ICS XX.XXX.XX
CCS R XX

团 体 标 准

T/XAZN XXX—2022

智慧城市 网络安全态势感知系统技术要求

Technical requirements of smart city network security situational awareness system

（征求意见稿）

2022 - xx - xx 发布　　2022 - xx - xx 实施

雄安新区智能城市创新联合会 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。

本文件由.....提出并归口。

本文件起草单位：

本文件主要起草人：

智慧城市 网络安全态势感知系统技术要求

1 范围

本标准规定了智慧城市网络安全态势感知系统的功能要求、性能要求。

本标准适用于智慧城市领域网络安全态势感知系统，指导相关产品的设计、研发和选型，适用对象包括智慧城市领域网络安全态势感知系统的建设及运维机构。

2 规范性引用文件

GB/T XXXX	信息安全技术 网络安全态势感知通用技术要求
GB/T XXXX	信息安全技术 网络安全态势感知系统安全技术要求
GB/T XXXX	信息安全技术 网络安全态势感知数据规范
GB/T 36643-2018	信息安全技术 网络安全威胁信息格式规范
GB/T 17859-1999	计算机信息系统 安全保护等级划分准则
GB/T 25069-2010	信息安全技术术语
YD/T 3734—2020	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
YD/T 1728-2008	电信网和互联网安全防护管理指南
YD/T 1730-2008	电信网和互联网安全风险评估实施指南
YD/T 1731-2008	电信网和互联网灾难备份及恢复实施指南
YD/T 1478-2006	电信管理网安全技术要求

3 术语、定义和缩略语

3.1 术语和定义

YD/T 3734—2020、YD/T 1728-2008、YD/T 1730-2008、YD/T 1731-2008、YD/T 1478-2006、GB 17859-1999、GB/T 36643-2018和GB/T 25069-2010界定的以及下列术语和定义适用于本标准。

3.1.1 智慧城市 Smart city

一种城市建设发展的形态,通过利用新一代的网络信息技术、人工智能技术等促进城市中信息空间、物理空间和社会空间的高度融合，使得城市经济发展、政府及公共服务的效率、市民的工作生活、资源和环境的保护与利用，高度智能化、科学化新型城市形态。

3.1.2 智慧城市网络安全态势感知系统 Smart city network security situation awareness system

适用于智慧城市关键信息基础设施领域，对智慧城市网络（包括并不限于移动通信网络、互联网、物联网、工业互联网等）中的网络流量和各种网络设备、安全设备和主机的日志进行信息收集，通过统计分析和数据挖掘等方法，对网络中的安全态势进行感知和预警、为智慧城市网络空间安全提供决策支持的系统。

3.1.3 网络安全信息 Cyber security information

网络安全威胁信息及防御措施，包括：对可能威胁网络正常运行的行为，用于描述其意图、方法、工具、过程、结果等的风险信息、事件信息等；可能暴露网络脆弱性的信息；检测、防止或减轻已知的或者可能的网络安全威胁或安全漏洞的行为、设备、程序、签名、技术或其他措施。

3.1.4 威胁信息 Threat information

一种基于证据的知识，包括上下文、供给机制、攻击目标、可信影响等信息，用于描述现有或可能出现的威胁，从而实现对威胁的响应和预防。

3.1.5 重要数据 Important data

一旦泄露可能直接影响国家安全、公共安全、经济安全和社会稳定的数据，包括未公开的政府信息，数量达到一定规模的基因、地理、矿产信息等，原则上不包括个人信息、企业内部经营管理信息等。

3.1.6 网络安全事件管理 Cybersecurity incident

由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。

3.1.7 网络安全漏洞 Cybersecurity vulnerability

网络产品和服务在需求分析、设计、实现、配置、测试、运行、维护等过程中，无意或有意产生的，有可能被利用的缺陷或薄弱点。这些缺陷或薄弱点以不同形式存在于网络产品和服务的各个层次和环节中，一旦被恶意主体所利用，就会对网络产品和服务的安全造成损害，从而影响其正常运行。

3.1.8 恶意文本 Malicious text

一种被恶意取代为病毒或者木马，威胁网络正常运行的文本。

3.2 缩略语

下列缩略语适用于本标准。

(R)AN	（无线）接入网络	（Radio）AccessNetwork
5GC	5G 核心网	5GCoreNetwork
Amf	接入和移动管理功能	accessandmobilemanagementfunction
API	应用程序接口	ApplicationProgrammingInterface
APK	Android 应用程序包	Androidapplicationpackage
APT	高级持续性威胁	AdvancedPersistentThreat
ATT&CK	对抗战术和技术的知识库	AdversarialTactics,Techniques,andCommonKnowledge
AUSF	认证服务器功能	AuthenticationServerFunction
BGP	边界网关协议	BorderGatewayProtocol
BSF	绑定支持功能	BindingSupportFunction
C&C	计算机与通信	Computer&Communication
CAPWAP	无线接入点的控制和配置协议	ControlAndProvisioningofWirelessAccessPointsProtocolSpecification
CCSDS	国际空间数据系统咨询委员会	ConsultativeCommitteeforSpaceDataSystems
CC 攻击	挑战黑洞（借助代理服务器实现攻击和伪装）	ChallengeCollapsar
CHF	计费功能	ChargingFunction
CIM	城市信息模型	CityInformationModeling

CNNVD	国家信息安全漏洞库	ChinaNationalVulnerabilityDatabaseofInformationSecurity
CNVD	国家信息安全漏洞共享平台	ChinaNationalVulnerabilityDatabase
CPU	中央处理器	CentralProcessingUnit
CVE	通用漏洞披露	CommonVulnerabilities&Exposures
DDoS	分布式拒绝服务	DistributedDenialofService
DGA	域名生成算法	DomainGenerationAlgorithm
DNS	域名解析服务器	DomainNameSystem
DOS	拒绝服务	DenialofService
DTN	延迟容忍网络	DelayTolerantNetwork
FTP	文件传输协议	FileTransferProtocol
GMLC	移动网关位置中心	GatewayMobileLocationCenter
GRE	通用路由封装协议	GenericRoutingEncapsulation
GSM	全球移动通信系统	GlobalSystemforMobileCommunications
HTTP	超文本传输协议	HypertextTransferProtocol
ICMP	Internet 控制报文协议	InternetControlMessageProtocol
IGP	内部网关协议	InteriorGatewayProtocol
IM	即时通信	InstantMessaging
IMAP	因特网消息访问协议	InternetMessageAccessProtocol
IMS	IP 多媒体系统	IPMultimediaSubsystem
IOC	控制反转	InversionofControl
IP	互联网协议地址	InternetProtocolAddress
IPTV	网络协议电视	InternetProtocolTelevision
IS-IS	中间系统到中间系统路由协议	IntermediateSystem-to-IntermediateSystem
JDBC	java 数据库连接	JavaDataBaseConnectivity
K-Means	k 均值聚类算法	k-meansclusteringalgorithm
Lmf	位置管理功能	LocationManagementFunction
LSP	分层服务提供程序	LayeredServiceProvider
LTE	长期演进技术	LongTermEvolution
MF	接入和移动性管理功能	AccessandMobilityManagementFunction
MP-BGP	多协议扩展边界网关协议	Multiprotocol-BorderGatewayProtocol
Namf	amf 服务化接口	Service-basedInterfaceExhibitedbyamf
Nausf	ausf 服务化接口	Service-basedInterfaceExhibitedbyausf
Nchf	chf 服务化接口	Service-basedInterfaceExhibitedbychf
nef	网络开放功能	networkexposurefunction
NEF	网络开放功能	NetworkExposureFunction,
NF	开源服务框架	NoahFrame/NoahGameFrame
Ngmlc	gmlc 服务化接口	Service-basedInterfaceExhibitedbygmlc
Nlmf	lmf 服务化接口	Service-basedInterfaceExhibitedbylmf
Nnef	nef 服务化接口	Service-basedInterfaceExhibitedbynef
Nnrf	nrf 服务化接口	Service-basedInterfaceExhibitedbynrf
Nnssf	nssf 服务化接口	Service-basedInterfaceExhibitedbynssf
Npcf	pcf 服务化接口	Service-basedInterfaceExhibitedbypcf
NRF	提供注册和发现功能	NFRepositoryFunction
Nrf	网络功能服务网络存储功能	Networkrepositoryfunction

Nsmf	smf 服务化接口	Service-basedInterfaceExhibitedbysmf
NSSF	网络切片选择功能	TheNetworkSliceSelectionFunction
Nudm udm	服务化接口	Service-basedInterfaceExhibitedbyudm
OCR	光学字符识别	OpticalCharacterRecognition
OSPF	开放式最短路径优先	OpenShortestPathFirst
PCF	策略控制功能	PolicyControlfunction
POP3 Post	邮局协议版本 3	OfficeProtocol-Version3
PSTN	公共交换电话网	PublicSwitchedTelephoneNetwork
RIP	路由信息协议	RoutingInformationProtocol
RTP	实时传输协议	Real-timeTransportProtocol
RTSP	实时串流协议	Real-timeStreamingProtocol
SFTP	安全文件传输协议	SecretFileTransferProtocol
SMF	会话管理功能	SessionManagementFunction
SMTP	简单邮件传输协议	SimpleMailTransferProtocol
SRv6	基于 IPv6 转发平面的段路由	SegmentRoutingIPv6
SSH	安全外壳协议	SecureShell
SVM	支持向量机	SupportVectorMachine
TCP	传输控制协议	TransmissionControlProtocol
TLS	安全传输协议	TransportLayerSecurity
UDM	统一数据管理功能	TheUnifiedDataManagement
UDP	用户数据包协议	UserDatagramProtocol
UDR	统一数据存储库	UnifiedDataRepository
UEBA	用户和实体行为分析技术	Userandentitybehavioranalytics
UPF	用户端口功能	UserPortFunction
URL	统一资源定位系统	Uniformresourcelocator
UTM	统一威胁管理	UnifiedThreatManagement
VLAN	虚拟局域网	VirtualLocalAreaNetwork
VXLAN	虚拟扩展局域网	VirtualeXtensibleLocalAreaNetwork
WAF	Web 应用防护系统	WebApplicationFirewall
WCDMA	宽带码分多址技术	WidebandCodeDivisionMultipleAccess
XSS	跨站脚本攻击	CrossSiteScripting

4 系统总体架构

4.1 智慧城市网络安全态势感知系统建设目标

a) 全面，从全网的角度感知全局和全部的网络安全事件；
b) 准确，发现准确的网络攻击，去除虚警和误报；
c) 实时，实时的检测和实时的评估是网络安全保卫的核心指标；
d) 有效，能与其他安全系统协作，有效阻断对核心保护系统的重大攻击和威胁。

4.2 系统主要任务

a) 数据采集，面向城市级网络进行相关大数据采集和融合；
b) 数据管理，对采集的数据通过清洗、过滤、归一和标识进行预处理，及对不同类型数据进行分级分类存储；

c) 安全事件检测，基于所获取的数据进行网络安全事件检测；
d) 态势评估，基于事件检测结果所发现的安全事件进行网络安全态势评估；
e) 态势可视化，以可视化的方式直观展示网络安全态势感知各个环节的结果；
f) 态势预警，基于安全事件检测所发现的重大安全事件进行预测和溯源，并与其他安全事件处置系统联动。

4.3 智慧城市网络安全态势感知系统架构图

智慧城市网络安全态势感知系统提供通用接口，一方面，可与雄安新区现有安全态势感知系统对接，形成整体性城市安全态势感知体系；另一方面，可与新区各委办局现有安全系统对接，为其提供安全态势源数据及威胁情报等。图4-1为智慧城市网络安全态势感知系统架构图，图4-2为智慧城市网络安全态势感知系统数据交互图。（数据交互要求见章节5.2.5）

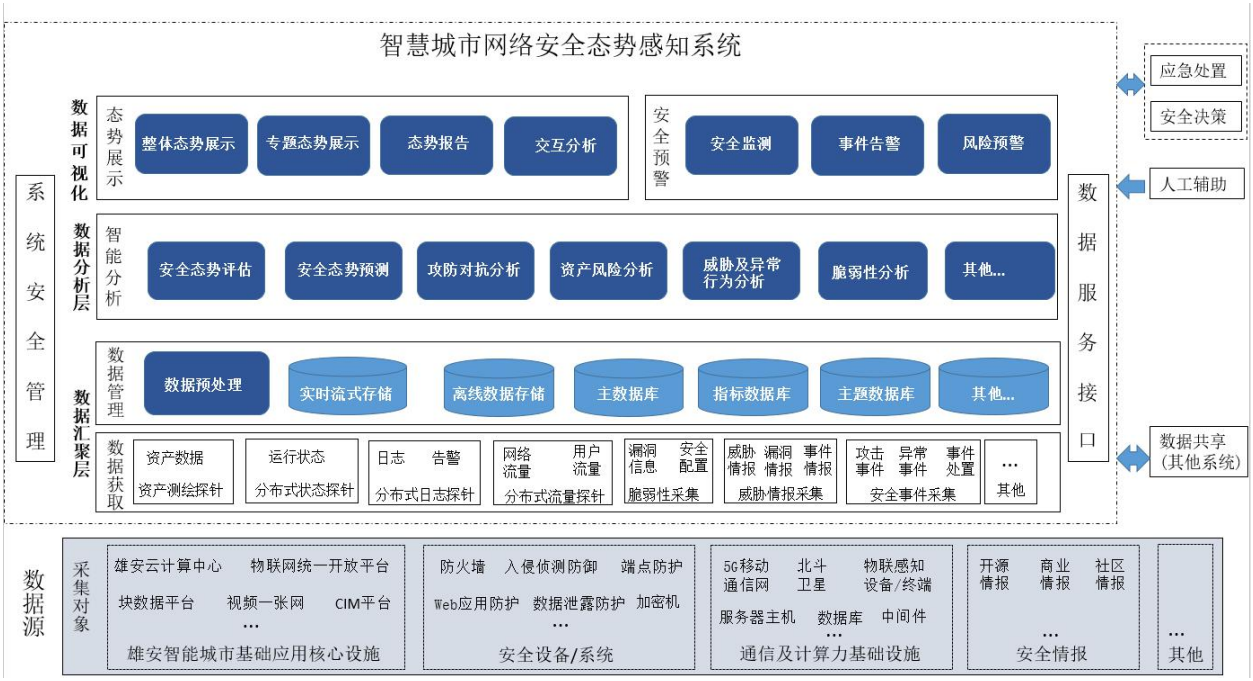

图4-1 智慧城市网络安全态势感知系统架构

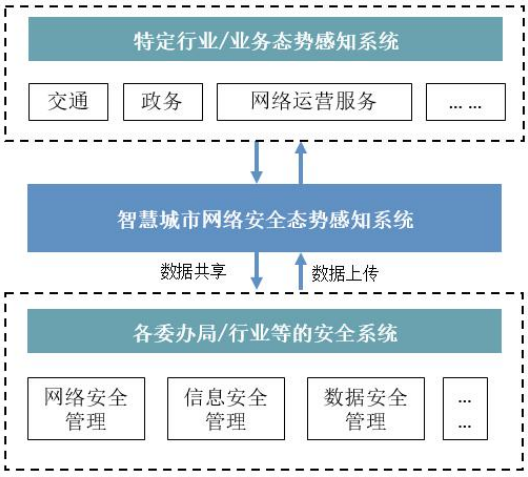

图4-2 智慧城市网络安全态势感知系统数据交互

4.4 智慧城市网络安全态势感知系统相关方

a) 系统使用方。新区管委会各部办局和下辖三县(以下简称为“管委会各部门”)以及公共服务机构是系统的使用方。
b) 系统建设运营方。系统建设运营方承担整体态势方案设计、建设和运行维护。

5 功能要求

主要功能包括:
a) 数据采集:对全网全数据类型采集,包括文件、包、流、会话、内存信息、注册表信息、地址信息、协议信息、服务信息、载荷传输信息等进行采集,支持大数据量存储规模。
b) 数据管理:对多源、异构数据进行预处理并对不同类型数据进行分级、分类、分层存储,实现各类数据的统一融合。
c) 态势量化计算:可量化的安全指标体系,能够描述目前城市宏观整体安全态势。
d) 安全态势分析:可对网络安全事件进行深入分析和发现,对当前的网络安全态势进行计算及多模式多维度的可视化输出。
e) 安全态势预测:可以准确预测将来某一时段内的安全趋势,计算的预测模块能够对木马攻击传播、DDoS 攻击、病毒态势、僵尸网络、APT 攻击进行预测。

5.1 数据采集要求

5.1.1 采集方式

对于不同类型的数据,系统应能支持多种采集方式,主要包括:
a) 主动采集:系统能够通过扫描、探测等方式采集数据,采集协议包括ftp/sftp、snmp、restful、数据库接口等。系统能够配置采集周期、采集规则,对采集设备进行状态监测;
b) 被动采集:系统能够通过syslog、restful等协议接收数据,并支持对采集数据的过滤,数据采集频率可由前端数据源的发送频率决定;
c) 文件导入:系统能够通过文件方式导入数据;
d) 人工录入:系统能够通过图形界面或命令行方式人工录入数据。

5.1.2 采集内容

a) 应支持基于采集策略从前端数据源的不同对象采集不同类型的数据,具体对象、数据类型可根据应用场景不同进行筛选。

5.1.3 数据源类型

系统应能采集不同类型的数据,具体数据类型如下:
a) 资产数据:包括物理主机资产、虚拟机资产、网络设备资产、安全设备资产、物联网资产、5G网络资产、应用软件资产等;
b) 网络流量数据:包括通过网络镜像采集的原始流量,以及通过netflow/sflow采集的流量数据。对于5G网络,网络流量包括5G信令流量和用户流量;
c) 运行状态数据:包括系统状态数据如CPU、内存、存储状态,以及进程、端口、服务等运行状态;
d) 日志数据:包括主机日志、web访问日志、登录日志、软件系统日志等;
e) 设备告警数据:主要是设备通过snmp、syslog等方式发出的告警数据;
f) 脆弱性数据:包括系统漏洞数据、安全核查数据等;
g) 安全事件数据:包括安全设备检测到的异常流量攻击事件、邮件攻击事件、异常访问事件等;

h) 威胁情报数据：包括恶意IP/域名/URL等情报数据，以及病毒样本、哈希值等数据；
i) 物理计算环境数据：包括物理环境的设备类型、厂家信息、型号、配置等；
j) 身份实体数据：包括身份标识、级别、角色、认证方式等；
k) 应急处置数据：包括应急处置案例的标识、状态、处置结果、负责人信息等；
l) 一中心四平台数据：系统应能通过接口采集一中心四平台数据，包括中心和各平台资产信息、资源使用状态、运行状态、用户状态、日志、事件信息等。

5.2 数据管理要求

5.2.1 数据（预）处理

数据预处理负责对采集器/流探针等上报的数据进行清洗、过滤、关联和富化，为日志/流量元数据等补全上下文相关信息，满足态势呈现、调查取证和威胁检测对数据的要求。

a) 应支持通过配置过滤规则对收集的数据进行筛选；
b) 应支持对收集的同构、异构数据进行预处理；
c) 应支持对数据进行分类分级标识，记录并保存数据收集过程中分类分级的操作过程，对数据分级分类变更的操作记录进行标识；
d) 应支持对采集的原始数据进行归并，如对同一事件的多次告警进行归并，对同一会话的日志进行归并等；
e) 应支持基于资产库、威胁信息库、地理信息库等对采集的原始数据进行补全，补全的内容可包括资产属性、关联事件、地理位置等。
f) 应支持将采集的同一类型、不同格式的原始数据转换为统一的数据格式，如统一时间格式、统一漏洞名称等，且转换时不能丢失或损坏关键数据项；
g) 应支持对于不同类型的数据进行不同预处理方式，包括实时处理和离线处理等。

5.2.2 数据传输

态势感知系统内部的数据传输，主要指数据接收器将接收到的采集数据送到数据总线的过程。

a) 应支持对传输任务的运行状态监控，并生成分析报告；
b) 应支持对传输任务的跟踪、调度、控制，对它进行终止、重启等操作；
c) 应支持数据传输缓存功能，确保网络中断或阻塞时，数据不丢失；（当目标接收端出现问题时，网络中断或出现阻塞时，支持将加载数据缓存在本地磁盘或者内存中，当目标端恢复后继续将数据加载到目标端中）。

5.2.3 数据存储

数据存储负责对格式化后的数据进行存储，针对不同类型的异构数据（日志、数据、文件等）进行分类存储，存储的数据主要用于威胁检测和威胁可视化。考虑到可靠性和高并发性能的要求，数据存储需采用分布式保存在多个检测/存储节点，并且可以按需扩展存储节点。

a) 应支持结构化数据、半结构化数据和非结构化数据的存储；
b) 应支持基于态势感知不同用户组的存储权限管理；
c) 应支持可伸缩的分布式数据存储架构，满足数据量持续增长需求；
d) 应支持集群的计算资源管理，以控制计算过程中的数据迁移；
e) 应支持操作审计日志存储不低于6 个月，网络安全事件存储不低于3 个月。
f) 应支持分布式索引技术对关键的格式化数据建立索引，为可视化调查分析提供基于关键字的快速检索服务，并保存在多个检测/存储节点，提供高可靠性和高并发索引能力，支持按需弹性扩展索引。

5.2.4 数据分析

5.2.4.1 数据处理

a) 应支持对系统数据增加、备份、过滤、排序等操作，其中对系统操作产生的业务数据可修改、对系统收集的原始数据不可修改；
b) 应支持对不同来源的数据格式进行归一化，形成可统一分析的数据记录；
c) 应支持对事件记录的去重处理，防止不同数据来源对同一安全事件的重复上报；
d) 应支持检索结果对接到数据统计和数据分析模块中进行进一步的处理和分析；
e) 应支持对网络安全告警和网络安全事件的快速检索，数据检索时间满足PB量级下不大于10分钟。

5.2.4.2 威胁分析

5.2.4.2.1 应支持报文异常检测

a) 支持TCP/UDP/HTTP/POP3/SMTP/IMAP/FTP等协议的流量重组还原能力；
b) 支持IP/ICMP网络层协议、TCP/UDP传输层协议以及HTTP/POP3/SMTP/IMAP/FTP等常见应用层协议的解析识别且协议变量数量不少于300个；
c) 支持网络层、传输层和常见应用层的报文检测匹配；
d) 支持IP定位功能；
e) 支持IPv6网络的监测分析能力；
f) 支持URL编解码、BASE64编解码、DEFLATE解压缩、ZLIB解压缩、GZIP解压缩等能力；
g) 支持封装报文（VXLAN、GRE、VLAN、CAPWAP、SRv6等）协议的解析；
h) 支持基于国家级特征库进行高速、智能的模式匹配，能够识别各种已知攻击的特征；
i) 支持通过动态分析网络报文中包含的协议特征，准确发现其所在协议；
j) 支持通过白名单规则过滤报文提高检测效率。

5.2.4.2.2 应支持未知威胁/高级威胁检测

a) 支持基于系统自学习或自定义配置的流量基线检测常规报文异常事件；
b) 支持通过分析WEB请求数据、WEB响应数据和WEB通信行为发现WEB异常访问；
c) 支持提取邮件流量元数据，通过分析邮件关键信息检测收发件人异常、下载恶意邮件、访问邮件服务器、邮件正文URL异常等事件；
d) 支持通过对协议流量（DNS/HTTP/TLS/3,4层协议）的分析检测C&C通信异常；
e) 支持发现被入侵主机通过正常的协议和通道传输非授权数据的异常；
f) 支持通过机器学习算法训练模型进行分类和识别，检测利用加密流量（TLS协议）的C&C流量，避免解密流量后再检测的泄露隐私问题；
g) 支持通过机器学习方法检测针对常见协议默认端口的暴力破解行为；
h) 支持基于矿机与矿池的通信流量特征检测挖矿的异常行为；
i) 支持通过挖掘事件之间的关联和时序关系发现有效攻击的关联分析能力；
j) 支持根据多个异常进行关联、评估和判定产生高级威胁，为威胁监控和攻击链路可视化提供数据的威胁判定能力；
k) 支持与诱捕陷阱或仿真环境等协同，发现、延迟或阻断攻击者的异常活动。

5.2.5 数据共享

应支持数据以直接或间接、实时或非实时的方式进行数据共享。其中包括纵向数据共享和横向数据共享两种方式。

5.2.5.1 纵向数据共享

数据上传

本级态势感知系统与上级态势感知系统间的数据交换与共享，包括资产、告警和情报等：

a) 应建立数据上报管理制度，明确上报数据等级、类型、内容、数据提供方、数据使用方；
b) 应支持对数据上报用户、角色的权限设置，对数据上报流程进行审核和审计；
c) 应保障上报数据信息的真实可靠，数据内容应符合数据上报要求，不得擅自改动数据字段所含内容，必填字段都应按规定填写；
d) 应支持上报数据可跟踪、可追溯。

数据下发

本级态势感知系统与下级态势感知系统间的数据交换与共享，包括资产、告警和情报等：

a) 应建立数据下发管理制度，明确数据下发的数据类型、数据内容、提供方、使用方；
b) 应建立数据下发审核机制，设置数据下发的用户、角色的访问权限，审计下发过程；
c) 应能够设置的各类数据下发模板，按照指定的周期完成对于指定对象的数据下发；
d) 应支持下发数据可跟踪、可追溯。

5.2.5.2 横向数据共享

本级本行业态势感知系统与本级不同行业态势感知系统间的数据交换与共享，以情报数据为主：

a) 应建立统一的情报数据共享管理制度，明确数据提供方、使用方，实现同级不同行业、不同地区态势感知系统情报数据的共享。数据类型包括但不限于：恶意IP、恶意域名、恶意软件、漏洞库、病毒库等；
b) 应建立数据共享审核机制，设置数据共享的用户、角色的访问权限，审计共享过程；
c) 应支持向不同使用方共享不同类型、不同范围的数据；
d) 应支持共享数据可跟踪、可追溯。

5.2.5.3 数据共享安全

a) 应明确数据共享范围和共享数据的安全控制机制，避免数据共享带来安全隐患；
b) 应明确约束数据提供者与其数据使用者的数据保护责任；
c) 应审核数据的开放和共享场景，确认没有超出提供方的数据所有权和使用权范围；
d) 应审核开放和共享的数据内容，确认属于满足业务场景需求的最小范围内；
e) 应记录操作事件中的操作人、操作内容、操作时间等信息，并设置操作行为规则，对上述操作事件进行识别，从用户信息查询风险、操作风险、权限风险等多个角度判断操作行为是否存在风险。

5.2.6 数据销毁

a) 应支持数据自定义销毁功能，设置销毁相关角色、监督角色，审计操作过程；
b) 应支持依照数据分类分级建立相应的数据销毁机制，明确销毁方式和销毁要求；
c) 应支持配置必要的数据销毁工具，确保以不可逆方式销毁数据内容。

5.3 安全态势分析要求

5.3.1 资产安全管理

5.3.1.1 资产采集能力

对于不同类型的资产数据，系统应支持主动或被动收集方式：

a) 支持通过监测、扫描、主动采集协议及接口等技术定期收集收据，主动发现资产信息；
b) 支持通过手工设置的方式导入资产数据；
c) 支持通过被动采集协议及接口与其他系统或者平台对接获取资产信息；

d) 支持数据过滤能力，支持配置规则对收集的资产数据内容进行过滤；平台应具备数据补采能力，在采集任务失败时，可对数据进行再次采集。

5.3.1.2 资产状态采集

系统应支持资产状态采集能力：

a) 支持通过监测、扫描、主动采集协议及接口等技术定期收集收据，主动发现开放端口；
b) 支持采集主要服务器的基本信息包括采集机编号、采集机IP、采集机CPU使用率、内存使用率、硬盘可用容量、进程数、线程数等；
c) 在设备宕机、相关软件的进程监控等软硬件出现异常时，提示解析设备告警信息。

5.3.1.3 资产漏洞分析

系统应支持资产漏洞信息分析能力：

a) 资产漏洞分析包括： web应用漏洞、安全产品漏洞、应用程序漏洞、操作系统漏洞、数据库漏洞、网络设备漏洞等漏洞信息分析；
b) 支持对接公共漏洞发布平台（如工信部网络安全威胁信息共享平台、CVE、CNVD、CNNVD等）的漏洞信息采集；
c) 支持按时间、业务系统、漏洞等级等维度统计分析存在漏洞利用风险的资产数据；
d) 支持对不同种类系统漏洞攻击总体情况的统计，分析当前系统漏洞攻击情况的趋势变化；
e) 支持通过关联漏洞情报数据，分析出本地资产存在的脆弱性并进行预警，预警具体内容包括：漏洞发现时间、漏洞名称、漏洞影响资产、漏洞类型、漏洞等级、处理建议、预警等级等。

5.3.1.4 资产脆弱性分析

平台应支持资产脆弱性分析，具体要求如

a) 支持对操作系统、数据库、网络设备、中间件、DNS等的配置合规检测结果进行分析；
b) 支持对摄像头、网关等物联网设备资产的合规检查结果进行分析；
c) 支持对配置不合规项被利用情况的统计分析，支持分析攻击者利用配置不合规项攻击资产的风险趋势；
d) 支持按时间、业务系统、违规类别等维度统计分析配置不合规的资产数据；
e) 支持对操作系统、数据库、网络设备、业务系统等弱口令检测结果进行分析；
f) 支持弱口令被利用情况的统计分析，支持分析攻击者利用弱口令登录资产进行攻击的风险趋势；
g) 支持按时间、业务系统等维度统计分析存在弱口令的资产数据。

5.3.2 威胁分析能力

5.3.2.1 流量威胁分析

支持通过流量进行威胁分析：

a) 应能识别流量中存在的应用、内容和环境等各层面攻击多种安全攻击事件，发现存在的攻击风险，全面掌握互联网安全态势；
b) 根据证书、网络特征、业务流特征，具备识别HTTPS加密应用流量及应用内行为；
c) 采用基于网络、协议、编码、流的组合特征，能够识别主流多种互联网应用；
d) 对常见僵尸网络或木马程序控制指令识别，可识别网页下载、网络传输中包含的恶意程序，恶意程序事件、网络攻击事件以及敏感数据传播事件；
e) 对流量采集的协议识别和样本捕获还原，以及基于实时流量对文本、图像、邮件等文件的还原能力；

f) 设备对流信息进行识别，识别有效的负载包，对流量包进行重组，还原、解码，还原数据文本、图像、APK、文档、邮件等文件。

5.3.2.2 恶意文件分析

对恶意文本分析能力：

a) Hash检测，匹配Hash规则库来实现文件威胁研判；
b) 内嵌文件研判，分析文件的二进制代码检测是否存在内嵌文件，然后再对检测出的内嵌文件进行威胁检测，包括AV检测，特征检测等；
c) 病毒引擎鉴定，实现对各类僵木蠕病毒及木马程序进行研判检测，支持黑白名单检测，通过匹配系统的黑白名单库来实现是否进行检测；
d) 动态研判，对于动态文件主要结合沙箱虚拟环境进行检测，支持API规则、进程规则、文件规则、注册表规则、网络规则、IOC规则、PE异常规则等。

5.3.2.3 日志安全分析

日志安全分析能力：

a) 对信息资产的实时监控、信息资产与用户管理、解析规则与关联规则的定义与分发、日志信息的统计与报表、海量日志的存储与快速检索以及管理;
b) 通过归一化处理，实现高性能的海量事件存储和检索优化功能，提供高速的事件检索能力、事后的合规性统计分析处理，数据二次挖掘分析。

5.3.2.4 UEBA 分析

UEBA分析能力：

a) 作为安全分析平面向用户和实体异常行为的分析能力组建立行为基线，从行为角度做人机识别。通过关联分析，利用外部威胁情报，判断异常的行为分析能力；
b) 基于特征的匹配分析升级到基于行为的异常分析，从基于攻击特征监测提升到给予攻击模型深度检测，从针对样本数据的分析拓展到针对全量数据的分析，从安全事件基于五元组的定位到基于大数据的溯源追踪，从而确定报警真实性、攻击源，评估攻击造成危害的能力。

5.3.2.5 关联分析

5.3.2.5.1 实时数据分析

实时数据关联分析：

a) 对采集的数据进行实时流式关联分析，从中发现高危风险并及时报警；
b) 对高危等级报警生成事件并实时推送至平台，至少包括报警事件的源地址、类型、时间等信息；
c) 监测行为包括是否遭受远程控制、数据盗取、系统破坏报警等。

5.3.2.5.2 历史数据分析

对历史数据分析：

a) 以大数据技术为核心，对网络资产、漏洞、威胁情报的综合关联分析能力；
b) 对于资产分析、漏洞预警、威胁识别、安全事件分析以及可视化管理等。

5.3.3 监测能力

5.3.3.1 规则管理能力

a) 具备高性能网络行为检测能力。能够基于五元组、域名和正则表达式等规则对网络威胁进行监测；

b) 具备实时处理在线网络数据和批量处理离线网络数据的监测能力；
c) 具备监测规则的添加、删除、修改功能。

5.3.3.2 攻击行为识别能力

a) 具备对网络流量中的异常网络流量进行监测的能力；
b) 具备对网络流量中的恶意攻击行为进行监测的能力。

5.3.3.3 未知特征攻击识别能力

基于大数据和人工智能等技术构建正常业务基线，及时发现异常特征，识别未知特征攻击并进行预测和预警:

a) 针对不同终端构建基线，识别针对终端的未知特征攻击；
b) 针对不同应用构建基线，识别针对应用的未知特征攻击；
c) 针对不同业务质量构建基线，识别针对业务质量的未知特征攻击；
d) 针对网络指标质量构建基线，识别针对网络质量的未知特征攻击。

5.3.3.4 木马识别能力

a) 具备木马病毒的监测识别能力；
b) 应支持通过人工导入或者自动方式对木马病毒库进行升级。

5.3.3.5 僵尸网络识别能力

a) 具备对僵尸网络的监测识别能力。

5.3.3.6 加密流量异常监测能力

a) 具备对流量中的加密流量，在不解密的情况下可实现对使用加密通信的恶意代码、加密通道中的恶意攻击行为、恶意或非法加密应用的有效检测。

5.3.3.7 隐蔽信道识别能力

a) 具备对隐蔽通信识别能力，可实现对于HTTP、HTTPS、DNS等多种网络隐蔽信道的混合检测，包括隐蔽隧道木马行为检测、未知窃密型木马的通信行为检测和木马双向通信属性的获取。

5.3.3.8 邮件安全监测能力

a) 具备对邮件恶意网址诱导、恶意网页及代码、恶意文件附件、邮件攻击事件还原及威胁邮件提取、邮件欺诈意图检测等多维邮件威胁检测能力。

5.3.3.9 黑客工具及行为监测能力

a) 具备从流量中识别区分网络扫描类行为流量、侦察突破类行为流量、隐蔽回传类行为流量、内网拓展类行为流量，识别出黑客攻击工具的名称和版本，能够对黑客攻击行为画像、杀伤链阶段行为画像和攻击溯源。

5.3.3.10 样本的提取与分析能力

a) 具备从数据流中提取样本的能力；
b) 具备对恶意代码特征的家族基因谱系进行分析的能力；
c) 具备样本分析能力，能够对样本进行白名单和黑名单特征匹配、静态分析、动态分析、沙箱分析；
d) 具备按时间切片后进行批量处理的能力；

e) 具备对多个样本的关联处理能力；
f) 具备样本分析过程的自动保存和回退等操作；
g) 分析结果宜使用可视化方式进行显示。

5.3.4 溯源能力

5.3.4.1 数据留存能力

a) 具备将在线采集网络流量全部原始流量数据包实时存储的能力，为溯源分析提供原始流量依据；
b) 具备用户自定义过滤条件的能力，可过滤掉无用数据，提取出重要数据，提高分析性能；
c) 具有特征检测类事件原始报文捕获能力；
d) 具有威胁情报类事件原始报文捕获能力；
e) 具备离线数据包导入与重放的能力，能够对离线数据进行重放分析。

5.3.4.2 数据解析能力

a) 具备HTTP、DNS、POP3、IMAP4、SMTP、FTP、ICMP、SSH、Telnet、Mysql等通用网络协议元数据字段的提取能力；
b) 具备常用以及私有网络通讯基础协议的识别能力；
c) 具备HTTP/POP3/SMTP/IMAP4等协议会话及传输内容的组报还原能力。

5.3.4.3 数据溯源取证能力

a) 具备筛选捕获网络数据包的能力，如按照IP/IP对、端口，协议，时间等条件筛选捕获到的数据包，同时支持数据包本地下载功能；
b) 具备数据包回溯分析功能，支持历史数据统计分析结果进行下载并进行二次分析，可以查看数据包的详细信息，分析结果可导出；
c) 具备实时流量监测能力，支持监控特定应用的网络传输性能指标，包括流量、数据包、会话数量、响应时间等。能够根据端口、端口组、IP地址、IP地址组、IP地址+端口、HTTP应用请求中的URL值等自定义应用，针对自定义的应用进行流量监测分析；
d) 具备威胁情报库（IOC），并能不定期的更新威胁情报库信息，确保威胁情报库的信息具有全面性、失效性；
e) 具备流量可视化分析能力，能够图形化的显示网络会话中的数据交互传输过程，并可多个维度进行流量可视化分析；
f) 具备安全事件的kill-chain溯源关联分析、ATT&CK溯源关联分析、时间序列溯源关联分析等相关分析能力；
g) 具备数据包Payload数据检索与分析能力，支持利用字符串或十六进制进行检索。检索结果以会话形式展现，支持下载对应原始数据包；
h) 具备溯源取证深度分析能力，能够灵活定制会话数据的分析模式，支持以人工方式进行分析，亦可应用系统内置智库策略或人工策略进行分析。

5.3.5 支撑能力

系统需对外部系统提供元数据支撑能力：

a) 网络流量监测数据：至少包含流量元数据、文件数据的支撑开放能力。流量元数据是通过原始协议字段的日志格式化输出；文件数据包含原始数据包以及还原文件数据；
b) 设备采集日志数据：包含不限于防火墙日志、入侵监测/防御设备日志、防病毒设备日志、WAF设备日志、DDoS设备日志、UTM设备日志等产生的日志；

c) 系统审计日志数据：包含不限于用户的FTP行为、HTTP行为、收发邮件的行为、IM行为、搜索关键字行为等行为日志；
d) 扫描监测数据：包含不限于扫描监测的漏洞、黑链、网页木马、网站可用性、钓鱼网站等监测数据。

5.3.5.1 漏洞数据支撑

系统需对外部系统提供漏洞数据支撑能力：
a) 漏洞基础信息：包含不限于漏洞名称、漏洞描述、漏洞类型、危险级别、漏洞发现时间、CNVD编号/CNNVD编号/CVE编号等漏洞基础信息；
b) 漏洞威胁等级信息：包含不限于漏洞访问路径（远程/邻接/本地）、利用复杂度、影响程度（保密性影响/完整性影响/可用性影响）等信息。

5.3.5.2 安全事件数据支撑

系统需对外部系统提供安全事件数据支撑能力：
a) 安全事件基本信息：包含不限于发生时间、源IP、源端口、目的IP、目的端口、安全事件规则大类、安全事件规则小类、危害等级等信息；
b) 安全事件分类信息：包含不限于有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障等；
c) 安全事件分级信息：按照信息系统重要程度、系统损失程度和社会影响程度，评估安全事件分级信息，分为特别重大事件、重大事件、较大事件和一般事件。

5.3.5.3 网络攻击威胁数据支撑

系统需对外部系统提供网络攻击威胁数据支撑能力：
a) 网络攻击威胁信息：包含不限于攻击名称、攻击时间、攻击源、攻击对象、攻击方式、脆弱性类别、攻击后果、攻击严重程度等信息。

5.3.6 应急响应能力

系统需支持对各类安全事件及威胁的应急响应能力：
a) 应急组织管理：应急组织角色包含不限于应急响应领导小组、应急响应技术保障小组、应急响应专家小组、应急响应实施小组、应急响应日常运行小组等，一人可承担两种或多种角色职责；
b) 应急场景管理：应支持应急场景的定义和管理，为可能出现的各种紧急事件启动对应的应急场景；
c) 应急预案管理：应支持应急预案的定义和管理，应急预案信息包含不限于预案名称、应急场景、告警时间、告警级别、事件状态、责任人等信息；
d) 应急资源管理：包含不限于各应急系统相关技术文档的管理，一级应急物资、应急设备的基本信息维护；
e) 应急响应流程管理：包含不限于事件通告、事件分级分类、应急启动、应急处置、后期处置等应急流程管理。

5.3.7 安全态势预警能力

平台应支持对资产安全威胁进行预警；支持对网络攻击态势进行预测，包括攻击目标、攻击类型、攻击时间段等；支持对高危用户行为进行预警；支持通过关联已发现的异常行为和原始日志，进行未知安全威胁的发现。具体要求如下：

a) 支持通过关联漏洞情报数据，分析出本地资产存在的脆弱性并进行预警，预警具体内容包括：漏洞发现时间、漏洞名称、漏洞影响资产、漏洞类型、漏洞等级、处理建议、预警等级等；
b) 支持基于历史及当前恶意扫描、密码猜测攻击、系统漏洞攻击等网络攻击的趋势，预测可能发生的网络攻击并进行预警，预警具体内容包括：攻击目标、攻击类型、攻击时间段、预警等级等；
c) 支持基于历史及当前注入攻击、WebShell攻击、跨站攻击及CC攻击等WEB攻击的趋势，预测可能发生的WEB攻击并进行预警，预警具体内容包括：攻击目标、攻击类型、攻击时间段、预警等级等；
d) 支持基于历史及当前Dos/DDos攻击、业务异常流量等异常流量攻击的趋势，预测可能发生的异常流量攻击并进行预警，预警具体内容包括：攻击目标、攻击类型、峰值流量、超过预警基线百分比、开始时间、结束时间、持续时间、预警等级等；
e) 支持基于历史及当前病毒、蠕虫、木马、僵尸程序等恶意程序攻击的趋势，预测可能发生的恶意程序攻击并进行预警，预警具体内容包括：攻击目标、恶意程序类型、攻击时间段、预警等级等；
f) 支持基于历史及当前恶意下载链接、主控地址、DGA域名等恶意网址的攻击传播变化趋势，预测可能出现的恶意网址攻击传播情况并进行预警，预警具体内容包括：攻击目标（群体），恶意网址类型、攻击传播时间段、预警等级等；
g) 支持基于历史及当前敏感数据异常操作、过期账号登录、非法外联及高危命令执行等用户异常行为趋势，预测可能发生的用户异常行为并进行预警，预警具体内容包括：目标资产、用户账户、异常行为类型、异常行为发生时间段、预警等级等；
h) 支持通过关联已发现的异常行为和原始日志，进行未知安全威胁的发现并预警，预警具体内容包括：目标资产、威胁类型、威胁发生时间、预警等级等；
i) 支持通过关联威胁情报，分析出本地可能发生的安全威胁事件并进行预警，预警具体内容包括：目标资产、威胁类型、威胁发生时间、预警等级等。

5.4 可视化要求

5.4.1 网络资产展示

a) 网络资产展示应呈现全网中所有资产信息，包括本地资产、云上资产以及业务应用资产，例如：设备、软件和网站等均属于网络资产；
b) 从资产类型、所属关系、所属单位、资产IP归属地、域名、数量、时间等多维度多层次展示网络资产的全貌。支持零代码构建网络资产分析模型，以手动拖拽的方式自由组合网络资产展示报表，并具备丰富的可视化能力。

5.4.2 安全态势展示

a) 通过汇聚网络流量、日志、威胁情报、安全事件、运行状态等相关数据，对攻击事件、威胁告警、攻击源头等安全风险进行进行分类统计和综合分析，实时为用户呈现网络安全态势，进而为安全事件的处置决策提供依据；
b) 安全态势展示应和安全风险识别、安全事件处理、处置反馈形成业务闭环，确保及时发现、及时处理、及时反馈。

5.4.3 可选择性展示

a) 应建立安全态势预警模型，对全网的安全趋势、潜在的安全风险进行趋势分析和预警，包括对网络流量态势、脆弱性态势、网络攻击态势的预警预测能力。通过建立态势预警分级管理机制，对来自不同威胁事件信息形成统一的不同级别的风险预警展示。

5.5 系统运维管理要求

智慧城市网络安全态势感知系统需要接入到信息系统的网络中进行数据采集,因此其自身安全也非常重要。为保证平台的有序运行，一方面应规范系统自身的安全策略、知识库、情报库、模型库的管理能力；另一方面，应考虑系统的自身安全，包括标识与鉴别、角色管理、安全审计、系统的性能、可用性、可扩展性等。

5.5.1 系统管理要求

5.5.1.1 用户及权限管理

包括用户身份鉴别和访问控制。

5.5.1.1.1 身份鉴别

a) 态势感知系统应对数据采集终端或导入服务组件实施身份鉴别；
b) 态势感知系统应对数据导出的终端或者导出服务组件实施身份鉴别；
c) 态势感知系统应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；
d) 态势感知系统应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现；
e) 态势感知系统应确保用户初次登录时口令的唯一性；
f) 态势感知系统应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
g) 当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；
h) 各类基础设施应具有可寻址的唯一性标识，发起信息传输时应进行自身身份标识。

5.5.1.1.2 访问控制

a) 态势感知系统应由授权主体配置基于数据分类分级的访问控制策略，规定主体对数据的访问规则；
b) 在对外提供态势评估等服务时，应确保第三方只有在被授权情况下才可以对态势感知系统的数据资源进行访问、使用和管理；
c) 应提供访问控制功能，对登录的用户分配账户和权限；
d) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
e) 应进行角色划分，并授予管理用户所需的最小权限，实现管理用户的权限分离；
f) 应重命名或删除默认账户，修改默认账户的默认口令；
g) 应及时删除或停用多余的、过期的账号，避免共享账号的存在；
h) 应授予不同账号为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

5.5.1.2 系统审计

a) 应提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 应保证态势感知系统所有采集组件、网络组件、安全组件的系统时间保持一致；
d) 应对审计进程进行保护，防止未经授权的中断；
e) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
f) 应确保审计记录的留存时间符合法律法规要求；
g) 系统应允许授权管理员创建、存档、删除和清空审计记录；
h) 系统应使存储于永久性审计记录中的所有审计数据可为人所理解；

i) 除了具有明确的访问权限的授权管理员之外，系统应禁止所有其他用户对审计日志的访问。

5.5.1.3 报表管理

a) 应提供智能报表统计功能，辅助系统日常运维管理。报表包括但不限于：用户状态、资产状态、网络连接状态、威胁统计、攻击分布统计、防护任务统计；
b) 应包含定期报表和一次性报表；
c) 报表应由统一管理人员进行内容审核、发布；
d) 报表只能在授权情况下访问、使用和管理。

5.5.2 系统性能要求

5.5.2.1 系统层面处理要求

本项要求包括：

a) 业务安全态势感知平台系统应能够连续 7 × 24 小时不间断工作；
b) 应支持 TB 级别海量数据的采集、分布式存储和分布式运算；
c) 应支持分钟级实时数据采集、运算和查询；
d) 平台认证响应时间应在 2 秒以内；
e) 应具有较高的自动化程度，如：自动任务调度、自动故障告警、自动任务恢复等；
f) 应具备相应容错手段，允许操作人员在有限范围内的误操作；
g) 任何软件模块的维护和更新都不影响其它软件模块，软件应具有容错能力。

5.5.2.2 网络传输能力要求

a) 智慧城市网络安全态势感知系统接入互联网带宽不小于 10Gbps；
b) 智慧城市网络安全态势感知系统集群中子系统之间网络传输带宽不小于 200Mbps；
c) 网络中的路由协议支持要求：
   - 路由器设备必须支持静态路由，静态路由条目不低于2000条；
   - 路由系统必须同时支持RIPv2、OSPF、IS-IS等IGP协议，要求IS-IS支持最少5000条LSP，OSPF支持最少5000条路由；
   - 路由系统必须支持BGP4+、MP-BGP协议，必须支持BGP community、AS path等基本属性，支持route-map、prefix-list等多种路由过滤方式。

5.5.2.3 系统算力要求

a) 智慧城市网络安全态势感知系统的底层分析计算应采用分布式计算方式，由大数据集群提供计算能力支撑；
b) 计算集群应包括但不限于：数据采集集群、实时计算集群、数据存储集群等，支持多集群部署；
c) 应支持实时计算和离线计算两种方式；
d) 计算实时性方面，对于外部实时采集到的数据，从采集数据开始，经过数据传输、存储，通过分析确认安全风险，依据处置策略向用户发送警示信息所需要的时间，应满足平台用户需求，在设定阈值下越小越好；
e) 计算准确性方面，应能够通过对安全数据的分析，正确评估当前系统监测范围内资产的安全状态，使用户准确了解安全状况。应将安全风险预测的误报率控制在用户许可的范围内，误报率应小于 5%；
f) 集群计算节点和管理节点的性能和 CPU 处理能力、内存容量、磁盘空间容量等，在业务峰值情况下始终留有 10%～15%的冗余；
g) 所有集群节点配置要求：CPU 不低于 8core，内存不低于 128G，硬盘不低于 5T。

5.5.3 系统可用性要求

a) 应具有针对系统资源、应用组件、数据质量综合监控和告警审计的能力；
b) 应能全面感知系统运行状态和安全指数，包括但不限于在线情况、CPU 及使用情况、内存及使用情况、网络使用情况等。

5.5.4 系统可扩展性要求

a) 数据可扩展
数据采集源头类型繁杂，智慧城市网络态势感知系统数据源管理采应用灵活的配置方式。新增已有的接入方式的数据源时，不需或尽可能减少开发工作，进行少量新增数据源配置即可完成数据源接入。如果有新的接入方式需求，也可方便地扩展一种新的接入方式。
b) 接口可扩展
智慧城市网络安全态势感知数据分析结果需要为各大平台服务，内外部接口众多，接口设计时应充分考虑可扩展性。接口数据格式尽量采用主流数据格式，如json报文方式。
c) 算力可扩展
应采用大数据集群等分布式方式灵活管理算力节点，扩展或删除计算节点秒级生效且不影响系统业务。
d) 存储可扩展
系统采集的数据源、计算的中间结果、最终分析结果需要多样化的存储方式来支撑，包括结构化数据存储和非结构化数据存储。存储方式上应至少可支持分布式文件系统存储和数据库存储。

5.5.5 知识库管理要求

a) 系统需构建开放的、动态更新的知识库和知识计算系统，形成对海量网络数据进行结构化、体系化组织与关联的技术系统，形成具有自主更新与学习能力的开放网络知识库；
b) 系统的知识库应包括但不限于：资产信誉库、IOC 情报库、黄赌毒库、恶意 APP 库、漏洞库、攻击规则库、僵尸网络库、APT 组织库、黑白名单等；
c) 知识构建的数据源包括系统内部数据挖掘、数据分析的输出结果和外部共享知识库；
d) 知识库内部数据源包括但不限于 OCR 识别、图片识别的结果、数据库等结构化数据、半结构化数据、漏洞描述短文本等非结构化数据；
e) 外部共享知识库包括各安全厂商自行维护的、国内外已公布的知识库成果，如漏洞库、攻击规则库等；
f) 系统提供包括但不限于机器学习引擎、深度学习引擎、图计算引擎、关系网络分析引擎对知识图谱构建提供计算处理支撑；
g) 对不同安全风险的识别能力方面，知识库要求如下：
- 当平台进行应用软件（包括 PC 端应用和移动应用）恶意行为识别时，宜具有识别应用软件恶意行为特征的信息库，恶意行为特征样本量宜不低于 2000 万；
- 当平台进行应用软件恶意开发者识别时，宜具有识别恶意应用软件开发者特征的信息库，应用开发者签名信息的储备量宜不低于 1000 万；
- 当平台进行应用软件恶意开发者识别时，宜具有识别应用软件正版和盗版信息的签名知识库，正版签名库签名量宜不低于 100 万；
- 当平台进行黑产设备行为识别时，宜具有与识别黑产行为特征有关知识的信息库；
- 当平台进行恶意 IP 识别时，宜具有与互联网安全风险相关联的恶意 IP 地址库；
- 当平台进行异常设备识别时，宜具有与互联网安全风险相关联的异常设备信息库；
- 当平台进行业务风险识别时，宜具有与实际业务相关联的风险规则信息库；

- 当平台用户有特定安全风险识别需求时，平台宜具备可根据平台用户需求定制化风险规则信息库。

h) 知识库应多地备份，以确保网络安全知识数据对外查询、数据更新服务不间断，确保安全设备、态势感知平台、运营人员持续不间断地获取高可用、完全一致的知识库数据；
i) 知识库需根据实时发生的网络安全事件实时更新，并对历史数据定期复盘修正。

5.5.6 情报库管理要求

系统情报库管理要求：

a) 威胁情报内容结构应符合国家标准 GB/T36643-2018，包含 8 个组件：可观测数据、攻击指标、安全事件、攻击活动、威胁主体、攻击目标、攻击方法、应对措施；
b) 情报库应包含不限于关于 IP、DNS、URL 等信息的基础网络情报，关于攻击团体活动信息的攻击团体情报，关于 APT 攻击事件溯源和分析的 APT 分析类情报；
c) 情报库的数据源应包括内部威胁情报挖掘和外部情报挖掘；
d) 威胁情报外部数据来源包含并不限于安全厂商的产品或服务、情报联盟开源数据分享、传统安全设备日志、各类安全技术的输出结果等；
e) 威胁情报库应实现各组织机构间的威胁情报共享，支持主动和被动两种方式与各安全厂商和情报联盟开源数据分享；
f) 主动共享是由系统自身通过监测、扫描等技术定期收集实时获取各组织机构（包括但不限于大型安全厂商与互联网公司、运营商级别的安全公司等）开放的情报数据，与本系统情报库比对并更新情报库；
g) 系统应具备情报共享开放 API；
h) 情报库应多地备份，以确保威胁情报对外查询、数据更新服务不间断，确保安全设备、态势感知平台、运营人员持续不间断地获取高可用、完全一致的威胁情报数据，为情报对运营商网络安全体系的基础支撑作用提供基础保障；
i) 情报库应根据实时发生的威胁事件实时更新有效的情报数据，并对历史情报数据定期复盘修正。

5.5.7 模型库管理要求

模型库管理要求包括：

a) 模型基础环境：智慧城市网络安全态势感知系统应提供算法和数据的存储配置功能、模型算法数据源的数据查询及接口配置功能，提供数据分析相关的系统基础环境和系统组件，为模型研究提供基础环境支撑。
b) 模型基本算法包括但不限于以下几种：
   - 数据预处理算法：标准化，缺失值填充，抽样等；
   - 标准算法：K-Means，决策树，逻辑回归，Apriori，SVM 等；
   - 评估算法：分类算法评估，其他通用算法评估。
c) 模型算法流程应可控、可管理，网络安全态势感知系统应提供算法流程检验、模板配置比对管理、算法流程配置、常用流程模板、自定义流程导入管理等功能，对模型信息、生命周期、模型版本、状态等进行管理。
d) 支撑网络安全态势感知系统数据分析的模型库模型，按照功能归类包括但不限于：碰撞模型、攻击链模型、溯源模型、时间轴模型、命中模型、跟踪模型、处置模型、渲染模型等。
e) 模型应根据实际运行需要不断优化，定期复盘修正。

6 接口要求

本章规定智慧城市网络安全态势感知系统的接口要求。

6.1 网络层接口要求

6.1.1 运营商网络接口

6.1.1.1 5G 移动核心网接口

运营商提供5G移动核心网的服务化接口和非服务化接口。

6.1.1.1.1 服务化接口

服务化接口是NF暴露自身能力的接口，NF通过服务化接口向授权用户提供了一种能力，网络功能可以提供不同的能力，从而为不同的用户提供不同的NF服务。由网络功能提供的每一个NF服务都应该是独立的，可重复使用的。一个业务流程可以通过一系列的NF服务来构建。

服务化接口包括但不限于：

- Nsmf：由SMF暴露的接口；
- Namf：由AMF暴露的接口；
- Nudm：由UDM暴露的接口；
- Npcf：由PCF暴露的接口；
- Nnrf：由NRF暴露的接口；
- Nudr：由UDR暴露的接口；
- Nausf：由AUSF暴露的接口；
- Nnssf：由NSSF暴露的接口；
- Nbsf：由BSF暴露的接口。
- Nlmf：由LMF暴露的接口
- Ngmlc：由GMLC暴露的接口
- Nchf：由CHF暴露的接口

6.1.1.1.2 非服务化接口

5G网络中，控制面功能和用户面功能之间，以及用户面功能之间仍采用非服务化接口，非服务化接口包括：

- N1：UE和AMF之间的接口；
- N2：(R)AN和AMF之间的接口；
- N3：(R)AN和UPF之间的接口；
- N4：SMF和UPF之间的接口；
- N6：UPF和数据网络之间的接口；
- N9：不同UPF之间的接口。

6.1.1.1.3 服务化接口协议栈

5GC中的NF应基于服务化架构。

NF服务是由NF服务生产者通过服务化接口向NF服务用户开发的一种能力。NF可以提供不同的功能，即提供不同的NF服务。由NF提供的多个NF服务之间应该是独立工作、独立管理的。

5GC中的以下控制面接口被定义为服务化接口：

- Namf, Nsmf, Nudm, Nnrf, Nnssf, Nausf, Nnef, Npcf, Nlmf, Ngmlc, Nchf

NF服务框架包括以下机制：

- NF服务注册和去注册：使NRF知道可用的NF实例和支持的服务；
- NF服务发现：使NF服务用户发现提供预期NF服务的NF服务生产者实例；
- NF服务授权：确保NF服务用户被授权访问NF服务生产者提供的NF服务。

服务化接口协议栈如下图所示。

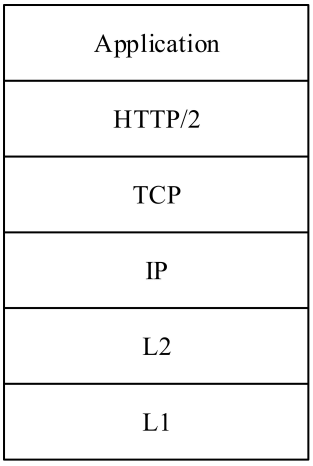

图 6-1 服务化接口协议栈

HTTP/2由IETF RFC 7540标准定义。

6.1.1.2 卫星接入

a) 接口要满足HTTP、RTSP、简单RTP通用协议；
b) 接口应具有在用户节点到播发服务器以及数据服务器到播发服务器的通信中的身份认证功能；
c) 接口应具有检测传输结束的功能；
d) 接入端应能处理收到的卫星传输编码；
e) 数据服务器或用户节点发出一个错误的请求时，播发服务器应能响应返回一个错误代码；
f) 播发服务器应能维护一个包含可用的数据源、数据源网络及播发服务器信息的源信息表，用于收到请求时发送至用户节点。

6.1.2 全域 IPv6 部署

智慧城市网络安全态势感知系统支持全域IPv6部署。

6.1.2.1 平台 IPv6 部署

a) 各业务平台应支持IPv6；
b) 各类接入系统应支持IPv6。

6.1.2.2 网络 IPv6 部署

a) 各类接入网络设备应支持IPv6；
b) 各类网络应支持IPv6。

6.1.2.3 终端 IPv6 部署

根据终端的不同特点，可将终端分为普通移动终端、固网终端、和行业终端三种。移动终端按网络制式可分为GSM终端、WCDMA终端和LTE终端；固网终端包括接入终端(家庭网关)和媒体终端；行业终端包括基于手机卡的行业终端和基于数据卡的行业终端。

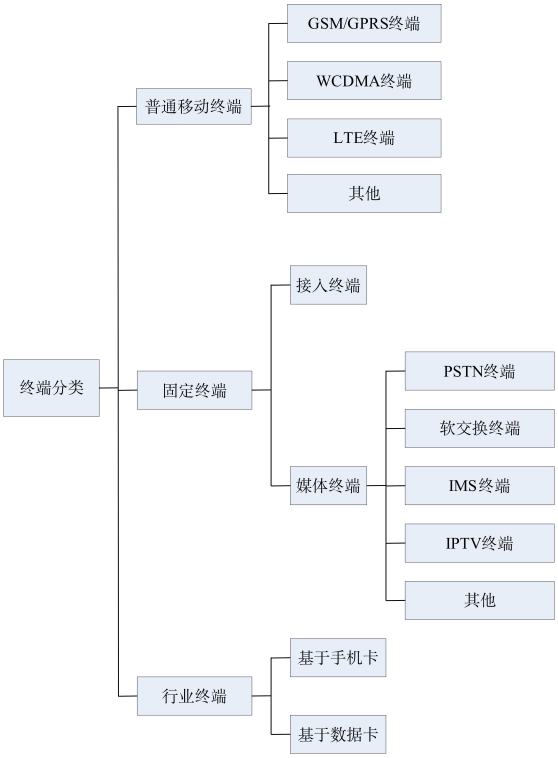

图 6-2 终端分类

a) 各类终端设备支持IPv6协议；
b) 终端上的应用在设计上应支持IPv6协议。

6.2 平台层接口要求

6.2.1 计算中心接口要求

a) 具备与计算中心对接接口，具备从计算中心主动获取数据资产数据、城市资产数据等相关数据能力；
b) 具备支持多种传输协议，如：FTP、SFTP、JDBC、Socket等；
c) 具备接口对接、数据传输认证机制；
d) 具备使用安全传输技术与计算中心接口机进行对接，支持端到端的通信加密；
e) 平台接口具备冗余技术，如多接口机负荷分担、热备等冗余技术，确保通信过程可靠；
f) 平台接口具备续传技术，如出现双方中任意一方中断情况能够保留一定时间的会话和文件，业务恢复后继续传输。

6.2.2 块数据平台接口要求

a) 具备与块数据平台对接，向块数据平台输出威胁情报数据能力，预留数据交换功能；
b) 具备支持多种传输协议，如：FTP、SFTP、JDBC、Socket等；
c) 具备接口对接、数据传输认证机制；
d) 具备使用安全传输技术与块数据平台接口机进行对接，具备端到端的通信加密；
e) 平台接口应具备冗余技术，如多接口机负荷分担、热备等冗余技术，确保通信过程可靠；
f) 平台接口应具备续传技术，如出现双方中任意一方中断情况能够保留一定时间的会话和文件，业务恢复后继续传输；

g) 具备对端接口机状态检测技术，定期对块数据平台接口机工作状态进行检测，评估其接收数据的能力，自动调整数据发送量。

6.2.3 CIM 平台接口要求

a) 系统提供与CIM平台的对接接口，通过该接口实现与CIM平台的数据对接共享；
b) 具备从CIM平台获取时空基础、规划管控、资源调查等相关信息资源的接口能力；
c) 具备从CIM平台获取城市建设、城市管理、城市体检、城市安全、住房、管线、交通、水务、规划、自然资源、工地管理、绿色建筑、社区管理、医疗卫生、应急指挥等领域信息的接口能力。

6.2.4 视频平台接口要求

a) 系统提供与物视频平台的对接接口，通过该接口实现与视频平台的数据对接共享；
b) 具备从视频平台获取相关视频设备的实现采集、录制视频的接口能力。

6.2.5 感知设备\终端平台\物联网平台接口要求

a) 系统提供与感知设备\终端平台\物联网平台的对接接口，通过该接口实现与感知设备\终端平台\物联网平台的数据对接共享；
b) 具备从物联网平台获取主流的物联网通讯协议的接口能力；
c) 具备从感知设备\终端平台\物联网平台获取相关设备\终端状态信息的接口能力。

6.3 应用层接口要求

a) 终端类接口，应包括基础数据、基线数据、流量数据、行为数据：
   - 终端基础数据应包括终端型号、终端名称、终端软件版本、终端编号、终端类型、终端开放端口、终端位置等；
   - 基线数据应至少包括底层对本地数据保密所做的配置、日志传输模块的数据类型配置、流量信息上传类型的配置等信息；
   - 流量数据应包括但不限于IP、端口、数据包类型、数据包大小、设备出口流量等网络信息；
   - 终端行为数据应至少包括终端与平台的连接、APP对终端的控制行为、云端对终端的控制行为等。
b) 业务类接口，包括安全数据、网络流量数据：
   - 安全数据应至少包括安全事件名称、事件类型、事件数量、上报日期、源业务系统（业务领域、平台信息、所在地区等）、源IP等信息；
   - 网络流量数据应至少包括Netflow数据、应用层报文等数据信息。
c) 信息资产数据类接口，包括资产元信息、资产指纹元信息：
   - 资产元信息：包含不限于资产名称、资产域名、资产IP、资产端口、资产类别、资产级别、所属单位、资产描述、采集日期等资产信息；
   - 资产指纹元信息：包含不限于资产端口对应的协议、资产端口对应的应用、设备、设备厂商、操作系统等资产指纹信息。
d) 数据服务类接口
   - 应支持与不同前端数据源、内部不同模块及其它外部系统通过接口进行数据交换；
   - 数据交换的内容应支持不同的类型、字段和格式，其中类型包括日志、告警信息、威胁信息、资产信息、用户信息、脆弱性信息、安全事件等，字段和格式应基于类型进行定义；
   - 应支持为内部不同模块及其它外部系统通过接口进行数据分析；
   - 应支持基于数据分析接口实现算术计算、逻辑关系计算、关联计算等分析能力；
   - 应支持为内部不同模块及其它外部系统通过接口进行联动处置；

- 应支持通过接口进行防护策略的更新、 扫描策略的下发等操作；
- 应具有相应的安全保障机制， 保证数据在传输过程中的保密性、 完整性和可用性。

7 系统安全要求

本章规定智慧城市网络安全态势感知系统的安全要求。

7.1 标识与鉴别

7.1.1 用户标识

应为用户提供唯一的身份标识，同时将用户的身份标识与该用户的所有可审计事件相关联。

7.1.2 用户鉴别

应提供用户鉴别的功能，包括:

a) 在用户访问系统时，应进行身份鉴别；
b) 应采用两种或两种以上的组合鉴别方式；
c) 若采用口令鉴别机制，需对口令进行定期更换并确保口令复杂度；
d) 鉴别数据不能被未授权查阅和修改。

7.1.3 超时锁定

a) 应具有访问超时锁定的功能，在设定的时间段内用户没有任何操作的情况下终止会话，需要再次进行身份鉴别才能重新操作。

7.1.4 鉴别失败处理

a) 当用户连续鉴别失败次数达到设定值后，应采取措施阻止用户的进一步请求，同时为防止恶意锁定，需更高权限解除锁定机制。

7.2 角色管理

本项要求包括:

a) 应能针对不同角色设定不同的访问权限，并按最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权限，形成相互制约关系；
b) 应及时对系统中多余、过期的账户权限进行删除。

7.3 远程管理

若提供远程管理功能，应采取以下措施保证远程管理安全:

a) 应能通过加密的方式来保护远程管理会话内容不被非授权获取；
b) 可设定远程登录的可信主机，如指定 IP 或 MAC 地址。

7.4 数据安全传输

a) 应实现传输安全业务数据和用户与实体身份鉴别数据完整性保护的安全功能；
b) 对平台和管理对象之间传输的用户与实体身份鉴别数据等安全功能相关数据、以及其他重要票据数据，应采用由密码技术支持的保密性保护机制，或具有相应强度的其他安全机制进行保护，确保数据在传输过程中不被泄露和窃取、篡改；
c) 对平台和安全管理对象之间传输的安全业务数据提供完整性保护，可采用由密码技术支持的完整性校验机制或具有相应强度的其他安全机制；

d) 平台组件之间通过网络进行通讯时，应对组件之间相互传输的数据进行保护，保证数据在传送过程中的保密性和完整性。

7.5 安全审计

7.5.1 审计日志生成

应能对以下事件生成审计日志：

a) 管理员的登录事件，包括成功和失败；
b) 因鉴别尝试不成功的次数达到设定值，导致的会话连接终止；
c) 对安全策略的相关操作；
d) 对安全事件的相关操作；
e) 对存储的数据的删除和备份操作；
f) 对前端采集源的相关操作；
g) 对通过主动方式采集数据的前端采集源的策略下发、时钟校准、状态变更等操作；
h) 对安全角色进行增加，删除和属性修改的操作；
i) 管理员的其他操作；
j) 审计日志中应记录事件发生的日期、时间、位置、用户标识、事件描述和结果等内容。若系统提供远程管理功能，还应记录远程登录主机的源地址和目的地址。

7.5.2 审计日志管理

应提供以下审计日志管理功能：

a) 只允许授权管理员访问审计日志；
a) 按条件对审计日志进行查询；
b) 对审计日志进行分析，并生成审计报表。

7.5.3 审计保护

应提供以下审计保护功能：

a) 应保护审计记录，避免受到未预期的删除、修改或覆盖等；
b) 应保护审计进程，避免受到未预期的中断。

7.6 数据保护

a) 应能够保护存储的数据免遭未经授权的读取、删除或修改。
b) 应提供防止存储数据的丢失能力，如：
   - 各类数据存储于掉电非易失性存储介质中；
   - 当存储容量达到阈值时，发出报警信息；
   - 在存储空间耗尽前采取措施，避免数据受到未预期的删除、修改或覆盖等。
c) 应提供以下存储数据的备份功能：
   - 支持备份策略的自定义及数据的自动或手动备份；
   - 通过自动化方式将存储数据进行转存。
d) 应提供以下存储数据的备份功能：
   - 支持对采集组件、数据处理组件、数据存储组件的状态以及数据吞吐量等进行监控；
   - 对数据采集量、持续性及处理失败率等指标进行监控。

7.7 系统报警

7.7.1 报警事件类型

应能在发现异常时根据预先设定的阈值对以下系统事件进行报警:

a) 存储空间、CPU 和内存等达到设定值;
b) 用户鉴别失败的次数达到设定值;
c) 组件监控的异常情况;
d) 授权管理员根据预先自定义的事件分析规则的其他系统事件。

7.7.2 报警消息

报警消息内容应至少包括事件发生的日期、时间、事件主体客体、事件类型和事件描述。

7.7.3 报警方式

报警方式应包含以下方式中的一种或多种，需满足相同事件合并告警能力:

a) 控制台对话框告警;
b) 电子邮件告警;
c) 手机短信告警;
d) 移动终端 APP 消息;
e) 创建工单;
f) 其他方式。

7.8 容错能力

应具有容错能力，在发生硬件故障或软件错误时，能够自动切换，保证功能的可用性。

7.9 系统升级

应定期对系统的组件、漏洞、补丁等信息进行及时更新升级，降低系统自身网络安全风险。

8 新技术应用要求

8.1 空天地一体化网络接入

a) 宜支持对信息基础设施进行实时监控，如，地理位置、存活状态、运行状态等;
b) 宜支持对重要资产数据的流转情况进行实时监控;
c) 宜支持提供更丰富的网络空间态势数据资源;
d) 宜同时具备卫星、3G/4G/5G、WiFi、Internet、物联网等多种网络的接入;
e) 在天、地基混合组网等多系统互联复杂异构环境下，宜具备多域互联场景的统一认证与跨域访问控制能力;
f) 宜兼容TCP/IP、CCSDS、DTN等不同协议体系的接入;
g) 宜支持融合空天地一体化网络中的安全威胁数据，并宜实现对安全威胁数据的关联融合分析和态势预警。

8.2 零信任

a) 宜具备对感知设备/终端的信息获取和身份认证能力，并对感知设备/终端唯一标识;
b) 宜具备持续安全监测和信任评估能力：支持根据访问主体、通信链路、访问客体反馈的信息和外部威胁情报等多源数据进行持续的安全分析，实时评估访问主体当前的信任状态;
c) 宜支持动态访问控制能力：根据安全监测和信任评估结果进行细粒度、动态的访问控制决策;
d) 宜支持提供零信任网关实现对访问流量的代理、鉴权、加密等功能，并依据访问控制决策对访问流量进行通过、阻断等操作。

8.3 AI 分析

a) 建立AI分析模型库，宜支持对不同类型安全威胁进行检测、识别；
b) 宜支持对海量异构多源的威胁数据进行智能化分析；
c) 宜支持对高级可持续威胁（APT）攻击行为的智能检测与识别；
d) 宜支持对病毒、木马、蠕虫、僵尸网络等恶意代码或恶意软件进行智能化检测、识别；
e) 宜支持对钓鱼攻击、恶意URL、SQL注入、XSS攻击等常见Web攻击进行智能化检测；
f) 宜支持对网络流量进行智能化检测，识别恶意加密或异常网络流量行为；
g) 宜支持基于系统日志、用户日志、Web服务器日志等海量日志的异常行为智能化检测；
h) 宜支持对网络信息内容进行智能化分析，识别有害信息、敏感信息；
i) 宜支持对高隐蔽未知网络攻击威胁进行监测识别和攻击分类；
j) 宜支持小样本或零样本场景下对未知攻击行为进行检测识别；
k) 宜支持对海量安全威胁事件进行时空关联分析；
l) 宜支持对跨域、跨网、跨类型的安全威胁事件进行溯源分析；
m) 宜考虑AI算法的迭代更新能力，算法检测识别率、算法的性能、算法的安全性。

8.4 数字孪生

通过数字孪生技术全面感知网络安全态势，对网络安全进行全要素数字化和语义化建模，实现物理网络与数字网络之间的映射，支撑网络安全可视化分析，满足如下要求：

a) 图形化的搭建工具

所见即所得式的配置方式，只需通过拖拉拽，无需掌握专业编程知识，运用现有模板库、组件库即可快速完成网络安全场景搭建，应降低可视化技术门槛。

b) 丰富的可视化组件库

针对不同网络安全场景，宜提供 2D 图表/地图及 3D 图表/地图于一体的可视化组件库来支持网络安全主题建设，提供直观，生动，可交互，可高度个性化定制的数据可视化组件。

c) 多样的酷炫业务主题模板

利用先进的视觉技术渲染、可定制化编辑配置、允许组件联动，深度切合网络安全数据，宜实现图表与数据的映射，展现网络安全业务主题。

d) 支持多种数据源，数据实时更新

网络安全态势感知系统的建设需要汇聚多源异构数据，网络安全的数字孪生建设宜支持数据库、文件、API 接口等多种数据源，数据库类支持 oracle、mysql、sqlServer 等，文件类支持静态 JSON、CSV、Excel 等。

e) 适配性强，适用于各种屏幕

网络安全的可视化展示宜适配大屏端、桌面端、网页端、移动端、一体机等，满足不同业务和应用场景需求。

8.5 可信网络

a) 宜支持网络内生安全体系、确定性IP技术、面向万物互联的新寻址与控制机制等创新技术；
b) 宜支持面向用户侧的网络安全能力；
c) 宜支持主动防御能力，通过网络态势感知手段实现对网络威胁的感知与分析，主动预测网络威胁变种，实现对未知威胁的主动防御。

8.6 安全多方计算

a) 宜具有安全威胁分析能力，内容包含模型恶意计算方的数量和能力等。

8.7 联邦机器学习

联邦机器学习可以避免非授权的数据扩散，解决数据孤岛问题。

a) 宜支持使用区块链等技术建立多方共识机制。

8.8 安全能力开放

安全能力开放包括:

a) 宜支持分析结果数据的上报/下发等推送服务；

b) 宜支持分析模型的迁移使用。

8.9 区块链

a) 区块链的安全态势感知宜具备异常区块监控，异常交易监控，异常地址监控以及智能合约监控的能力。

T/XAZN XXX-XXXX

雄安新区智能城市创新联合会

标准

新型智慧园区评价标准

T/XAZN XXX-2022

河北省雄安新区容城县奥威路 100 号（071700）

雄安新区智能城市创新联合会印刷

网址：www.xaicif.org.cn

202X 年 X 月第一版　202X 年 X 月第一次印刷