ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 44886.1-2024

Cybersecurity technology-Cybersecurity product interconnectivity-Part 1: Framework

网络安全技术 网络安全产品互联互通 第1部分：框架

Issued on: November 28, 2024 **Implemented on: June 1, 2025**

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

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting is required.

This document is Part 1 of GB/T 44886 "Cybersecurity Technology and Cybersecurity Product Interoperability".

The following parts have been published. Part 1: Framework. - Please note that some of the contents of this document may involve patents. The issuing organization of this document does not assume the responsibility for identifying patents.

This document was proposed and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC 260).

This document was drafted by: Beijing CESI Technology Development Co., Ltd., National Information Center, National Computer Network Emergency Response Technical Processing Co., Ltd.

Coordination Center, China Electronics Standardization Institute, Institute of Information Engineering, Chinese Academy of Sciences, China Mobile Communications Group Co., Ltd., Beijing University, China Unicom, Tianyi Security Technology Co., Ltd., Shenyang Neusoft System Integration Engineering Co., Ltd., Hangzhou Ahnheng Information Technology Co., Ltd., Sangfor Technologies Co., Ltd., Beijing Topsec Network Security Technology Co., Ltd., Beijing Shenzhou Green Alliance Technology Co., Ltd., Beijing Shengxin Network Technology Co., Ltd., Antiy Technology Group Co., Ltd., China Radio and Television Metrology and Testing Group Co., Ltd.

Co., Ltd., Huawei Technologies Co., Ltd., and Qi'anxin Technology Group Co., Ltd.

The main drafters of this document are: Yang Jianjun, Yao Xiangzhen, Zhao Xinqiang, Sun Yan, Xu Yuna, Liu Bei, Li Jianqiang, Chen Yunran, Jiang Zhengwei, Qiu Qin, Xie Anming, Wang Zhiming, Wang Yingxin, Yan Dong, Sun Ling, Chen Xing, An Gaofeng, He Maogen, Yan Guixun, Bian Jianchao, Tang Di, Sun Keren, Wang Xizi, Zhang Weibo, Yao Yepeng, Li Qiang, and Ding Yuzheng.

Introduction

In recent years, national cybersecurity-related laws, regulations, and policy documents have been issued one after another to establish and improve a unified and efficient cybersecurity risk monitoring system.

The establishment of a cross-departmental and cross-industry efficient cybersecurity protection system has become a key step in strengthening the country's cybersecurity capabilities.

The focus of network security barrier work.

The interconnection and interoperability of network security products is a necessary condition for building efficient and coordinated network security protection capabilities. Standardization is the key to achieving network security product GB/T 44886 "Network Security Technology Network Security Product Interconnection" is a guide for network security products.

The basic and general standards for interconnection construction are planned to consist of six parts.

Part 1: Framework. The purpose is to clarify the application scenarios of network security product interconnection and interoperability and propose ideas for interoperability construction. - Part 2: Asset Information Format. The purpose is to propose asset descriptions when network security products are interconnected. - Part 3: Alarm Information Format. The purpose is to effectively integrate the alarm information reported by network security products and improve the emergency response of alarms. Setting efficiency.

Part 4: Threat Information Format. The purpose is to unify the threat information sharing format of network security products and organizations. - Part 5: Behavior Information Format. The purpose is to facilitate the analysis and utilization of network security product behavior information. - Part 6: Functional Interface. The purpose is to efficiently integrate network security information and promote the functional coordination of network security products.

Cybersecurity technologies Cybersecurity product interoperability Part 1: Framework

1 Scope

This document establishes the interoperability framework for network security products and provides interoperability functions and information.

This document is applicable to guiding the design, development and application of network security products.

2 Normative references

GB/T 20986-2023

GB/T 25066

3 Terms and definitions

The terms and definitions defined in GB/T 25066 and the following apply to this document.

3.1 cybersecurity product

Software, hardware, or a combination thereof specifically used to ensure network security.

3.2 Cybersecurity product interconnectivity

Through unified network security information description and functional interface definition, the information perceived or generated by network security products can be effectively shared, and different With the functions of network security products, it supports monitoring and early warning, information sharing, emergency response, situation awareness and other applications, and improves network security protection capabilities.

A mechanism to improve the capacity and efficiency of handling cybersecurity incidents.

3.3 Interconnect function

The security functions used by network security products to achieve interconnection and interoperability and their implementation methods.

3.4 Interconnect information

Network security products support the interconnection and interoperability of the provided data types, structures and data formats.

4 Abbreviations

The following abbreviations apply to this document.

APT. Advanced Persistent Threat IP. Internet Protocol TCP. Transmission Control Protocol

WEB. World Wide Web