|  |  |
| --- | --- |
| ICS | 35.030 |
| CCS | |  | | --- | | D:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T.pngD:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T后面的反斜杠.png CCSCIOT |   L 80 |

     团体标准

T/CCSCIOT 000X—2022

物联网安全态势感知通用技术要求

General technical requirements for the network security situation awareness

（本草案完成时间：2022-11-18）

2022 - 11 - 18发布

2022 - 11 - 18实施

无锡“感知中国”物联网商会  发布

目次

[前言 III](#_Toc119675536)

[1 范围 1](#_Toc119675537)

[2 规范性引用文件 1](#_Toc119675538)

[3 术语和定义 1](#_Toc119675539)

[4 缩略语 2](#_Toc119675540)

[5 概述 2](#_Toc119675541)

[6 基础数据采集层技术要求 3](#_Toc119675542)

[6.1 物联网基础数据采集组件 3](#_Toc119675543)

[6.1.1 采集终端 3](#_Toc119675544)

[6.1.2 采集方式 3](#_Toc119675545)

[6.1.3 采集协议 3](#_Toc119675546)

[6.1.4 采集内容 3](#_Toc119675547)

[6.2 物联网基础数据预处理 4](#_Toc119675548)

[6.2.1 数据筛选 4](#_Toc119675549)

[6.2.2 数据转换 4](#_Toc119675550)

[6.2.3 数据归并 4](#_Toc119675551)

[6.2.4 数据补全 4](#_Toc119675552)

[6.2.5 数据标签 4](#_Toc119675553)

[6.3 物联网协议解析组件 4](#_Toc119675554)

[6.4 物联网基础数据存储组件 4](#_Toc119675555)

[6.4.1 数据格式 4](#_Toc119675556)

[6.4.2 存储内容 4](#_Toc119675557)

[7 业务支撑层技术要求 4](#_Toc119675558)

[7.1 数据服务接口 4](#_Toc119675559)

[7.1.1 数据交换接口 4](#_Toc119675560)

[7.1.2 数据分析接口 4](#_Toc119675561)

[7.1.3 联动处置接口 5](#_Toc119675562)

[7.1.4 接口安全性 5](#_Toc119675563)

[7.2 数据分析组件 5](#_Toc119675564)

[7.2.1 网络攻击分析 5](#_Toc119675565)

[7.2.2 资产风险分析 5](#_Toc119675566)

[7.2.3 异常行为分析 5](#_Toc119675567)

[7.3 联动处置组件 5](#_Toc119675568)

[7.3.1 关联分析 5](#_Toc119675569)

[7.3.2 协同分析 6](#_Toc119675570)

[7.3.3 智能算法 6](#_Toc119675571)

[7.4 接口安全性 6](#_Toc119675572)

[8 应用层技术要求 6](#_Toc119675573)

[8.1 监测预警组件 6](#_Toc119675574)

[8.1.1 监测告警 6](#_Toc119675575)

[8.1.2 安全预警 6](#_Toc119675576)

[8.1.3 分析研判 6](#_Toc119675577)

[8.2 态势展示组件 6](#_Toc119675578)

[8.2.1 整体态势展示 6](#_Toc119675579)

[8.2.2 专题态势展示 7](#_Toc119675580)

[8.2.3 态势报告 8](#_Toc119675581)

[9 资源管理要求 8](#_Toc119675582)

[9.1 策略管理 8](#_Toc119675583)

[9.2 数据处理规则管理 8](#_Toc119675584)

[9.3 数据分析模型管理 8](#_Toc119675585)

[9.4 安全事件管理 8](#_Toc119675586)

[9.5 威胁信息管理 8](#_Toc119675587)

1. 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。

本文件由无锡“感知中国”物联网商会提出并归口。

本文件起草单位：无锡物联网产业研究院

本文件主要起草人：

物联网安全态势感知通用技术要求

* 1. 范围

本文件给出了物联网安全态势感知总体技术框架，规定了物联网安全态势感知总体技术框架中核心组件的通用技术要求。

本文件适用于指导物联网安全态势能力的规划、设计、开发、建设和运营等活动，也可供第三方机构对物联网安全态势感知能力进行评估时提供框架性参考。

* 1. 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 32924-2016 信息安全技术 物联网安全预警指南

GB/T 36635-2018 信息安全技术 物联网安全监测基本要求与实施指南

GB/T 36643-2018 信息安全技术 物联网安全威胁信息格式规范

GB/T 37027-2018 信息安全技术 网络攻击定义及描述规范

* 1. 术语和定义

GB/T 25069、GB/T 32924-2016、GB/T 36635-2018、GB/T 36643-2018和GB/T 37027-2018界定的术语和定义适用于本文件。

威胁 threat

对资产或组织可能导致负面结果的一个事件的潜在源。

[来源：GB/T 25069—2010，2.3.94]

威胁信息 threat information

一种基于证据的知识，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。

注：威胁信息包括上下文、攻击机制、攻击指标、可能影响等信息。

[来源：GB/T 36643—2018，3.3]

物联网安全态势感知 iot(internet of things) security situation awareness

通过采集物联网流量、资产信息、日志、漏洞信息、用户行为、威胁信息等数据，分析物联网访问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、显示能够引物联网态势变化的安全要素，预测物联网安全态势发展趋势。

前端数据源 front-end data source

向物联网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。

画像 profiling

针对某类对象，在多维度上构建其描述性标签属性，并利用这些标签属性，分析对象多方面的特征，抽象概括其全貌。

安全预警 security warning

针对即将发生或正在发生的物联网安全事件、威胁、潜在风险等，提前或及时发出安全警示。

物理空间 physical space

指物联网物理设备所存在的时间空间，构成了整体的物理空间，与互联网的信息空间相对应。

* 1. 缩略语

下列缩略语适用于本文件：

IOT： 物联网（Internet Of Things）

RFID： 射频信号识别类协议通称（Radio Frequency Identification）

NB-IOT: 窄带物联网协议（Narrow Band Internet of Things）

LORA: 远距离无线电（Long Range Radio）

WIFI: 无线保真（Wireless Fidelity）

BLUETOOTH: 蓝牙（Bluetooth）

ZIGBEE: 一种短距低功耗低速物联网物联网协议（Zigbee）

4G/5G: 第4/5代无线通信技术(4/5th Generation mobile communication technology)

CPU：中央处理器（Central Processing Unit）

FTP：文件传输协议（File Transfer Protocol）

FTPS：文件传输协议安全（FTP Secure）

HTTP：超文本传输协议（Hyper Text Transfer Protocol）

HTTPS：安全超文本传输协议（Hyper Text Transfer Protocol over Secure Socket Layer）

IP：网际互连协议（Internet Protocol）

SFTP：安全文件传输协议（Secure FTP）

SNMP：简单网络管理协议（Simple Network Management Protocol）

SSH：安全外壳协议（Secure Shell）

* 1. 概述

物联网安全态势感知总体架构主要包括前端数据源、物联网安全态势感知的核心组件和影响物联网安全态势的要素（如应急处置、安全决策、数据共享等）三部分，其中物联网安全态势感知的核心组件（表现形式可为产品、系统或平台，也可以是不同的功能组件）是实现物联网安全态势感知能力的重要技术保障，但物联网安全态势感知能力的实现同样也依赖于应急处置、安全决策、数据共享等要素。本文件给出了物联网安全态势感知总体技术框架，规定了物联网安全态势感知的核心组件的通用技术要求，不包括总体技术框架中相对独立的前端数据源和影响物联网安全态势的要素（如应急处置、安全决策、数据共享等），具体框图如图1所示。

在物联网安全态势感知能力的建设中，功能组件通常具备较大的伸缩性。依据最大适用性并保证物联网安全态势感知功能完整性原则，本文件所指的物联网安全态势感知核心组件由基础数据采集层（物联网基础数据采集组件、物联网基础数据预处理组件、物联网协议解析组件、物联网基础数据存储组件）、业务支撑层（数据服务接口、数据分析组件、联动处置组件）、应用层（安全检测组件、态势展示组件）三层架构和资源管理组件构成。

各功能组件通过业务支撑层的数据服务接口实现数据对接，其中数据交换接口支持与不同前端数据源、内部不同组件及其它外部系统通过接口进行数据交换，数据分析接口支持为内部不同组件及其它外部系统通过接口进行数据分析，联动处置接口支持为内部不同组件及其它外部系统通过接口进行联动处置；此外接口本身还需满足安全性要求。

物联网安全态势感知核心组件的正常运行离不开资源管理，主要包括策略管理、数据处理规则管理、数据分析模型管理、安全事件管理和威胁信息管理。



1. 物联网安全态势感知总体技术框架
   1. 基础数据采集层技术要求
      1. 物联网基础数据采集组件
         1. 采集终端

物联网基础数据采集组件应支持多样化的智能采集终端，包括传感器采集终端、多媒体采集终端、条码识别终端、二维码识别终端、射频识别终端和生物特征识别终端。

* + - 1. 采集方式

对于不同的前端数据源，物联网基础数据采集组件应支持以下采集方式：

1. 被动获取：被动接收前端数据源发送的数据，数据采集频率可由前端数据源的发送频率决定；
2. 主动采集：主动发起获取前端数据源的数据，数据采集频率可设置；
3. 手动导入：本地手动导入的数据。
   * + 1. 采集协议

物联网基础数据采集组件应能根据应用场景支持两种或两种以上的采集协议进行数据采集，采集协议包括但不限于RFID、NB-IoT、LoRa、WIFI、BlueTooth、ZigBee、4G/5G、Syslog、FTP/FTPS、SFTP、HTTP/HTTPS、SSH、SNMP。

* + - 1. 采集内容

物联网基础数据采集组件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。采集数据类型包括但不限于网络流量、资产信息、日志、漏洞信息、用户行为、告警信息、威胁信息等。

* + 1. 物联网基础数据预处理
       1. 数据筛选

物联网基础数据预处理组件应支持基于既定策略，如必填字段缺失、重要字段格式错误、重复数据等，对采集的原始数据进行筛选。

* + - 1. 数据转换

物联网基础数据预处理组件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。

* + - 1. 数据归并

物联网基础数据预处理组件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。

* + - 1. 数据补全

物联网基础数据预处理组件应支持基于资产库、威胁信息库、地理信息库等对采集的原始数据进行补全，补全的内容可包括设备健康检查、资产属性、关联事件、地理位置等。

* + - 1. 数据标签

物联网基础数据预处理组件应支持根据相关数据字段对采集的原始数据进行标签化处理，标签内容应基于分析需求进行设置，可包括数据可信度、重要程度、数据来源、区域、行业等。

* + 1. 物联网协议解析组件

物联网协议解析组件用于监控设备网络数据协议和流量，应针对主流物联网协议进行识别和解析，支持的协议包括AMQP、MQTT、CoAP、XMPP、Zigbee、LoRa等。

* + 1. 物联网基础数据存储组件
       1. 数据格式

物联网基础数据存储组件应支持存储结构化、半结构化和非结构化等不同格式的数据。

* + - 1. 存储内容

物联网基础数据存储组件应支持存储以下数据内容：

1. 业务数据，如采集的端非流量数据、流量数据、日志数据等；
2. 管理数据，如安全策略数据、用户数据、系统日志、操作日志等；
3. 知识数据，如资产信息、地理信息、漏洞、标签数据、安全事件、威胁信息等。
   1. 业务支撑层技术要求
      1. 数据服务接口
         1. 数据交换接口

数据交换接口应符合以下要求：

1. 支持与不同前端数据源、内部不同组件及其它外部系统通过接口进行数据交换；
2. 数据交换的内容支持不同的类型、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。
   * + 1. 数据分析接口

数据分析接口宜符合以下要求：

1. 支持为内部不同组件及其它外部系统通过接口进行数据分析；
2. 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。
   * + 1. 联动处置接口

联动处置接口宜符合以下要求：

1. 支持为内部不同组件及其它外部系统通过接口进行联动处置；
2. 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。
   * + 1. 接口安全性

数据服务接口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。

* + 1. 数据分析组件
       1. 网络攻击分析

网络攻击分析分为物联网攻击分析和物联网攻击属性分析两种。

1. 物联网攻击分析，攻击类别包括但不限于漏洞利用攻击、拒绝服务攻击、Web应用攻击、数据窃取攻击、恶意邮件攻击、恶意代码攻击、物理攻击等；
2. 物联网攻击属性分析，攻击属性包括但不限于攻击时间、攻击来源、攻击对象、攻击结果、攻击方式等，分析内容包括但不限于攻击的分布情况、攻击频次、危害范围、危害程度等。

网络攻击分析宜符合以下要求：

1. 支持根据时间顺序、攻击来源、攻击对象等对物联网攻击进行关联分析，还原攻击路径；
2. 支持对物联网攻击方进行分析，建立攻击方画像；
3. 支持对物联网攻击的变化趋势、影响范围、危害程度等进行预测。
   * + 1. 资产风险分析

资产风险分析应符合以下要求：

1. 支持结合资产类型、资产位置、资产重要程度、资产脆弱性、资产暴露性、资产可信性、资产是否失陷及威胁信息等分析资产风险，评估资产风险等级；
2. 支持建立资产画像。

资产风险分析宜支持对资产的风险等级、变化趋势等进行预测。

* + - 1. 异常行为分析

异常行为分析应符合以下要求：

1. 支持通过行为基线、关联分析等技术发现用户或实体的异常行为，如：设备物理异常、登录异常、访问异常、操作异常、数据下载异常、可疑域名访问等；
2. 支持建立用户行为画像，包括用户个体行为画像和群体行为画像。

异常行为分析宜支持基于历史数据学习对用户或实体的异常行为进行预测。

* + 1. 联动处置组件
       1. 关联分析

联动处置组件宜采用关联分析，利于数据的深度关联分析对业务组件的数据进行梳理、分析、呈现，自动化与平台中的物联网知识库、节点资产库、物联网漏洞库进行匹配。

1. 物联网知识库，包括物联网威胁情报、主流物联网设备信息、公开物联网漏洞、IOC库等信息。
2. 节点资产库，包括静态属性和动态属性库。
   1. 静态属性库

静态属性库包括已掌握的物联网资产设备的详细属性，包括物联网设备的设备信息、归属、设备位置等重要的资产数据，本功能通过列表进行展示，展示的类别：设备IP、设备端口、国家、省份、通讯协议、厂商、产品、资产类型。

* 1. 动态属性库

动态属性库包括物联网设备的状态、配置、行为等信息，数据形态多样，可以是一条记录、一个数据文件等。动态属性集主要用于设备监控，为异常行为分析提供数据支撑。

1. 物联网漏洞库

物联网漏洞库包括物联网产品、漏洞类型、影响版本、威胁等级、CVE编号、POC、端口等。

* + - 1. 协同分析

联动处置组件宜采用协同分析，充分利用大数据协同分析技术手段，从物联网数据中发现物联网威胁攻击，结合物联网攻击事件、数据分析、可视化分析等技术形成安全状况分析、威胁活动关联分析、安全事件的关联分析等威胁大数据分析能力。

* + - 1. 智能算法

联动处置组件宜采用智能算法，通过智能算法在流量中自动识别出物联网资产，将其归属到机器学习资产库中，在大数据流量中以模型化方式，形成对应设备的详细信息。

* + 1. 接口安全性

数据服务接口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。

* 1. 应用层技术要求
     1. 监测预警组件
        1. 监测告警

监测预警组件应符合以下监测告警要求：

1. 支持基于监测策略对物联网安全状况进行监测，具体监测内容可根据应用场景不同进行筛选；
2. 支持进行监测范围和规则的自定义；
3. 支持基于监测结果和告警策略进行分级别告警；
4. 支持告警方式至少包含平台、短信、邮件、即时通信等中的一种；
5. 支持对告警结果执行相关操作，如忽略、加白名单、联动处置等。
   * + 1. 安全预警

监测预警组件应符合以下安全预警要求：

1. 支持依据设定的流程发布安全预警；
2. 支持进行预警规则和流程的自定义。
3. 支持对安全预警进行分级管理，按照重要程度、影响范围等确定预警级别；
4. 支持不少于两种预警方式，预警方式包括但不限于平台、短信、邮件或即时通信等；
5. 支持通过预警信息与受影响资产信息的关联分析，得出资产名称、资产地址、资产类型等。
   * + 1. 分析研判

监测预警组件应对恶意行为通过关联分析、同源分析等技术手段对物联网端的海量数据进行梳理与挖掘，扩充相关信息。

* + 1. 态势展示组件
       1. 整体态势展示

整体态势展示组件应符合以下要求：

1. 支持对物联网态势整体安全状况用分值或等级等方式进行评估和展示；
2. 支持对不同行业、不同区域、不同业务单元或不同资产等的局部物联网安全状况采用分值或等级等方式进行评估和展示；
3. 支持对不同时间段的物联网安全状况进行评估和展示；
4. 支持采用多种视图展示安全态势，展示视图至少包括雷达图、地理信息图、关联关系图、威胁路径图等中的一种；
5. 根据应用场景不同，支持专题态势、展示内容、展示视图的自定义。
   * + 1. 专题态势展示
          1. 资产态势

资产态势展示组件应符合以下要求：

1. 支持以图表方式展示当前资产的类型和数量；
2. 支持展示资产类型、重要程度、设备地址、开放端口、联网状态等；
3. 支持对资产的安全状况进行评估和展示，包括资产风险等级及具体资产的安全状况描述。
   * + - 1. 流量态势

流量态势展示组件应符合以下要求：

1. 对物联网数据基于协议、时间、源地址、目的地址、前端数据源等进行统计和展示；
2. 统计和展示的范围包括但不限于设备底层流量、网络流量、特定用户流量及特定资产流量等。
   * + - 1. 运行态势

运行态势展示组件应符合以下要求：

1. 支持对资产的资源（CPU、内存、网络、物理状态）使用情况、可用性指标、时间等进行统计和展示；
2. 统计和展示的范围包括但不限于资产重要资产、运行异常资产（如资源使用异常）、所有资产。
   * + - 1. 脆弱性态势

脆弱性态势展示组件应符合以下要求：

1. 支持展示物联网系统中存在的物理损坏、漏洞、弱口令、不安全配置等脆弱性；
2. 支持展示存在安全威胁的资产、漏洞的类型分布、漏洞的级别分布等；
3. 支持基于资产信息统计和展示脆弱性分析结果，包括漏洞资产总数、弱口令资产数、不安全配置资产数及详情等。
   * + - 1. 攻击态势

攻击态势展示组件应符合以下要求：

1. 支持实时获取并展示当前物联网系统的受攻击情况，包括攻击时间、攻击源地址、目的地址、攻击方式、攻击路径等；
2. 支持统计和展示攻击方式分布、攻击时间段、攻击来源分布等。
   * + - 1. 异常行为态势

异常行为态势展示组件应符合以下要求：

1. 支持展示偏离用户行为基线的用户异常行为，如健康监查发现物理攻击，违规或越权访问网络或服务、非授权下载数据等；
2. 支持展示偏离实体访问基线的实体异常行为，实体包括主机操作系统、网络设备、安全设备、数据库、中间件、应用系统等；
3. 支持展示内容包括用户/实体、异常行为对象、异常行为类型、异常行为描述等。
   * + - 1. 安全事件态势

安全事件态势展示组件应符合以下要求：

1. 支持展示物联网系统中发现的安全事件，包括事件时间、事件类型、事件名称、事件等级、事件对象、攻击者地址及意图、事件描述、影响范围等；
2. 支持基于安全事件数量、类型、等级、资产分布等进行安全事件的统计和展示；
3. 支持展示安全事件的处置情况，如基于未处理、处理中、已处理等维度进行统计和展示。
   * + 1. 态势报告
          1. 数据查询

态势报告展示组件应符合以下数据查询要求：

1. 支持对态势相关数据进行查询；
2. 支持基于时间或其它数据字段进行组合查询，条件组合支持与、或等逻辑关系；
3. 支持对查询结果根据字段进行聚合、排序等。
   * + - 1. 统计报表

态势报告展示组件应符合以下统计报表要求：

1. 支持根据数据分析、态势评估的结果生成统计报表并导出；
2. 支持基于指定时间段生成统计报表或生成周期性报表；
3. 支持自定义设置统计视图和报表模板，采用多种视图生成统计报表。
   * + - 1. 分析报告

态势报告展示组件应符合以下分析报告要求：

1. 支持根据数据分析结果生成整体物联网安全状况分析报告并导出；
2. 支持根据数据分析结果生成不同区域、不同业务单元等的局部物联网安全状况分析报告并导出；
3. 支持根据数据分析结果提供修复建议；
4. 支持基于指定时间段产生分析报告或生成周期性分析报告；
5. 支持自定义设置分析报告的模板。
   1. 资源管理要求
      1. 策略管理

资源管理组件应为授权管理员提供策略管理的功能，支持策略的集中管理和自定义设置，包括采集策略、告警策略、监测策略等。

* + 1. 数据处理规则管理

资源管理组件应为授权管理员提供管理数据处理规则的功能，包括新增、删除、修改、查询、启用、停用数据处理规则等。

* + 1. 数据分析模型管理

资源管理组件宜为授权管理员提供数据分析模型的管理，包括新增、删除、修改数据分析模型等。

* + 1. 安全事件管理

资源管理组件应为授权管理员提供安全事件管理的功能，包括建立并动态维护安全事件库，对安全事件进行分类和分级等。

* + 1. 威胁信息管理

资源管理组件应为授权管理员提供威胁信息管理的功能，支持建立威胁信息库并及时更新，信息库的内容至少包括：信息来源、更新时间、内容描述、关联事件、关联设备地址等。

