**便携式全流量系统**

**产品与技术白皮书**

**1.产品概述**

**1.1.背景**

随着信息化的加速，企业网络日趋完善。企业数字化的加速，让越来越多的关键业务运行在计算机网络基础之上，越来越多的重要信息通过网络传送，企业网络面临日益严重的安全威胁，这些安全威胁以窃取信息和收集情报为主，具备长时间隐蔽工作的能力，对国家和企业的数据安全造成了严重威胁。特别是在新冠疫情席卷全球后，国际关系变化莫测，国家关键信息基础设施建设也面临着无形的网络安全威胁，我们应当未雨绸缪，厉兵秣马，化被动为主动。针对网络流量具有随机、分散、海量的特点，高速、灵活、全面的存储和检索技术支持是解决当前网络流量问题的重要特征，所以，基于全流量数据海量存储、快速检索、灵活分析、精准溯源一体化解决方案是当前网络安全领域的迫切需求。再者获取经济利益为目的病毒的新特点日益猖獗：

1)隐蔽性（兼容性、程序不可见性，任务完成后自杀）：越隐蔽的病毒越难被用户发现，从而越不容易被反病毒公司收集。

2)抗杀性：对老病毒进行改造，采用加花指令、加壳、修改特征值等免杀技术，躲避杀毒软件查杀。采用内核技术加强对病毒的保护，使杀毒软件即使发现也难以清除。直接对杀毒软件进行攻击，导致杀毒软件不能正常工作。

3)针对性：针对特定的目标，采用特定的病毒攻击。如果被攻击的用户没有发现，反病毒公司就无法收集到这个病毒，这个病毒将在用户的计算机中长期与杀毒软件共处。

4)小批量、多变种、自动更新，减少病毒被发现和清除的几率。

5)工具化、自动化：自动生成病毒变种，导致病毒数量呈几何级数增长，反病毒公司处于难以应付的境地。

**1.2.产品介绍**

便携式全流量系统-NTA流量取证，适应用户业务逻辑的实时监测与智能分析平台。NTA流量取证系统以攻防为核心理念，通过数据处理技术，深度分析和解码网络协议数据，结合网络攻击识别与流量安全分析技术，检测并安全分析分析网络流量中的安全事件，将攻防技术研判转换为业务风险结果。结合资产架构、采集存储、解析检索等产品能力的全流量安全分析平台，具备全流量记录、全日志留存、全数据检索、威胁发现等能力特点，为实现攻击取证与用户定责提供强有力的数据支撑。

NTA流量取证以大数据、高速抓包、全流量存储、深度分析、威胁情报、可视化为技术基础,融合网络空间资产测绘、网络流量行为分析、日志挖掘、事件安全响应等技术在安全告警事件的基础上提供统一的网络安全高层视图，使安全管理员能够快速准确地把握网络当前的安全状态，并以此为依据采取相应的措施。实现全网流量存储分析及网络安全态势感知，需要在广域网环境中部署大量的、多种类型的流量探针，结合外部情报，来监测目标网络系统的安全状态。通过采集这些传感器提供的信息，并加以分析、处理，明确所受攻击的特征，包括攻击的来源、规模、速度、危害性等，准确地描述网络的安全状态，从而支持对网络流量及安全态势的全局理解和及时做出正确的响应。

**1.3.系统介绍**

NTA流量取证通过采集、处理、分发、检测、展示等五个层次的处理逻辑，对实时流量镜像数据进行捕获、过滤、分析、分发、检测、存储及统计，实现高效的高内聚、低耦合的模块化处理机制。系统从总体实现逻辑上，分为综合管理模块、数据采集模块、数据预处理模块、数据分发模块、威胁检测引擎及业务分析展示模块六个部分组成。系统逻辑架构如下图所示。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 综合管理   |  | | --- | | 用户权限 |  |  | | --- | | 运维管理 |  |  | | --- | | 日志审计 |  |  | | --- | | 系统配置 |  |  | | --- | | 第三方接口 | |

|  |
| --- |
| 元数据集 |

|  |
| --- |
| 数据清洗 |

|  |
| --- |
| 数据归并 |

|  |
| --- |
| 数据关系 |

|  |  |
| --- | --- |
| 流量数据预处理   |  | | --- | | 数据标签化 | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 业务分析展示   |  | | --- | | 资产管理 |  |  | | --- | | 事件管理 |  |  | | --- | | 行为分析 |  |  | | --- | | 威胁检测 |  |  | | --- | | 数据统计 |  |  | | --- | | 通报处置 |  |  | | --- | | 追踪溯源 | |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 威胁检测引擎   |  | | --- | | IP资产识别 |  |  | | --- | | IP端口识别 |  |  | | --- | | IP协议识别 |  |  | | --- | | IP应用识别 |  |  | | --- | | 流量方向识别 |  |  | | --- | | 动态行为检测 |  |  | | --- | | 黑域名检测 |  |  | | --- | | 黑IP检测 |  |  | | --- | | 业务模型分析 |  |  | | --- | | 会话模型分析 |  |  | | --- | | 可视化分析模型 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据分发模块   |  | | --- | | API接口 |  |  | | --- | | 消息队列 |  |  | | --- | | 文件传输 |  |  | | --- | | 数据库同步 | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 协议信息预处理   |  | | --- | | 流量重组 |  |  | | --- | | 协议识别 |  |  | | --- | | 协议还原 |  |  | | --- | | 域名分析 |  |  | | --- | | 文件分析 |  |  | | --- | | 资产属性分析 |  |  | | --- | | 数据包存储 |  |  | | --- | | 元数据提取 | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  | | --- | | 硬件加速 | | 数据采集模块   |  | | --- | | 并行处理 | | |  | | --- | | 离线数据文件导入 | |

**图1便携式全流量流量取证系统架构图**

[1.3.1](1.3.1.1) 数据采集模块

数据采集模块主要能够实现在大流量环境下。对于全网产生的数据进行实时的捕获及过滤，而后分发给检测引擎支撑流量分析、事件还原、协议还原、证书还原等业务运转。

**1.3.1.1.动态流量实时捕获**

通过流量镜像数据接入，收集和存储流量中的数据。通过高速存储转发引擎，实现数据流量的快速过滤、整合、关联和转发。

系统硬件均配备1对光口和2对电口。其中，电口为以太网接口，光口支持配置EPON、GPON光模块，便于光网络数据信号的接入；为实现全网流量数据的动态实时采集以及提升数据过滤及分发的效率，采用以下几种方式提升系统性能：

（1）硬件加速：接入硬件加速卡，释放CPU资源，提高资源利用率，实现万兆多网卡多路全流量高速采集，并同步进行数据实时处理和分发的资源调用；

（2）并行处理：将捕获的数据分割成多个流，使用并行处理框架、分布式系统等技术，对每个流进行并行处理，从而提高处理的吞吐量和效率，满足对大流量数据的全面采集和实时处理需求；

系统支持基于端口聚合的方式，可同时采集多个端口的网络数据，且支持大于10Gbps网络流量的实时处理能力。

**1.3.1.2.离线数据文件导入**

除支持通过分光或镜像方式，实施全流量数据被动接入外，还支持不小于50G大小的离线数据包高速导入，可自动检测监控路径下新增的网络原始数据包文件，并及时的实施导入操作。使用基于零拷贝的网络数据包捕获技术，使得数据包减少多次拷贝，直接从网络接口送入用户缓冲区，同时导入后的数据包保持原数据包中的时间戳，且对于导入数据包的数量及大小不做限制，极大提高数据处理性能。

系统支持两种挂载方式：硬件挂载和网络挂载；

系统内置数据包格式转换工具，支持丰富的数据格式转换，包括5vw、bfr、cap、pcap、pcapng、snoop、tr1、pkt、erf、rfs等；

系统数据接入支持离线文件包形式，提供多源数据包文件方式导入，导入的格式包括本地文件、被检设备文件数据采集文件、NAS存储文件、FTP数据源文件以及通过外接USB存储介质导入文件。本地文件采用直接打开文件进行导入的操作加载离线文件，外接设备可识别设备接入后打开文件选择对话框，加载离线文件即可。

[1.3.2](1.3.1.2).数据预处理模块

数据预处理是系统威胁分析检测的核心支撑部分，是为业务中日常管理，分析关联，业务流转等提供相对标准数据资源必备的重要环节。预处理采用动态，可配置、可扩展的开放式架构，分为统一数据规范、协议识别、解析及转发、数据包文件索引、数据共享等部分。

**1.3.2.1.统一数据规范**

统一数据规范主要解决的是数据的整合、清洗、去重、索引等工作，包括多源数据整合、数据清洗、数据归并、数据关联补全及数据标签化等功能。统一数据规范功能可设置相关规则及条件，对所采集数据去重、规约化处理、错误数据丢弃等处理方式，对剩余数据进行预处理和清洗。形成元数据库，可针对元数据库中内容定制化筛选，支持从链路层到应用层协议多元组定制化数据筛选，并对相关数据进行重组，支持根据时间、物理地址、端口、协议等多重条件，进行会话重组。另外针对元数据提取包括以下类型：

（1）针对网络协议基础信息、关键应用、文件等级别的元数据提取功能；关键应用支持DNS、HTTP、HTTPS、ICMP数据进行协议还原，提取并记录协议中请求和对应响应的关键信息，如ICMP的Type和Code，DNS中的请求域名、回应地址、查询状态，HTTP中URL、请求方式，HTTPS中的证书指纹等；

（2）针对文件提取和还原包括HTTP、邮箱协议（SMTP、POP3、IMAP）、SSL证书等。



开始



|  |
| --- |
| 检查是否是http第一个包（请求，或 者200ok包） |

否



请求包



|  |
| --- |
| 重组包 |



|  |
| --- |
| 检查是否有内容需要输出? |



有之前请求内容？

有

否



|  |
| --- |
| 拼装文件内容，包含gzip和chunk解码 |

否



|  |
| --- |
| 输出文件和日志 |



|  |
| --- |
| 解析请求头信息，获取文件名和长度 |



结束

**图2文件还原实现过程**

**1.3.2.2.协议识别解析及转发**

数据过滤及转发主要是在将多源数据进行整合、清洗、索引后进行协议识别、解析还原工作，基于流量重组、协议识别、协议还原、IP分析、域名分析、文件分析、元数据提取、数据包存储、资产识别、检测结果查询及资源监控引擎等，实现多源流量数据的预处理；同时提供告警功能，将数据包转发给威胁检测引擎解析pcap流量文件，从而对数据包做会话重组，同时保存数据包在原始pcap文件中的位置，对于命中告警规则的会话数据，输出告警信息，并从原始pcap流量中，读取数据包保存到对应的pcap告警包中。系统内置协议样本库，可支撑主流协议识别和解析，支持TCP、UDP、ICMP、IP、ARP、HTTP、FTP、SMTP、POP3、IMAP、DNS、SSL/TLS、SSH、Telnet等主流协议完整解析，同时支持识别不少于1200余种协议或应用，不少于500余种协议的解码识别分析，可解析协议字段攻击不少于10000个，通用应用层协议（RFC完全认可的标准协议）解析率不低于95%。并可根据需要自定义配置协议识别、解析功能的启停。

协议识别、解析技术实现：

将规则样本进行解析，从规则文件中读取规则，生成规则结构体数据给hyperscan进行使用。

1.首先将规则逐行加入到链表，把规则按照正则规则，sip规则dip规则sport规则，dport规则，和组合规则，放到6个不同的链表

2.然后构造6个链表对应的内部规则id列表和对应的规则内容列表数组。对于payload规则则进行规则加入到hyperscan的动作，编译对应的hyperscan库

3.对于含有or的正则规则，或者组合规则中包含payload规则的，把规则加载到扩展规则库并编译子hyperscan库。



开始



|  |
| --- |
| 构造四元组key |



|  |
| --- |
| 匹配纯ip端口库 |

匹配上？



|  |
| --- |
| 判断是否是组合规则 |

否

组合规则？

否



|  |
| --- |
| 匹配内容 |



|  |
| --- |
| 回调命中接口 |



匹配上？



|  |
| --- |
| 回调命中接口 |

否



结束

**图3协议识别、解析流程图**

协议识别、解析规则格式样例：



**图4协议识别、解析规则格式样例图**

规则的基本定义如上图。前面的为ruleid，上图列出了常见的几种规则和规则组合的样例。

**1.3.2.3.数据包文件索引**

具备多种索引方式实现对采集的网络数据进行全包索引。可通过L2-L7协议层多元组定制化数据筛选，并可基于威胁检测引擎能力依据网络情况智能过滤安全数据。可根据时间、TTL、节点、物理地址等多重条件，进行会话重组。

**1.3.2.4.数据共享**

数据共享功能在全流量分析检测系统中扮演着重要角色。通过安全传输和存储、匿名化和隐私保护、标准化和格式兼容性、实时更新、元数据和关联信息的提供，以及协作和交互能力的支持，数据共享功能能够促进与其他安全机构和情报共享平台的合作，有效增强威胁情报的共享和响应能力。这进一步提高整体安全防御的效力，促进更快速、准确的威胁识别和应对，打击网络攻击和安全威胁，确保网络环境的安全稳定。

（1）安全传输和存储：使用对称加密和非对称加密技术确保共享的数据在传输和存储过程中得到适当的加密和保护，以防止未经授权的访问和泄露。

（2）匿名化和隐私保护：对共享的数据进行匿名化处理，以保护用户的隐私和个人身份信息。

（3）标准化和格式兼容性：确保共享的数据符合行业标准和特定交换格式，以确保数据的一致性和可操作性。

（4）实时更新：及时更新共享的数据，以确保数据的准确性和实用性。

（5）元数据和关联信息：共享的数据包括足够的元数据和关联信息，以便接收方能够解数据的来源、上下文和可信度。

[1.3.3](1.3.1.3).数据分发模块

数据分发模块是系统中的一个重要组件，根据应用场景不同，可提供基于硬盘或内存维度的数据转发与共享；面向小流量场景，可在捕获流量的同时对流量进行过滤后分发给检测引擎；面向大流量场景可提供标准的API接口、使用消息队列和文件传输等数据分发方式，实现将系统所捕获及处理后的数据分发给第三方平台。使得便携式全流量系统数据分发过程更加灵活可控，可与第三方平台实现解耦和扩展效果。

**1.3.3.1.API接口**

系统提供标准的API接口，第三方平台可以通过调用接口来获取所需的数据，且可通过简单配置编辑API协议和数据格式，促使数据分发更加灵活可控；

**1.3.3.2.消息队列**

将消息队列做为中间件，将系统所捕获的数据发生到消息队列中，第三方平台可通过订阅该消息队列接受所需数据，消息队列具备异步通信的能力，能够有效的解耦及扩展第三方平台；

**1.3.3.3.文件传输**

将数据转存为特定格式，如JSON、CSV等，然后可通过FTP、SFTP、HTTP等协议将转为文件的数据发生给第三方平台，第三方平台可以周期性的在特定位置下载文件后解析处理；

[1.3.4](1.3.1.4).威胁检测引擎

以全流量存储为基础，通过威胁检测引擎进行网络外部攻击实时检测，不漏过任何一条威胁告警，并对单次攻击及整体入侵事件进行成功与否研判，从而回溯整体攻击过程。

**1.3.4.1.IP资产属性深度识别**

设备对流量进行分析后，运用端口应用识别技术和UAAE应用识别模型技术，对发现的资产指纹进行深度刻画，并记录在数据库中。在UAAE应用识别模型技术中主要利用协商协议模型、隧道协议模型，这两类模型是针对IP协议族中的层次关系，对每个协议的特征进行分解，从获得的上层协议建立应用协议树，从而获取应用协议中的资产指纹信息。

利用流量分析技术手段，对IPv4/IPv6网络环境下的数据进行还原，实时分析网络流量中的资产开放端口、服务应用等信息，实时与工作阶段产生的数据进行比对，达到结合和去重的目的，完善网络内资产指纹列表。并对资产自适应属性识别确认，对于缺失信息，支持手动标记、编辑资产信息，同时，支持根据业务情况，配置业务规则并进行资产矫正，以提高资产画像完整度。

**1.3.4.2.PCRE正则表达式库**

系统中嵌入PCRE正则表达式库，可通过自定义正则表达式来作为Suricata和Snort语法的解析器，主要可解析Suricata和Snort规则文件的语法结构。解析器负责解析规则中的各个字段、操作符和条件，并将其转化为内部数据模型，从而提升系统的威胁检测效果。

**1.3.4.3.攻击行为检测**

全流量安全分析系统支持丰富的基于攻击链的攻击检测，目前可以检测的攻击类型有二十余大类，共计千余种入侵行为识别。

支持检测主流的的威胁类型，包括业务安全定制化规则检测、端口探测、信息探测行为检测、身份认证攻击检测、蠕虫病毒检测、挖矿检测、黑客指令执行检测、溢出类攻击检测、会话攻击检测、可疑文件的异常传统检测、隐秘隧道检测、脚本工具攻击检测、木马攻击检测、拒绝服务攻击检测、应用漏洞攻击检测、内网渗透痕迹检测、数据库异常行为检测，SQL注入攻击、弱口令攻击、网络扫描、僵尸网络、勒索软件、流氓推广、后门程序等；

总的攻击行为识别包括：WannaCry勒索软件、勒索蠕虫、勒索软件挖矿蠕虫、僵尸网络挖矿、Cobaltstrike远控木马、StrutsRCE漏洞攻击、Tomcat远程代码执行等主流攻击行为。

主要攻击行为检测能力，列举如下：

(1)支持特征域名、特征IP、威胁URL、可疑MD5、木马通信特征检测，同时支持批量导入用户自定义特征。系统支持云端联动公司自研威胁情报库，并可接入其他威胁情报平台，离线模式使用离线库，进行特征IP、特征域名、木马特征检测。特征域名、特征IP、木马特征等威胁情报自定义特征导入；

（2）支持自定义通信特征的实时检测，特征规则包含十六进制特征、字符串特征、yara规则、正则表达式。

（3）支持对网络设备进行注入攻击、远程漏洞执行等漏洞攻击检测。

（4）支持DNS、ICMP隐蔽隧道、HTTP隐蔽通道检测。

（5）支持网络异常检测，异常主动外联检测会话心跳、WebShell检测等。

（7）支持远程控制检测，检测包含暴力破解。

（8）系统支持网络流量异常综合性检测，通过协议识别、心跳检测、数字证书检测等手段，对包含非法证书检测等。

（9）支持包括永恒之蓝漏洞检测等内网任何横向移动网络攻击行为检测。

（10）支持多种网络扫描行为检测，包括主机扫描检测、端口扫描检测。

（11）支持WEB服务风险综合性检测，包含webshell、SQL注入、非授权访问、XSS攻击、Apache远程漏洞等。

（12）支持APT威胁检测。有多年APT经验，收录多种APT组织木马样本、恶意域名与IP、受害者IP与攻击手法特征，无论威胁检测或是威胁情报在APT特种方向有很强大的检

出率。

（13）具备告警功能，威胁检测引擎引擎解析pcap流量文件，对数据包做会话重组，同时保存数据包在原始pcap文件中的位置，基于系统内置数据采集脚本能力提取数据IP、DNS协议域名、HTTP协议URL、文件MD5值，匹配威胁情报黑ip、黑域名和恶意文件的md5信息，输出命中威胁情报的告警数据，并从原始pcap流量中，读取数据包保存到对应的pcap告警包中。

**1.3.4.4.场景化检测**

以威胁检测为核心，基于用户真实业务环境，根据不同的网络活动方向建立应用场景模型；通过全流量威胁检测与分析技术，进行场景/场景组智能化一键威胁检测，快速、有效、清晰的呈现攻击事件；实现业务风险一键获取，满足各行业的网络安全需求。

支持根据L2-L7协议层多种元素、应用层协议等预设条件，单独抓取网络数据会话，并进行存储。

支持数据采集时，根据源、目的IP，源、目的端口号，协议、MAC地址等过滤条件，通过“与”“或”“非”等组合方式，过滤流量数据，同时根据业务应用层的数据使用请求，可将过滤后的数据转发至威胁检测引擎中支撑顶层业务流转。

系统内置常用典型的数据包分析模板，用户可对模板进行编辑修改保存，实现快照的快速分析；系统同时支持针对用户业务场景定制化模型编辑，通过表达式和条件过滤等方式，实现多级迭代过滤，系统内置常见表达式和分析挖掘模板，可供用户随时调取使用，系统提供标准的插件接口，用户可根据接口方式自行编辑表达式和挖掘插件，支持即插即用。

基于业务场景建模，通过网络行为梳理与资产识别功能提供攻击告警的大数据检索和场景建模能力，便于分析师在发现安全事件后对事件进行全方位检索与关联；基于访问关系建模，访问关系梳理主要包括主机访问关系和业务访问关系。通过深度访问关系梳理，可有效发现未知威胁；主机访问关系建模，通过协议、应用、攻击类型梳理出主机访问关系，解攻击IP“从哪来”“到哪去”，有效解决跳板机发现的问题；基于业务访问关系建模：通过多层次IP关联的深度业务关系梳理，解决不同网域之间的访问关系，辅助威胁分析，研判违规跨域连接等高风险异常行为。

基于系统的协议识别、解析能力及元数据索引能力，系统提供对已规整分类分列的数据结果进行组合透视分析，包括系统中已整理成表格的规整数据，以及以列表方式记录和存储的协议识别、解析数据、日志数据等，系统支持任意字段的数据透视分析，并支持不同分类的多级任意字段组合检索、建立分析状态快照。

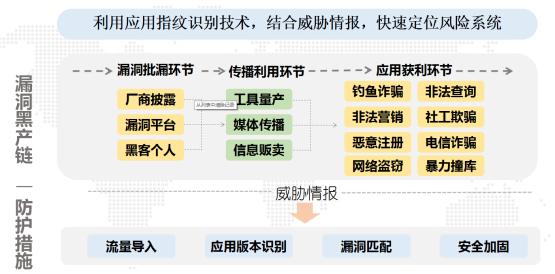
系统支持基于现有元数据字段的全局建模能力，提供预设的数据分析建模，以及用户可自定义的多元数据字段等自主建模分析功能。

系统支持基于协议、应用、事件的检索和过滤功能，最大可支持TB级数据的实时分析能力，提供传输层以下多层元数据的快速检索。

系统支持对Web目录、网络异常行为、HTTP、DNS信息回查，以及统计表方式回查和特征值回查，提供可视化操作界面，回查速度快，操作简单。

**1.3.4.5.威胁情报联动**

威胁情报中往往带有该攻击或恶意软件使用的系统安全漏洞，表现形式为CVE漏洞编号、存在漏洞的应用版本信息。通过在内网建立CVE漏洞信息库或实时访问官网漏洞信息，可以获取该漏洞的影响范围和修复方法。包括影响的系统类型、版本，修复该漏洞的版本等，将这些信息在内网资产库中进行比对，即可精确定位面临威胁的资产，针对性的组织修复。



|  |
| --- |
|  |

**图5漏洞快速定位技术框架图**

产品提供威胁情报IOCs导入功能，涵盖黑IP，黑URL以及黑样本等信息，并可基于IOC进行监测告警。威胁情报数据支持离线导入并能实时生效。对于威胁情报触发的安全事件具有独立标签标示。

系统具备根据可疑域名、可疑IP、Web攻击进行实时告警的能力；能够对TCP/UDP数据流进行监测。

系统内置恶意IP资源库、恶意域名管理，支持离线方式管理。

支持通过配置重点关注的对象，检索和过滤相关数据流量和会话。对于关注的域名，可增加关注域名规则，设置之后系统自动关联与域名相关的话单。

便携式全流量系统支持基于威胁情报的联动，公司会不断收集和挖掘黑IP、恶意域名、恶意文件HASH、APT组织关联信息等热情报，同时联动现网部署的各套设备中抓取到的鲜活数据，形成用户侧自身的内部威胁情报体系，并根据外部情报热点实时更新。联动内外部情报与实时监测溯源，解决外部威胁情报证据链不完善、内部情报攻击源画像不清晰等问题，配合自定义威胁情报添加、重点监控等功能，完善外部/内部情报在具体单位的活动轨迹及威胁描述，提供完整证据链。

[1.3.5](1.3.1.5).业务分析展示模块

主要是在系统管理界面上以图形化方式直观的展现网络流量曲线图、威胁数量、任务分布、协议分析等信息。

**1.3.5.1.数据统计**

系统支持协议会话流的统计功能。

系统支持可视化展示流量情况。如基于IP流量维度统计的网络流量数据统计曲线图和基于会话端口统计的会话端口流量数据统计曲线图。

系统支持IP维度的统计，支持以会话端口维度对流量数据统计。

系统提供对协议数据的统计、模糊查询功能，会话流统计计算，支持不同维度统计方式。

提供对元数据标注字段进行模糊查询。同时系统可以由用户进行自定义的字段关联匹配能力，对IP、域名等关键字段的进行自定义标注，方便用户根据业务进行自定义方式扩展使用。

**1.3.5.2.数据可视化**

随着可视化技术的发展和应用，系统从多个维度应用可视化技术，帮助用户在资产管理、数据统计、数据检索、追踪溯源等多个业务单元，快速理解业务成果，操作便捷，降低分析难度。具体功能包括但不限于：

(1)系统提供可视化的操作界面，提供拖拉拽的方式实现自定义的检索条件编辑模式，呈现直观易用易理解的数据分析操作平台，降低数据分析人员的分析操作难度，聚焦业务逻辑。

(2)系统针对用户的数据分析过程提供分析行为记录，可根据用户需要建立分析快照，支持以树形结构或者链式路径记录用户检索分析动作，结合检索条件编辑平台，为用户提供高效操作分析功能。

**1.3.5.3.资产态势**

通过大数据分析，综合分析资产或业务系统遭受攻击、恶意操作以及系统自身的脆弱性情况。以业务系统视图呈现资产安全态势，业务系统名称、包含资产数、被攻击次数、恶意操作类型等。

基于资产信息数据，类型、重要程度等，结合资产安全事件、漏洞信息进行多维深度分析。

形成资产数量对比、资产类型分布以遭受攻击和弱点等分析数据，并进行视图态势展示。

**1.3.5.4.威胁态势**

资产在运行的过程中，会不断的遭受到入侵者的攻击，针对资产的平台按照攻击者的攻击步骤：扫描探测、渗透攻击、获取权限、命令控制、资产破坏等进行归类分析，展示整个资产被客户的攻击的全部手段，基于资产面临的特定的攻击、漏洞、病毒、违规行为等多维数据进行关联分析，发现系统中存在的安全事件、安全风险点，进行实时安全威胁预警。让安全管理人员能够快速针对资产方面做相应的安全事件处置。

[1.3.6](1.3.1.6).综合管理模块

**1.3.6.1.用户权限**

基于良好的用户操作性和严格的用户管理机制，通过授权机制实现用户权限的层级属性。系统配置有管理员账户、审计账户、普通用户等多种用户权限级别。

**1.3.6.2.运维管理**

同时，当设备在启动和正常工作时，周期性或按照授权管理员的要求执行自检。

为保证设备自身的安全性，设备支持黑白名单功能，支持隐藏探测器IP地址等安全防护技术，使设备在网络中不可见，任何不被信任的IP都无法发现该设备（ping或TCP连接该设备），且只有经过认证后的信任IP在有效时间内可见、可访问，超时后需重新认证。

**1.3.6.3.日志审计**

能够实现对系统运行期间所生成的各类日志数据进行全面的收集、存储、分析和管理。系统从多个来源获取日志数据，并确保数据的完整性和可靠性。收集到的日志数据存储至数据库，支持长达半年的存储期限。同时提供了高效的查询和检索工具，可进行快速定位和查找关键事件，并支持对日志进行高级分析和报告生成。此外，系统还支持实时监控和告警功能，可以及时发现异常行为和事件，并触发相应的响应措施。通过这些综合的日志审计功能，该系统能够帮助用户实现合规性要求、保护系统安全以及优化运行效率。

**1.3.6.4.第三方接口**

基于灵活适配的原则，系统预留第三方平台接口，具体包括：

(1)支持使用SYSLOG、kafka、TCP/UDP等模式将警报日志、行为日志、元数据日志、会话日志等数据推送给第三方平台；

(2)支持将风险数据、原始流量数据推送给第三方平台。

**2.价值与应用**

**2.1.NTA流量取证子系统**

2.1.1.全数据包留存，实现溯源取证及用户定责

全流量安全分析系统产品支持将全流量以会话流PCAP文件的形式存储于本地空间，基于深度包检测技术，通过深度包检测技术和协议解析还原技术，分析流量中的会话，还原攻击事件和异常行为，实现攻击过程完整还原，达到溯源取证及用户定责的目的。

2.1.2.海量数据秒级检索，助力用户高效查询

系统可根据五元组、网络活动方向，所属国家，时间等多维度进行便捷检索，利用大数据构架，实现秒级检索亿级日志数据，助力用户在海量数据中精准且的获取所需数据；同时，支持数据批量导出，便于用户二次分析利用。

2.1.3.威胁情报，内置威胁情报联动分析

在流量分析-场景分析中流量数据与内部威胁情报进行联动分析，系统内置丰富的黑IP、黑域名的外部威胁情报库与情报说明，记录告警资产与黑客的会话连接数据；同时，利用威胁识别模块生产的内部威胁情报，记录黑客在资产区的全部活动轨迹。便携式全流量系统产品威胁情报模块内置API接口。

2.1.4.实时分析，满足7\*24的安全运营使用

通过实时刷新对不同网域的告警数量监控，展示攻击者在全网的活动检测，清晰明了地向监控人员展示不同网络区域面对的不同安全威胁，安全分析通过对不同区域的关注重点，根据自己分析节奏，联动自动封禁，可快速响应安全威胁。

2.1.5.全面监测，多维度威胁检测能力

覆盖全网络协议的检测能力

系统支持全网络协议的识别、解析和检测，

提供专业化威胁分析模型和复杂关联计算，将攻击者的活动过程、影响范围、入侵进度等以时间轴、攻击可视化等功能简单易懂地展示给分析人员，实现告警找人，避免了人在大数据日志中苦苦寻找告警的困扰。

未知威胁检测能力

采用特征检测+行为分析+攻击链锚点的方式解决APT攻击及0day威胁的高级威胁发现问题，通过攻击者前后网络行为对比、威胁行为所处攻击链锚点的关联分析准确发现高级恶意活动，在客户日常监测、全国性攻防保障期间多次发现0day攻击和高级威胁活动。

**3.系统功能**

**3.1.NTA流量取证子系统**

3.1.1.全面的流量统计分析

通过高性能的流量采集模块，系统实现对网络数据包的全面捕获，并通过高效的聚合算法进行深度解析。采用流量特征提取、协议识别等技术，为用户提供准确、全面的网络活动统计分析，涵盖流量、协议分布、访问模式等多维度信息，支持用户全局洞察网络状态。

3.1.2.基于会话的流量数据展示

通过会话追踪技术，系统对网络流量进行会话级别的关联，实现了对会话数据的动态展示。借助深度数据解析，系统提供对特定会话的详尽可视化，包括数据包流、协议分布、连接时序等，使用户能够深入分析和监控网络会话活动。

3.1.3.基于内容快速取证

运用深度流量解析技术，系统能够快速提取网络流量中的关键内容信息，包括但不限于URL、文件哈希值、报文载荷等。结合元数据关联，系统为安全团队提供了迅速定位和审查潜在威胁的手段，有效支持安全取证工作。

3.1.4.基于多级索引的智能检索

利用多级索引技术，系统建立了高效索引体系，支持多条件组合的智能检索。通过合理的索引层级划分和数据预处理，系统在保证检索速度的同时，提供了对复杂查询条件的支持，使用户能够以更精准的方式检索感兴趣的流量数据。

3.1.5.海量数据的原始流量超快检索

系统做流量存储，存储量级可达PB级别的数据，系统能够做到在PB级别的原始流量或者百亿级的会话量级中，快速检索到会话级原始流量，并提供下载。百亿级会话检索源/目的IP、源/目的端口、源/目的MAC，可以在1秒内返回，并且查询无时间范围限制，实现真正的全流量溯源取证。

运用分布式存储和高度优化的检索引擎，系统实现了对海量原始流量的实时检索。通过并行计算和分布式查询策略，系统在毫秒级别内响应用户检索请求，确保在大规模网络环境下依然能够高效地进行流量检索和分析。

3.1.6.在线PCAP深度分析

基于高性能的PCAP解析引擎，系统支持在线深度解析网络数据包，包括协议解析、数据包重组等。通过提供对协议细节的深度挖掘，用户可以在不离开系统界面的情况下，直接对网络报文进行详尽分析，实现对网络行为的深入理解。

3.1.7.详细的通联关系分析

结合流量关联技术，系统以设备为节点，通过设备之间的通信建立全面的关系图谱。借助图数据库和关系分析算法，系统提供了详细的通联关系，帮助用户识别横向移动、异常通信等潜在威胁，为网络安全提供有力支持。

3.1.8.丰富直观的图表展示

利用先进的可视化技术，系统提供多样化、直观的图表展示模块。通过曲线图、柱状图、饼图等形式，系统将庞大的数据集转化为易于理解的图形化展示，助力用户迅速洞察网络状态，支持决策与分析流程。