需求一览表

序号	采购产品名称	数量（台/套）	*交付期（日历日）	试运行期（日历日）	*质保期（年）	交付地点
1	骨干网络间大流量网络安全和数据安全监测软件开发	1	90	60	3	采购人指定地点

注：

1. 交付期从合同签订之日开始起算，至软件/系统通过初步验收，具备上线试运行条件为止。

2. 运行期从交付期第二日开始算起，到可以终验为止。试运行期内所有出现的问题应得到解决，软件系统运行稳定。

3.质保期自买卖双方验收签署“验收报告”的日期开始计算。

二、具体采购需求

1.本章中加注“*”或“★”号的条款，投标人应完全满足并提供相关正面应答或承诺，否则将被视为实质性不响应，其投标将被拒绝；若技术规格中对“*”或“★”号条款还有证明材料要求的，投标人还应按照招标文件要求提供相应的证明材料，否则也将被视为实质性不响应，其投标将被拒绝。

2.本章中未加注“*”或“★”号的条款，投标人应进行响应并提供相关正面应答或承诺，否则将被视为不满足招标文件要求；如技术规格中对未加注“*”或“★”号的条款有证明材料要求的，投标人应按照招标文件要求提供相应的证明材料，否则也将被视为不满足招标文件要求。

3.以上2条所指的证明材料，如没有特殊说明，指生产厂家官方网站截图或产品白皮书或产品彩页或功能详细描述及设计图，并加盖投标人公章。招标文件中有其他证明材料要求的，以具体要求为准。

（一）详细技术需求

1.采购用途

采集基础电信企业互联链路的流量，实现对流量的数据安全分析及网络安全分析。

2.需实现的功能要求

以数据及网络安全监测为主，开展安全监测，并通过敏感数据识别、数据分级分类、数据泄露检测等技术手段，面向个人信息和重要数据（通信行业和工业互联网行业）对互联互通流量进行数据安全监测管理、威胁分析和事件追溯，实现对数据安全事件和网络安全事件的发现、分析。主要包括数据资产自动识别、数据分级分类、数据安全风险监测、数据安全主体追溯、数据流动态势感知、网站安全监测分析、域名安全监测分析、DDoS 攻击综合分析、僵木蠕综合分析、恶意代码综合分析、网络安全态势感知与预警通报。

3. 详细技术要求

3.1 网络数据安全监测平台软件

3.1.1 数据资产自动识别需求

（1）协议识别需求：系统需支持对互联链路流量进行协议识别，识别出其中承载数据资产的文件，包括：文本类、文件类、压缩文件类等。

（2）数据资产识别需求：系统需支持通过特征匹配、正则匹配、关键词匹配、自然语言分析、机器学习算法等，对协议识别后筛选的数据资产解析还原后的信息进行深度处理，提取并识别文件中的内容。

（3）# 敏感数据识别需求：系统需支持对敏感数据进行识别，包括个人敏感信息、通信业、工业互联网数据，并对等敏感属性进行标注。

（4）# 重要数据/核心数据识别需求：系统需支持对重要数据/核心数据进行识别。

3.1.2 数据分级分类需求

（1）# 数据资产分类分级需求：系统需支持通过数据分级分类模型对还原后的文件进行深度处理，提取并识别文件中的内容，识别个人信息、通信业数据、工业数据，按照数据分类分级要求进行输出数据并展示。

（2）# 数据资产管理需求：系统需支持以清单形式对用户个人信息、重要

数据、核心数据、网络资产进行集中管理，包括但不限于：承载数据传输的业务系统、数据库、FTP、邮件系统等。

（3）# 行业企业信息管理需求：系统需支持接入网间互通流量解析数据，监测发现的个人信息和行业数据等数据资产管理能力，对数据资产的企业主体信息、IP 信息、域名信息进行管理。

3.1.3 数据安全风险监测需求

数据安全风险监测需对数据识别结果、流量解析日志进行综合分析研判，发现数据安全风险的能力，风险识别能力主要包括数据安全风险监测、数据跨境异常监测。

（1）# 数据安全风险监测需求

1）重要数据明文传输：系统需支持应用层使用 HTTP 非加密协议传送明文的个人敏感信息或通信行业重要数据（数据分级为第四级和第三级的数据）以非加密协议形式明文传输的情况。

2）工业互联网数据明文传输：系统需支持对工业互联网数据以 HTTP 非加密协议形式明文传输进行监测。

3）数据接口不安全：系统需支撑对接口进行数据安全风险监测，主要包括：数据接口缺少访问控制、身份认证等技术措施，接口安全防护能力不足，存在接口违规调用、数据泄露风险。

4）个人信息去标识化不规范：系统需支持对个人信息去标识化不规范，即是网站或系统页面展示个人信息时，未进行去标识化或去标识化不合规的情况进行监测。

5）敏感数据越权访问：系统需支持对个人敏感信息、通信业数据或工业数据等敏感数据进行越权访问监测。

6）敏感数据批量访问：系统需支持对敏感数据批量访问进行监测。

7）敏感数据高频访问：系统需支持对敏感数据高频访问进行监测。

8）数据流转范围异常：系统需支持对数据流转范围异常进行监测。

9）数据流转时间异常：系统需支持对数据流转时间异常进行监测。

10）数据流转路径异常：系统需支持对数据流转路径异常进行监测。

（2）# 数据跨境异常监测需求

1)重要数据明文跨境传输：系统需支撑对重要数据明文跨境传输进行监测。

2）敏感数据批量跨境：系统需支持对敏感数据批量跨境进行监测。

3）境外对敏感数据高频访问：系统需支持境外对敏感数据高频访问进行监测。

4）数据跨境流转范围异常：系统需支持接收流量数据后进行流量识别解析和数据文件还原，监测分析数据跨境流转范围异常。

5）数据跨境时间异常：系统需支持对数据流转范围异常进行监测。

6）数据跨境路径异常：系统需支持对数据跨境流转路径异常进行监测。

（3）# 数据安全风险定级需求

系统需支持对数据安全风险进行定级。

1）风险定级策略配置：系统需支持对风险定级策略进行配置。

2）数据安全风险定级：系统需支持对数据安全风险定级策略进行配置，主要用于设置不同安全事件分类及高级日志的危害等级和置信度的风险等级。

3.1.4 # 数据安全主体追溯需求

系统需支持对风险所属主体进行统计分析，风险主体包括：单位，域名，IP。

（1）单位溯源需求：系统需支持对单位进行溯源。

（2）IP 溯源需求：系统需支持对 IP 进行溯源，包括 IP 基本信息、IP 统计信息、IP 风险详情。

（3）域名溯源需求：系统需支持对域名进行溯源，包括域名基础信息、域名统计分析、域名风险情况。

3.1.5 # 数据流动态势感知需求

（1）态势感知需求：系统需支持对数据安全风险进行分析形成态势感知数据，包括数据安全风险分析、数据风险相关联的数据类型和级别分析、并且针对数据出境风险和数据安全风险主机进行持续跟踪展示。

（2）数据安全统计分析展示需求：系统需支持根据相关策略或分析模型，对数据安全信息进行统计分析和趋势分析，形成属地数据安全态势风险情况，以可视化视图呈现。

（3）数据安全风险预警需求：系统需支持对数据安全风险进行研判后及时预警。并根据国家标准《信息安全风险评估规范》要求，为实现对风险的控制与

管理，可以对风险评估的结果进行等级化处理。

（4）数据安全风险检索需求：需支持对互联链路中的数据资产进行发现、检索，并可追溯数据安全风险 IP 传输路径，以及展示风险详情数据。

3.2 网络安全事件综合监管系统软件

网络安全事件综合监管系统软件是针对大规模网络攻击事件、恶意地址访问、僵木蠕等网络安全问题，开展网络安全监测，对网络流量进行网络安全威胁分析和事件追溯，实现对网络流量中安全事件的发现、分析。

3.2.1 # 网站安全监测分析

需实现通过对网站访问日志进行分析，统计网站基本信息情况，并支持进一步对重点网站安全事件、黑链、恶意网站访问等进行安全监测分析。

1）需支持网站统计分析：需支持通过 URL 访问日志，可以统计网站数量，网站受欢迎程度(以被访问次数排名)；也可对网站访问用户来源进行统计分析，统计用户访问网站时所产生的上行流量的网站排名、下行流量的网站排名，统计各类应用下载情况。

2）需支持重点网站安全事件检测分析：需支持通过对网络流量进行监测，并对 URL 访问日志进行深入分析，重点挖掘 SQL 注入攻击、XSS 跨站脚本攻击、CSRF 攻击、WebShell 攻击等网站安全事件。

3）需支持黑链检测分析：需支持通过页面缓存重组、自然语言分析、关键字关联、特征分析、KNN、页面属性识别、动态权重等技术，实现识别相关服务器是否被植入黑链。

4）需支持恶意网站访问检测分析：需支持对已经确认的恶意网站、域名，可通过 URL 日志统计分析用户的访问恶意网站的情况，实现恶意网站访问用户数量统计、区域分布统计。此外，对恶意域名访问量激增等情况进行深入分析和跟踪，发现关联安全事件。

3.2.2 # 域名安全监测分析

需实现基于网络流量对域名解析次数、异常解析域名、请求应答比例等关键指标进行分析，及时发现利用域名服务的攻击行为，包括域名劫持、恶意域名、DGA 域名、仿冒域名、CDN 域名等域名安全事件和服务的监测。

1）域名基础信息监测：需支持对于域名请求应答的分向对准，并对访问递

归数据、递归与权威交互数据、CDN 域名等基础信息进行监测分析。

2）域名服务统计分析：需支持对于域名访问的流量统计、特征统计、分布统计、排名统计等功能。

3）域名篡改攻击检测分析：包括域名污染和域名劫持。需支持采用被动监测方式对于一段时间内所有与重要域名相关的域名访问日志记录，检查其应答中的 IP 地址是否与域名备案的 IP 地址一致。

4）恶意域名检测分析：需支持基于网络流量分析，识别木马和僵尸网络使用的控制域名，并支持根据域名访问记录并结合域名备案信息、域名白名单等数据，发现识别网络钓鱼攻击使用的恶意域名，并可采用人工分析等手段做进一步的判定。

5）DGA 域名检测分析：需支持对 DNS 元数据进行分析，检测利用 DGA 算法生成的恶意域名，对域名数据中的元音比例、长辅音序列、熵值等进行计算，对具有 DGA 特性的域名进行筛选发现。

6）仿冒域名检测分析：需支持利用基础的域名访问日志记录，收集统计知名正常域名，采用机器自动学习方法，建立常用字符的仿冒规则库，发现与知名正常域名相似的可疑域名。

7）CDN 域名服务检测分析：需支持利用 CDN 服务特性，对使用 CDN 服务的域名进行检测，对于首次发现数据中同一域名被大量不同域名映射为 CNAME 的二级域名进行分析处理。

3.2.3 # DDoS攻击综合分析

需实现通过采集网络流量数据，对流量中的 DoS 和 DDoS 攻击情况进行监测分析，利用 AI 模型算法开展大规模网络攻击监测，包括 DDoS 攻击的源 IP、被攻击 IP、攻击峰值流量、攻击类型、被攻击物理位置、告警级别、攻击总值、攻击峰值、攻击开始时间、攻击结束时间、攻击持续时间等。

需支持通过基线、等比、环比、熵等方法，实时监测全量流量中的 DDoS 攻击事件，展示攻击源、攻击目标的分布情况，包括源目的 IP 信息、端口信息、流量熵等信息用于 DDoS 事件的事后追溯分析。攻击类型包括 TCP Flood、UDP Flood、HTTP Flood、DNS Flood 等。结合应用层协议识别功能，还可进一步发现 SYN Flood，NTP/SSDP/DNS 等反射放大攻击。

3.2.4 # 僵木蠕综合分析

需实现通过对网络流量进行的解析，实现僵木蠕数据管理、趋势分析及统计，准确发现僵尸网络与木马控制端、受控端，蠕虫爆发感染区域，保障用户的网络安全。

需支持木马和僵尸网络事件深度挖掘分析，针对网页挂马事件、DDoS 攻击事件等关联触发的木马和僵尸网络事件，以及相关通报、上报的木马和僵尸网络事件，通过 NetFlow 记录、域名访问记录、域名备案库和域名注册信息进一步挖掘该木马和僵尸网络的受控主机、控制端、控制域名等详细信息，对僵木蠕程序数量、主控端数量、受控端数量等进行监测及统计。

需支持僵尸网络、木马攻击和蠕虫感染的态势分析，针对木马和僵尸网络受控主机（特别是窃密木马事件的受控主机），通过关联域名访问记录持续跟踪发现新的控制域名及控制端 IP；通过关联其他系统 NetFlow 数据，持续跟踪发现新的控制端 IP 或者窃密木马向外传送数据的目的地 IP，实现对整体僵尸网络、木马攻击等的态势分析。

3.2.5 # 恶意代码综合分析

需实现通过采集网络流量数据，对多种来源的恶意代码样本进行静态分析、行为分析、同源性分析等进行综合分析，获得恶意代码的传播疫情、家族判定、演进过程、行为特征、事件关联等关键数据，并针对入库恶意代码建立样本及分析数据的索引查询。

3.2.6 网络安全态势感知与预警通报

需实现对各类网络安全监测分析结果数据和其他相关系统接入数据等进行网络安全态势综合分析、汇聚融合，从不同视角感知安全综合态势、威胁风险态势、网络攻击态势和安全事件态势。同时，支持依托预定义的预警通报模板和预警策略，生成预警通报，实现网络安全预警通报信息发布和反馈跟踪功能，定制生成安全事件专题报告、月度/年度态势分析报告等各类工作报表和报告。

1）需支持综合展示网络安全状况，对涉及单位、服务遭受到的扫描探测、WEB 攻击、漏洞提权、弱口令破解、SQL 注入、恶意代码感染、恶意代码传播、攻击组织等维度数据影响范围、攻击频率、攻击次数等数据态势 TOPN 展示，并根据涉及单位、服务等维度重要等级程度结合攻击态势数据。需支持多维度态势

关联分析，包括地域态势关联分析、安全事件态势关联分析、单位态势关联分析、时序态势关联分析等。

2）需支持对网络安全态势进行感知。以综合角度出发，汇集威胁风险、网络攻击、安全事件、预警通报总体分布情况，通过柱形图、饼图、趋势曲线图等多种方式进行综合展现。

3）需支持以攻击角度出发，从攻击、访问两个维度，可实时获取当前攻击、访问总体情况，并结合地图展现攻击实况，包括攻击时间、攻击源 IP、目标 IP、攻击类型方式、攻击路线图。

4）需支持以安全事件角度出发，实时获取不同事件类型总量，支持按地域、行业、时间分布。可查看最新安全事件发生时间、事件类型、涉及的单位重要信息系统 IP、所在地区、行业、来源、取证截图等信息。

5）需支持网络安全预警通报，主要包括网络安全事件通报、重要应用服务安全通报、特定对象网络安全通报等，根据预定义的预警通报模板和预警策略，生成预警通报。

4.性能要求

支持国内常见的 900 余种应用协议，应用识别不低于 95%；能够支持对 TCP、UDP、HTTP、FTP、TFTP、SMTP、IMAP、POP3、DNS、SSL/TLS、SSH、ICMP 等 12 种以上协议的解析、监测匹配；能够实现对 DDoS 攻击、域名安全、网站安全、僵木蠕、恶意代码等类型网络安全事件的监测。

（二）服务需求

1、质保期

1.1 ★质保期自买卖双方在签署的终验验收单的日期开始计算，卖方提供免费质保期为(3)年。

1.2 在质保期内，如果卖方出售的相同型号产品硬件和软件有 BUG 修复方案，卖方应将新发布的硬件和软件 BUG 修复方案在一个月内提供给买方。

2、培训内容及要求

提供不少于 10 人天的培训，培训内容包括但不限于系统架构及设计说明、功能使用、运营维护方法等。培训费用均由投标人负责。

3、项目文档要求

序号	文档名称	说 明	提交阶段
1	需求规格说明书	系统开发最重要依据	需求完成后提交
2	需求变更说明书（如有）		需求变更后提交
3	设计文档	说明相关系统结构、业务流程、系统功能	设计阶段完成时提交
4	测试用例		初验提交
5	测试报告	包含开发方内部相关测试及第三方相关测试（若有）	初验提交
6	初验报告	按照初验要求提交	初验提交
7	终验报告	按照终验要求提交	终验提交
8	用户手册/使用手册		终验提交
9	培训资料文档		培训前提交
10	源代码		培训前提交

4、项目团队要求

项目团队需包括但不限于项目经理、开发工程师、测试工程师、现场实施人员、售后服务及技术支持人员等，项目团队人数不少于 20 人（不含项目经理）。

5、项目进度要求

投标人需承诺从合同签订之日 90 日内软件/系统部署完成并与上下游系统完成对接联调，通过初步验收并具备上线试运行条件。提供承诺书，格式自拟，加盖公章。

6、技术支持及服务响应

6.1 买方可以通过访问网页接入的方式获得最新的技术信息以及其他资料。

6.2 卖方将最新的技术信息和资料及时主动提供给买方。

6.3 技术响应时间要求：

6.3.1 质保期内，卖方免费为买方提供技术指导和维修服务。

6.3.2 质保期内，在标的物出现故障和缺陷时，或接到买方提出的技术服务要求后（ 4 ）小时内予以答复，如买方有要求或必要时，卖方应在接到买方通知后（ 24 ）小时内派技术支持工程师到买方提供现场指导和免费维修；如果出现紧急技术问题，卖方的技术人员应在（ 1 ）小时内予以答复并解决问题。

6.3.3 质保期届满后，如果因标的物硬件或软件的固有缺陷和瑕疵出现紧急

故障和事故，经买方双方协商同意，卖方在接到买方通知之后（24）小时内到达现场。

6.4 其他要求：

6.4.1 平台巡检

(1)每月进行两次，对系统组件进行检查，对于巡检结果发送到关系人，进行处理通知。

(2)针对平台集群及系统中出现的软件问题进行处理。

(3)系统巡检报告。

6.4.2 平台账号管理

(1)平台 ftp 账号新建、延期、回收。

(2)运维门户、调度系统、服务中心、管理中心账号新建、回收。

6.4.3 处理故障邮件、通告

(1)通过程序报错分析发现及各方反馈的异常情况分析并进行处理，完成后反馈相关人员。

(2)对无法处理的异常状况及时通知平台或可处理人员

(3)总结前一天调度任务运行状况，邮件告知相关负责人。

(4)随时解答回复系统使用人的相关问题。

6.4.4 平台系统安全

(1)主机系统安全漏洞修复加固，对外的服务应用安全漏洞修复，及已查明的安全漏洞修复加固。

(2)对扫描出的 mysql、ssh、vsftp、redis 等弱密码进行整改。

6.4.5 数据运营监控

(1)监控数据源采集情况，如发生延期等情况，及时通告；

(2)监控数据处理情况，对出现的任务失败、任务锁死等问题进行处理；

6.4.6 应用巡检

(1)应用门户日巡检报告

(2)应用访问日志收集、检测

(3)访问日志分析

6.4.7 应用资源监控

(1)监控应用服务器访问资源，评估访问资源风险，对存在的资源情况行上报

(2)监控 mysql、redis 的使用资源情况，维护资源空间

6.4.8 应用 BUG 处理

(1)收集整理应用的 BUG，对 BUG 内容进行处理

(2)收集整理各门户的功能改进优化需求

(3)针对新功能及需求不明确项讨论相关问题

7、其他

7.1 投标人应提供详尽的售后服务方案。

7.2 投标人应提供详细的服务质量保障方案。

7.3 投标人应提供详细的测试方案与验收方案。

7.4 投标人应提供详细的实施部署方案。

8、履约验收需求

8.1 验收方案（验收内容、方法及流程）

（1） 验收内容：软件产品

1） 系统部署验收；

2） 系统功能完整度；

3） 系统可靠性和安全性；

（2） 验收程序

工程验收应包括初步验收（初验）和最终验收（终验）。

按照如下的步骤实施验收：

1） 提出验收申请；

2） 制定验收计划；

3） 进行验收测试；

4） 进行验收评审；

5） 形成验收报告；

6） 系统移交。

30 个日历日试运行期结束后，所有性能指标达到技术需求后，进行终验，终验通过之日即为系统保修期开始之日。

8.2 验收标准

（1）初验

设备安装、调试达到技术需求规定的指标并投入使用，可进行验收测试（初验）。

验收规范（包括项目、指标、方式和测试方法等）需要提前提交给招标人。

招标人可根据合同及技术需求和有关规定进行修改和补充，经双方确认后形成验收文件作为验收依据。

验收测试合格后，双方签署验收协议，系统正式投入试运行。

（2）系统试运行

经初验后即进入合同规定的试运行期。

经过合同约定的试运行期，所有性能指标达到技术需求的要求时，可进行最终验收。

为了保证产品在试运行期间及以后的正常运行，技术小组在设备安装时应对用户维护人员进行必要的现场培训。

在试运行期间，应标方将定期了解系统运行情况，并填写《试运行情况跟踪表》，以确保按期终验。

（3）系统终验

系统经过试运行期，所有性能指标达到技术需求的要求时，可进行最终验收。