# 一、项目概况

项目属性：货物类

品目分类：其他计算机设备及软件（A020199）

本项目对应的中小微企业划分标准所属行业为：软件和信息技术服务业。

★本次采购产品为非进口产品（进口产品指通过中国海关报关验放进入中国境内且产自关境外的产品）。

本项目属于不专门面向中小微企业预留采购份额的项目，原因和情形为：照《政府采购促进中小企业发展管理办法》规定预留采购份额无法确保充分供应、充分竞争，或者存在可能影响政府采购目标实现的情形。

本项目核心产品为态势感知与预警通报、网络安全流量探针、日志采集器（多家投标人提供的核心产品中任意一个产品品牌相同的，按一家投标人计算）。投标人必须在投标文件中填写所投核心产品的品牌，否则按无效投标处理。

★凡属于《中华人民共和国实施强制性产品认证的产品目录》的产品，请投标人在投标文件中承诺在交货时提供该产品的“中国强制性产品认证”（CCC 认证）证书。

根据《广播电视网络安全管理办法》《广播电视网络安全事件应急预案》等相关规定，广州市广播电视监测中心应开展网络安全监测监管和信息通报预警、监督检查相关运营单位网络安全保障情况等工作，现需采购一套网络安全监测的系统，包括系统的供应、运输、安装调试、培训及售后服务。具体采购范围及所应达到的具体要求，以本采购文件中商务、技术和服务的相应规定为准。

预算金额：775 万元。

最高限价：775 万元。

## 1.1 项目依据

《广州市广播电视监测中心新址监测系统迁建项目方案》（2021 年）；

《全国广播电视与视听新媒体监测监管总体发展规划（2019 年－2025 年）》（2018 年国家广电总局）；

《中华人民共和国网络安全法》（中华人民共和国主席令第 53 号〔2016〕）；

《互联网视听节目服务管理规定》（国家广电总局令第 56 号〔2015 修订〕）；

《广播电视网络安全管理办法》（2020）；

《广播电视安全播出管理规定》（国家广播电视总局令第 62 号〔2009〕）；

《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019；

《信息安全技术 网络安全等级保护安全设计技术要求》GB/T 25070-2019；

《信息安全技术 网络安全等级保护定级指南》GB/T 22240-2020；

《信息安全技术 信息系统密码应用基本要求》GB/T 39786-2021；

GY/T 337—2020《广播电视网络安全等级保护定级指南》；

GA/T 1389-2017《信息安全技术网络安全等级保护定级指南》。

## 1.2 系统监测的范围

网络安全监测系统主要对 6 个主要播出机构（市广播电视台、4 家区电视台和白云电视中心）的办公网系统以及对外发布网站、新媒体发布平台等互联网业务系统；中国广电广州网络股份有限公司的办公网系统以及互联网业务系统进行安全监测。

## 1.3 系统的功能

实现对辖区内 6 个主要播出机构（市广播电视台、4 家区电视台和白云电视中心）以及中国广电广州网络股份有限公司关键信息基础设施及相关网络的安全监测，评估各单位安全状态，为市局提供态势感知数据支撑，对威胁行业安全的事件进行汇总、分析、研判，及时报告上级部门并对相关责任单位进行通报预警；与上级行业相关系统以及同级网信、公安等部门有关系统对接或通过离线导入的方式，实现安全数据与安全情报共享、安全通报。系统具备多源数据采集的功能，包括内部系统日志数据、流量数据、漏洞数据，资产数据，还包括外部威胁情报数据；具备大数据安全分析能力，对采集到的数据通过大数据技术进行加工、处理、存储，形成有效的数据源，支撑后续的数据分析和数据安全建模；具备能够通过事件监控、态势感知（包括攻击态势、资产、漏洞、安全威胁、风险可视化）统计分析实现安全态势多维度可视化功能；具备对辖区内被监管单位定期渗透测试的功能。

针对安全事件形成安全事件分析报告并跟踪整改情况；具备配合上级广播电视技术监管中心进行较大安全事件的分析调查工作。

# 二、项目需求

## 2.1 网络安全检测数据处理、存储空间、带宽需求

每天处理的日志数据约为 8 亿条，流量数据约为 10TB，在大数据处理架构下，数据采集需要 2 台 32 核 CPU，256GB 内存的处理设备；数据存储需要 6 台 32 核 CPU，256GB 内存的处理设备；关联分析与指挥调度展示需要 2 台 32 核 CPU，256GB 内存的处理设备。

在满足网络安全等级保护基本要求对在线日志存储满足 180 天且有备份的前提下，需要存储空间不少于 509TB。

番禺区电视台需要回传市监测中心带宽 40M 左右；3 家区电视台和白云电视中心各需要回传市监测中心带宽 10M 左右；广州市广播电视台需要回传市监测中心出口带宽约 50Mbps 左右；中国广电广州网络股份有限公司需要回传市监测中心出口带宽约 100Mbps 左右；上述带宽由广州市广播电视监测中心负责提供。

## 2.2 安全需求

系统要达到网络安全等级保护二级的要求，充分利用现有的网络安全防护设备对监测系统进行防护，在项目建设完成后，实施单位应配合建设方完成系统的定级测评（首评及第一次复评），并负责完成后续的整改工作。

网络安全监测相关工作和数据涉及工作秘密，中标方需与采购方签订保密协议。

## 2.3 系统验收标准

具备对 6 个主要播出机构（市广播电视台、4 家区电视台和白云电视中心）的办公网系统以及对外发布网站、新媒体发布平台等互联网业务系统以及中国广电广州网络股份有限公司的办公网系统以及互联网业务系统进行安全监测的能力（包括技术方案中的能力）。

系统具备对相关责任单位进行通报预警的能力。

系统具备数据的存储能力，存储容量≥600T。

每秒处理日志数量不低于 50000 条。

能够将高于 30Gbps 的流量按需清洗并可按 1-10Gbps 动态进行数据分流。

半年内数据查询响应时间不超过 5 秒。

支持业内通用标准数据获取方式，获取方式不少于 10 种，包括 Syslog、SFTP、文件、Kafka、HDFS、主机终端(win/linux)Agent、DB2、Mysql、Oracle、Sqlserver、Postgrel、SNMP、Netflow 等。

支持内置 180 余种的数据源类型，默认可接入各类硬件设备和应用系统，包含但不限于主机、防火墙、IPS/IDS、WAF、网络设备、安全设备、数据库、应用系统、中间件、存储。设备、虚拟化设备、机房设备等多种设备和系统的日志接入方式。

支持不少于 60 种，700 条规则的安全检测分析，包括：扫描探测类、主机异常类、异常通信类、运维监控告警类、中间人攻击类、Web 攻击类、账号异常类、拒绝服务类、邮件攻击类等。

内置不低于 15 种聚合事件威胁场景。

## 2.4 系统部署需求

在市台、中国广电广州网络股份有限公司、区电视台、区电视中心网络进出口附近的核心交换镜像接口部署流量探针和日志采集器，对安全数据进行采集并回传中心（部署方式由厂家根据被监管单位要求进行深化设计），互联网视听监测系统部署在现网的业务服务区，网络安全监测系统部署在现网的安全管理区，相关业务系统设备布置监测中心设备机房、监控大厅等位置，机房所有设备均由 UPS 供电，需可靠接地，接地电阻不大于 1 欧姆。

依据需求租用通信链路（由广州市广播电视监测中心负责提供）。

## 2.5 驻场服务、培训服务及质保期要求

提供 3 年的驻场服务（驻场 1 人，驻场服务是通过驻场人员对安全监测中各种问题提供专业的服务，包含实时安全事件监控、定期安全事件分析、定期安全评估等，形成《安全事件分析报告》、《安全评估报告》、《安全通告周报》等专项报告，同时在系统建设完成后 3 年内配合中心每季度完成一次对被监管单位的漏洞扫描和渗透测试，并配合中心每年完成一次攻防演练。日常驻场时间满足 5 天×8 小时的要求，按上级管理部门确定的重要保障期和法定节假日（春节、元旦、清明节、端午节、劳动节、中秋节、国庆节）期间驻场时间满足全天 24 小时值班值守要求。

提供网络安全监测系统操作培训，及安全态势感知平台现场技术培训（包括但不限于安全态势感知平台内容培训等网络安全培训）。

完成在质保期 3 年内每个季度一次的渗透测试和漏洞扫描服务，并配合中心每年完成一次攻防演练；每年至少完成 30 份《安全通告简报》，15 份《安全事件分析报告》和《安全评估报告》；实现匹配安全事件发现率不低于 70%，安全告警事件收敛 50%以上，未来三年在病毒特征库、情报库、知识库持续更新的情况下，逐步实现匹配安全事件发现率不低于 90%，安全告警事件收敛至 30%以上。

质量保证期（简称“质保期”）为 3 年，从项目完成验收之日起计算。质保服务包含但不限于硬件更换、软件升级、情报更新、特征库升级、问题处理服务、巡检服务、保障服务、重大故障恢复等内容。质保期内对所供货物实行包修、包换、包退及合同约定的其它事项，期满后可同时提供终身(免费/有偿)维修保养服务。质保期内，如设备或零部件因质量原因出现故障而造成短期停用时，则质保期和免费维修期相应顺延。如停用时间累计超过 60 天则质保期重新计算。质保期内，对采购人的服务通知，投标方在接报后 1 小时内响应，4 小时内到达现场，48 小时内处理完毕。若在 48 小时内仍未能有效解决，投标方须免费提供同档次的设备予采购人临时使用。

## 2.6 定制开发需求

提供产品功能定制开发满足用户需求，包括但不限于 7 个大屏展示定制内容：

1、威胁攻击态势：基于全局态势展示目的，提供威胁攻击态势大屏，包含但不限于基于地图的攻击源、目的 TOP10 的 IP 属地动态展示等可视化的功能。默认 3D 地球形式动态地展示，同时支持 2D 地图的形式的切换。

2、资产安全态势：基于全局了解资产的风险情况与变化趋势的目的，展示内容包括资产拓扑图、资产域的总体风险，以及资产待处理的安全事件等信息的可视化展示功能。

3、安全事件态势：基于掌控安全事件处置情况的目的，包括不同安全级别所发生的安全事件数量统计，安全事件的增长趋势，分布情况、安全事件处置等情况可视化展示功能。

4、安全监管态势：安全监管态势主要用于安全监管部门，可以通过被监管单位的网络安全数据采集分析，直观有效了解当前被监管单位网络安全事件的发展趋势以及危害程度。显示的内容由日志事件、安全设备告警、关联告警及安全事件组成。

5、威胁情报态势：为了解威胁情报为当前网络威胁检测带来的成效，展示的内容包括：命中情报种类分布及次数、威胁类型统计、威胁情报摘要、命中情报 Top10、情报告警趋势、命中情报家族/团伙统计。

6、系统运行态势：系统运行态势用于展示系统整体运行状态，包括各数据接入实时状态、平台模块运行实时状态、数据存储状态、数据采集速度、告警生成速度、事件入库速度等信息。

7、综合展示：用于组合上述态势中重点数据，除可视化大屏中默认的展示元素外，还可以基于实际工作需求对大屏展示元素进行拖拽替换，定制业主当前所关注要素自由排列组合的大屏。

投标方应通过成套软件以及定制开发的方式来完全满足采购方提出的关于网络安全监测系统的所有功能要求以及对应的实施效果要求，定制开发与上级行业相关系统以及同级网信、公安等部门有关系统对接接口，过程产生的费用由投标方负责，并持续改进直到验收通过。

## 三、技术需求

投标人应遵守国家法律法规：网络安全统一监测平台建设遵循国家法律法规以及国家等级保护标准规范。

投标人应遵守统一开发接口规范：统一监测平台建设完成后需要形成标准开发接口规范，为第三方平台提供数据共享和调用，同时为现有各个办公区已有的安全监测手段提供接入条件。

技术先进性：平台利用大数据分析、机器学习、多维关联分析等新技术，能够满足当前和未来监测中心海量数据的采集、处理、分析和展示。

具有可扩展性：为了满足监测中心业务的不断发展及接入需求，监测中心统一监测平台采用模块化、分布式设计，安全策略集中管理，横向弹性扩展，平滑性升级，保护原有投资。

“态势感知与预警通报”应具备数据接入能力：数据采集-采集管理-支持采集规则可以进行灵活操作，对于需要留存的解析规则可以进行启动、停止来临时生效而不用删除，以便下次使用。

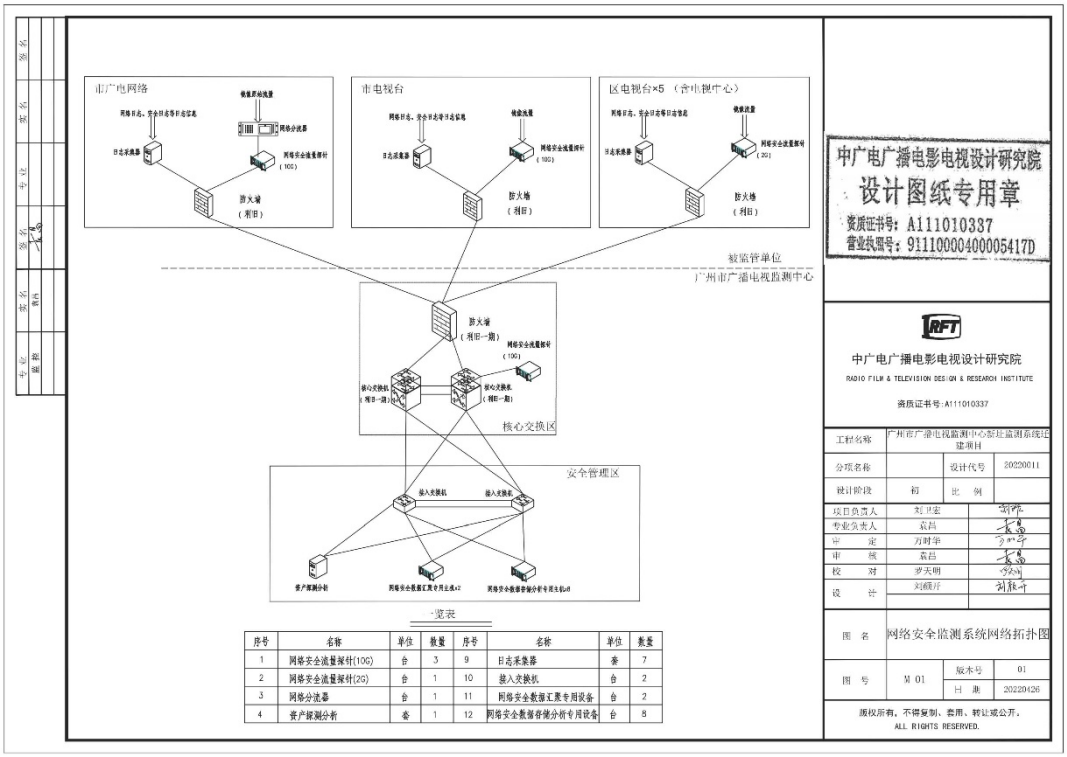
“态势感知与预警通报”应具备安全分析能力：关联分析-检索分析-支持同比分析算子，根据历史的同周期数据进行对比并判定偏差度来发现异常线索。支持通过同比昨天、上周、上个月及自定义周期的方式来计算，支持根据统计变化率（如同比增长 10%，增长 20%-40%等）或变化的绝对值（如登录次数同比增长 5 次）来进行同比分析。

“网络分流器”应具备汇聚分流能力：对采集的原始流量中的业务低价值数据进行过滤。按照项目需求提供数据采集方案及汇聚分流逻辑架构图。

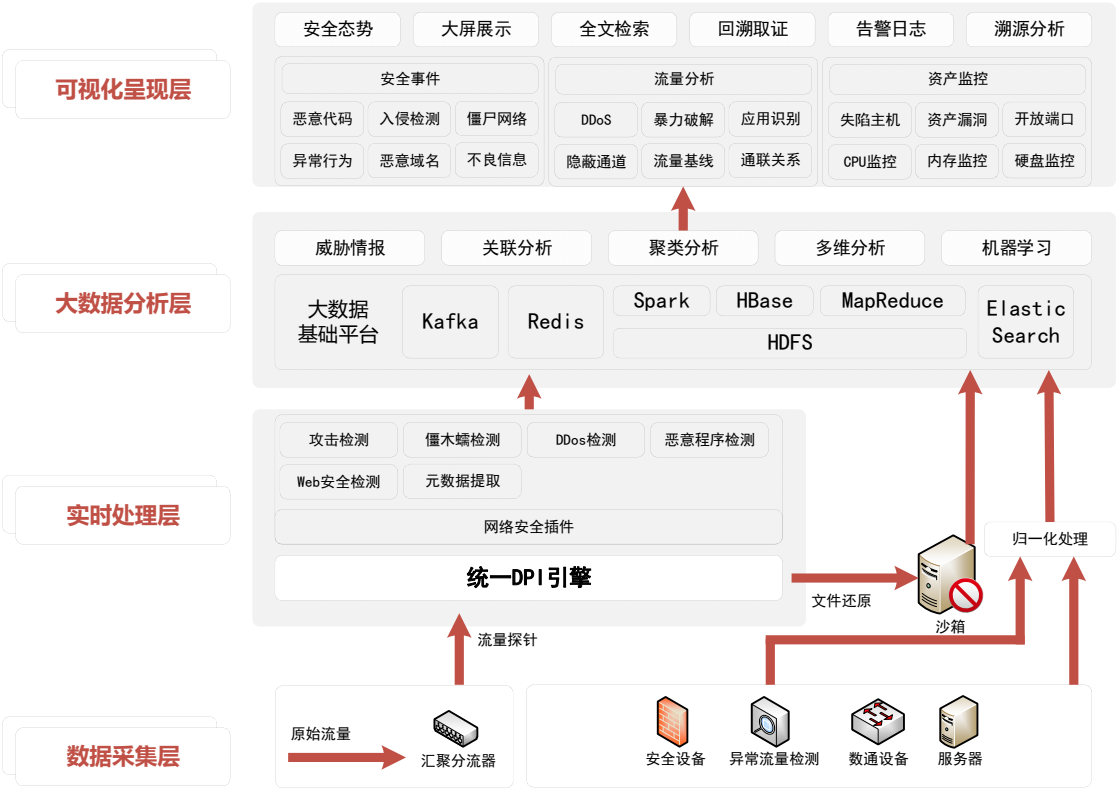
系统概述：

系统以统一的基础平台为依托，实现对辖区内播出机构网络安全的监测，为监测中心业务人员提供数据采集、数据存储、数据分析处理、数据可视化等服务。

系统拓扑图如下：

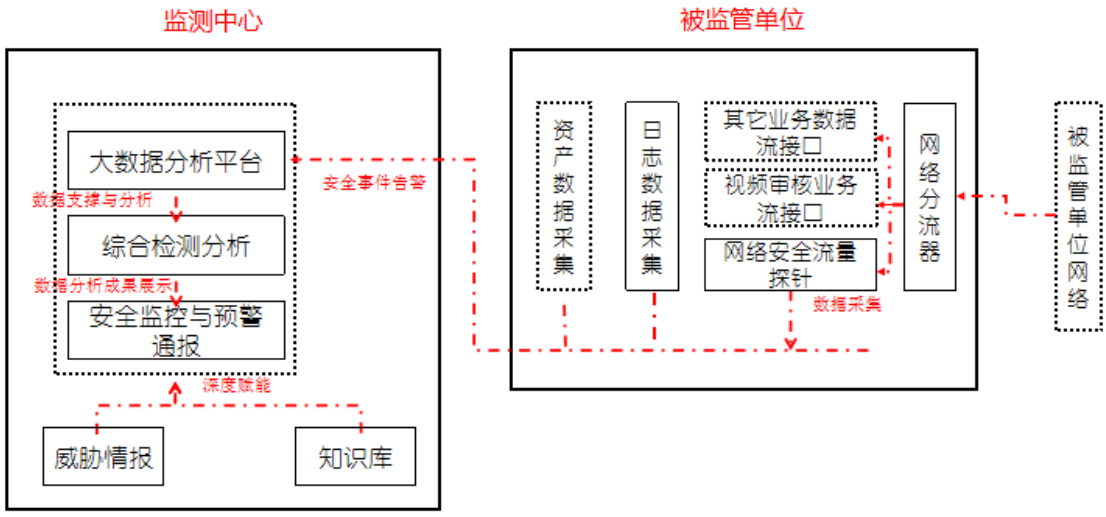



系统的整体架构图如下图所示：



整体架构图

通过在 7 个单位（广州市广播广播电视台、4 个区电视台、1 个电视中心、中国广电广州网络股份有限公司）部署网络安全数据采集设备采集日志数据、流量数据回传到监测中心平台，对网络安全监测数据集中分析，实时掌握被监管单位相关网络和信息系统的网络安全情况，以及收集最新网络安全风险、威胁情报，并可以将相关监测报警信息下发到被监测单位。逻辑架构图如下图所示：




逻辑架构图

3.1.2　网络安全监测数据采集

通过网络安全流量探针、日志采集设备及在线信息资产安全数据采集，对流量数据、安全日志数据、资产数据进行集中收集，并将其转发至市监测中心平台（利用被监管单位防火墙做边界防护）。

其中日志数据包括网络日志、安全日志、主机日志、应用日志、数据库日志等信息，流量数据主要为流量探针采集的网络流量日志数据和威胁检测数据，同时考虑到系统的扩展性，也支持各类第三方数据采集，如漏洞扫描数据、终端安全数据等。

3.1.2.1.　日志数据采集

日志数据采集可对现有安全设备、主机设备、网络设备和应用系统的日志进行自动解析、过滤、富化、内容转译、范式化；支持 Syslog、WMI、SFTP、SNMP、Netflow、API 接口、文件等多种采集方式。

数据采集可采集以下信息：

1）　网络日志：流量会话、应用行为、文件传输、账号登录等；

2）　安全日志：网络设备、主机、数据库、安全设备、中间件、虚拟化、应用系统、网关系统等；

3）　终端日志：文件行为、进程行为、邮件行为、注册表等；

4） 系统日志：系统登录、系统操作、业务查询、应用信息等。

3.1.2.2. 流量数据采集与分析处理

流量数据采集可实现对网络流量进行深度协议采集、协议识别、重组还原，提取网络层、传输层和应用层的头部信息，包括重要负载信息、样本信息等。采用的流量探针可以在IPv4/IPv6 网络环境下，支持 HTTP 、邮件、数据库等主流协议的深度解析，支持主流协议的文件还原，包括文档类文件、可执行文件、压缩文件等，同时支持全流量存储能力。

在流程采集的同时具备对流量进行检测的能力，支持从多个维度综合识别评估网络威胁：

1） 网络攻击检测

流量探针内置威胁检测引擎可检测多种网络协议中的攻击行为，提供攻击检测、攻击成功检测等多种维度的威胁监测，可精准识别如 sql 注入、跨站命令执行、文件包含等多种 web 攻击，也可检测木马、勒索软件、僵尸网络、常规渗透入侵、内网横向渗透等各类黑客攻击和恶意流量，实现精准告警。

2） 恶意文件检测

具备文件威胁分析能力，可对网络中传输的文件样本进行高级威胁检测。将还原的 PE 或非 PE 类型的文件样本提交给虚拟沙箱进行检测，样本经过虚拟沙箱的威胁情报、静态检测、动态检测等多种检测引擎后，能够及时发现有恶意行为的文件并进行告警，同时会将样本的检测结果以及详细的行为分析报告发送到中心平台进行统一管理和分析。

3） 行为异常检测

基于攻击行为、数据分析技术构建的异常行为分析引擎，提取攻击行为特征，分析异常流量数据，发现异常行为，产生告警。异常行为分析引擎支持暴力破解、特权账号登录、弱口令登录、明文密码泄漏、用户名枚举、域渗透、钓鱼邮件等异常行为检测。

4） 高级威胁检测

具备对潜在威胁、异常行为等进行狩猎分析，发现高级威胁活动。可对 APT 攻击、新型木马、特种免杀木马进行规则化描述。通过流量的精细分析，确认攻击手段、攻击对象以及攻击的目的，通过人工智能结合大数据知识以及攻击者的多个维度特征还原出攻击者的全貌，持续的发现未知威胁，最终确保发现的未知威胁的准确性。

5） 资产发现

对于资产信息，通过手工填报及批量导入的方式录入，同时根据上报各业务子系统 IP 地址段，利用流量识别技术对被动发现的陌生 IP 地址及该 IP 地址所携带的系统版本、设备类型等信息进行分析生成资产标签。

3.1.2.3. 威胁情报采集

具有同步国内高质量、高时效、高精度的威胁情报数据的能力。情报数据主要来自于中央网信办、公安部网络空间安全技术研发基地、互联网安全应急中心、第三方安全公司等机构。威胁情报类型涵盖 APT 情报、失陷检测情报、IP 信誉情报、TTP 情报等。

3.1.3 监测中心平台

包括大数据平台，综合检测分析、安全监控与预警通报。

3.1.3.1. 大数据平台

面对海量日志数据和流量数据，大数据计算处理是安全数据分析处置的基础。大数据平台采用先进的大数据处理技术，提供安全全量数据的集中采集、处理、存储、查询、分析等功能。

1) 多样化异构数据采集

数据采集模块支持第三方安全设备或系统的日志、告警、事件等多各类海量异构数据的实时采集，为平台分析提供多样化的高价值数据。支持业内通用标准数据获取方式，包括Syslog、FTP、文件、JDBC、ODBC、Kafka、API 接口等方式。

利用大数据技术，数据采集方式可进行支持水平扩展，并支持分布式数据采集。数据采集支持丰富的数据源类型，支持各类硬件设备和软件系统，包含但不限于主机、防火墙、IPS、IDS、WAF、网络设备、数据库、应用系统、中间件、存储设备、机房设备等。

2) 数据解析与标准化

数据解析与标准化模块可将采集的多种安全设备或系统的原始信息格式转化为大数据中心模块可处理标准化格式。数据解析预置近千条范式化解析规则，支持国内外千余种常见设备和系统日志的自动解析和标准化。日志解析支持多种匹配方式，日志标准化支持分隔符、CEF、XML、JSON、脚本等解析方式，提供索引浏览方式并支持条件查询，并支持可视化的配置界面。

日志解析规则支持规则嵌套和逻辑组合方式，能够对一组事件进行多层规则解析处理，添加、删除、重命名、合并与裁剪现有字段，对标准化后字段再解析处理，范式匹配支持精准匹配、正则匹配后从数据头或尾进行二次解析处理方式。

3) 多种类数据丰富化

数据丰富化模块对解析标准化后的数据进行信息的丰富化，提供更为全面的安全日志进行分析。数据的丰富化来源包括多类信息，如数据来源、资产信息、数据种类、地理位置信息、组织人员信息、监测时间等。

4) 海量数据存储

数据存储采用可灵活扩展的 Elastic Search 大数据分布式存储，支持灵活横向扩展、多集群部署，可存储 PB 级数据，具有如下特性：

支持数据快速检索；

支持原始日志、范式化日志事件、告警等数据全量集群存储与备份；

支持提供 API 接口给第三方调用存储数据。

数据存储可基于不同的数据源，单独配置数据存储策略，提高数据存储使用效率，并提供数据存储冷、热分区功能，可实现 TB 级数据秒级访问，满足对数据查询性能和存储容量的需求。

5) 全方位数据检索与分析

数据检索与分析模块提供多种数据检索方式与分析能力对安全日志进行全方位的检测和分析，在不同场景下快速准确的获取分析结果。

流式分析引擎可对采集到的安全日志数据进行实时规则分析，支持多数据源事件行为序列相关分析，支持基于事件的多属性相关分析，支持多级 and、or、not 等逻辑操作符，属性字段支持 IP、字符串、数字、时间等多种类型，属性字段操作支持网段包含、字符串匹配、情报匹配、正则表达式匹配等多种匹配方式。

检索分析引擎基于检索语言生成检索分析模型，可对长周期安全日志数据进行复杂运算，包括去重、求和、平均值、最大、最小值、方差、标准差等，同时支持同比统计变化率的计算。

3.1.3.2. 综合检测分析

综合检测分析利用各类特色检测分析引擎，可以从多维度对威胁攻击进行全方位的检测和分析。

1) 情报检测分析

依托海量的恶意样本、安全日志、域名信息等情报大数据，提取出多维度（如：Hash、Domain、IP）高可信威胁情报 IOC，提供给各分析引擎使用。

利用高可信威胁情报关联安全日志和流量，可实时检测出恶意攻击，并根据情报的威胁分值设定相应的威胁等级。在溯源分析过程中，情报云还可提供情报的丰富化信息，包括攻击画像、恶意团伙、相关事件等多维度信息，支撑安全人员进行分析和研判。

威胁情报数据覆盖全球当前流行的勒索软件、ExploitKit 以及 APT 攻击事件、攻击团伙等，包括但不限于：

累计收集的百亿级别的 PE 样本；

交换获得的数十家安全厂商的木马、蠕虫、远控工具样本；

国内领先的的 APT 发现能力和相关数据积累；

全球安全组织的开源共享情报 OSINT；

安全厂商、组织发布的安全报告或 Blog；

互联网主机扫描数据；

基于 pDNS、Whois 等基础数据关联和监控。

原始安全数据经过威胁情报中心分析加工后形成如下几种情报分类：

失陷检测情报

有关攻击者的远程命令与控制服务器情报，用以发现内部被 APT 组织、僵尸网络、木马软件、后门工具等控制的失陷主机。失陷检测情报聚合业界数十家领先安全厂商的恶意软件检测分析结果。

文件信誉

样本信誉库用于识别恶意软件。以文件的 HASH 为索引，包括是否是白文件、是否恶意、恶意类型、家族信息等信息，针对已知木马、蠕虫类恶意软件，提供期对应的网络 IOC 信息。

IP 情报

针对来自互联网攻击 IP 地址的情报信息，包括：是否有历史攻击行为、是否是 IDC 主机、是否是傀儡主机、是否是代理或 Tor 网主机、是否可能是扫描机器人等，用以过滤出优先级较高（或较低）的攻击事件，或了解攻击者的背景信息。

TTP 情报

有关攻击者工具、技术、技战术手法的情报，具体包括和客户相关的攻击事件、恶意样本、软件漏洞等分析报告和预警通告，内容一般包括事件危害、影响范围、攻击机制、防范或检查机制能力。可以帮助组织提前预防攻击，并且有针对性的增强安全架构。

TTP 情报基于跟踪全球不同政府机构和安全厂商发现的重要事件、漏洞、恶意软件，同时包括威胁情报中心和其它安全研究团队的跟踪、挖掘成果，提供最新的、全面的安全漏洞、行业相关威胁事件及攻击软件、攻击相关态势数据等内容，帮助组织有针对性的防御面对的真实攻击者，预防重大攻击事件的发生。

2) 样本查杀检测

收集并研究各种恶意代码，如僵尸程序、木马、蠕虫、挂马网站、页面恶意脚本、Rootkit、漏洞等，按照需求对样本进行整理，并提供样本和样本分析报告。对于特定的典型恶意代码，能够进行详细逆向分析，了解恶意代码程序流程；对于当前主流的恶意代码，能够进行快速分析，以恶意代码家族或典型变种进行分类，找出其具有规则性，可匹配性的网络监测特征，以进行监测、追踪。

集成强大的样本查杀技术，拥有多种特征识别、启发式、智能识别及云查杀引擎，可对各种新兴恶意样本进行有效检测和查杀。

终端文件落地检测，EDR 支持对通过网络、邮件、移动存储介质等落地终端的文件立即进行样本检测，实现样本执行前的检测。

网络文件还原检测，NDR 支持对网络传输的常见的可执行文件、文档文件、压缩文件进行还原，并联动样本检测模块，实现网络中样本的检测。

针对 PE 文件，采用广谱反病毒引擎查杀。引擎拥有超百亿病毒木马样本特征库，支持通过安全大数据掌握流向趋势，高效查杀流行病毒，支持对感染性病毒样本进行修复。

针对非 PE 类宏病毒、VBS、REG 等恶意文件，脚本查杀引擎进行检测。支持数百种非 PE 格式识别、查杀，支持脚本虚拟执行查杀；支持机器查杀算法、支持文档修复。

3) 关联分析

XDR 关联分析支持深度关联 EDR、NDR 打点数据、告警，关联维度包括但不限于终端 IP、DNS 请求、TCP、UDP 会话信息和文件样本。

XDR 场景化关联分析，内置 XDR 场景关联分析规则，覆盖违规行为、恶意程序、网络攻击、数据泄露、拒绝服务、运维监控、漏洞利用、网站安全、主机安全、暴力破解、探测扫描等十多大类场景。

多维数据关联分析包括基于 IP 地址的关联分析、基于时间维度的关联分析、基于用户行为的关联分析等内容。

基于 IP 的关联分析

通过原始报文流的当前会话和历史元数据信息，以及各子系统上报的告警信息，可以关联出可疑攻击 IP 地址的整个活动行为，比如邮件发送，FTP 下载，端口扫描，木马注入等行为动作。从而对分析判断攻击事件的行为模式做出分析判断。

基于时间维度的关联分析

不同的子系统数据都具有时间属性，通过对某一时间点或是一个时间周期范围为分析点，可以把各子系统的相关数据进行关联，从而对安全事件在某一时间段所表现出来的行为特征能精确分析判断，比如在某一时间段内出现大量文件下载，并存在关键业务系统出现大量数据外泄告警。

基于用户行为的关联分析

安全事件不光可能会来自外部的网络攻击所造成，还有很大部分是来自内部人员的非法访问。通过以用户为主体，可以关联用户在一段时间范围内的所有行为特征，并通过与正常用户行为模式的比较，从而分析判断内部用户是否存在违规行为。

基于安全漏洞的关联分析

安全事件的出现往往是由于网络攻击找到了系统的某个漏洞或薄弱环节，内部网络整体环境都可能存在类似的问题，因此以漏洞为维度进行关联分析，可以从宏观上对攻击行为所表现出来的特征来进行分析，比如某一特定通信协议的流量激增等。

基于特定文件的关联分析

以安全事件所产生的特定文件为主体进行关联分析，可以倒推溯源分析其所产生的一系列行为模式，比如端口扫描，漏洞渗透，特马注入，文件下载，最后出现安全事件告警。也就是说从安全事件所产生的结果为起点来逆向关联分析出其所具备的一些通用的行为属性特征。

4) ATT&CK 检测

利用 ATT&CK 知识库可检测识别威胁攻击各阶段中的攻击技术，并可以 ATT&CK 图谱的方式展示出来。

将 EDR、NDR 等安全产品检测能力和安全分析映射到 ATT&CK 检测框架中，根据其检测结果覆盖度，可以发现哪些检测点未覆盖到，发现不足，然后进行主动完善。

可以试举 ATT&CK 框架实现关联分析，结合安全事件的命中情况，从 ATT&CK 矩阵可刻画出攻击者所采用攻击技术之间的关系，清晰的展现攻击者的入侵过程，通过不断地攻击溯源分析，抓取攻击向量，形成精确的检测规则。

5) AI 检测

支持对未知病毒、恶意样本进行动态分析，并根据机器学习模型查杀，识别恶意代码族系。支持查杀引擎自学习、自进化，无需频繁升级特征库。

AI Web 攻击检测，通过无监督异常识别和有监督攻击识别结合的方式，识别 SQLInjection、XSS、DGA 等攻击手段，能够学习、自适应客户的业务环境。通过自学习从而过滤客户环境中大部分的正常流量，只把异常流量送入检测模型，通过多模型融合的方法

降低误报，并提高检测效果。混合算法多模型，支持机器学习和深度学习双算法模型（包括但不限于：HMM、XGBOOST、CNN、LSTM）进行 Web 威胁检测。

6) 终端行为分析

终端行为分析的目标是构建多层次的终端威胁检测体系，主要包括：

终端 EDR 初步检测：

依托终端 EDR 神经元进行轻量级的威胁鉴定，快速判断已知恶意代码；

如果终端 EDR 检测均被绕过，二次检测技术可保证绕过初步检测技术后的未知威胁行为依然可被发现。

平台二次检测

终端行为数据采集：以埋点和打点的方式采集终端用户行为数据，发送到大数据平台进行存储和分析，为终端行为分析分析提供数据基础；

威胁情报应用：基于威胁情报相关的样本 HASH、特征、IOC、以及相关指标等信息做为检索条件，对终端行为数据进行主动、实时快速的分析；

异常行为分析：结合终端行为历史画像和威胁情报，进行终端异常行为分析，实现对绕过一次检测技术的未知威胁行为的二次检测，识别终端异常行为，对威胁进行定级和预警。

终端行为分析能够对多种终端异常行为进行识别和分析，比如异常域名请求、非法 IP 访问、敏感命令执行、恶意启动项创建、高危 API 调用等。同时支持同步分析、异步分析，做到对简单威胁的实时发现和对复杂威胁的有效检测。

终端行为分析通过恶意文档分析、恶意脚本分析、合法工具恶意利用分析、内存恶意代码扫描等多种技术，可检测无文件攻击行为。

7) 网络行为分析

网络行为分析基于网络流量，整合和优化用户行为数据，监控业务访问的整体情况，同时基于大数据分析平台和高级分析算法，有效发现内部人员的恶意或异常的行为，进行风险预警，及时发现问题。

网络行为分析通过整合网络、主机和应用、用户等各方面的数据，具备以下能力：

整合

终端数据、AD 数据、网络设备数据，支持 SYSLOG、JSON、CSV 等多种格式数据存储水平扩展、支持快速查找。

关联

基于人员、账号、组织结构等信息的关联，对缺少上下文的事件完善补充（用户数据、地理位置数据等）。

分析

用户行为数据的分析、基线数据的异常分析，对关键资产、用户属性等方面机器学习。

检测

通过风险值量化内部威胁；通过风险事件类型统计、时间分布预知内部威胁，人员调查取证时，提供基于时间、时间、人员等多维度的证据。

网络行为分析可检测各种主流常见网络异常，包括但不限于网络扫描、漏洞利用、代码执行、后门连接、WebShell、Web 攻击、蠕虫、木马、间谍软件、登录成功、暴力破解、拒绝服务、P2P 流量、入侵检测、远程桌面连接、SQL 注入、违规访问、文件还原、可疑 UA、黑客工具、手机间谍软件、DNS 请求异常、FTP 攻击、SMB 攻击、Telnet 攻击、TFTP 攻击、SNMP 攻击、SQL 攻击、POP3 攻击、IMAP 攻击、Tor 节点流量、僵尸网络流量等。

网络行为分析可基于攻击链对多阶段攻击场景进行有效检测。可进行流量动态基线异常分析，并支持“有监督学习+无监督学习”的 Web 异常 AI 检测。

8) APT 检测

检测能力同时覆盖网络流量和终端行为

单纯从网络流量或者终端行为中看到的信息并不全面，比如从网络流量中可以识别样本外联行为，如果恶意样本通过 U 盘等途径进入终端并且处于潜伏期时，是无法从网络流量中识别出来的。

安全大数据分析能力发现威胁

未知威胁的发现，应当有历史全量数据的支撑，才能为威胁关联分析和事件取证提供充分的依据。

对应用负载进行深度检测

一次成功的 APT 攻击，通常都会利用到免杀木马，并且可能有很多的变种。一个新制作的样本可能并不携带恶意代码，能顺利通过第一道检测在终端上运行起来，然后通过创建新的变种或者通过互联网下载攻击代码。因此需要对数据包里的 payload 进行深度检测分析。

具体威胁检测技术方面，APT 检测包括多种 APT 检测方法：

APT 专项情报，有效覆盖 APT 攻击相关 IOC。

APT 专项行为规则检测（QAPT），利用行为规则快速发现高级威胁攻击。

APT 回扫功能，通过将专家分析获得的一系列 APT 攻击行为特征下发到 APT 检测模块，回扫历史数据，筛查相关 APT 攻击行为。

APT 攻击终端排查，将特定 APT 攻击的特性行为转化为检测条件，实时排查终端、网络行为，确认内部受攻击状态。

3.1.3.3. 安全监控与预警通报

主要包括安全状态的监控、态势分析，威胁攻击的分析溯源和响应处置，也包括资产风险评估、仪表盘安全数据监控、自动化报告，以及知识库的管理维护、安全体系的评估和加固。

通过给被监管单位设定不同的权限实现本单位范围内安全事件、整体态势的监看，同时能将相关数据输出到省局监管中心。

1）安全事件监控

持续自动分析和关联整合攻击相关的上下文安全数据信息，包括各攻击阶段的告警、攻击行为的日志、相关的威胁情报和资产信息，按攻击时序生成安全事件、可视化的攻击链路图，并提供处置建议，便于进行威胁分析和处置。

以图谱方式展现当前信息系统遭受到威胁攻击，包括攻击利用到的战术和攻击技术，可以方便的了解哪类攻击是主要攻击以及这些攻击利用何种攻击战术和技术。提供多维度事件信息展现，以发生时间顺序展现，用图形化的方式展现攻击链路图，动态展示与回放攻击过程，以直观的可视化方式分析攻击过程。

在告警事件中，可获取相关联的攻击技术说明，包括攻击技术的解释说明，攻击技术的数据源等信息辅助分析。

安全事件总览基于严重等级和威胁分值展现处于活跃状态的安全事件列表，提供命令行交互检索查询方式。

2）安全态势

安全态势以大屏方式展示整体安全状况，主要包括全局态势、业务态势、攻击态势以及漏洞态势。

全局态势

全局态势可对全局安全情况进行宏观分析和态势展示。全局态势可从安全数据统计、业务系统概况、实时攻击展示、全局风险趋势、安全管理信息、攻击事件排行和漏洞排行几个维度对整体网络安全情况进行分析展示。

业务态势

可对监测范围内的业务系统数量进行统计，直观了解业务系统的攻击及漏洞概况、业务系统应急响应和安全事件情况。

攻击态势

利用多维统计分析模型和多样的可视化图表，对整体的攻击态势进行直观呈现。以动态攻击地图的形式对当前的攻击路径、攻击趋势、攻击热度等状态进行展示，包括对情报的命中情况展示、对当前遭受攻击的状态、攻击趋势的评估定性。从多种时间段维度展示不同攻击类型的攻击走势曲线、攻击端口的分布、攻击源 TOP 排名，攻击事件详情的分布等，可分别从各业务系统和安全域的视角展示攻击信息，可从各资产攻击事件的数量、增量、持续时间等维度对攻击事件进行分析呈现。

可分别从全网攻击、境外攻击、境内攻击、内网攻击几个维度分别对全网攻击情况进行态势分析。能够以直观的展示方式呈现世界地图中的实时动态攻击行为及在中国地图中实时动态攻击行为，并且支持攻击事件数量统计，包括攻击事件总数、影响较大的攻击事件、中高危告警总数和收到威胁行为总数，可根据事件数量和时间的变化生成攻击趋势图便于用户掌握攻击态势。

通过攻击态势分析，可了解到各被监管单位受到的攻击情况、业务系统受到的攻击情况，同时也能针对事件名称和事件源进行排名分析。

漏洞态势

以漏洞情况为视角，从漏洞弱点的危险性、影响性、分布情况、变化趋势、处置情况等多个维度分析全网安全漏洞整体情况。能够以地理方式显示各被监管单位的漏洞分布情况，并且可对全网中高危漏洞总数、不处置中高危漏洞数量、已处置中高危漏洞数量、漏洞总数进行统计展示。可直观展示业务系统中漏洞的分布情况。并对漏洞类型进行排名分析。

3）威胁溯源

提供多种威胁溯源方式，包括各类交互式检索分析以及自动化威胁溯源结果展示。支持命令行交互检索查询（类 SQL 语言）方式对目标数据进行查询操作，便于人员快速的进行查询。

支持以时间轴维度溯源展示安全事件过程以及全部上下文信息，自动智能聚合关联的日志、流量以及告警信息，支持对日志及流量数据的信息下钻，便于进行安全事件的分析溯源和处置。

4）可视化分析及展示

提供强大的数据分析功能，可快速以多维度展现数据的价值，自主式的对数据进行分析，提高工作效率。安全数据分析结果通过可视化图表展示与分析，图表展示包括直方图、折线图、面积图、饼图、表格、统计值、同比、环比等多种类型，同时提供自定义功能，快速生成所需的分析图表，生成的图表还可应用到仪表盘和安全报告中。

可视化展示能针对广播电视特点呈现网络安全监测各相关数据，报警，报告并根据建设方要求进行定制开发。

5）资产风险评估

资产风险评估功能提供资产信息和资产的风险状态信息，资产风险评估包括资产的重要性、资产的脆弱性情况、资产受到的威胁攻击情况等多维度信息。

资产信息可对接已有资产系统，从中获取资产和安全相关字段信息，支持导入外部资产列表，导入资产信息，支持添加资产自定义标签，支持导入业务系统、安全域、物理位置、组织机构等信息方便从多维度进行资产风险展示。

资产风险展示支持资产与相关漏洞、威胁的关联，从资产维度了解资产相关的漏洞与威胁信息。

6）智能仪表盘

智能仪表盘可自定义各类图表，实时查看各类安全指标，主要特性如下：

支持对安全事件类型、级别、阶段及状态进行图表展示，能够通过界面事件内容直接下钻到详细事件内容，通过事件内容下钻到关联资产和原始事件内容。

支持自定义仪表盘配置，可根据需要添加不同的监控组件，自定义选择过滤条件和过滤条件组的监控组件添加、修改和删除。

支持多种展示图形，如饼状图、条形图、面积图等，能够灵活配置，显示展示图的同时可选择分组字段进行 TOP N 的统计排名。

智能仪表盘支持丰富功能，当仪表盘异常时，可关联至具体事件、告警进一步检查，也可跳转至自定义仪表盘，进行定制化分析。

智能仪表盘图表库包含上百种内置图表，并可通过 BI 快速自定义图表进行扩充。

7）自动化报告

具备自动生成监测周报、月报的功能。

自动化报告提供安全状态、安全事件、威胁攻击、评估结果等安全报告，支持报表和报表模板管理，可自定义报表和报表模板，区分不同类别的报表。

可配置报告周期（如：每日、每周、每月）自动生成报表，并通过邮件、下载、导出等方式发布报告。

安全报告支持 WORD、XLS、HTML 和 PDF 等多种格式。

8）安全知识库

安全知识库是总结学习安全知识和实际发生的高价值安全案例的功能模块，可容纳各类安全知识，如用户环境内的特殊场景、特殊规定，录入至安全知识库供学习和使用，记录和总结内部安全知识和安全案例。

9）持续评估

持续评估对安全系统、设备进行模拟攻击演练，评估现有安全体系能力，发现潜在安全隐患，进行安全架构策略调优，改善信息系统整体安全防御水平。主要具有以下特性：

可评估客户各类安全检测和防护产品，如防火墙、安全网关、入侵防御系统、入侵检测系统、网络流量分析系统、网络应用防火墙、邮件网关、终端管理系统等。

提供多种类模拟攻击方案可供用户选择，如边界防护、内网检测、终端检测、Email 防护等，进行各种方式的安全评估、检验。

攻击任务可配置为一次运行或定时定期运行，可对安全系统进行持续化验证，及时发现各种原因引起的安全弱点。

入侵者模拟系统的攻击方案可从云端获取更新，利用最新的评估用例发现当前最新的漏洞和问题。

可自动生成评估报告并通知相关负责人。评估报告支持以 ATT&CK 框架评估现有安全体系，并给出结果和相关改进建议，进行系统加固和安全体系改善。

10）预警通报

预警通报将监测分析产生的漏洞利用告警、网络攻击告警、威胁情报告警及手工导入的外部获取的安全告警，及时通报涉事的被监管单位，协调被监管单位完成对网络安全隐患及网络安全事件的处置工作。被监管单位可以通过平台在自己的权限范围内查看本单位的网络安全情况。

通报概览

通报概览指在一定时间范围内对于平台的通报工作进行统计和分析，可根据所选时间周期，进行当前系统已通报的各威胁类型安全事件数量统计、通报类型数量统计、通报事件类型统计、受影响资源排名、通报整改工作阶段统计、超时未反馈的通报任务列表、被通报的安全事件来源统计、被通报单位问题严重情况统计、通报整改效率分析。

安全事件

安全事件分析支持接入网络安全监测基础数据，基于单位维度以列表形式展现网络安全监测告警情况，并支持按照行业、单位、事件级别、监测类型等维度进行筛选。支持从业务分析角度以单位维度进行数据分析，统计分析重保单位各类安全隐患的数量。

日常通报

日常通报基于平台监测的各类网络安全隐患及事件，分析研判后对被监管单位的安全隐患情况展开网络安全隐患及事件通报，支持对于通报反馈情况的跟踪和记录。

专项通报

专项通报，支持创建、发起针对多个通报对象的专项通报任务。

综合通报

综合通报管理，针对设置的各类通报模板，按照指定的周期完成对于指定单位、管辖区域的网络安全综合数据分析，并形成通报文件。支持通报文件的上传、下载及通报发布。

通报配置

平台将符合通报预警业务的数据自动推送到数据分析模块，通报流程可配置。

# 四、采购需求

| 序号 | 名称 | 技术参数配置 | 单位 | 数量 |
|---|---|---|---|---|
| 1 | 网络安全监测数据采集 | | | |
| 1.1 | 市广电网络 | | | |
| 1.1.1 | 网络分流器 | 接口：≥96 个 SFP+端口（提供前置辅助接口扩展 2 个 40G 速率 QSFP+端口，4 个 100G 速率 QSFP28 端口）；<br>处理能力：单设备处理能力不低于 0.9Tbps；<br>功能：支持 7 元组规则不小于 2000 条（源/目的 IP 地址，源/目的 TCP 端口号，源目的 Mac 地址，协议号）过滤，支持六元组规则不小于 10W 条，支持组合规则不小于 1000 条；<br>数据包脱敏规则，对输入口的特定 ip 通讯对进行按 | 套 | 1 |

| | | | | |
|---|---|---|---|---|
| | | 固定偏移量脱敏。 | | |
| 1.1.2 | 网络安全流量探针（10G） | 功能：接收网络安全流量探针的数据，进行安全数据分析，过滤网络流量数据噪音，并将安全事件相关信息回传给中心<br>性能：吞吐量≥10Gbps | 套 | 1 |
| 1.1.3 | 日志采集器 | 功能：日志数据采集、数据解析，采集部分包括网络安全设备日志、服务器日志、日志服务器以及已有态势感知系统的日志平台等多源异构数据的接入<br>处理器：核数≥32 核；<br>内存：≥128G；<br>硬盘：≥1TB RAID5。 | 套 | 1 |
| 1.2 | 市电视台 | | | |
| 1.2.1 | 网络安全流量探针（10G） | 功能：接收网络安全流量探针的数据，进行安全数据分析，过滤网络流量数据噪音，并将安全事件相关信息回传给中心<br>性能：吞吐量≥10Gbps。 | 台 | 1 |
| 1.2.2 | 日志采集器 | 功能：日志数据采集、数据解析，采集部分包括网络安全设备日志、服务器日志、日志服务器以及已有态势感知系统的日志平台等多源异构数据的接入；<br>处理器：核数≥32 核；<br>内存：≥128G；<br>硬盘：≥1TB RAID5。 | 套 | 1 |
| 1.3 | 区电视台（含 | | | |

| | | | | |
|---|---|---|---|---|
| | 电视中心） | | | |
| 1.3.1 | 网络安全流量探针（2G） | 功能：接收网络安全流量探针的数据，进行安全数据分析，过滤网络流量数据噪音，并将安全事件相关信息回传给中心<br>性能：吞吐量≥2Gbps | 台 | 5 |
| 1.3.2 | 日志采集器 | 功能：日志数据采集、数据解析，采集部分包括网络安全设备日志、服务器日志、日志服务器以及已有态势感知系统的日志平台等多源异构数据的接入<br>处理器：核数≥32 核；<br>内存：≥128G；<br>硬盘：≥1TB RAID5。 | 套 | 5 |
| 2 | 监测中心<br>分析平台 | | | |
| 2.1 | 硬件部分 | | | |
| 2.1.1 | 网络安全流量探针（10G） | 功能：接收网络安全流量探针的数据，进行安全数据分析，过滤网络流量数据噪音，并将安全事件相关信息回传给中心<br>性能：吞吐量≥10Gbps | 台 | 1 |
| 2.1.2 | 资产探测分析 | 通过各种主动探测技术对用户关注的目标网络进行探测，发现目标网络中存在的资产并实时更新资产信息，包括：开放的端口、开放的服务、操作系统类型、设备类型、厂商、型号等，构建并形成基础资产信息库。用户可以通过目标特征快速从基础资产信息库中找到所关注的资产，并了解其详情并掌握实时变化情况。 | 套 | 1 |
| 2.1.3 | 交换机 | 24 口万兆业务交换机（满配光模块） | 台 | 2 |

| | | | | | |
|---|---|---|---|---|---|
| 2.1.4 | 网络安全数据汇聚处理专用主机 | | 用于网络安全数据汇聚、处理的专用主机，配置专用转件，实现被监管单位网络安全数据的汇聚<br>处理器：2 颗，单处理器主频≥2.4GHz，核数≥16 核<br>内存：≥32 个内存插槽，≥8*32G DDR4 内存；硬盘：≥ 2*960G ≥ 10*8T 7.2K SATA3 RAID 卡：≥1 块 RAID 卡 SAS3(12Gbps)控制器，大于等于 2GBCache，支持 RAID0/1/5/6/10/50/60 网络接口：≥ 2*SFP+/10GE 电源风扇：冗余电源，冗余热拔插风扇 | 台 | 2 |
| 2.1.5 | 网络安全数据存储分析专用主机 | | 用于网络安全数据存储分析的专用设备，配置专用软件，实现网络安全数据的存储以及攻击链分析等 处理器：2 颗，单处理器主频≥2.4GHz，核数≥ 16 核<br>内存：≥32 个内存插槽，≥8*32G DDR4 内存；硬盘：≥ 10*8T 7.2K SATA3 RAID 卡：≥1 块 RAID 卡 SAS3(12Gbps)控制器，大于等于 2GBCache，支持 RAID0/1/5/6/10/50/60 网络接口：≥ 2*SFP+/10GE 电源风扇：冗余电源，冗余热拔插风扇 | 台 | 8 |
| 2.2 | 软件部分 | | | | |
| 2.2.1 | 态势感知与预警通报（含 3 年的驻场服务以及 3 年内每个季度一次的渗透测试和漏洞扫描服务） | 大数据平台 | 含数据采集、数据标准化、数据补全、数据存储、数据分析等功能。实现全量数据的集中采集、处理、存储、查询、分析，为上层模块提供数据检测与管理的基础。提供多源数据关联分析功能，提供实时数据分析和历史数据分析，可基于预定规则关联情报、资产分析生成相关安全告警。包括数据采集、数据解析、数据标准化、数据丰富化、数据存储、数据检索、数据计算、数据管理。 | 套 | 1 |
| 2.2.2 | | 综合监测分析 | 综合检测分析利用各类特色检测分析引擎，可以从多维度对威胁攻击进行全方位的检测和分析。<br>具备情报检测分析、样本查杀检测、关联分析、ATT&CK 检测、AI 检测、终端行为分析、网络行为分析、APT 检测的能力。 | 套 | 1 |
| 2.2.3 | | 全监控与预警 | 主要包括安全状态的监控、态势分析，威胁攻击的分析溯源和响应处置，也包括资产风险评估、仪表盘安全数据监控、自动化报告，以及知识库的 | 套 | 1 |

| | | | | | |
|---|---|---|---|---|---|
| | | 通报 | 管理维护、安全体系的评估和加固。 | | |
| 2.2.4 | 威胁情报、知识库更新 | | 攻击者的远程命令与控制服务器等情报信息（恶意家族信息、攻击团伙信息）更新。<br>解析规则、检测规则、分析规则与模型更新<br>含 3 年的情报更新许可。 | 套 | 1 |
| 2.2.5 | 定制开发 | | 提供产品功能定制开发满足客户需求，包括大屏定制、系统对接定制、功能定制等。（详见第二章 2.6 定制开发需求） | 人*天 | 352 |
| 3 | 边界防火墙 | | 接口：≥4 个千兆电口，≥2 个千兆光口<br>吞吐量：≥1.5G<br>支持病毒防护；支持入侵检测。 | 台 | 2 |