专网流量分析版解决方案V2.1

**初步设计方案**

**建设单位：**

**编制单位：**

**编制时间：**

**2018年5月**

**目录**

**第一章** **详细设计方案** 4

1.1 **流量分析介绍** 4

1.2 **流量数据采集** 4

**1.2.1** **流量协议还原** 4

**1.2.2** **网络元数据日志采集** 5

**1.2.3** **网络原始流量采集** 5

**1.2.4** **威胁情报采集** 5

**1.2.5** **IDS安全检测** 5

1.3 **流量异常检测** 6

**1.3.1** **流量异常** 6

**1.3.2** **上下行流量异常** 6

**1.3.3** **间隙会话连接** 6

**1.3.4** **主动外联** 6

**1.3.5** **访问DGA域名** 7

**1.3.6** **端口异常检测** 7

**1.3.7** **隐蔽通道** 7

1.4 **流量攻击检测** 8

**1.4.1** **主机失陷检测** 8

**1.4.2** **蠕虫病毒检测分析** 8

**1.4.3** **DDos攻击检测** 9

**1.4.4** **高级入侵攻击检测** 10

**1.4.5** **IDS安全检测** 11

**1.4.6** **Web攻击** 11

1.5 **流量监控分析** 11

**1.5.1** **网络链路利用率分析** 12

**1.5.2** **流量统计分析** 12

1.5.3 **连接关系分析** 13

**1.5.4** **数据包数量监控分析** 13

**1.5.5** **网络连接分析** 13

**1.5.6** **应用处理请求与响应分析** 14

1.6 **威胁情报** 14

1.7 **追踪溯源** 14

**1.7.1** **溯源分析** 14

1.8 **资产管理** 15

**1.8.1** **新发现资产** 15

1.9 **原始流量包采集** 15

**1.9.1** **采集策略** 15

**1.9.2** **资产流量采集策略** 15

**1.9.3** **告警采集策略** 16

**第二章** **部署与应用** 17

2.1 **标准部署方案** 17

2.2 **典型案例部署方案（供参考）** 17

# **背景介绍**

随着“互联网+”的全面推进，信息技术在国家社会经济建设中的应用也越来越广泛，新型网络安全威胁也更加突出，传统以“防护”为主的安全体系面临着极大的挑战。未来网络安全防御体系将更加看重网络安全的检测和响应能力，因此，运用网络安全态势感知、大数据分析及网络安全趋势预测，能够大幅提高安全事件检测预警和快速响应能力，应对大量未知安全威胁。

很多企业和单位在安全防护上进行了大量投入，用户认为部署了防火墙、入侵检测系统和杀毒产品，网络的安全能够得到充分保障。然而，新型攻击者往往使用高级的攻击手段，绕过或控制这些安全设备，并且长期潜伏在网络中，伺机而动。木马植入、数据资料泄露、用户信息窃取等安全事件还是时有发生，给企业和单位造成难以估量的损失。

目前在高级恶意程序以及逐渐成为主流的情况下，隐蔽通道也已经开始想企业内部渗透，各种安全事故层出不穷不断翻新，已知的手段包括非授权访问、远程代码执行、重定向、系统漏洞等。这些手段不断威胁着我们的信息系统，被攻击的企业已经从耳熟能详的超大型企业逐渐转向大企业、中型企业等。据相关报告显示，2016年有36个APT攻击组织向我国境内发起攻击，占已公布组织的83%，威胁形势严峻。国内包括学校、电信、政府等重要的信息部门都受到了不同程度的APT攻击，波及行业广，关键数据的泄露风险高。鱼叉式钓鱼邮件APT攻击等针对性攻击事件层出不穷，受攻击的企业数量多。

传统的基于事件的安全防御体系总是基于已知知识，包括已知安全漏洞与缺陷、已知木马行为与特征、已知攻击行为和基于五元组的访问控制，这样的安全体系难以应对来自高级攻击的未知安全威胁。很多用户账号长期被盗用、重要服务器被控，甚至核心数据被窃取，用户都还未感知到。企业单依托传统的安全产品已无法全方位的保护重点资产数据，造成了“事前难以预防，事中难以察觉，事后缺乏取证”的现状。传统的安全防护在高级攻击面前形同虚设，企业亟需一种更加全面、更加智能、能够对已知和未知的威胁进行全面感知，从“事前、事中、事后”全方位保障网络安全的高级防护手段。

随着新技术的不断涌现，为了应对当前复杂的网络安全形势，以数据为驱动的安全防御手段逐渐浮现到安管人员面前。所有网络行为都会留下痕迹，数据流量是网络空间中最基本、最核心的组成单元，因此所有的网络行为都会在数据流量中体现。对于数据流量的分析、解析是态势感知技术实现的重要依托，从网络安全的角度出发，能够从流量中分析出网络安全事件、攻击事件、恶意代码回传、恶意扫描行为等，并根据数据流转路线进行追踪溯源。

通过对原始网络数据进行全流量采集和保存，结合人工智能与数据挖掘技术进行鉴别和分析，使海量的网络流量数据清晰可视，同时网络元数据的存储保证了数据的可用性，也为后续的使用和分析提供了前提和基础。针对可疑事件帮助用户进行原始数据取证分析，通过还原数据流和安全事件发生过程、事件关联分析对安全事件影响进行评估，全方位保障网络空间安全。

# **方案依据**

**政策性依据**

《国土资源信息化“十三五”规划》

《中华人民共和国网络安全法》

《全国人民代表大会常务委员会关于加强网络信息保护的决定》

《国家网络空间安全战略》

《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23号）

《关于加快推进网络与信息安全通报机制建设的通知》（公信安[2015]21号）

《国家信息化领导小组关于加强信息安全保障工作的意见》（由于保密原因文号隐去）

《关于加强国家网络安全标准化工作的若干意见》（中网办发文〔2016〕5号）

**技术性依据**

《中华人民共和国计算机信息系统安全保护条例》（国务院令第147号）

《信息技术信息安全管理实用规则》（GB/T19716-2005）

《信息安全技术信息系统安全管理要求》（GBT 20269-2006）

《信息安全技术网络基础安全技术要求》（GBT 20270-2006）

《计算机信息网络国际联网安全保护管理办法》（公安部令第33号）

**网络安全事件管理制度**

《国家网络安全事件应急预案》

《工业控制系统信息安全事件应急管理工作指南》

《信息安全技术 网络攻击定义及描述规范（征求意见稿）》

《信息安全技术 网络安全威胁信息表达模型（征求意见稿）》

《信息安全技术 网络安全漏洞发现与报告管理制度（征求意见稿）》

# **方案目标**

针对网络安全的新挑战，企业亟需发现各类已知和未知威胁，构建全面、纵深和动态的感知能力，同时具备智能的威胁分析能力。具体来说包括以下几点：

* **感知网络威胁**

实时分析网络信息，及时发现主动外联、木马通讯、隐蔽信道等行为，并且对具有明确特征的已知攻击行为进行实时检测与发现警报，包括DDOS攻击、僵木蠕活动、渗透扫描、漏洞利用、SQL注入、恶意劫持、跨站脚本攻击等，帮助用户建立灵敏的网络威胁感知能力。

对绕过防御进入到内网的各类未知威胁进行发现和预警，包括APT攻击、未知恶意代码攻击、漏洞利用、失陷主机通信、数据窃密行为等。

* **安全态势可视化**

基于各类安全数据的多维度整合，利用可视化的手段，可准确、高效地感知整个网络的安全状态以及发展趋势。 针对当前网络的安全现状，本方案采用最新的大数据可视化技术对各类网络攻击、网络威胁和资产安全现状等进行展示，为安全运维人员提供直观全面的安全视图。

* **流量监测**

对网络关键的链路进行日常网络流量分析，目的是对网络关键链路的运行情况进行评估，包括网络的基本运行情况、影响网络的用户和应用情况、异常网络行为情况、关键应用服务的运行情况，确保用户网络及业务应用的正常运行。

* **全流量分析**

通过对原始网络数据进行全流量采集和保存，结合人工智能与数据挖掘技术进行鉴别和分析，使海量的网络流量数据清晰可视，同时网络元数据的存储保证了数据的可用性，也为后续的使用和分析提供了前提和基础。针对可疑事件帮助用户进行原始数据取证分析，通过还原数据流和安全事件发生过程、事件关联分析对安全事件影响进行评估，全方位保障网络空间安全。

* **攻击回溯**

能够对感知到的威胁、可疑线索和已知安全事件进行追踪、溯源、取证，对流量行为分析和溯源，从海量数据中定位准确的数据，还原事件发生过程，了解事件严重程度和影响范围，为用户提供安全响应与分析能力，做出及时正确的响应，并采取防御措施。通过追踪外网攻击者或黑客组织，帮助企业或政府单位采取有效的防范措施，保障网络空间安全。

* **取证分析**

通过对原始网络数据进行全流量采集和保存，结合人工智能与数据挖掘技术进行鉴别和分析，使海量的网络流量数据清晰可视，同时网络元数据的存储保证了数据的可用性，也为后续的使用和分析提供了前提和基础。针对可疑事件帮助用户进行原始数据取证分析，通过还原数据流和安全事件发生过程、事件关联分析对安全事件影响进行评估，帮助用户进行责任认定。

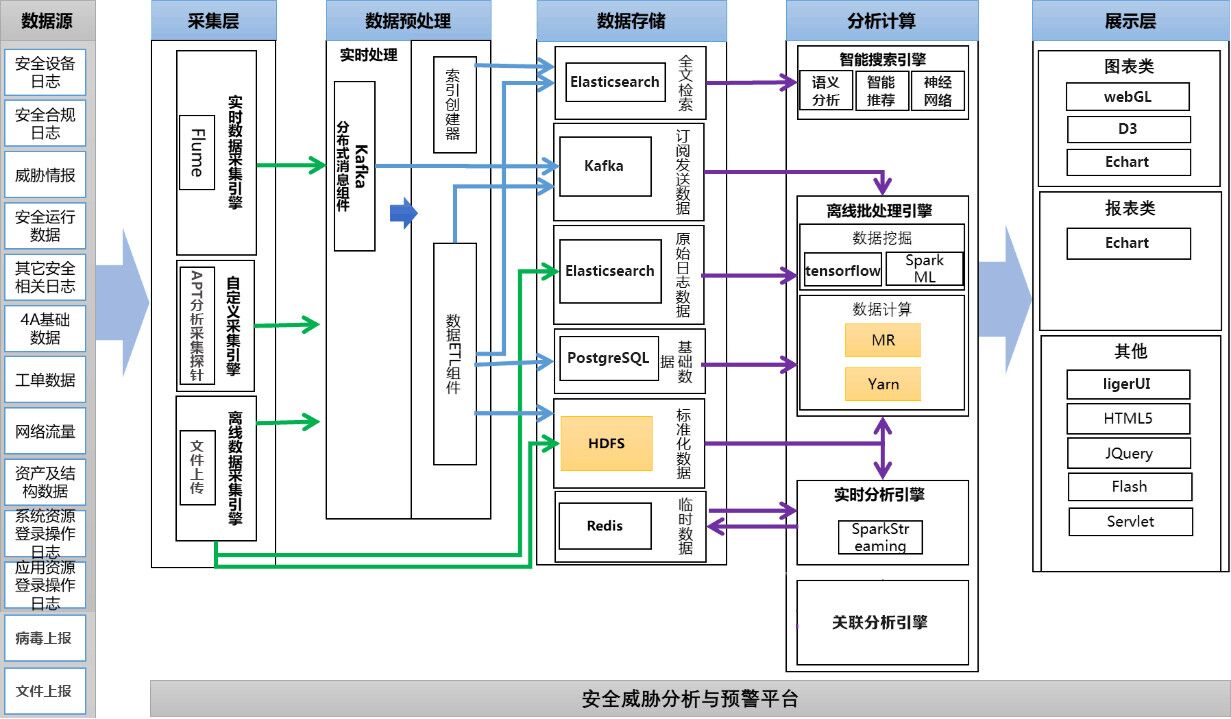
* **安全管理与运维**

系统针对信息安全事件的应急响应、处理流程进行综合管理，对各方资源的有效整合、集中管理、集中监控、集中维护，实现应急预案数字化管理、实时应急调度、应急过程全程追踪及应急事件库同步更新等应用，最终建立统一指挥、功能完善、反应灵敏、协调有序、运转高效的应急机制，预防和妥善应对信息安全突发事件。

# **总体设计方案**

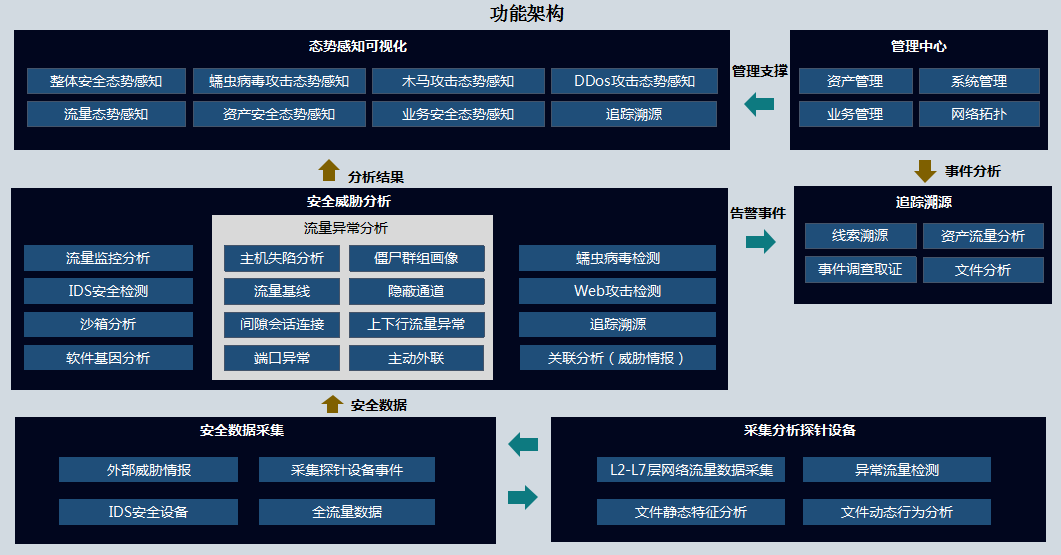
## **总体框架设计**

### **系统设计**



1. 由数据采集系统收集各终端、安全设备、网络设备、中间件、数据库等网元的日志和状态信息，以及实时网络流量数据，发送到大数据平台。
2. 大数据平台采用分布式并行存储方式，提供海量数据存储环境以及秒级的数据查询、调用功能，支持结构化与非结构化的数据存储。
3. 数据防泄漏检测系统、流量分析系统、网络安全威胁预警系统、业务安全监控系统从大数据平台各取所需，进行安全分析和防护，同时能对部分设备进行联动，实时调整安全策略。子系统内嵌多元化报表，用户能有针对性地了解安全状态。
4. 受控设备的监控以及安全分析结果，存储在大数据平台中。由网络安全态势感知系统调取相关数据，形成安全、资产、业务等多维度的整体态势视图，使用户快速直观的把握当前网络安全状态，并且为用户加固安全防护方向提供事实依据。
5. 由网络安全威胁通报与应急系统统一接收各个子系统上报的告警信息，并发出通告、预定处置办法，支持多级区域的通报与应急。

### **功能架构**



态势感知安全平台建设项目总体架构包括5横3纵。其中，5横包括感知基础设施层、数据采集层、数据层、应用层、展现层；3纵包括标准规范体系、安全保障体系和运维保障体系。其中：

（1）展现层

展现层是实现各类网络安全态势、网络安全事件、重要网络安全通知公告等信息及时发布的重要渠道系统，包括：安全态势WEB展现系统、指挥室大屏展示系统和移动终端展示系统等。

（2）应用层

应用层是态势感知安全平台建设的核心内容，包括：应急指挥系统、网络安全态势感知系统、信息通报处置系统和安全大数据分析系统等。

（3）数据层

数据层是态势感知安全平台数据存储、管理及共享控制中枢，在数据采集层之上，包括：数据库管理系统、各个数据库（数据采集库、等保合规库、应用服务管理库、态势感知数据库、数据共享管理库等）及安全态势感知数据总线。

（4）数据采集层

数据采集层是态势感知安全平台统一的数据采集系统，支持多种数据采集方式，包括：第三方监测和情报的采集；安全检测和采集系统对本地数据的采集；通过人工录入方式对资产、等保、漏洞等信息的采集完善；通过数据总线与网络管理、运维管理、环境控制系统等现有系统集成对接。

（5）基础设施层

基础设施层是指为系统运行提供实体支撑的网络设备、安全设备、存储系统、终端设备、应用支撑中间件、工控设备等软硬件设施。同时包括机房、应急指挥室等内容。

（7）标准规范体系

标准规范体系是确保态势感知安全平台规范化的基础，包括但不限于业务标准、数据标准、技术标准等。

（8）安全保障体系

安全保障体系依托工信委现有安全保障体系，并结合态势感知安全平台自身安全等级保护合规性要求而建设的相关措施，包括安全技术体系和安全管理体系。

（9）运维保障体系

运维保障体系一方面依托工信委现有运维保障体系对本项目进行日常运维管理，另一方面要集成用户现有运维系统中的数据，在安全态势感知系统中集成展现。

## **关键技术路线**

引入大数据技术建立态势感知安全平台，收集网络、终端、系统、应用层等各层面数据，进一步挖掘与分析，为网络安全纵深防御、安全运营管理和应急提供支撑，并在此基础之上形成可视化的安全态势感知系统。

### **数据采集技术**

本次方案涉及到的数据是指通过不同方式获得的各种类型的结构化、半结构化（或称之为弱结构化）及非结构化的海量数据，是大数据知识服务模型的根本。重点是通过分布式的采集器实现高速高可靠数据采集、高速数据全映像等大数据收集技术；突破高速数据解析、转换与装载等大数据整合技术。

### **数据预处理技术**

主要完成对已接收数据的清洗、格式化等操作。

1. 清洗：对于数据，并不全是有价值的，有些数据并不是我们所关心的内容，而另一些数据则是完全错误的干扰项，因此要对数据通过过滤“去噪”从而提取出有效数据。
2. 格式化：因获取的数据可能具有多种结构和类型，数据抽取、格式化过程可以帮助我们将这些复杂的数据转化为单一的或者便于处理的构型，以达到快速分析处理的目的。

### **数据存储及管理技术**

数据存储与管理要用存储器把采集到的数据存储起来，建立相应的数据库，并进行管理和调用。重点解决复杂结构化、半结构化和非结构化大数据管理与处理技术。主要解决大数据的可存储、可表示、可处理、可靠性及有效传输等几个关键问题。

开发可靠的分布式文件系统（HDFS）、能效优化的存储、计算融入存储、大数据的去冗余及高效低成本的大数据存储技术；突破分布式非关系型大数据管理与处理技术，异构数据的数据融合技术，数据组织技术，研究大数据建模技术；突破大数据索引技术；突破大数据移动、备份、复制等技术；开发大数据可视化技术。

### **数据分析及挖掘技术**

数据分析引擎可采用Apache Spark ，Apache Spark是专为大规模数据处理而设计的快速通用的计算引擎。Spark是UC Berkeley AMP lab (加州大学伯克利分校的AMP实验室)所开源的类Hadoop MapReduce的通用并行框架，Spark，拥有Hadoop MapReduce所具有的优点；但不同于MapReduce的是Job中间输出结果可以保存在内存中，从而不再需要读写HDFS，因此Spark能更好地适用于数据挖掘与机器学习等需要迭代的MapReduce的算法。

数据挖掘是从大量的、不完全的、有噪声的、模糊的、随机的实际应用数据中，提取隐含在其中的、人们事先不知道的、但又是潜在有用的信息和知识的过程。数据挖掘涉及的技术方法很多，有多种分类法。根据挖掘任务可分为分类或预测模型发现、数据总结、聚类、关联规则发现、序列模式发现、依赖关系或依赖模型发现、异常和趋势发现等等；根据挖掘对象可分为关系数据库、面向对象数据库、空间数据库、时态数据库、文本数据源、多媒体数据库、异质数据库、遗产数据库以及环球网Web；根据挖掘方法分，可粗分为:机器学习方法、统计方法、神经网络方法和数据库方法。机器学习中，可细分为:归纳学习方法（决策树、规则归纳等）、基于范例学习、遗传算法等。统计方法中，可细分为:回归分析（多元回归、自回归等）、判别分析（贝叶斯判别、费歇尔判别、非参数判别等）、聚类分析（系统聚类、动态聚类等）、探索性分析（主元分析法、相关分析法等）等。神经网络方法中，可细分为:前向神经网络（BP算法等）、自组织神经网络（自组织特征映射、竞争学习等）等。数据库方法主要是多维数据分析或OLAP方法，另外还有面向属性的归纳方法。

### **数据存储查询技术**

针对本次项目，在设计建设过程中将采用ElasticSearch技术实现系统数据的存储和查询。ElasticSearch是一个基于Lucene构建的开源，分布式，RESTful搜索引擎;设计用于云计算；能够达到实时搜索，稳定，可靠，快速。相比其他技术，ElasticSearch技术具备如下优势：

* 横向可扩展性：只需要增加一台服务器，做一点儿配置，启动一下ES进程就可以并入集群；
* 分片机制提供更好的分布性：同一个索引分成多个分片（sharding），这点类似于HDFS的块机制；分而治之的方式来提升处理效率；
* 高可用：提供复制（replica）机制，一个分片可以设置多个复制，使得某台服务器宕机的情况下，集群仍旧可以照常运行，并会把由于服务器宕机丢失的复制恢复到其它可用节点上。

# **详细设计方案**

## **流量分析介绍**

随着系统的升级与漏洞的修补，入侵主机进而进行破坏的病毒攻击方式在攻击中所占比例逐渐减少，这些攻击转而改为恶意的消耗网络有限的资源或占用系统，进而破坏系统对外提供服务的能力；但传统的系统升级无法检测并预防此类攻击。针对此类攻击，我们以检测网络数据流的方法来判断网络异常和攻击：借助实时的检测网络数据流信息，通过与历史记录模式匹配（判断是否正常）、或者与异常模式匹配（判断是否被攻击），可以实时查看全网的状态，检测网络性能可能出现的瓶颈，并进行自动处理或告警显示，以保证网络高效、可靠地运转。

流量安全分析解决方案通过网络流量数据采集，利用大数据技术进行数据处理、存储和分析，进行海量数据的融合，提供网络链路全流量存储、全数据分析能力。借助全流量存储分析，安全分析人员可以对已经发生的攻击行为进行多角度、全方位、可反复回溯的深度检测，从而更容易检测出潜在的入侵行为，发现识别已知和未知的各种网络攻击。

流量安全分析为用户识别和发现失陷主机、木马通讯、APT攻击、web攻击等已知和未知的安全威胁，对网络攻击进行定位和取证。帮助安全分析人员从海量的数据中聚焦真正的入侵行为，通过追踪溯源和调查取证，发现攻击者或攻击组织，帮助用户提升安全分析能力和响应能力，最终降低安全损失。

## **流量数据采集**

### **流量协议还原**

基于分光流量的深度检测技术，支持针对网络流量协议的深层次解析功能，包括以下协议：包括HTTP、SMTP、POP3、IMAP、SMB、FTP等，支持的应用类型：网络邮件、博客、搜索引擎、微博、网盘、网络论坛、网络购物、视频、网页浏览、FTP、翻墙软件、网络游戏、木马事件、Telnet、QQ通信、P2P软件。系统提供二至七层全协议内容还原，并存储在大数据存储系统中作为后续数据挖掘分析的基础。

### **网络元数据日志采集**

流量安全分析支持多种网络元数据字段的提取、封装和上传。网络元数据是描述一次网络通信会话的数据，包含如通讯传输流信息即TCP/UDP会话的统计（主要字段有源目IP、源目端口、发送数据量、接收数据量、开始时间、结束时间、持续时间、平均包长等）、还有关键的元数据如HTTP关键字段，如user-agent、content-type、cookie、host、refer等等）、DNS协议关键解码字段信息、协议包头关键信息。

### **网络原始流量采集**

流量安全分析支持全量采集、索引网络原始流量，高级定向威胁在大规模网络流量中只会占到非常小的比例，因此如果无法在第一时间发现，往往需要通过事后的多线索关联和回溯分析后才能有效定性和取证，进而就必须对原始流量进行一段时间的完整保存以备事后的回溯分析。原始数据包保留攻击过程内所有数据信息，能够帮助安全人员追踪发现攻击者。

### **威胁情报采集**

大数据安全态势感知平台支持接入第三方情报入库进行关联分析。平台存储威胁情报通过及时跟踪和获取安全厂商、安全论坛、 应急响应组织、漏洞平台上的开源情报，再通过机器学习和人工确认进行过滤、分析和整理，最后生成机器可读的威胁情报。覆盖：APT 攻击报告、重大互联网泄密事件、重大安全 漏洞曝光事件、恶意文件、恶意 IP 以及恶意 URL等。可以通过在线更新和离线的方式提供给本地大数据安全态势感知平台。

### **IDS安全检测数据**

态势感知平台提供采集现有网络安全设备日志的数据接口，包括IDS入侵检测系统，支持Syslog和SNMP Trap的方式进行采集。

## **流量异常检测**

### **流量异常**

流量异常可能是资产被木马端控制，向外大量发送数据，或者资产账户被盗用，产生异常的使用行为。识别单个资产内网访问外网的异常流量数据，对单个资产刻画流量的行为基线，当资产上流量偏离基线，检测判断当前时刻是否发生流量异常事件。

### **上下行流量异常**

利用木马控制端和被控端命令交互阶段，上下行流量和上下行流量包不对称的特点，对上下行流量异常进行检测。通过对比分析上下行的通信流量，在正常的通信行为中，下行流量较高或基本相当（如P2P流量）,而窃密木马因为需要回传数据，在主动外联后，大多数时候上行的流量会比下行流量高。

### **间隙会话连接**

木马的被控端一般会主动、周期性地链接控制端，以更新状态、获取新的指令。木马被控端在与控制端建立连接后，双方为了保持这一会话，会向对方发送心跳包来表征自身的存活性。这种心跳信号的特征表现出一定的波动性，比正常网络通信信号在时频分析中表现更为平稳，对心跳间隙做时频分析，利用中频和高频系数的值域来检测是否存在木马间歇会话连接。

由于连接的周期和频率较为固定，间歇会话连接分析可以检测到主机的间歇性链接行为，从而发现木马被控端。

### **主动外联**

服务器一般不会主动发起对外的网络连接请求和域名请求行为，如果有主动外联行为的发生，可能是感染了恶意代码。单资产的流量行为，如内外网访问异常分析，分别以源地址、目的地址判断该资产是否出现访问异常。如果原本不会访问外网的目的资产出现在源地址方向，则可以发现该资产从内网访问外网，并且可以进一步检测该访问行为是否属于内网访问外网异常。

### **访问DGA域名**

异常域名检测技术主要用于发现僵尸网络或木马等恶意代码被控制端对其控制端服务器的动态域名请求行为，是依据特殊域名、特殊IP地址、请求次数突变、非池IP个数、特殊的非池IP段变化时间以及非池IP变化次数等异常特征对域名记录进行检测，发现异常域名。

通过对ISP的DNS流量进行检测与分析，发现感染主机为获取C&C服务器的IP地址，在域名请求行为上具有明显的组行为特征，即请求大量的新域名与失效域名。系统通过采集网络中主机的域名请求信息，将请求同一组新域名的主机集合作为检测对象，利用域名本身的字符特征，通过机器学习算法分类器对集合内主机请求的失效域名（域名解析中RCODE为“0X3，NXDOMAIN”）进行检测，有效地提取出恶意域名集合。

### **端口异常检测**

端口扫描是入侵的先兆，黑客一般是先通过扫描来确定用户系统的类型，然后针对性的进行攻击。平台具备识别端口扫描功能。

资产通讯所使用的端口和协议一般都是固定的，通过对历史数据进行长时间的学习，可以知道目标资产通常使用的是哪些端口，使用这些端口的时候走的是哪些协议，从而学习出资产端口的特性。当资产使用了非常用的端口，或者使用常用端口，但是却不走常用的协议，则认为存在异常。

### **隐蔽通道**

DNS隐蔽通道是指恶意软件在客户端与服务器端之间，绕过网络安全策略，通过合法DNS报文，进行数据传输的一种行为。攻击者向失陷主机传输恶意指令，对失陷主机进行控制，进行恶意操作，失陷主机向控制端传输数据，泄露用户隐私数据和情报。  
 隐蔽信息可能封装在请求报文的域名字段，TXT类型的应答报文中，因此异常DNS报文的各字段具有一定的特征。例如域名长度异常，域名字节分布异常，TXT类型报文量多等。提取各字段特征，使用随机森林模型，对报文进行分类，从而识别异常DNS报文，检测DNS隐蔽通道。

## **流量攻击检测**

### **主机失陷检测**

主机失陷检测通过十个异常检测模块：流量异常，上下行流量异常，端口异常，间隙会话连接，隐蔽通道，异常域名，主动外联，僵尸网络命中，安全事件，威胁情报命中。通过评分机制，判定资产主机失陷，可对失陷资产进行确认失陷操作，并将该操作结果作为标签，作为未来机器学习的数据。

### **蠕虫病毒检测分析**

网络蠕虫会对目标主机进行扫描，探测目标主机是否存在、是否活动、是否有操作系统或应用程序漏洞，然后决定如何进行渗透，由于网络蠕虫的目标是短时间内感染尽量多的目标系统，所以其传播过程，发送连接的请求时间间隔会很短，而正常主机访问外部网络时请求时间一般较长。建立分析模型通过流量样本数据进行训练，检测一段时间内的流量数据发现异常。

检测方式主要有以下几种：

1. 通过分析主机发送/接收数据包的数量来定位被感染的主机主动扫描网络中的主机，目的地址很多，产生大量的数据包，每秒发送大量数据包，但收到的回应很少。
2. 通过分析主机的会话对来定位被感染的主机会向很多主机发送连接请求，大多数通信对流量少。
3. 通过发包的异常目的来定位，很多发送的目的IP根本不存在或者没有被启用。

### **DDos攻击检测**

异常流量检测功能是通过自学习，根据网络流量的正常行为轮廓特征建立正常流量模型，如果检测到当前流量偏离了正常流量模型，则认为流量出现了异常，通过对采集到的原始流记录进行异常检测，可发现DDoS\_Syn\_flood、 DDoS\_udp\_flood、DDoS\_ack\_flood、DDoS\_ICMP\_flood。

* DDoS\_Syn\_flood

攻击者伪装大量的IP地址给服务器发送SYN报文，服务器将会维持一个庞大的等待列表，不停的重试回复SYN ACK报文，同时占用着大量的资源无法释放

* DDoS\_ack\_flood

TCP连接建立之后，所有的数据传输TCP[报文](https://baike.baidu.com/item/%E6%8A%A5%E6%96%87)都是带有ACK标志位的，[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "https://baike.baidu.com/item/_blank)在接收到一个带有ACK标志位的数据包的时候，需要检查该数据包是否合法。当发包速率很大的时候，[主机操作系统](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F" \t "https://baike.baidu.com/item/_blank)将耗费大量的精力接收[报文](https://baike.baidu.com/item/%E6%8A%A5%E6%96%87)、判断状态。攻击发生时，导致服务器丢失大量正常需要处理的数据包，系统资源不足等

* DDoS\_udp\_flood

当受害系统接收到一个 UDP 数据包的时候，它会确定目的端口正在等待中的应用程序。当它发现该端口中并不存在正在等待的应用程序，它就会产生一个目的地址无法连接的 ICMP 数据包发送给该伪造的源地址。如果向受害者[计算机端口](https://www.baidu.com/s?wd=%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%AB%AF%E5%8F%A3&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YLrHN9uHnvmHNbPHnYnWP-0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3En1Dvn1mznW6" \t "_blank)发送了足够多的 UDP 数据包的时候，整个系统就会瘫痪

* DDoS\_ICMP\_flood

采用多线程的方法一次性发送多个ICMP请求报文，让目标主机处理过程问题而速度缓慢或者宕机

### **高级入侵攻击检测**

#### 沙箱文件检测

对网路攻击分析和恶意文件分析检测不出的未知威胁，系统可以制定策略将采集的文件或者请求操作放到动态虚拟沙箱中进行实时模拟，并生成文件行为报告供用户进行确定APT攻击的参考。

无论是 0day 或者精心构造的恶意程序，传统的基于特征库的被动防御体系都无法抵御定向攻击的入侵。这些高级定向攻击（APT）通过钓鱼邮件，发送带有恶意程序的附件。通过水坑攻击，如熟人给企业内部的员工发送具有针对性的恶意链接，诱骗用户访问这个链接之后并入侵内网终端。

动态行为安全沙箱能够对多个仿真的虚拟机环境，还原邮件（SMTP,POP3,IMAP和Webmail）附件和FTP，HTTP传输的文件，进行可疑行为检测，将生成行为报告，报告中包括文件在沙箱中的注册表行为，文件操作，网络行为，互斥锁操作等。根据这些行为，利用算法模型来计算这些样本文件的行为是否异常行为，从而判断文件是否携带未知恶意代码。

系统使用多种虚拟机环境运行被检测文件，检测文件打开后的各种行为和系统环境等以确定文件是否具有恶意行为。动态检测的优点是检测率高、误报率低。

动态检测能在很大程度上克服静态检测的通过代码混淆，压缩加密等方式便被绕过的特点，直接把样本放到真实环境中模拟运行，并观察样本的恶意行为。当样本存在可疑漏洞利用行为、可疑文件动作行为以及可疑网络行为时则报警提示给用户。

#### 恶意文件基因检测

恶意文件基因检测，通过恶意代码的基因提取，自动提取样本数据，对深度学习的模型进行样本训练，进行基因分析，判断是否为恶意文件。文件行为分析，通过软件基因的沙箱规则支持反逃逸技术，并可以生成恶意文件行为阶段的报告。

知识图谱能够进行应用识别、恶意文件的行为提取，并进一步结合黑客组织的特征，形成关联知识图谱。

根据安全告警事件还原攻击链，提供外部威胁情报获取关于外网IP的各类信息，并通过可视化技术进行呈现。

#### 病毒文件检测

基于FTP、HTTP、POP3、SMTP等协议进行文件重组，识别恶意软件和未知威胁，可以通过防病毒引擎进行文件病毒查杀。

### **IDS安全检测**

IDS入侵检测能够实时检测网络入侵，自动检测可疑行为，分析来自网络外部和内部的入侵信号。IDS检测包括网络攻击、木马检测-基于网络特征的木马检测、端口扫描、DDOS攻击、Sql注入、异常流量、恶意文件检测、蠕虫病毒等。全流量分析采集IDS上报的安全事件，可在溯源分析时作为取证分析的支撑。

### **Web攻击**

从数据链路层、网络层、传输层和应用层逐层拆封数据报文，解析协议头部中的 IP 地址信息、访问路径，请求参数等，获取每一条网络行为的审计信息。模拟各种web 攻击提取训练样本库，或通过运维工程师确认后web攻击事件（Sql注入攻击/恶意代码注入等）作为训练数据样本建立机器学习分析模型。利用机器学习识别web攻击，提高准确性，通过分析请求URL参数特征、参数内容，基于机器学习样本库直接检测web应用层攻击，SQL注入攻击及XSS攻击。

监测日常流量数据，当模型的输出结果为非正常时，输出告警事件。

## **流量监控分析**

对网络关键的链路进行日常网络流量评估分析目的是对网络关键链路的运行情况进行评估，包括网络的基本运行情况、影响网络的用户和应用情况、异常网络行为情况、关键应用服务的运行情况。

### **网络链路利用率分析**

网络链路利用率是一段时间内网络中实际网络流量同网络理论最大传输流量的比率，代表拥塞程度。通过对网络链路利用率的分析，能够找到网络瓶颈从而提升网络性能，并根据应用和用户进行带宽的分配与监控，更好管理资源配置网络，合理使用带宽资源。

### **流量统计分析**

#### 链路利用率异常分析

通过对网络链路利用率的监控，对单个资产刻画网络链路利用率的基线，统计流量进出计算利用率。如果利用率在某一天出现严重长时间违背正常流量规律的现象，判断是否发生链路利用率基线异常。

#### TOPN分析

TOPN分析通过多维度的统计方式，掌控用户网络中资产实时流量情况，并针对发生流量异常的资产及时进行处理。TOPN分析统计主要监测：

* 网络总流量最大的资产
* 分协议统计流量最大的资产（主要统计HTTP和UDP）
* 统计发现发包数最多的资产
* 统计发现连接数(会话数)最大的主机

#### 流量基线分析

对不同目标对象的流量基线进行拟合，实现自适应的异常流量发现。可细至单个IP的特定端口、特定协议，特定应用的流量基线，也能够对全网安全域间的整体流量进行基线学习，并且模型可调整。

从上下行流量大小、协议、连接次数等维度建立整体和单个资产的流量基线。检测的方法包括：

* 分类过滤：不同标准将流量分类，过滤出重点部分分析
* 统计分析：对数据流量按照设定的标准进行统计；基于历史数据建立不同属性的安全基线
* TOP排序：对流量率、发包速率、流速率或者流量、发包数、流数进行排序
* 模式匹配：根据已有的异常数据库的规则，对特定的流属性进行匹配，常用的匹配类型包括特定端口匹配、IANA保留IP地址匹配、特定IP地址匹配等

### **连接关系分析**

连接关系分析能够直观的看出资产访问其他IP的流量情况，访问IP的数量和流量大小。例如两台主机一段时间内会话情况也能通过会话时序图进行直观展示。

系统支持按一段时间内进行统计源IP、目的IP之间的流量大小，构成IP视网膜图，表达源IP到目的IP连接的次数和流量的大小，当流量越大时，源IP到目的IP的宽度则越宽。

### **数据包数量监控分析**

网络中传输的数据包的大小是不一样的，IP包最小为40字节，最大为1500字节。以太网的帧最小为64节，最大为1518节（包含4字节的CRC）。通常来说网络中的最大包和最小包最多，这是因为网络中应用最多的协议TCP/IP的实际传输情况造成的(TCP的SYC、SYC ACK、Acknowledgement、RST、FIN)等包都是小包，而在数据传输时都是大包。某些攻击（比如syn flood）会发出大量小包，正常大包与小包的比率基本相同，通过对数据包的监控能够识别攻击。

### **网络连接分析**

网络连接分析能够监测出当前网络的健康状态，也可能识别出一些异常情况。分析的内容包括统计资产的网络连接总数，每个端口的协议和连接数，识别出半连接（TCP三次握手不完整），统计资产拒绝连接数和尝试连接的端口，统计资产的TCP连接重传数和数据包数量。

### **应用处理请求与响应分析**

针对应用安全，从业务应用的功能角度出发进行分析。当业务系统遭受攻击时，业务功能可能出现异常，功能的检测可以从访问、响应和流量等方面进行分析。通过统计业务应用每个功能的响应时间和流量情况，建立业务功能基线，当业务行为超过基线时进行告警。

## **威胁情报**

威胁库中的威胁信息可在关联规则中引用，用于发现对企业的高级持续性攻击，通过订阅外部情报中心的外部威胁库：恶意域名、恶意IP库、恶意URL库、恶意病毒库，可以带来如下价值：

* 发现新的安全事件
* 确认安全事件的准确性
* 扩大分析范围：实时调用外部情报中心的分析引擎，分析恶意IP和恶意域名，发现僵尸网络中其他的IP，与企业内部信息关联，发现企业内部范围内其他可能感染的IP
* 通过结合外部情报，分析内部和外部整个攻击路径

## **追踪溯源**

### **溯源分析**

确认攻击事件后，按事件线索汇总所有分析的结果，按时间顺序、网络拓扑路径、网络连接访问路径进行攻击路径还原，进入还原黑客整个攻击行为。系统也提供原始流量包供取证使用。

在告警发生后，通过追踪溯源系统，结合完整的原始流量包数据进行取证分析，还原完整攻击过程，并且能够分析攻击在内部的影响范围，并关联相关的业务系统，及时发现业务系统存在的安全隐患。对流量行为分析和溯源，从海量数据中定位准确的数据，为用户提供安全响应与分析能力。通过追踪外网攻击者或黑客组织，帮助企业或政府单位采取有效的防范措施，保障网络空间安全。

## **原始流量包采集**

### **采集策略**

流量采集策略可按照方案需求进行配置，分为按核心资产采集和告警事件采集，并对采集的流量进行存储，支撑后续溯源分析。

### **资产流量采集策略**

核心资产通常部署有核心业务系统，支撑企业或政府单位正常运转，因此保障核心资产的安全是安全工作的重中之重。对核心资产上的流量进行全量采集存储，通过流量异常检测，及时发现资产安全问题，保障核心业务系统安全。同时，在告警发生后，通过追踪溯源系统，结合完整的原始流量包数据进行取证分析，还原完整攻击过程，并且能够分析攻击在内部的影响范围，追踪外网攻击者或黑客组织，帮助企业或政府单位采取有效的防范措施，保障网络空间安全。

### **告警采集策略**

在告警发生后，采集探针会对告警前后一段时间内流量进行存储，通过追踪溯源系统，结合采集到告警发生前后一段时间内的原始流量包数据进行取证分析，还原完整攻击过程，并且能够分析攻击在内部的影响范围，追踪外网攻击者或黑客组织，帮助企业或政府单位采取有效的防范措施，保障网络空间安全。

## **态势感知可视化**

态势感知是一种动态实时的网络安全分析与可视化技术，对存在的主要安全威胁和攻击事件进行检测，利用大数据分析方法对各种安全信息进行深层次关联融合，以攻防的视角，从整体安全态势、攻击态势、资产安全态势、数据泄露安全态势、流量态势、恶意域名访问态势等维度进行立体化深入分析，从而实现对大型系统网络安全状况动态实时分析，也为大型信息系统安全运维管理提供整体安全视图，并对安全状况发展趋势进行预测。

## **安全事件应急处置**

系统针对信息安全事件的应急响应、处理流程进行综合管理，对各方资源的有效整合、集中管理、集中监控、集中维护，实现应急预案数字化管理、实时应急调度、应急过程全程追踪及应急事件库同步更新等应用，最终建立统一指挥、功能完善、反应灵敏、协调有序、运转高效的应急机制，预防和妥善应对信息安全突发事件。

现有的安全系统或者安全管理平台要发挥应有的作用，必要的、贴合组织架构的工作流程必不可少，运维流程要遵循ITIL规范，符合等级保护管理和ISO27001要求中对于安全运维的相关要求。考虑安全运维的特点，结合实际工作需要，系统内置以下运维流程：

* 安全事件处理流程
* 安全知识库管理流程
* 安全问题管理流程
* 漏洞评估处理流程
* 安全事件应急响应流程
* 通报流程
* 安全作业计划流程

## **基础安全运维门户系统**

作为态势感知平台的基础管理支撑，负责用户管理、角色管理、权限控制、门户定义、资产管理、业务管理、日志范式化库、事件告警管理、各种策略管理、各种统计分析报表以及整个平台组件的监控管理等等。

### **资产网络拓扑**

系统应提供资产网络拓扑，帮助用户对资产进行管理和运维。

### **新增资产发现**

资产自动发现是很多企业和单位安全运维和管理中必不可少的需求，资产自动发现能够帮助运维人员快速了解企业或单位当前的资产总体情况，便于管理、配置和运维。运维人员以往需要花费大量时间精力进行逐一对企业内资产进行排查，不但浪费人力物力，而且可能会有遗漏和错误。

本方案使用流量检测手段发现网络内新资产，通过采集流量数据进行流量解析，对源IP符合生产网公网网段条件，且不存在于资产库则直接发出告警。同时，对目的IP与资产库进行比对，如果不存在于资产库且符合生产网公网地址网段条件，发现新增未知资产。运维人员可对自动发现的资产在管理中心内添加必要的资产信息，便于日后维护和管理，极大提高了管理工作效率。

### **资产管理**

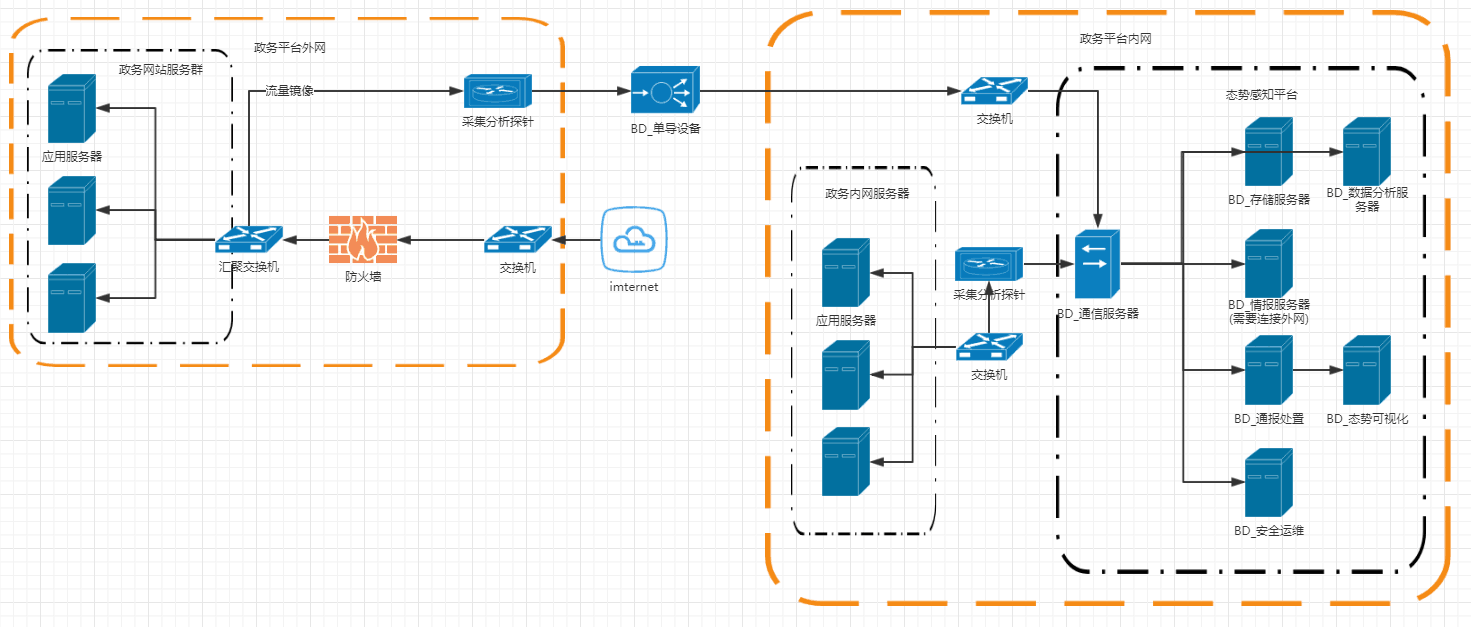
网络拓扑功能显示了整个网络拓扑结构，包括资产价值，风险等级，威胁等级，漏洞等级，发起攻击总数，受攻击总数。

### **运维支撑**

本系统完全采用分布式架构，多个独立进程组件，为了便于后期维护，提供所有组件的性能监控页面，及时定位问题。

# **部署方案**

## 系统部署

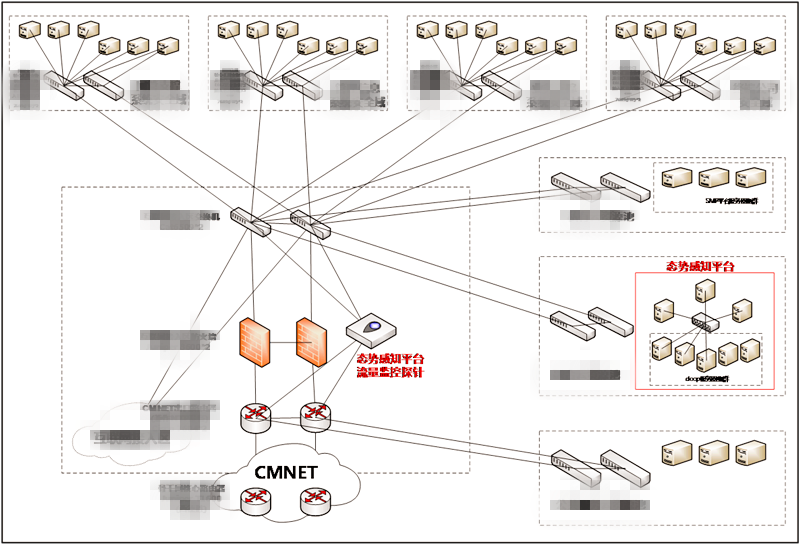


# **案例分析**

## **某运营商基地**

**行业背景**

在安全形势不断恶化的今天，运营商承载中国网络的基础资源，从网络安全和信息安全，经常会面临来自互联网的攻击威胁，虽然运营商组织中均设立信息和网络安全相关部门，并且安全管理人员已经在网络中的各个位置部署了大量的安全设备， 但仍然会有部分威胁绕过所有防护直达运营商内部，对重要数据资产造成泄漏、损坏或篡改等严重损失。因此需要在其网络中部署威胁感知产品，及时发现潜藏在其网络中的安全威胁，对威胁的恶意行为实现早期的快速发现，对受害目标及攻击源头进行精准定位，对入侵途径及攻击者背景的研判与溯源，从源头上解决网络与信息系统中的安全问题，尽可能地减少安全威胁对运营商带来的损失。



**用户需求**

* 发现自身网络安全威胁
* 发现未知威胁
* 异常流量分析
* 网络攻击安全回溯分析

**解决方案**

在运营商基地部署一套蓝盾态势感知系统，实现：

1.网络入侵安全态势感知预警功能，用大数据安全分析技术，将海量安全攻击日志转化为少数攻击事件，并将攻击事件以攻击链的形式展示。

2.异常流量安全态势感知预警功能，利用全流量分析技术，基于成熟的异常流量检测技术，实现拒绝服务安全预警动态检测。

3.僵木蠕传播安全态势感知预警功能，利用网络流量监控等手段发现僵木蠕传播、并实现僵尸网络发现、打击、效果评估。

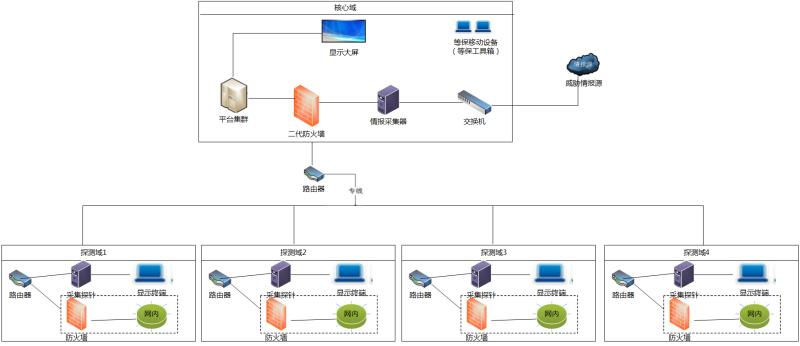
4.系统漏洞安全态势感知预警功能，对暴露在互联网上的信息系统漏洞情况进行评估，结合网络安全等级保护测评漏洞数据，全面评估各类信息系统漏洞情况，有针对性的对系统漏洞安全态势感知预警。

5.大屏展示功能，能够呈现整体综合分析态势、风险态势、资产态势、数据态势、系统管理、等保测评等。

## **某省广播电视安全调度指挥中心**

**行业背景**

新一轮信息技术革命正在向智能化、智慧化方向发展，大数据、云计算、物联网、移动互联和人工智能技术都在引发“智慧浪潮”。在信息技术和社会生活融合度越来越高的当今时代，广播影视不应仅是信息的生产者、传播者，更应成为新的生活方式发起者、组织者、提供者，应成为未来社会生活的中心枢纽之一。为贯彻落实《网络安全法》，按照总局《新闻出版广播影视网络安全管理办法（试行）》和《新闻出版广播影视网络安全事件应急预案（试行）》的要求，省局安全播出调度指挥中心计划建设省新闻出版广播影视网络安全态势感知预警平台项目。



**用户需求**

* 核心域、探测域多级部署
* 结构模块化，层级设计理念
* 网络入侵检测
* 异常流量分析
* 网络攻击安全回溯分析

**解决方案**

在广电信息中心部署一套蓝盾态势感知系统，实现：

1.网络入侵安全态势感知预警功能，用大数据安全分析技术，将海量安全攻击日志转化为少数攻击事件，并将攻击事件以攻击链的形式展示。

2.异常流量安全态势感知预警功能，利用全流量分析技术，基于成熟的异常流量检测技术，实现拒绝服务安全预警动态检测。

3.僵木蠕传播安全态势感知预警功能，利用网络流量监控等手段发现僵木蠕传播、并实现僵尸网络发现、打击、效果评估。

4.系统漏洞安全态势感知预警功能，对暴露在互联网上的信息系统漏洞情况进行评估，结合网络安全等级保护测评漏洞数据，全面评估各类信息系统漏洞情况，有针对性的对系统漏洞安全态势感知预警。

5.大屏展示功能，能够呈现整体综合分析态势、风险态势、资产态势、数据态势、系统管理、等保测评等。