ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 44886.3—2025

网络安全技术　网络安全产品互联互通 第3部分:告警信息格式

Cybersecurity technology—Cybersecurity product interconnectivity—Part 3:Alarm information format

2025-12-02 发布　　2026-07-01 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。

本文件是GB/T 44886《网络安全技术　网络安全产品互联互通》的第3部分。GB/T 44886已发布了以下部分：

——第1部分：框架；

——第2部分：资产信息格式；

——第3部分：告警信息格式。

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。

本文件由全国网络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：国家信息中心、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、清华大学、公安部第三研究所、中国科学院信息工程研究所、中国信息安全测评中心、北京国信京宁信息安全科技有限公司、北京赛西科技发展有限责任公司、北京江民新科技术有限公司 、北京天融信网络安全技术有限公司、山东省大数据中心、宁波市数据服务中心、亚信科技(成都)有限公司、北京升鑫网络科技有限公司、北京神州绿盟科技有限公司、深信服科技股份有限公司、杭州安恒信息技术股份有限公司、安天科技集团股份有限公司、奇安信网神信息技术(北京)股份有限公司、长扬科技(北京)股份有限公司、新疆维吾尔自治区数据资源和政务服务中心、北京邮电大学、中国雄安集团数字城市科技有限公司、山东中测信息技术有限公司。

本文件主要起草人：刘蓓、闫桂勋、禄凯、陈韵然、程浩、张卫博、杨莹、朱雪峰、郭红、许玉娜、包莉娜、孙彦、刘楠、赵新强、张涛、李广恺、段斯斯、崔牧凡、陈妍、刘玉岭、梁利、高洋、李烨昊、隋笑、严冬、寇增杰、刘洞宾、卞建超、郭英华、杨信磊、袁志千、文博、何茂根、孙凌、林明峰、苗佳艺、丁宇征、白荣华、赵华、马向亮、姚凯旋、吴博。

引　言

GB/T 44886《网络安全技术　网络安全产品互联互通》拟由以下部分构成。

——第1部分：框架。目的在于明确网络安全产品互联互通应用场景，提出互通建设思路。

——第2部分：资产信息格式。目的在于提出网络安全产品互联互通时的资产描述。

——第3部分：告警信息格式。目的在于有效整合网络安全产品报送的告警信息，提高告警应急处置效率。

——第4部分：威胁信息格式。目的在于统一网络安全产品及各组织威胁信息共享格式。

——第5部分：行为信息格式。目的在于促进网络安全产品行为信息的分析利用。

——第6部分：功能接口。目的在于高效整合网络安全信息，促进网络安全产品功能协同。

网络安全技术　网络安全产品互联互通
第3部分:告警信息格式

1　范围

本文件给出了网络安全产品互联互通时告警分类和告警信息的描述格式。

本文件适用于网络安全产品互联互通的设计、开发、应用和测试。

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

3　术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

网络安全产品互联互通　cybersecurity product interconnectivity

通过统一的网络安全信息描述和功能接口定义,有效共享网络安全产品感知或产生的信息,协同不同网络安全产品的功能,支撑监测预警、信息共享、应急响应、态势感知等应用,提升网络安全防护能力和网络安全事件处置效率的一种机制。

[来源:GB/T 44886.1—2024,3.2]

3.2

告警信息　alarm information

网络安全产品依据设定的规则,对采集到的网络安全信息自动进行规则匹配、归并、分析等活动后产生的警示信息。

4　缩略语

APT:高级持续性威胁(Advanced Persistent Threat)

CPU:中央处理器(Central Processing Unit)

IP:网际互连协议(Internet Protocol)

SYN:同步序列编号(Synchronize Sequence Numbers)

UDP:用户数据报协议(User Datagram Protocol)

URL:统一资源定位符(Uniform Resource Locator)