ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 42453—2023

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 network security situation awareness

2023-03-17 发布　　2023-10-01 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。

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专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：公安部第三研究所、北京锐安科技有限公司、国家信息技术安全研究中心、北京天融信网络安全技术有限公司、中国信息安全测评中心、北京奇虎科技有限公司、新华三技术有限公司、奇安信科技集团股份有限公司、启明星辰信息技术集团股份有限公司、长扬科技(北京)股份有限公司、北京神州绿盟科技有限公司、深信服科技股份有限公司、中国科学院信息工程研究所、北京山石网科信息技术有限公司、华为技术有限公司、杭州安恒信息技术股份有限公司、腾讯云计算(北京)有限责任公司、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、中电长城网际系统应用有限公司、西安交大捷普网络科技有限公司、杭州中电安科现代科技有限公司、陕西省网络与信息安全测评中心、中国民航大学、中科国昱(合肥)科技有限公司、北京威努特技术有限公司、远江盛邦(北京)网络安全科技股份有限公司。

本文件主要起草人：陈妍、李京春、顾健、李雪莹、李斌、张屹、万晓兰、李军华、吕明、汪义舟、陶智、刘晨、万月亮、刘玉岭、张永皓、孙默、张华涛、聂桂兵、陶夏溦、刘慧芳、王涛、刘鹏、杨帆、何建锋、苗维杰、查正朋、周景贤。

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技术框架，规定了该框架中核心组件的通用技术要求。

本文件适用于网络安全态势感知产品、系统或平台等的规划、设计、开发、建设和测评。

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—2022 信息安全技术 术语

GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范

GB/T 28517—2012 网络安全事件描述和交换格式

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

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—2022 界定的以及下列术语和定义适用于本文件。

3.1

威胁 threat

可能对系统或组织造成危害的不期望事件的潜在因素。

[来源：GB/T 25069—2022，3.628]

3.2

威胁信息 threat information

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，有修改]

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、告警信息、威胁信息等数据，分析和处理网络行为及用户行为等因素，掌握网络安全状态，预测网络安全趋势，并进行展示和监测预警的活动。

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。