ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 44886.3-2025

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

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

Issued on: December 2, 2025 **Implemented on: July 1, 2026**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part

1.Structure and Drafting Rules of Standardization Documents". Drafting. This document is Part 3 of GB/T 44886 "Network Security Technology - Interoperability of Network Security Products". GB/T 44886 has been issued. The following parts were laid out.

2.Asset Information Format;

3.Alarm Message Format Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying

patents. This document was proposed and is under the jurisdiction of the National Cybersecurity Standardization Technical Committee (SAC/TC260). This document was drafted by: the State Information Center, the China Electronics Technology Standardization Institute, and the National Computer Network Emergency Response Technical Team/Coordination Center. Center, National Information Technology Security Research Center, Tsinghua University, Third Research Institute of the Ministry of Public Security, Institute of Information Engineering of the Chinese Academy of Sciences, China Information Technology Center Information Security Evaluation Center, Beijing Guoxin Jingning Information Security Technology Co., Ltd., Beijing CESI Technology Development Co., Ltd., Beijing Jiangmin New Technology Co., Ltd., Beijing Topsec Network Security Technology Co., Ltd., Shandong Provincial Big Data Center, Ningbo Data Service Center, AsiaInfo Technology (Chengdu) Co., Ltd., Beijing Shengxin Network Technology Co., Ltd., Beijing Shenzhou Green Alliance Technology Co., Ltd., Sangfor Technologies Inc. The company, Hangzhou Anheng Information Technology Co., Ltd., Antiy Labs Technology Group Co., Ltd., and Qi An Xin NetSec Information Technology (Beijing) Co., Ltd. Limited Liability Company, Changyang Technology (Beijing) Co., Ltd., Xinjiang Uygur Autonomous Region Data Resources and Government Service Center, Beijing University of Posts and Telecommunications, China Xiong'an Group Digital City Technology Co., Ltd. and Shandong Zhongce Information Technology Co., Ltd. The main drafters of this document are. Liu Bei, Yan Guixun, Lu Kai, Chen Yunran, Cheng Hao, Zhang Weibao, Yang Ying, Zhu Xuefeng, Guo Hong, Xu Yuna, and Bao Lina. Sun Yan, Liu Nan, Zhao Xinqiang, Zhang Tao, Li Guangkai, Duan Sisi, Cui Mufan, Chen Yan, Liu Yuling, Liang Li, Gao Yang, Li Yehao, Sui Xiao, Yan Dong Kou Zengjie, Liu Dongbin, Bian Jianchao, Guo Yinghua, Yang Xinlei, Yuan Zhiqian, Wen Bo, He Maogen, Sun Ling, Lin Mingfeng, Miao Jiayi, Ding Yuzheng, Bai Ronghua, Zhao Hua, Ma Xiangliang, Yao Kaixuan, Wu Bo.

GB/T 44886 "Network Security Technology - Interoperability of Network Security Products" is proposed to consist of the following parts.

1.Framework. The purpose is to clarify the application scenarios for interoperability of network security products and propose an approach to interoperability construction.

2.Asset Information Format. The purpose is to provide an asset description for interoperability of network security products.

3.Alarm Message Format. The purpose is to effectively integrate alarm information reported by network security products and improve alarm emergency response. Efficiency.

4.Threat Information Format. The aim is to standardize the threat information sharing format for cybersecurity products and across organizations.

5.Behavioral Information Format. The purpose is to facilitate the analysis and utilization of behavioral information from cybersecurity products.

6.Functional Interfaces. The aim is to efficiently integrate network security information and

promote the synergy of network security product functions. Interoperability of network security technologies and network security products Part

1 Scope

GB/T 44886.3-2025 is the Chinese national standard covering the format in which one security product tells another that something happened - the fields of an alarm, the severity and confidence, the affected asset and the evidence, so that a SIEM can consume the output of vendors that never spoke to each other. Part 3 of the series, first edition, with Part 2 on asset information format. It was issued on 2 December 2025 and has been in force since 1 July 2026, as a first edition. The document is under the responsibility of the Standardization Administration of China. This page is published from the official record of the 2025 edition; the clause text of a standard this recent is not yet in circulation, and the figures, limits and tables it contains are those of the document itself, delivered in full with the English translation.

This document provides the alarm classification and alarm information description format when network security products are interconnected. This document applies to the design, development, application, and testing of network security product interoperability.

2 Normative references

The contents of the following documents, through normative references within the text, constitute essential provisions of this document. Dated citations are not included. For references to documents, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies. This document.

GB/T 25069 Information Security Technical Terminology

3 Terms and Definitions

The terms and definitions defined in GB/T 25069 and the following terms and definitions apply to this document.

3.1 By unifying network security information descriptions and functional interface definitions, information perceived or generated by network security products can be effectively shared, enabling collaborative efforts. Similar to the functions of network security products, it supports applications such as monitoring and early warning, information sharing, emergency response, and situational awareness, thereby enhancing network security protection capabilities. A mechanism to improve the efficiency of handling cybersecurity incidents. [Source: GB/T 44886.1-2024, 3.2]

3.2 Alarm information Network security products automatically perform rule matching,

merging, and analysis on the collected network security information according to predefined rules. The generated warning message.