ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 网络安全态势感知通用技术要求

Information security technology — General technical requirements for the network security situation awareness

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

（本稿完成日期：2021-04-28）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：北京锐安科技有限公司、公安部第三研究所、北京天融信网络安全技术有限公司、新华三技术有限公司、北京神州绿盟科技有限公司、北京奇虎科技有限公司、启明星辰信息技术集团股份有限公司、中移动信息技术有限公司、奇安信科技集团股份有限公司、长扬科技(北京)有限公司、华为技术有限公司、中国科学院信息工程研究所、上海观安信息技术股份有限公司、国家计算机网络应急技术处理协调中心、杭州安恒信息技术股份有限公司、北京中测安华科技有限公司、北京山石网科信息技术有限公司、深信服科技股份有限公司、北京瑞星网安技术股份有限公司、上海工业自动化仪表研究院有限公司、杭州迪普科技股份有限公司、国汽（北京）智能网联汽车研究院有限公司、陕西省网络与信息安全测评中心、北京微智信业科技有限公司、蓝盾信息安全技术股份有限公司、杭州立思辰安科科技有限公司、海信集团控股股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京威努特技术有限公司、中国电子信息产业集团有限公司第六研究所、厦门服云信息科技有限公司、中国民航大学、国能信息技术有限公司网络与信息安全中心、北京安博通科技股份有限公司

本标准主要起草人：陈妍、李京春、李斌、顾健、王龑、杨洪起、张屹、吕明、郭旭、汪义舟、陶夏微、郑亮、吴天昊、张华涛、聂桂兵、刘玉岭、吴槟、陈宇耀、李旋、刘星材、孙默、王涛、饶毓、刘晨、叶荣军、杨帆、张宁、刘强、刘慧芳、崔婷婷、权小文、张淯易、刘志磊、石凌志、李亚玲、苗维杰、何春根、周景贤、王许培

信息安全技术 网络安全态势感知通用技术要求

1 范围

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

本文件适用于指导网络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网络安全态势感知能力进行评估时提供框架性参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 网络安全预警指南

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

GB/T 36643-2018 信息安全技术 网络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

3 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界定的以及下列术语和定义适用于本文件。

3.1

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]

3.2

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]

3.3

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。

3.4

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。

3.5

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。

3.6

安全预警 security warning

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

4 缩略语

下列缩略语适用于本文件：

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）

5 概述

网络安全态势感知总体架构主要包括前端数据源、网络安全态势感知的核心组件和影响网络安全态势的要素（如应急处置、安全决策、数据共享等）三部分，其中网络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）是实现网络安全态势感知能力的重要技术保障，但网络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。本文件给出了网络安全态势感知总体技术框架，规定了网络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网络安全态势的要素（如应急处置、安全决策、数据共享等）。

在网络安全态势感知能力的建设中，功能模块通常具备较大的伸缩性。依据最大适用性并保证网络安全态势感知功能完整性原则，本文件所指的网络安全态势感知核心组件由数据汇聚、数据分析、态势展示、监测预警、数据服务接口、资源管理等必不可少的功能模块构成，具体框图如图1所示。

数据汇聚包括数据采集、数据预处理和数据存储。数据分析包括网络攻击分析、异常行为分析和资产风险分析。态势展示包括整体态势展示、专题态势展示和态势报告。监测预警包括监测告警和安全预警。各功能模块通过数据服务接口实现数据对接，因此数据服务接口包括数据交换接口、数据分析接口

和联动处置接口；其中数据交换接口支持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，数据分析接口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，联动处置接口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；此外接口本身还需满足安全性要求。网络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。

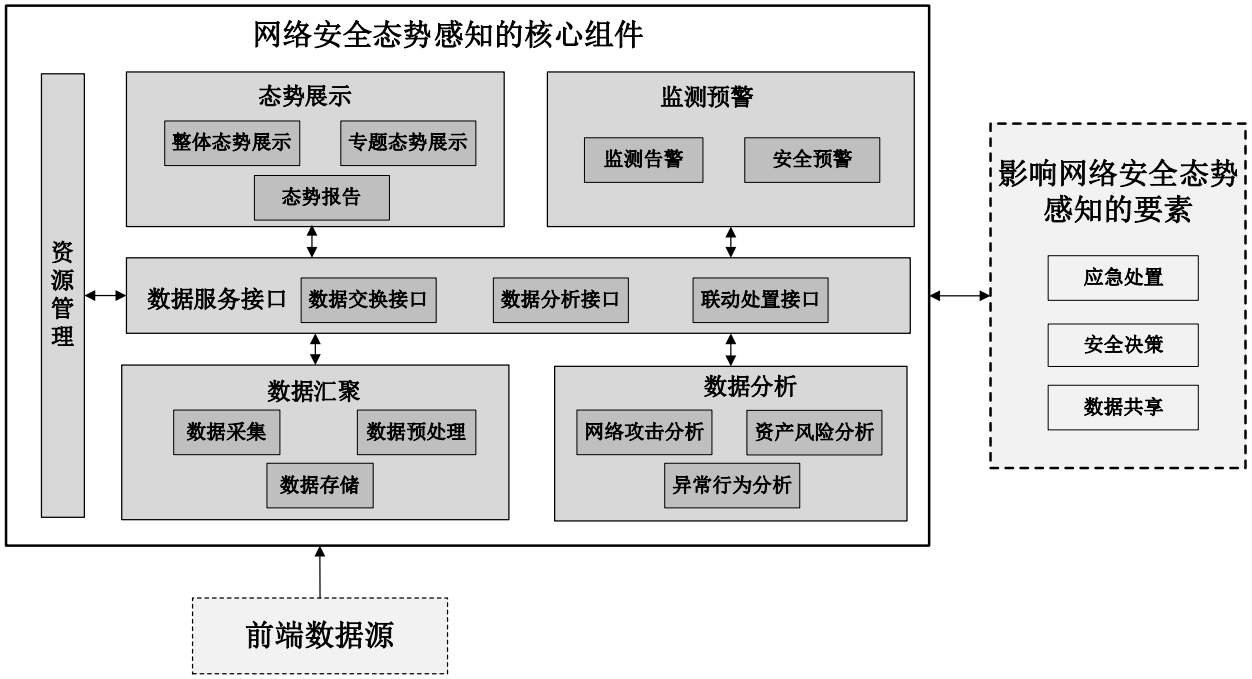

图1 网络安全态势感知总体技术框架

6 安全技术要求

6.1 数据汇聚要求

6.1.1 数据采集

6.1.1.1 采集方式

对于不同的前端数据源，数据汇聚组件应支持以下采集方式：

a) 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；
b) 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。
c) 手动导入：本地手动导入的数据。

6.1.1.2 采集协议

数据汇聚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Syslog、FTP/FTPS、SFTP、HTTP/HTTPS、SSH、SNMP。

6.1.1.3 采集内容

数据汇聚组件：

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；

b) 应支撑的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。

6.1.2 数据预处理

6.1.2.1 数据筛选

数据汇聚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。

6.1.2.2 数据转换

数据汇聚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。

6.1.2.3 数据归并

数据汇聚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。

6.1.2.4 数据补全

数据汇聚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，补全的内容可包括资产属性、关联事件、地理位置等。

6.1.2.5 数据标签

数据汇聚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。

6.1.3 数据存储

6.1.3.1 数据格式

数据汇聚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。

6.1.3.2 存储内容

数据汇聚组件：

a) 应支持存储业务数据，如采集的流量数据、日志数据等；
b) 应支持存储管理数据，如的安全策略数据、用户数据、系统日志、操作日志等；
c) 应支持存储知识数据，如资产信息、地理信息、漏洞、标签数据、安全事件、威胁信息等。

6.2 数据分析要求

6.2.1 网络攻击分析

数据分析组件：

a) 应支持网络攻击分析，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、恶意代码攻击等；

b) 应支持网络攻击属性分析，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；
c) 宜支持根据时间顺序、攻击来源、攻击对象等对网络攻击进行关联分析，还原攻击路径；
d) 宜支持对网络攻击方进行分析，建立攻击方画像；
e) 宜支持对网络攻击的变化趋势、影响范围、危害程度等进行预测。

6.2.2 资产风险分析

数据分析组件：

a) 应支持结合资产类型、资产位置、资产重要程度、资产脆弱性、资产是否失陷及威胁信息等分析资产风险，评估资产风险等级；
b) 应支持建立资产画像；
c) 宜支持对资产的风险等级、变化趋势等进行预测。

6.2.3 异常行为分析

数据分析组件：

a) 应支持通过行为基线、关联分析等技术发现用户或实体的异常行为，如：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；
b) 应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；
c) 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。

6.3 态势展示要求

6.3.1 整体态势展示

态势展示组件：

a) 应支持对网络的整体安全状况用分值或等级等方式进行评估和展示；
b) 应支持对不同行业、不同区域、不同业务单元或不同资产等的局部网络安全状况采用分值或等级等方式进行评估和展示；
c) 应支持对不同时间段的网络安全状况进行评估和展示；
d) 应支持采用多种视图展示安全态势，展示视图至少包括以下一种：雷达图、地理信息图、关联关系图、威胁路径图等；
e) 根据应用场景不同，应支持专题态势、展示内容、展示视图的自定义。

6.3.2 专题态势展示

6.3.2.1 资产态势

态势展示组件：

a) 应支持以图表方式展示当前资产的类型和数量；
b) 应支持展示资产类型、重要程度、IP地址、开放端口、联网状态等；
c) 应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。

6.3.2.2 流量态势

态势展示组件：

a) 应支持对流量数据基于协议、时间、源IP地址、目的IP地址、前端数据源等进行统计和展示；
b) 应支持统计和展示的范围至少包括互联网流量、特定用户流量及特定资产流量等。

6.3.2.3 运行态势

态势展示组件：

a) 应支持对资产的资源（如CPU、内存、网络）使用情况、可用性指标、时间等进行统计和展示；
b) 应支持统计和展示的范围至少包括重要资产、运行异常资产（如资源使用异常）等。

6.3.2.4 脆弱性态势

态势展示组件：

a) 应支持展示网络中存在的漏洞、弱口令、不安全配置等脆弱性；
b) 应支持展示存在漏洞的资产、漏洞的类型分布、漏洞的级别分布等；
c) 应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。

6.3.2.5 攻击态势

态势展示组件：

a) 应支持实时获取并展示当前网络的受攻击情况，包括攻击时间、攻击源IP地址、目的IP地址、攻击方式、攻击路径等；
b) 应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。

6.3.2.6 异常行为态势

态势展示组件：

a) 应支持展示偏离用户行为基线的用户异常行为，如违规或越权访问网络或服务、非授权下载数据等；
b) 应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；
c) 应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。

6.3.2.7 安全事件态势

态势展示组件：

a) 应支持展示网络中发现的安全事件，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IP地址及意图、事件描述、影响范围等；
b) 应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；
c) 应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。

6.3.3 态势报告

6.3.3.1 数据查询

态势展示组件：

a) 应支持对态势相关数据进行查询；
b) 应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；
c) 应支持对查询结果根据字段进行聚合、排序等。

6.3.3.2 统计报表

态势展示组件：

a) 应支持根据数据分析、态势评估的结果生成统计报表并导出；
b) 应支持基于指定时间段生成统计报表或生成周期性报表；
c) 应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。

6.3.3.3 分析报告

态势展示组件：
a) 应支持根据数据分析结果生成整体网络安全状况分析报告并导出；
b) 应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网络安全状况分析报告并导出；
c) 应支持根据数据分析结果提供修复建议；
d) 应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；
e) 应支持自定义设置分析报告的模板。

6.4 监测预警要求

6.4.1 监测告警

监测预警组件：
a) 应支持基于监测策略对网络安全状况进行监测，具体监测内容可根据应用场景不同进行筛选；
b) 应支持进行监测范围和规则的自定义；
c) 应支持基于监测结果和告警策略进行分级别告警；
d) 告警方式应至少包含以下一种：平台、短信、邮件、即时通信等；
e) 应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。

6.4.2 安全预警

监测预警组件：
a) 应支持依据设定的流程发布安全预警；
b) 应支持进行预警规则和流程的自定义。
c) 应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；
d) 应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；
e) 应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、IP地址、资产类型等。

6.5 数据服务接口要求

6.5.1 数据交换接口

数据服务接口组件：
a) 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；
b) 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。

6.5.2 数据分析接口

数据服务接口组件：
a) 宜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；
b) 宜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。

6.5.3 联动处置接口

数据服务接口组件：

a) 宜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；

b) 宜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。

6.5.4 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。

6.6 资源管理要求

6.6.1 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。

6.6.2 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。

6.6.3 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。

6.6.4 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。

6.6.5 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IP地址等。