：巡检报告、测试报告、技术服务工作报告和年终维保总结报告，所有报告都有日期和人员签字，年终维保总结报告还需要盖章。维保工作量：定期巡检服务：每月1次考核技术支持服务：每月1次升级服务：按需服务应急响应服务：按需服务 | 三年 |
| 12 | 数据交互链路 | 探针 | 硬件规格：标准机架式设备，采用经过裁剪与安全加固的Linux操作系统；接口：6个千兆电口，1个串口，2个USB口。设备性能：吞吐量：500Mbps最大并发连接数：≥10万系统延时：<2ms日志存储数量≥20G可管理的业务量≥500个应用功能：提供对其他安全应用的syslog数据采集功能；提供对其他安全应用的snmp数据采集功能；支持对监控探针服务进程的运行日志进行保存，可自定义保存大小；可与集控监管平台集成，将采集数据传输给集中监控平台，统一管理使用；支持对snmp get 和 snmp trap信息的采集，对每个数据包进行oid唯一的过滤认证；提供对收集的syslog和snmp数据进行其他tcp或udp形式的转发（支持转源或不转源）；支持对监控探针服务器的接口流量、cpu、内存进行实时监。 | 4台 |
| 集中管控中心 | 硬件规格：标准机架式设备，采用经过裁剪与安全加固的Linux操作系统；接口：6千电口，1个串口，2个USB口。基础性能：吞吐量：≥400Mbps最大并发连接数：≥20万日志存储量：≥200GB可管理的业务量：≥1000（个）查询响应时间≤5秒应用功能：支持根据应用网络结构描绘出网络拓扑图，并绑定对于的安全设备进行拓扑图监控和告警管理，实时监控设备的数据流向、运行状态、在线状态、告警状态和实时流量显示；支持安全应用设备的网络接入功能，关联设备管理地址、通讯地址或管理端口和通讯端口，设备基本信息，厂家信息及运维信息等；支持纵向等级划分，提供对下级的业务管理和对上级的业务上报功能；支持对业务交换的内容进行统计分析，区分业务种类统计，业务量统计，业务告警统计。同时按时生成统计相关报表；支持对安全交换设备的snmp配合功能，通过snmp协议获取设备的运行信息或其他信息，提供snmp trap 和 snmp get 以及 V2和V3版本的支持。可自定义获取的属性值和oid值；管理独立于平台运行的采集组件，提供监听的端口、地址以及get模式下的轮询配置。采集信息的入库操作配置，采集日志管理配置等；支持级联上报；支持自定义统计报表功能，可加载数据源并自定义选择报表类型，横纵坐标，数量等信息，同时可保存模板；提供对数据库和配置信息的备份和恢复功能，配置可选择需要备份的信息并加密打包保存，数据库备份sql文件；支持对告警信息的通知管理配置，提供邮件通知，和短信通知（可设定多个邮件接收和短信接收）。可自定义运行信息的告警阀值；提供标准格式日志和非标准格式日志的管理和统计功能，其中标准格式日志分为：操作系统日志、权限认证日志、配置管理日志、服务认证日志、非法阻断日志和服务配置日志；支持对交换业务日志的按时自动备份功能，可自定义选择备份目录和时间间隔。产品要求：产品具备自主知识产权，提供计算机软件著作权证书；公安部计算机信息系统安全专用产品销售许可证。 | 2台 |
| 交换机 | 端口数量：24个10/100/1000Base-T以太网端口；4个千兆SFP背板带宽：336Gbps/3.024Tbps包转发率：51Mbps/126MbpsVLAN：支持4K个VLAN；支持Guest VLAN、Voice VLAN；支持GVRP协议；支持MUX VLAN功能；支持基于MAC/协议/IP子网/策略/端口的VLAN；支持1:1和N:1 VLAN Mapping功能。QOS：支持对端口接收和发送报文的速率进行限制；支持报文重定向；支持基于端口的流量监管，支持双速三色CAR功能，每端口支持8个队列；支持WRR、DRR、SP、WRR＋SP、DRR+SP队列调度算法；支持WRED；支持报文的802.1p和DSCP优先级重新标记；支持L2（Layer 2）-L4（Layer 4）包过滤功能，提供基于源MAC地址、目的MAC地址、源IP地址、目的IP地址、TCP/IP协议源/目的端口号、协议、VLAN的包过滤功能；支持基于队列限速和端口整形功能。组播管理支持IGMP v1/v2/v3 Snooping和快速离开机制；支持VLAN内组播转发和组播多VLAN复制；支持捆绑端口的组播负载分担；支持可控组播；支持基于端口的组播流量统计。网络管理 支持智能iStack堆叠；支持虚拟电缆检测（Virtual Cable Test）；支持Telnet远程配置、维护；支持SNMPv1/v2/v3；支持RMON；支持网管系统、支持WEB网管特性；支持HTTPS；支持LLDP/LLDP-MED；支持系统日志、分级告警；支持802.3az能效以太网EEE；支持断电告警Dying gasp功能。 | 4台 |
| 防火墙 | ▲硬件规格：采用先进的多核网络专用架构，使用64位MIPS多核处理器，非X86的多核架构或ASIC架构；双交流电源；1TB硬盘；网口数量：含12\*GE电口，12\*SFP光口，4\*SFP+光口。设备性能：网络吞吐量20Gbps；最大并发连接数大于500万，每秒新建HTTP连接数大于50万。部署模式：支持路由、网桥、旁路、混合、虚拟线工作模式；部署模式切换无需重启设备。端口镜像：支持端口镜像功能，支持入流量、出流量和双向流量等维度镜像。接口：接口支持配置second IP地址，每个接口要求支持至少200个second IP。4G支持：支持4G接入，并可实现4G连接与有线链路之间的互为备份；支持的4G网卡必须包括华为E3372；支持在4G接口上运行IPSec VPN。NAT：支持支持源NAT、目的NAT、静态NAT、NAT44；支持FTP、H323、PPTP、RTSP、SIP、TFTP等应用协议ALG。路由支持：支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目标地址、用户、服务、应用、时间、域名的策略路由；ISP路由支持内置联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义。链路负载均衡：支持基于7元组、域名的链路负载均衡策略；负载算法支持优先级和权重；支持过载保护、会话保持和健康检查，会话保持可实现用户的访问请求均分配至同一出口。服务器负载均衡：支持5元组的服务器负载均衡策略；支持服务器健康检查和会话保持；负载算法支持权重、源地址散列+权重。DNS代理：支持DNS透明代理功能，代理算法包括：优先级、权重和流量；支持基于多出口的DNS代理功能，可根据配置实现对不同外网线路的DNS服务器地址管理，当一条链路出现故障时，流量自动切换到其他链路的同时将DNS服务器进行切换，避免出现跨运营商解析而导致访问变慢或中断；支持静态域名配置，支持特定域名由特定DNS服务器解析，支持DNS Proxy缓存控制。DDNS：支持配置基于IPv6地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL过滤、应用识别等安全功能支持6to4、ISATAP、IPv6手工等IPv6隧道技术。VRF：接口默认属于root，创建VRF后可把接口添加到VRF内，一个接口只能属于一个VRF；不同VRF下的接口可以配置相同的IP地址；支持VRF的静态路由。双机热备：支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动，链路探测。访问控制：支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、日志记录、会话老化时间、终端过滤等高级访问控制功能。用户认证：支持本地认证、Radius认证、LDAP认证 和LDAP用户同步；支持IP+MAC准入、本地WEB认证、Portal认证、短信认证、免认证、微信认证、混合认证、AD域单点登录和访客二维码认证；微信认证功能支持使用微信连WiFi2.0接口，限制微信流量放通（移动端，认证通过放通），支持基于http获取access\_token，支持微信内部浏览器http弹portal；强制关注功能（定时检查用户是否关注公众号）；Portal认证功能支持联动portal服务器，radius服务器，支持portal逃生；支持针对HTTPS网页推送portal页面；支持伪portal推送抑制，可限制应用产生的HTTP伪推请求，有效缓解认证服务器压力。SSL解密：支持对SSL协议进行解密，解密类型支持https和邮箱。流量管理：支持基于线路和多层通道嵌套的带宽管理和流量控制功能，提供至少四层管道嵌套；支持基于地址、用户、服务、应用、时间等匹配条件进行流量控制；并支持配置保障带宽、最大带宽、每IP带宽、每用户带宽、带宽优先级等QoS动作；支持带宽动态调整技术，带宽繁忙通道支持动态借用空闲通道的带宽，避免带宽浪费；支持流量限额、时长限额，超过限额阈值提供弹窗提示且可自定义。网络攻击防护：支持防ARP欺骗、ARP flood攻击防御；支持IPv4、IPv6双协议栈异常包攻击防御，攻击类型至少包含：Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP选项、IP Spoof、Jolt2等；支持扫描攻击防御，可基于设定的阈值识别扫描，并自动对发起扫描的主机进行限制；支持基于目的IP和接口的SYN、UDP、ICMP、DNS等flood攻击防御。入侵防御：内置IPS规则库，不少于4000条主流攻击规则，包含安全漏洞、CGI攻击、缓存溢出、木马后门、网络数据库攻击、蠕虫病毒、间谍软件、欺骗劫持等安全类型（提供相关功能证明）；并支持在线升级和手动升级；支持自定义IPS特征，至少支持IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP等8种协议自定义入侵攻击特征；可拓展协议字段，设置数据包中的匹配内容，支持选择包含、等于、不等于、大于、正则匹配等匹配方式，可选择多种匹配条件，支持设置“与”和“或”的匹配顺序；至少支持telnet、ftp、imap、pop3、smtp、rlogin、http、oracle、mysql、postgres等常见协议的防暴力破解功能，针对每种协议可自定义检测时长、阈值和阻断时长；至少支持telnet、ssh、ftp、imap、pop3、smtp、mysql、postgresql、mssql、rlogim、vnc等常见协议的弱密码检测功能，支持弱口令、空密码、用户名和密码相同等检测方式，弱口令字典可自定义设置；支持DNS隧道传输检测，用于检测DNS隧道协议中的恶意流量；支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口；支持通过流量自学习获得服务器合法的外联行为，检测流量中的异常访问流量，实现自动拦截；学习时长可选择1小时、12小时、一天、一周等；支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者SYSLOG告警，不同告警规则可以发送给不同的用户。Web防护：支持HTTP协议的精确访问控制，可针对IP、URL、Method、Referer、User-Agent、Cookie、Url-args等字段设置内容，匹配内容包括但不少于：包括、不包含、等于、不等于、属于、不属于、长度小于、长度等于、长度大于、正则匹配等；日志级别包括但不少于：不记录、危急、告警、严重、错误、警告、通知、信息等；支持防盗链、CSRF攻击、CC攻击、应用隐藏、网页防篡改等防护；应用隐藏可隐藏Server信息、X-Powered-By信息、替换客户端出错页面(4xx)、替换服务器端出错页面(5xx)等；内置Web防护特征库，提供SQL注入攻击、XSS攻击、恶意扫描与爬虫、服务器防护、CMS漏洞防护等不少于10种的防护类型；特征库库支持手动升级和自动升级；支持网页防篡改，可手动清理缓存内容。云端威胁情报订阅模块：提供威胁情报离线库并支持更新。威胁情报：拥有自有数据来源，每日可获得不低于6亿次的互联网访问样本；具有情报数据置信度算法，提供高置信度活跃威胁情报数据不低于160万。支持20余种威胁分类，包括C&C节点、僵尸网络、木马、勒索、钓鱼等；提供在设备端上的全网威胁情报的搜索查询，包括IP、域名、文件（MD5/SHA1等）情报的查询；提供最新的威胁情报信息，能够对新爆发的0day、高危漏洞等进行预警，并提供配置向导协助管理员生成安全防护策略；支持实时获取威胁情报，并应用威胁情报对本地资产进行威胁检测，并可对检测到的威胁情报支持单点登陆威胁情报云平台查看该情报详情。IPSec VPN：支持与第三方的IPSec VPN接入，支持DES、3DES、AES等加密算法和SM3、SM4等国密算法；支持IPSec快速配置，当跟自有设备对接时，自动生成加密算法等参数，仅需配置保护子网、共享密钥、IP地址；支持GRE隧道，支持GRE over IPSec VPN。SSL VPN：支持自定义资源类型，可定义发布的协议和端口，资源支持导入导出，可快速完成配置；支持自定义门户页面中的标题、logo和公告内容；支持SSL VPN用户防暴力破解功能，可根据用户和IP设置防护阈值；支持SSL VPN账号与VPN资源唯一绑定，针对拨入用户设置拨入时间段和强制下线时间，精细管控用户访问权限。应用缓存：支持文件缓存，支持安卓和IOS形式的文件，文件形式不限于视频、APP、文本文件等；并支持自学习性缓存，设备可自动缓存特定服务器的所有终端应用。共享接入管理：支持识别和封堵私接主机，包括360随身wifi、猎豹wifi、无线路由器等软硬件网络共享方式；可制定策略分别设置私接终端类型个数为阀值进行封堵，同时支持基于IP配置白名单，支持自定义阻断时间，支持限速时长内添加到惩罚通道。支持私接用户的PPPoE账号展现，支持状态监控、解锁操作，支持基于用户、MAC、终端数量的监控和搜索。广告推送：支持配置在用户上网时弹出广告页面，支持本地和第三方广告；支持PC端推送4个方位的广告，手机端支持推送全屏广告，支持配置广告跳转链接和广告推送间隔。PKI：支持X.509 V3数字证书；支持CER/PEM/PKCS12多种证书编码；支持内置CA，为其他设备或移动用户签发证书；支持本地CA根证书、根私钥的更新；支持在线CRL列表。会话管理：支持基于IP的会话限制和每秒新建限制；实时显示当前会话数和历史1小时、1天、1周会话数；支持基于会话的源地址、目的地址、目的端口的排名统计；会话监控界面展示当前会话数信息，显示会话属性至少包含用户、用户组、源地址、源端口、目的地址、目的端口、协议、类型、应用、策略ID、发送包数、接收包数、总包数、发送流量、接收流量、总流量、会话状态、本地连接、策略动作、创建时间、超时时间、存在时间、入接口、出接口、源NAT地址、源NAT端口、目的NAT地址、目的NAT端口等25项，并且可根据任意条件进行查询和排序。策略分析：支持策略分组，每条策略添加到一个策略组，便于管理员区分化管理和运维；提供策略分析引擎，支持一键全局分析和单独策略的即时分析，至少支持检测出冗余策略、隐藏策略、冲突策略、可合并策略、空策略、过期策略；提供问题策略的原因说明、优化建议，并提供快捷的编辑修改方式；支持以表格和柱状统计图形式展示全局策略的分析概况、问题策略详情；支持全局策略宽松度分析，以引用策略中的源地址、目的地址中的实际IP地址数目换算得到极宽松、较宽松、正常、准确这4种宽松度级别，并以表格和柱状统计图形式展示地址精确度分析结果。安全分析：具备对检测到的攻击行为按照攻击源地址的地理位置进行威胁信息展示，并支持将攻击源地址一键加入到黑名单的操作；支持基于资产的安全分析，支持展示网络中存在安全风险的资产以及对应的风险级别，至少可查看资产基本信息、攻击态势、攻击日志统计、攻击的具体事件类型、攻击时间等；支持基于攻击不同阶段的方式来匹配并展示攻击者发起攻击的具体所处状态，资产遭受到攻击的具体所处状态，展示出具体的攻击链并可对威胁进行取证。系统日志：支持本地日志记录和远程日志输出，SYSLOG日志支持同时发给多个日志服务器。业务告警：支持针对设备健康状态，业务信息等维度告警；支持预设告警阀值；告警日志支持导出；支持邮件等方式告警。统计报表：支持统计设备健康状态、用户行为、网络质量、网络安全等报表；支持每天、每周、每月生成报表；支持HTML、PDF等报表格式，并可通过邮件、FTP等方式外发。系统维护：web管理界面支持Ping、Traceroute、TCP Syn诊断工具；可支持基于接口、协议、IP地址、端口、应用进行网络抓包，并可下载导出分析；支持通过ICMP、TCP、DNS等协议实现对链路可用性的多重健康检查，并支持统计探测目标的成功率和延时；支持三权管理方式，包括账号管理员、权限管理员、审核员，各管理员权限制约；权限管理员支持分配权限，可细致分配界面中每一个模块的读写权限；支持管理员双因子认证。配置管理：支持中英文Web界面管理及命令行管理，支持基于SSL协议的远程安全管理；支持通过集中管理平台进行集中管理，包括统一状态检测、配置下发、配置自动备份，版本升级、特征库升级、日志收集；支持U盘零配置上线，设备端无需预配置，将U盘插入设备USB接口中，即可实现快速上线实施；支持SNMPv1、v2、v3版本，支持跨三层自学习MAC地址；支持多配置切换，配置文件之间相对独立，灾备场景可快速恢复业务，保障业务正常运行。产品要求：具备公安部颁发的防火墙《计算机信息系统安全专用产品销售许可证（增强级）》 | 5台 |
| 高性能防火墙 | ▲硬件规格：采用先进的多核网络专用架构，使用64位MIPS多核处理器，非X86的多核架构或ASIC架构；双交流电源；1TB硬盘；网口数量：含12\*GE电口，12\*SFP光口，8\*SFP+光口。设备性能：网络吞吐量80Gbps；最大并发连接数大于1000万，每秒新建HTTP连接数大于90万。部署模式：支持路由、网桥、旁路、混合、虚拟线工作模式；部署模式切换无需重启设备。端口镜像：支持端口镜像功能，支持入流量、出流量和双向流量等维度镜像。接口：接口支持配置second IP地址，每个接口要求支持至少200个second IP。4G支持：支持4G接入，并可实现4G连接与有线链路之间的互为备份；支持的4G网卡必须包括华为E3372；支持在4G接口上运行IPSec VPN。NAT：支持支持源NAT、目的NAT、静态NAT、NAT44；支持FTP、H323、PPTP、RTSP、SIP、TFTP等应用协议ALG。路由支持：支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目标地址、用户、服务、应用、时间、域名的策略路由；ISP路由支持内置联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义。链路负载均衡：支持基于7元组、域名的链路负载均衡策略；负载算法支持优先级和权重；支持过载保护、会话保持和健康检查，会话保持可实现用户的访问请求均分配至同一出口；服务器负载均衡：支持5元组的服务器负载均衡策略；支持服务器健康检查和会话保持；负载算法支持权重、源地址散列+权重。DNS代理：支持DNS透明代理功能，代理算法包括：优先级、权重和流量；支持基于多出口的DNS代理功能，可根据配置实现对不同外网线路的DNS服务器地址管理，当一条链路出现故障时，流量自动切换到其他链路的同时将DNS服务器进行切换，避免出现跨运营商解析而导致访问变慢或中断；支持静态域名配置，支持特定域名由特定DNS服务器解析，支持DNS Proxy缓存控制。DDNS：支持配置基于IPv6地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL过滤、应用识别等安全功能支持6to4、ISATAP、IPv6手工等IPv6隧道技术。VRF：接口默认属于root，创建VRF后可把接口添加到VRF内，一个接口只能属于一个VRF；不同VRF下的接口可以配置相同的IP地址；支持VRF的静态路由。双机热备：支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动，链路探测。访问控制：支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、日志记录、会话老化时间、终端过滤等高级访问控制功能。用户认证：支持本地认证、Radius认证、LDAP认证 和LDAP用户同步；支持IP+MAC准入、本地WEB认证、Portal认证、短信认证、免认证、微信认证、混合认证、AD域单点登录和访客二维码认证；微信认证功能支持使用微信连WiFi2.0接口，限制微信流量放通（移动端，认证通过放通），支持基于http获取access\_token，支持微信内部浏览器http弹portal；强制关注功能（定时检查用户是否关注公众号）；Portal认证功能支持联动portal服务器，radius服务器，支持portal逃生；支持针对HTTPS网页推送portal页面；支持伪portal推送抑制，可限制应用产生的HTTP伪推请求，有效缓解认证服务器压力。SSL解密：支持对SSL协议进行解密，解密类型支持https和邮箱。流量管理：支持基于线路和多层通道嵌套的带宽管理和流量控制功能，提供至少四层管道嵌套；支持基于地址、用户、服务、应用、时间等匹配条件进行流量控制；并支持配置保障带宽、最大带宽、每IP带宽、每用户带宽、带宽优先级等QoS动作；支持带宽动态调整技术，带宽繁忙通道支持动态借用空闲通道的带宽，避免带宽浪费；支持流量限额、时长限额，超过限额阈值提供弹窗提示且可自定义。网络攻击防护：支持防ARP欺骗、ARP flood攻击防御；支持IPv4、IPv6双协议栈异常包攻击防御，攻击类型至少包含：Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP选项、IP Spoof、Jolt2等；支持扫描攻击防御，可基于设定的阈值识别扫描，并自动对发起扫描的主机进行限制；支持基于目的IP和接口的SYN、UDP、ICMP、DNS等flood攻击防御。入侵防御：内置IPS规则库，不少于4000条主流攻击规则，包含安全漏洞、CGI攻击、缓存溢出、木马后门、网络数据库攻击、蠕虫病毒、间谍软件、欺骗劫持等安全类型（提供相关功能证明）；并支持在线升级和手动升级；支持自定义IPS特征，至少支持IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP等8种协议自定义入侵攻击特征；可拓展协议字段，设置数据包中的匹配内容，支持选择包含、等于、不等于、大于、正则匹配等匹配方式，可选择多种匹配条件，支持设置“与”和“或”的匹配顺序；至少支持telnet、ftp、imap、pop3、smtp、rlogin、http、oracle、mysql、postgres等常见协议的防暴力破解功能，针对每种协议可自定义检测时长、阈值和阻断时长；至少支持telnet、ssh、ftp、imap、pop3、smtp、mysql、postgresql、mssql、rlogim、vnc等常见协议的弱密码检测功能，支持弱口令、空密码、用户名和密码相同等检测方式，弱口令字典可自定义设置；支持DNS隧道传输检测，用于检测DNS隧道协议中的恶意流量；支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口；支持通过流量自学习获得服务器合法的外联行为，检测流量中的异常访问流量，实现自动拦截；学习时长可选择1小时、12小时、一天、一周等；支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者SYSLOG告警，不同告警规则可以发送给不同的用户。Web防护：支持HTTP协议的精确访问控制，可针对IP、URL、Method、Referer、User-Agent、Cookie、Url-args等字段设置内容，匹配内容包括但不少于：包括、不包含、等于、不等于、属于、不属于、长度小于、长度等于、长度大于、正则匹配等；日志级别包括但不少于：不记录、危急、告警、严重、错误、警告、通知、信息等；支持防盗链、CSRF攻击、CC攻击、应用隐藏、网页防篡改等防护；应用隐藏可隐藏Server信息、X-Powered-By信息、替换客户端出错页面(4xx)、替换服务器端出错页面(5xx)等；内置Web防护特征库，提供SQL注入攻击、XSS攻击、恶意扫描与爬虫、服务器防护、CMS漏洞防护等不少于10种的防护类型；特征库库支持手动升级和自动升级；支持网页防篡改，可手动清理缓存内容。云端威胁情报订阅模块：提供威胁情报离线库并支持更新。威胁情报：拥有自有数据来源，每日可获得不低于6亿次的互联网访问样本；具有情报数据置信度算法，提供高置信度活跃威胁情报数据不低于160万。支持20余种威胁分类，包括C&C节点、僵尸网络、木马、勒索、钓鱼等；提供在设备端上的全网威胁情报的搜索查询，包括IP、域名、文件（MD5/SHA1等）情报的查询；提供最新的威胁情报信息，能够对新爆发的0day、高危漏洞等进行预警，并提供配置向导协助管理员生成安全防护策略；支持实时获取威胁情报，并应用威胁情报对本地资产进行威胁检测，并可对检测到的威胁情报支持单点登陆威胁情报云平台查看该情报详情。IPSec VPN：支持与第三方的IPSec VPN接入，支持DES、3DES、AES等加密算法和SM3、SM4等国密算法；支持IPSec快速配置，当跟自有设备对接时，自动生成加密算法等参数，仅需配置保护子网、共享密钥、IP地址；支持GRE隧道，支持GRE over IPSec VPN。SSL VPN：支持自定义资源类型，可定义发布的协议和端口，资源支持导入导出，可快速完成配置；支持自定义门户页面中的标题、logo和公告内容；支持SSL VPN用户防暴力破解功能，可根据用户和IP设置防护阈值；支持SSL VPN账号与VPN资源唯一绑定，针对拨入用户设置拨入时间段和强制下线时间，精细管控用户访问权限。应用缓存：支持文件缓存，支持安卓和IOS形式的文件，文件形式不限于视频、APP、文本文件等；并支持自学习性缓存，设备可自动缓存特定服务器的所有终端应用。共享接入管理：支持识别和封堵私接主机，包括360随身wifi、猎豹wifi、无线路由器等软硬件网络共享方式；可制定策略分别设置私接终端类型个数为阀值进行封堵，同时支持基于IP配置白名单，支持自定义阻断时间，支持限速时长内添加到惩罚通道。支持私接用户的PPPoE账号展现，支持状态监控、解锁操作，支持基于用户、MAC、终端数量的监控和搜索。广告推送：支持配置在用户上网时弹出广告页面，支持本地和第三方广告；支持PC端推送4个方位的广告，手机端支持推送全屏广告，支持配置广告跳转链接和广告推送间隔。PKI：支持X.509 V3数字证书；支持CER/PEM/PKCS12多种证书编码；支持内置CA，为其他设备或移动用户签发证书；支持本地CA根证书、根私钥的更新；支持在线CRL列表。会话管理：支持基于IP的会话限制和每秒新建限制；实时显示当前会话数和历史1小时、1天、1周会话数；支持基于会话的源地址、目的地址、目的端口的排名统计；会话监控界面展示当前会话数信息，显示会话属性至少包含用户、用户组、源地址、源端口、目的地址、目的端口、协议、类型、应用、策略ID、发送包数、接收包数、总包数、发送流量、接收流量、总流量、会话状态、本地连接、策略动作、创建时间、超时时间、存在时间、入接口、出接口、源NAT地址、源NAT端口、目的NAT地址、目的NAT端口等25项，并且可根据任意条件进行查询和排序。策略分析：支持策略分组，每条策略添加到一个策略组，便于管理员区分化管理和运维；提供策略分析引擎，支持一键全局分析和单独策略的即时分析，至少支持检测出冗余策略、隐藏策略、冲突策略、可合并策略、空策略、过期策略；提供问题策略的原因说明、优化建议，并提供快捷的编辑修改方式；支持以表格和柱状统计图形式展示全局策略的分析概况、问题策略详情；支持全局策略宽松度分析，以引用策略中的源地址、目的地址中的实际IP地址数目换算得到极宽松、较宽松、正常、准确这4种宽松度级别，并以表格和柱状图形式展示地址精确度分析结果。安全分析：具备对检测到的攻击行为按照攻击源地址的地理位置进行威胁信息展示，并支持将攻击源地址一键加入到黑名单的操作；支持基于资产的安全分析，支持展示网络中存在安全风险的资产以及对应的风险级别，至少可查看资产基本信息、攻击态势、攻击日志统计、攻击的具体事件类型、攻击时间等；支持基于攻击不同阶段的方式来匹配并展示攻击者发起攻击的具体所处状态，资产遭受到攻击的具体所处状态，展示出具体的攻击链并可对威胁进行取证。系统日志：支持本地日志记录和远程日志输出，SYSLOG日志支持同时发给多个日志服务器。业务告警：支持针对设备健康状态，业务信息等维度告警；支持预设告警阀值；告警日志支持导出；支持邮件等方式告警。统计报表：支持统计设备健康状态、用户行为、网络质量、网络安全等报表；支持每天、每周、每月生成报表；支持HTML、PDF等报表格式，并可通过邮件、FTP等方式外发。系统维护：web管理界面支持Ping、Traceroute、TCP Syn诊断工具；可支持基于接口、协议、IP地址、端口、应用进行网络抓包，并可下载导出分析；支持通过ICMP、TCP、DNS等协议实现对链路可用性的多重健康检查，并支持统计探测目标的成功率和延时；支持三权管理方式，包括账号管理员、权限管理员、审核员，各管理员权限制约；权限管理员支持分配权限，可细致分配界面中每一个模块的读写权限；支持管理员双因子认证。配置管理：支持中英文Web界面管理及命令行管理，支持基于SSL协议的远程安全管理；支持通过集中管理平台进行集中管理，包括统一状态检测、配置下发、配置自动备份，版本升级、特征库升级、日志收集；支持U盘零配置上线，设备端无需预配置，将U盘插入设备USB接口中，即可实现快速上线实施；支持SNMPv1、v2、v3版本，支持跨三层自学习MAC地址；支持多配置切换，配置文件之间相对独立，灾备场景可快速恢复业务，保障业务正常运行。产品要求：具备公安部颁发的防火墙《计算机信息系统安全专用产品销售许可证（增强级）》 | 1台 |
| 光闸 | 全面支持64位计算技术；支持多核心CPU硬件技术；使用内核级IDS，确保系统关键进程安全，阻止非授权访问；操作系统内核以及关键进程部分进行硬件固化；摒弃通用的系统函数调用，私有系统调用不对外开放，仅供内部使用；身份认证：采用身份认证技术对使用光闸的用户进行身份鉴别，以确保只有合法用户和计算机能使用光闸系统传输数据，包括高强度双重口令认证、CA证书认证等； 数据导入：支持专用客户端等方式的文件数据物理单向传输（外向内）；支持针对不同的传输任务开启鉴权认证控制功能。数据传输时将会先判断任务是否已鉴权完成，鉴权成功的才可以正常执行数据传输。支持文件单向摆渡；支持文件类型过滤；支持文件后缀过滤；支持多文件并发传输；支持本地FTP服务、远程FTP服务、本地SMB服务、远程SMB服务、NFS服务、光盘塔服务、client服务、认证同步服务等，实现目录下特定文件的单向导入；根据权限划分每个用户的文件传输通道；数据传输高度可靠，采用缓存确认机制进行保证；支持数据库单向摆渡：支持Oracle、SQLServer、MySQL、DB2、SYBase等主流数据库，支持人大金仓、达梦等国产数据库，支持对以上数据库插入、删除和更新等操作的监控，并对操作产生的表记录内容进行单向传；数据库同步功能：支持异构数据库同步；自增字段同步；主从表外键同步；支持容错处理；同步方式支持增量、全表方式，支持多种同步模式，支持任务调度等。支持BLOB、CLOB、TEXT、IMAGE等大字段同步；实时访问扩展：支持正反单向光闸与数据安全交换前后置系统结合部署，构建支持基于TCP实时访问应用，支持指令交换扩展；系统与数据交换前后置系统之间通过内部可认证的API私有接口传输，不采用通用协议进行数据传输；日志功能：提供系统日志显示、读取功能，日志信息可配置、可管理，支持SYSLOG输出专用日志服务程序处理系统日志；提供日志审计、导出、过滤等强化功能；支持全文审计功能；管理功能：通过浏览器对光闸进行管理；系统配置信息可导出备份、导入恢复；系统支持一键还原功能，在系统出现严重配置错误、系统损坏时可通过后台管理员操作将系统还原成初始状态；管理口与业务口分离，增强配置信息抗干扰能力；业务能力：文件传输性能600Mbps；数据库传输能力2000条/秒；数据差错率<1Bit/1TBit；系统处理能力2Gbps；底层硬件数据吞吐量单向1Gbps；产品要求：具备公安部销售许可证（增强级）；具备自主知识产权软件著作权证书 | 8台 |
| 数据交换前置 | ▲硬件规格：标准机架式设备；采用经过裁剪与安全加固的Linux操作系统；与后置机配套使用；接口：接口：6个千兆电口，1个串口，2个USB口；具备接口聚合功能；具备双机热备功能。设备性能：吞吐率≥800Mbps，系统延时≤40ms；并发数≥10万；大文件传输速度≥500Mbps/s；小文件传输速度(10KB)≥60个/s，单个文件≥20G；数据库记录传输速度≥2000条/s，交换并发表≥2048个。安全功能：能够对提请交换的应用和设备进行真实性认证，禁止未认证应用和设备上线；支持对系统服务的访问控制功能；支持通过手动或特定时间自动清理缓存中的各文件碎片、修复文件系统错误；系统内置恢复引擎实现故障的事后恢复，恢复进程与当前数据集成交换进程保持独立；数据交换过程出现业务故障时报警。应用功能：支持本地FTP、本地SMB、远程FTP、SFTP、SMB、NFS服务；支持对图片的文字进行识别和过滤；支持断点重传功能；支持ORACLE、Sql server、sybase、mysql及国产数据库(武汉达梦、人大金仓KINGBASE、神舟通用OSCAR) 等主流数据库间的数据交换，支持全表同步、增量同步模式，支持数据库定时同步、实时同步，支持一对一、一对多、多对一数据库表同步；支持数据库自定义字段同步和自增字段的同步，用户可自定义需要同步的字段；授权用户仅可通过产品的ftp客户端方可访问不同ftp资源，卸载或关闭ftp安全客户端后,用户无法访问ftp资源；ftp客户端与ftp服务器之间采用加密访问。文件同步方式：具备剪切和复制模式同步，支持定时同步、实时同步，支持一对多、多对一同步。文件同步安全：支持在FTP同步方式和SMB同步方式下文件的恶意代码检查功能，能够将包含恶意代码的文件进行隔离，通过设置黑名单能够对同步的文件名和文件内容关键字过滤，通过设置黑白名单对具有特定后缀的文件进行过滤，对文件特征进行过滤，支持TXT、pdf、xls、xlsx、doc、docx、ppt、pptx、wps、dps、et格式文件。数据库同步容错(数据库服务中断恢复后同步正常)：支持Orac1e、Sq1Server、Sybase、Mysq1及达梦DM等主流数据库的条件同步和外键同步；支持数据库条件同步。混合数据同步：采用分布式数据队列技术,能够将数据传输队列分配到不同硬盘进行存储；支持同步阻塞和异步传输两种数据交换方式。数据加密：数据存储非明文能够配置数据交付优先级,并对数据交付优先级进行控制;可查询数据交换状态和日志信息,日志信息有登录日志信息、和队列配置操作信息支持数据对账功能,提供与业务系统间的自动对账功能 。设备管理：采用B/S结构或串口管理, GUI图形管理界面，采用HTTPS协议连接管理设备；采用三权分立管理；智能自动匹配功能，能对结构不同的表可以进行自动比对和映射支持显示所有接口信息，并能显示连接状态；支持常用网管命令，如ping、telnet、trace route、arp等；支持链路自动侦测功能，能对数据库同步、文件同步、请求服务的链路状态进行侦测；支持设备系统升级；支持设备配置备份和恢复。日志审计：能针对所有任务进行统计，并能根据时间、任务名、表名、ip等关键字进行筛选；能对数据库同步日志进行详细记录，包括同步成功，同步失败，可根据主键、时间、表名、业务名、任务名等关键字进行筛选支持通过SYSLOG、SNMP方式输出。产品要求：公安部计算机信息系统安全专用产品销售许可证增强级 | 8台 |
| 数据交换后置 | 硬件规格：标准机架式设备；采用经过裁剪与安全加固的Linux操作系统；与前置机配套使用；接口：接口：6个千电口，1个串口，2个USB口；具备接口聚合功能；具备双机热备功能。设备性能：吞吐率≥800Mbps，系统延时≤40ms；并发数≥10万；大文件传输速度≥500Mbps/s；小文件传输速度(10KB)≥60个/s，单个文件≥20G；数据库记录传输速度≥2000条/s，交换并发表≥2048个。安全功能：能够对提请交换的应用和设备进行真实性认证，禁止未认证应用和设备上线；支持对系统服务的访问控制功能；支持通过手动或特定时间自动清理缓存中的各文件碎片、修复文件系统错误；系统内置恢复引擎实现故障的事后恢复，恢复进程与当前数据集成交换进程保持独立；数据交换过程出现业务故障时报警。应用功能：支持本地FTP、本地SMB、远程FTP、SFTP、SMB、NFS服务；支持对图片的文字进行识别和过滤；支持断点重传功能；支持ORACLE、Sql server、sybase、mysql及国产数据库(武汉达梦、人大金仓KINGBASE、神舟通用OSCAR) 等主流数据库间的数据交换，支持全表同步、增量同步模式，支持数据库定时同步、实时同步，支持一对一、一对多、多对一数据库表同步；支持数据库自定义字段同步和自增字段的同步，用户可自定义需要同步的字段；授权用户仅可通过产品的ftp客户端方可访问不同ftp资源，卸载或关闭ftp安全客户端后,用户无法访问ftp资源；ftp客户端与ftp服务器之间采用加密访问。文件同步方式：具备剪切和复制模式同步，支持定时同步、实时同步，支持一对多、多对一同步。文件同步安全：支持在FTP同步方式和SMB同步方式下文件的恶意代码检查功能，能够将包含恶意代码的文件进行隔离，通过设置黑名单能够对同步的文件名和文件内容关键字过滤，通过设置黑白名单对具有特定后缀的文件进行过滤，对文件特征进行过滤，支持TXT、pdf、xls、xlsx、doc、docx、ppt、pptx、wps、dps、et格式文件。数据库同步容错(数据库服务中断恢复后同步正常)：支持Orac1e、Sq1Server、Sybase、Mysq1及达梦DM等主流数据库的条件同步和外键同步；支持数据库条件同步。混合数据同步：采用分布式数据队列技术,能够将数据传输队列分配到不同硬盘进行存储；支持同步阻塞和异步传输两种数据交换方式。数据加密：数据存储非明文能够配置数据交付优先级,并对数据交付优先级进行控制;可查询数据交换状态和日志信息,日志信息有登录日志信息、和队列配置操作信息支持数据对账功能,提供与业务系统间的自动对账功能。设备管理：采用B/S结构或串口管理, GUI图形管理界面，采用HTTPS协议连接管理设备；采用三权分立管理；智能自动匹配功能，能对结构不同的表可以进行自动比对和映射支持显示所有接口信息，并能显示连接状态；支持常用网管命令，如ping、telnet、trace route、arp等支持链路自动侦测功能，能对数据库同步、文件同步、请求服务的链路状态进行侦测；支持设备系统升级；支持设备配置备份和恢复。日志审计：能针对所有任务进行统计，并能根据时间、任务名、表名、ip等关键字进行筛选；能对数据库同步日志进行详细记录，包括同步成功，同步失败，可根据主键、时间、表名、业务名、任务名等关键字进行筛选支持通过SYSLOG、SNMP方式输出。产品要求：公安部计算机信息系统安全专用产品销售许可证增强级 | 8台 |
| 定制协议高速传输系统（前置机/后置机） | 硬件规格：标准机架式设备，采用经过裁剪与安全加固的Linux操作系统，由定制协议高速传输系统前置机与定制协议高速传输系统后置机组成；接口：4个千兆电口，1个串口，2个USB口，具备接口聚合功能；标配冗余电源。设备性能：吞吐率≥800Mbps；系统延时：<0.5ms；10B大小的数据每秒处理≥6500个，10KB大小的数据每秒处理≥5000个；300KB大小的数据吞吐量≥85MB/S，延时≤50ms；每秒新建API服务连接数：>1500/秒；500KB大小的数据吞吐量≥95MB/S，延时≤100ms。部署模式：支持网关型与旁路部署方式安全功能：对登录会话进行控制，可限制超时时长，登录错误数以及锁定账号时长等；支持唯一Token认证，只有经过认证的应用才能进行数据安全交互；支持数据加密，数据存储非明文，保证数据安全；对所传输的文件格式进行检查，避免在数据交换过程中交换可执行程序，而造成病毒、木马夹杂在交换数据中进行传播；采用数据队列技术，实现集群环境下的分布式数据队列；采用分布式体系架构，支持链路负载均衡集群服务。应用功能：系统采用定制化数据传输协议，支持短信息、结构化数据、非结构化数据、自定义数据及以上数据类型的混合数据同步交换；支持同步阻塞和异步传输两种数据交换方式；采用文件方式实现数据交换；支持数据对账功能，提供与业务系统间的自动对账功能；支持数据交付优先级控制。设备管理：采用B/S结构或串口管理, GUI图形管理界面，采用HTTPS协议连接管理设备；采用三权分立管理；具备通过浏览器可以查看拓扑结构及定制协议应用情况；通过监控页面及时查询数据交换运行状态(队列类型、队列说明、队列数、预警值、风险值等信息)和硬盘存储信息(前置硬盘\后置硬盘路径、容量、空余、百分比等)；支持设备系统升级；支持设备配置备份和恢复；支持负载均衡。日志审计：支持通过SYSLOG、SNMP方式输出。产品要求：公安部计算机信息系统安全专用产品销售许可证增强级 | 4台 |
| 边界可信网关 | 硬件规格：标准机架式，6千电口,2千光口；1个串口，2个USB口。设备性能：吞吐量≥3Gbps；延时≤80us，并发数≥80万，IPSec VPN隧道数1000条，IPSec加密吞吐率350Mbps，SSL VPN并发用户数800。身份认证：与公安PKI/PMI体系无缝集成，支持证书认证，保证接入用户身份合法性。设备认证：支持IP、MAC方式的设备认证，保证接入设备的合法性。权限管理：可以根据边界接入的需求，设置角色，制定相应的资源访问权限，防止非授权访问和越权访问。访问控制：基于角色、权限分配，设置细粒度访问控制策略，达到非法用户不能访问，合法用户不能越权访问的目的。传输保护：与客户端之间采用ssl协议对通讯过程进行加密和完整性保护。保证数据传输的安全性。监控审计：对接入用户的访问过程进行详细记录，并实时报送给集中监控与审计系统，保证用户访问过程可控、可查和可追溯。 | 2台 |
| 13 | 等保测评 | 衢州公安门户网站 | 衢州市公安局官网、各类信息发布、办事服务等 | 三级 | 一次 |
| 衢州公安网上审批系统 | 办理衢城通办、身后事联办、不宜网办的业务 |
| 衢州智能应用平台 | 子模块：衢州智能应用平台、衢州市视频图像信息共享平台、衢州市一体化智慧平台 |
| 信息采集系用 | 子模块：北大高科指纹自动识别系统、足迹信息查询系统、刑事技术管理系统、DNA信息录入及比对、DNA信息管理及上报 |
| 交警综合管理平台 | 子模块：综合平台外挂系统、影像化系统、隐患排查系统、机动车扩充系统、驾驶人拍照系统 |
| 道路交通智能监控平台（指挥中心平台） |  “公安交通指挥中心集成平台”是城市智能交通管理系统的核心业务应用，它是在已建成的各种外场设施、各类交通管理信息系统的基础上，以数据交换和数据共享为纽带 |
| 衢州公安数据交换系统 | 公安网9条边界链路 |
| 公共场所无线WIFI数据采集和处理 |  |
| 警格联动 | \*\*\*门户，基础数据排查 | 二级 |
| 浙江政务服务网统一行政权力运行系统 | 办理开具电子证明、审批货车入城通行证等业务 |
| 衢州公安信息资源综合应用平台 | 综合查询 |
| 信息共享平台 | 子模块：衢州市公安局警用地理信息系统、部门间信息共享服务平台 |
| 城际管理分析系统 | IMSI接入、综合应用 |
| 经济协同平台 | 财物报销等 |
| 散装汽油管控系统 | 实现全市散装汽油购销实名购买、实情登记、实时传输、实时比对、实时预警。 |
| 档案管理系统 |  |
| 网吧安全管理审计系统 |  |
| 银行对账系统 | 为提高执法效率，实现银行服务网点渠道自由选择缴纳罚没款，依据我市业务实际，建设交通违法罚没款对账系统，实现交通违法缴费功能。 |
| 黑名单比对报警系统 | 对过车车辆进行系统黑名单实时比对，便于路面民警实时拦截处理。 |
| 移动\*\*采集平台 | 子模块：执法记录仪采集平台、衢州交警移动\*\*系统 |
| 衢州市交通运行指数实时监测平台 | 道路交通运行指数（TPI）是综合反映道路网交通拥堵运行状况的标准化定量指标。  |
| 政工系统 | 对全局队伍管理 |
| 非机动车管理平台 | 提供非机动车注册登记管控功能；114移车服务：为电信提供本市机动车所有人联系方式的接口开放功能。 |
| 全市重要信息系统与网站安全态势感知和预警 |  |
| IV007涉案车辆研判系统 | 车辆卡口智能查询 |

## 5、培训赋能及运维应急服务

|  |  |  |  |
| --- | --- | --- | --- |
| **培训****赋能** | 培训对象 | 管理人员主要包括：高层管理、业务专家等。培训目标：对管理人员的培训，目的是使他们了解国家相关部门对系统信息安全管理和建设的相关标准，同时建立起一套具有针对性和适用性的安全管理办法。技术人员主要包括：操作人员、开发人员、维护人员等。培训目标：对技术人员的培训，目的是使他们了解信息系统所面临的严峻安全威胁和挑战，以及如何进行全面有效的安全防护措施。全员培训主要包括：安全意识培训等。培训目标：通过专业、全面的信息安全理论、信息安全实践等课程，提高全员的安全意识，提高技术人员的安全技术能力，提高管理人员的安全安全管理水平。提供培训课程包括但不限于安全意识培训、安全运维培训、安全攻防培训、安全开发培训、等保安全培训及定制化培训等。 | 三年 |
| 培训课程 | 安全形势及安全管理：《网络安全法》、《网络安全形势分析》、《网络安全管理》、《等保2.0标准》。 | 1年/次40人次 |
| 安全意识培训：《信息安全事件和安全威胁》、《日常安全和必备安全习惯》、《信息安全基础》。 | 1年/次40人次 |
| 安全工程师培训：《信息安全基础》、《常见操作系统安全》、《系统检查和加固》、《应急响应和入侵调查》、《网络安全设备》、《攻击目标信息采集与识别》、《入侵防护技术》。 | 3个月/次36人次 |
| 《信息安全事件和安全威胁》：通过大量典型的安全事件导入，反映当前安全形势的极端恶化，从感性认识层面对安全威胁给予直观、形象的描述，并形成一定的安全现象/知识冲击结果，分析、强调漠视信息安全的严重后果，以及安全威胁的发展趋势：速度更快、范围更广、影响更深刻。 | 3个月/次36人次 |
| 《日常安全和必备安全习惯》：通过实际案例和安全事件，表述信息安全对于个人生活、工作、学习无处不在的事实，同时阐明安全问题并非孤立、遥远的技术，在此基础上按照一般的安全技术的划分深入浅出地描述信息安全所包含的各个领域，以及这些领域和日常工作、生活的密切联系，对常见客户端应用工具/系统的安全问题进行分析，采用实证方式阐明OE、IE、Foxmail、MSN/QQ、P2P工具等的安全设置，对Windows操作系统存在的安全问题进行叙述和演示。同时，就日益猖獗的病毒、木马等威胁进行必要的描述，并阐明具体的防范措施，最终协助建立起适合个人、企业的用户行为基准。 | 1年/次40人次 |
| 《信息安全基础》：从ISO 7498-2模型出发，结合CBK领域、BS 7799领域划分，对信息安全中涉及到的标准、协议、技术手段、工具/产品、过程方法等，通过对安全领域和知识的清晰划分和描述，最终能够形成一张信息安全的知识结构图。 | 6个月/次36人次 |
| 《常见操作系统安全》：从Windows以及Unix的安全结构入手，对windows安全子系统中的重要组件如SAM、LSA、GINA等进行详细分析，分别阐明帐户安全、文件系统安全、注册表安全，对于Windows的常见应用（如IIS、Netbios、Terminal Server等）的安全性加以分析。针对Unix系统，则对帐号安全、文件系统安全、常见应用安全的讨论，强调Unix系统本身安全配置的同时，还将重点描述Unix主要应用服务（Mail、HTTP等）的安全问题。 | 6个月/次36人次 |
| 《系统检查和加固》：通过对系统安全加固的流程进行介绍，说明安全加固工作的主要工作任务。完全参照实际的工作过程，通过大量的现场模拟环境的加固实践，针对不同操作系统（Windows、Linux、HP UX、IBM AIX、BSD、Cisco IOS等）和相应应用系统（Web、Mail等）描述其检查流程、入侵调查、加固方案和相应的checklist。 | 6个月/次36人次 |
| 《应急响应和入侵调查》：从将结合应急响应演练，通过多个应急响应经典案例，对应急响应预案等核心步骤进行清晰的分析和描述，并且对在多个系统上对入侵痕迹的调查，易消失证据的获取进行详解介绍和演示。 | 3个月/次36人次 |
| 《攻击目标信息采集与识别》：在分析目标端网络数据采集方法的基础上，简明扼要地说明一些典型的工具应用，通过掌握目标端信息辨别的方法和原理，能够有效地进行Footprinting资料搜集、挖掘和准确的人工判断。 | 6个月/次36人次 |
| 《入侵防护技术》：介绍一般的黑客攻击途径，着重描述当前流行的攻击技术和防御手段，从踩点扫描着手，重点分析网络嗅探、病毒与木马攻击、拒绝服务攻击、SQL Injection原理、XSS跨站脚本攻击等，并阐明相应的防御措施，通过一次完整、完美的黑客攻击过程的实践展示，首先对黑客攻击的一般步骤进行分析，阐明黑客攻防的基本思路，并按照步骤顺序对其中涉及到的工具、平台、弱点、手法进行叙述，对黑客的惯常思维方式进行归纳总结。 | 6个月/次36人次 |
| 培训形式 | 培训采用集中内训的形式。建设方提供场地、投影仪、白板及其它必要的设施。建议每期学员不超过36人，课堂布置成便于交流与讨论的形式。 |
| 培训成果 | 安全培训PPT、培训教材等；同时内部培训通过在实际工作中抽查方式考核等。 |
| **运维****服务** | 通过对各建设平台、用户网络设备及安全设备的监控，实时掌握平台的安全状况，为用户信息化安全的信息安全提出意见或建议，保障平台的安全运行，同时协助用户进行信息化日常安全维护等工作。▲1.提供8名驻场运维服务人员，至少3人从项目实施团队中选取，能独立完成系统维修、维护工作；2.范围：web应用扫描报告，主机漏洞扫描报告等，按需提供服务；3.合同期限内不限次数；4.交付物：各扫描模块报告。 | 三年 |
| WEB应用弱点扫描报告 | 对Web应用进行深度弱点探测，可帮助应用开发者和管理者了解应用系统存在的脆弱性，为改善并提高应用系统安全性提供依据，帮助用户建立安全可靠的Web应用服务。 |
| 主机漏洞扫描报告 | 对Linux、windows等系统的扫描，通过检测主机上安装软件的版本信息，与CVE官方的漏洞库进行匹配，检测出存在漏洞的软件并发送详细漏洞信息。 |
| 协助安全加固 | 发现系统漏洞进行统一安全加固，确保系统的高安全性和高可用性。 |
| 风险评估 | 1.一年至少开展2次信息系统风险评估工作2.范围：安全技术、安全管理两大层面 |
| 设备安全巡检 | 1.一年进行12次安全巡检2.范围：网络设备、主机设备、安全设备 |
| 基线检查 | 1.一年进行12次基线检查2.范围：服务器、网络及安全设备 |
| 行业报告 | 全年提供不少于4次的行业安全态势分析报告。 |
| 主题报告 | 提供当月服务内容汇总（电子版/纸质版），汇总内容如下：1、日志分析情况；2、安全通报汇总；3、安全预警；4、安全态势分析。  |
| 敏感数据访问告警 | 非指定的用户从规定的IP地址访问访问敏感数据进行告警 |
| 特权账号告警 | 未按照安全策略操作的特权账号及人员进行告警和通报。 |
| 通报预警 | 数据安全监控、用户行为审计、大脑平台安全态势评估、终端安全监控、安全检查管理等模块发现的问题进行告警。 |
| 安全巡检 | 定期对客户信息系统中包括网络设备、主机设备、安全设备进行全面地安全巡检，如有异常情况，及时与项目接口人沟通，提供管理或行业安全合规咨询的建议。 |
| **应急****响应** | 1.提供远程和现场应急响应服务。2.范围：病毒木马事件、网络安全事件，按需提供服务。3.合同期限内不限次数。4.交付物：《安全事件应急响应报告》 | 三年 |
| 应急预案 | 1.协助完善应急预案编制和修订。2.范围：现有应急预案3.交付物：《网络安全应急预案》 |
| 应急演练 | 1. 根据应急预案，一年开展2次应急模拟演练工作2.范围：模拟网络和业务系统环境。3.交付物：《应急演练方案》、《应急演练总结报告》 |
| 定制开发 | 涉及平台定制开发，由中标方免费提供该项服务 |
| **售后****服务** | 售后服务 | 产品质保：软、硬件提供免费升级与维护服务▲服务响应：提供7\*24小时现场服务支持；工作时间0.5小时内现场应急响应，非工作时间1小时内现场应急响应。软件故障，2小时内解决问题；硬件故障，3小时内解决问题；未在规定时间内修复的，每次扣除1000元。售后培训：系统安装调试后对业主单位进行1天本地操作培训并提供培训材料（包括ppt，白皮书等）▲专业培训：提供8个CISP培训和考试名额。 | 三年 |

1. **项目实施管理要求**
	1. 实施管理要求

项目实施管理内容至少包括项目实施承诺、项目组织机构和人员安排、项目管理和实施质量保证、文档管理、项目实施阶段划分与进度安排、项目评审验收等内容。投标人必须证明自身有足够的能力实施，并且提出有效的实施方案。投标人必须承担本项目与相关项目的系统集成和组织协调等工作。

* 1. 项目组织要求

为使工程按质、按量、按时及有序实施，中标人对本项目须建立一个完善和稳定的管理组织机构。根据项目要求设置专业岗位，并组织人员，负责本项目的实施。

* 1. 项目文档要求

投标人在本项目软件开发实施过程中，技术文档应参考《GB/T8567-2006计算机软件文档编制规范》的要求提供相应的文档。中标方须根据开发进度及时提供相关文档资料，技术文件包括但不限于以下文件：

3.1项目实施方案

3.2详细设计方案

3.3数据库设计说明书

3.4系统安装部署手册

3.5系统操作手册

3.6培训服务方案

3.7软件评测报告

* 1. 关于软件

4.1招标文件的技术要求中列出了买方可以接受的最低的技术要求。投标人提供的所有软件必须在功能、性能等方面不低于采购人的要求。

4.2投标人所提供的软件必须是在中国有合法使用权。

4.3.投标人在投标方案中如果包含有采购的第三方软件，应单独报价，且系统交付时应将此软件移交给采购人。

* 1. 保密要求

投标人须提供对本项目的保密承诺，保证对项目技术文件以及由采购人提供的所有数据、内部资料、技术文档和信息予以保密。未经采购人书面许可，投标人不得将采购人提供的本项目数据、资料以及项目成果以任何形式向第三方透露或使用。本条款在项目完成或无论何种原因导致合同终止后依然有效。

* 1. 知识产权约定

6.1投标人保证准备或提交的全部软件系统和设计文件在中国境内或境外没有且不会侵犯任何其他人的知识产权（包括但不限于版权、商标权、专利权）或专有技术或商业秘密。

6.2本项目所开发的软件系统其知识产权归采购人所有。

* 1. 培训要求

中标人须向系统各类用户免费提供操作及维护工作的相关培训。要求结合实际情况，针对技术人员及业务人员制定培训计划。依据培训人员人数，确定培训时间、地点、内容等，采用相应的培训方式对使用的不同人群进行培训。投标人需解决培训的培训师资、教材、课件等，采购人提供场地。

* 1. 验收要求

8.1在项目合同签订后，开发方须按照合同及经双方确认的需求报告，完成标准规范编制、数据整合建仓、衢州市平台部署及相关文档整理工作，

8.2采购人组织项目初验，初验通过后正式进入试运行阶段。

8.3针对验收中存在的问题，开发方进行系统完善；

8.4采购人邀请相关部门组织终验。

8.5终验通过后本项目进入维保阶段。

8.6（参照《浙江省公安厅科技建设项目验收操作指南（2020-08-17）》执行）

* 1. 售后服务

提供自项目最终验收完成之日起3年的免费维保服务，售后服务期内安排8名技术人员驻场（至少3人从项目实施团队中选取，能独立完成系统维修、维护的技术工作人员）。系统服务内容包括故障排除、版本维护、故障修复、补丁和主要版本升级。数据部分提供入库数据更正服务。

提供7\*24小时现场服务支持；工作时间0.5小时内现场应急响应，非工作时间1小时内现场应急响应。软件故障，2小时内解决问题；硬件故障，3小时内解决问题；未在规定时间内修复的，每次扣除1000元。

* 1. 付款方式
		1. 中标人通过电汇、转账或银行出具履约保函向采购人交纳合同总价5%的履约保证金。
		2. 签定合同后，采购人在十个工作日内按合同总价的 30 %支付首付款。
		3. 系统初验合格后，十个工作日内按合同总价的 30%付款。
		4. 系统终验通过后，十个工作日内按合同总价的 40% 付款并退还履约保证金。采购人需在中标人提交完整竣工验收资料符合验收条件的三十日内，组织相关单位进行项目终验。
	2. 其他要求：中标人负责免费提供项目实施中需要而采购清单中未列出的软、硬件、人工以及与其它平台、系统对接所需要的一切资源。