ICS 33.040
CCS M 10

YD

中华人民共和国通信行业标准

YD/T XXXXX—XXXX

5G 网络安全态势感知系统技术要求

Technical specification of network security situational awareness system for 5G

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国联合网络通信集团有限公司、中兴通讯股份有限公司、中国信息通信研究院、华为技术有限公司、中国移动通信集团有限公司、杭州安恒信息技术股份有限公司、北京东方通网信科技有限公司、北京天融信网络安全技术有限公司、恒安嘉新（北京）科技股份公司、北京奇虎科技有限公司、新华三技术有限公司、北京神州绿盟科技有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：谢泽铖，张曼君，徐雷，田甜，王静，姚戈，王蕴实，马苏安，成黎，贺倩，吴荣，李科，韩科科，张峰，于乐，马禹昇，李剑锋，崔婷婷，陈乔，赵开勇，王龑，庞韶敏，李蓉，张屹，万晓兰，周慧芳，刘献伦，刘为华。

5G 网络安全态势感知系统技术要求

1 范围

本文件规定了 5G 网络安全态势感知系统的技术要求，主要包括 5G 网络安全态势感知系统的技术框架、功能要求、安全要求等。

本文件适用于基础电信运营企业的 5G 网络安全态势感知系统的设计与开发等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件。不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069	信息安全技术 术语
GB/T 32924	信息安全技术 网络安全预警指南
GB/T 35273	信息安全技术 个人信息安全规范
GB/T 36635	信息安全技术 网络安全监测基本要求与实施指南
GB/T 37027	信息安全技术 网络攻击定义及描述规范
YD/T 3734	基础电信企业网络安全态势感知系统技术要求
YD/T XXXX	电信网和互联网网络安全态势感知系统安全要求

3 术语和定义

GB/T 25069、GB/T 32924、GB/T 36635、GB/T 37027 和 YD/T 3734 界定的以及下列术语和定义适用于本文件。

3.1

网络安全态势感知 network security situation awareness

通过采集网络流量、资产信息、日志、漏洞信息、用户行为、威胁信息等数据，分析网络行为及用户行为等因素构成的安全状态和变化趋势，获取、理解、回溯、显示能够引起网络态势变化的安全要素，预测网络安全态势发展趋势。

3.2

前端数据源 front-end data source

向网络安全态势感知核心组件提供数据的软硬件，包括部件、代理或设备。

4 缩略语

下列缩略语适用于本文件。

5G	第 5 代移动通信网络	5th Generation network
API	应用程序接口	Application Programming Interface
ARP	地址解析协议	Address Resolution Protocol

DOS	拒绝服务攻击	Denial of Service
EMS	网元管理系统	Element Management System
FTP	文件传输协议	FileTransfer Protocol
GNSS	全球导航卫星系统	Global Navigation Satellite System
GTP	GPRS 隧道协议	GPRS Tunnelling Protocol
HDFS	分布式文件系统	Hadoop Distributed File System
IDS	入侵检测系统	Intrusion Detection System
IP	网际互连协议	Internet Protocol
IPS	入侵防御系统	Intrusion Prevention System
JDBC	Java 数据库连接	Java Database Connectivity
MEC	移动边缘计算	Mobile Edge Computing
ODBC	开放数据库连接	Open Database Connectivity
PFCP	报文转发控制协议	Packet Forwarding Control Protocol
RAN	无线接入网	Radio Acess Network
REST	表述性状态转移	Representational State Transfer
SFTP	安全文件传输协议	Secure FTP
SNMP	简单网络管理协议	Simple Network Management Protocol
SQL	结构化查询语言数据库	Structured Query Language server database
NoSQL	非结构化查询语言数据库	No Structured Query Language server database
WAF	Web 应用防护系统	Web Application Firewall
WEB	全球广域网	World Wide Web
XDR	详细记录	X Detailed Record

5 5G 网络安全态势感知系统技术框架

5.1 建设原则

5G网络安全态势感知系统应遵循以下建设原则：

a) 数据汇总原则：可覆盖5G网络流量数据、资产数据、日志数据、运维用户行为数据、恶意程序事件、网络攻击事件、安全告警数据、漏洞信息、威胁情报等相关安全数据的全面采集，使安全数据可以反映出各个时段、各个安全层面、关键设备的安全态势情况。

b) 高质量存储原则：针对大数据技术特点，所采集数据原则上保留原始数据，同时按数据使用需求进行脱敏、加解密处理；按数据内容进行标准化、标签化处理；按数据分析需要进行批处理分析、实时分析、全文检索、数据库查询等需要进行存储。各个处理环节均需要保证完整性与准确性。

c) 场景可扩展原则：基于全量高质量的安全数据，系统具备针对5G网络及业务特点进行多种场景的安全分析能力伸缩性，最终实现对安全威胁情况的准确把握与预警。

5.2 系统框架

5G 网络安全态势感知系统面向 5G 网络的业务场景，提供网络安全态势感知分析及展示能力，其表现形式可为产品、系统或平台，也可以是不同的功能组件，主要实现数据管理、安全分析、安全评估、安全态势预警及处置、可视化展示等功能。为保证 5G 网络安全态势感知系统的功能完整性，本文件给出了 5G 网络安全态势感知系统的技术框架，如图 1 所示。

5G 网络安全态势感知系统从流量采集探针、资产安全管理平台、日志平台、安全设备等采集数据，

并与公共漏洞发布平台等对接获取漏洞和威胁情报；数据管理包括数据收集、数据处理、数据存储三方面的内容；5G 网络的脆弱性分析包括漏洞分析、配置合规分析、弱口令分析等；结合 5G 网络的具体架构和场景，5G 网络安全分析包括 5G RAN 安全分析、5G 承载 IP 网安全分析、5G MEC 安全分析、5G 云化核心网安全分析、运维操作行为分析；建立评估模型和评估指标对 5G 网络进行安全评估；安全态势预警及处置包括安全态势预警、应急处置、安全威胁溯源、检索查询；可采用多种视图展示 5G 网络的整体安全态势、专题安全态势、区域安全态势；同时从标识与鉴别、访问控制、通信安全、安全审计、数据保护、系统升级等方面保障 5G 网络安全态势感知系统的安全可靠。

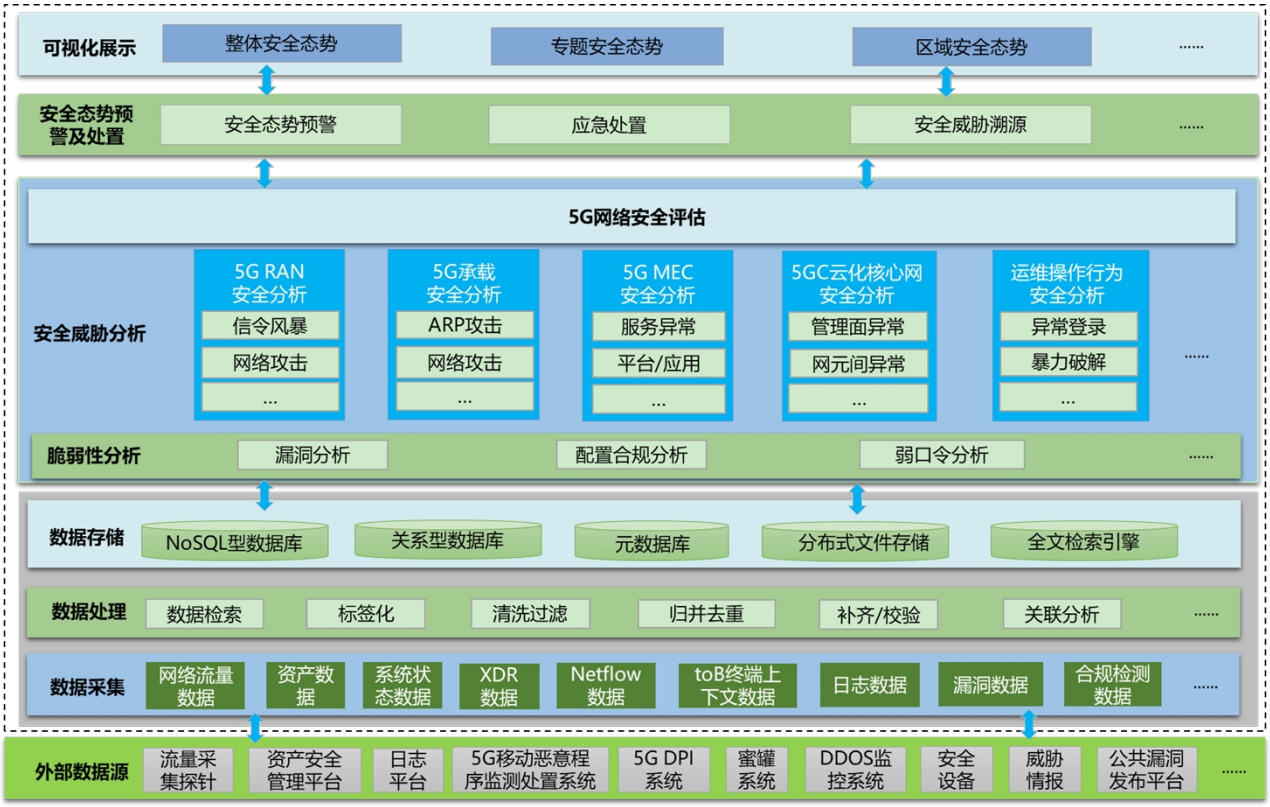

图 1 5G 网络安全态势感知系统框架

5.3 技术架构

5G 网络态势感知系统应结合 5G 网络的组网特点，支持各种网络域的安全态势分析及综合态势呈现。根据 5G 网络态势感知系统的具体功能需求、作用对象以及 5G 网络的架构特点，5G 网络安全态势感知系统的参考技术架构如图 2 所示，覆盖从设备级到网络级的安全态势分析和呈现。不同于图 1 的系统框架，图 2 从 5G 组网角度呈现系统的技术架构，分为端点/网元态势感知、单域态势感知、全网态势感知三层架构，其中端点/网元层主要向上提供基础分析数据，同时响应下发的策略；单域态势感知层包括对 5G 资产的脆弱性管理以及针对 5G RAN、5G 承载 IP 网、5G MEC、5G 核心网、运维操作的安全分析检测，并协同处理响应策略；全网态势感知层进行威胁情报管理、态势的呈现、安全资产管理、全网事件关联分析、安全态势预警、安全威胁溯源等。

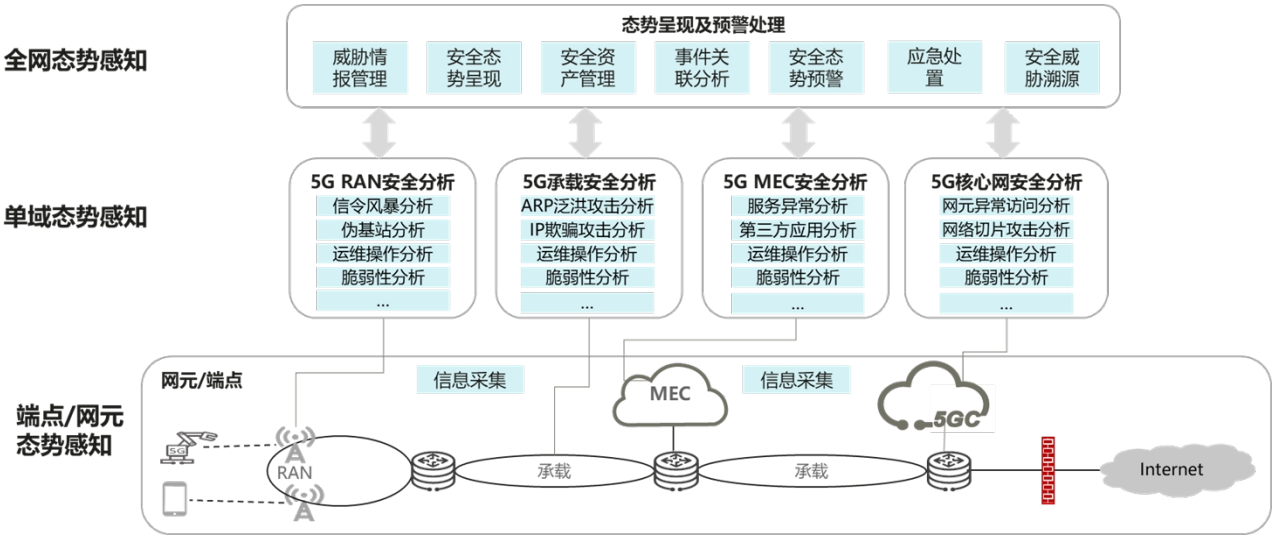

图 2 5G 网络安全态势感知系统参考技术架构

6 5G 网络安全态势感知系统功能要求

6.1 数据管理要求

5G 网络安全态势感知系统应满足数据收集、数据处理和数据存储三个方面的数据管理要求。数据收集应支持多源数据和多种方式的采集能力。数据处理应满足支持多源数据的抽取、转换、清洗、标准化等。数据存储应支持多源数据的原始数据、处理后数据等数据的存储，支持多种数据类型的存储。

6.1.1 数据收集要求

6.1.1.1 数据收集内容

5G 网络安全态势感知系统应支持以下至少一种或多种 5G 网络安全数据的采集，本项要求包括：

a) 资产数据：应支持采集 5G 网络中各类网络资产，包括不限于网络切片、网元、虚拟机、物理机、网络设备、安全设备、网管系统、应用软件、系统账号等；

b) 系统状态数据：对于物理机、虚拟机，系统应支持采集系统当前进程、开放端口等数据以及网络设备和安全设备的版本信息和配置信息等；

c) 网络流量数据：应支持采集 5G 网络流量，包括控制面流量、用户面流量和管理面流量。如 Uu、N4、EMS 等接口或系统的流量。

d) XDR 数据：XDR 包含 5G 信令过程记录和用户面业务记录，分为控制面和用户面数据，系统应支持这两类 XDR 数据的采集；

e) Netflow 数据：Netflow 数据包含流的属性和统计信息，系统应支持从网络设备采集 netflow 数据；

f) 日志数据：应支持各种日志的采集，包括从防火墙、IPS/IDS、WAF 等安全设备采集的告警数据和日志数据，从主机、网元采集的系统日志，从数据库、中间件、Web 应用采集的应用日志，从 5G RAN、承载网、核心网等管理维护系统采集的告警日志、操作日志等；

g) 漏洞数据：应支持从公共漏洞发布平台采集漏洞信息，以及应支持从漏洞扫描系统采集漏洞扫描数据，包括漏洞名称、级别、编号、扫描对象等；

h) 合规检测数据：应支持采集合规检测数据，包括操作系统、数据库、中间件、网络设备等各类资产的安全配置核查结果等；

i） 其它系统数据：应支持与其他系统对接采集相关数据，包括5G网络中存在的分区域/分子域/分专题的其它态势感知系统、资产安全管理平台、配置安全管理平台等。

6.1.1.2 数据收集方式

针对不同数据源，系统应支持多种采集方式，本项要求包括：

a） 应支持主动收集方式：系统应能通过FTP/SFTP、RESTful、Web Service、SNMP、JDBC/ODBC等方式以及部署程序探针等方式主动从数据源采集数据；系统应能配置采集任务，设置任务采集周期，监控采集任务的运行状态；系统应能配置数据源的认证方式和认证参数；

b） 应支持被动收集方式：系统应支持通过如Syslog、Netflow、Kafka消息队列等协议接收前端数据源的数据；

c） 应支持文件导入方式：系统应支持通过本地文件上传等方式将数据导入到系统。

6.1.2 数据预处理要求

系统应支持将采集到的数据进行过滤、抽取、转换、清洗、标准化等处理，以满足数据质量的要求，本项要求包括：

a） 应支持对采集数据进行完整性和准确性校验，去除不完整和错误的数据；

b） 应支持对数据进行清洗过滤、去重合并，对不同来源的相同数据进行去重合并，减少数据冗余；

c） 应支持对数据标准化处理，对不同来源的原始数据进行统一格式化处理，支持将个别、特殊的日志处理为一般信息，便于后续存储、分析；

d） 应支持将数据标签化，结合数据所属业务系统、设备类型等信息，在原数据基础上进行标记；

e） 应支持通过数据挖掘技术对于不同类型的数据进行关联分析，利用数据源之间存在的关联性，以及威胁情报信息，进行数据融合、碰撞和分析；

f） 应支持实时处理和离线处理，支持批量处理操作。

6.1.3 数据存储要求

本项要求包括：

a） 应支持结构化数据、半结构化数据和非结构化数据等多种数据类型的存储能力；

b） 应支持的存储类型包括关系型数据库（如Oracle、MySQL）、NoSQL型数据库（如HBase、Cassandra、Redis）及分布式文件存储系统（如HDFS）、索引存储等；

c） 应保证存储数据的可用性、完整性和机密性，如采用数据存储加解密、数据备份恢复、存储访问控制及安全审计等措施；

d） 应支持数据存储半年以上，并支持存储周期的扩展，满足合规要求；

e） 应支持对数据的读写进行分级分权管理；

f） 应支持定期备份、故障恢复机制。

6.2 安全分析要求

6.2.1 5G网络脆弱性分析

5G网络安全态势感知系统应对5G网络部署范围内的资产（如网络产品、安全产品、服务应用、系统软件、支撑系统等）进行脆弱性分析，以识别网络中的薄弱点。5G网络脆弱性分析包括但不限于漏洞分析、配置合规性分析、弱口令分析等，本项要求包括：

a） 漏洞分析
   1） 应支持资产漏洞波及情况分析，包括资产存在的漏洞以及漏洞影响的资产范围；
   2） 应支持对主机操作系统、数据库、网络设备操作系统、应用、中间件、系统软件等资产的漏洞检测结果进行分析；
   3） 应支持按时间区间、漏洞等级、漏洞类型等维度统计分析存在漏洞利用风险的资产数据；
b） 配置合规分析
   1） 应支持对无线基站、承载网网元、核心网网元、网管设备等网络设备的配置合规情况进行核查；
   2） 应支持对操作系统、数据库、中间件等的配置合规情况进行核查；
   3） 应支持对资产存在的配置不合规项进行统计分析；
   4） 应支持按时间、违规类型等维度统计分析配置不合规的资产情况；
c） 弱口令分析
   1） 应支持对操作系统、数据库、中间件等的弱口令情况进行分析；
   2） 应支持对资产存在的弱口令项进行统计分析；
   3） 应支持按时间维度统计分析存在弱口令的资产情况；
d） 应支持基于上述资产脆弱性因素支持对资产整体脆弱性进行评估，提供具体资产的脆弱性等级、脆弱性修复优先级。

6.2.2 5G 网络安全检测与分析

6.2.2.1 5G RAN 安全检测与分析

本项要求包括：

a） 应支持对无线侧发起的信令风暴进行检测和分析的能力；
b） 应支持对 5G 基站工作范围内发射无线信号的伪基站攻击进行检测和分析的能力；
c） 应支持 GNSS 伪造信号的检测和分析的能力。

6.2.2.2 5G 承载 IP 网安全检测与分析

本项要求包括：

a) 应支持对 ARP 泛洪攻击进行检测和分析的能力；
b) 应支持对 ARP 欺骗攻击进行检测和分析的能力；
c) 应支持对 IP 欺骗攻击进行检测和分析的能力；
d) 应支持对 IP 畸形报文攻击进行检测和分析的能力。

6.2.2.3 5G MEC 安全检测与分析

本项要求包括：

a） 应支持对 MEC 用户面流量攻击进行检测和分析的能力，如对 N6 接口的流量分析；
b） 应支持对 MEC 服务异常攻击进行检测和分析的能力，如攻击者利用 MEC 服务与核心网之间的信令，在 MEC 侧对核心网进行的攻击；
c） 应支持利用第三方应用进行攻击的检测和分析的能力，如第三方应用利用服务的 API 接口对 MEC 服务进行的攻击及其他异常及恶意行为；
d） 应支持针对 MEC 平台的攻击进行检测和分析的能力，如攻击者利用软硬件漏洞对 MEC 平台及系统进行的攻击；
e） 应支持对 MEC 行业终端异常进行检测和分析的能力，如攻击者通过非法替换、冒用、刷机 MEC 终端等手段对 MEC 及核心网进行的攻击。

6.2.2.4 5G 云化核心网安全分析

本项要求包括：

a) 应支持对重放攻击、畸形报文攻击、N4 接口信令风暴、N4 接口异常协议（如非 PFCP 数据）、GTP 攻击等进行检测和分析的能力；
b) 应支持对网元间异常访问和非法服务注册进行检测和分析的能力，如网元的非法访问及嗅探行为；
c) 应支持对网元间异常流量进行检测和分析的能力，如网元间出现与业务相悖的协议类型、出现非法异常流量；
d) 应支持对网络切片攻击进行检测和分析的能力，包括尝试注册到非授权切片，通过漏洞、网络攻击等行为非法访问未授权切片，窃取数据或干扰业务正常运行；恶意消耗切片资源等；
e) 应支持对开放接口异常进行检测和分析的能力，如利用开放接口进行 DoS 攻击、Web 攻击、漏洞利用等；
f) 应支持对东西向流量异常进行检测和分析的能力，如利用云平台虚拟机之间、容器之间的流量交互进行横向攻击；
g) 应支持对虚拟化平台攻击进行检测和分析的能力，如篡改 Hypervisor、主机内核/模块/服务等；受感染的虚拟机访问无权访问的邻居虚拟机资源；虚拟机利用漏洞逃逸获得未授权的权限。

6.2.2.5 运维操作行为分析

本项要求包括：

a) 应支持对用户行为异常进行检测和分析的能力，如高危操作、用户操作习惯异常，包括登录时间、登录次数、操作内容等异常；
b) 应支持对异常登录进行检测和分析的能力，如未授权访问、同一账号同一时间多个 IP 登录，账号非常规时间非授权 IP 的异常登录等；
c) 应支持对越权访问进行检测和分析的能力，如尝试非授权操作、访问非授权数据、基于系统漏洞等方式进行越权操作；
d) 应支持对用户名/口令猜测、暴力破解进行检测和分析的能力，如多次尝试用户名和口令登录等异常行为。

6.3 安全评估要求

本项要求包括：

a) 应支持对各种网络攻击建立相应的识别模型和安全评估模型；
b) 应当建立安全态势评估指标体系，根据安全分析的结果，通过模型计算、预测的安全风险等各个要素和态势信息进行安全态势评估；
c) 评估态势应至少包含综合态势、资产安全态势、切片安全态势、脆弱性态势、攻击态势、5G 不同网络域的安全态势等方面；
d) 应支持对攻击可能造成的影响进行安全评估，包括但不限于将要造成的威胁和破坏程度。

6.4 安全态势预警及处置要求

6.4.1 安全态势预警

本项要求包括：

a) 应具备安全威胁预警能力，能够对全网的安全趋势、潜在的安全风险、网络攻击态势进行趋势

分析和预警，包括攻击源、攻击目标、攻击类型、攻击时间段等；

b) 预警内容应至少包括预警级别及其事件性质、威胁方式、影响范围、涉及对象、影响程度、防范对策等信息等；

c) 应具备将各种异常行为按风险程度进行分级的能力，并按照风险等级、发生风险区域进行预警；

d) 应支持一种或多种预警方式，例如平台消息、短信、邮件或即时通信等；

e) 应支持预警规则自定义，包括预警指标、指标阈值、预警对象、预警周期等；

f) 应支持预警流程自定义，发生预警事件时，支持依照设定的流程发布预警。

6.4.2 应急处置

本项要求包括：

a) 应支持预警响应能力，根据预警结果进行决策和处置；

b) 应支持为第三方开发者或系统提供处置响应接口，以提供安全事件处置能力，例如通知相关人员进行安全事件处置，更新安全设备的检测规则或策略配置等；

c) 应支持安全威胁处置跟踪能力，对安全威胁处置流程及结果进行跟踪；

d) 应支持对处置结果进行记录。

6.4.3 安全威胁溯源

本项要求包括：

a) 应支持攻击溯源分析能力，通过对时间，主机 IP 等攻击特征信息以及攻击行为的分析，追溯到攻击源、攻击路径、攻击方式等，记录分析的过程并对被追溯到的关联安全事件进行关联分析并展示关系网图；

b) 应支持对攻击事件的攻击过程进行追溯，还原事件的攻击链，回溯攻击发生全过程，并追踪攻击源；

c) 应支持查看攻击者画像信息的能力，其中画像信息可包括：目标偏好、攻击习惯、技术特点等。

6.5 可视化展示要求

本项要求包括：

a) 应支持对网络的整体安全态势、不同类型的专题态势等进行展示；

b) 应支持对不同网络域、不同业务单元、不同设备、不同切片等的网络安全状况进行展示；

c) 应支持对不同时间段的网络安全态势进行展示；

d) 应支持采用多种视图展示安全态势的细节，如雷达图、地理信息图、关联关系图、威胁路径图、态势图等，并支持自定义态势展示视图、数据内容等。

7 5G 网络安全态势感知系统安全要求

数据处理过程中涉及的用户个人信息，应符合 GB/T 35273 及国家行业主管部门的相关要求。

5G 网络安全态势感知系统安全要求应符合 YD/T XXXX 中规定的相关安全要求。